1. Release Note

1.1. 本章について

- 本章は、Senju DevOperation Conductor Extension Pack について、マニュアルの補足事項、制限事項、その他利用上での注意事項等の情報をまとめたものです。
- 本章は、Senju DevOperation Conductor Extension Pack をインストールまたは利用する前に一読して下さい。なお、万一ご不審な点や誤り、記載漏れなど、お気づきの点がございましたら弊社までお知らせ下さい。
- 本章に記載した内容は予告無く変更することがあります。
- 本章の内容の一部または全部を無断でコピーすることは法律で禁止されています。

1.1.1. 登録商標表記について

- 「Senju DevOperation Conductor」「Senju Operation Conductor」「Senju Enterprise Navigator」「eXsenju」「EX千手/EXSENJU」「千手/SENJU」「e-千手/e-SENJU」および「セキュア・キューブ/SecureCube」は（株）野村総合研究所の登録商標です。
- Amazon Web Services、“Powered by Amazon Web Services”ロゴ、[およびかかる資料で使用されるその他のAWS商標]は、米国その他の諸国における、Amazon.com, Inc.またはその関連会社の商標です。
- Google、Google Cloud、Google Cloud Platform、および、GCP は、Google LLC の商標です。
- IBM、IBM ロゴ、および ibm.com は、世界の多くの国で登録された International Business Machines Corp. の商標です。他の製品名およびサービス名等は、それぞれ、IBM または各社の商標である場合があります。現時点での IBM商標リストについては、http://www.ibm.com/legal/copytrade.shtml の『Copyright and trademark information』をご覧ください。
- UNIXは、X/Open Company Limitedが独占的にライセンスしている米国ならびに他の国における登録商標です。
- Linuxは、Linus Torvalds氏の登録商標です。
- Windows、Windows Server、Azureは、米国Microsoft Corporationの米国及びその他の国における登録商標または商標です。
- OracleとJavaは、Oracle Corporation 及びその子会社、関連会社の米国及びその他の国における登録商標です。文中の社名、商品名等は各社の商標または登録商標である場合があります。
- Dockerは、Docker,Inc.の米国およびその他の国における登録商標または商標です。
- Kubernetesは、The Linux Foundationの米国およびその他の国における登録商標または商標です。
- OpenShiftは、Red Hat, Inc.の米国およびその他の国における登録商標または商標です。
- その他、本誌で引用の製品名・会社名はそれぞれの会社の商標、もしくは登録商標です。なお、本誌中では、™、® マークなどは明記していません

1.1.2. 関連資料

本章を参照するにあたっては、以下の各マニュアルなどを参照して下さい。

- 統合運用管理ツール「Senju DevOperation Conductor」Extension Pack Cloud Monitoring
- 統合運用管理ツール「Senju DevOperation Conductor」Extension Pack Job Scheduler Cloud
- 統合運用管理ツール「Senju DevOperation Conductor」Extension Pack Container Monitoring

1.2. Extension Packの概要

Senju DevOperation Conductor Extension Pack はSenju/DCにおいてクラウド／コンテナ関連の機能を拡張する追加適用パッケージです。下記のような機能を提供します。

- クラウド監視(AWS/Azure/Google Cloud/OCI/IBM Cloud) は Amazon Web Services(AWS)、Microsoft の Azure、Google Cloud、Oracle Cloud Infrastructure(OCI)、およびIBM Cloudと連携させることができます。この連携により、Senju/DCのモニタリング機能からクラウドサービスを監視することができるようになります。
- Job Scheduler for Cloud はAmazon Web Services(AWS)のElastic MapReduce、Lambda Functionの機能、AzureのDurable Functionsの機能、Google CloudのCloud Functionsの機能、Oracle Cloud Infrastructure(OCI)のCloud Functionsの機能とSenju/DCのジョブスケジュール機能を連携させることができます。この連携により、Senju/DCのジョブスケジュール機能からAWS/Elastic MapReduceのジョブフロー、Lambda Function、Azure/Durable Functions、Google Cloud Functions、OCI/Oracle Functionsを実行および監視することができるようになります。
- コンテナ監視(Docker/Kubernetes/Podman/OpenShift)エクステンション は Docker、Kubenetes、Podman および OpenShift などのコンテナ運用基盤について、Senju DevOperation Conductor のモニタリング機能を連携させることができます。この連携により、Senju DevOperation Conductorのモニタリング機能からDocker、Kubernetes、PodmanおよびOpenShiftを監視することができるようになります。

1.3. 各Extension Packの主な新機能

1.3.1. Extension Pack 2312の新機能

- Oracle Cloud Infrastructureリソース一覧取得機能

  Oracle Cloud Infrastructure（以下、OCI）上に作成されたリソースの一覧を取得し、プローブに収集してDevOpsポータルのファイル参照機能と連携できる以下の監視項目を追加しました。ファイル取得や情報の持ち出しに制約がある環境において、問い合わせ時等リソースのOCIDを確認したい場面で、DevOpsポータルから参照が可能となります。

  - OCI：リソース一覧取得

- Oracle Analytics Cloud監視機能

  OCIのOracle Analytics Cloudに対して、以下の監視項目を追加しました。インスタンスの異常を早期検知することにより、迅速な復旧対応が可能となります。

  - OCI：Analytics インスタンス状態

- Docker コンテナログ監視機能

  Dockerのコンテナログをプローブに収集してログ監視と連携できる機能を追加しました。コンテナの増減により流動的に作成されるログを追従して監視することが可能となります。

  - Docker：コンテナログ監視

- VMware連携機能 Extension Packによる提供

  従来Senju/DCの機能として提供していたVMware連携を、Extension Packによる提供方式に変更しました。これにより、Senju/DCのバージョンアップを行わずとも最新化された機能を使用することが可能となります。また、連携方式の刷新により性能が向上し、VMware vSphere SDK for Perlのインストールが不要となります。

- ログ取得監視項目におけるファイル名指定パラメータ追加

  各パブリッククラウドのログ情報/アナウンスメント情報取得等のプローブにログファイルを書き出す機能において、出力ファイル名をユーザーが指定できるようにパラメータを追加しました。

- Azure連携監視項目におけるディメンション指定パラメータ追加

  Azure連携監視項目において、ディメンションを指定して監視ができるようにパラメータを追加しました。ディメンションで監視対象を絞り込むことにより、より細分化された特定の範囲での異常検知が可能となります。

- 汎用メトリクス監視 メトリクス一覧更新

  汎用メトリクス監視で選択可能なメトリクス一覧を更新、追加しました。

1.3.2. Extension Pack 2308の新機能

- Amazon Athena連携機能

  AWSのAmazon Athenaと連携し、ログのクエリ結果をプローブに収集してログ監視と連携できる以下の監視項目を追加しました。

  - AWS：Athena ログ情報取得機能

  S3に格納されたログもAthena経由でクエリした上で収集が可能となり、コスト等を考慮した運用設計に応じて使い分けが可能です。

- Amazon SQS連携機能

  AWSのAmazon SQSと連携し、メッセージをプローブに収集してログ監視と連携できる以下の監視項目を追加しました。

  - AWS：SQS メッセージ取得

  Cloudwatch Logsへ出力する場合は作り込みが必要となるログに関して、SQS経由で直接Senjuに収集でき、構成をシンプルにすることができます。

- Google Cloud Composer連携機能強化

  千手ブラウザからCloud ComposerのDAGに対しての、起動タスクの情報取得、DAGの基本情報取得のコマンドを追加しました。

- Kubernetes連携機能 監視タスク単位のkubectlコマンドパス指定機能追加

  監視タスクごとに利用するkubectlコマンドのパスを指定できる機能を追加しました。Kubernetesのバージョンアップ対応期間等、新旧の環境が混在している環境でそれぞれのKubernetesに対応するバージョンのkubectlコマンドを指定可能です。

- 汎用メトリクス監視 メトリクス一覧更新

  汎用メトリクス監視で選択可能なメトリクス一覧を更新、追加しました。

1.3.3. Extension Pack 2304の新機能

- 外形監視（WEBシナリオ監視）の追加

  WEBブラウザ上と同じ操作をシステムで再現し、WEBサイト利用者の視点で正常性、応答時間を監視する監視項目を追加しました。E2E(End-to-End)テストツールであるPlaywrightと連携し、WEBサイトの利用の一連の動作における異常の即時検知やパフォーマンス把握が可能になります。

  - Synthetics：ステップ別レスポンスタイム
  - Synthetics：テスト別レスポンスタイム
  - Synthetics：シナリオテストコンプリート

- OCI監視　クロスリージョン監視のサポート

  インスタンス・プリンシパル認証を利用してメトリクス監視を行う際、インスタンスの属するリージョンの情報だけでなく、異なるリージョンも指定して情報を取得できる機能を追加を追加しました。複数リージョンのリソースを監視したい場合、リージョン毎にプローブの用意が不要、且つインターネットを経由せずに監視が可能になります。

- OCI メトリクス監視(MQL)

  Monitoring Query Language (MQL)式を指定し、複数のメトリクスを計算した結果をしきい値判定する監視項目を追加しました。メトリクスを柔軟に組み合わせることによって、事前に定義された値ではない使用率や処理の遅延を監視することが可能となります。

- Azure　ユーザー割り当てマネージドIDを指定した認証方式追加

  認証に使用するユーザー割り当てマネージドIDを監視タスク単位で切り替えて指定できる機能を追加しました。プローブノードに複数のユーザー割り当てマネージドIDを割り当てることで、ロールを切り替えて複数のリソースを同一のプローブノードから監視することが可能となります。

- Azure　証明書による認証方式追加

  プローブノードがサービスプリンシパルによる認証を行う方式の場合に、従来のクライアントシークレットによる認証に加えて、証明書による認証に対応しました。

- Kubernetes/OpenShift　Pod/デプロイメント/レプリカセット/デーモンセット別CPU使用率監視機能追加

  Podおよび各種コントローラ(デプロイメント/レプリカセット/デーモンセット)別のCPUの制限に対するCPU使用率を取得する監視項目を追加しました。コンテナのリソースマニフェストによってCPU制限をしている場合に使用率による監視が有効となります。

- 汎用メトリクス監視 メトリクス一覧更新

  汎用メトリクス監視で選択可能なメトリクス一覧を更新、追加しました。

1.3.4. Extension Pack 2212の新機能

- WEBサービス監視機能

  WEBサービスの高度な監視のため、以下二つの監視項目を追加しました。

  - Webサイトコンテンツ監視：WEBサイトに対してより高度な監視を行うため、WEBサイトのコンテンツ（DOM）の内容をチェックする監視項目を追加しました。
  - WebAPI応答監視：ヘルスチェックAPIなどに対してより高度な監視を行うため、レスポンスボディ（JSON）の内容をチェックする監視項目を追加しました。

- Google Cloud Composer連携機能

  Google CloudのCloud Composerと連携し、千手ブラウザからDAGの各種操作を行う機能を追加しました。

- ログ取得機能のJSONフォーマット対応

  クラウドログやアナウンスメント、コンテナログの取得を行う監視項目で、JSONフォーマットでの出力を選択できるようにしました。

- OCI Audit ログ情報取得機能のログサイクル方法追加

  OCI Audit ログ情報取得機能において、ログサイクルに日次を選択できるようにしました。

- OCI監視 リソース指定方法追加

  OCI連携の各監視項目において、従来OCIDで指定する必要のあったパラメータを、コンパートメント名やログ名でも指定可能にしました。

- 汎用メトリクス監視 メトリクス一覧更新

  汎用メトリクス監視で選択可能なメトリクス一覧を更新、追加しました。

1.3.5. Extension Pack 2208の新機能

- AWS Step Functions連携機能

  AWSのStep Functionsと連携し、Step Functionsを千手ジョブから動作させるためのジョブテンプレートを追加しました。

- Azure Data Explorer連携機能

  AzureのData Explorerと連携し、ログをプローブに収集してログ監視と連携できる機能を追加しました。

- OCI サービス制限監視機能

  OCIで使用状況とサービス制限を取得可能なメトリクスにおいて、現在の使用率を取得する監視項目を追加しました。

- 汎用メトリクス監視 メトリクス一覧更新

  汎用メトリクス監視で選択可能なメトリクス一覧を更新、追加しました。

1.3.6. Extension Pack 2204の新機能

- OCI Streaming連携機能

  OCIのStreamingと連携し、プローブにログを収集してログ監視と連携できる機能を追加しました。

- OCI Data Guard連携機能

  OCIのData Guardと連携し、同期遅延等の情報を監視可能な監視項目を追加しました。

- AWS キャパシティ監視機能

  AWSで使用状況とサービスクォータを取得可能なメトリクスにおいて、現在の使用率を取得する監視項目を追加しました。

- OpenShift コンテナログ監視機能

  OpenShiftのコンテナログをプローブに収集してログ監視と連携できる機能を追加しました。

- 汎用メトリクス監視 メトリクス一覧更新

  汎用メトリクス監視で選択可能なメトリクス一覧を更新、追加しました。

1.3.7. Extension Pack 2112の新機能

- IBM Cloud ログ監視機能

  IBM CloudのLog Analysis with LogDNAと連携し、プローブにログを収集してログ監視と連携できる機能を追加しました。

- IBM Cloud 課金監視機能

  IBM CloudのUsage Reportと連携し、請求および使用量の課金情報を監視可能な監視項目を追加しました。

- IBM Cloud Functions連携ジョブ

  IBM Cloud Functionsを千手のジョブから実行するためのジョブテンプレートを追加しました。

- AWS Health Events連携機能

  顧客の環境に影響を及ぼす可能性のある AWS イベントのアラートやガイダンスに関するEventsをプローブに収集し、ログ監視と連携できる機能を追加しました。

- Azure Service Health連携機能

  進行中のサービスの問題、次に予定されている定期的なメンテナンス、関連する正常性の勧告などのアクティブなイベントログをプローブに収集し、ログ監視と連携できる機能を追加しました。

- OCI Logging連携機能

  OCI Loggingと連携し、プローブにログ取得してログ監視と連携できる機能を追加しました。

1.3.8. Extension Pack 2108の新機能

- IBM Cloud監視機能

  IBM Cloudの各種サービスの情報を監視する監視項目を追加しました。既存の監視機能と併用することで、マルチクラウド／ハイブリッドクラウド環境の一元管理が可能になります。

- Podman監視機能

  Podmanコマンド経由で取得できる各種メトリクス情報を監視する監視項目を追加しました。

- OpenShift監視

  OpenShiftコマンド経由で取得できる各種メトリクス情報を監視する監視項目を追加しました。

- 汎用メトリクス監視

  AWS,Azure,Google Cloud, OCI, IBM Cloudにおいて、APIで取得可能なメトリックを自由に設定可能な汎用メトリクス監視項目を追加しました。

1.3.9. Extension Pack 2104の新機能

- Oracle Cloud Infrastructure お知らせ情報取得機能

  Oracle Cloud Infrastructureのお知らせ情報を取得し、千手のログ監視と連携可能とする機能を追加しました。

  - OCI:アナウンス情報取得

- Oracle Cloud Infrastructure アラームのステータス監視機能

  Oracle Cloud Infrastructureのアラームのステータスを監視する監視項目を追加しました。

  - OCI:アラーム状態

- Oracle Cloud Infrastructure ログ・アナリティクス ログ情報取得機能

  Oracle Cloud Infrastructure ログ・アナリティクスのログ情報を取得し、千手のログ監視と連携可能とする機能を追加しました。

  - OCI:Log Anallytics ログ情報取得

- Amazon Aurora Serverless監視機能の監視項目追加

  Amazon Aurora Serverlessの情報を監視する監視項目を追加しました。

  - AWS:RDS Auroraクラスター状態
  - AWS:RDS Auroraクラスター作成日時
  - AWS:RDS Auroraスナップショット数
  - AWS:RDS Auroraスナップショット合計サイズ(GB)
  - AWS:RDS Auroraスナップショットサイズ(GB)

1.3.10. Extension Pack 2012の新機能

- Microsoft Azure監視、Azure Functions連携ジョブの稼働環境追加

  Microsoft Azure監視、Azure Functions連携ジョブの稼働環境にLinuxを追加しました。稼働環境の詳細はExtension Packのマニュアル「Cloud Monitoring」、「Cloud JOB Scheduler」を参照してください。

- Microsoft Azure監視機能におけるAzure Powershellの使用廃止

  Microsoft Azure監視でAzure Powershellの使用を廃止し、設定手順でAzure Powershellのインストールを不要にしました。

- Microsoft Azure監視の認証方法機能追加

  Microsoft Azure監視において、ユーザ割り当てマネージドIDによる認証をサポートしました。

- Microsoft Azure監視の認証プロファイル指定機能

  Microsoft Azure監視において、監視タスク単位で認証プロファイルの切り替えをできるようにしました。

- Microsoft Azure情報設定ファイル更新コマンド登録機能

  Microsoft Azure情報設定ファイル更新コマンドを千手ブラウザからユーザーコマンドに登録し、現在値の参照、作成と更新をできるようにしました。詳細な手順についてはExtension Packのマニュアル「Cloud Monitoring」を参照してください。

- Amazon Web Services情報設定ファイル更新コマンド登録機能

  Amazon Web Services情報設定ファイル更新コマンドを千手ブラウザからユーザーコマンドに登録し、現在値の参照、作成と更新をできるようにしました。詳細な手順についてはExtension Packのマニュアル「Cloud Monitoring」を参照してください。

1.3.11. Extension Pack 2008の新機能

- Oracle Cloud Infrastructure監視機能

  Oracle Cloud Infrastructureの各種サービスの情報を監視する監視項目を追加しました。既存の監視機能と併用することで、マルチクラウド／ハイブリッドクラウド環境の一元管理が可能になります。

- Oracle Cloud Infrastructure Audit監視機能

  Oracle Cloud Infrastructure Auditのログ情報を取得し、千手のログ監視と連携可能とする機能を提供します。

- Oracle Functions連携ジョブ

  Oracle Functionsを千手のジョブから実行するためのジョブテンプレートを提供します。

- Amazon Web Services監視機能の監視項目追加

  Amazon Web Services監視機能で監視項目として指定できるサービス、メトリクスを追加しました。

  - AWS：RDS Auroraディスク未使用量(MB)
  - AWS：RDS Auroraリードレプリカ反映遅延時間(ミリ秒)

- Microsoft Azure監視機能で使用されるAzure Powershell変更

  Microsoft Azure監視機能で使用されるAzure PowerShellをAzureRMからAzへ変更しました。稼働環境の詳細はExtension Packのマニュアル「Cloud Monitoring」を参照してください。

- Amazon Web Services監視、AWS Lambda連携ジョブにおけるJava SEの稼働バージョン変更

  Amazon Web Services監視、AWS Lambda連携ジョブにおいて、Java SEの稼働バージョンを変更しました。稼働環境の詳細はExtension Packのマニュアル「Cloud Monitoring」を参照してください。

- Docker監視の検索方法指定機能

  以下の監視項目において、パラメータに「検索方法」を追加し、完全一致、部分一致を指定できるようにしました。

  - Docker：コンテナ別稼働状況
  - Docker：コンテナ別CPU使用率(%)
  - Docker：コンテナ別メモリ使用率(%)
  - Docker：コンテナ別メモリ使用量(KB)
  - Docker：コンテナ別メモリ使用量(MB)
  - Docker：コンテナ別ネットワーク受信バイト数(kBps)
  - Docker：コンテナ別ネットワーク送信バイト数(kBps)

1.3.12. Extension Pack 2004の新機能

- Google Cloud監視機能

  Google Cloudの各種サービスの情報を監視する監視項目を追加しました。既存の監視機能と併用することで、マルチクラウド／ハイブリッドクラウド環境の一元管理が可能になります。

- Google Cloud Logging監視機能

  Google Cloud Loggingのログ情報を取得し、ログ監視と連携可能とする機能を提供します。

- Google Cloud Functions連携ジョブ

  Google Cloud Functionsをジョブから実行するためのジョブテンプレートを提供します。

- Amazon Web Services連携のSTSエンドポイント対応

  Amazon Web Servicesの監視実行、ジョブ実行に対してAWS STSエンドポイントを利用した認証機能を提供します。

- Kubernetes監視機能の監視項目追加

  Kubernetes監視機能で監視項目として指定できるメトリクスを追加しました。

1.3.13. Extension Pack 1912の新機能

- Docker監視機能

  Dockerコマンド経由で取得できる各種メトリクス情報を監視する監視項目を追加しました。

- Kubernetes監視

  Kubectl(API)経由で取得できる各種メトリクス情報を監視する監視項目を追加しました。

1.3.14. Extension Pack 1908の新機能

- Amazon Web Services監視機能の監視項目追加

  Amazon Web Services監視機能で監視項目として指定できるサービス、メトリクスを追加しました。

- Amazon Web Services監視機能の性能改善

  Amazon Web Services監視機能の性能を改善し、リソース消費量を削減しました。

- AWS Billing監視機能改善

  従来のAWS Billing監視機能は、AWSアカウント単位で課金情報を取得していましたが、タグ指定やリソース種別などのグループ単位で課金情報を取得できるように改善しました。

- Amazon CloudWatch Logs監視機能

  Amazon CloudWatch Logsのログ情報を取得し、ログ監視と連携可能とする機能を提供します。

- Microsoft Azure監視機能の監視項目追加

  Microsoft Azure監視機能で監視項目として指定できるサービス、メトリクスを追加しました。

- Microsoft Azure監視機能の性能改善

  Microsoft Azure監視機能の性能を改善し、リソース消費量を削減しました。

- Azure Log Analytics監視

  Azure Log Analyticsのログ情報を取得し、ログ監視と連携可能とする機能を提供します。

- Azureリソースのマネージドid対応

  Azureリソースのマネージドidによる認証機能を提供します。これにより、Azure Active Directoryのアプリケーションidやパスワードをパラメータとして保持する必要がなくなります。

- Microsoft Azure監視のProxy対応

  Microsoft Azureの各種サービスの情報を監視する監視項目について、Proxy経由で監視を行うことが可能になりました。プライベートクラウドやオンプレミス環境からMicrosoft Azureの各サービスを監視することが可能となります。

- Microsoft Azure課金情報のEA(Enterprise Agreement)契約対応

  Microsoft AzureがEA(Enterprise Agreement)契約の場合における、課金情報およびリソース使用量を監視する監視項目を追加しました。

- Microsoft Azure Stack監視機能

  Microsoft Azure Stackの各種サービスの情報を監視する監視項目を追加しました。

- AWS Lambda連携ジョブ

  AWS Lambda関数をジョブから実行するためのジョブテンプレートを提供します。

- Azure Functions連携ジョブ

  Azure FunctionsやDurable Functionsをジョブから実行するためのジョブテンプレートを提供します。

1.4. 稼働環境

1.4.1. クラウド連携の稼働環境

1.4.1.1. AWS連携の稼働環境

対応機種	下記対応OSのx64およびARM64アーキテクチャを持つPC、及び周辺機器
対応OS	プローブノード: 千手エージェント (Linux、Windows) の稼働環境に準じる
ネットワーク	AWSエンドポイントに接続可能なネットワーク環境

1.4.1.2. Azure連携の稼働環境

対応機種	下記対応OSのx64およびARM64アーキテクチャを持つPC、及び周辺機器
対応OS	プローブノード: 千手エージェント (Linux、Windows) の稼働環境に準じる
ネットワーク	Azureエンドポイントに接続可能なネットワーク環境

1.4.1.3. Google Cloud連携の稼働環境

対応機種	下記対応OSのx64およびARM64アーキテクチャを持つPC、及び周辺機器
対応OS	プローブノード: 千手エージェント (Linux、Windows) の稼働環境に準じる
ネットワーク	Google Cloudエンドポイントに接続可能なネットワーク環境

1.4.1.4. OCI連携の稼働環境

対応機種	下記対応OSのx64およびARM64アーキテクチャを持つPC、及び周辺機器
対応OS	プローブノード: 千手エージェント (Linux、Windows) の稼働環境に準じる
ネットワーク	OCIエンドポイントに接続可能なネットワーク環境

1.4.1.5. IBM Cloud連携の稼働環境

対応機種	下記対応OSのx64およびARM64アーキテクチャを持つPC、及び周辺機器
対応OS	プローブノード: 千手エージェント (Linux、Windows) の稼働環境に準じる
ネットワーク	IBM Cloudエンドポイントに接続可能なネットワーク環境

1.4.2. コンテナ連携の稼働環境

1.4.2.1. コンテナ監視(Docker)の稼働環境

対応機種	Senju DevOperation Conductor及びDockerエンジンの動作するコンピュータ
対応バージョン	Docker Engine 18.09, 19.03, 20.10, 24.0
対応OS	千手エージェント (Linux) の稼働環境に準じる

1.4.2.2. コンテナ監視(Kubernetes)の稼働環境

対応機種	Senju DevOperation Conductor及びKubernetesの動作するノード
対応バージョン	Kubernetes 1.19, 1.20, 1.21, 1.22, 1.23, 1.24, 1.25, 1.26, 1.27, 1.28
対応OS	千手エージェント (Linux) の稼働環境に準じる

1.4.2.3. コンテナ監視(Podman)の稼働環境

対応機種	Senju DevOperation Conductor及びPodmanの動作するコンピュータ
対応バージョン	Podman 2.2, 3.0
対応OS	千手エージェント (Linux) の稼働環境に準じる

1.4.2.4. コンテナ監視(OpenShift)の稼働環境

対応機種	Senju DevOperation Conductor及びOpenShiftの動作するノード
対応バージョン	OpenShift 4.6, 4.7, 4.8, 4.9, 4.10, 4.11, 4.12, 4.13
対応OS	千手エージェント (Linux) の稼働環境に準じる

1.4.2.5. 追加インストールが必要なライブラリ

以下の追加モジュールをエージェント(プローブ)にインストールしてください。

1.4.2.5.1. JSONライブラリのインストール

この機能では、PerlのJSONライブラリを利用しています。ディストリビューションごとに、以下のパッケージをインストールしてください。

対応OS	必要パッケージ
Red Hat Enterprise Linux Server 6.x	perl-JSON-2.xxxx.el6.noarch
Red Hat Enterprise Linux Server 7.x	perl-JSON-2.xxxx.el7.noarch
Red Hat Enterprise Linux 8.x	perl-JSON-2.xxxx.el8.noarch
Amazon Linux AMI	perl-JSON-2.xxxx.amzn1.noarch
Amazon Linux 2	perl-JSON-2.xxxx.amzn2.noarch
Oracle Linux Server 6.x	perl-JSON-2.xxxx.el6.noarch
Oracle Linux Server 7.x	perl-JSON-2.xxxx.el7.noarch
Oracle Linux Server 8.x	perl-JSON-2.xxxx.el8.noarch
Ubuntu 18.04 LTS	libjson-perl_2.xxxx_all
Ubuntu 20.04 LTS	libjson-perl_4.xxxx_all
SUSE Linux Enterprise Server 12	perl-JSON-2.xxxx.noarch
SUSE Linux Enterprise Server 15	perl-JSON-2.xxxx.noarch

1.4.2.6. 大規模環境向けの追加設定

以下の追加モジュールをエージェント(プローブ)にインストールしてください。

1.4.2.6.1. FileCacheライブラリのインストール

この機能では、PerlのFileCacheライブラリを利用しています。

参考

FileCacheライブラリのインストール方法などについては、下記のWEBサイトを参照してください。

- CPAN – Cache::File URL: https://metacpan.org/pod/Cache::FileCache

FileCacheライブラリのインストール後、sjusershrc、sjusercshrcに環境変数PERL5LIBの設定をする必要があります。

例：$SENJUHOME/dat/opt/sjusershrcの記述

```
export PERL5LIB={Perlモジュールサーチパス}
```

例：$SENJUHOME/dat/opt/sjusercshrcの記述

```
setenv PERL5LIB {Perlモジュールサーチパス}
```

文言を追加後、ノードモニタからsjANM_monExtdプロセスを停止および起動してください。

注釈

大規模な運用環境においては、dockerコマンド、kubectlコマンド、podmanコマンドおよびocコマンドの実行が遅くなり、また監視タスクが増えることによって、状況収集コマンドの実行が遅延する可能性があります。そのような環境の場合には、PerlのFileCacheライブラリを追加インストールすることで、監視タスクの数が増えた際の性能を向上させることができます。

1.4.3. Web監視の稼働環境

1.4.3.1. URL監視の稼働環境

対応機種	Senju DevOperation Conductorの動作するコンピュータ
対応OS	千手エージェント (Linux、Windows) の稼働環境に準じる
ネットワーク	監視対象URLに接続可能なネットワーク環境

1.4.3.2. 外形監視の稼働環境

対応機種	Senju DevOperation Conductor及びPlaywrightの動作するコンピュータ
対応OS	千手エージェント (Linux、Windows) 及びPlaywrightの稼働環境に準じる
ネットワーク	監視対象Webサイトに接続可能なネットワーク環境
対応バージョン	Playwright 1.31, 1.35, 1.38

1.4.3.3. Playwrightと千手エージェントの対応OS

Playwrightの対応OSのうち、千手エージェントでも対応OSとなっているものは以下の通りです。

表 1.1 Playwrightと千手エージェントの対応OS

Playwrightバージョン	Senju/DC 2020	Senju/DC 2021	Senju/DC 2022	Senju/DC 2023
v1.31	• Windows Server 2016 • Windows Server 2019	• Windows Server 2016 • Windows Server 2019 • Ubuntu 20.04 LTS	• Windows Server 2016 • Windows Server 2019 • Windows Server 2022 • Ubuntu 20.04 LTS	• Windows S • Windows S • Windows S • Ubuntu 20. • Ubuntu 22.
v1.35	• Windows Server 2016 • Windows Server 2019	• Windows Server 2016 • Windows Server 2019 • Ubuntu 20.04 LTS	• Windows Server 2016 • Windows Server 2019 • Windows Server 2022 • Ubuntu 20.04 LTS	• Windows S • Windows S • Windows S • Ubuntu 20. • Ubuntu 22.
v1.38	• Windows Server 2016 • Windows Server 2019	• Windows Server 2016 • Windows Server 2019 • Ubuntu 20.04 LTS	• Windows Server 2016 • Windows Server 2019 • Windows Server 2022 • Ubuntu 20.04 LTS	• Windows S • Windows S • Windows S • Ubuntu 20. • Ubuntu 22.

1.4.4. SAP連携の稼働環境

1.4.4.1. CCMS Monitoring for mySAPの稼働環境

対応機種	Senju DevOperation Conductor及びCCMS(BC-XAL 1.0)の動作するコンピュータ
対応プロダクトバージョン	SAP ERP 6.0 (旧名称：SAP ERP 2005) (BC-XAL 6.10) SAP Netweaver 7.5 SAP S/4 HANA 1809, 1909, 2020
対応OS	千手エージェント (Linux, Windows) の稼働環境に準じる

千手エージェント（プローブ）のCCMS Monitoring for mySAP機能と、mySAPシステムとのTCP/IPの通信で使用するサービスポート番号は、saprfc.iniに記述するサービスポート番号です。（saprfc.iniについては、「saprfc.iniの設定」を参照して下さい。）

1.4.4.2. SAP Job Schedulerの稼働環境

対応機種	Senju DevOperation Conductor及びSAP R/3(BC-XBP 3.0)、SAP BW(BW-SCH 3.0)の動作するコンピュータ
対応プロダクトバージョン	SAP ERP 6.0 (旧名称：SAP ERP 2005) SAP Netweaver 7.5 SAP S/4 HANA 1809, 1909, 2020
対応OS	千手エージェント (Linux, Windows) の稼働環境に準じる

エージェントのR/3ジョブ連携コマンド群と、SAP R/3サーバーとのTCP/IPの通信で使用するサービスポート番号は、saprfc.iniに記述するサービスポート番号です。（saprfc.iniについては、「saprfc.iniの設定」を参照して下さい。）

警告

Job Scheduler for R/3コマンド群を実行する際は、該当エージェントの千手稼働アカウントで行ってください。

1.5. 既知の問題と対策

1.5.1. SAP Job Scheduler

1. BWプロセスチェーンプロセス一覧コマンド(sjPEX_bwChain_processList) の問題点

   問題

   BWプロセスチェーンプロセス一覧コマンド(sjPEX_bwChain_processList) は現在のリリースバージョンではサポート対象外であり、正常に動作できません。

2. BWプロセスチェーンプロセスログ取得コマンド(sjPEX_bwChain_processLog) の問題点

   問題

   BWプロセスチェーンプロセスログ取得コマンド(sjPEX_bwChain_processLog) は現在のリリースバージョンではサポート対象外であり、正常に動作できません。

2. Cloud Monitoring

2.1. はじめに

2.1.1. 本章について

- 本章では、クラウド監視(AWS/Azure/Google Cloud/OCI/IBM Cloud)エクステンション の機能や使用方法について説明します。
- クラウド監視(AWS/Azure/Google Cloud/OCI/IBM Cloud) は Amazon Web Services(AWS)、Microsoft の Azure、Google Cloud、Oracle Cloud Infrastructure(OCI)、およびIBM Cloudと連携させることができます。この連携により、Senju/DCのモニタリング機能からクラウドサービスを監視することができるようになります。
- 「Senju DevOperation Conductor」は（株）野村総合研究所の登録商標です。
- Amazon Web Services、“Powered by Amazon Web Services”ロゴ、[およびかかる資料で使用されるその他のAWS商標]は、米国その他の諸国における、Amazon.com, Inc.またはその関連会社の商標です。
- Windows、Windows Server、Azure は、米国Microsoft Corporationの米国及びその他の国における登録商標または商標です。
- Google、Google Cloud、Google Cloud Platform、および、GCP は、Google LLC の商標です。
- OracleとJavaは、Oracle Corporation 及びその子会社、関連会社の米国及びその他の国における登録商標です。文中の社名、商品名等は各社の商標または登録商標である場合があります。
- IBM、IBM ロゴ、および ibm.com は、世界の多くの国で登録された International Business Machines Corp. の商標です。他の製品名およびサービス名等は、それぞれ、IBM または各社の商標である場合があります。現時点での IBM商標リストについては、http://www.ibm.com/legal/copytrade.shtml の『Copyright and trademark information』をご覧ください。
- Linuxは、Linus Torvalds氏の登録商標です。
- その他、本誌で引用の製品名・会社名はそれぞれの会社の商標、もしくは登録商標です。なお、本誌中では、™、® マークなどは明記していません

2.1.2. 読者の対象

本章は Senju DevOperation Conductorのモニタリング機能からAWSやAzure、Google Cloud、OCI、IBM Cloudのクラウドサービスを監視するシステム・アドミニストレータのためのものです。従って、本章の読者は以下のような概念に精通していることを前提にしています。

- Amazon Web Services（AWS）
- Microsoft Azure
- Google Cloud
- Oracle Cloud Infrastructure（OCI）
- IBM Cloud
- Senju DevOperation Conductorの各種コンポーネント（千手ブラウザ、千手マネージャ、千手エージェント）
- Senju DevOperation Conductorのモニタリング機能
- オペレーティング・システムについての知識

2.1.3. 前提条件と関連資料

本章を参照するにあたっては、以下の各マニュアルなどを参照して下さい。

- 統合運用管理ツール「Senju DevOperation Conductor」リリースノート
- 統合運用管理ツール「Senju DevOperation Conductor」ユーザーズガイド
- Amazon Web Servicesドキュメント
- Microsoft Azureドキュメント
- Google Cloudドキュメント
- Oracle Cloud Infrastructureドキュメント
- IBM Cloudドキュメント

2.2. クラウド監視(AWS/Azure/Google Cloud/OCI/IBM Cloud)の概要

クラウド監視(AWS/Azure/Google Cloud/OCI)機能では、AWSやAzure、Google Cloud、OCI、IBM Cloudと連携し、クラウドサービスを監視するために、以下の機能を提供します。

- AWSの各種リソースおよびメトリクス監視
- AWSのCloudWatch Logのログ取得とログフィルタを用いた監視
- AWSのHealthイベント情報取得とログフィルタを用いた監視
- AWSのAthenaログ情報取得とログフィルタを用いた監視
- AWSのSQSメッセージ情報取得とログフィルタを用いた監視
- AWSの使用状況とサービスクォータを取得するキャパシティ監視
- Azureの各種リソースおよびメトリクス監視
- AzureのLogAnalyticsのログ取得とログフィルタを用いた監視
- AzureのService Health情報取得とログフィルタを用いた監視
- AzureのDataExplorerログ取得とログフィルタを用いた監視
- Google Cloudの各種リソースおよびメトリクス監視
- Google CloudのCloud Loggingのログ取得とログフィルタを用いた監視
- OCIの各種リソースおよびメトリクス監視
- OCIのAuditログ取得とログフィルタを用いた監視
- OCIのLogAnalyticsのログ取得とログフィルタを用いた監視
- OCIのAnnouncements情報取得とログフィルタを用いた監視
- OCIのLoggingのログ取得とログフィルタを用いた監視
- OCIのStreamingのログ情報取得とログフィルタを用いた監視
- OCIの使用状況と使用率を取得するサービス制限監視
- IBM Cloudの各種リソースおよびメトリクス監視
- IBM CloudのLog Analysisのログ取得とログフィルタを用いた監視

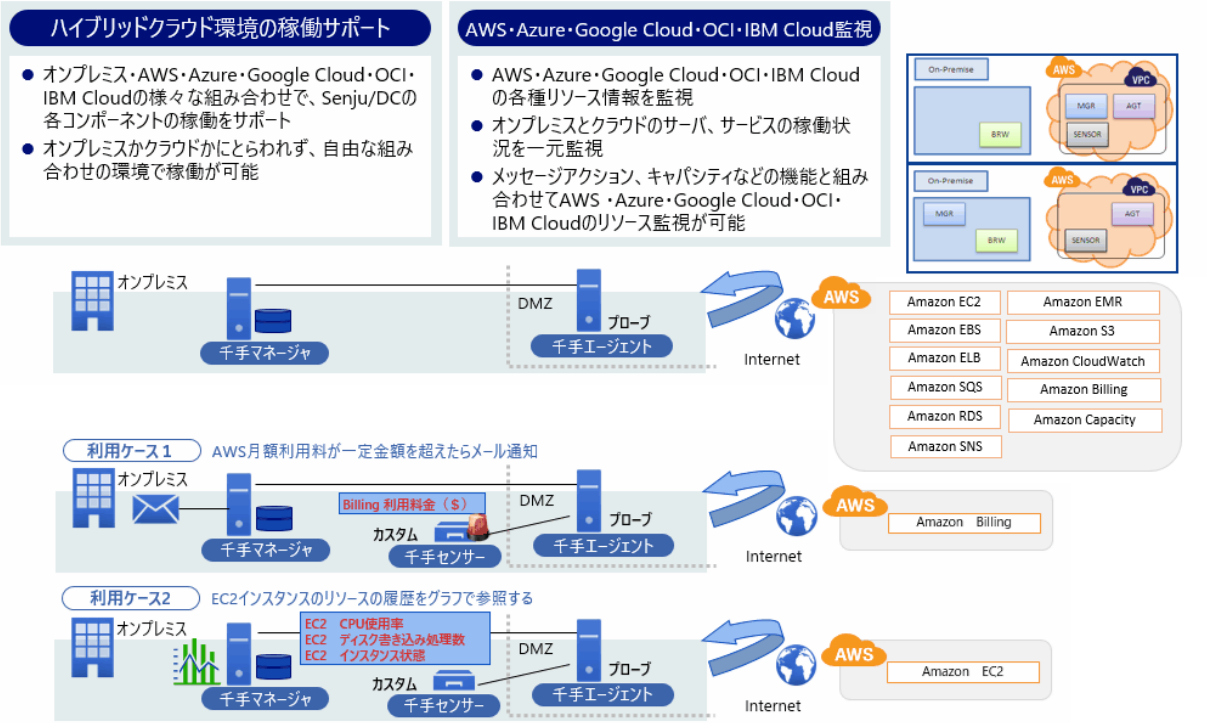


図 2.1 Senju DevOperation Conductorと AWS/Azure/Google Cloud/OCI/IBM Cloud との連携

各種メトリクス取得機能では、Senju DevOperation Conductorモニタリング機能を使用して、AWS や Azure、Google Cloud、OCI、IBM Cloudに対して定期的にデータ取得を行い、しきい値監視することが出来ます。（モニタリング機能については、**ユーザーズガイド「4．モニタリング」**

を参照して下さい。）

2.2.1. AWS監視機能の概要

AWS監視機能では、AWS の各サービスのAmazon Web Services APIを利用して情報を取得します。そのため、エージェント(プローブ)から Amazon Web Services APIにアクセスできる必要があります。

利用しているAmazon Web Services APIについては、API利用状況 を参照して下さい

取得可能な項目については、AWS監視 を参照して下さい。

2.2.2. Azure監視機能の概要

Azure監視機能では、Azure REST APIを利用して、リソース情報やメトリクスを取得します。そのため、エージェント(プローブ)からAzure REST API にアクセスできる必要があります。

利用しているAzure REST API については、API利用状況 を参照して下さい。

取得可能な項目については、Azure監視 を参照して下さい。

2.2.3. Google Cloud監視機能の概要

Google Cloud監視機能では、Google Cloud APIを利用して、リソース情報やメトリクスを取得します。そのため、エージェント(プローブ)から Google Cloud APIにアクセスできる必要があります。

利用しているGoogle Cloud APIについては、API利用状況 を参照して下さい。

取得可能な項目については、Google Cloud監視 を参照して下さい。

2.2.4. OCI監視機能の概要

OCI監視機能では、Oracle Cloud Infrastructure APIを利用して、リソース情報やメトリクスを取得します。そのため、エージェント(プローブ)から Oracle Cloud Infrastructure APIにアクセスできる必要があります。

利用しているOracle Cloud Infrastructure APIについては、API利用状況 を参照して下さい。

取得可能な項目については、OCI監視 を参照して下さい。

2.2.5. IBM Cloud監視機能の概要

IBM Cloud監視機能では、IBM Cloud APIを利用して、リソース情報やメトリクスを取得します。そのため、エージェント(プローブ)からIBM Cloud APIにアクセスできる必要があります。

利用しているIBM Cloud APIについては、API利用状況 を参照して下さい。

取得可能な項目については、IBM Cloud監視 を参照して下さい。

2.3. クラウド監視(AWS)監視設定手順と使い方

AWS監視設定を行う際には、以下の設定が必要になります。

- ライセンスの購入とライセンスキーの入手
    - AWS監視

注釈

監視対象数に応じて、カスタムセンサーのライセンスが必要です。

- Senju DevOperation Conductor Extension Packの入手と適用

    運用管理サーバーおよび、クラウド監視を行う管理対象ノードに、同一バージョンの Senju DevOperation Conductor Extension Pack の適用が必要です
    - 運用管理サーバー(千手マネージャ)への適用(監視項目の更新)
    - 管理対象ノード(千手エージェント(プローブノード))への適用(情報取得コマンドの更新)

警告

適用可能な Senju DevOperation Conductor のバージョンやパッチ状況に制限がある場合があります。詳しくは、Senju DevOperation Conductor Extension Pack の README をご参照下さい。

参考

Senju DevOperation Conductor Extension Packの適用手順につきましては、Senju DevOperation Conductor Extension Pack の README をご参照下さい。

注釈

Senju DevOperation Conductor Extension Packの適用に際しては、千手システムの停止は不要ですが、関連する監視タスクの停止が必要です。

2.3.1. 設定

- **説明**

    モニタリングサブシステムを用いてAWSの監視項目を使用するための設定を行います。

- **設定手順**

    AWS監視を設定するには以下の手順が必要です。
    - Amazon Web Servicesアカウントの登録
    - AWS情報設定ファイルの作成
    - プロファイルの設定

2.3.1.1. Amazon Web Servicesアカウントの登録

AWSの監視項目の利用において、事前にAmazon Web Servicesアカウントの登録が必要です。Amazon Web Servicesサイトよりアカウント登録を行って下さい。

AWS Health イベントの監視項目を利用する場合、サポートプランが「ビジネス」または「エンタープライズ」である必要があります。

2.3.1.1.1. IAMユーザーの作成

AWSアカウントのルートアカウントの認証情報は、アカウント内のすべてのリソースへのフルアクセスが許可されていますので、AWS監視を行うためには AWS Identity and Access Management (IAM) ユーザーの認証情報を使用する事をお薦めします。Amazon Web ServicesサイトよりIAMユーザーの作成を行って下さい。

AWS監視では、監視項目毎に必要とされるアクセス権限が異なります。IAMユーザーに**「AWS監視に必要なアクセス権限」**に示すアクセス権限を付与して下さい。

表 2.1 AWS監視に必要なアクセス権限

監視項目	必要なアクセス権
AWS：EC2 ~	ec2:DescribeRegions ec2:DescribeInstances cloudwatch:ListMetrics cloudwatch:GetMetricStatistics
AWS：EBS ~	ec2:DescribeRegions ec2:DescribeVolumes cloudwatch:ListMetrics cloudwatch:GetMetricStatistics
AWS：ELB ~	ec2:DescribeRegions elasticloadbalancing:DescribeInstanceHealth elasticloadbalancing:DescribeLoadBalancers cloudwatch:ListMetrics cloudwatch:GetMetricStatistics
AWS：RDS ~	ec2:DescribeRegions rds:DescribeDBInstances rds:DescribeDBSnapshots rds:DescribeDBClusters rds:DescribeDBClusterSnapshots cloudwatch:ListMetrics cloudwatch:GetMetricStatistics
AWS：S3 ~	s3:ListAllMyBuckets s3:ListBucket s3:GetBucketLocation
AWS：AS ~	ec2:DescribeRegions autoscaling:DescribeAutoScalingGroups autoscaling:DescribeScalingActivities
AWS：CW ~	ec2:DescribeRegions cloudwatch:DescribeAlarmHistory cloudwatch:DescribeAlarms
AWS：SQS ~ AWS：SNS ~ AWS：EMR ~ AWS：Billing 利用料金($)	ec2:DescribeRegions cloudwatch:ListMetrics cloudwatch:GetMetricStatistics
AWS：CE ~	CE:GetCostAndUsage
AWS：CWL ~	cloudwatch logs:FilterLogEvents
AWS：Health ~	health:DescribeEvents health:DescribeEventDetails health:DescribeAffectedEntities
AWS：Capacity ~	ec2:DescribeRegions cloudwatch:GetMetricData
AWS：Athena ~	glue:GetDatabases glue:GetTables athena:StartQueryExecution athena:GetQueryResults s3:GetObject s3:PutObject
AWS：SQS Message ~	sqs:SendMessage sqs:DeleteMessage

2.3.1.2. AWS情報設定ファイル(sj_aws.ini)の作成

sj_aws.iniファイルは、AWSに関する情報の設定ファイルです。設定ファイルを作成することで、監視タスク作成時にパラメータ値を省略することができます。設定ファイルを作成しなかった場合、及び項目を省略した場合は、監視タスク作成時にパラメータで値を指定する必要があります。

同じ項目を、sj_aws.iniとAWSの監視タスクのパラメータの両方で指定した場合は、AWSの監視タスクのパラメータで指定した値が有効になります。

sj_aws.iniはデフォルトで「千手ホームディレクトリ/dat/opt/sj_aws.ini」に作成されます。パスおよびファイル名は任意に指定することが可能です。

設定方法については、sj_setup_aws ― AWS情報設定ファイル更新 ― を参照して下さい。

表 2.2 sj_aws.iniの記述内容

項目	省略	デフォルト	暗号化対象	説明
accessKey	可	—	○	AWS接続用のアクセスキーID
secretKey	可	—	○	AWS接続用のシークレットアクセスキー
iamRoleRetryCount	可	5	×	プロファイル使用時、IAMロール認証情報取得失敗時のリトライ回数
iamRoleRetryInterval	可	1	×	プロファイル使用時、IAMロール認証情報取得失敗時のリトライ間隔(秒)
proxyHost	可	—	×	AWS接続時に経由するプロキシサーバーのホスト名
proxyPort	可	—	×	AWS接続時に経由するプロキシサーバーのポート番号
proxyUsername	可	—	×	AWS接続時に経由するプロキシサーバーアクセス用ユーザーID
proxyPassword	可	—	○	AWS接続時に経由するプロキシサーバーアクセス用パスワード(暗号化後のパスワード)
maxLogSize	可	—	×	省略する場合はログファイルを出力する際の最大サイズが10240(単位:KB)になります。
maxLogCnt	可	—	×	省略する場合はログファイルを出力する際のローテーション最大個数が7になります。
retryCount	可	3	×	API実行失敗時のリトライ回数
waitTime	可	30	×	API実行時のタイムアウト時間
logFormat	可	—	×	取得したログの出力フォーマットをLTSVもしくはJSONに切り替えます。省略する場合はLT
logBufferTime	可	—	×	省略する場合は前回取得した最後のログより遡る時間が5(単位:分)になります。

- AWS接続用のアクセスキーIDおよびシークレットアクセスキーは、Amazon Web Servicesのサイトで確認して下さい。
- アクセスキーIDおよびシークレットアクセスキーの一方のみを指定することはできません。
- プロキシサーバーのホスト名およびポート番号の両方を指定しなかった場合、プロキシサーバーを利用しません。
- プロキシサーバーアクセス用ユーザーIDおよびパスワードの両方を指定しなかった場合、プロキシサーバーの認証に利用しません。
- 一回以上ログを取得している状態でlogBufferTimeを現在よりも大きい値に変更した場合、変更後の1回目の実行で過去に取得したログを重複して取得する場合があります。ご注意ください。

2.3.1.2.1. sj_setup_aws ー AWS情報設定ファイル更新 ー

- 指定形式
  - [参照]

```
sj_setup_aws
```

  - [作成＆更新]

```
sj_setup_aws
  [-ak[access key ID for AWS connection]]
  [-sk[secret access key for AWS connection]]
  [-reg[Target Region]]
  [-jp[Java Virtual Machine parameter]]
  [-jh[Java Virtual Machine heap setting]]
  [-bk[S3 Bucket]]
  [-ic[EC2 Instance counts]]
  [-mit[EC2 Instance Type(master)]]
  [-sit[EC2 Instance Type(slave)]]
  [-mrlu[Elastic MapReduce Job Flow LogUri]]
  [-ci[check interval(seconds)(10-600)]]
  [-hv[hadoop version]]
  [-phost[hostname of proxy server]]
  [-pport[port number of proxy server]]
  [-puser[User ID of proxy server]]
  [-ppswd[password for accessing the proxy server when connecting to AWS]]
  [-irrc[number of retries when acquisition of IAM role authentication
  information fails when using profile]]
  [-irri[Retry interval(seconds) when acquisition of IAM role authentication
  information fails when using profile]]
  [-mls[If omitted, the maximum size of the log file output by log monitoring is
  10240 (unit: KB)]]
  [-mlc[If omitted, the maximum number of log file rotations output by log
```

```
monitoring is 7.]]
[-rc[number of retries when API call fails]]
[-wt[wait time(seconds) when no response is returned]]
[-cf[AWS information setting file path]]
[-lf[format of log file output by log monitoring]]
[-lbt[bufferTime of log file output by log monitoring]]
```

- 目的

  AWS情報設定ファイル(/dat/opt/sj_aws.ini) の現在値の参照、作成と更新を行います。

- オプション

  - -ak

    AWS接続用のアクセスキーID（accessKey）に設定する場合に指定して下さい。
    設定値の指定は対話形式で行われます。
    この項目は暗号化した値がAWS情報設定ファイルに書き込まれます。

  - -sk

    AWS接続用のシークレットアクセスキー（secretKey）に設定する場合に指定して下さい。
    設定値の指定は対話形式で行われます。
    この項目は暗号化した値がAWS情報設定ファイルに書き込まれます。

  - -reg

    AWSの接続先リージョン（region）に設定する値を指定して下さい。
    値を省略するとAWS情報設定ファイルに設定されている値を削除します。

  - -jp

    Java Virtual Machineパラメータ（jvm_param）に設定する値を指定して下さい。
    値を省略するとAWS情報設定ファイルに設定されている値を削除します。

  - -jh

    Java Virtual Machineヒープ設定（jvm_heap）に設定する値を指定して下さい。
    値を省略するとAWS情報設定ファイルに設定されている値を削除します。

  - -bk

    AWS/S3のバケット（bucket）に設定する値を指定して下さい。
    値を省略するとAWS情報設定ファイルに設定されている値を削除します。

  - -ic

    AWS/EC2インスタンス数（instanceCount）に設定する値を指定して下さい。
    値を省略するとAWS情報設定ファイルに設定されている値を削除します。

  - -mit

    AWS/EC2インスタンスタイプ（マスター）（masterInstanceType）に設定する値を指定して下さい。
    値を省略するとAWS情報設定ファイルに設定されている値を削除します。

  - -sit

    AWS/EC2インスタンスタイプ（スレーブ）（slaveInstanceType）に設定する値を指定して下さい。
    値を省略するとAWS情報設定ファイルに設定されている値を削除します。

  - -mrlu

    AWS/Elastic MapReduceジョブフローのログ出力先URI（mapreduceLogUri）に設定する値を指定して下さい。
    値を省略するとAWS情報設定ファイルに設定されている値を削除します。

  - -ci

    チェックインターバル(秒)[10-600]（checkInterval）に設定する値を指定して下さい。
    値を省略するとAWS情報設定ファイルに設定されている値を削除します。

- -hv

  hadoopバージョン(hadoopVersion)に設定する値を指定して下さい。
  値を省略するとAWS情報設定ファイルに設定されている値を削除します。

- -phost

  AWS接続時に経由するプロキシサーバーのホスト名(proxyHost)に設定する値を指定して下さい。
  値を省略するとAWS情報設定ファイルに設定されている値を削除します。

- -pport

  AWS接続時に経由するプロキシサーバーのポート番号(proxyPort)に設定する値を指定して下さい。
  値を省略するとAWS情報設定ファイルに設定されている値を削除します。

- -puser

  AWS接続時に経由するプロキシサーバーアクセス用ユーザーID(proxyUsername)に設定する値を指定して下さい。
  値を省略するとAWS情報設定ファイルに設定されている値を削除します。

- -ppswd

  AWS接続時に経由するプロキシサーバーアクセス用パスワード(proxyPassword)に設定する場合に指定して下さい。
  設定値の指定は対話形式で行われます。
  この項目は暗号化した値がAWS情報設定ファイルに書き込まれます。

- -irrc

  プロファイル使用時、IAMロール認証情報取得失敗時のリトライ回数(iamRoleRetryCount)に設定する値を指定して下さい。
  値を省略するとAWS情報設定ファイルに設定されている値を削除します。

- -irri

  プロファイル使用時、IAMロール認証情報取得失敗時のリトライ間隔(秒)(iamRoleRetryInterval)に設定する値を指定して下さい。
  値を省略するとAWS情報設定ファイルに設定されている値を削除します。

- -mls

  出力するログファイルの、最大サイズ(maxLogSize)に設定する値を指定して下さい。
  値を省略するとAWS情報設定ファイルに設定されている値を削除します。

- -mlc

  出力するログファイルの、ローテーション最大個数(maxLogCnt)に設定する値を指定して下さい。
  値を省略するとAWS情報設定ファイルに設定されている値を削除します。

- -rc

  API実行失敗時のリトライ回数(retryCount)に設定する値を指定して下さい。
  値を省略するとAWS情報設定ファイルに設定されている値を削除します。

- -wt

  API実行時のタイムアウト時間(waitTime)に設定する値を指定して下さい。
  値を省略するとAWS情報設定ファイルに設定されている値を削除します。

- -cf

  現在値の参照、作成と更新を行う任意のAWS情報設定ファイルを絶対パスで指定して下さい。
  値を省略した場合はデフォルトのAWS情報設定ファイル(/dat/opt/sj_aws.ini) の参照、作成と更新を行います。

- -lf

  ログフォーマット(logFormat)に設定する値を指定して下さい。
  値を省略するとAWS情報設定ファイルに設定されている値を削除します。

- -lbt

最後に取得したログより遡る時間(logBufferTime)を指定して下さい。
値を省略するとAWS情報設定ファイルに設定されている値を削除します。

- 実行結果
  - (例1)現在の設定値参照

```
% sj_setup_aws
#Com
accessKey=
secretKey=
keyEncryption=ON
maxLogSize=
maxLogCnt=
retryCount=3
waitTime=30
logFormat=
logBufferTime=

#Job
region=
jvm_param=
jvm_heap=
bucket=
instanceCount=5
masterInstanceType=m1.small
slaveInstanceType=m1.small
mapreduceLogUri=
checkInterval=60
hadoopVersion=1.0.3

#Proxy
proxyHost=
proxyPort=
proxyUsername=
proxyPassword=

#IamRole
iamRoleRetryCount=
iamRoleRetryInterval=
%
```

  - (例2)アクセスキーとシークレットキー、リージョンを設定

```
% sj_setup_aws -ak -sk -regap-northeast-1
Please enter the value.
accessKey=
Please enter the value.
secretKey=

The value of accessKey has changed from (**********) to (**********).
The value of secretKey has changed from (**********) to (**********).
The value of region has changed from () to (ap-northeast-1).

The AWS information file successfully updated.

% sj_setup_aws
accessKey=**********
secretKey=**********
keyEncryption=ON
maxLogSize=
maxLogCnt=
retryCount=3
waitTime=30
logFormat=
logBufferTime=

#Job
region=ap-northeast-1
jvm_param=
jvm_heap=
bucket=
instanceCount=5
masterInstanceType=m1.small
slaveInstanceType=m1.small
mapreduceLogUri=
checkInterval=60
hadoopVersion=1.0.3

#Proxy
proxyHost=
proxyPort=
proxyUsername=
proxyPassword=
```

```
#IamRole
iamRoleRetryCount=
iamRoleRetryInterval=
%
```

- (例3)設定を削除

```
% sj_setup_aws -ak -sk -reg
Please enter the value.
accessKey=
Please enter the value.
secretKey=

The value of accessKey has changed from (**********) to (**********).
The value of secretKey has changed from (**********) to (**********).
The value of region has changed from (ap-northeast-1) to ().

The AWS information file successfully updated.

% sj_setup_aws
accessKey=
secretKey=
keyEncryption=ON
maxLogSize=
maxLogCnt=
retryCount=3
waitTime=30
logFormat=
logBufferTime=

#Job
region=
jvm_param=
jvm_heap=
bucket=
instanceCount=5
masterInstanceType=m1.small
slaveInstanceType=m1.small
mapreduceLogUri=
checkInterval=60
hadoopVersion=1.0.3

#Proxy
proxyHost=
proxyPort=
proxyUsername=
proxyPassword=

#IamRole
iamRoleRetryCount=
iamRoleRetryInterval=
%
```

注釈

- 暗号化対象項目の標準出力への表示は全てアスタリスクでマスクされます。
- 暗号化対象項目の値の設定は、キーボードからの入力が一切表示されません。コピー＆ペーストで入力することをお勧めします。
- 暗号化対象項目の値を削除する場合、何も入力せずにリターンキーを押下して下さい。

- 標準エラー出力
  - Failed to acquire Senju home directory.
  - The AWS information file does not exist.
  - Invalid data have been set in this file.
  - Failed to update the AWS information file.
- 終了ステータス
  - 0：正常終了
  - 1：異常終了

2.3.1.2.2. AWS情報設定ファイル更新コマンドの登録

AWS情報設定ファイルの現在値の参照、作成と更新を行うため、AWS情報設定ファイル更新コマンドを千手ブラウザからユーザーコマンドに登録します。詳細な手順については、ユーザーズガイド**「2.3.2.1 ユーザーコマンド」**を参照して下さい。

- ユーザーコマンドグループの作成

  AWS情報設定ファイル更新コマンドを登録するユーザーコマンドグループを千手ブラウザから登録して下さい。

- AWS情報設定ファイル更新コマンドの登録

  作成したユーザーコマンドグループに、以下に示す起動シーケンスを指定してコマンドを登録して下さい。

  - 現在値の参照

```
sj_remshe "@ノード名@" -l "@ユーザ名@" sj_setup_aws "-cf@@対象ファイルパス@@"
```

  - 作成と更新

```
sj_remshe "@ノード名@" -l "@ユーザ名@" sj_setup_aws "-ak@@AWS接続用アクセスキーID@@" "-sk@@AWS接続用シークレットアクセスキー@@" "-reg@@AWS接続先リージョン@@" "-jp@@Java Virtual Machineパラメータ@@" "-jh@@Java Virtual Machineヒープ設定@@" "-bk@@AWS/S3バケット@@" "-ic@@AWS/EC2インスタンス数@@" "-mit@@AWS/EC2インスタンスタイプ(マスター)@@" "-sit@@AWS/EC2インスタンスタイプ(スレーブ)@@" "-mrlu@@AWS/Elastic MapReduceジョブフローログ出力先URI@@" "-ci@@チェックインターバル(秒)@@" "-hv@@hadoopバージョン@@" "-phost@@プロキシサーバーホスト名@@" "-pport@@プロキシサーバーポート番号@@" "-puser@@プロキシサーバーアクセス用ユーザーID@@" "-ppswd@@プロキシサーバーアクセス用パスワード@@" "-irrc@@IAMロール認証情報取得失敗時リトライ回数@@" "-irri@@IAMロール認証情報取得失敗時リトライ間隔(秒)@@" "-mls@@ログファイルの最大サイズ@@" "-mlc@@ログファイルのローテーション最大個数@@" "-rc@@API実行失敗時のリトライ回数@@" "-wt@@API実行時のタイムアウト時間@@" "-cf@@対象ファイルパス@@" "-lf@@ログフォーマット@@" "-lbt@@最後に取得したログより遡る時間@@"
```

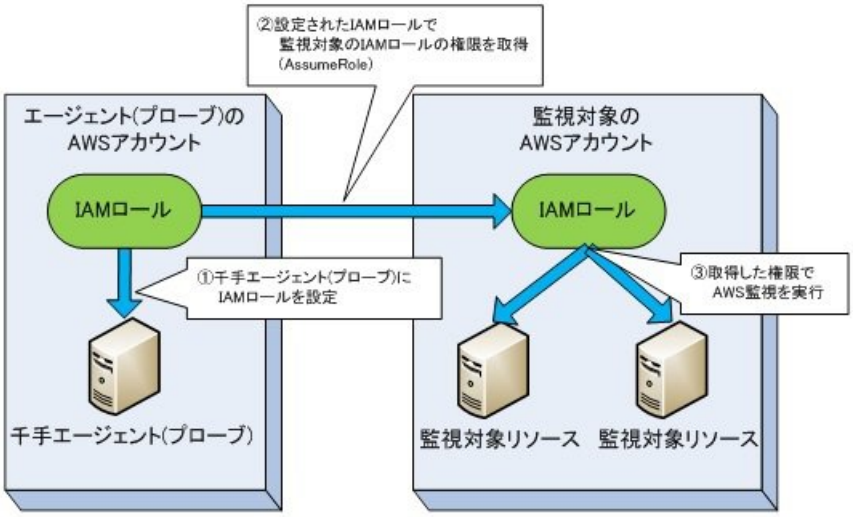
注釈

上記の起動シーケンスは項目を全て変更する仕様となっています。項目別に変更を行いたい場合は、起動シーケンスから任意の「**-オプション@@パラメータ名@@**」を指定したユーザーコマンドを別途登録して下さい。

（例）sj_remshe "@ノード名@" -l "@ユーザ名@" sj_setup_aws "-reg@@AWS接続先リージョン@@" "-cf@@対象ファイルパス@@"

2.3.1.3. プロファイルの設定

IAMロールを設定したEC2インスタンス上の千手エージェント(プローブ)でAWS監視を行う場合、プロファイルを指定してAssumeRoleを利用した監視を行う事ができます。この設定を行うと、複数のアカウントに対して監視を行う際の設定を簡素化する事ができます。



プロファイルを設定するには以下の手順が必要です。

- 監視対象アカウントでのIAMロールの作成
- インスタンスに設定されたIAMロールへの権限付与
- プロファイル作成コマンドの登録
- プロファイルの作成

2.3.1.3.1. 監視対象アカウントでのIAMロールの作成

AWS監視の監視対象となるAWSアカウントで、Amazon Web Servicesサイトより次のようなIAMロールの作成を行って下さい。

- エージェント（プローブノード）のAWSアカウントからAssumeRoleを許可して下さい。
- 監視を行いたい監視項目が実行できるように、**「AWS監視に必要なアクセス権限」**に示すアクセス権限を付与して下さい。

2.3.1.3.2. インスタンスに設定されたIAMロールへの権限付与

監視対象のIAMロール(監視対象アカウントでのIAMロールの作成)で作成したもの) へAssumeRoleができるように、AWS監視を行うEC2インスタンスに設定されたIAMロールに、Amazon Web Servicesサイトより以下に示すアクセス権限を付与して下さい。

表 2.3 IAMロールに必要なアクセス権限

項目	必要なアクセス権
IAMロール	sts:AssumeRole

2.3.1.3.3. プロファイル作成コマンドの登録

プロファイルの作成・編集を行うためのプロファイル作成コマンドを、千手ブラウザからユーザーコマンドに登録します。作業については、ユーザーズガイド**「2.3.2.1 ユーザーコマンド」**を参照して下さい。プロファイル作成コマンドの詳細については、「 sjAwsSetProfile －AWS監視プロファイル作成コマンド－ 」を参照して下さい。

- ユーザーコマンドグループの作成

  プロファイル作成コマンドを登録するユーザーコマンドグループを千手ブラウザから登録して下さい。

- プロファイル作成コマンドの登録

  作成したユーザーコマンドグループに、以下に示す起動シーケンスを指定して5種類のコマンドを登録して下さい。

  - プロファイルの追加
    - UNIX/Linuxマネージャの場合

```
remsh @ノード名@ -l "@ユーザ名@" -k AGT sjAwsSetProfile -m add -p @プロファイル名@ -ar
@IAMロール@ -ei @AWS外部ID@
```

    - Windowsマネージャの場合

```
sj_remshe.exe @ノード名@ -l "@ユーザ名@" -k AGT sjAwsSetProfile -m add -p @プロファイル名@
-ar @IAMロール@ -ei @AWS外部ID@
```

注釈

AWS外部IDを設定しないプロファイルを追加する場合は、上記の起動シーケンスから **-ei @AWS外部ID@** を除いたユーザーコマンドを別途登録して下さい。

  - プロファイルの変更
    - UNIX/Linuxマネージャの場合

```
remsh @ノード名@ -l "@ユーザ名@" -k AGT sjAwsSetProfile -m chg -p @プロファイル名@ -ar
@IAMロール@ -ei @AWS外部ID@
```

    - Windowsマネージャの場合

```
sj_remshe.exe @ノード名@ -l "@ユーザ名@" -k AGT sjAwsSetProfile -m chg -p @プロファイル名@
-ar @IAMロール@ -ei @AWS外部ID@
```

注釈

AWS外部IDを設定しないプロファイルを変更する場合は、上記の起動シーケンスから **-ei @AWS外部ID@** を除いたユーザーコマンドを別途登録して下さい。

  - プロファイルの削除
    - UNIX/Linuxマネージャの場合

```
remsh @ノード名@ -l "@ユーザ名@" -k AGT sjAwsSetProfile -m del -p @プロファイル名@
```

    - Windowsマネージャの場合

```
sj_remshe.exe @ノード名@ -l "@ユーザ名@" -k AGT sjAwsSetProfile -m del -p @プロファイル名@
```

  - プロファイル一覧の表示
    - UNIX/Linuxマネージャの場合

```
remsh @ノード名@ -l "@ユーザ名@" -k AGT sjAwsSetProfile -m list
```

- Windowsマネージャの場合

```
sj_remshe.exe @ノード名@ -l "@ユーザ名@" -k AGT sjAwsSetProfile -m list
```

- プロファイルの詳細表示
  - UNIX/Linuxマネージャの場合

```
remsh @ノード名@ -l "@ユーザ名@" -k AGT sjAwsSetProfile -m detail -p @プロファイル名@
```

- Windowsマネージャの場合

```
sj_remshe.exe @ノード名@ -l "@ユーザ名@" -k AGT sjAwsSetProfile -m detail -p @プロファイル名@
```

2.3.1.3.4. プロファイルの作成

「 プロファイル作成コマンドの登録 」で登録したプロファイル作成コマンドを使って、プロファイルを作成します。作業については、ユーザーズガイド**「2.3.2.1.5 登録したユーザーコマンドの実行」**を参照して下さい。

- ［プロファイルの追加］コマンドの実行

  ［プロファイルの追加］コマンドに、以下のパラメータを入力して実行して下さい。

  ノード名：
  監視を行う千手エージェント(プローブ)のノード名を入力します。
  ユーザー名：
  入力したノードの千手稼働アカウントを入力します。
  プロファイル名：
  追加するプロファイル名を入力します。
  IAMロール:
  監視対象のIAMロールを以下の形式で入力します。
  arn:aws:iam::(監視対象のアカウントID):role/(監視対象のロール)
  AWS外部ID:
  IAMロールの外部IDを入力します。

  ここまでの設定を行う事で、監視項目の[プロファイル]に作成したプロファイル名を指定してAWS監視を行う事ができます。

2.3.1.3.5. sjAwsSetProfile －AWS監視プロファイル作成コマンド－

- 指定形式

  [追加、変更]
  sjAwsSetProfile -m {add|chg} -p プロファイル名 -ar IAMロール [-ei AWS外部ID]

  [削除、詳細表示]
  sjAwsSetProfile -m {del|detail} -p プロファイル名

  [一覧]
  sjAwsSetProfile -m list

  [usage]
  sjAwsSetProfile -h

- 目的
  AWS監視で使用するプロファイルの作成・編集を行います。

- オプション

  -m { add | chg }、{ del | detail }、{list}

  コマンドのモードを指定します。以下の5つから選択できます。
  - add：追加モード。新しいプロファイルを作成します。
  - chg：変更モード。既存のプロファイルを変更します。
  - del：削除モード。既存のプロファイルを削除します。

- detail：詳細表示モード。指定したプロファイルの詳細を表示します。
- list：一覧モード。全てのプロファイルの一覧を表示します。

-p プロファイル名

操作対象のプロファイル名を指定します。
一覧モードを除き省略不可です。一覧モードでは指定不可です。

-ar IAMロール

監視対象のIAMロールを以下の形式で指定します。
追加、変更モードで省略不可です。それ以外のモードでは指定不可です。
arn:aws:iam::(監視対象のアカウントID):role/(監視対象のロール)

-ei AWS外部ID

IAMロールの外部IDを指定します。
追加、変更モードで指定可能、省略可です。それ以外のモードでは指定不可です。

- 実行結果

以下は、プロファイル名を" **myprofile** "、監視対象のアカウントIDを" **111111111111** "、監視対象のIAMロールを" **myrole** "としてプロファイルを新規作成した場合の実行例です。

```
% sjAwsSetProfile -m add -p myprofile -ar arn:aws:iam::111111111111:role/myrole
add:myprofile
role_arn = arn:aws:iam::111111111111:role/myrole
```

- 終了ステータス

0：正常終了
1：異常終了（実行に失敗した場合）

2.3.2. 使い方

AWSの各サービスのエンドポイントから情報を取得し、Senju DevOperation Conductorのモニタリング機能を使って、監視することができます。

監視定義を千手ブラウザより登録し、監視を実施します。監視結果は、各種モニタ画面（グローバルノードモニタ／ノードモニタ）にてその監視状況を表示できます。予め設定したしきい値により障害を検知した場合は、メッセージモニタにメッセージが通知されます。
（モニタリング機能については、ユーザーズガイド「 **4．モニタリング** 」を参照して下さい。）

注釈

監視項目によっては、監視間隔を10分未満に設定すると値が取得できないことがあります。その場合は監視間隔を10分以上に設定して下さい。

参考

各種パラメータの設定値が分からない場合は、Amazon Web Servicesより提供されているCloudWatch Management Consoleのメトリクスにて確認して下さい。
参考URL：https://console.aws.amazon.com/cloudwatch/ (2019年8月現在)

2.3.2.1. AWSの接続先リージョンについて

監視タスク設定の際に指定可能なAWSリージョンは、AWSが各サービスを提供しているリージョンに依存します。下記の表にAWSリージョンと設定する値の例を示します。詳細についてはAmazon Web Servicesよりご確認下さい。

表 2.4 AWSの接続先リージョンと設定値の例

AWSリージョン	設定値
米国東部(バージニア)	us-east-1
米国西部(カルフォルニア)	us-west-1
米国西部(オレゴン)	us-west-2
南米(サンパウロ)	sa-east-1
欧州(フランクフルト)	eu-central-1
欧州(アイルランド)	eu-west-1
アジアパシフィック(シンガポール)	ap-southeast-1
アジアパシフィック(シドニー)	ap-southeast-2
アジアパシフィック(東京)	ap-northeast-1
アジアパシフィック(大阪)	ap-northeast-3

2.3.2.2. VPCエンドポイント(AWS PrivateLink)について

VPCエンドポイント(AWS PrivateLink)を使用したサービスへの接続を行う場合は、下記のいずれかの設定でVPCエンドポイントのリージョンを指定して下さい。

- 監視タスクの「リージョン」オプション

参考

VPCエンドポイント(AWS PrivateLink)に対応したサービスについては、Amazon Web Servicesよりご確認下さい。
参考URL: https://docs.aws.amazon.com/ja_jp/vpc/latest/userguide/vpce-interface.html (2020年4月現在)

2.3.2.3. AWS監視の各パラメータの上限値および制限事項

AWS監視で設定できるパラメータにはAmazon Web Servicesの上限値とは別に千手固有の上限値および制限事項があります。下記の表に上限値および制限事項を示します。

表 2.5 AWS監視の各パラメータの上限値および制限事項

パラメータ名	上限値、制限事項
プロファイル名	50byte 、半角英数字
タグキー	80byte 、半角英数字
タグ値	80byte 、半角英数字

2.3.2.4. Amazon CloudWatch Logs連携機能

監視項目「AWS：CWL AWSログ情報取得」では Amazon CloudWatch Logs から取得したログをログファイルに蓄積します。このログファイルを監視することでアラートの検知をすることが可能です。

2.3.2.4.1. ログファイル

監視項目「AWS：CWL AWSログ情報取得」で取得したログファイルは、パラメータ「ログファイル」で指定したファイル(絶対パス)に出力されます。複数の監視タスクを設定する場合は、出力先のログファイルが重複しないように設定する必要があります。パラメータでログファイルを指定しない場合は、ログフォーマットがLTSVあるいはJSONによってファイル名が変わります。ただし、ファイル名に使用できない記号は「-」(半角ハイフン)に置き換えます。

ログフォーマットがLTSVの場合：

<千手ホームディレクトリ>/log/cloud.aws.d/CloudWatch_<リージョン>_<ロググループ名>.log

ログフォーマットがJSONの場合：

<千手ホームディレクトリ>/log/cloud.aws.d/CloudWatch_<リージョン>_<ロググループ名>.json

複数の監視タスクを設定する場合は、出力先のログファイルが重複しないように設定する必要があります。リージョン、ロググループ名を指定して下さい。

ログメッセージに含まれる改行、タブ、「\」記号は、”\t”⇒”\\t” “\n”⇒ “\\n”, “\”⇒ “\\”に置換されログファイルに出力されます。

出力されるログファイルの文字コードは UTF-8 になります。テキストログ監視の設定で監視対象ログの「文字コードを指定する」を UTF-8 に指定して

下さい。

2.3.2.4.2. ログフォーマット

以下にAmazon CloudWatch Logs ログ情報取得で取得したログファイルのレコード形式について説明します。レコードは LTSV形式で、項目間はタブ区切りとなります。

【Amazon CloudWatch Logsログファイル　レコード形式】

- ログフォーマットがLTSVの場合：

ログストリーム名　イベントID　タイムスタンプ　ログメッセージ

表 2.6 AWSログファイルレコード形式

No.	項目	説明
1	タイムスタンプ	「Timestamp:」に続き、取得したイベントが出力されたタイムスタンプ(UTC)が入ります。フォーマット：YYYY-MM-DDThh:r
2	ログストリーム名	「LogStreamName:」に続き、取得したログストリーム名が入ります。
3	イベントID	「EventId:」に続き、取得したイベントのイベントのIDが入ります。
4	ログメッセージ	「LogMessage:」に続き、取得したイベントのメッセージが入ります。

- ログフォーマットがJSONの場合：

ログメッセージ

表 2.7 AWSログファイルレコード形式

No.	項目	説明
1	ログメッセージ	取得したイベントのメッセージが入ります。メッセージはJSONの形式で出力されます。

2.3.2.4.3. テキストログ監視の設定方法

以下にSenju DevOperation Conductorのテキストログ監視を利用して、Amazon CloudWatch Logs ログ情報取得で取得したログメッセージを監視する運用例を示します。この例では、ログメッセージにキーワードが発生時にメッセージモニタに通知されるようにログフィルタを登録し、監視する場合について説明します。

＜ログフィルタの登録＞
千手ブラウザのツリービューで＜ドメイン＞→“フィルタ”→“ログフィルタ”を選択します。ログフィルタのエンティティでリストビューの何も表示されていない部分でマウスの右ボタンを押してコンテキストメニューを表示し、[新規作成]メニューを選択します。ログフィルタのプロパティが表示されます。ログフィルタ名などの各項目を入力し[OK]ボタンを押下します。これにより、ログフィルタの登録が完了します。

＜フィルタ監視項目の追加＞
千手ブラウザのツリービューの＜ドメイン＞→“フィルタ”→“ログフィルタ”→＜ログフィルタ＞でフィルタ監視項目を登録するログフィルタを選択し、リストビューの何も表示されていない部分でマウスの右ボタンを押してコンテキストメニューを表示し、[新規作成]メニューを選択します。フィルタ監視項目のプロパティが表示されますので、指定フィールドを検知するキーワードで監視設定し、通知したいメッセージIDを登録します。

＜テキストログ監視の設定＞
アラートファイルのテキストログ監視を行うには、千手ブラウザのツリービューで、＜ドメイン＞→“ノードグループ”→＜ノードグループ＞を選択し、そのリストビューからAmazon CloudWatch Logs ログ情報取得のプローブとして設定したノードを選択し、マウスの右ボタンをクリックしコンテキストメニューを表示し、[プロパティ]メニューを選択します。ノードのプロパティウィンドウが表示されますので、[ログ監視]タブを選択します。ノードのプロパティ（[ログ監視]タブ）にて、監視対象のパス名とファイル名にAmazon CloudWatch Logs ログファイルを指定し、監視方法に先に作成したログフィルタを指定します。ログ監視を登録した後に、登録したノードに対して[反映(監視属性)]を実行することにより、ログファイルの監視を開始します。

以上で、テキストログ監視の設定方法は完了です。この設定によりAmazon CloudWatch Logs ログファイルにキーワードが出力された場合、メッセージモニタに通知されます。

警告

管理対象ノードにおいて千手が起動していない状態で、[反映(監視属性)]を行うと失敗しますので、注意して下さい。

2.3.2.5. AWS Health イベント監視機能

監視項目「AWS：Health イベント情報取得」ではAWS Health から取得したイベント情報をログファイルに蓄積します。このログファイルを監視することでHealth イベント情報を検知することが可能です。

2.3.2.5.1. AWS Health連携機能の制限事項

AWS Healthの監視対象が多い場合に、ログ取得の途中で強制停止される可能性があります。

2.3.2.5.2. ログファイル

監視項目「AWS：Health イベント情報取得」で取得したログファイルは、パラメータ「ログファイル」で指定したファイル(絶対パス)に出力されます。複数の監視タスクを設定する場合は、出力先のログファイルが重複しないように設定する必要があります。パラメータでログファイルを指定しない場合は、ログフォーマットがLTSVあるいはJSONによってファイル名が変わります。ただし、ファイル名に使用できない記号は「-」(半角ハイフン)に置き換えます。

ログフォーマットがLTSVの場合：

<千手ホームディレクトリ>/log/cloud.aws.d/HealthEvents_<モード>_<フィルター>.log

ログフォーマットがJSONの場合：

<千手ホームディレクトリ>/log/cloud.aws.d/HealthEvents_<モード>_<フィルター>.json

複数の監視タスクを設定する場合は、出力先のログファイルが重複しないように設定する必要があります。モードとフィルターを指定して下さい。

出力されるログファイルの文字コードは UTF-8 になります。テキストログ監視の設定で監視対象ログの「文字コードを指定する」を UTF-8 に指定して下さい。

2.3.2.5.3. ログフォーマット

以下にAWS Health イベント情報取得で取得したログファイルのレコード形式について説明します。レコードは LTSV形式で、項目間はタブ区切りとなります。

【AWS Health イベント情報ログファイル　レコード形式】

- ログフォーマットがLTSVの場合：

タイムスタンプ　イベント内容

表 2.8 AWSログファイルレコード形式

No.	項目	説明
1	タイムスタンプ	「Timestamp:」に続き、取得したイベント情報の作成時間または更新時間のタイムスタンプ(UTC)が入ります。フォーマット：Y（例：2020-08-13T07:09:06Z）。
2	イベント内容	「Health:」に続き、取得したイベント内容が入ります。イベント内容はJSONの形式で出力されます。

- ログフォーマットがJSONの場合：

イベント内容

表 2.9 AWSログファイルレコード形式

No.	項目	説明
1	イベント内容	取得したイベント内容が入ります。イベント内容はJSONの形式で出力されます。

2.3.2.5.4. テキストログ監視の設定方法

以下にSenju DevOperation Conductorのテキストログ監視を利用して、AWS Health イベント情報取得で取得したイベント情報を監視する運用例を示します。この例では、イベント内容にキーワードが発生した時にメッセージモニタに通知されるようにログフィルタを登録し、監視する場合について説明します。

＜ログフィルタの登録＞
千手ブラウザのツリービューで＜ドメイン＞→“フィルタ”→“ログフィルタ”を選択します。ログフィルタのエンティティでリストビューの何も表示されていない部分でマウスの右ボタンを押してコンテキストメニューを表示し、[新規作成]メニューを選択します。ログフィルタのプロパティが表示されます。ログフィルタ名などの各項目を入力し[OK]ボタンを押下します。これにより、ログフィルタの登録が完了します。

＜フィルタ監視項目の追加＞

千手ブラウザのツリービューの＜ドメイン＞→“フィルタ”→“ログフィルタ”→＜ログフィルタ＞でフィルタ監視項目を登録するログフィルタを選択し、リストビューの何も表示されていない部分でマウスの右ボタンを押してコンテキストメニューを表示し、[新規作成]メニューを選択します。フィルタ監視項目のプロパティが表示されますので、指定フィールドを検知するキーワードで監視設定し、通知したいメッセージIDを登録します。

＜テキストログ監視の設定＞
アラートファイルのテキストログ監視を行うには、千手ブラウザのツリービューで、＜ドメイン＞→“ノードグループ”→＜ノードグループ＞を選択し、そのリストビューからAWS Health イベント情報取得のプローブとして設定したノードを選択し、マウスの右ボタンをクリックしコンテキストメニューを表示し、[プロパティ]メニューを選択します。ノードのプロパティウィンドウが表示されますので、[ログ監視]タブを選択します。ノードのプロパティ（[ログ監視]タブ）にて、監視対象のパス名とファイル名にAWS Health イベント情報ログファイルを指定し、監視方法に先に作成したログフィルタを指定します。監視対象ログの「文字コードを指定する」を UTF-8 に指定し、ログ監視を登録した後に、登録したノードに対して[反映(監視属性)]を実行することにより、ログファイルの監視を開始します。

2.3.2.6. Amazon Athena連携機能

監視項目「AWS：Athena ログ情報取得」ではAmazon Athenaから取得したログをログファイルに蓄積します。このログファイルを監視することでアラートの検知をすることが可能です。

2.3.2.6.1. ログファイル

監視項目「AWS：Athena ログ情報取得」で取得したログファイルは、パラメータ「ログファイル」で指定したファイル(絶対パス)に出力されます。複数の監視タスクを設定する場合は、出力先のログファイルが重複しないように設定する必要があります。パラメータでログファイルを指定しない場合は、ログフォーマットがLTSVあるいはJSONによってファイル名が変わります。ただし、ファイル名に使用できない記号は「-」(半角ハイフン)に置き換えます。

ログフォーマットがLTSVの場合：

<千手ホームディレクトリ>/log/cloud.aws.d/AwsAthena_<ワークグループ名>_<データベース名>_<監視タスクID>.log

ログフォーマットがJSONの場合：

<千手ホームディレクトリ>/log/cloud.aws.d/AwsAthena_<ワークグループ名>_<データベース名>_<監視タスクID>.json

ログファイル名に含まれる「ワークグループ名」と「データベース名」は監視タスクのパラメータで指定できます。

ログメッセージに含まれる改行、タブ、「\」記号は、”\t”⇒”\\t” “\n”⇒ “\\n”, “\”⇒ “\\”に置換されログファイルに出力されます。

出力されるログファイルの文字コードは UTF-8 になります。テキストログ監視の設定で監視対象ログの「文字コードを指定する」を UTF-8 に指定して下さい。

2.3.2.6.2. ログフォーマット

以下にAmazon Athenaログ情報取得で取得したログファイルのレコード形式について説明します。レコードは LTSV形式で、項目間はタブ区切りとなります。

【Amazon Athenaログファイル　レコード形式】

- ログフォーマットがLTSVの場合：

ログメッセージ

表 2.10 AWSログファイルレコード形式

No.	項目	説明
1	ログ内容	各項目は「<項目名>:<値>」の形式で出力し、各項目間はTABで区切られています。タイムスタンプのフォーマットはyyyy-MM-d

- ログフォーマットがJSONの場合：

ログメッセージ

表 2.11 AWSログファイルレコード形式

No.	項目	説明
1	ログ内容	取得したログのメッセージが入ります。メッセージはJSONの形式で出力されます。

2.3.2.6.3. テキストログ監視の設定方法

以下にSenju DevOperation Conductorのテキストログ監視を利用して、Amazon Athenaログ情報取得で取得したログメッセージを監視する運用例を示します。この例では、ログメッセージにキーワードが発生時にメッセージモニタに通知されるようにログフィルタを登録し、監視する場合について説明します。

＜ログフィルタの登録＞
千手ブラウザのツリービューで＜ドメイン＞→“フィルタ”→“ログフィルタ”を選択します。ログフィルタのエンティティでリストビューの何も表示されていない部分でマウスの右ボタンを押してコンテキストメニューを表示し、[新規作成]メニューを選択します。ログフィルタのプロパティが表示されます。ログフィルタ名などの各項目を入力し[OK]ボタンを押下します。これにより、ログフィルタの登録が完了します。

＜フィルタ監視項目の追加＞
千手ブラウザのツリービューの＜ドメイン＞→“フィルタ”→“ログフィルタ”→＜ログフィルタ＞でフィルタ監視項目を登録するログフィルタを選択し、リストビューの何も表示されていない部分でマウスの右ボタンを押してコンテキストメニューを表示し、[新規作成]メニューを選択します。フィルタ監視項目のプロパティが表示されますので、指定フィールドを検知するキーワードで監視設定し、通知したいメッセージIDを登録します。

＜テキストログ監視の設定＞
アラートファイルのテキストログ監視を行うには、千手ブラウザのツリービューで、＜ドメイン＞→“ノードグループ”→＜ノードグループ＞を選択し、そのリストビューからAmazon Athenaログ情報取得のプローブとして設定したノードを選択し、マウスの右ボタンをクリックしコンテキストメニューを表示し、[プロパティ]メニューを選択します。ノードのプロパティウィンドウが表示されますので、[ログ監視]タブを選択します。ノードのプロパティ（[ログ監視]タブ）にて、監視対象のパス名とファイル名にAmazon Athenaログファイルを指定し、監視方法に先に作成したログフィルタを指定します。ログ監視を登録した後に、登録したノードに対して[反映(監視属性)]を実行することにより、ログファイルの監視を開始します。

以上で、テキストログ監視の設定方法は完了です。この設定によりAmazon Athenaログファイルにキーワードが出力された場合、メッセージモニタに通知されます。

警告

管理対象ノードにおいて千手が起動していない状態で、[反映(監視属性)]を行うと失敗しますので、注意して下さい。

2.3.2.7. Amazon SQS連携機能

監視項目「AWS：SQS メッセージ取得」ではAmazon SQSから取得したメッセージ情報をログファイルに蓄積します。このログファイルを監視することでAmazon SQSメッセージ情報を検知することが可能です。

2.3.2.7.1. ログファイル

監視項目「AWS：SQS メッセージ取得」で取得したログファイルは、パラメータ「ログファイル」で指定したファイル(絶対パス)に出力されます。複数の監視タスクを設定する場合は、出力先のログファイルが重複しないように設定する必要があります。パラメータでログファイルを指定しない場合は、ログフォーマットがLTSVあるいはJSONによってファイル名が変わります。ただし、ファイル名に使用できない記号は「-」(半角ハイフン)に置き換えます。

ログフォーマットがLTSVの場合：

<千手ホームディレクトリ>/log/cloud.aws.d/SQSMessage_<リージョン>_<キュー名>.log

ログフォーマットがJSONの場合：

<千手ホームディレクトリ>/log/cloud.aws.d/SQSMessage_<リージョン>_<キュー名>.json

複数の監視タスクを設定する場合は、出力先のログファイルが重複しないように設定する必要があります。リージョンとキュー名を指定して下さい。

メッセージ情報に含まれる改行、タブ、「\」記号は、”\t”⇒”\\t” “\n”⇒ “\\n”, “\”⇒ “\\”に置換されログファイルに出力されます。

出力されるログファイルの文字コードは UTF-8 になります。テキストログ監視の設定で監視対象ログの「文字コードを指定する」を UTF-8 に指定して下さい。

2.3.2.7.2. ログフォーマット

以下にAWS SQSメッセージ情報取得で取得したログファイルのレコード形式について説明します。レコードは LTSV形式で、項目間はタブ区切りとなります。

【AWS SQSメッセージ情報ログファイル　レコード形式】

- ログフォーマットがLTSVの場合：

タイムスタンプ　メッセージ情報内容

表 2.12 AWSログファイルレコード形式

No.	項目	説明
1	タイムスタンプ	「Timestamp:」に続き、取得したメッセージ情報の送信時刻のタイムスタンプ(UTC)が入ります。フォーマット：YYYY-M（例：2020-08-13T07:09:06Z）。
2	メッセージ情報内容	「LogMessage:」に続き、取得したメッセージ情報内容が入ります。メッセージ情報内容はJSONの形式で出力されま

- ログフォーマットがJSONの場合：

イベント内容

表 2.13 AWSログファイルレコード形式

No.	項目	説明
1	メッセージ情報内容	取得したメッセージ情報内容が入ります。メッセージ情報内容はJSONの形式で出力されます。

2.3.2.7.3. テキストログ監視の設定方法

以下にSenju DevOperation Conductorのテキストログ監視を利用して、AWS SQSメッセージ取得で取得したメッセージ情報を監視する運用例を示します。この例では、メッセージ内容にキーワードが発生した時にメッセージモニタに通知されるようにログフィルタを登録し、監視する場合について説明します。

＜ログフィルタの登録＞
千手ブラウザのツリービューで＜ドメイン＞→“フィルタ”→“ログフィルタ”を選択します。ログフィルタのエンティティでリストビューの何も表示されていない部分でマウスの右ボタンを押してコンテキストメニューを表示し、[新規作成]メニューを選択します。ログフィルタのプロパティが表示されます。ログフィルタ名などの各項目を入力し[OK]ボタンを押下します。これにより、ログフィルタの登録が完了します。

＜フィルタ監視項目の追加＞
千手ブラウザのツリービューの＜ドメイン＞→“フィルタ”→“ログフィルタ”→＜ログフィルタ＞でフィルタ監視項目を登録するログフィルタを選択し、リストビューの何も表示されていない部分でマウスの右ボタンを押してコンテキストメニューを表示し、[新規作成]メニューを選択します。フィルタ監視項目のプロパティが表示されますので、指定フィールドを検知するキーワードで監視設定し、通知したいメッセージIDを登録します。

＜テキストログ監視の設定＞
アラートファイルのテキストログ監視を行うには、千手ブラウザのツリービューで、＜ドメイン＞→“ノードグループ”→＜ノードグループ＞を選択し、そのリストビューからAWS SQSメッセージ情報取得のプローブとして設定したノードを選択し、マウスの右ボタンをクリックしコンテキストメニューを表示し、[プロパティ]メニューを選択します。ノードのプロパティウィンドウが表示されますので、[ログ監視]タブを選択します。ノードのプロパティ（[ログ監視]タブ）にて、監視対象のパス名とファイル名にAWS SQSメッセージ情報ログファイルを指定し、監視方法に先に作成したログフィルタを指定します。監視対象ログの「文字コードを指定する」を UTF-8 に指定し、ログ監視を登録した後に、登録したノードに対して[反映(監視属性)]を実行することにより、ログファイルの監視を開始します。

2.3.2.8. 汎用メトリクス監視機能

監視項目「AWS：メトリクス監視」では Amazon CloudWatch から任意のメトリクスの値を取得し、監視することでアラートの検知をすることが可能です。

注釈

Senju DevOperation Conductor Extension Packリリース時点でAmazon Web Servicesドキュメントに記載されているメトリクスが「リソースタイプ:メトリクス」から選択可能です。

2.3.2.8.1. 汎用メトリクス監視の設定方法

以下に汎用メトリクス監視の監視定義を千手ブラウザより登録する手順を記載します。例として AWS/EC2 のインスタンスで受信されたバイト数を10分間隔で監視します。

＜汎用メトリクス監視タスクの登録＞
千手ブラウザのツリービューで＜ドメイン＞→“モニタリング”→“千手カテゴリ”→“クラウドサービス”を選択します。クラウドサービスのエンティティでリストビューの何も表示されていない部分でマウスの右ボタンを押してコンテキストメニューを表示し、[新規作成]→[メトリクス監視タスク]メニューを選択します。汎用メトリクス監視タスクのプロパティが表示されますので、監視項目名で「AWS：メトリクス監視」を選択し、各項目を設定します。

「監視タスク名」を”AWS：メトリクス監視（AWS/EC2:NetworkIn）”のように適当な名前に変更します。「計算式の変数の値」フィールドの「リソースタイプ:メトリクス」の選択ボタンを押し、候補一覧から”AWS/EC2:NetworkIn”を選択し[OK]ボタンを押下します。「計算式」から”A1”を選択、「計算結果の型」から”小数”を選択、「計算結果の比較方法」から”通常”を選択、「計算式の変数Aの値」から”Sum”を選択、「単位」に”byte”を入力、「判定条件」に異常、警告と判定するしきい値を、「検査間隔」を10分に設定します。「パラメータ」フィールドの「ディメンション」に”InstanceId=i-xxxxxxxxxxxxxxxx”のように監視対象のEC2のインスタンスIDを指定します。[OK]ボタンを押し、監視タスクを登録します。

監視項目「AWS：メトリクス監視」の設定項目を以下に示します。

表 2.14 AWS：メトリクス監視の設定項目

項目名	設定内容
リソースタイプ:メトリクス	Amazon CloudWatch から監視するメトリクスを【ネームスペース:メトリクス】の形式で指定して下さい。候補一覧から選択する
計算式	計算に使用する式です。「計算式の変数Aの値」で指定したプロパティの値を計算し監視結果の値として扱います。「A0」や「A1
計算式の変数Aの値	Amazon CloudWatch から監視するメトリクスの統計を候補一覧から選択して下さい。以下の種類があります。 • Average • Maximum • Minimum • Samples • Sum • Unit
計算結果の型	計算結果の型です。計算結果を判定条件の値と比較する際の型となります。候補一覧から選択して下さい。以下の種類があり • 整数 • 小数 • 指数 • 文字列
単位	ノードモニタに表示される単位です。
計算結果の比較方法	「判定条件」フィールド(値)の値と、比較する方法を表します。候補一覧から選択して下さい。以下の種類があります。 • 通常 • 絶対値 • 前回との差分(新たな監視対象を正常とする) • 常に正常 • 前回との差分(新たな監視対象を異常とする) • 通常(無くなった監視対象を異常とする) • 初回との差分(新たな監視対象を正常とする) • 初回との差分(新たな監視対象を異常とする) • 合計

2.3.2.9. キャパシティ監視機能

監視項目「AWS：キャパシティ監視」では使用状況とサービスクォータを取得できるすべてのメトリクスにおいて、使用率（使用状況/サービスクォータ*100）を取得し、監視することでアラートの検知をすることが可能です。

注釈

Senju DevOperation Conductor Extension Packリリース時点でAmazon Web Servicesドキュメントに記載されている使用状況とサービスクォータを取得できるメトリクスが「リソースタイプ:メトリクス」から選択可能です。

2.3.2.9.1. キャパシティ監視の設定方法

以下にキャパシティ監視の監視定義を千手ブラウザより登録する手順を記載します。例としてCloudWatch使用状況メトリクスがアカウントで実行されたオペレーションの数を15分間隔で監視します。

＜キャパシティ監視タスクの登録＞

千手ブラウザのツリービューで＜ドメイン＞→“モニタリング”→“千手カテゴリ”→“監視タスク”→“クラウドサービス”を選択します。クラウドサービスのエン

ティティでリストビューの何も表示されていない部分でマウスの右ボタンを押してコンテキストメニューを表示し、[新規作成]→[メトリクス監視タスク]メニューを選択します。
[監視項目名]の選択ボタンを押し、候補一覧から[AWS：キャパシティ監視]を選択し[OK]ボタンを押下します。キャパシティ監視タスクのプロパティが表示されますので、監視項目名で「AWS：キャパシティ監視」を選択し、各項目を設定します。
「監視タスク名」を”AWS：キャパシティ監視（CallCount,CloudWatch）”のように適当な名前に変更します。「計算式の変数の値」フィールドの「リソースタイプ:メトリクス」の選択ボタンを押し、候補一覧から”AWS/Usage:CallCount,Service=CloudWatch,Type=API,Resource=DeleteAlarms,Class=None”を選択し[OK]ボタンを押下します。「計算式」から”100*A1/B1”を選択、「計算結果の型」から”小数”を選択、「計算結果の比較方法」から”通常”を選択、「単位」に”%”を入力、「判定条件」に異常、警告と判定するしきい値を、「検査間隔」を15分に設定します。「パラメータ」フィールドの「リージョン」に”ap-northeast-1”に指定し、「統計」に”Average”を指定し、「ゼロパブリッシュ」に”ON”を指定します。[OK]ボタンを押し、監視タスクを登録します。

監視項目「AWS：キャパシティ監視」の設定項目を以下に示します。

表 2.15 AWS：キャパシティ監視の設定項目

項目名	設定内容
リソースタイプ:メトリクス	Amazon CloudWatch から監視できる使用状況メトリクスを【ネームスペース:メトリクス】の形式で指定して下さい。候補一覧か
計算式	計算に使用する式です。「A1」は使用状況メトリックの値で「B1」はサービスクォータの値を表します。計算式は【100*A1/B1】と
計算結果の型	計算結果の型です。計算結果を判定条件の値と比較する際の型となります。現状は【小数】と固定されています。
単位	ノードモニタに表示される単位です。
計算結果の比較方法	「判定条件」フィールド(値)の値と、比較する方法を表します。現状は【通常】と固定されています。

2.4. クラウド監視(Azure)監視設定手順と使い方

Azure監視設定を行う際には、以下の設定が必要になります。

- ライセンスの購入とライセンスキーの入手
    - Azure監視

注釈

監視対象数に応じて、カスタムセンサーのライセンスが必要です。

- Senju DevOperation Conductor Extension Packの入手と適用

    運用管理サーバーおよび、クラウド監視を行う管理対象ノードに、同一バージョンの Senju DevOperation Conductor Extension Pack の適用が必要です
    - 運用管理サーバー(千手マネージャ)への適用(監視項目の更新)
    - 管理対象ノード(千手エージェント(プローブノード))への適用(情報取得コマンドの更新)

警告

適用可能な Senju DevOperation Conductor のバージョンやパッチ状況に制限がある場合があります。詳しくは、Senju DevOperation Conductor Extension Pack の README をご参照下さい。

参考

Senju DevOperation Conductor Extension Packの適用手順につきましては、Senju DevOperation Conductor Extension Pack の README をご参照下さい。

注釈

Senju DevOperation Conductor Extension Packの適用に際しては、千手システムの停止は不要ですが、関連する監視タスクの停止が必要です。

2.4.1. 設定

- **説明**

    モニタリングサブシステムを用いてAzureの監視項目を使用するための設定を行います。

- **設定手順**

    Azure監視を設定するには以下の手順が必要です。
    - Microsoft Azureアカウントの登録
    - 認証設定
    - Azureユーザー情報設定ファイルの作成

2.4.1.1. Microsoft Azureアカウントの登録

Azureの監視項目の利用において、事前にMicrosoft Azureアカウントの登録が必要です。Microsoft Azureサイトよりアカウント登録を行って下さい。

2.4.1.2. 認証設定

2.4.1.2.1. マネージドIDで認証する

Azure内のエージェントからAzure監視を行う場合は、システム割り当てマネージドID(仮想マシン)、ユーザ割り当てマネージドIDを利用した認証が行えます。Azureユーザー情報設定ファイル(sj_azure_user.conf)の作成 でAzureユーザー情報設定ファイルのmanageIdを1に設定して下さい。マネージドIDの割り当てが1つの場合はAzureユーザー情報設定ファイルのuserAssignedManagedIdを設定する必要はありません。複数のマネージドIDが割り当てられている場合、userAssignedManagedIdを設定することで認証を行うマネージドIDを指定することが可能です。

マネージドIDの設定方法は下記Microsoftのサイトをご参照下さい。

参考URL：https://docs.microsoft.com/ja-jp/azure/active-directory/managed-identities-azure-resources/overview (2020年12月現在)

2.4.1.2.2. Azure ADへのアプリケーションの登録

Azure外のエージェントからAzure監視を行う場合は、Azure ADアプリケーションを利用した認証を行います。Azureポータルサイトより Azure ADへアプリケーションの登録を行って下さい。
シークレットキーで認証する場合、AzureポータルサイトよりclientId、tenantId、keyを取得して下さい。Azureユーザー情報設定ファイル(sj_azure_user.conf)の作成 でAzureユーザー情報設定ファイルにclientId、tenantId、keyを設定して下さい。
証明書で認証する場合、事前にアプリケーション登録ポータルで証明書をアプリケーションに登録してください。AzureポータルサイトよりclientId、tenantIdを取得し、Azureユーザー情報設定ファイル(sj_azure_user.conf)の作成 でAzureユーザー情報設定ファイルにclientId、tenantId、certificatePath、certificatePasswordを設定して下さい。

Azure ADへアプリケーションの登録方法と証明書のアップロード方法は下記Microsoftのサイトをご参照下さい。

参考URL：https://learn.microsoft.com/ja-jp/azure/active-directory/develop/howto-create-service-principal-portal (2023年3月現在)

2.4.1.2.3. ロールの割り当て

Azure監視を使用するため、サブスクリプションのアクセス制御から、利用する認証方法に対して「Azure監視に必要なアクセス権限」に示すロールの割り当てを行って下さい。

表 2.16 Azure監視に必要なアクセス

監視項目	必要なロール
Azure: Batch ~	Microsoft.Insights/Metrics/Read Microsoft.Batch/batchAccounts/read
Azure: Redis Cache ~	Microsoft.Insights/Metrics/Read Microsoft.Cache/Redis/read
Azure: Compute ~	Microsoft.Insights/Metrics/Read Microsoft.Compute/virtualMachines/read Microsoft.Compute/virtualMachineScaleSets/read Microsoft.Compute/virtualMachineScaleSets/virtualMachines/read
Azure: IoT Hub ~	Microsoft.Insights/Metrics/Read Microsoft.Devices/IotHubs/read
Azure: Event Hub ~	Microsoft.Insights/Metrics/Read Microsoft.EventHub/namespaces/read Microsoft.EventHub/clusters/read
Azure: Logic Apps ~	Microsoft.Insights/Metrics/Read Microsoft.Logic/workflows/read
Azure: Search ~	Microsoft.Insights/Metrics/Read Microsoft.Search/searchServices/read
Azure: SQL Database ~	Microsoft.Insights/Metrics/Read Microsoft.Sql/servers/databases/read
Azure: SQL Elastic Pools ~	Microsoft.Insights/Metrics/Read Microsoft.Sql/servers/elasticpools/read
Azure: SQL Managed Instance ~	Microsoft.Insights/Metrics/Read Microsoft.Sql/managedInstances/read
Azure: Stream Analytics ~	Microsoft.Insights/Metrics/Read Microsoft.StreamAnalytics/streamingjobs/read
Azure: App Service ~	Microsoft.Insights/Metrics/Read Microsoft.Web/serverFarms/read
Azure: Web App ~	Microsoft.Insights/Metrics/Read Microsoft.Web/serverfarms/read Microsoft.Web/sites/read Microsoft.Web/sites/slots/read
Azure: API Management ~	Microsoft.Insights/Metrics/Read Microsoft.ApiManagement/service/read
Azure: Container Instances ~	Microsoft.Insights/Metrics/Read Microsoft.ContainerInstance/containerGroups/read
Azure: Container Service ~	Microsoft.Insights/Metrics/Read Microsoft.ContainerService/managedClusters/read
Azure: Azure Database for PostgreSQL ~	Microsoft.Insights/Metrics/Read Microsoft.DBforPostgreSQL/servers/read
Azure: Azure Cosmos DB ~	Microsoft.Insights/Metrics/Read Microsoft.DocumentDB/databaseAccounts/read
Azure: Load balancers ~	Microsoft.Insights/Metrics/Read Microsoft.Network/loadBalancers/read
Azure: Public IP DDoS ~	Microsoft.Insights/Metrics/Read Microsoft.Network/publicIPAddresses/read
Azure: ExpressRoute circuits ~	Microsoft.Insights/Metrics/Read Microsoft.Network/expressRouteCircuits/read
Azure: Storage accounts blob ~	Microsoft.Insights/Metrics/Read Microsoft.Storage/storageAccounts/blobServices/read
Azure: メトリクス監視	上記にある各メトリクス監視用のロール
Azure: Service Health ~	Microsoft.ResourceHealth/events/read
Azure: Log Analytics ~	Microsoft.operationalinsights/workspaces/query/read
Azure: DataExplorer ~	サブスクリプションのアクセス制御からロールの割り当ては不要で、AzureDataExplorerクラスターの「セキ
Azure: 利用料金 ~ Azure: リソース使用量(EA)	課金データ閲覧者

2.4.1.3. Azureシステム情報設定ファイル(sj_azure_sys.conf)の作成

sj_azure_sys.confファイルは、Azureに関する監視を行うためにシステム情報を記載する設定ファイルです。

Azureシステム情報設定ファイル(千手ホームディレクトリ/dat/opt/sj_azure_sys.conf)を作成し、以下の項目を設定して下さい。

表 2.17 sj_azure_sys.confの記述内容

項目	省略	デフォルト	暗号化対象	説明
offerDurableId	可	MS-AZR-0003P	×	Microsoft Azureプラン(従量課金の場合はMS-AZR-0003P
currency	可	JPY	×	料金の単位（JPY:日本円固定）
locale	可	en-US	×	料金を取得するリージョンのロケール
region	可	JP	×	料金を取得するリージョンのロケールを2文字で指定します。
monitorApiVersion	可	2018-01-01	×	メトリックAPIのバージョン
billingApiVersion	可	2015-06-01-preview	×	Billing API のバージョン
loginURL	可	https://login.windows.net	×	Azure Active Directory への承認に利用するエンドポイントの
apiURL	可	https://management.azure.com	×	Azure API のエンドポイント
providerApiVer	可	2014-04-01-preview	×	providerAPIのバージョン
waitTime	可	—	×	省略する場合はAPI実行時のタイムアウト時間が30(単位:秒
retryCount	可	—	×	省略する場合はAPI実行失敗時のリトライ回数が3になります。
logMaxSize	可	—	×	省略する場合はログファイルを出力する際の最大サイズが102
logMaxCnt	可	—	×	省略する場合はログファイルを出力する際のローテーション最大
queryLimit	可	—	×	省略する場合は1回のAPI実行で最大取得件数が5000にな
logBufferTime	可	—	×	省略する場合は前回取得した最後のログより遡る時間が5(単
dataExplorerWaitTime	可	—	×	省略する場合はAzureDataExplorerAPI実行時のタイムアウ
logFormat	可	—	×	取得したログの出力フォーマットをLTSVもしくはJSONに切り替

- offerDurableId、currency、locale、region、billingApiVersionは「Azure：利用料金（当月）」「Azure：利用料金（昨日）」の監視を行う場合に設定して下さい。
- offerDurableId:Microsoft Azureプランの詳細は右記URLを参照してください。https://azure.microsoft.com/ja-jp/support/legal/offer-details/
- currency:国と通貨単位の組み合わせは右記URLを参照してください。https://azure.microsoft.com/ja-jp/offers/ms-azr-0003p/
- currency:通貨の相場は右記URLを参照してください。https://azureprice.net/exchange
- region:日本=JP、アメリカ=US、ドイツ=DEとしてください。
- monitorApiVersion:メトリック API のバージョンは 2018-01-01 です。
- providerApiVer:リソースエクスプローラに合わせて、2014-04-01-previewを指定します。
- logMaxSize、logMaxCnt:Azureユーザー情報設定ファイル(sj_azure_user.conf)で値を設定する場合は、ユーザー情報設定ファイルの値を使います。
- 一回以上ログを取得している状態でlogBufferTimeを現在よりも大きい値に変更した場合、変更後の1回目の実行で過去に取得したログを重複して取得する場合があります。ご注意ください。
- dataExplorerWaitTime:AzureDataExplorerで指定したクエリが180秒以上かかる場合、dataExplorerWaitTimeの値を大きくしてください。

- sj_azure_sys.conf の記載例

```
{
        "offerDurableId": "MS-AZR-0003P",
        "currency": "JPY",
        "locale": "en-US",
        "region": "JP",
        "monitorApiVersion": "2018-01-01",
        "billingApiVersion": "2015-06-01-preview",
        "loginURL": "https://login.windows.net",
        "apiURL": "https://management.azure.com",
        "providerApiVer": "2014-04-01-preview",
        "waitTime": "",
        "retryCount": "",
        "logMaxSize": "",
        "logMaxCnt": "",
        "queryLimit": "",
        "logBufferTime": "",
        "dataExplorerWaitTime": "",
        "logFormat": ""
}
```

2.4.1.4. Azureユーザー情報設定ファイル(sj_azure_user.conf)の作成

sj_azure_user.confファイルは、Azureに関する監視を行うためにユーザーが設定する情報を記載する設定ファイルです。

sj_azure_user.confはデフォルトで「千手ホームディレクトリ/dat/opt/sj_azure_user.conf」に作成されます。パスおよびファイル名は任意に指定することが可能です。

設定方法については、sj_setup_azure ー Azureユーザー情報設定ファイル更新 ー を参照して下さい。

表 2.18 sj_azure_user.confの記述内容

項目	省略	デフォルト	暗号化対象	説明
clientId	可	—	×	Azure接続用のID(Azure ポータルで登録したアプリのID)
tenantId	可	—	×	Azure接続用のテナントID(Azure Active Directory のディレクトリID)
proxyURL	可	—	×	Azure接続時に経由するプロキシサーバー
closingDate	可	—	×	Billingで使用する締め日
key	可	—	○	Azure ポータルで登録したアプリのキー(暗号化後のキー)
manageId	可	—	×	マネージドIDで認証するかどうか（1:認証する/省略:認証しない）
proxyUsername	可	—	×	プロキシサーバーアクセス用ユーザーID
proxyPassword	可	—	○	プロキシサーバーアクセス用パスワード(暗号化後のパスワード)
enrollmentNumber	可	—	×	BillingAPIアクセス用のアカウントナンバー
apiKey	可	—	○	BillingAPIアクセス用のAPIキー(暗号化後のAPIキー)
logMaxSize	可	—	×	省略する場合はログファイルを出力する際の最大サイズが10240(単位:KB)になります
logMaxCnt	可	—	×	省略する場合はログファイルを出力する際のローテーション最大個数が7になります。
logFormat	可	—	×	取得したログの出力フォーマットをLTSVもしくはJSONに切り替えます。省略する場合
userAssignedManagedId	可	—	×	認証用のユーザー割り当てマネージドID
certificatePath	可	—	×	証明書ファイルの絶対パス
certificatePassword	可	—	○	証明書パスワード(暗号化後のパスワード)

- clientID、tenantID、keyはAzure ポータルで確認して下さい。Azure ADアプリケーションを利用した認証を行う場合に指定して下さい。マネージドIDで認証する場合は設定する必要はありません。
- proxyURLを省略した場合、プロキシサーバーを利用しません。
- プロキシサーバーアクセス用ユーザーIDおよびパスワードの両方を指定しなかった場合、プロキシサーバーの認証に利用しません。
- keyはアプリ登録時に確認できるので忘れずに控えて下さい。
- enrollmentNumber、apiKeyは「Azure：利用料金(EA)」「Azure：リソース使用量(EA)」の監視を行う場合に設定して下さい。
- closingDateには"01"～"28"の2桁で指定して下さい。"01"を指定することで「Azure：利用料金（当月）」の毎月1日の監視結果には前月1日から当日までの料金が報告され、毎月2日から月末までは当月1日から当日までの料金が報告されます。
- userAssignedManagedIdを利用する場合は、manageIdを1に設定する必要があります。システムマネージドIDを利用する場合、userAssignedManagedIdを設定する必要はありません。
- certificatePath、certificatePasswordを利用する場合は、manageIdを0に設定する必要があります

- sj_azure_user.conf の記載例

```
{
        "clientId": "XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX",
        "tenantId": "XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX",
        "proxyURL": "http://ipアドレス:ポート番号"
        "closingDate": "01",
        "key": "=AVvMrR5jTefXB9prmQ=="
        "manageId": "",
        "proxyUsername": "",
        "proxyPassword": "",
        "enrollmentNumber": "",
        "apiKey": "",
        "logMaxSize": "",
        "logMaxCnt": "",
        "logFormat": "",
        "userAssignedManagedId": "",
        "certificatePath": "",
        "certificatePassword": ""
}
```

2.4.1.4.1. sj_setup_azure ー Azureユーザー情報設定ファイル更新 ー

- 指定形式

- [参照]

```
sj_setup_azure
```

- [作成＆更新]

```
sj_setup_azure
  [-ci[Connection ID(Application (client)ID which registerd in Azure Portal)]]
  [-ti[Tenant ID(Directory ID of Azure Active Directory)]]
  [-pu[Proxy server]]
  [-cd[Closing date of Billing]]
  [-key[key of application registered in Azure portal]]
  [-mi[managedID of certify]]
  [-pn[user of proxy server]]
  [-en[account nember of BillingAPI access]]
  [-pp[password for access to proxy server]]
  [-ak[API key for billing API access]]
  [-cf[Azure user information setting file path]]
  [-lms[If omitted, the maximum size of the log file output by log monitoring is
  10240 (unit: KB)]]
  [-lmc[If omitted, the maximum number of log file rotations output by log
  monitoring is 7.]]
  [-uami[User assigned managed id]]
  [-ctf[Absolute path of certificate file]]
  [-ctp[Password of certificate]]
```

- 目的

  Azureユーザー情報設定ファイル(/dat/opt/sj_azure_user.conf) の現在値の参照、作成と更新を行います。

- オプション

  - -ci

    Azure接続用のID(Azure ポータルで登録したアプリのID)（clientId）に設定する値を指定して下さい。
    値を省略するとAzureユーザー情報設定ファイルに設定されている値を削除します。

  - -ti

    Azure接続用のテナントID(Azure Active Directory のディレクトリID)（tenantId）に設定する値を指定して下さい。
    値を省略するとAzureユーザー情報設定ファイルに設定されている値を削除します。

  - -pu

    Azure接続時に経由するプロキシサーバー（proxyURL）に設定する値を指定して下さい。
    値を省略するとAzureユーザー情報設定ファイルに設定されている値を削除します。

  - -cd

    Billingで使用する締め日（closingDate）に設定する値を指定して下さい。
    値を省略するとAzureユーザー情報設定ファイルに設定されている値を削除します。

  - -key

    Azure ポータルで登録したアプリのキー（key）に設定する場合に指定して下さい。
    設定値の指定は対話形式で行われます。
    この項目は暗号化した値がAzureユーザー情報設定ファイルに書き込まれます。

  - -mi

    マネージドIDで認証するかどうか（manageId）に設定する値（1:認証する/省略:認証しない）を指定して下さい。
    値を省略するとAzureユーザー情報設定ファイルに設定されている値を削除します。

  - -pn

    プロキシサーバーのユーザ（proxyUsername）に設定する値を指定して下さい。
    値を省略するとAzureユーザー情報設定ファイルに設定されている値を削除します。

- -pp

  プロキシサーバーのパスワード(proxyPassword)に設定する値を指定して下さい。
  設定値の指定は対話形式で行われます。
  この項目は暗号化した値がAzureユーザー情報設定ファイルに書き込まれます。

- -en

  BillingAPIアクセス用のアカウントナンバー(enrollmentNumber)に設定する値を指定して下さい。
  値を省略するとAzureユーザー情報設定ファイルに設定されている値を削除します。

- -ak

  BillingAPIアクセス用のAPIキー(apiKey)に設定する値を指定して下さい。
  設定値の指定は対話形式で行われます。
  この項目は暗号化した値がAzureユーザー情報設定ファイルに書き込まれます。

- -cf

  現在値の参照、作成と更新を行う任意のAzureユーザー情報設定ファイルを絶対パスで指定して下さい。
  値を省略した場合はデフォルトのAzureユーザー情報設定ファイル(/dat/opt/sj_azure_user.conf) の参照、作成と更新を行います。

- -lms

  出力するログファイルの、最大サイズ(logMaxSize)に設定する値を指定してください。
  値を省略するとAzureユーザー情報設定ファイルに設定されている値を削除します。

- -lmc

  出力するログファイルの、ローテーション最大個数(logMaxCnt)に設定する値を指定してください。
  値を省略するとAzureユーザー情報設定ファイルに設定されている値を削除します。

- -uami

  認証用のユーザー割り当てマネージドID(userAssignedManagedId)に設定されている値を指定して下さい。
  値を省略するとAzureユーザー情報設定ファイルに設定されている値を削除します。

- -ctf

  証明書ファイルの絶対パス(certificatePath)に設定する値を指定して下さい。
  値を省略するとAzureユーザー情報設定ファイルに設定されている値を削除します。

- -ctp

  証明書パスワード(certificatePassword)に設定する値を指定して下さい。
  設定値の指定は対話形式で行われます。
  この項目は暗号化した値がAzureユーザー情報設定ファイルに書き込まれます。

- 実行結果

  - (例1)現在の設定値参照

```
% sj_setup_azure
{
        "clientId": "ABCD",
        "tenantId": "XXXXX",
        "proxyURL": "XXXXX",
        "closingDate": "DD",
        "key": "**********"
        "manageId": "",
        "proxyUsername": "",
        "proxyPassword": "",
        "enrollmentNumber": "",
        "apiKey": "",
        "logMaxSize": "",
        "logMaxCnt": "",
        "userAssignedManagedId": "",
        "certificatePath": "",
        "certificatePassword": ""
}

%
```

- (例2)クライアントIDとテナントID、キーを設定

```
% sj_setup_azure -ciXXXXX-XXXXX -tiXXXX-XXXX -key
Please enter the value.
        "key":

        The value of clientId has changed from (ABCD) to (XXXXX-XXXXX).
        The value of tenantId has changed from (XXXXX) to (XXXX-XXXX).
        The value of key has changed from (**********) to (**********).

The Azure user information file successfully updated.

% sj_setup_azure
{
        "clientId": "XXXXX-XXXXX",
        "tenantId": "XXXX-XXXX",
        "proxyURL": "XXXXX",
        "closingDate": "DD",
        "key": "**********"
        "manageId": "",
        "proxyUsername": "",
        "proxyPassword": "",
        "enrollmentNumber": "",
        "apiKey": "",
        "logMaxSize": "",
        "logMaxCnt": "",
        "userAssignedManagedId": "",
        "certificatePath": "",
        "certificatePassword": ""
}

%
```

- (例3)設定を削除

```
% sj_setup_azure -ci -ti -key
Please enter the value.
        "key":

        The value of clientId has changed from (XXXXX-XXXXX) to ().
        The value of tenantId has changed from (XXXX-XXXX) to ().
        The value of key has changed from (**********) to (**********).

The Azure user information file successfully updated.

% sj_setup_azure
{
        "clientId": "",
        "tenantId": "",
        "proxyURL": "XXXXX",
        "closingDate": "DD",
        "key": ""
        "manageId": "",
        "proxyUsername": "",
        "proxyPassword": "",
        "enrollmentNumber": "",
        "apiKey": "",
        "logMaxSize": "",
        "logMaxCnt": "",
        "userAssignedManagedId": "",
        "certificatePath": "",
        "certificatePassword": ""
}

%
```

注釈

- 暗号化対象項目の標準出力への表示は全てアスタリスクでマスクされます。
- 暗号化対象項目の値の設定は、キーボードからの入力が一切表示されません。コピー＆ペーストで入力することをお勧めします。
- 暗号化対象項目の値を削除する場合、何も入力せずにリターンキーを押下して下さい。

- 標準エラー出力
  - Failed to acquire Senju home directory.
  - The Azure user information file does not exist.
  - Invalid data have been set in this file.
  - Failed to update the Azure user information file.

- 終了ステータス
    - 0：正常終了
    - 1：異常終了

2.4.1.4.2. Azureユーザー情報設定ファイル更新コマンドの登録

Azureユーザー情報設定ファイルの現在値の参照、作成と更新を行うため、Azureユーザー情報設定ファイル更新コマンドを千手ブラウザからユーザーコマンドに登録します。詳細な手順については、ユーザーズガイド**「2.3.2.1 ユーザーコマンド」**を参照して下さい。

- ユーザーコマンドグループの作成

  Azureユーザー情報設定ファイル更新コマンドを登録するユーザーコマンドグループを千手ブラウザから登録して下さい。

- Azureユーザー情報設定ファイル更新コマンドの登録

  作成したユーザーコマンドグループに、以下に示す起動シーケンスを指定してコマンドを登録して下さい。

    - 現在値の参照

```
sj_remshe "@ノード名@" -l "@ユーザ名@" sj_setup_azure "-cf@@対象ファイルパス@@"
```

    - 作成と更新

```
sj_remshe "@ノード名@" -l "@ユーザ名@" sj_setup_azure "-ci@@Azure接続用ID@@" "-ti@@Azure接続用テナントID@@" "-pu@@Azure接続時に経由するプロキシサーバー@@" "-cd@@Billingで使用する締め日@@" "-key@@Azure ポータルで登録したアプリのキー@@" "-mi@@マネージドID認証有無@@" "-pn@@プロキシサーバーのユーザ名@@" "-pp@@プロキシサーバーのパスワード@@" "-ak@@BillingAPIアクセス用のAPIキー@@" "-cf@@対象ファイルパス@@" "-lms@@ログファイルの最大サイズ@@" "-lmc@@ログファイルのローテーション最大個数@@" "-uami@@認証用のユーザー割り当てマネージドID@@" "-ctf@@証明書ファイルの絶対パス@@" "-ctp@@証明書のパスワード@@"
```

注釈

上記の起動シーケンスは項目を全て変更する仕様となっています。項目別に変更を行いたい場合は、起動シーケンスから任意の「**-オプション@@パラメータ名@@**」を指定したユーザーコマンドを別途登録して下さい。

（例）sj_remshe "@ノード名@" -l "@ユーザ名@" sj_setup_azure "-ci@@Azure接続用ID@@" "-cf@@対象ファイルパス@@"

2.4.2. 使い方

Azure REST APIで情報を取得し、Senju DevOperation Conductorのモニタリング機能を使って、監視することができます。

監視定義を千手ブラウザより登録し、監視を実施します。監視結果は、各種モニタ画面（グローバルノードモニタ／ノードモニタ）にてその監視状況を表示できます。予め設定したしきい値により障害を検知した場合は、メッセージモニタにメッセージが通知されます。
（モニタリング機能については、ユーザーズガイド「 **4．モニタリング** 」を参照して下さい。）

注釈

監視項目によっては、監視間隔を10分未満に設定すると値が取得できないことがあります。その場合は監視間隔を10分以上に設定して下さい。

参考

各種パラメータの設定値が分からない場合は、Azure ポータルにて確認して下さい。

2.4.2.1. Azure監視の各パラメータの上限値および制限事項

Azure監視で設定できるパラメータにはMicrosoft Azureの上限値とは別に千手固有の上限値および制限事項があります。下記の表に上限値および制限事項を示します。

表 2.19 Azure監視の各パラメータの上限値および制限事項

パラメータ名	上限値、制限事項
タグ名	80byte
タグ値	80byte

参考URL：https://docs.microsoft.com/ja-jp/azure/architecture/best-practices/naming-conventions#naming-rules-and-restrictions （2018年11月現在）

2.4.2.2. Azure Log Analytics連携機能

監視項目「Azure：Log Analytics ログ情報取得」では Azure Log Analytics から取得したログをログファイルに蓄積します。このログファイルを監視することでアラートの検知をすることが可能です。

2.4.2.2.1. ログファイル

監視項目「Azure：Log Analytics ログ情報取得」で取得したログファイルは、パラメータ「ログ出力ファイル」で指定したファイル(絶対パス)に出力されます。複数の監視タスクを設定する場合は、出力先のログファイルが重複しないように設定する必要があります。パラメータでログファイルを指定しない場合は、ログフォーマットがLTSVあるいはJSONによってファイル名が変わります。ただし、ファイル名に使用できない記号は「-」(半角ハイフン)に置き換えます。

ログフォーマットがLTSVの場合：

<千手ホームディレクトリ>\log\cloud.azure.d\sjANM_LogAnalytics_<リソースグループ名>_<ワークスペース名>_<識別子>.log

ログフォーマットがJSONの場合：

<千手ホームディレクトリ>\log\cloud.azure.d\sjANM_LogAnalytics_<リソースグループ名>_<ワークスペース名>_<識別子>.json

複数の監視タスクを設定する場合は、出力先のログファイルが重複しないように設定する必要があります。リソースグループ名、ワークスペース名、識別子を指定して下さい。

ログ内容に含まれる改行、タブ、「\」記号は、"\t"⇒"\\t" "\n"⇒ "\\n", "\"⇒ "\\"に置換されログファイルに出力されます。

出力されるログファイルの文字コードは UTF-8 になります。テキストログ監視の設定で監視対象ログの「文字コードを指定する」を UTF-8 に指定して下さい。

2.4.2.2.2. ログフォーマット

以下にAzure Log Analytics ログ情報取得で取得したログファイルのレコード形式について説明します。レコードは LTSV形式で、項目間はタブ区切りとなります。

【Azure Log Analyticsログファイル　レコード形式】

- ログフォーマットがLTSVの場合：

システム時間　プロセス名[プロセスID]　ログ内容

表 2.20 Azureログファイルレコード形式

No.	項目	説明
1	タイムスタンプ	「Timestamp:」に続き、取得したログが出力されたタイムスタンプ(UTC)が入ります。フォーマット：YYYY-MM-DDThh:mm:dd ※通常は「TimeGenerated」の時間がタイムスタンプとなります。出力するログ情報の中に、「EventSubmissionTimestamp
2	ログ内容	クエリにより取得されたログ内容が入ります。各項目は「<項目名>:<値>」の形式で出力され、各項目間はTABで区切られて ログは「TimeGenerated」のソート順で出力されます。出力するログ情報の中に、「EventSubmissionTimestamp」が存在す

- ログフォーマットがJSONの場合：

ログ内容

表 2.21 Azureログファイルレコード形式

No.	項目	説明
1	ログ内容	取得したログ内容が入ります。ログ内容はJSONの形式で出力されます。

2.4.2.2.3. テキストログ監視の設定方法

以下にSenju DevOperation Conductorのテキストログ監視を利用して、Azure Log Analytics ログ情報取得で取得したログ内容を監視する運用例を示します。この例では、ログ内容にキーワードが発生時にメッセージモニタに通知されるようにログフィルタを登録し、監視する場合について説明します。

＜ログフィルタの登録＞
千手ブラウザのツリービューで＜ドメイン＞→"フィルタ"→"ログフィルタ"を選択します。ログフィルタのエンティティでリストビューの何も表示されていない部分でマウスの右ボタンを押してコンテキストメニューを表示し、[新規作成]メニューを選択します。ログフィルタのプロパティが表示されます。ログフィルタ名などの各項目を入力し[OK]ボタンを押下します。これにより、ログフィルタの登録が完了します。

＜フィルタ監視項目の追加＞
千手ブラウザのツリービューの＜ドメイン＞→“フィルタ”→“ログフィルタ”→＜ログフィルタ＞でフィルタ監視項目を登録するログフィルタを選択し、リストビューの何も表示されていない部分でマウスの右ボタンを押してコンテキストメニューを表示し、[新規作成]メニューを選択します。フィルタ監視項目のプロパティが表示されますので、指定フィールドを検知するキーワードで監視設定し、通知したいメッセージIDを登録します。

＜テキストログ監視の設定＞
アラートファイルのテキストログ監視を行うには、千手ブラウザのツリービューで、＜ドメイン＞→“ノードグループ”→＜ノードグループ＞を選択し、そのリストビューからAzure Log Analytics ログ情報取得のプローブとして設定したノードを選択し、マウスの右ボタンをクリックしコンテキストメニューを表示し、[プロパティ]メニューを選択します。ノードのプロパティウィンドウが表示されますので、[ログ監視]タブを選択します。ノードのプロパティ([ログ監視]タブ)にて、監視対象のパス名とファイル名にAzure Log Analytics ログファイルを指定し、監視方法に先に作成したログフィルタを指定します。ログ監視を登録した後に、登録したノードに対して[反映(監視属性)]を実行することにより、ログファイルの監視を開始します。

以上で、テキストログ監視の設定方法は完了です。この設定によりAzure Log Analytics ログファイルにキーワードが出力された場合、メッセージモニタに通知されます。

警告

管理対象ノードにおいて千手が起動していない状態で、[反映(監視属性)]を行うと失敗しますので、注意して下さい。

2.4.2.3. Azure Service Health監視機能

監視項目「Azure:Service Health情報取得」ではAzure Service Healthから取得したイベント情報をログファイルに蓄積します。このログファイルを監視することでService Health情報を検知することが可能です。

2.4.2.3.1. ログファイル

監視項目「Azure：Service Health情報取得」で取得したログファイルは、パラメータ「ログ出力ファイル」で指定したファイル(絶対パス)に出力されます。複数の監視タスクを設定する場合は、出力先のログファイルが重複しないように設定する必要があります。パラメータでログファイルを指定しない場合は、ログフォーマットがLTSVあるいはJSONによってファイル名が変わります。ただし、ファイル名に使用できない記号は「-」(半角ハイフン)に置き換えます。

ログフォーマットがLTSVの場合：

<千手ホームディレクトリ>/log/cloud.azure.d/Service Health_<サブスクリプションID>_<モード>.log

ログフォーマットがJSONの場合：

<千手ホームディレクトリ>/log/cloud.azure.d/Service Health_<サブスクリプションID>_<モード>.json

複数の監視タスクを設定する場合は、出力先のログファイルが重複しないように設定する必要があります。サブスクリプションIDとモードを指定して下さい。

イベント情報に含まれる改行、タブ、「\」記号は、”\t”⇒”\\t” “\n”⇒ “\\n”, “\”⇒ “\\”に置換されログファイルに出力されます。

出力されるログファイルの文字コードは UTF-8 になります。テキストログ監視の設定で監視対象ログの「文字コードを指定する」を UTF-8 に指定して下さい。

2.4.2.3.2. ログフォーマット

以下にAzure Service Health情報取得で取得したログファイルのレコード形式について説明します。レコードは LTSV形式で、項目間はタブ区切りとなります。

【Azure Service Health情報ログファイル　レコード形式】

- ログフォーマットがLTSVの場合：

タイムスタンプ　イベント内容

表 2.22 Azureログファイルレコード形式

No.	項目	説明
1	タイムスタンプ	「Timestamp:」に続き、取得したイベント情報の作成時間または更新時間のタイムスタンプ(UTC)が入ります。フォーマット:Y（例:2020-08-13T07:09:06Z）。
2	イベント内容	「Service Health」に続き、取得したイベント内容が入ります。イベント内容はJSONの形式で出力されます。

- ログフォーマットがJSONの場合:

イベント内容

表 2.23 Azureログファイルレコード形式

No.	項目	説明
1	イベント内容	取得したイベント内容が入ります。イベント内容はJSONの形式で出力されます。

2.4.2.3.3. テキストログ監視の設定方法

以下にSenju DevOperation Conductorのテキストログ監視を利用して、Azure Service Health情報取得で取得したイベント情報を監視する運用例を示します。この例では、イベント内容にキーワードが発生した時にメッセージモニタに通知されるようにログフィルタを登録し、監視する場合について説明します。

＜ログフィルタの登録＞
千手ブラウザのツリービューで＜ドメイン＞→“フィルタ”→“ログフィルタ”を選択します。ログフィルタのエンティティでリストビューの何も表示されていない部分でマウスの右ボタンを押してコンテキストメニューを表示し、[新規作成]メニューを選択します。ログフィルタのプロパティが表示されます。ログフィルタ名などの各項目を入力し[OK]ボタンを押下します。これにより、ログフィルタの登録が完了します。

＜フィルタ監視項目の追加＞
千手ブラウザのツリービューの＜ドメイン＞→“フィルタ”→“ログフィルタ”→＜ログフィルタ＞でフィルタ監視項目を登録するログフィルタを選択し、リストビューの何も表示されていない部分でマウスの右ボタンを押してコンテキストメニューを表示し、[新規作成]メニューを選択します。フィルタ監視項目のプロパティが表示されますので、指定フィールドを検知するキーワードで監視設定し、通知したいメッセージIDを登録します。

＜テキストログ監視の設定＞
アラートファイルのテキストログ監視を行うには、千手ブラウザのツリービューで、＜ドメイン＞→“ノードグループ”→＜ノードグループ＞を選択し、そのリストビューからAzure Service Health情報取得のプローブとして設定したノードを選択し、マウスの右ボタンをクリックしコンテキストメニューを表示し、[プロパティ]メニューを選択します。ノードのプロパティウィンドウが表示されますので、[ログ監視]タブを選択します。ノードのプロパティ（[ログ監視]タブ）にて、監視対象のパス名とファイル名にAzure Service Health情報ログファイルを指定し、監視方法に先に作成したログフィルタを指定します。監視対象ログの「文字コードを指定する」を UTF-8 に指定し、ログ監視を登録した後に、登録したノードに対して[反映(監視属性)]を実行することにより、ログファイルの監視を開始します。

2.4.2.4. 汎用メトリクス監視機能

監視項目「Azure:メトリクス監視」では Azure Resource Manager API で任意のメトリクスの値を取得し、監視することでアラートの検知をすることが可能です。

注釈

Senju DevOperation Conductor Extension Packリリース時点でMicrosoft Azureドキュメントに記載されているメトリクスが「リソースタイプ:メトリクス」から選択可能です。

2.4.2.4.1. 汎用メトリクス監視の設定方法

以下に汎用メトリクス監視の監視定義を千手ブラウザより登録する手順を記載します。例として仮想マシンインスタンスで受信されたバイト数を10分間隔で監視します。

＜汎用メトリクス監視タスクの登録＞
千手ブラウザのツリービューで＜ドメイン＞→“モニタリング”→“千手カテゴリ”→“クラウドサービス”を選択します。クラウドサービスのエンティティでリストビューの何も表示されていない部分でマウスの右ボタンを押してコンテキストメニューを表示し、[新規作成]→[メトリクス監視タスク]メニューを選択します。汎用メトリクス監視タスクのプロパティが表示されますので、監視項目名で「Azure:メトリクス監視」を選択し、各項目を設定します。
「監視タスク名」を”Azure:メトリクス監視（Microsoft.Compute/virtualMachines:Network In）”のように適当な名前に変更します。「計算式の変数の値」フィールドの「リソースタイプ:メトリクス」の選択ボタンを押し、候補一覧から”Microsoft.Compute/virtualMachines:Network In”を選択し

[OK]ボタンを押下します。「計算式」から"A1"を選択、「計算結果の型」から"小数"を選択、「計算結果の比較方法」から"通常"を選択、「計算式の変数Aの値」から"total"を選択、「単位」に"byte"を入力、「判定条件」に異常、警告と判定するしきい値を設定します。「検査間隔」を10分に設定します。「パラメータ」フィールドの「リソースグループ名」、「リソース名」を設定します。[OK]ボタンを押し、監視タスクを登録します。

監視項目「Azure：メトリクス監視」の設定項目を以下に示します。

表 2.24 Azure：メトリクス監視の設定項目

項目名	設定内容
リソースタイプ:メトリクス	Azure Resource Manager API で監視するメトリクスを【リソースタイプ:メトリック】の形式で指定して下さい。候補一覧から選択
計算式	計算に使用する式です。「計算式の変数Aの値」で指定したプロパティの値を計算し監視結果の値として扱います。「A0」や「A1
計算式の変数Aの値	Azure Resource Manager API で監視するメトリクスの統計を候補一覧から選択して下さい。以下の種類があります。 • average • maximum • minimum • total
計算結果の型	計算結果の型です。計算結果を判定条件の値と比較する際の型となります。候補一覧から選択して下さい。以下の種類があり • 整数 • 小数 • 指数 • 文字列
単位	ノードモニタに表示される単位です。
計算結果の比較方法	「判定条件」フィールド(値)の値と、比較する方法を表します。候補一覧から選択して下さい。以下の種類があります。 • 通常 • 絶対値 • 前回との差分(新たな監視対象を正常とする) • 常に正常 • 前回との差分(新たな監視対象を異常とする) • 通常(無くなった監視対象を異常とする) • 初回との差分(新たな監視対象を正常とする) • 初回との差分(新たな監視対象を異常とする) • 合計

2.4.2.5. Azure Data Explorer連携機能

監視項目「Azure：DataExplorer ログ情報取得」では Azure Data Explorer から取得したログをログファイルに蓄積します。このログファイルを監視することでアラートの検知をすることが可能です。

2.4.2.5.1. ログファイル

監視項目「Azure：DataExplorer ログ情報取得」で取得したログファイルは、パラメータ「ログ出力ファイル」で指定したファイル(絶対パス)に出力されます。複数の監視タスクを設定する場合は、出力先のログファイルが重複しないように設定する必要があります。パラメータでログファイルを指定しない場合は、ログフォーマットがLTSVあるいはJSONによってファイル名が変わります。ただし、ファイル名に使用できない記号は「-」(半角ハイフン)に置き換えます。

ログフォーマットがLTSVの場合：

<千手ホームディレクトリ>\log\cloud.azure.d\AzureDataExplorer_<dbName>_<tableName>_<TaskID>.log

ログフォーマットがJSONの場合：

<千手ホームディレクトリ>\log\cloud.azure.d\AzureDataExplorer_<dbName>_<tableName>_<TaskID>.json

出力されるログファイルの文字コードは UTF-8 になります。テキストログ監視の設定で監視対象ログの「文字コードを指定する」を UTF-8 に指定して下さい。

2.4.2.5.2. ログフォーマット

以下にAzure Data Explorer ログ情報取得で取得したログファイルのレコード形式について説明します。レコードは文字列のリスト形式で、項目間はカンマ区切りとなります。

【Azure Data Explorerログファイル　レコード形式】

- ログフォーマットがLTSVの場合：

[タイムスタンプ,ログ内容]

表 2.25 Azureログファイルレコード形式

No.	項目	説明
1	タイムスタンプ	取得したログが出力されたタイムスタンプ(UTC)が入ります。フォーマット：YYYY-MM-DDThh:mm:ddZ（例：2022-09-13T07:
2	ログ内容	クエリにより取得されたログ内容が入ります。各項目は値のみの形式で出力され、各項目間はカンマで区切られています。 ログはタイムスタンプのソート順で出力されます。

- ログフォーマットがJSONの場合：

ログ内容

表 2.26 Azureログファイルレコード形式

No.	項目	説明
1	ログ内容	取得したログ内容が入ります。ログ内容はJSONの形式で出力されます。

2.4.2.5.3. テキストログ監視の設定方法

以下にSenju DevOperation Conductorのテキストログ監視を利用して、Azure Data Explorer ログ情報取得で取得したログ内容を監視する運用例を示します。この例では、ログ内容にキーワードが発生時にメッセージモニタに通知されるようにログフィルタを登録し、監視する場合について説明します。

＜ログフィルタの登録＞
千手ブラウザのツリービューで＜ドメイン＞→“フィルタ”→“ログフィルタ”を選択します。ログフィルタのエンティティでリストビューの何も表示されていない部分でマウスの右ボタンを押してコンテキストメニューを表示し、[新規作成]メニューを選択します。ログフィルタのプロパティが表示されます。ログフィルタ名などの各項目を入力し[OK]ボタンを押下します。これにより、ログフィルタの登録が完了します。

＜フィルタ監視項目の追加＞
千手ブラウザのツリービューの＜ドメイン＞→“フィルタ”→“ログフィルタ”→＜ログフィルタ＞でフィルタ監視項目を登録するログフィルタを選択し、リストビューの何も表示されていない部分でマウスの右ボタンを押してコンテキストメニューを表示し、[新規作成]メニューを選択します。フィルタ監視項目のプロパティが表示されますので、指定フィールドを検知するキーワードで監視設定し、通知したいメッセージIDを登録します。

＜テキストログ監視の設定＞
アラートファイルのテキストログ監視を行うには、千手ブラウザのツリービューで、＜ドメイン＞→“ノードグループ”→＜ノードグループ＞を選択し、そのリストビューからAzure Data Explorer ログ情報取得のプローブとして設定したノードを選択し、マウスの右ボタンをクリックしコンテキストメニューを表示し、[プロパティ]メニューを選択します。ノードのプロパティウィンドウが表示されますので、[ログ監視]タブを選択します。ノードのプロパティ（[ログ監視]タブ）にて、監視対象のパス名とファイル名にAzure Data Explorer ログファイルを指定し、監視方法に先に作成したログフィルタを指定します。ログ監視を登録した後に、登録したノードに対して[反映(監視属性)]を実行することにより、ログファイルの監視を開始します。

以上で、テキストログ監視の設定方法は完了です。この設定によりAzure Data Explorer ログファイルにキーワードが出力された場合、メッセージモニタに通知されます。

警告

管理対象ノードにおいて千手が起動していない状態で、[反映(監視属性)]を行うと失敗しますので、注意して下さい。

2.5. クラウド監視(Google Cloud)監視設定手順と使い方

Google Cloud監視設定を行う際には、以下の設定が必要になります。

- ライセンスの購入とライセンスキーの入手
    - Google Cloud監視

注釈

監視対象数に応じて、カスタムセンサーのライセンスが必要です。

- Senju DevOperation Conductor Extension Packの入手と適用

    運用管理サーバーおよび、クラウド監視を行う管理対象ノードに、同一バージョンの Senju DevOperation Conductor Extension Pack の適用が必要です
    - 運用管理サーバー(千手マネージャ)への適用(監視項目の更新)
    - 管理対象ノード(千手エージェント(プローブノード))への適用(情報取得コマンドの更新)

警告

適用可能な Senju DevOperation Conductor のバージョンやパッチ状況に制限がある場合があります。詳しくは、Senju DevOperation Conductor Extension Pack の README をご参照下さい。

参考

Senju DevOperation Conductor Extension Packの適用手順につきましては、Senju DevOperation Conductor Extension Pack の README をご参照下さい。

注釈

Senju DevOperation Conductor Extension Packの適用に際しては、千手システムの停止は不要ですが、関連する監視タスクの停止が必要です。

2.5.1. 設定

- **説明**

    モニタリングサブシステムを用いてGoogle Cloudの監視項目を使用するための設定を行います。

- **設定手順**

    Google Cloud監視を設定するには以下の手順が必要です。
    - Google Cloudアカウントの登録
    - Google Cloud情報設定ファイルの作成

2.5.1.1. Google Cloudアカウントの登録

Google Cloudの監視項目の利用において、事前にGoogle Cloud サービスアカウントの登録が必要です。Google Cloudサイトよりアカウント登録を行って下さい。

2.5.1.1.1. ロールの作成

Google Cloud監視では、監視項目毎に必要とされるアクセス権限が異なります。**「Google Cloud監視に必要なアクセス権限」**に示すアクセス権限を付与したロールを作成して下さい。

表 2.27 Google Cloud監視に必要なアクセス権限

監視項目	必要なアクセス権
GCP: App Engine ~ GCP: BigQuery ~ GCP: Cloud Functions ~ GCP: Cloud SQL ~ GCP: Stackdriver Trace ~ GCP: Compute Engine ~ GCP: Kubernetes Engine ~ GCP: Cloud Datastore ~ GCP: Clould DNS ~ GCP: Cloud Load Balancing ~ GCP: Stackdriver Logging ~ GCP: Stackdriver Monitoring ~ GCP: Pub/Sub ~ GCP: Cloud Spanner ~ GCP: Cloud Storage ~	monitoring.groups.list monitoring.metricDescriptors.get monitoring.metricDescriptors.list monitoring.timeSeries.list resourcemanager.projects.get
GCP: Cloud Logging	logging.logEntries.list logging.privateLogEntries.list
GCP: 利用料金 ~	bigquery.jobs.create bigquery.tables.getData

2.5.1.1.2. サービスアカウントの作成

Google Cloud監視を行うためにはサービスアカウントによる認証が必要となります。Google Cloudサイトよりサービスアカウントの作成を行って下さい。サービスアカウントの作成時に、ロールの作成 で作成したロールを割り当てて下さい。

2.5.1.2. 認証設定

2.5.1.2.1. Compute Engineにサービスアカウントを設定し認証する

Google Cloud内のエージェントからGoogle Cloud監視を行う場合は、エージェントとなるCompute Engineにサービスアカウントを割り当てて認証します。Google Cloudサイトよりサービスアカウントを関連付けて下さい。また、Google Cloud情報設定ファイル(sj_gcp_sys.json)の作成 でGoogle Cloud情報設定ファイルにプロジェクトIDを設定して下さい。

2.5.1.2.2. APIキーで認証する

Google Cloud外のエージェントからGoogle Cloud監視を行う場合は、エージェントからサービスアカウントで作成したAPIキーの認証ファイルを利用して認証します。Google Cloudサイトよりサービスアカウントから APIキーを作成し、APIキー認証ファイルをダウンロードして下さい。ダウンロードしたAPIキー認証ファイルをエージェントの千手稼働アカウントでアクセスできる位置に配置し、Google Cloud情報設定ファイル(sj_gcp_sys.json)の作成 でGoogle Cloud情報設定ファイルにAPIキー認証ファイルのパスを設定して下さい。

2.5.1.3. Google Cloud情報設定ファイル(sj_gcp_sys.json)の作成

sj_gcp_sys.jsonファイルは、Google Cloudに関する情報の設定ファイルです。sj_gcp_sys.jsonとGoogle Cloudの監視タスクのパラメータの両方で認証ファイルを指定した場合は、Google Cloudの監視タスクのパラメータで指定した値が有効になります。

Google Cloud情報設定ファイル(dat/opt/sj_gcp_sys.json)を作成し、以下の項目を設定して下さい。

表 2.28 sj_gcp_sys.jsonの記述内容

項目	省略	デフォルト	暗号化対象	説明
proxyURL	可	—	×	Google Cloud接続時に経由するプロキシサーバー。(次の形式で記載して下さい "<プロトコル
proxyUsername	可	—	×	プロキシサーバーアクセス用ユーザーID
proxyPassword	可	—	○	プロキシサーバーアクセス用パスワード(暗号化後のパスワード)
maxLogSize	可	—	×	省略する場合は「GCP：Stackdriver ログ情報取得」で出力するログファイルの最大サイズが1(
maxLogCnt	可	—	×	省略する場合は「GCP：Stackdriver ログ情報取得」で出力するログファイルのローテーション最大
retryCount	可	3	×	API実行失敗時のリトライ回数
waitTime	可	30	×	API実行時のタイムアウト時間
logWaitTime	可	600	×	「GCP：Stackdriver ログ情報取得」で利用するAPI実行時のタイムアウト時間
project_id	可	—	×	Compute Engineにサービスアカウントを割り当てた場合の認証用プロジェクトID
accountFilePath	可	—	×	サービスアカウントのAPIキー認証ファイルの絶対パス
logFormat	可	—	×	取得したログの出力フォーマットをLTSVもしくはJSONに切り替えます。省略する場合はLTSV&
logBufferTime	可	—	×	省略する場合は前回取得した最後のログより遡る時間が5(単位:分)になります。

- project_idはCompute Engineにサービスアカウントを割り当てた場合に指定して下さい。
- accountFilePathは、APIキーによる認証を行う場合に指定して下さい。
- proxyUsernameおよびproxyPasswordの両方を指定しなかった場合、プロキシサーバーの認証に利用しません。
- 一回以上ログを取得している状態でlogBufferTimeを現在よりも大きい値に変更した場合、変更後の1回目の実行で過去に取得したログを重複して取得する場合があります。ご注意ください。

- sj_gcp_sys.json の記載例

```
{
        "proxyURL": "http://10.1.0.9:8080",
        "proxyUsername": "gcpuser",
        "proxyPassword": "=AYvZ4/99j4vF+A==",
        "maxLogSize": "",
        "maxLogCnt": "",
        "retryCount": "3",
        "waitTime": "30",
        "logWaitTime": "600",
        "project_id": "xxxxx-project",
        "accountFilePath": "",
        "logFormat": "",
        "logBufferTime": ""
}
```

2.5.1.3.1. sj_setup_gcp ー Google Cloud情報設定ファイル更新 ー

- 指定形式
    - [参照]

      ```
      sj_setup_gcp
      ```

    - [作成＆更新]

      ```
      sj_setup_gcp
        [-purl[Proxy server via when connecting to Google Cloud]]
        [-puser[User ID for proxy server access]]
        [-ppswd[Password for proxy server access]]
        [-mls[If omitted, the maximum size of the log file output by log monitoring is
        10240 (unit: KB)]]
        [-mlc[If omitted, the maximum number of log file rotations output by log
        monitoring is 7.]]
        [-rc[number of retries when API call fails]]
        [-wt[wait time(seconds) when no response is returned]]
        [-lwt[Timeout when executing API used in log monitoring]]
        [-pid[Project ID for authentication when a service account is assigned to
        Compute Engine]]
        [-afp[Absolute path of API key authentication file for service account]]
        [-lf[format of log file output by log monitoring]]
        [-lbt[bufferTime of log file output by log monitoring]]
      ```

- 目的

  Google Cloud情報設定ファイル(/dat/opt/sj_gcp_sys.json) の現在値の参照、作成と更新を行います。

- オプション

  - -purl

    GCP接続時に経由するプロキシサーバー（proxyURL）に設定する値を指定して下さい。
    値を省略するとGoogle Cloud情報設定ファイルに設定されている値を削除します。

  - -puser

    プロキシサーバーのユーザ（proxyUsername）に設定する値を指定して下さい。
    値を省略するとGoogle Cloud情報設定ファイルに設定されている値を削除します。

  - -ppswd

    プロキシサーバーのパスワード（proxyPassword）に設定する値を指定して下さい。
    設定値の指定は対話形式で行われます。
    この項目は暗号化した値がGoogle Cloud情報設定ファイルに書き込まれます。

  - -mls

    出力するログファイルの、最大サイズ（maxLogSize）に設定する値を指定して下さい。
    値を省略するとGoogle Cloud情報設定ファイルに設定されている値を削除します。

  - -mlc

    出力するログファイルの、ローテーション最大個数（maxLogCnt）に設定する値を指定して下さい。
    値を省略するとGoogle Cloud情報設定ファイルに設定されている値を削除します。

  - -rc

    API実行失敗時のリトライ回数(retryCount)に設定する値を指定して下さい。
    値を省略するとGoogle Cloud情報設定ファイルに設定されている値を削除します。

  - -wt

    API実行時のタイムアウト時間(waitTime)に設定する値を指定して下さい。
    値を省略するとGoogle Cloud情報設定ファイルに設定されている値を削除します。

  - -lwt

    ログを取得する時、API実行時のタイムアウト時間(logWaitTime)に設定する値を指定して下さい。
    値を省略するとGoogle Cloud情報設定ファイルに設定されている値を削除します。

  - -pid

    サービスアカウントがCompute Engineに割り当てられている場合の認証用のプロジェクトID（project_id）に設定する値を指定して下さい。
    値を省略するとGoogle Cloud情報設定ファイルに設定されている値を削除します。

  - -afp

    サービスアカウントのAPIキー認証ファイルの絶対パス（accountFilePath）に設定する値を指定して下さい。
    値を省略するとGoogle Cloud情報設定ファイルに設定されている値を削除します。

  - -lf

    出力するログフォーマット（logFormat）に設定する値を指定して下さい。
    値を省略するとGoogle Cloud情報設定ファイルに設定されている値を削除します。

  - -lbt

    最後に取得したログより遡る時間(logBufferTime)を指定して下さい。
    値を省略するとGoogle Cloud情報設定ファイルに設定されている値を削除します。

- 実行結果

- (例1)現在の設定値参照

```
% sj_setup_gcp
{
        "proxyURL": "XXXXX",
        "proxyUsername": "",
        "proxyPassword": "**********",
        "maxLogSize": "",
        "maxLogCnt": ""
        "retryCount": "",
        "waitTime": "",
        "logWaitTime": "",
        "project_id": "ABCD",
        "accountFilePath": "",
        "logFormat": "",
        "logBufferTime": ""
}

%
```

- (例2)proxyURLとproject_id、proxyPasswordを設定

```
% sj_setup_gcp -purlXXXXX-XXXXX -pidXXXX-XXXX -ppswd
Please enter the value.
        "proxyPassword":

        The value of proxyURL has changed from (XXXXX) to (XXXXX-XXXXX).
        The value of project_id has changed from (ABCD) to (XXXX-XXXX).
        The value of proxyPassword has changed from (**********) to (**********).

The update is complete.

% sj_setup_gcp
{
        "proxyURL": "XXXXX-XXXXX",
        "proxyUsername": "",
        "proxyPassword": "**********",
        "maxLogSize": "",
        "maxLogCnt": ""
        "retryCount": "",
        "waitTime": "",
        "logWaitTime": "",
        "project_id": "XXXX-XXXX",
        "accountFilePath": "",
        "logFormat": "",
        "logBufferTime": ""
}

%
```

- (例3)設定を削除

```
% sj_setup_gcp -purl -pid -ppswd
Please enter the value.
        "proxyPassword":

        The value of proxyURL has changed from (XXXXX-XXXXX) to ().
        The value of project_id has changed from (XXXX-XXXX) to ().
        The value of proxyPassword has changed from (**********) to (**********).

The update is complete.

% sj_setup_gcp
{
        "proxyURL": "",
        "proxyUsername": "",
        "proxyPassword": "",
        "maxLogSize": "",
        "maxLogCnt": ""
        "retryCount": "",
        "waitTime": "",
        "logWaitTime": "",
        "project_id": "",
        "accountFilePath": "",
        "logFormat": "",
        "logBufferTime": ""
}

%
```

注釈

- 暗号化対象項目の標準出力への表示は全てアスタリスクでマスクされます。

- 暗号化対象項目の値の設定は、キーボードからの入力が一切表示されません。コピー＆ペーストで入力することをお勧めします。
- 暗号化対象項目の値を削除する場合、何も入力せずにリターンキーを押下して下さい。

- 標準エラー出力
  - Failed to acquire Senju home directory
  - The GCP System information file does not exist.
  - Invalid data have been set in this file.
  - Failed to update the GCP System information file.
  - File update failed.

- 終了ステータス
  - 0：正常終了
  - 1：異常終了

2.5.1.3.2. Google Cloud情報設定ファイル更新コマンドの登録

Google Cloud情報設定ファイルの現在値の参照、作成と更新を行うため、GCP情報設定ファイル更新コマンドを千手ブラウザからユーザーコマンドに登録します。詳細な手順については、ユーザーズガイド**「2.3.2.1 ユーザーコマンド」**を参照して下さい。

- ユーザーコマンドグループの作成

  Google Cloud情報設定ファイル更新コマンドを登録するユーザーコマンドグループを千手ブラウザから登録して下さい。

- Google Cloud情報設定ファイル更新コマンドの登録

  作成したユーザーコマンドグループに、以下に示す起動シーケンスを指定してコマンドを登録して下さい。

  - 現在値の参照

```
sj_remshe "@ノード名@" -l "@ユーザ名@" sj_setup_gcp
```

  - 作成と更新

```
sj_remshe "@ノード名@" -l "@ユーザ名@" sj_setup_gcp "-purl@@GCP接続時に経由するプロキシサーバー@@" "-puser@@プロキシサーバーのユーザ名@@" "-ppswd@@プロキシサーバーのパスワード@@" "-mls@@ログファイルの最大サイズ@@" "-mlc@@ログファイルのローテーション最大個数@@" "-rc@@API実行失敗時のリトライ回数@@" "-wt@@API実行時のタイムアウト時間@@" "-lwt@@ログ取得時のAPIタイムアウト時間@@" "-pid@@サービスアカウントがCompute Engineに割り当てられている場合の認証用プロジェクトID@@" "-afp@@サービスアカウントのAPIキー認証ファイルパス@@" "-lf@@ログフォーマット@@" "-lbt@@最後に取得したログより遡る時間@@"
```

注釈

上記の起動シーケンスは項目を全て変更する仕様となっています。項目別に変更を行いたい場合は、起動シーケンスから任意の「**-オプション@@パラメータ名@@**」を指定したユーザーコマンドを別途登録して下さい。

（例）sj_remshe "@ノード名@" -l "@ユーザ名@" sj_setup_gcp "-purl@@GCP接続時に経由するプロキシサーバー@@"

2.5.2. 使い方

Google CloudのCloud Monitoringに接続し、Senju DevOperation Conductorのモニタリング機能を使って、監視することができます。

監視定義を千手ブラウザより登録し、監視を実施します。監視結果は、各種モニタ画面（グローバルノードモニタ／ノードモニタ）にてその監視状況を表示できます。予め設定したしきい値により障害を検知した場合は、メッセージモニタにメッセージが通知されます。
（モニタリング機能については、ユーザーズガイド「 **4．モニタリング** 」を参照して下さい。）

注釈

監視項目によっては、監視間隔を15分未満に設定すると値が取得できないことがあります。その場合は監視間隔を15分以上に設定して下さい。

参考

各種パラメータの設定値が分からない場合は、Google Cloudより提供されているMetrics Explorerにて確認して下さい。
参考URL: https://console.cloud.google.com/monitoring (2020年4月現在)

2.5.2.1. Google Cloud監視の各パラメータの上限値および制限事項

Google Cloud監視で設定できるパラメータにはGoogle Cloudの上限値とは別に千手固有の上限値および制限事項があります。下記の表に上限値および制限事項を示します。

表 2.29 Google Cloud監視の各パラメータの上限値および制限事項

パラメータ名	上限値、制限事項
ユーザーラベルキー	半角英数字
ユーザーラベル値	半角英数字

参考URL：https://cloud.google.com/compute/docs/labeling-resources?hl=ja （2020年12月現在）

2.5.2.2. Cloud Logging連携機能

監視項目「GCP：Stackdriver ログ情報取得」ではCloud Loggingから取得したログをログファイルに蓄積します。このログファイルを監視することでアラートの検知をすることが可能です。

2.5.2.2.1. Cloud Logging連携機能の上限値および制限事項

Cloud Loggingの使用量上限により、監視対象が多い場合に監視エラーが発生する可能性があります。下記の表に関連項目を示します。

表 2.30 Cloud Logging連携機能の上限値

項目	上限値
1 つの entries.list API 呼び出しにおけるプロジェクトなどのリソース名数	100
entries.list API 呼び出し回数	1 プロジェクトあたり 1 回/秒

参考URL：https://cloud.google.com/logging/quotas （2020年4月現在）

注釈

BigQuery、Cloud Load Balancing 等、一部サービスのログ情報取得はサポート対象外となります。

2.5.2.2.2. ログファイル

監視項目「GCP：Stackdriver ログ情報取得」で取得したログファイルは、パラメータ「ログ出力ファイル」で指定したファイル(絶対パス)に出力されます。複数の監視タスクを設定する場合は、出力先のログファイルが重複しないように設定する必要があります。パラメータでログファイルを指定しない場合は、ログフォーマットがLTSVあるいはJSONによってファイル名が変わります。ただし、ファイル名に使用できない記号は「-」(半角ハイフン)に置き換えます。

ログフォーマットがLTSVの場合：

<千手ホームディレクトリ>/log/cloud.gcp.d/Logging_<プロジェクトID>_<リソースタイプ>_<リソースラベル>_<ログ名>_<ログレベル>.log

ログフォーマットがJSONの場合：

<千手ホームディレクトリ>/log/cloud.gcp.d/Logging_<プロジェクトID>_<リソースタイプ>_<リソースラベル>_<ログ名>_<ログレベル>.json

複数の監視タスクを設定する場合は、出力先のログファイルが重複しないように設定する必要があります。リソースタイプ、ログ名(省略可能)、ログレベル(省略可能)を指定して下さい。

出力されるログファイルの文字コードは UTF-8 になります。テキストログ監視の設定で監視対象ログの「文字コードを指定する」を UTF-8 に指定して下さい。

2.5.2.2.3. ログフォーマット

以下にCloud Logging ログ情報取得で取得したログファイルのレコード形式について説明します。レコードは LTSV形式で、項目間はタブ区切りとなります。

【Cloud Loggingログファイル　レコード形式】

- ログフォーマットがLTSVの場合：

タイムスタンプ　重大度　ログメッセージ

表 2.31 Google Cloudログファイルレコード形式

No.	項目	説明
1	タイムスタンプ	「Timestamp:」に続き、取得したログエントリが出力されたタイムスタンプ(UTC)が入ります。フォーマット: YYYY-MM-DDThh:
2	重大度	「Severity:」に続き、取得したログエントリの重大度が入ります。
3	ログメッセージ	「LogMessage:」に続き、取得したログエントリが入ります。ログエントリはJSONの形式で出力されます。

- ログフォーマットがJSONの場合:

ログメッセージ

表 2.32 Google Cloudログファイルレコード形式

No.	項目	説明
1	ログメッセージ	取得したログエントリが入ります。ログエントリはJSONの形式で出力されます。

2.5.2.2.4. テキストログ監視の設定方法

以下にSenju DevOperation Conductorのテキストログ監視を利用して、Cloud Logging ログ情報取得で取得したログメッセージを監視する運用例を示します。この例では、ログメッセージにキーワードが発生時にメッセージモニタに通知されるようにログフィルタを登録し、監視する場合について説明します。

＜ログフィルタの登録＞
千手ブラウザのツリービューで＜ドメイン＞→“フィルタ”→“ログフィルタ”を選択します。ログフィルタのエンティティでリストビューの何も表示されていない部分でマウスの右ボタンを押してコンテキストメニューを表示し、[新規作成]メニューを選択します。ログフィルタのプロパティが表示されます。ログフィルタ名などの各項目を入力し[OK]ボタンを押下します。これにより、ログフィルタの登録が完了します。

＜フィルタ監視項目の追加＞
千手ブラウザのツリービューの＜ドメイン＞→“フィルタ”→“ログフィルタ”→＜ログフィルタ＞でフィルタ監視項目を登録するログフィルタを選択し、リストビューの何も表示されていない部分でマウスの右ボタンを押してコンテキストメニューを表示し、[新規作成]メニューを選択します。フィルタ監視項目のプロパティが表示されますので、指定フィールドを検知するキーワードで監視設定し、通知したいメッセージIDを登録します。

＜テキストログ監視の設定＞
アラートファイルのテキストログ監視を行うには、千手ブラウザのツリービューで、＜ドメイン＞→“ノードグループ”→＜ノードグループ＞を選択し、そのリストビューからCloud Logging ログ情報取得のプローブとして設定したノードを選択し、マウスの右ボタンをクリックしコンテキストメニューを表示し、[プロパティ]メニューを選択します。ノードのプロパティウィンドウが表示されますので、[ログ監視]タブを選択します。ノードのプロパティ（[ログ監視]タブ）にて、監視対象のパス名とファイル名にCloud Logging ログファイルを指定し、監視方法に先に作成したログフィルタを指定します。監視対象ログの「文字コードを指定する」を UTF-8 に指定し、ログ監視を登録した後に、登録したノードに対して[反映(監視属性)]を実行することにより、ログファイルの監視を開始します。

以上で、テキストログ監視の設定方法は完了です。この設定によりCloud Logging ログファイルにキーワードが出力された場合、メッセージモニタに通知されます。

警告

管理対象ノードにおいて千手が起動していない状態で、[反映(監視属性)]を行うと失敗しますので、注意して下さい。

2.5.2.3. 汎用メトリクス監視機能

監視項目「GCP:メトリクス監視」では Cloud Monitoring から任意のメトリクスの値を取得し、監視することができます。

注釈

Senju DevOperation Conductor Extension Packリリース時点でGoogle Cloudドキュメントに記載されているメトリクスが「リソースタイプ:メトリクス」から選択可能です。

2.5.2.3.1. 汎用メトリクス監視の設定方法

以下に汎用メトリクス監視の監視定義を千手ブラウザより登録する手順を記載します。例として仮想マシンのインスタンスで受信されたバイト数を10分間隔で監視します。

＜汎用メトリクス監視タスクの登録＞

千手ブラウザのツリービューで＜ドメイン＞→“モニタリング”→“千手カテゴリ”→“クラウドサービス”を選択します。クラウドサービスのエンティティでリストビューの何も表示されていない部分でマウスの右ボタンを押してコンテキストメニューを表示し、[新規作成]→[メトリクス監視タスク]メニューを選択します。汎用メトリクス監視タスクのプロパティが表示されますので、監視項目名で「GCP：メトリクス監視」を選択し、各項目を設定します。

「監視タスク名」を”GCP：メトリクス監視（gce_instance:received_bytes_count）”のように適当な名前に変更します。「計算式の変数の値」フィールドの「リソースタイプ:メトリクス」の選択ボタンを押し、候補一覧から”gce_instance:compute.googleapis.com/instance/network/received_bytes_count”を選択し[OK]ボタンを押下します。「計算式」から”A1”を選択、「計算結果の型」から”小数”を選択、「計算結果の比較方法」から”通常”を選択、「計算式の変数Aの値」から”Sum”を選択、「単位」に”byte”を入力、「判定条件」に異常、警告と判定するしきい値を設定します。「検査間隔」を10分に設定します。「パラメータ」フィールドの「メトリクスラベル」に”instance_name=xxxxxxxx”のように監視対象の仮想マシンのinstance_nameを指定します。[OK]ボタンを押し、監視タスクを登録します。

監視項目「GCP：メトリクス監視」の設定項目を以下に示します。

表 2.33 GCP：メトリクス監視の設定項目

項目名	設定内容
リソースタイプ:メトリクス	Cloud Monitoring から監視するメトリクスを【リソースタイプ:メトリクスタイプ】の形式で指定して下さい。候補一覧から選択するこ
計算式	計算に使用する式です。「計算式の変数Aの値」で指定したプロパティの値を計算し監視結果の値として扱います。「A0」や「A1
計算式の変数Aの値	Cloud Monitoring から監視するメトリクスの統計を候補一覧から選択して下さい。以下の種類があります。 • 50thPercentile • 5thPercentile • 95thPercentile • 99thPercentile • Average • Count • CountTrue • FractionTrue • Maximum • Minimum • State • Sum
計算結果の型	計算結果の型です。計算結果を判定条件の値と比較する際の型となります。候補一覧から選択して下さい。以下の種類があ • 整数 • 小数 • 指数 • 文字列
単位	ノードモニタに表示される単位です。
計算結果の比較方法	「判定条件」フィールド(値)の値と、比較する方法を表します。候補一覧から選択して下さい。以下の種類があります。 • 通常 • 絶対値 • 前回との差分(新たな監視対象を正常とする) • 常に正常 • 前回との差分(新たな監視対象を異常とする) • 通常(無くなった監視対象を異常とする) • 初回との差分(新たな監視対象を正常とする) • 初回との差分(新たな監視対象を異常とする) • 合計

2.6. クラウド監視(OCI)監視設定手順と使い方

OCI監視設定を行う際には、以下の設定が必要になります。

- ライセンスの購入とライセンスキーの入手
    - OCI監視

注釈

監視対象数に応じて、カスタムセンサーのライセンスが必要です。

- Senju DevOperation Conductor Extension Packの入手と適用

    運用管理サーバーおよび、クラウド監視を行う管理対象ノードに、同一バージョンの Senju DevOperation Conductor Extension Pack の適用が必要です
    - 運用管理サーバー（千手マネージャ）への適用（監視項目の更新）
    - 管理対象ノード（千手エージェント(プローブノード)）への適用（情報取得コマンドの更新）

警告

適用可能な Senju DevOperation Conductor のバージョンやパッチ状況に制限がある場合があります。詳しくは、Senju DevOperation Conductor Extension Pack の README をご参照下さい。

参考

Senju DevOperation Conductor Extension Packの適用手順につきましては、Senju DevOperation Conductor Extension Pack の README をご参照下さい。

注釈

Senju DevOperation Conductor Extension Packの適用に際しては、千手システムの停止は不要ですが、関連する監視タスクの停止が必要です。

2.6.1. 設定

- **説明**

    モニタリングサブシステムを用いてOCIの監視項目を使用するための設定を行います。

- **設定手順**

    OCI監視を設定するには以下の手順が必要です。
    - Oracle Cloud Infrastructureユーザーの登録
    - 認証設定
    - OCI情報設定ファイルの作成

2.6.1.1. Oracle Cloud Infrastructureユーザーの登録

OCIの監視項目の利用において、事前にOracle Cloud Infrastructure ユーザーの登録が必要です。Oracle Cloud Infrastructureサイトよりユーザー登録を行って下さい。

2.6.1.1.1. ポリシーの作成

OCI監視を使用するため、**「OCI監視に必要なアクセス権限」**に示すポリシーを作成して、ユーザーグループにアクセス権限を付与します。

表 2.34 C

監視項目	必要なアクセス権
OCI: Compute ~ OCI: Block Volume ~ OCI: VNIC ~ OCI: Autonomous Database ~ OCI: Events ~ OCI: Load Balancing ~ OCI: FastConnect ~ OCI: VPN Connect ~ OCI: Notifications ~ OCI: Object Storage ~ OCI: Function ~ OCI: File Storage ~	Allow group <group-name> to read metrics in compartment <compartment-name> Allow group <group-name> to inspect compartments in tenancy Allow group <group-name> to read buckets in compartment <compartment-name> Allow group <group-name> to read objectstorage-namespace in compartment <compartment-name> Allow group <group-name> to read instances in compartment <compartment-name>
OCI: Audit ~	Allow group <group-name> to inspect compartments in tenancy Allow group <group-name> to read audit-events in compartment <compartment-name>
OCI: Budget ~	Allow group <group-name> to inspect compartments in tenancy Allow group <group-name> to read usage-budgets in tenancy
OCI: Announcements ~	Allow group <group-name> to read announcements in tenancy
OCI: LogAnalytics ~	Allow service loganalytics to read loganalytics-features-family in tenancy Allow group <group-name> to manage loganalytics-resources-family in tenancy Allow group <group-name> to {LOG_ANALYTICS_LIFECYCLE_READ, LOG_ANALYTICS_QUERY_V
OCI: Alarms ~	Allow group <group-name> to inspect alarms in tenancy Allow group <group-name> to inspect metrics in tenancy
OCI: Logging ~	Allow group <group-name> to read log-groups in tenancy Allow group <group-name> to read log-content in tenancy
OCI: Streaming ~	Allow group <group-name> to use stream-pull in compartment <compartment-name>
OCI: Data Guard ~	Allow group <group-name> to inspect databases in compartment <compartment-name>
OCI: Service Limits ~	Allow group <group-name> to inspect limits in tenancy
OCI: Analytics ~	Allow group <group-name> to inspect analytics-instances in compartment <compartment-name>
OCI: Resource List ~	Allow group <group-name> to read <service-name> in compartment <compartment-name>

2.6.1.2. 認証設定

2.6.1.2.1. インスタンス・プリンシパルで認証する

OCI内のエージェントからOCI監視を行う場合は、インスタンス・プリンシパルを認可する方法で認証します。Oracle Cloud Infrastructureサイトより動的グループを作成し、インスタンスを動的グループのメンバーとして追加します。その後、OCIサービスへのAPIコールを許可するポリシーを作成して下さい。

表 2.3

監視項目	必要なアクセス権
OCI: Compute ~ OCI: Block Volume ~ OCI: VNIC ~ OCI: Autonomous Database ~ OCI: Events ~ OCI: Load Balancing ~ OCI: FastConnect ~ OCI: VPN Connect ~ OCI: Notifications ~ OCI: Object Storage ~ OCI: Function ~ OCI: File Storage ~	Allow dynamic-group <group-name> to read metrics in compartment <compartment-name> Allow dynamic-group <group-name> to inspect compartments in tenancy Allow dynamic-group <group-name> to read buckets in compartment <compartment-name> Allow dynamic-group <group-name> to read objectstorage-namespace in compartment <compartmer Allow dynamic-group <group-name> to read instances in compartment <compartment-name>
OCI: Audit ~	Allow dynamic-group <group-name> to inspect compartments in tenancy Allow dynamic-group <group-name> to read audit-events in compartment <compartment-name>
OCI: Budget ~	Allow dynamic-group <group-name> to inspect compartments in tenancy Allow dynamic-group <group-name> to read usage-budgets in tenancy
OCI: Announcements ~	Allow dynamic-group <group-name> to read announcements in tenancy
OCI: LogAnalytics ~	Allow service loganalytics to read loganalytics-features-family in tenancy Allow dynamic-group <group-name> to manage loganalytics-resources-family in tenancy Allow dynamic-group <group-name> to {LOG_ANALYTICS_LIFECYCLE_READ, LOG_ANALYTICS_C
OCI: Alarms ~	Allow dynamic-group <group-name> to inspect alarms in tenancy Allow dynamic-group <group-name> to inspect metrics in tenancy
OCI: Logging ~	Allow dynamic-group <group-name> to read log-groups in tenancy Allow dynamic-group <group-name> to read log-content in tenancy
OCI: Streaming ~	Allow dynamic-group <group-name> to use stream-pull in compartment <compartment-name>
OCI: Data Guard ~	Allow dynamic-group <group-name> to inspect databases in compartment <compartment-name>
OCI: Service Limits ~	Allow dynamic-group <group-name> to inspect limits in tenancy
OCI: Analytics ~	Allow dynamic-group group <group-name> to inspect analytics-instances in compartment <compartm
OCI: Resource List ~	Allow dynamic-group <group-name> to read <service-name> in compartment <compartment-name>

2.6.1.2.2. APIキーで認証する

OCI外のエージェントからOCI監視を行う場合は、ユーザーで作成したユーザー設定ファイルを利用して認証します。Oracle Cloud Infrastructureサイトよりapiキー、フィンガープリント、テナンシのOCID、ユーザーのOCID、リージョンを取得し、ユーザー設定ファイルの作成 で作成して下さい。作成したユーザー設定ファイルをエージェントの千手稼働アカウントでアクセスできる位置に配置し、OCI情報設定ファイル(sj_oci_sys.json)の作成 でOCI情報設定ファイルにユーザー設定ファイルのパスを設定して下さい。

参照URL：https://docs.cloud.oracle.com/ja-jp/iaas/Content/API/Concepts/apisigningkey.htm

2.6.1.2.3. ユーザー設定ファイルの作成

ユーザー設定ファイルは、OCIに関する認証情報の設定ファイルです。dat/opt/sj_oci_user.json.sample をコピーして以下の項目を設定して下さい。

表 2.36 ユーザー設定ファイルの記述内容

項目	省略	説明
tenantOCID	可	テナンシのOCID、指定する場合はAPIキーによる認証を行い、省略する場合はインスタンス・プリンシパル認証を行い
userOCID	不可	ユーザーのOCID
region	不可	リージョン
fingerprint	不可	APIキーのフィンガープリント
privateKeyLocation	不可	秘密キー・ファイルの絶対パス
privateKeyPassphrase	可	秘密キーを生成する時、設定したパスフレーズ

2.6.1.3. OCI情報設定ファイル(sj_oci_sys.json)の作成

sj_oci_sys.jsonファイルは、OCIに関する情報の設定ファイルです。sj_oci_sys.jsonとOCIの監視タスクのパラメータの両方で認証ファイルを指定した場合は、OCIの監視タスクのパラメータで指定した値が有効になります。

OCI情報設定ファイル(dat/opt/sj_oci_sys.json)を作成し、以下の項目を設定して下さい。

表 2.37 sj_oci_sys.jsonの記述内容

項目	省略	デフォルト	暗号化対象	説明
proxyURL	可	—	×	OCI接続時に経由するプロキシサーバー。(次の形式で記載して下さい "<プロトコル>://<ipアド
proxyUsername	可	—	×	プロキシサーバーアクセス用ユーザーID
proxyPassword	可	—	○	プロキシサーバーアクセス用パスワード(暗号化後のパスワード)
maxLogSize	可	—	×	省略する場合は出力するログファイルの最大サイズが10240(単位:KB)になります。
maxLogCnt	可	—	×	省略する場合は出力するログファイルのローテーション最大個数が7になります。
retryCount	可	3	×	API実行失敗時のリトライ回数
waitTime	可	30	×	API実行時のタイムアウト時間(単位:秒)
userFilePath	可	—	×	ユーザー設定ファイルの絶対パス
logFormat	可	—	×	取得したログの出力フォーマットをLTSVもしくはJSONに切り替えます。省略する場合はLTSVと
logBufferTime	可	—	×	省略する場合は前回取得した最後のログより遡る時間が5(単位:分)になります。

- userFilePathはAPIキーによる認証を行う場合に指定必須です。指定しなかった場合はインスタンス・プリンシパル認証による監視を行います。OCI監視を行うエージェントが所属するリージョンが監視対象となります。ただし、userFilePathで指定したユーザー設定ファイルにtenantOCIDが指定されていない場合はインスタンス・プリンシパル認証となります。この場合、ユーザー設定ファイル内のregionの情報のみ使用され、OCI監視を行うエージェントが所属するリージョン以外を監視対象とすることが可能です。
- proxyUsernameおよびproxyPasswordの両方を指定しなかった場合、プロキシサーバーの認証に利用しません。
- 一回以上ログを取得している状態でlogBufferTimeを現在よりも大きい値に変更した場合、変更後の1回目の実行で過去に取得したログを重複して取得する場合があります。ご注意ください。

- sj_oci_sys.json の記載例

```
{
        "proxyURL": "http://10.1.0.9:8080",
        "proxyUsername": "ociuser",
        "proxyPassword": "=AYvZ4/99j4vF+A==",
        "maxLogSize": "",
        "maxLogCnt": "",
        "retryCount": "3",
        "waitTime": "30",
        "userFilePath": "",
        "logFormat": "",
        "logBufferTime": ""
}
```

2.6.1.3.1. sj_setup_oci ー OCI情報設定ファイル更新 ー

- 指定形式
  - [参照]

    ```
    sj_setup_oci
    ```

  - [作成＆更新]

    ```
    sj_setup_oci
       [-purl[Proxy server via when connecting to Oracle Cloud Infrastructure]]
       [-puser[User ID for proxy server access]]
       [-ppswd[Password for proxy server access]]
       [-mls[If omitted, the maximum size of the log file output by log monitoring is
       10240 (unit: KB)]]
       [-mlc[If omitted, the maximum number of log file rotations output by log
       monitoring is 7.]]
       [-rc[number of retries when API call fails]]
       [-wt[wait time(seconds) when no response is returned]]
       [-ufp[Absolute path to the user's API key authentication file]]
       [-lf[format of log file output by log monitoring]]
       [-lbt[bufferTime of log file output by log monitoring]]
    ```

- 目的

  OCI情報設定ファイル(/dat/opt/sj_oci_sys.json) の現在値の参照、作成と更新を行います。

- オプション

  - -purl

    OCI接続時に経由するプロキシサーバー（proxyURL）に設定する値を指定して下さい。
    値を省略するとOCI情報設定ファイルに設定されている値を削除します。

  - -puser

    プロキシサーバーのユーザ（proxyUsername）に設定する値を指定して下さい。
    値を省略するとOCI情報設定ファイルに設定されている値を削除します。

  - -ppswd

    プロキシサーバーのパスワード（proxyPassword）に設定する値を指定して下さい。
    設定値の指定は対話形式で行われます。
    この項目は暗号化した値がOCI情報設定ファイルに書き込まれます。

  - -mls

    出力されるログファイルの最大サイズ（maxLogSize）に設定する値を指定して下さい。
    値を省略するとOCI情報設定ファイルに設定されている値を削除します。

  - -mlc

    出力されるログファイルローテーションの最大個数（maxLogCnt）に設定する値を指定して下さい。
    値を省略するとOCI情報設定ファイルに設定されている値を削除します。

  - -rc

    API実行失敗時のリトライ回数(retryCount)に設定する値を指定して下さい。
    値を省略するとOCI情報設定ファイルに設定されている値を削除します。

  - -wt

    API実行時のタイムアウト時間(waitTime)に設定する値を指定して下さい。
    値を省略するとOCI情報設定ファイルに設定されている値を削除します。

  - -ufp

    ユーザーのAPIキー認証ファイルへの絶対パス（userFilePath）に設定する値を指定して下さい。
    値を省略するとOCI情報設定ファイルに設定されている値を削除します。

  - -lf

    出力されるログフォーマット（logFormat）に設定する値を指定して下さい。
    値を省略するとOCI情報設定ファイルに設定されている値を削除します。

  - -lbt

    最後に取得したログより遡る時間(logBufferTime)を指定して下さい。
    値を省略するとOCI情報設定ファイルに設定されている値を削除します。

- 実行結果

  - (例1)現在の設定値参照

```
% sj_setup_oci
{
        "proxyURL": "XXXXX",
        "proxyUsername": "ABCD",
        "proxyPassword": "**********",
        "maxLogSize": "",
        "maxLogCnt": ""
        "retryCount": "",
        "waitTime": "",
        "userFilePath": "",
        "logFormat": "",
        "logBufferTime": ""
}

%
```

- (例2)proxyURLとproxyUsername、proxyPasswordを設定

```
% sj_setup_oci -purlXXXXX-XXXXX -puserXXXX-XXXX -ppswd
Please enter the value.
        "proxyPassword":

        The value of proxyURL has changed from (XXXXX) to (XXXXX-XXXXX).
        The value of proxyUsername has changed from (ABCD) to (XXXX-XXXX).
        The value of proxyPassword has changed from (**********) to (**********).

The update is complete.

% sj_setup_oci
{
        "proxyURL": "XXXXX-XXXXX",
        "proxyUsername": "XXXX-XXXX",
        "proxyPassword": "**********",
        "maxLogSize": "",
        "maxLogCnt": ""
        "retryCount": "",
        "waitTime": "",
        "accountFilePath": "",
        "logFormat": "",
        "logBufferTime": ""
}

%
```

- (例3)設定を削除

```
% sj_setup_oci -purl -puser -ppswd
Please enter the value.
        "proxyPassword":

        The value of proxyURL has changed from (XXXXX-XXXXX) to ().
        The value of proxyUsername has changed from (XXXX-XXXX) to ().
        The value of proxyPassword has changed from (**********) to (**********).

The update is complete.

% sj_setup_oci
{
        "proxyURL": "",
        "proxyUsername": "",
        "proxyPassword": "",
        "maxLogSize": "",
        "maxLogCnt": ""
        "retryCount": "",
        "waitTime": "",
        "accountFilePath": "",
        "logFormat": "",
        "logBufferTime": ""
}

%
```

注釈

- 暗号化対象項目の標準出力への表示は全てアスタリスクでマスクされます。
- 暗号化対象項目の値の設定は、キーボードからの入力が一切表示されません。コピー＆ペーストで入力することをお勧めします。
- 暗号化対象項目の値を削除する場合、何も入力せずにリターンキーを押下して下さい。

- 標準エラー出力

- Failed to acquire Senju home directory
- The OCI System information file does not exist.
- Invalid data have been set in this file.
- Failed to update the OCI System information file.
- File update failed.

- 終了ステータス
  - 0：正常終了
  - 1：異常終了

2.6.1.3.2. OCI情報設定ファイル更新コマンドの登録

OCI情報設定ファイルの現在値の参照、作成と更新を行うため、OCI情報設定ファイル更新コマンドを千手ブラウザからユーザーコマンドに登録します。詳細な手順については、ユーザーズガイド**「2.3.2.1 ユーザーコマンド」**を参照して下さい。

- ユーザーコマンドグループの作成

  OCI情報設定ファイル更新コマンドを登録するユーザーコマンドグループを千手ブラウザから登録して下さい。

- OCI情報設定ファイル更新コマンドの登録

  作成したユーザーコマンドグループに、以下に示す起動シーケンスを指定してコマンドを登録して下さい。

  - 現在値の参照

```
sj_remshe "@ノード名@" -l "@ユーザ名@" sj_setup_oci
```

  - 作成と更新

```
sj_remshe "@ノード名@" -l "@ユーザ名@" sj_setup_oci "-purl@@OCI接続時に経由するプロキシサーバー@@" "-puser@@プロキシサーバーのユーザ名@@" "-ppswd@@プロキシサーバーのパスワード@@" "-mls@@ログファイルの最大サイズ@@" "-mlc@@ログファイルローテーションの最大個数@@" "-rc@@API実行失敗時のリトライ回数@@" "-wt@@API実行時のタイムアウト時間@@" "-ufp@@ユーザーのAPIキー認証ファイルパス@@" "-lf@@ログフォーマット@@" "-lbt@@最後に取得したログより遡る時間@@"
```

注釈

上記の起動シーケンスは項目を全て変更する仕様となっています。項目別に変更を行いたい場合は、起動シーケンスから任意の「**-オプション@@パラメータ名@@**」を指定したユーザーコマンドを別途登録して下さい。

（例）sj_remshe "@ノード名@" -l "@ユーザ名@" sj_setup_oci "-purl@@OCI接続時に経由するプロキシサーバー@@"

2.6.2. 使い方

OCIのCloud Monitoringに接続し、Senju DevOperation Conductorのモニタリング機能を使って、監視することができます。

監視定義を千手ブラウザより登録し、監視を実施します。監視結果は、各種モニタ画面（グローバルノードモニタ／ノードモニタ）にてその監視状況を表示できます。予め設定したしきい値により障害を検知した場合は、メッセージモニタにメッセージが通知されます。
（モニタリング機能については、ユーザーズガイド「 **4．モニタリング** 」を参照して下さい。）

注釈

監視項目によっては、監視間隔を15分未満に設定すると値が取得できないことがあります。その場合は監視間隔を15分以上に設定して下さい。

参考

各種パラメータの設定値が分からない場合は、Oracle Cloud Infrastructureより提供されているMetrics Explorerにて確認して下さい。
参考URL: https://console.us-ashburn-1.oraclecloud.com/monitoring/explore (2020年9月現在)

2.6.2.1. Oracle Cloud Infrastructure Audit連携機能

監視項目「OCI:Audit ログ情報取得」ではOracle Cloud Infrastructure Auditから取得したログをログファイルに蓄積します。このログファイルを監視することでアラートの検知をすることが可能です。

2.6.2.1.1. Oracle Cloud Infrastructure Audit連携機能の制限事項

Oracle Cloud Infrastructure Auditの監視対象が多い場合に、ログ取得の途中で強制停止される可能性があります。

2.6.2.1.2. ログファイル

監視項目「OCI:Audit ログ情報取得」で取得したログファイルは、パラメータ「ログファイル」で指定したファイル(絶対パス)に出力されます。複数の監視タスクを設定する場合は、出力先のログファイルが重複しないように設定する必要があります。パラメータでログファイルを指定しない場合は、ログフォーマットがLTSVあるいはJSONによってファイル名が変わります。ただし、ファイル名に使用できない記号は「-」(半角ハイフン)に置き換えます。

ログサイクルがサイズ(S)の場合:

- ログフォーマットがLTSVの場合:

<千手ホームディレクトリ>/log/cloud.oci.d/Audit_<コンパートメント名>.log

- ログフォーマットがJSONの場合:

<千手ホームディレクトリ>/log/cloud.oci.d/Audit_<コンパートメント名>.json

ログサイクルが日付(D)の場合:

- ログフォーマットがLTSVの場合:

<千手ホームディレクトリ>/log/cloud.oci.d/Audit_<コンパートメント名>_日付.log

- ログフォーマットがJSONの場合:

<千手ホームディレクトリ>/log/cloud.oci.d/Audit_<コンパートメント名>_日付.json

複数の監視タスクを設定する場合は、出力先のログファイルが重複しないように設定する必要があります。コンパートメント名を指定して下さい。

出力されるログファイルの文字コードは UTF-8 になります。テキストログ監視の設定で監視対象ログの「文字コードを指定する」を UTF-8 に指定して下さい。

2.6.2.1.3. ログフォーマット

以下にOracle Cloud Infrastructure Auditログ情報取得で取得したログファイルのレコード形式について説明します。レコードは LTSV形式で、項目間はタブ区切りとなります。

【Oracle Cloud Infrastructure Auditログファイル　レコード形式】

- ログフォーマットがLTSVの場合:

タイムスタンプ　重大度　ログメッセージ

表 2.38 OCIログファイルレコード形式

No.	項目	説明
1	タイムスタンプ	「Timestamp:」に続き、取得したログエントリが出力されたタイムスタンプ(UTC)が入ります。フォーマット:YYYY-MM-DDThh:（例:2020-08-13T07:09:06Z）。
2	ログメッセージ	「LogMessage:」に続き、取得したログエントリが入ります。ログエントリはJSONの形式で出力されます。

- ログフォーマットがJSONの場合:

ログメッセージ

表 2.39 OCIログファイルレコード形式

No.	項目	説明
1	ログメッセージ	取得したログエントリが入ります。ログエントリはJSONの形式で出力されます。

2.6.2.1.4. テキストログ監視の設定方法

以下にSenju DevOperation Conductorのテキストログ監視を利用して、Oracle Cloud Infrastructure Auditログ情報取得で取得したログメッセージを監視する運用例を示します。この例では、ログメッセージにキーワードが発生時にメッセージモニタに通知されるようにログフィルタを登録し、監視する場合について説明します。

＜ログフィルタの登録＞

千手ブラウザのツリービューで＜ドメイン＞→“フィルタ”→“ログフィルタ”を選択します。ログフィルタのエンティティでリストビューの何も表示されていない部分でマウスの右ボタンを押してコンテキストメニューを表示し、[新規作成]メニューを選択します。ログフィルタのプロパティが表示されます。ログフィルタ名などの各項目を入力し[OK]ボタンを押下します。これにより、ログフィルタの登録が完了します。

＜フィルタ監視項目の追加＞
千手ブラウザのツリービューの＜ドメイン＞→“フィルタ”→“ログフィルタ”→＜ログフィルタ＞でフィルタ監視項目を登録するログフィルタを選択し、リストビューの何も表示されていない部分でマウスの右ボタンを押してコンテキストメニューを表示し、[新規作成]メニューを選択します。フィルタ監視項目のプロパティが表示されますので、指定フィールドを検知するキーワードで監視設定し、通知したいメッセージIDを登録します。

＜テキストログ監視の設定＞
アラートファイルのテキストログ監視を行うには、千手ブラウザのツリービューで、＜ドメイン＞→“ノードグループ”→＜ノードグループ＞を選択し、そのリストビューからOracle Cloud Infrastructure Auditログ情報取得のプローブとして設定したノードを選択し、マウスの右ボタンをクリックしコンテキストメニューを表示し、[プロパティ]メニューを選択します。ノードのプロパティウィンドウが表示されますので、[ログ監視]タブを選択します。ノードのプロパティ（[ログ監視]タブ）にて、監視対象のパス名とファイル名にOracle Cloud Infrastructure Auditログファイルを指定し、監視方法に先に作成したログフィルタを指定します。監視対象ログの「文字コードを指定する」を UTF-8 に指定し、ログ監視を登録した後に、登録したノードに対して[反映(監視属性)]を実行することにより、ログファイルの監視を開始します。

以上で、テキストログ監視の設定方法は完了です。この設定によりOracle Cloud Infrastructure Auditログファイルにキーワードが出力された場合、メッセージモニタに通知されます。

警告

管理対象ノードにおいて千手が起動していない状態で、[反映(監視属性)]を行うと失敗しますので、注意して下さい。

2.6.2.2. Oracle Cloud Infrastructure LogAnalytics連携機能

監視項目「OCI：Log Analytics ログ情報取得」ではOracle Cloud Infrastructure LogAnalyticsから取得したログをログファイルに蓄積します。このログファイルを監視することでアラートの検知をすることが可能です。

2.6.2.2.1. ログファイル

監視項目「OCI：Log Analytics ログ情報取得」で取得したログファイル、パラメータ「ログファイル」で指定したファイル(絶対パス)に出力されます。複数の監視タスクを設定する場合は、出力先のログファイルが重複しないように設定する必要があります。パラメータでログファイルを指定しない場合は、ログフォーマットがLTSVあるいはJSONによってファイル名が変わります。ただし、ファイル名に使用できない記号は「-」(半角ハイフン)に置き換えます。

ログフォーマットがLTSVの場合：

<千手ホームディレクトリ>/log/cloud.oci.d/LogAnalytics_ネームスペース名_コンパートメント名_logGroup名_logSource名.log

ログフォーマットがJSONの場合：

<千手ホームディレクトリ>/log/cloud.oci.d/LogAnalytics_ネームスペース名_コンパートメント名_logGroup名_logSource名.json

複数の監視タスクを設定する場合は、出力先のログファイルが重複しないように設定する必要があります。ネームスペース名、コンパートメント名、logGroup名、logSource名を指定して下さい。

ログメッセージに含まれる改行、タブ、「\」記号は、”\t”⇒”\\t” “\n”⇒ “\\n”, “\”⇒ “\\”に置換されログファイルに出力されます。

出力されるログファイルの文字コードは UTF-8 になります。テキストログ監視の設定で監視対象ログの「文字コードを指定する」を UTF-8 に指定して下さい。

2.6.2.2.2. ログフォーマット

以下にOracle Cloud Infrastructure LogAnalyticsログ情報取得で取得したログファイルのレコード形式について説明します。レコードは LTSV形式で、項目間はタブ区切りとなります。

【Oracle Cloud Infrastructure LogAnalyticsログファイル　レコード形式】

- ログフォーマットがLTSVの場合：

タイムスタンプ　重大度　ログメッセージ

表 2.40 OCIログファイルレコード形式

No.	項目	説明
1	タイムスタンプ	「Timestamp:」に続き、取得したログエントリが出力されたタイムスタンプ(UTC)が入ります。フォーマット：YYYY-MM-DDThh（例：2021-04-14T07:09:06Z）。
2	LogGroup名	「LogGroup:」に続き、取得したLogGroup名が入ります。
3	LogSource名	「LogSource:」に続き、取得したLogSource名が入ります。
4	ログメッセージ	「LogMessage:」に続き、取得した[Original Log Content]が入ります。

- ログフォーマットがJSONの場合：

ログメッセージ

表 2.41 OCIログファイルレコード形式

No.	項目	説明
1	ログメッセージ	取得したログエントリが入ります。ログエントリはJSONの形式で出力されます。

2.6.2.2.3. テキストログ監視の設定方法

以下にSenju DevOperation Conductorのテキストログ監視を利用して、Oracle Cloud Infrastructure LogAnalyticsログ情報取得で取得したログメッセージを監視する運用例を示します。この例では、ログメッセージにキーワードが発生時にメッセージモニタに通知されるようにログフィルタを登録し、監視する場合について説明します。

＜ログフィルタの登録＞
千手ブラウザのツリービューで＜ドメイン＞→“フィルタ”→“ログフィルタ”を選択します。ログフィルタのエンティティでリストビューの何も表示されていない部分でマウスの右ボタンを押してコンテキストメニューを表示し、[新規作成]メニューを選択します。ログフィルタのプロパティが表示されます。ログフィルタ名などの各項目を入力し[OK]ボタンを押下します。これにより、ログフィルタの登録が完了します。

＜フィルタ監視項目の追加＞
千手ブラウザのツリービューの＜ドメイン＞→“フィルタ”→“ログフィルタ”→＜ログフィルタ＞でフィルタ監視項目を登録するログフィルタを選択し、リストビューの何も表示されていない部分でマウスの右ボタンを押してコンテキストメニューを表示し、[新規作成]メニューを選択します。フィルタ監視項目のプロパティが表示されますので、指定フィールドを検知するキーワードで監視設定し、通知したいメッセージIDを登録します。

＜テキストログ監視の設定＞
アラートファイルのテキストログ監視を行うには、千手ブラウザのツリービューで、＜ドメイン＞→“ノードグループ”→＜ノードグループ＞を選択し、そのリストビューからOracle Cloud Infrastructure LogAnalyticsログ情報取得のプローブとして設定したノードを選択し、マウスの右ボタンをクリックしコンテキストメニューを表示し、[プロパティ]メニューを選択します。ノードのプロパティウィンドウが表示されますので、[ログ監視]タブを選択します。ノードのプロパティ（[ログ監視]タブ）にて、監視対象のパス名とファイル名にOracle Cloud Infrastructure LogAnalyticsログファイルを指定し、監視方法に先に作成したログフィルタを指定します。監視対象ログの「文字コードを指定する」を UTF-8 に指定し、ログ監視を登録した後に、登録したノードに対して[反映(監視属性)]を実行することにより、ログファイルの監視を開始します。

以上で、テキストログ監視の設定方法は完了です。この設定によりOracle Cloud Infrastructure LogAnalyticsログファイルにキーワードが出力された場合、メッセージモニタに通知されます。

警告

管理対象ノードにおいて千手が起動していない状態で、[反映(監視属性)]を行うと失敗しますので、注意して下さい。

2.6.2.3. Oracle Cloud Infrastructure Announcements連携機能

監視項目「OCI：アナウンス情報取得」ではOracle Cloud Infrastructure Announcementsから取得したアナウンス情報をログファイルに蓄積します。このログファイルを監視することでアナウンス情報を検知することが可能です。

2.6.2.3.1. Oracle Cloud Infrastructure Announcements連携機能の制限事項

Oracle Cloud Infrastructure Announcementsの監視対象が多い場合に、ログ取得の途中で強制停止される可能性があります。

2.6.2.3.2. ログファイル

監視項目「OCI:アナウンス情報取得」で取得したログファイルは、パラメータ「ログファイル」で指定したファイル(絶対パス)に出力されます。複数の監視タスクを設定する場合は、出力先のログファイルが重複しないように設定する必要があります。パラメータでログファイルを指定しない場合は、ログフォーマットがLTSVあるいはJSONによってファイル名が変わります。ただし、ファイル名に使用できない記号は「-」(半角ハイフン)に置き換えます。

ログフォーマットがLTSVの場合:

<千手ホームディレクトリ>/log/cloud.oci.d/Announcements_<ルート・コンパートメント名>_<モード>.log

ログフォーマットがJSONの場合:

<千手ホームディレクトリ>/log/cloud.oci.d/Announcements_<ルート・コンパートメント名>_<モード>.json

ログファイル名に含まれる「モード」は監視タスクで指定したモードになります。

複数の監視タスクを設定する場合は、出力先のログファイルが重複しないように設定する必要があります。ルート・コンパートメント名を指定して下さい。

出力されるログファイルの文字コードは UTF-8 になります。テキストログ監視の設定で監視対象ログの「文字コードを指定する」を UTF-8 に指定して下さい。

2.6.2.3.3. ログフォーマット

以下にOracle Cloud Infrastructure アナウンス情報取得で取得したログファイルのレコード形式について説明します。レコードは LTSV形式で、項目間はタブ区切りとなります。

【Oracle Cloud Infrastructure アナウンス情報ログファイル　レコード形式】

- ログフォーマットがLTSVの場合:

タイムスタンプ　アナウンス内容

表 2.42 OCIログファイルレコード形式

No.	項目	説明
1	タイムスタンプ	「TimeCreated:」または「TimeUpdated:」に続き、取得したアナウンス情報の作成時間または更新時間のタイムスタンプ(U（例:2020-08-13T07:09:06Z)。
2	アナウンス内容	「Announcement:」に続き、取得したアナウンス内容が入ります。アナウンス内容はJSONの形式で出力されます。

- ログフォーマットがJSONの場合:

アナウンス内容

表 2.43 OCIログファイルレコード形式

No.	項目	説明
1	アナウンス内容	取得したアナウンス内容が入ります。アナウンス内容はJSONの形式で出力されます。

2.6.2.3.4. テキストログ監視の設定方法

以下にSenju DevOperation Conductorのテキストログ監視を利用して、Oracle Cloud Infrastructure アナウンス情報取得で取得したアナウンス情報を監視する運用例を示します。この例では、アナウンス内容にキーワードが発生した時にメッセージモニタに通知されるようにログフィルタを登録し、監視する場合について説明します。

＜ログフィルタの登録＞
千手ブラウザのツリービューで＜ドメイン＞→“フィルタ”→“ログフィルタ”を選択します。ログフィルタのエンティティでリストビューの何も表示されていない部分でマウスの右ボタンを押してコンテキストメニューを表示し、[新規作成]メニューを選択します。ログフィルタのプロパティが表示されます。ログフィルタ名などの各項目を入力し[OK]ボタンを押下します。これにより、ログフィルタの登録が完了します。

＜フィルタ監視項目の追加＞
千手ブラウザのツリービューの＜ドメイン＞→“フィルタ”→“ログフィルタ”→＜ログフィルタ＞でフィルタ監視項目を登録するログフィルタを選択し、リストビューの何も表示されていない部分でマウスの右ボタンを押してコンテキストメニューを表示し、[新規作成]メニューを選択します。フィルタ監視項目のプロパティが表示されますので、指定フィールドを検知するキーワードで監視設定し、通知したいメッセージIDを登録します。

＜テキストログ監視の設定＞
アラートファイルのテキストログ監視を行うには、千手ブラウザのツリービューで、＜ドメイン＞→“ノードグループ”→＜ノードグループ＞を選択し、そのリストビューからOracle Cloud Infrastructure アナウンス情報取得のプローブとして設定したノードを選択し、マウスの右ボタンをクリックしコンテキストメ

ニューを表示し、[プロパティ]メニューを選択します。ノードのプロパティウィンドウが表示されますので、[ログ監視]タブを選択します。ノードのプロパティ([ログ監視]タブ)にて、監視対象のパス名とファイル名にOracle Cloud Infrastructure アナウンス情報ログファイルを指定し、監視方法に先に作成したログフィルタを指定します。監視対象ログの「文字コードを指定する」を UTF-8 に指定し、ログ監視を登録した後に、登録したノードに対して[反映(監視属性)]を実行することにより、ログファイルの監視を開始します。

以上で、テキストログ監視の設定方法は完了です。この設定によりOracle Cloud Infrastructure アナウンス情報ログファイルにキーワードが出力された場合、メッセージモニタに通知されます。

警告

管理対象ノードにおいて千手が起動していない状態で、[反映(監視属性)]を行うと失敗しますので、注意して下さい。

2.6.2.4. Oracle Cloud Infrastructure Logging連携機能

監視項目「OCI:Logging ログ情報取得」ではOracle Cloud Infrastructure Loggingから取得したログをログファイルに蓄積します。このログファイルを監視することでアラートの検知をすることが可能です。

2.6.2.4.1. ログファイル

監視項目「OCI:Logging ログ情報取得」で取得したログファイルは、パラメータ「ログファイル」で指定したファイル(絶対パス)に出力されます。複数の監視タスクを設定する場合は、出力先のログファイルが重複しないように設定する必要があります。パラメータでログファイルを指定しない場合は、ログフォーマットがLTSVあるいはJSONによってファイル名が変わります。ただし、ファイル名に使用できない記号は「-」(半角ハイフン)に置き換えます。

ログフォーマットがLTSVの場合:

<千手ホームディレクトリ>/log/cloud.oci.d/Logging_コンパートメント名_ロググループ名_ログ名.log

ログフォーマットがJSONの場合:

<千手ホームディレクトリ>/log/cloud.oci.d/Logging_コンパートメント名_ロググループ名_ログ名.json

ロググループ名、ログ名が取れない場合、IDのままで使われます。

複数の監視タスクを設定する場合は、出力先のログファイルが重複しないように設定する必要があります。ロググループIDまたはロググループ名、ログIDまたはログ名を指定して下さい。

出力されるログファイルの文字コードは UTF-8 になります。テキストログ監視の設定で監視対象ログの「文字コードを指定する」を UTF-8 に指定して下さい。

2.6.2.4.2. ログフォーマット

以下にOracle Cloud Infrastructure Loggingログ情報取得で取得したログファイルのレコード形式について説明します。レコードは LTSV形式で、項目間はタブ区切りとなります。

【Oracle Cloud Infrastructure Loggingログファイル　レコード形式】

- ログフォーマットがLTSVの場合:

タイムスタンプ　ログメッセージ

表 2.44 OCIログファイルレコード形式

No.	項目	説明
1	タイムスタンプ	「Timestamp:」に続き、取得したログエントリが出力されたタイムスタンプ(UTC)が入ります。フォーマット:YYYY-MM-DDThh:(例:2021-04-14T07:09:06Z)。
2	ログメッセージ	「LogMessage:」に続き、取得した[LogContent]が入ります。

- ログフォーマットがJSONの場合:

ログメッセージ

表 2.45 OCIログファイルレコード形式

No.	項目	説明
1	ログメッセージ	取得した[LogContent]が入ります。[LogContent]はJSONの形式で出力されます。

2.6.2.4.3. テキストログ監視の設定方法

以下にSenju DevOperation Conductorのテキストログ監視を利用して、Oracle Cloud Infrastructure Loggingログ情報取得で取得したログメッセージを監視する運用例を示します。この例では、ログメッセージにキーワードが発生時にメッセージモニタに通知されるようにログフィルタを登録し、監視する場合について説明します。

＜ログフィルタの登録＞
千手ブラウザのツリービューで＜ドメイン＞→“フィルタ”→“ログフィルタ”を選択します。ログフィルタのエンティティでリストビューの何も表示されていない部分でマウスの右ボタンを押してコンテキストメニューを表示し、[新規作成]メニューを選択します。ログフィルタのプロパティが表示されます。ログフィルタ名などの各項目を入力し[OK]ボタンを押下します。これにより、ログフィルタの登録が完了します。

＜フィルタ監視項目の追加＞
千手ブラウザのツリービューの＜ドメイン＞→“フィルタ”→“ログフィルタ”→＜ログフィルタ＞でフィルタ監視項目を登録するログフィルタを選択し、リストビューの何も表示されていない部分でマウスの右ボタンを押してコンテキストメニューを表示し、[新規作成]メニューを選択します。フィルタ監視項目のプロパティが表示されますので、指定フィールドを検知するキーワードで監視設定し、通知したいメッセージIDを登録します。

＜テキストログ監視の設定＞
アラートファイルのテキストログ監視を行うには、千手ブラウザのツリービューで、＜ドメイン＞→“ノードグループ”→＜ノードグループ＞を選択し、そのリストビューからOracle Cloud Infrastructure Loggingログ情報取得のプローブとして設定したノードを選択し、マウスの右ボタンをクリックしコンテキストメニューを表示し、[プロパティ]メニューを選択します。ノードのプロパティウィンドウが表示されますので、[ログ監視]タブを選択します。ノードのプロパティ（[ログ監視]タブ）にて、監視対象のパス名とファイル名にOracle Cloud Infrastructure Loggingログファイルを指定し、監視方法に先に作成したログフィルタを指定します。監視対象ログの「文字コードを指定する」を UTF-8 に指定し、ログ監視を登録した後に、登録したノードに対して[反映(監視属性)]を実行することにより、ログファイルの監視を開始します。

以上で、テキストログ監視の設定方法は完了です。この設定によりOracle Cloud Infrastructure Loggingログファイルにキーワードが出力された場合、メッセージモニタに通知されます。

警告

管理対象ノードにおいて千手が起動していない状態で、[反映(監視属性)]を行うと失敗しますので、注意して下さい。

2.6.2.5. Oracle Cloud Infrastructure Streaming連携機能

監視項目「OCI：Streaming ログ情報取得」ではOracle Cloud Infrastructure Streamingから取得したログをログファイルに蓄積します。このログファイルを監視することでアラートの検知をすることが可能です。

2.6.2.5.1. ログファイル

監視項目「OCI：Streaming ログ情報取得」で取得したログファイルは、パラメータ「ログファイル」で指定したファイル(絶対パス)に出力されます。複数の監視タスクを設定する場合は、出力先のログファイルが重複しないように設定する必要があります。パラメータでログファイルを指定しない場合は、ログフォーマットがLTSVあるいはJSONによってファイル名が変わります。ただし、ファイル名に使用できない記号は「-」(半角ハイフン)に置き換えます。

ログフォーマットがLTSVの場合：

<千手ホームディレクトリ>/log/cloud.oci.d/Streaming_リージョン_ストリーム名.log

ログフォーマットがJSONの場合：

<千手ホームディレクトリ>/log/cloud.oci.d/Streaming_リージョン_ストリーム名.json

複数の監視タスクを設定する場合は、出力先のログファイルが重複しないように設定する必要があります。リージョン、ストリーム名を指定して下さい。

ログメッセージに含まれる改行、タブ、「\」記号は、”\t”⇒”\\t” “\n”⇒ “\\n”, “\”⇒ “\\”に置換されログファイルに出力されます。

出力されるログファイルの文字コードは UTF-8 になります。テキストログ監視の設定で監視対象ログの「文字コードを指定する」を UTF-8 に指定して下さい。

2.6.2.5.2. ログフォーマット

以下にOracle Cloud Infrastructure Streamingログ情報取得で取得したログファイルのレコード形式について説明します。レコードは LTSV形式で、項目間はタブ区切りとなります。

【Oracle Cloud Infrastructure Streamingログファイル　レコード形式】

- ログフォーマットがLTSVの場合：

タイムスタンプ　ログメッセージ

表 2.46 OCI Streamingログファイルレコード形式

No.	項目	説明
1	タイムスタンプ	「Timestamp:」に続き、取得したログエントリが出力されたタイムスタンプ(UTC)が入ります。フォーマット：YYYY-MM-DDThh:（例：2021-04-14T07:09:06Z）。
2	ストリーム	「Stream:」に続き、取得したストリームが入ります。
3	パーティション	「Partition:」に続き、取得したパーティションが入ります。
4	キー	「Key:」に続き、取得したキーが入ります。
5	ログメッセージ	「LogMessage:」に続き、取得したメッセージが入ります。

- ログフォーマットがJSONの場合：

ログメッセージ

表 2.47 OCI Streamingログファイルレコード形式

No.	項目	説明
1	ログメッセージ	取得したログエントリが入ります。ログエントリはJSONの形式で出力されます。

2.6.2.5.3. テキストログ監視の設定方法

以下にSenju DevOperation Conductorのテキストログ監視を利用して、Oracle Cloud Infrastructure Streamingログ情報取得で取得したログメッセージを監視する運用例を示します。この例では、ログメッセージにキーワードが発生時にメッセージモニタに通知されるようにログフィルタを登録し、監視する場合について説明します。

＜ログフィルタの登録＞
千手ブラウザのツリービューで＜ドメイン＞→“フィルタ”→“ログフィルタ”を選択します。ログフィルタのエンティティでリストビューの何も表示されていない部分でマウスの右ボタンを押してコンテキストメニューを表示し、[新規作成]メニューを選択します。ログフィルタのプロパティが表示されます。ログフィルタ名などの各項目を入力し[OK]ボタンを押下します。これにより、ログフィルタの登録が完了します。

＜フィルタ監視項目の追加＞
千手ブラウザのツリービューの＜ドメイン＞→“フィルタ”→“ログフィルタ”→＜ログフィルタ＞でフィルタ監視項目を登録するログフィルタを選択し、リストビューの何も表示されていない部分でマウスの右ボタンを押してコンテキストメニューを表示し、[新規作成]メニューを選択します。フィルタ監視項目のプロパティが表示されますので、指定フィールドを検知するキーワードで監視設定し、通知したいメッセージIDを登録します。

＜テキストログ監視の設定＞
アラートファイルのテキストログ監視を行うには、千手ブラウザのツリービューで、＜ドメイン＞→“ノードグループ”→＜ノードグループ＞を選択し、そのリストビューからOracle Cloud Infrastructure Streamingログ情報取得のプローブとして設定したノードを選択し、マウスの右ボタンをクリックしコンテキストメニューを表示し、[プロパティ]メニューを選択します。ノードのプロパティウィンドウが表示されますので、[ログ監視]タブを選択します。ノードのプロパティ（[ログ監視]タブ）にて、監視対象のパス名とファイル名にOracle Cloud Infrastructure Streamingログファイルを指定し、監視方法に先に作成したログフィルタを指定します。監視対象ログの「文字コードを指定する」を UTF-8 に指定し、ログ監視を登録した後に、登録したノードに対して[反映(監視属性)]を実行することにより、ログファイルの監視を開始します。

以上で、テキストログ監視の設定方法は完了です。この設定によりOracle Cloud Infrastructure Streamingログファイルにキーワードが出力された場合、メッセージモニタに通知されます。

警告

管理対象ノードにおいて千手が起動していない状態で、[反映(監視属性)]を行うと失敗しますので、注意して下さい。

2.6.2.6. Oracle Cloud Infrastructure リソース一覧取得

監視項目「OCI:リソース一覧取得」ではOracle Cloud Infrastructureから取得したリソース情報を一覧ファイルに蓄積します。

2.6.2.6.1. リソース一覧ファイル

監視項目「OCI:リソース一覧取得」で取得したリソース情報は、リソース一覧ファイルパスが指定される場合、指定するファイルに出力されます。リソース一覧ファイルパスが指定されない場合、次のデフォルトファイルに出力されます。ただし、ファイル名に使用できない記号は「-」(半角ハイフン)に置き換えます。

ログフォーマットがLTSVの場合:

<千手ホームディレクトリ>/log/cloud.oci.d/OCIResources_リージョン_taskID.log

ログフォーマットがJSONの場合:

<千手ホームディレクトリ>/log/cloud.oci.d/OCIResources_リージョン_taskID.json

出力されるログファイルの文字コードは UTF-8 になります。

2.6.2.6.2. リソース一覧ファイルフォーマット

以下にOracle Cloud Infrastructure リソース一覧取得で取得したリソース一覧ファイルのレコード形式について説明します。フィールドネームが指定された場合、指定されたフィールドで出力します。フィールドネームが指定されない場合、デフォルト「displayName,resourceType,resourceType」で出力します。レコードは LTSV形式で、項目間はタブ区切りとなります。

【Oracle Cloud Infrastructure リソース一覧ファイル　レコード形式】

- ファイルフォーマットがLTSVの場合:

ファイルメッセージ

表 2.48 リソース一覧ファイルレコード形式

No.	項目	説明
1	displayName	「displayName:」に続き、取得したdisplayNameが入ります。
2	resourceType	「resourceType:」に続き、取得したresourceTypeが入ります。
3	identifier	「identifier:」に続き、取得したidentifierが入ります。

- ファイルフォーマットがJSONの場合:

ファイルメッセージ

表 2.49 リソース一覧ファイルレコード形式

No.	項目	説明
1	リソース情報	取得した[ResourceSummary]が入ります。[ResourceSummary]はJSONの形式で出力されます。

2.6.2.7. 汎用メトリクス監視機能

監視項目「OCI:メトリクス監視」では Cloud Monitoring から任意のメトリクスの値を取得し、監視することができます。

注釈

Senju DevOperation Conductor Extension Packリリース時点でOracle Cloud Infrastructureドキュメントに記載されているメトリクスが「リソースタイプ:メトリクス」から選択可能です。

2.6.2.7.1. 汎用メトリクス監視の設定方法

以下に汎用メトリクス監視の監視定義を千手ブラウザより登録する手順を記載します。例として仮想マシンのインスタンスで受信されたバイト数を10分間隔で監視します。

＜汎用メトリクス監視タスクの登録＞
千手ブラウザのツリービューで＜ドメイン＞→"モニタリング"→"千手カテゴリ"→"クラウドサービス"を選択します。クラウドサービスのエンティティでリストビューの何も表示されていない部分でマウスの右ボタンを押してコンテキストメニューを表示し、[新規作成]→[メトリクス監視タスク]メニューを選択します。汎用メトリクス監視タスクのプロパティが表示されますので、監視項目名で「OCI:メトリクス監視」を選択し、各項目を設定します。
「監視タスク名」を"OCI:メトリクス監視(oci_computeagent:NetworksBytesIn)"のように適当な名前に変更します。「計算式の変数の値」フィールドの「リソースタイプ:メトリクス」の選択ボタンを押し、候補一覧から"oci_computeagent:NetworksBytesIn"を選択し[OK]ボタンを押下します。
「計算式」から"A1"を選択、「計算結果の型」から"小数"を選択、「計算結果の比較方法」から"通常"を選択、「計算式の変数Aの値」から"Sum"を選択、「単位」に"byte"を入力、「判定条件」に異常、警告と判定するしきい値を設定します。「検査間隔」を10分に設定します。「パラメータ」フィールドの「コンパートメント」を、「統計」に"sum"を、「ディメンション」に"resourceDisplayName=xxxxxxx"のように監視対象の仮想マシンのresourceDisplayNameを指定します。[OK]ボタンを押し、監視タスクを登録します。

監視項目「OCI:メトリクス監視」の設定項目を以下に示します。

表 2.50 OCI:メトリクス監視の設定項目

項目名	設定内容
リソースタイプ:メトリクス	Cloud Monitoring から監視するメトリクスを【メトリックネームスペース:メトリック】の形式で指定して下さい。候補一覧から選択す
計算式	計算に使用する式です。「計算式の変数Aの値」で指定したプロパティの値を計算し監視結果の値として扱います。「A0」や「A1
計算式の変数Aの値	Cloud Monitoring から監視するメトリクスの統計を候補一覧から選択して下さい。以下の種類があります。 • Count • Maximum • Mean • Minimum • Sum
計算結果の型	計算結果の型です。計算結果を判定条件の値と比較する際の型となります。候補一覧から選択して下さい。以下の種類があ • 整数 • 小数 • 指数 • 文字列
単位	ノードモニタに表示される単位です。
計算結果の比較方法	「判定条件」フィールド(値)の値と、比較する方法を表します。候補一覧から選択して下さい。以下の種類があります。 • 通常 • 絶対値 • 前回との差分(新たな監視対象を正常とする) • 常に正常 • 前回との差分(新たな監視対象を異常とする) • 通常(無くなった監視対象を異常とする) • 初回との差分(新たな監視対象を正常とする) • 初回との差分(新たな監視対象を異常とする) • 合計

注釈

「計算式の変数Aの値」で指定した統計に合わせて「統計」パラメータの値を指定して下さい。「統計」パラメータは全て小文字となります。

2.6.2.8. サービス制限監視機能

監視項目「OCI:サービス制限監視」では使用量とサービス制限を取得できるすべてのサービスにおいて、使用率(使用量/サービス制限*100)を取得し、監視することが可能です。

注釈

Senju DevOperation Conductor Extension Packリリース時点でOCIコンソールで「制限、割当ておよび使用状況」に表示されている使用量とサービス制限を取得できる制限が「リソースタイプ:メトリクス」から選択可能です。

2.6.2.8.1. サービス制限監視の設定方法

以下にサービス制限監視の監視定義を千手ブラウザより登録する手順を記載します。例としてサービスComputeのcustom-image-count制限を15分間隔で監視します。

＜サービス制限監視タスクの登録＞
千手ブラウザのツリービューで＜ドメイン＞→“モニタリング”→“千手カテゴリ”→“監視タスク”→“クラウドサービス”を選択します。クラウドサービスのエンティティでリストビューの何も表示されていない部分でマウスの右ボタンを押してコンテキストメニューを表示し、[新規作成]→[メトリクス監視タスク]メニューを選択します。
[監視項目名]の選択ボタンを押し、候補一覧から[OCI:サービス制限監視]を選択し[OK]ボタンを押下します。サービス制限監視タスクのプロパティが表示されますので、監視項目名で「OCI:サービス制限監視」を選択し、各項目を設定します。

「計算式の変数の値」フィールドの「リソースタイプ:メトリクス」の選択ボタンを押し、候補一覧から”serviceName=compute,limitName=custom-image-count”を選択し[OK]ボタンを押下します。
「計算式」から”A1”を選択、「計算結果の型」から”小数”を選択、「計算結果の比較方法」から”通常”を選択、「単位」に”%”を入力、「判定条件」に異常、警告と判定するしきい値を入力(一般は異常が90、警告が70を入力する)、「検査間隔」を15分に設定します。「パラメータ」フィールドの「コンパートメントID(ルート)」にルートのコンパートメントIDを指定します。[OK]ボタンを押し、監視タスクを登録します。

監視項目「OCI:サービス制限監視」の設定項目を以下に示します。

表 2.51 OCI:

項目名	設定内容
リソースタイプ:メトリクス	OCIコンソールで「制限、割当ておよび使用状況」に表示されている制限を【サービス名,制限名】の形式で指定して下さい。候補
計算式	計算に使用する式です。「A1」は使用率(使用量/サービス制限*100)の値を表します。
計算結果の型	計算結果の型です。計算結果を判定条件の値と比較する際の型となります。現状は【小数】と固定されています。
単位	ノードモニタに表示される単位です。
計算結果の比較方法	「判定条件」フィールド(値)の値と、比較する方法を表します。現状は【通常】と固定されています。

2.6.2.9. 「ORACLE:テーブルスペース ~」の監視項目の設定方法

以下の手順で「ORACLE:テーブルスペース ~」の監視が使用できます。本機能はExtensionPackのOCI連携機能のライセンスでなく、Oracle監視ライセンスが必要となります。

2.6.2.9.1. Linux環境で設定

- Oracle Instant Clientをダウンロード

  Autonomous Database 21cに接続するため、以下URLからOracle Instant ClientのVersion 21.10.0.0.0 をダウンロードします。
  https://www.oracle.com/database/technologies/instant-client/linux-x86-64-downloads.html
  ダウンロードした「instantclient-basic-linux.x64-21.10.0.0.0dbru.zip」と「instantclient-sqlplus-linux.x64-21.10.0.0.0dbru.zip」を$HOME/tmpout(他の一時保存できるフォルダでも可)に格納します。

- 環境変数設定

  下記コマンドを実行し、環境変数を設定します。

  ```
  % export ORACLE_BASE=$HOME/oracle
  % export ORACLE_HOME=$HOME/oracle/instantclient_21_10
  % export TNS_ADMIN=$ORACLE_HOME/network/admin
  % export LD_LIBRARY_PATH=$ORACLE_HOME
  % export PATH=$PATH:$ORACLE_HOME
  ```

- インストール

  下記のコマンドを実行して、/home/senjuに移動します。

  ```
  % cd /home/senju
  ```

  下記のコマンドを実行して、$ORACLE_BASEディレクトリを作成します。

  ```
  % mkdir ~/oracle
  ```

  下記のコマンドを実行して、Oracle Instant ClientとOracle Instant Client sqlplusを$HOME/oracle配下にインストールします。

  ```
  % cd ~/oracle
  % unzip /home/senju/tmpout/instantclient-basic-linux.x64-21.10.0.0.0dbru.zip
  % unzip /home/senju/tmpout/instantclient-sqlplus-linux.x64-21.10.0.0.0dbru.zip
  ```

- 資格証明ダウンロード

  Autonomous Databaseに接続するための資格証明のzipファイルを、作成したDatabaseの画面からダウンロードします。
  Autonomous Database画面で、OCIコンソールから、作成したAutonomous Database画面にある [データベース接続]をクリックします。
  クライアント資格証明(ウォレット)のダウンロード画面が表示されるので、[ウォレットのダウンロード]ボタンをクリックして、Client Credentialsをダウンロードします。
  ダウンロードしたzipファイルを$HOME/tmpout(他の一時保存できるフォルダでも可)に格納します。

- Wallet Client Credentials配置

  下記のコマンドを実行して、TNS_ADMINディレクトリを作成します。Wallet Client Credentialsを配置して、解凍します。

```
% mkdir -p $ORACLE_HOME/network/admin
% cd $TNS_ADMIN
% mv /home/senju/tmpout/Wallet_xxxxx.zip $TNS_ADMIN/
% unzip Wallet_xxxxx.zip
```

- sqlnet.ora 修正

  sqlnet.ora ファイルの DIRECTORY パスは、"?/network/admin" となっているため、書き換える必要があります。
  「?」をORACLE_HOMEのパスに書き換えます。

- tnsnames.ora 内容確認

  下記のコマンドを実行して、ネットサービス名を確認します。
  tnsnames.ora ファイルには、tpurgent、tp、high、mediumおよびlowといった5つのデータベース・サービス名が含まれています。

```
% cat tnsnames.ora
xxxxxxxxxxxxxxx_high = (description= (retry_count=20)(retry_delay=3)(address=
(protocol=tcps)(port=1522)(host=adb.ap-tokyo-1.oraclecloud.com))(connect_data=
(service_name=yyyyyyyyyyyyyy_xxxxxxxxxxxxxxx_high.adb.oraclecloud.com))(security=
(ssl_server_dn_match=yes)))
xxxxxxxxxxxxxxx_low = (description= (retry_count=20)(retry_delay=3)(address=
(protocol=tcps)(port=1522)(host=adb.ap-tokyo-1.oraclecloud.com))(connect_data=
(service_name=yyyyyyyyyyyyyy_xxxxxxxxxxxxxxx_low.adb.oraclecloud.com))(security=
(ssl_server_dn_match=yes)))
xxxxxxxxxxxxxxx_medium = (description= (retry_count=20)(retry_delay=3)(address=
(protocol=tcps)(port=1522)(host=adb.ap-tokyo-1.oraclecloud.com))(connect_data=
(service_name=yyyyyyyyyyyyyy_xxxxxxxxxxxxxxx_medium.adb.oraclecloud.com))(security=
(ssl_server_dn_match=yes)))
xxxxxxxxxxxxxxx_tp = (description= (retry_count=20)(retry_delay=3)(address=
(protocol=tcps)(port=1522)(host=adb.ap-tokyo-1.oraclecloud.com))(connect_data=
(service_name=yyyyyyyyyyyyyy_xxxxxxxxxxxxxxx_tp.adb.oraclecloud.com))(security=
(ssl_server_dn_match=yes)))
xxxxxxxxxxxxxxx_tpurgent = (description= (retry_count=20)(retry_delay=3)(address=
(protocol=tcps)(port=1522)(host=adb.ap-tokyo-1.oraclecloud.com))(connect_data=
(service_name=yyyyyyyyyyyyyy_xxxxxxxxxxxxxxx_tpurgent.adb.oraclecloud.com))(security=
(ssl_server_dn_match=yes)))
```

- 千手環境変数設定

  下記のコマンドを実行して、datに移動します。

```
% cd /home/senju/dat
```

  下記のコマンドを実行して、千手の環境変数に設定します。

```
% sj_source.com -cORACLE_BASE=$HOME/oracle
% sj_source.com -cORACLE_HOME=$HOME/oracle/instantclient_21_10
% sj_source.com -cTNS_ADMIN=$ORACLE_HOME/network/admin
% sj_source.com -cLD_LIBRARY_PATH=$LD_LIBRARY_PATH:$ORACLE_HOME
% sj_source.com -cPATH=$PATH:$ORACLE_HOME
```

  下記のコマンドを実行して、上記環境変数を正しく設定したのかを確認します。

```
% cat sjEnviron.override_cshrc
% cat sjEnviron.override_shrc
```

- 千手再起動

  環境変数の設定変更を反映するため、千手の再起動が必要となります。
  下記のコマンドを実行して、千手を再起動してください。

```
% sj_halt.com
% sj_boot.com
```

2.6.2.9.2. Windows環境で設定

- Oracle Instant Clientをダウンロード

  Autonomous Database 21cに接続するため、以下URLからOracle Instant ClientのVersion 21.10.0.0.0 をダウンロードします。
  https://www.oracle.com/database/technologies/instant-client/downloads.html
  ダウンロードした「instantclient-basic-windows.x64-21.12.0.0.0dbru.zip」と「instantclient-sqlplus-windows.x64-21.12.0.0.0dbru.zip」を適切なフォルダに保存します。

- インストール

  C:\senjuの下に「oracle」フォルダを新規作成してください。
  上記ダウンロードした「instantclient-basic-windows.x64-21.12.0.0.0dbru.zip」と「instantclient-sqlplus-windows.x64-21.12.0.0.0dbru.zip」を解凍します。
  解凍した「instantclient_21_12」を作成した「oracle」フォルダに格納します。

- 資格証明ダウンロード

  Autonomous Databaseに接続するための資格証明のzipファイルを、作成したDatabaseの画面からダウンロードします。
  Autonomous Database画面で、OCIコンソールから、作成したAutonomous Database画面にある [データベース接続]をクリックします。
  クライアント資格証明(ウォレット)のダウンロード画面が表示されるので、[ウォレットのダウンロード]ボタンをクリックして、Client Credentialsをダウンロードします。
  ダウンロードしたzipファイルを適切なフォルダに保存します。

- Wallet Client Credentials配置

  ダウンロードしたWallet Client Credentialsを下記フォルダに格納して、解凍してください。
  C:\senju\oracle\instantclient_21_12\network\admin

- sqlnet.ora 修正

  sqlnet.ora ファイルの DIRECTORY パスは、"?/network/admin" となっているため、書き換える必要があります。
  「?/network/admin」を「C:\senju\oracle\instantclient_21_12\network\admin」に書き換えます。

- tnsnames.ora 内容確認

  tnsnames.ora ファイルを参照して、ネットサービス名を確認します。
  tnsnames.ora ファイルには、tpurgent、tp、high、mediumおよびlowといった5つのデータベース・サービス名が含まれています。

  ```
  xxxxxxxxxxxxxxx_high = (description= (retry_count=20)(retry_delay=3)(address=
  (protocol=tcps)(port=1522)(host=adb.ap-tokyo-1.oraclecloud.com))(connect_data=
  (service_name=yyyyyyyyyyyyyy_xxxxxxxxxxxxxxx_high.adb.oraclecloud.com))(security=
  (ssl_server_dn_match=yes)))
  xxxxxxxxxxxxxxx_low = (description= (retry_count=20)(retry_delay=3)(address=
  (protocol=tcps)(port=1522)(host=adb.ap-tokyo-1.oraclecloud.com))(connect_data=
  (service_name=yyyyyyyyyyyyyy_xxxxxxxxxxxxxxx_low.adb.oraclecloud.com))(security=
  (ssl_server_dn_match=yes)))
  xxxxxxxxxxxxxxx_medium = (description= (retry_count=20)(retry_delay=3)(address=
  (protocol=tcps)(port=1522)(host=adb.ap-tokyo-1.oraclecloud.com))(connect_data=
  (service_name=yyyyyyyyyyyyyy_xxxxxxxxxxxxxxx_medium.adb.oraclecloud.com))(security=
  (ssl_server_dn_match=yes)))
  xxxxxxxxxxxxxxx_tp = (description= (retry_count=20)(retry_delay=3)(address=
  (protocol=tcps)(port=1522)(host=adb.ap-tokyo-1.oraclecloud.com))(connect_data=
  (service_name=yyyyyyyyyyyyyy_xxxxxxxxxxxxxxx_tp.adb.oraclecloud.com))(security=
  (ssl_server_dn_match=yes)))
  xxxxxxxxxxxxxxx_tpurgent = (description= (retry_count=20)(retry_delay=3)(address=
  (protocol=tcps)(port=1522)(host=adb.ap-tokyo-1.oraclecloud.com))(connect_data=
  (service_name=yyyyyyyyyyyyyy_xxxxxxxxxxxxxxx_tpurgent.adb.oraclecloud.com))(security=
  (ssl_server_dn_match=yes)))
  ```

- 千手環境変数設定

  「コントロールパネル＞システム＞システムの詳細設定」の「環境変数(N)」ボタンを押します。
  ユーザー環境変数の「PATH」を選択して、「編集」ボタンを押します。
  既存の設定値の最後尾に「C:\senju\oracle\instantclient_21_12」を追加して、「OK」ボタンを押します。

- 千手再起動

  環境変数の設定変更を反映するため、千手の再起動が必要となります。
  下記のコマンドをコマンドプロンプトで実行して、千手を再起動してください。

  ```
  > sj_halt
  > sj_boot
  ```

2.6.2.9.3. 千手ブラウザで監視項目「ORACLE：テーブルスペース～」の設定方法

「パラメータ」フィールドの各パラメータを下記の通りに指定します。

パラメータ名	説明
SID名	tnsnames.oraの中身のxxxxxxxxxxxxxxx_highを指定します。省略不可です。
テーブルスペース名	監視するAutonomousDBのテーブルスペース名を指定します。省略不可です。
ユーザー名	監視するAutonomousDBのユーザー名を指定します。省略不可です。
パスワード	監視するAutonomousDBのパスワードを指定します。省略不可です。
ネットサービス名	tnsnames.oraの中身のxxxxxxxxxxxxxxx_highを指定します。省略不可です。

2.7. クラウド監視(IBM Cloud)監視設定手順と使い方

IBM Cloud監視設定を行う際には、以下の設定が必要になります。

- ライセンスの購入とライセンスキーの入手
    - IBM Cloud監視

注釈

監視対象数に応じて、カスタムセンサーのライセンスが必要です。

- Senju DevOperation Conductor Extension Packの入手と適用

    運用管理サーバーおよび、クラウド監視を行う管理対象ノードに、同一バージョンの Senju DevOperation Conductor Extension Pack の適用が必要です
    - 運用管理サーバー(千手マネージャ)への適用(監視項目の更新)
    - 管理対象ノード(千手エージェント(プローブノード))への適用(情報取得コマンドの更新)

警告

適用可能な Senju DevOperation Conductor のバージョンやパッチ状況に制限がある場合があります。詳しくは、Senju DevOperation Conductor Extension Pack の README をご参照下さい。

参考

Senju DevOperation Conductor Extension Packの適用手順につきましては、Senju DevOperation Conductor Extension Pack の README をご参照下さい。

注釈

Senju DevOperation Conductor Extension Packの適用に際しては、千手システムの停止は不要ですが、関連する監視タスクの停止が必要です。

2.7.1. 設定

- **説明**

    モニタリングサブシステムを用いてIBM Cloudの監視項目を使用するための設定を行います。

- **設定手順**

    IBM Cloud監視を設定するには以下の手順が必要です。
    - IBM Cloudユーザーの登録
    - IBM Cloudサービスインスタンスの作成
    - 認証設定
    - IBM Cloud情報設定ファイルの作成

2.7.1.1. IBM Cloudユーザーの登録

IBM Cloudの監視項目の利用において、事前にIBM Cloud ユーザーの登録が必要です。IBM Cloudサイトよりユーザー登録を行って下さい。

2.7.1.2. IBM Cloudサービスインスタンスの作成

IBM Cloudの監視を行うためにはIBM Cloud Monitoring のインスタンスが必要となります。IBM CloudサイトよりIBM Cloud Monitoring のインスタンスを作成して下さい。IBM Cloud Monitoring のインスタンスのIDを取得し、IBM Cloud情報設定ファイル(sj_ibc_sys.json)の作成 で、IBM Cloud情報設定ファイルのmoniInstanceIdの値に設定して下さい。

IBM Cloud Log Analysisのログ監視を行うためにはIBM Log Analysis with logDNAサービスのインスタンスが必要となります。IBM CloudサイトよりIBM Log Analysis with logDNAサービスのインスタンスを作成して下さい。

2.7.1.3. 認証設定

2.7.1.3.1. APIキーで認証する

IBM Cloud監視を行う場合は、IBM Cloudユーザーまたはサービスに結び付いたAPIキーを使って認証します。IBM Cloudサイトより、IBM Cloudユーザーまたはサービスに IBM Cloud各サービスへのアクセスを許可するアクセスポリシーを設定して下さい。IBM Cloudユーザーまたはサービスの APIキーを取得し、IBM Cloud情報設定ファイル(sj_ibc_sys.json)の作成 で、APIキーを暗号化した値をapiKeyの値に設定して下さい。

表 2.52 IBM Cloud メトリクス監視に必要なアクセス権限

項目	設定値
サービス	IBM Cloud Monitoring with Sysdig
アクセス権限の範囲指定	すべてのリソース
プラットフォームアクセス	未指定
サービス・アクセス	リーダー

表 2.53 IBM Cloud Billing監視に必要なアクセス権限

項目	設定値
サービス	Billing サービス
アクセス権限の範囲指定	すべてのリソース
プラットフォームアクセス	未指定
サービス・アクセス	管理者

2.7.1.3.2. serviceKeyで認証する

IBM Cloud Log Analysisのログ監視を行う場合は、serviceKeyを使って認証します。IBM Cloudサイトより、IBM CloudユーザーにIBM Log Analysis with logDNAサービスへのアクセスを許可するアクセスポリシーを設定して下さい。IBM Log Analysis with logDNAサービスインスタンスのダッシュボードよりserviceKeyを作成し、IBM Cloud情報設定ファイル(sj_ibc_sys.json)の作成 で、serviceKeyを暗号化した値をserviceKeyの値に設定して下さい。

表 2.54 IBM Cloud Log Analysisのログ監視に必要なアクセス権限

項目	設定値
サービス	IBM Log Analysis with logDNA
アクセス権限の範囲指定	すべてのリソース
プラットフォームアクセス	未指定
サービス・アクセス	リーダー

2.7.1.4. IBM Cloud情報設定ファイル(sj_ibc_sys.json)の作成

sj_ibc_sys.jsonファイルは、IBM Cloudに関する監視を行うためにユーザーが設定する情報を記載する設定ファイルです。デフォルトでは「千手ホームディレクトリ/dat/opt/sj_ibc_sys.json」が使用されます。IBM Cloudの監視タスクのパラメータで認証ファイルを指定した場合は、IBM Cloudの監視タスクのパラメータで指定した認証ファイルが有効になります。

「千手ホームディレクトリ/dat/opt/sj_ibc_sys.json.sample をコピーして以下の項目を設定して下さい。

表 2.55 sj_ibc_sys.jsonの記述内容

項目	省略	デフォルト	暗号化対象	説明
moniInstanceId	不可	—	×	IBM Cloud Monitoringサービスのインスタンス ID
serviceKey	不可	—	○	認証用serviceKey(暗号化後のserviceKey)
apiKey	不可	—	○	認証用APIキー(暗号化後のAPIキー)
region	不可	—	×	IBM Cloud APIエンドポイントリージョン。
proxyURL	可	—	×	IBM Cloud接続時に経由するプロキシサーバー。(次の形式で記載して下さい "<プロトコル>:/
proxyUsername	可	—	×	プロキシサーバーアクセス用ユーザーID
proxyPassword	可	—	○	プロキシサーバーアクセス用パスワード(暗号化後のパスワード)
maxLogSize	可	—	×	省略する場合はログ監視で出力するログファイルの最大サイズが10240(単位:KB)になります。
maxLogCnt	可	—	×	省略する場合はログ監視で出力するログファイルのローテーション最大個数が7になります。
retryCount	可	3	×	API実行失敗時のリトライ回数
waitTime	可	30	×	API実行時のタイムアウト時間(単位:秒)
logFormat	可	—	×	取得したログの出力フォーマットをLTSVもしくはJSONに切り替えます。省略する場合はLTSVと
logBufferTime	可	—	×	省略する場合は前回取得した最後のログより遡る時間が5(単位:分)になります。

- proxyUsernameおよびproxyPasswordの両方を指定しなかった場合、プロキシサーバーの認証に利用しません。
- 一回以上ログを取得している状態でlogBufferTimeを現在よりも大きい値に変更した場合、変更後の1回目の実行で過去に取得したログを重複して取得する場合があります。ご注意ください。

- sj_ibc_sys.json の記載例

```
{
        "moniInstanceId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
        "apiKey": "=AfEz45kfzMeZ8Zi0xKUmacRamLTEpSZpxFqYtMSlJmnEWpi0xKUmacRamLTEpXzHMg==",
        "region":"jp-tok",
        "serviceKey": "=AT+JNez5dr8zP/zf7FN2KXaU2bQOSQt9Ul4JFV77euonHp8/mg==",
        "proxyURL": "http://10.1.0.9:8080",
        "proxyUsername": "ibcuser",
        "proxyPassword": "=Abt4+Mf0wO53Fw==",
        "maxLogSize": "",
        "maxLogCnt": "",
        "retryCount": "3",
        "waitTime": "30",
        "logFormat": "",
        "logBufferTime": ""
}
```

2.7.1.4.1. sj_setup_ibc ー IBM Cloud情報設定ファイル更新 ー

- 指定形式
  - [参照]

    ```
    sj_setup_ibc
    ```

  - [作成＆更新]

    ```
    sj_setup_ibc
       [-miid[Instance ID of the IBM Cloud Monitoring service]]
       [-sk[ServiceKey for authentication (encrypted serviceKey)]]
       [-ak[API key for authentication (API key after encryption)]]
       [-region[IBM Cloud API endpoint region]]
       [-purl[A proxy server that goes through when connecting to IBM Cloud. (Enter in
       the following format <protocol>: // <ip address | host name>: <port number>)]]
       [-puser[User ID for proxy server access]]
       [-ppswd[Password for proxy server access]]
       [-mls[If omitted, the maximum size of the log file output by log monitoring is
       10240 (unit: KB).]]
       [-mlc[If omitted, the maximum number of log file rotations output by log
       monitoring will be 7.]]
       [-rc[number of retries when API call fails]]
       [-wt[wait time(seconds) when no response is returned]]
       [-lf[format of log file output by log monitoring]]
    ```

```
[-lbt[bufferTime of log file output by log monitoring]]
```

- 目的

  IBM Cloud情報設定ファイル(/dat/opt/sj_ibc_sys.json) の現在値の参照、作成と更新を行います。

- オプション

  - -miid

    IBM Cloudモニタリングサービスのインスタンス ID（moniInstanceId）に設定する値を指定して下さい。
    値を省略するとIBM Cloud情報設定ファイルに設定されている値を削除します。

  - -sk

    認証用のサービスキー（serviceKey）に設定する値を指定して下さい。
    設定値の指定は対話形式で行われます。
    この項目は暗号化した値がIBM Cloud情報設定ファイルに書き込まれます。

  - -ak

    認証用のAPIキー（apiKey）に設定する値を指定して下さい。
    設定値の指定は対話形式で行われます。
    この項目は暗号化した値がIBM Cloud情報設定ファイルに書き込まれます。

  - -region

    IBM Cloud APIエンドポイントリージョン（region）に設定する値を指定して下さい。
    値を省略するとIBM Cloud情報設定ファイルに設定されている値を削除します。

  - -purl

    IBM Cloud接続時に経由するプロキシサーバー（proxyURL）に設定する値を指定して下さい。
    値を省略するとIBM Cloud情報設定ファイルに設定されている値を削除します。

  - -puser

    プロキシサーバーのユーザ（proxyUsername）に設定する値を指定して下さい。
    値を省略するとIBM Cloud情報設定ファイルに設定されている値を削除します。

  - -ppswd

    プロキシサーバーのパスワード（proxyPassword）に設定する値を指定して下さい。
    設定値の指定は対話形式で行われます。
    この項目は暗号化した値がIBM Cloud情報設定ファイルに書き込まれます。

  - -mls

    ログ監視によって出力されるログファイルの最大サイズ（maxLogSize）に設定する値を指定して下さい。
    値を省略するとIBM Cloud情報設定ファイルに設定されている値を削除します。

  - -mlc

    ログ監視によって出力されるログファイルのローテーション最大個数（maxLogCnt）に設定する値を指定して下さい。
    値を省略するとIBM Cloud情報設定ファイルに設定されている値を削除します。

  - -rc

    API実行失敗時のリトライ回数(retryCount)に設定する値を指定して下さい。
    値を省略するとIBM Cloud情報設定ファイルに設定されている値を削除します。

  - -wt

    API実行時のタイムアウト時間(waitTime)に設定する値を指定して下さい。
    値を省略するとIBM Cloud情報設定ファイルに設定されている値を削除します。

  - -lf

    ログ監視によって出力されるログフォーマット（logFormat）に設定する値を指定して下さい。
    値を省略するとIBM Cloud情報設定ファイルに設定されている値を削除します。

- -lbt

  最後に取得したログより遡る時間(logBufferTime)を指定して下さい。
  値を省略するとIBM Cloud情報設定ファイルに設定されている値を削除します。

- 実行結果

  - (例1)現在の設定値参照

```
% sj_setup_ibc
{
        "moniInstanceId": "XXXXX",
        "serviceKey": "**********",
        "apiKey": "",
        "region": "ABCD",
        "proxyURL": "",
        "proxyUsername": "",
        "proxyPassword": "",
        "maxLogSize": "",
        "maxLogCnt": ""
        "retryCount": "",
        "waitTime": "",
        "logFormat": "",
        "logBufferTime": ""
}

%
```

  - (例2)moniInstanceIdとserviceKey、regionを設定

```
% sj_setup_ibc -miidXXXXX-XXXXX -regionXXXX-XXXX -sk
Please enter the value.
        "serviceKey":

        The value of moniInstanceId has changed from (XXXXX) to (XXXXX-XXXXX).
        The value of region has changed from (ABCD) to (XXXX-XXXX).
        The value of serviceKey has changed from (**********) to (**********).

The update is complete.

% sj_setup_ibc
{
        "moniInstanceId": "XXXXX-XXXXX",
        "serviceKey": "**********",
        "apiKey": "",
        "region": "XXXX-XXXX",
        "proxyURL": "",
        "proxyUsername": "",
        "proxyPassword": "",
        "maxLogSize": "",
        "maxLogCnt": ""
        "retryCount": "",
        "waitTime": "",
        "logFormat": "",
        "logBufferTime": ""
}

%
```

  - (例3)設定を削除

```
% sj_setup_ibc -miid -region -sk
Please enter the value.
        "serviceKey":

        The value of moniInstanceId has changed from (XXXXX-XXXXX) to ().
        The value of region has changed from (XXXX-XXXX) to ().
        The value of serviceKey has changed from (**********) to (**********).

The update is complete.

% sj_setup_ibc
{
        "moniInstanceId": "",
        "serviceKey": "",
        "apiKey": "",
        "region": "",
        "proxyURL": "",
        "proxyUsername": "",
        "proxyPassword": "",
        "maxLogSize": "",
        "maxLogCnt": ""
        "retryCount": "",
        "waitTime": "",
        "logFormat": "",
        "logBufferTime": ""
}

%
```

注釈

- 暗号化対象項目の標準出力への表示は全てアスタリスクでマスクされます。
- 暗号化対象項目の値の設定は、キーボードからの入力が一切表示されません。コピー＆ペーストで入力することをお勧めします。
- 暗号化対象項目の値を削除する場合、何も入力せずにリターンキーを押下して下さい。

- 標準エラー出力
  - Failed to acquire Senju home directory
  - The IBC System information file does not exist.
  - Invalid data have been set in this file.
  - Failed to update the IBC System information file.
  - File update failed.

- 終了ステータス
  - 0：正常終了
  - 1：異常終了

2.7.1.4.2. IBM Cloud情報設定ファイル更新コマンドの登録

IBM Cloud情報設定ファイルの現在値の参照、作成と更新を行うため、IBM情報設定ファイル更新コマンドを千手ブラウザからユーザーコマンドに登録します。詳細な手順については、ユーザーズガイド**「2.3.2.1 ユーザーコマンド」**を参照して下さい。

- ユーザーコマンドグループの作成

  IBM Cloud情報設定ファイル更新コマンドを登録するユーザーコマンドグループを千手ブラウザから登録して下さい。

- IBM Cloud情報設定ファイル更新コマンドの登録

  作成したユーザーコマンドグループに、以下に示す起動シーケンスを指定してコマンドを登録して下さい。

  - 現在値の参照

```
sj_remshe "@ノード名@" -l "@ユーザ名@" sj_setup_ibc
```

  - 作成と更新

```
sj_remshe "@ノード名@" -l "@ユーザ名@" sj_setup_ibc "-miid@@IBM CloudモニタリングサービスのインスタンスID@@" "-sk@@認証用のサービスキー@@" "-ak@@認証用のAPIキー@@" "-region@@IBM Cloud APIエンドポイントリージョン@@" "-purl@@IBM Cloud接続時に経由するプロキシサーバー@@" "-puser@@プロキシサーバーのユーザ名@@" "-ppswd@@プロキシサーバーのパスワード@@" "-mls@@ログファイルの最大サイズ@@" "-mlc@@ログファイルのローテーション最大個数@@" "-rc@@API実行失敗時のリトライ回数@@" "-wt@@API実行時のタイムアウト時間@@" "-lf@@ログフォーマット@@" "-lbt@@最後に取得したログより遡る時間@@"
```

注釈

上記の起動シーケンスは項目を全て変更する仕様となっています。項目別に変更を行いたい場合は、起動シーケンスから任意の「**-オプション@@パラメータ名@@**」を指定したユーザーコマンドを別途登録して下さい。

（例）sj_remshe "@ノード名@" -l "@ユーザ名@" sj_setup_ibc "-miid@@IBM CloudモニタリングサービスのインスタンスID@@"

2.7.2. 使い方

IBM Cloud Monitoringに接続し、Senju DevOperation Conductorのモニタリング機能を使って、監視することができます。

監視定義を千手ブラウザより登録し、監視を実施します。監視結果は、各種モニタ画面（グローバルノードモニタ／ノードモニタ）にてその監視状況を表示できます。予め設定したしきい値により障害を検知した場合は、メッセージモニタにメッセージが通知されます。
（モニタリング機能については、ユーザーズガイド「 **4．モニタリング** 」を参照して下さい。）

注釈

メトリクス監視項目の監視間隔は1分、10分、60分、1440分（1日）のみ指定可能です。

参考

各種パラメータの設定値が分からない場合は、IBM Cloudより提供されているIBM Cloud Monitoring Web UI にて確認して下さい。

2.7.2.1. IBM Cloud Log Analysis連携機能

監視項目「IBM Cloud：Log Analysis ログ情報取得」ではIBM Cloud Log Analysisから取得したログをログファイルに蓄積します。このログファイルを監視することでアラートの検知をすることが可能です。

2.7.2.1.1. IBM Cloud Log Analysis連携機能の制限事項

IBM Cloud Log Analysisの料金プランにより、最大取得期間が制限されます。例えば「7日間のログ検索」プランの場合、現在日時が10月25日 UTC の場合、2021-10-18T00:00:00Z 以降のログが保存されています。
料金プランの参考URL：https://cloud.ibm.com/catalog/services/logdna

2.7.2.1.2. ログファイル

監視項目「IBM Cloud：Log Analysis ログ情報取得」で取得したログファイルは、パラメータで指定したファイル(絶対パス)に出力されます。ただし、ファイル名に使用できない記号は「-」(半角ハイフン)に置き換えます。

ログファイルが重複しないように設定する必要があります。

ログメッセージに含まれる改行、タブ、「\」記号は、”\t”⇒”\\t” “\n”⇒ “\\n”, “\”⇒ “\\”に置換されログファイルに出力されます。

出力されるログファイルの文字コードは UTF-8 になります。テキストログ監視の設定で監視対象ログの「文字コードを指定する」を UTF-8 に指定して下さい。

2.7.2.1.3. ログフォーマット

以下にIBM Cloud Log Analysisログ情報取得で取得したログファイルのレコード形式について説明します。レコードは LTSV形式で、項目間はタブ区切りとなります。

【IBM Cloud Log Analysisログファイル　レコード形式】

- ログフォーマットがLTSVの場合：

タイムスタンプ　タグ　ホスト　アプリケーション　重大度　ログメッセージ

表 2.56 IBMログファイルレコード形式

No.	項目	説明
1	Timestamp	「Timestamp:」に続き、取得したログエントリが出力されたタイムスタンプ(UTC)が入ります。フォーマット：YYYY-MM-DDThh（例：2021-04-14T07:09:06Z）。
2	Tag	「Tag:」に続き、取得したタグ名が入ります。
3	Host	「Host:」に続き、取得したホスト名が入ります。
4	App	「App:」に続き、取得したアプリケーション名が入ります。
5	Level	「Level:」に続き、取得したレベルが入ります。
6	LogMessage	「LogMessage:」に続き、取得したログ情報が入ります。ログ情報はJSONの形式で出力されます。

- ログフォーマットがJSONの場合：

ログメッセージ

表 2.57 IBMログファイルレコード形式

No.	項目	説明
1	LogMessage	取得したログ情報が入ります。ログ情報はJSONの形式で出力されます。

2.7.2.1.4. テキストログ監視の設定方法

以下にSenju DevOperation Conductorのテキストログ監視を利用して、IBM Cloud Log Analysisログ情報取得で取得したログメッセージを監視する運用例を示します。この例では、ログメッセージにキーワードが発生時にメッセージモニタに通知されるようにログフィルタを登録し、監視する場合について説明します。

＜ログフィルタの登録＞
千手ブラウザのツリービューで＜ドメイン＞→“フィルタ”→“ログフィルタ”を選択します。ログフィルタのエンティティでリストビューの何も表示されていない部分でマウスの右ボタンを押してコンテキストメニューを表示し、[新規作成]メニューを選択します。ログフィルタのプロパティが表示されます。ログフィルタ名などの各項目を入力し[OK]ボタンを押下します。これにより、ログフィルタの登録が完了します。

＜フィルタ監視項目の追加＞
千手ブラウザのツリービューの＜ドメイン＞→“フィルタ”→“ログフィルタ”→＜ログフィルタ＞でフィルタ監視項目を登録するログフィルタを選択し、リストビューの何も表示されていない部分でマウスの右ボタンを押してコンテキストメニューを表示し、[新規作成]メニューを選択します。フィルタ監視項目のプロパティが表示されますので、指定フィールドを検知するキーワードで監視設定し、通知したいメッセージIDを登録します。

＜テキストログ監視の設定＞
アラートファイルのテキストログ監視を行うには、千手ブラウザのツリービューで、＜ドメイン＞→“ノードグループ”→＜ノードグループ＞を選択し、そのリストビューからIBM Cloud Log Analysisログ情報取得のプローブとして設定したノードを選択し、マウスの右ボタンをクリックしコンテキストメニューを表示し、[プロパティ]メニューを選択します。ノードのプロパティウィンドウが表示されますので、[ログ監視]タブを選択します。ノードのプロパティ（[ログ監視]タブ）にて、監視対象のパス名とファイル名にIBM Cloud Log Analysisログファイルを指定し、監視方法に先に作成したログフィルタを指定します。監視対象ログの「文字コードを指定する」を UTF-8 に指定し、ログ監視を登録した後に、登録したノードに対して[反映(監視属性)]を実行することにより、ログファイルの監視を開始します。

以上で、テキストログ監視の設定方法は完了です。この設定によりIBM Cloud Log Analysisログファイルにキーワードが出力された場合、メッセージモニタに通知されます。

警告

管理対象ノードにおいて千手が起動していない状態で、[反映(監視属性)]を行うと失敗しますので、注意して下さい。

2.7.2.2. 汎用メトリクス監視機能

監視項目「IBM Cloud：メトリクス監視」では IBM Cloud Monitoring から任意のメトリクスの値を取得し、監視することができます。

注釈

Senju DevOperation Conductor Extension Packリリース時点でIBM Cloudドキュメントに記載されているメトリクスが「リソースタイプ:メトリクス」から選択可能です。

2.7.2.2.1. 汎用メトリクス監視の設定方法

以下に汎用メトリクス監視の監視定義を千手ブラウザより登録する手順を記載します。例として仮想マシンのインスタンス起動以降の累積受信バイト数を10分間隔で監視します。

＜汎用メトリクス監視タスクの登録＞

千手ブラウザのツリービューで＜ドメイン＞→“モニタリング”→“千手カテゴリ”→“クラウドサービス”を選択します。クラウドサービスのエンティティでリストビューの何も表示されていない部分でマウスの右ボタンを押してコンテキストメニューを表示し、[新規作成]→[メトリクス監視タスク]メニューを選択します。汎用メトリクス監視タスクのプロパティが表示されますので、監視項目名で「IBM Cloud：メトリクス監視」を選択し、各項目を設定します。「監視タスク名」を”IBM Cloud：メトリクス監視（ibm_is_instance_network_in_bytes）”のように適当な名前に変更します。「計算式の変数の値」フィールドの「リソースタイプ:メトリクス」の選択ボタンを押し、候補一覧から”IBM Cloud Virtual Servers:ibm_is_instance_network_in_bytes”を選択し[OK]ボタンを押下します。「計算式」から”A1”を選択、「計算結果の型」から”小数”を選択、「計算結果の比較方法」から”通常”を選択、「計算式の変数Aの値」から”Maximum”を選択、「単位」に”byte”を入力、「判定条件」に異常、警告と判定するしきい値を設定します。「検査間隔」を10分に設定します。「パラメータ」フィールドの「ラベル」に”ibm_resource,ibm_resource_name”を、「統計」に”max”を、「フィルター」に”ibm_resource_name=xxxxxxx”のように監視対象の仮想マシンのibm_resource_nameを指定します。[OK]ボタンを押し、監視タスクを登録します。

監視項目「IBM Cloud：メトリクス監視」の設定項目を以下に示します。

表 2.58 IBM Cloud：メトリクス監視の設定項目

項目名	設定内容
リソースタイプ:メトリクス	IBM Cloud Monitoring から監視するメトリクスを【サービス:メトリック】の形式で指定して下さい。候補一覧から選択することも、
計算式	計算に使用する式です。「計算式の変数Aの値」で指定したプロパティの値を計算し監視結果の値として扱います。「A0」や「A1
計算式の変数Aの値	IBM Cloud Monitoring から監視するメトリクスの統計を候補一覧から選択して下さい。以下の種類があります。 • Average • Maximum • Minimum • Sum • TimeAvg
計算結果の型	計算結果の型です。計算結果を判定条件の値と比較する際の型となります。候補一覧から選択して下さい。以下の種類があ • 整数 • 小数 • 指数 • 文字列
単位	ノードモニタに表示される単位です。
計算結果の比較方法	「判定条件」フィールド(値)の値と、比較する方法を表します。候補一覧から選択して下さい。以下の種類があります。 • 通常 • 絶対値 • 前回との差分(新たな監視対象を正常とする) • 常に正常 • 前回との差分(新たな監視対象を異常とする) • 通常(無くなった監視対象を異常とする) • 初回との差分(新たな監視対象を正常とする) • 初回との差分(新たな監視対象を異常とする) • 合計

注釈

「計算式の変数Aの値」で指定した統計に合わせて「統計」パラメータの値を指定して下さい。「統計」パラメータは全て小文字、Average、Maximum、Minimum は3文字の短縮形となります。

2.8. 付録

2.8.1. 監視項目

2.8.1.1. AWS監視

注釈

監視項目によっては、監視間隔を10分未満に設定すると値が取得できないことがあります。その場合は監視間隔を10分以上に設定して下さい。

参考

各種パラメータの設定値が分からない場合は、Amazon Web Servicesより提供されているCloudWatch Management Consoleのメトリクスにて確認して下さい。
参考URL: https://console.aws.amazon.com/cloudwatch/ (2019年8月現在)

- AWS：EC2 CPU使用率(%)

  説明 EC2インスタンスのCPUの負荷状態を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたEC2インスタンスのCPUごとの負荷率(使用率)が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は%です。デフォルト値は98です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
インスタンスID	EC2インスタンスIDを指定します。省略可です。省略した場合はすべてのEC2インスタンスについて監視を行います。タグキ
タグキー	EC2インスタンスを識別するタグのキーを指定します。省略可です。省略した場合はすべてのEC2インスタンスについて監視
タグ値	EC2インスタンスを識別するタグの値を指定します。省略可です。省略した場合はすべてのEC2インスタンスについて監視を

- AWS：EC2 ディスク読み込みバイト数(KB)

  説明 EC2インスタンスの1分あたりのエフェメラルディスクへの読み込み量を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたEC2インスタンスのディスク読み込み量が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はKBです。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
インスタンスID	EC2インスタンスIDを指定します。省略可です。省略した場合はすべてのEC2インスタンスについて監視を行います。タグキ
タグキー	EC2インスタンスを識別するタグのキーを指定します。省略可です。省略した場合はすべてのEC2インスタンスについて監視
タグ値	EC2インスタンスを識別するタグの値を指定します。省略可です。省略した場合はすべてのEC2インスタンスについて監視を

  備考 EC2インスタンスにアタッチされているebsデバイスについては、時間当たりの読み込みバイト数は監視することはできません。

- AWS：EC2 ディスク書き込みバイト数(KB)

  説明 EC2インスタンスの1分あたりのエフェメラルディスクへの書き込み量を監視します。取得データは検査間隔期間内の平均値となります。

判定条件 取得されたEC2インスタンスのディスク書き込み量が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はKBです。

パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
インスタンスID	EC2インスタンスIDを指定します。省略可です。省略した場合はすべてのEC2インスタンスについて監視を行います。タグキ
タグキー	EC2インスタンスを識別するタグのキーを指定します。省略可です。省略した場合はすべてのEC2インスタンスについて監視
タグ値	EC2インスタンスを識別するタグの値を指定します。省略可です。省略した場合はすべてのEC2インスタンスについて監視を

備考 EC2インスタンスにアタッチされているebsデバイスについては、時間当たりの書き込みバイト数は監視することはできません。

- AWS：EC2 ディスク読み込み処理数(/秒)

  説明 EC2インスタンスの1分あたりのエフェメラルディスクへの読み込み処理数を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたEC2インスタンスの1分あたりのディスク読み込み処理数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は回/秒です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
インスタンスID	EC2インスタンスIDを指定します。省略可です。省略した場合はすべてのEC2インスタンスについて監視を行います。タグキ
タグキー	EC2インスタンスを識別するタグのキーを指定します。省略可です。省略した場合はすべてのEC2インスタンスについて監視
タグ値	EC2インスタンスを識別するタグの値を指定します。省略可です。省略した場合はすべてのEC2インスタンスについて監視を

  備考 EC2インスタンスにアタッチされているebsデバイスについては、監視項目「AWS：EBS 読み込み処理数(/秒)」で監視を行って下さい。

- AWS：EC2 ディスク書き込み処理数(/秒)

  説明 EC2インスタンスの1分あたりのエフェメラルディスクへの書き込み処理数を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたEC2インスタンスの1分あたりのディスク書き込み処理数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は回/秒です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
インスタンスID	EC2インスタンスIDを指定します。省略可です。省略した場合はすべてのEC2インスタンスについて監視を行います。タグキ
タグキー	EC2インスタンスを識別するタグのキーを指定します。省略可です。省略した場合はすべてのEC2インスタンスについて監視
タグ値	EC2インスタンスを識別するタグの値を指定します。省略可です。省略した場合はすべてのEC2インスタンスについて監視を

  備考 EC2インスタンスにアタッチされているebsデバイスについては、監視項目「AWS：EBS 書き込み処理数(/秒)」で監視を行って下さい。

- AWS：EC2 ネットワーク受信バイト数(KB)

  説明 EC2インスタンスの1分あたりのネットワーク受信量を監視します。取得データは検査間隔期間内の平均値となります。

判定条件 取得されたEC2インスタンスのネットワーク受信量が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はKBです。

パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
インスタンスID	EC2インスタンスIDを指定します。省略可です。省略した場合はすべてのEC2インスタンスについて監視を行います。タグキ
タグキー	EC2インスタンスを識別するタグのキーを指定します。省略可です。省略した場合はすべてのEC2インスタンスについて監視
タグ値	EC2インスタンスを識別するタグの値を指定します。省略可です。省略した場合はすべてのEC2インスタンスについて監視を

- AWS：EC2 ネットワーク送信バイト数(KB)

  説明 EC2インスタンスの1分あたりのネットワーク送信量を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたEC2インスタンスのネットワーク送信量が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はKBです。

  パラメータ

アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
インスタンスID	EC2インスタンスIDを指定します。省略可です。省略した場合はすべてのEC2インスタンスについて監視を行います。タグキ
タグキー	EC2インスタンスを識別するタグのキーを指定します。省略可です。省略した場合はすべてのEC2インスタンスについて監視
タグ値	EC2インスタンスを識別するタグの値を指定します。省略可です。省略した場合はすべてのEC2インスタンスについて監視を

- AWS：EC2 ステータスチェック[EC2システム]

  説明 EC2インスタンスのステータスチェック[EC2システム]の結果を監視します。チェックがパスしていれば0を、そうでなければ1を返します。取得データは瞬間値となります。

  判定条件 取得されたEC2インスタンスのステータスチェック[EC2システム]の結果が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
インスタンスID	EC2インスタンスIDを指定します。省略可です。省略した場合はすべてのEC2インスタンスについて監視を行います。タグキ
タグキー	EC2インスタンスを識別するタグのキーを指定します。省略可です。省略した場合はすべてのEC2インスタンスについて監視
タグ値	EC2インスタンスを識別するタグの値を指定します。省略可です。省略した場合はすべてのEC2インスタンスについて監視を
追加オプション	EC2インスタンスのステータスチェックのインターバルを指定します。固定値の6(分)が設定されます。値は変更しないで下さ

- AWS：EC2 ステータスチェック[EC2インスタンス]

  説明 EC2インスタンスのステータスチェック[EC2インスタンス]の結果を監視します。チェックがパスしていれば0を、そうでなければ1を返します。取得データは瞬間値となります。

  判定条件 取得されたEC2インスタンスのステータスチェック[EC2インスタンス]の結果が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
インスタンスID	EC2インスタンスIDを指定します。省略可です。省略した場合はすべてのEC2インスタンスについて監視を行います。タグキ
タグキー	EC2インスタンスを識別するタグのキーを指定します。省略可です。省略した場合はすべてのEC2インスタンスについて監視
タグ値	EC2インスタンスを識別するタグの値を指定します。省略可です。省略した場合はすべてのEC2インスタンスについて監視を
追加オプション	EC2インスタンスのステータスチェックのインターバルを指定します。固定値の6(分)が設定されます。値は変更しないで下さ

- AWS：EC2 ステータスチェック

  説明 EC2インスタンスのステータスチェックの結果を監視します。[EC2システム][EC2インスタンス]のどちらも0であれば0を、そうでなければ1を返します。取得データは瞬間値となります。

  判定条件 取得されたEC2インスタンスのステータスチェックの結果が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
インスタンスID	EC2インスタンスIDを指定します。省略可です。省略した場合はすべてのEC2インスタンスについて監視を行います。タグキ
タグキー	EC2インスタンスを識別するタグのキーを指定します。省略可です。省略した場合はすべてのEC2インスタンスについて監視
タグ値	EC2インスタンスを識別するタグの値を指定します。省略可です。省略した場合はすべてのEC2インスタンスについて監視を
追加オプション	EC2インスタンスのステータスチェックのインターバルを指定します。固定値の6(分)が設定されます。値は変更しないで下さ

- AWS：EC2 インスタンス状態

  説明 EC2インスタンスの状態を監視します。取得データは瞬間値となります。

  判定条件 取得されたEC2インスタンスの状態が異常しきい値の文字列と異なる場合に正常とみなします。異常・警告しきい値には文字列のみ入力可能です。デフォルト値は"running"です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
インスタンスID	EC2インスタンスIDを指定します。省略可です。省略した場合はすべてのEC2インスタンスについて監視を行います。タグキ
タグキー	EC2インスタンスを識別するタグのキーを指定します。省略可です。省略した場合はすべてのEC2インスタンスについて監視
タグ値	EC2インスタンスを識別するタグの値を指定します。省略可です。省略した場合はすべてのEC2インスタンスについて監視を

- AWS：EC2 CPU クレジット数

  説明 [T3/T2 インスタンス] CPU 使用率に関してインスタンスで消費される CPU クレジットの数を監視します。

  判定条件 取得されたCPU クレジットの数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
インスタンスID	EC2インスタンスIDを指定します。省略可です。省略した場合はすべてのEC2インスタンスについて監視を行います。タグキ
タグキー	EC2インスタンスを識別するタグのキーを指定します。省略可です。省略した場合はすべてのEC2インスタンスについて監視
タグ値	EC2インスタンスを識別するタグの値を指定します。省略可です。省略した場合はすべてのEC2インスタンスについて監視を

- AWS:EBS 読み込みバイト数(KB)

  説明 EBSボリュームの読み込み処理一件あたりの読み込み量を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたEBSボリュームの読み込み量が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はKBです。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
ボリュームID	EBSボリュームIDを指定します。省略可です。省略した場合はすべてのEBSボリュームについて監視を行います。タグキー
タグキー	EBSボリュームを識別するタグのキーを指定します。省略可です。省略した場合はすべてのEBSボリュームについて監視を
タグ値	EBSボリュームを識別するタグの値を指定します。省略可です。省略した場合はすべてのEBSボリュームについて監視を

  備考 EBSの一回の処理での読み込み量の上限は64KBとなっています。

- AWS:EBS 書き込みバイト数(KB)

  説明 EBSボリュームの書き込み処理一件あたりの書き込み量を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたEBSボリュームの書き込み量が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はKBです。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
ボリュームID	EBSボリュームIDを指定します。省略可です。省略した場合はすべてのEBSボリュームについて監視を行います。タグキー
タグキー	EBSボリュームを識別するタグのキーを指定します。省略可です。省略した場合はすべてのEBSボリュームについて監視を
タグ値	EBSボリュームを識別するタグの値を指定します。省略可です。省略した場合はすべてのEBSボリュームについて監視を

  備考 EBSの一回の処理での書き込み量の上限は64KBとなっています。

- AWS:EBS 読み込み処理数(/秒)

  説明 EBSボリュームの5分または1分あたりの読み込み処理数を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたEBSボリュームの5分または1分あたりの読み込み処理数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は回/秒です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
ボリュームID	EBSボリュームIDを指定します。省略可です。省略した場合はすべてのEBSボリュームについて監視を行います。タグキー
タグキー	EBSボリュームを識別するタグのキーを指定します。省略可です。省略した場合はすべてのEBSボリュームについて監視を
タグ値	EBSボリュームを識別するタグの値を指定します。省略可です。省略した場合はすべてのEBSボリュームについて監視を行

備考 ボリュームのタイプにより、何分あたりのデータを取得するかが異なります。Provisioned IOPSの場合は1分あたり、それ以外は5分あたりとなります。

- AWS：EBS 書き込み処理数(/秒)

  説明 EBSボリュームの5分または1分あたりの書き込み処理数を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたEBSボリュームの5分または1分あたりの書き込み処理数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は回/秒です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
ボリュームID	EBSボリュームIDを指定します。省略可です。省略した場合はすべてのEBSボリュームについて監視を行います。タグキー
タグキー	EBSボリュームを識別するタグのキーを指定します。省略可です。省略した場合はすべてのEBSボリュームについて監視を
タグ値	EBSボリュームを識別するタグの値を指定します。省略可です。省略した場合はすべてのEBSボリュームについて監視を行

  備考 ボリュームのタイプにより、何分あたりのデータを取得するかが異なります。Provisioned IOPSの場合は1分あたり、それ以外は5分あたりとなります。

- AWS：EBS 読み込み処理時間(秒)

  説明 EBSボリュームの読み込み処理一件あたりの処理時間を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたEBSボリュームの読み込み処理時間が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は秒です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
ボリュームID	EBSボリュームIDを指定します。省略可です。省略した場合はすべてのEBSボリュームについて監視を行います。タグキー
タグキー	EBSボリュームを識別するタグのキーを指定します。省略可です。省略した場合はすべてのEBSボリュームについて監視を
タグ値	EBSボリュームを識別するタグの値を指定します。省略可です。省略した場合はすべてのEBSボリュームについて監視を行

- AWS：EBS 書き込み処理時間(秒)

  説明 EBSボリュームの書き込み処理一件あたりの処理時間を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたEBSボリュームの書き込み処理時間が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は秒です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
ボリュームID	EBSボリュームIDを指定します。省略可です。省略した場合はすべてのEBSボリュームについて監視を行います。タグキー
タグキー	EBSボリュームを識別するタグのキーを指定します。省略可です。省略した場合はすべてのEBSボリュームについて監視を
タグ値	EBSボリュームを識別するタグの値を指定します。省略可です。省略した場合はすべてのEBSボリュームについて監視を行

- AWS:EBS アイドル時間(秒)

  説明 EBSボリュームの5分または1分あたりのアイドル時間を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたEBSボリュームのアイドル時間が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は秒です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
ボリュームID	EBSボリュームIDを指定します。省略可です。省略した場合はすべてのEBSボリュームについて監視を行います。タグキー
タグキー	EBSボリュームを識別するタグのキーを指定します。省略可です。省略した場合はすべてのEBSボリュームについて監視を
タグ値	EBSボリュームを識別するタグの値を指定します。省略可です。省略した場合はすべてのEBSボリュームについて監視を行

- AWS:EBS 完了待ち要求数

  説明 EBSボリュームの完了待ちとなっている要求の数を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたEBSボリュームの完了待ちとなっている要求の数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
ボリュームID	EBSボリュームIDを指定します。省略可です。省略した場合はすべてのEBSボリュームについて監視を行います。タグキー
タグキー	EBSボリュームを識別するタグのキーを指定します。省略可です。省略した場合はすべてのEBSボリュームについて監視を
タグ値	EBSボリュームを識別するタグの値を指定します。省略可です。省略した場合はすべてのEBSボリュームについて監視を行

- AWS:ELB リクエスト処理遅延時間(秒)

  説明 ELBのリクエスト処理遅延時間を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたELBのリクエスト処理遅延時間が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は秒です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になりま
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはでき
リージョン	AWSリージョンを指定します。省略不可です。
ロードバランサネーム	ロードバランサネームを指定します。省略可です。省略した場合はすべてのELBについて監視を行います。(※1)

備考 ※1 この監視項目は「Classic Load Balancer(CLB) 」のみ対応しております。

- AWS：ELB リクエスト処理数

  説明 ELBのリクエスト処理数を監視します。取得データは検査間隔期間内の合計値となります。

  判定条件 取得されたELBのリクエスト処理数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になりま
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはでき
リージョン	AWSリージョンを指定します。省略不可です。
ロードバランサネーム	ロードバランサネームを指定します。省略可です。省略した場合はすべてのELBについて監視を行います。（※1）

  備考 ※1　この監視項目は「Classic Load Balancer(CLB) 」のみ対応しております。

- AWS：ELB アベイラビリティゾーン内ヘルスチェック成功数

  説明 ELBのヘルスチェックに成功したEC2インスタンス数をアベイラビリティゾーンごとに監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたELBのヘルスチェックに成功したEC2インスタンス数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.i
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時
リージョン	AWSリージョンを指定します。省略不可です。
ロードバランサネーム,アベイラビリティゾーン	ロードバランサネームおよびAWSリージョン内のアベイラビリティゾーンをカンマ区切りで指定します

  備考 ※1　この監視項目は「Classic Load Balancer(CLB) 」のみ対応しております。

- AWS：ELB アベイラビリティゾーン内ヘルスチェック失敗数

  説明 ELBのヘルスチェックに失敗したEC2インスタンス数をアベイラビリティゾーンごとに監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたELBのヘルスチェックに失敗したEC2インスタンス数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.i
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時
リージョン	AWSリージョンを指定します。省略不可です。
ロードバランサネーム,アベイラビリティゾーン	ロードバランサネームおよびAWSリージョン内のアベイラビリティゾーンをカンマ区切りで指定します

  備考 ※1　この監視項目は「Classic Load Balancer(CLB) 」のみ対応しております。

- AWS：ELB 4XX(クライアントエラー)HTTPレスポンス数

  説明 ELBのクライアントエラーとなったHTTPレスポンス数を監視します。取得データは検査間隔期間内の合計値となります。

  判定条件 取得されたELBのクライアントエラーとなったHTTPレスポンス数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になりま
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはでき
リージョン	AWSリージョンを指定します。省略不可です。
ロードバランサネーム	ロードバランサネームを指定します。省略可です。省略した場合はすべてのELBについて監視を行います。(※1)

備考 ※1 この監視項目は「Classic Load Balancer(CLB) 」のみ対応しております。

- AWS:ELB 5XX(サーバーエラー)HTTPレスポンス数

  説明 ELBのサーバーエラーとなったHTTPレスポンス数を監視します。取得データは検査間隔期間内の合計値となります。

  判定条件 取得されたELBのサーバーエラーとなったHTTPレスポンス数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になりま
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはでき
リージョン	AWSリージョンを指定します。省略不可です。
ロードバランサネーム	ロードバランサネームを指定します。省略可です。省略した場合はすべてのELBについて監視を行います。(※1)

  備考 ※1 この監視項目は「Classic Load Balancer(CLB) 」のみ対応しております。

- AWS:ELB バックエンドインスタンス 2XX(成功)HTTPレスポンス数

  説明 ELBバックエンドインスタンスがコード2XXを返したHTTPレスポンス数を監視します。取得データは検査間隔期間内の合計値となります。

  判定条件 取得されたELBバックエンドインスタンスがコード2XXを返したHTTPレスポンス数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になりま
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはでき
リージョン	AWSリージョンを指定します。省略不可です。
ロードバランサネーム	ロードバランサネームを指定します。省略可です。省略した場合はすべてのELBについて監視を行います。(※1)
ゼロパブリッシュ	検査間隔内にデータポイントが無かった場合に取得データの値を「0」とする場合にONを指定します。省略可能です。

  備考 ※1 この監視項目は「Classic Load Balancer(CLB) 」のみ対応しております。

  注釈

  ゼロパブリッシュがONの場合は、監視間隔でデータポイントの有無に変化があると、監視結果の状態にかかわらずメッセージモニタにメッセージが通知されます。

- AWS:ELB バックエンドインスタンス 3XX(要ユーザアクション)HTTPレスポンス数

  説明 ELBバックエンドインスタンスがコード3XXを返したHTTPレスポンス数を監視します。取得データは検査間隔期間内の合計値となります。

  判定条件 取得されたELBバックエンドインスタンスがコード3XXを返したHTTPレスポンス数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になりま
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはでき
リージョン	AWSリージョンを指定します。省略不可です。
ロードバランサネーム	ロードバランサネームを指定します。省略可です。省略した場合はすべてのELBについて監視を行います。(※1)
ゼロパブリッシュ	検査間隔内にデータポイントが無かった場合に取得データの値を「0」とする場合にONを指定します。省略可能です。

備考 ※1 この監視項目は「Classic Load Balancer(CLB) 」のみ対応しております。

注釈

ゼロパブリッシュがONの場合は、監視間隔でデータポイントの有無に変化があると、監視結果の状態にかかわらずメッセージモニタにメッセージが通知されます。

- AWS:ELB バックエンドインスタンス 4XX(クライアントエラー)HTTPレスポンス数

  説明 ELBバックエンドインスタンスがコード4XXを返したHTTPレスポンス数を監視します。取得データは検査間隔期間内の合計値となります。

  判定条件 取得されたELBバックエンドインスタンスがコード4XXを返したHTTPレスポンス数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になりま
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはでき
リージョン	AWSリージョンを指定します。省略不可です。
ロードバランサネーム	ロードバランサネームを指定します。省略可です。省略した場合はすべてのELBについて監視を行います。(※1)
ゼロパブリッシュ	検査間隔内にデータポイントが無かった場合に取得データの値を「0」とする場合にONを指定します。省略可能です。

  備考 ※1 この監視項目は「Classic Load Balancer(CLB) 」のみ対応しております。

  注釈

  ゼロパブリッシュがONの場合は、監視間隔でデータポイントの有無に変化があると、監視結果の状態にかかわらずメッセージモニタにメッセージが通知されます。

- AWS:ELB バックエンドインスタンス 5XX(サーバーエラー)HTTPレスポンス数

  説明 ELBバックエンドインスタンスがコード5XXを返したHTTPレスポンス数を監視します。取得データは検査間隔期間内の合計値となります。

  判定条件 取得されたELBバックエンドインスタンスがコード5XXを返したHTTPレスポンス数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になりま
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはでき
リージョン	AWSリージョンを指定します。省略不可です。
ロードバランサネーム	ロードバランサネームを指定します。省略可です。省略した場合はすべてのELBについて監視を行います。(※1)
ゼロパブリッシュ	検査間隔内にデータポイントが無かった場合に取得データの値を「0」とする場合にONを指定します。省略可能です。

  備考 ※1 この監視項目は「Classic Load Balancer(CLB) 」のみ対応しております。

  注釈

  ゼロパブリッシュがONの場合は、監視間隔でデータポイントの有無に変化があると、監視結果の状態にかかわらずメッセージモニタにメッセージが通知されます。

- AWS：ELB EC2インスタンス状態

  説明 ELBに関連するEC2インスタンスの状態を監視します。取得データは瞬間値となります。

  判定条件 取得されたELBに関連するEC2インスタンスの状態が異常しきい値の文字列と異なる場合に異常とみなします。異常・警告しきい値には文字列のみ入力可能です。デフォルト値は"InService,N/A"です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になりま
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはでき
リージョン	AWSリージョンを指定します。省略不可です。
ロードバランサネーム	ロードバランサネームを指定します。省略可です。省略した場合はすべてのEC2インスタンスについて監視を行います。

  備考 ※1　この監視項目は「Classic Load Balancer(CLB) 」のみ対応しております。

- AWS：ELB EC2インスタンス数

  説明 ELBに関連するEC2インスタンス数を監視します。取得データは瞬間値となります。

  判定条件 取得されたELBに関連するEC2インスタンス数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になりま
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはでき
リージョン	AWSリージョンを指定します。省略不可です。
ロードバランサネーム	ロードバランサネームを指定します。省略可です。省略した場合はすべてのEC2インスタンスについて監視を行います。

  備考 ※1　この監視項目は「Classic Load Balancer(CLB) 」のみ対応しております。

- AWS：ELB ヘルスチェック成功EC2インスタンス数

  説明 ELBのヘルスチェックが成功したEC2インスタンス数を監視します。取得データは瞬間値となります。

  判定条件 取得されたELBのヘルスチェックが成功したEC2インスタンス数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になりま
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはでき
リージョン	AWSリージョンを指定します。省略不可です。
ロードバランサネーム	ロードバランサネームを指定します。省略可です。省略した場合はすべてのEC2インスタンスについて監視を行います。

  備考 ※1　この監視項目は「Classic Load Balancer(CLB) 」のみ対応しております。

- AWS：ELB ヘルスチェック失敗EC2インスタンス数

  説明 ELBのヘルスチェックが失敗したEC2インスタンス数を監視します。取得データは瞬間値となります。

  判定条件 取得されたELBのヘルスチェックが失敗したEC2インスタンス数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になりま
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはでき
リージョン	AWSリージョンを指定します。省略不可です。
ロードバランサネーム	ロードバランサネームを指定します。省略可です。省略した場合はすべてのEC2インスタンスについて監視を行います。

備考 ※1 この監視項目は「Classic Load Balancer(CLB) 」のみ対応しております。

- AWS：ELB 異常ターゲット数[ApplicationELB]

  説明 [ApplicationELB] 異常と見なされるターゲットの数。

  判定条件 取得された異常と見なされるELBのターゲットの数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定す
リージョン	AWSリージョンを指定します。省略不可です。
ロードバランサ,ターゲットグループ	ロードバランサ、ターゲットグループを指定します。【項目名=値】で条件を指定して下さい。省略不可です

備考 ※2 この監視項目は「Application Load Balancer(ALB)」のみ対応しております。

- AWS：ELB 異常ターゲット数[NetworkELB]

  説明 [NetworkELB] 異常と見なされるターゲットの数。

  判定条件 取得された異常と見なされるELBのターゲットの数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定す
リージョン	AWSリージョンを指定します。省略不可です。
ロードバランサ,ターゲットグループ	ロードバランサ、ターゲットグループを指定します。【項目名=値】で条件を指定して下さい。省略不可です

備考 ※3 この監視項目は「Network Load Balancer(NLB)」のみ対応しております。

- AWS：SQS 取得不可メッセージ数

  説明 SQSキューの取得不可メッセージ数を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたSQSキューの取得不可メッセージ数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
キューネーム	SQSキューネームを指定します。省略可です。省略した場合はすべてのSQSキューについて監視を行います。

- AWS：SQS 取得可能メッセージ数

  説明 SQSキューの取得可能メッセージ数を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたSQSキューの取得可能メッセージ数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値に

は数値のみ入力可能です。

パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
キューネーム	SQSキューネームを指定します。省略可です。省略した場合はすべてのSQSキューについて監視を行います。

- AWS：SQS 保留メッセージ数

  説明 SQSキューの保留メッセージ数を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたSQSキューの保留メッセージ数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
キューネーム	SQSキューネームを指定します。省略可です。省略した場合はすべてのSQSキューについて監視を行います。

- AWS：SQS 取得失敗回数

  説明 SQSキューの取得失敗回数を監視します。取得データは検査間隔期間内の合計値となります。

  判定条件 取得されたSQSキューの取得失敗回数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
キューネーム	SQSキューネームを指定します。省略可です。省略した場合はすべてのSQSキューについて監視を行います。

- AWS：SQS 削除されたメッセージ数

  説明 SQSキューの削除されたメッセージ数を監視します。取得データは検査間隔期間内の合計値となります。

  判定条件 取得されたSQSキューの削除されたメッセージ数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
キューネーム	SQSキューネームを指定します。省略可です。省略した場合はすべてのSQSキューについて監視を行います。

- AWS：SQS 取得されたメッセージ数

  説明 SQSキューの取得されたメッセージ数を監視します。取得データは検査間隔期間内の合計値となります。

  判定条件 取得されたSQSキューの取得されたメッセージ数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
キューネーム	SQSキューネームを指定します。省略可です。省略した場合はすべてのSQSキューについて監視を行います。

- AWS：SQS 追加されたメッセージ数

  説明 SQSキューの追加されたメッセージ数を監視します。取得データは検査間隔期間内の合計値となります。

  判定条件 取得されたSQSキューの追加されたメッセージ数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
キューネーム	SQSキューネームを指定します。省略可です。省略した場合はすべてのSQSキューについて監視を行います。

- AWS：SQS 追加されたメッセージサイズ(KB)

  説明 SQSキューの追加されたメッセージサイズを監視します。取得データは検査間隔期間内の合計値となります。

  判定条件 取得されたSQSキューの追加されたメッセージサイズが異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はKBです。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
キューネーム	SQSキューネームを指定します。省略可です。省略した場合はすべてのSQSキューについて監視を行います。

- AWS：RDS バイナリログサイズ(MB)

  説明 DBインスタンスのバイナリログサイズを監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたDBインスタンスのバイナリログサイズが異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はMBです。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効に
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
DBインスタンスID	DBインスタンスIDを指定します。省略可です。省略した場合はすべてのDBインスタンスについて監視を行います。

- AWS：RDS CPU使用率(%)

  説明 DBインスタンスのCPUの負荷状態を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたDBインスタンスのCPU使用率が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は%です。デフォルト値は98です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効に
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできま
リージョン	AWSリージョンを指定します。省略不可です。
DBインスタンスID	DBインスタンスIDを指定します。省略可です。省略した場合はすべてのDBインスタンスについて監視を行います。Server

- AWS：RDS 仮想メモリ領域 使用量(KB)

  説明 DBインスタンスの仮想メモリ領域の使用量を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたDBインスタンスの仮想メモリ領域の使用量が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はKBです。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効に
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできま
リージョン	AWSリージョンを指定します。省略不可です。
DBインスタンスID	DBインスタンスIDを指定します。省略可です。省略した場合はすべてのDBインスタンスについて監視を行います。Server

- AWS：RDS DB接続数

  説明 DBインスタンスの接続数を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたDBインスタンスの接続数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効に
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできま
リージョン	AWSリージョンを指定します。省略不可です。
DBインスタンスID	DBインスタンスIDを指定します。省略可です。省略した場合はすべてのDBインスタンスについて監視を行います。Server

- AWS：RDS メモリ未使用量(MB)

  説明 DBインスタンスのメモリ未使用量を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたDBインスタンスのメモリ未使用量が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はMBです。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効に
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできま
リージョン	AWSリージョンを指定します。省略不可です。
DBインスタンスID	DBインスタンスIDを指定します。省略可です。省略した場合はすべてのDBインスタンスについて監視を行います。Server

- AWS：RDS ディスク未使用量(MB)

  説明 DBインスタンスのディスク未使用量を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたDBインスタンスのディスク未使用量が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はMBです。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効に
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできま
リージョン	AWSリージョンを指定します。省略不可です。
DBインスタンスID	DBインスタンスIDを指定します。省略可です。省略した場合はすべてのDBインスタンスについて監視を行います。

- AWS:RDS 読み込み処理数(/秒)

  説明 DBインスタンスの1秒あたりの読み込み処理数を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたDBインスタンスの1秒あたりの読み込み処理数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は回/秒です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効に
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできま
リージョン	AWSリージョンを指定します。省略不可です。
DBインスタンスID	DBインスタンスIDを指定します。省略可です。省略した場合はすべてのDBインスタンスについて監視を行います。Server

- AWS:RDS 書き込み処理数(/秒)

  説明 DBインスタンスの1秒あたりの書き込み処理数を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたDBインスタンスの1秒あたりの書き込み処理数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は回/秒です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効に
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできま
リージョン	AWSリージョンを指定します。省略不可です。
DBインスタンスID	DBインスタンスIDを指定します。省略可です。省略した場合はすべてのDBインスタンスについて監視を行います。Server

- AWS:RDS 読み込み遅延時間(秒)

  説明 DBインスタンスの読み込み遅延時間を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたDBインスタンスの読み込み遅延時間が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は秒です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効に
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできま
リージョン	AWSリージョンを指定します。省略不可です。
DBインスタンスID	DBインスタンスIDを指定します。省略可です。省略した場合はすべてのDBインスタンスについて監視を行います。Server

- AWS:RDS 書き込み遅延時間(秒)

  説明 DBインスタンスの書き込み遅延時間を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたDBインスタンスの書き込み遅延時間が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は秒です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効に
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできま
リージョン	AWSリージョンを指定します。省略不可です。
DBインスタンスID	DBインスタンスIDを指定します。省略可です。省略した場合はすべてのDBインスタンスについて監視を行います。Server

- AWS：RDS 読み込みスループット(Kbps)

  説明 DBインスタンスの読み込みスループットを監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたDBインスタンスの読み込みスループットが異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はKB/秒です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効に
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできま
リージョン	AWSリージョンを指定します。省略不可です。
DBインスタンスID	DBインスタンスIDを指定します。省略可です。省略した場合はすべてのDBインスタンスについて監視を行います。Server

- AWS：RDS 書き込みスループット(Kbps)

  説明 DBインスタンスの書き込みスループットを監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたDBインスタンスの書き込みスループットが異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はKB/秒です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効に
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできま
リージョン	AWSリージョンを指定します。省略不可です。
DBインスタンスID	DBインスタンスIDを指定します。省略可です。省略した場合はすべてのDBインスタンスについて監視を行います。Server

- AWS：RDS リードレプリカ反映遅延時間(秒)

  説明 DBインスタンスのリードレプリカ反映遅延時間を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたDBインスタンスのリードレプリカ反映遅延時間が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は秒です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効に
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできま
リージョン	AWSリージョンを指定します。省略不可です。
DBインスタンスID	DBインスタンスIDを指定します。省略可です。省略した場合はすべてのDBインスタンスについて監視を行います。

- AWS：RDS ディスク全体容量(GB)

  説明 DBインスタンスのディスク全体容量を監視します。取得データは瞬間値となります。

  判定条件 取得されたDBインスタンスのディスク全体容量が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はGBです。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効に
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできま
リージョン	AWSリージョンを指定します。省略不可です。
DBインスタンスID	DBインスタンスIDを指定します。省略可です。省略した場合はすべてのDBインスタンスについて監視を行います。

- AWS：RDS インスタンス状態

  説明 DBインスタンスの状態を監視します。取得データは瞬間値となります。

  判定条件 取得されたDBインスタンスの状態が異常しきい値の文字列と異なる場合に正常とみなします。異常・警告しきい値には文字列のみ入力可能です。デフォルト値は"available"です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効に
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできま
リージョン	AWSリージョンを指定します。省略不可です。
DBインスタンスID	DBインスタンスIDを指定します。省略可です。省略した場合はすべてのDBインスタンスについて監視を行います。

- AWS：RDS インスタンス作成日時

  説明 DBインスタンス作成日時を監視します。取得データは瞬間値となります。

  判定条件 取得されたDBインスタンス作成日時は常に正常とみなします。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効に
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできま
リージョン	AWSリージョンを指定します。省略不可です。
DBインスタンスID	DBインスタンスIDを指定します。省略可です。省略した場合はすべてのDBインスタンスについて監視を行います。

- AWS：RDS スナップショット数

  説明 DBインスタンスに関連するスナップショット数を監視します。取得データは瞬間値となります。

  判定条件 取得されたDBインスタンスに関連するスナップショット数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効に
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできま
リージョン	AWSリージョンを指定します。省略不可です。
DBインスタンスID	DBインスタンスIDを指定します。省略可です。省略した場合はすべてのDBインスタンスについて監視を行います。

- AWS：RDS スナップショット合計サイズ(GB)

  説明 DBインスタンスに関連するスナップショットの合計サイズを監視します。取得データは瞬間値となります。

  判定条件 取得されたDBインスタンスに関連するスナップショットの合計サイズが異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はGBです。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効に
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできま
リージョン	AWSリージョンを指定します。省略不可です。
DBインスタンスID	DBインスタンスIDを指定します。省略可です。省略した場合はすべてのDBインスタンスについて監視を行います。

- AWS：RDS スナップショットサイズ(GB)

  説明 DBスナップショットのサイズを監視します。取得データは瞬間値となります。

  判定条件 取得されたDBスナップショットのサイズが異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はGBです。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になりま
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはでき
リージョン	AWSリージョンを指定します。省略不可です。
DBスナップショットID	DBスナップショットIDを指定します。省略可です。省略した場合はすべてのDBスナップショットについて監視を行います

- AWS：RDS Auroraディスク未使用量(MB)

  説明 AuroraDBインスタンスのディスク未使用量を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたAuroraDBインスタンスのディスク未使用量が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はMBです。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効に
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできま
リージョン	AWSリージョンを指定します。省略不可です。
DBインスタンスID	DBインスタンスIDを指定します。省略可です。省略した場合はすべてのDBインスタンスについて監視を行います。

- AWS：RDS Auroraリードレプリカ反映遅延時間(ミリ秒)

  説明 AuroraDBインスタンスのリードレプリカ反映遅延時間を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたAuroraDBインスタンスのリードレプリカ反映遅延時間が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はミリ秒です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効に
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできま
リージョン	AWSリージョンを指定します。省略不可です。
DBインスタンスID	DBインスタンスIDを指定します。省略可です。省略した場合はすべてのDBインスタンスについて監視を行います。

- AWS：RDS Auroraクラスター状態

  説明 Auroraクラスターの状態を監視します。取得データは瞬間値となります。

  判定条件 取得されたDBクラスターの状態が異常しきい値の文字列と異なる場合に正常とみなします。異常・警告しきい値には文字列のみ入力可能です。デフォルト値は"available"です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
DBクラスターID	DBクラスターIDを指定します。省略可です。省略した場合はすべてのDBクラスターについて監視を行います。

- AWS：RDS Auroraクラスター作成日時

  説明 Auroraクラスターの作成日時を監視します。取得データは瞬間値となります。

  判定条件 取得されたDBクラスター作成日時は常に正常とみなします。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
DBクラスターID	DBクラスターIDを指定します。省略可です。省略した場合はすべてのDBクラスターについて監視を行います。

- AWS：RDS Auroraスナップショット数

  説明 Auroraクラスターに関連するスナップショット数を監視します。取得データは瞬間値となります。

  判定条件 取得されたDBクラスターに関連するスナップショット数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
DBクラスターID	DBクラスターIDを指定します。省略可です。省略した場合はすべてのDBクラスターについて監視を行います。

- AWS：RDS Auroraスナップショット合計サイズ(GB)

  説明 Auroraクラスターに関連するスナップショットの合計サイズを監視します。取得データは瞬間値となります。

  判定条件 取得されたDBクラスターに関連するスナップショットの合計サイズが異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はGBです。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
DBクラスターID	DBクラスターIDを指定します。省略可です。省略した場合はすべてのDBクラスターについて監視を行います。

- AWS：RDS Auroraスナップショットサイズ(GB)

  説明 Auroraクラススナップショットのサイズを監視します。取得データは瞬間値となります。

  判定条件 取得されたDBクラススナップショットのサイズが異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はGBです。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定する
リージョン	AWSリージョンを指定します。省略不可です。
DBクラスタースナップショットID	DBクラスタースナップショットIDを指定します。省略可です。省略した場合はすべてのDBクラスタースナップシ

- AWS：SNS 発行メッセージ数

  説明 SNSトピックの発行メッセージ数を監視します。取得データは検査間隔期間内の合計値となります。

  判定条件 取得されたSNSトピックの発行メッセージ数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
トピックネーム	SNSトピックネームを指定します。省略可です。省略した場合はすべてのSNSトピックについて監視を行います。
ゼロパブリッシュ	検査間隔内にデータポイントが無かった場合に取得データの値を「0」とする場合にONを指定します。省略可能です。省略

注釈

ゼロパブリッシュがONの場合は、監視間隔でデータポイントの有無に変化があると、監視結果の状態にかかわらずメッセージモニタにメッセージが通知されます。

- AWS：SNS 送信済みメッセージ数

  説明 SNSトピックの送信済みメッセージ数を監視します。取得データは検査間隔期間内の合計値となります。

  判定条件 取得されたSNSトピックの送信済みメッセージ数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
トピックネーム	SNSトピックネームを指定します。省略可です。省略した場合はすべてのSNSトピックについて監視を行います。
ゼロパブリッシュ	検査間隔内にデータポイントが無かった場合に取得データの値を「0」とする場合にONを指定します。省略可能です。省略

注釈

ゼロパブリッシュがONの場合は、監視間隔でデータポイントの有無に変化があると、監視結果の状態にかかわらずメッセージモニタにメッセージが通知されます。

- AWS：SNS 送信失敗メッセージ数

  説明 SNSトピックの送信失敗メッセージ数を監視します。取得データは検査間隔期間内の合計値となります。

  判定条件 取得されたSNSトピックの送信失敗メッセージ数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
トピックネーム	SNSトピックネームを指定します。省略可です。省略した場合はすべてのSNSトピックについて監視を行います。
ゼロパブリッシュ	検査間隔内にデータポイントが無かった場合に取得データの値を「0」とする場合にONを指定します。省略可能です。省略

注釈

ゼロパブリッシュがONの場合は、監視間隔でデータポイントの有無に変化があると、監視結果の状態にかかわらずメッセージモニタにメッセージが通知されます。

- AWS：SNS 送信メッセージサイズ(KB)

  説明 SNSトピックの一件あたりの送信メッセージサイズを監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたSNSトピックの送信メッセージサイズが異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はKBです。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
トピックネーム	SNSトピックネームを指定します。省略可です。省略した場合はすべてのSNSトピックについて監視を行います。
ゼロパブリッシュ	検査間隔内にデータポイントが無かった場合に取得データの値を「0」とする場合にONを指定します。省略可能です。省略

注釈

ゼロパブリッシュがONの場合は、監視間隔でデータポイントの有無に変化があると、監視結果の状態にかかわらずメッセージモニタにメッセージが通知されます。

- AWS：EMR 割り当て待ちコアノード数

  説明 EMRの割り当て待ちコアノード数を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたEMRの割り当て待ちコアノード数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
ジョブフローID	EMRジョブフローIDを指定します。省略可です。省略した場合はすべてのEMRジョブフローについて監視を行います。

- AWS：EMR 稼働中コアノード数

  説明 EMRの稼働中コアノード数を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたEMRの稼働中コアノード数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
ジョブフローID	EMRジョブフローIDを指定します。省略可です。省略した場合はすべてのEMRジョブフローについて監視を行います。

- AWS：EMR HDFSストレージ 読み込みバイト数(MB)

  説明 EMRの5分あたりのHDFSストレージの読み込み量を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたEMRのHDFSストレージの読み込み量が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はMBです。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
ジョブフローID	EMRジョブフローIDを指定します。省略可です。省略した場合はすべてのEMRジョブフローについて監視を行います。

- AWS：EMR HDFSストレージ 書き込みバイト数(MB)

  説明 EMRの5分あたりのHDFSストレージの書き込み量を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたEMRのHDFSストレージの書き込み量が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はMBです。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
ジョブフローID	EMRジョブフローIDを指定します。省略可です。省略した場合はすべてのEMRジョブフローについて監視を行います。

- AWS：EMR HDFSストレージ 使用率(%)

  説明 EMRのHDFSストレージの使用率を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたEMRのHDFSストレージの使用率が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は%です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
ジョブフローID	EMRジョブフローIDを指定します。省略可です。省略した場合はすべてのEMRジョブフローについて監視を行います。

- AWS：EMR アイドル状態

  説明 EMRのアイドル状態を監視します。アイドル状態であれば1を、そうでなければ0を返します。取得データは瞬間値となります。

  判定条件 取得されたEMRのアイドル状態が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
ジョブフローID	EMRジョブフローIDを指定します。省略可です。省略した場合はすべてのEMRジョブフローについて監視を行います。
追加オプション	EMRのアイドル状態の取得インターバルを指定します。固定値の6(分)が設定されます。値は変更しないで下さい。

- AWS：EMR 異常終了ジョブ数

  説明 EMRの異常終了ジョブ数を監視します。取得データはクラスター作成時からの累積値となります。

  判定条件 取得されたEMRの異常終了ジョブ数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
ジョブフローID	EMRジョブフローIDを指定します。省略可です。省略した場合はすべてのEMRジョブフローについて監視を行います。

- AWS：EMR 稼働中ジョブ数

  説明 EMRの稼働中ジョブ数を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたEMRの稼働中ジョブ数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
ジョブフローID	EMRジョブフローIDを指定します。省略可です。省略した場合はすべてのEMRジョブフローについて監視を行います。

- AWS：EMR データノード使用率(%)

  説明 EMRのデータノード使用率を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたEMRのデータノード使用率が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は%です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
ジョブフローID	EMRジョブフローIDを指定します。省略可です。省略した場合はすべてのEMRジョブフローについて監視を行います。

- AWS：EMR タスクトラッカー使用率(%)

  説明 EMRのタスクトラッカー使用率を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたEMRのタスクトラッカー使用率が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は%です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
ジョブフローID	EMRジョブフローIDを指定します。省略可です。省略した場合はすべてのEMRジョブフローについて監視を行います。

- AWS：EMR 空きMapスロット数

  説明 EMRの空きMapスロット数を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたEMRの空きMapスロット数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
ジョブフローID	EMRジョブフローIDを指定します。省略可です。省略した場合はすべてのEMRジョブフローについて監視を行います。

- AWS：EMR 破損ブロック数

  説明 EMRの破損ブロック数を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたEMRの破損ブロック数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
ジョブフローID	EMRジョブフローIDを指定します。省略可です。省略した場合はすべてのEMRジョブフローについて監視を行います。

- AWS：EMR 空きReduceスロット数

  説明 EMRの空きReduceスロット数を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたEMRの空きReduceスロット数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
ジョブフローID	EMRジョブフローIDを指定します。省略可です。省略した場合はすべてのEMRジョブフローについて監視を行います。

- AWS：EMR 残りMapタスク数

  説明 EMRの残りMapタスク数を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたEMRの残りMapタスク数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
ジョブフローID	EMRジョブフローIDを指定します。省略可です。省略した場合はすべてのEMRジョブフローについて監視を行います。

- AWS：EMR 残りMapタスク／Mapスロット

  説明 EMRのMapスロット数に対する残りMapタスク数の割合を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたEMRのMapスロット数に対する残りMapタスク数の割合が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
ジョブフローID	EMRジョブフローIDを指定します。省略可です。省略した場合はすべてのEMRジョブフローについて監視を行います。

- AWS：EMR 残りReduceタスク数

  説明 EMRの残りReduceタスク数を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたEMRの残りReduceタスク数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
ジョブフローID	EMRジョブフローIDを指定します。省略可です。省略した場合はすべてのEMRジョブフローについて監視を行います。

- AWS：EMR 稼働中Mapタスク数

  説明 EMRの稼働中Mapタスク数を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたEMRの稼働中Mapタスク数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
ジョブフローID	EMRジョブフローIDを指定します。省略可です。省略した場合はすべてのEMRジョブフローについて監視を行います。

- AWS：EMR 稼働中Reduceタスク数

  説明 EMRの稼働中Reduceタスク数を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたEMRの稼働中Reduceタスク数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
ジョブフローID	EMRジョブフローIDを指定します。省略可です。省略した場合はすべてのEMRジョブフローについて監視を行います。

- AWS：EMR S3読み込みバイト数(KB)

  説明 EMRの5分あたりのS3読み込み量を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたEMRのS3読み込み量が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はKBです。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
ジョブフローID	EMRジョブフローIDを指定します。省略可です。省略した場合はすべてのEMRジョブフローについて監視を行います。

- AWS：EMR S3書き込みバイト数(KB)

  説明 EMRの5分あたりのS3書き込み量を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたEMRのS3書き込み量が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はKBです。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
ジョブフローID	EMRジョブフローIDを指定します。省略可です。省略した場合はすべてのEMRジョブフローについて監視を行います。

- AWS：EMR 割り当て待ちタスクノード数

  説明 EMRの割り当て待ちタスクノード数を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたEMRの割り当て待ちタスクノード数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
ジョブフローID	EMRジョブフローIDを指定します。省略可です。省略した場合はすべてのEMRジョブフローについて監視を行います。

- AWS：EMR 稼働中タスクノード数

  説明 EMRの稼働中タスクノード数を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたEMRの稼働中タスクノード数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
ジョブフローID	EMRジョブフローIDを指定します。省略可です。省略した場合はすべてのEMRジョブフローについて監視を行います。

- AWS：EMR 同時データ転送

  説明 EMRの同時データ転送の合計数を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたEMRの同時データ転送の合計数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
ジョブフローID	EMRジョブフローIDを指定します。省略可です。省略した場合はすべてのEMRジョブフローについて監視を行います。

- AWS：EMR Hbaseバックアップ成否

  説明 EMRのHbaseジョブフローにて、直近のバックアップ結果を監視します。バックアップに成功していれば0を、そうでなければ1を返します。取得データは瞬間値となります。

  判定条件 取得されたEMRのHbaseジョブフローにて、直近のバックアップ結果が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。デフォルト値は0です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
ジョブフローID	EMRジョブフローIDを指定します。省略可です。省略した場合はすべてのEMRジョブフローについて監視を行います。
追加オプション	バックアップ結果の取得インターバルを指定します。固定値の6(分)が設定されます。値は変更しないで下さい。

- AWS：EMR Hbaseバックアップ処理時間(分)

  説明 EMRのHbaseジョブフローにて、直近のバックアップに要した時間を監視します。取得データは瞬間値となります。

  判定条件 取得されたEMRのHbaseジョブフローにて、直近のバックアップに要した時間が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は分です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
ジョブフローID	EMRジョブフローIDを指定します。省略可です。省略した場合はすべてのEMRジョブフローについて監視を行います。
追加オプション	バックアップに要した時間の取得インターバルを指定します。固定値の6(分)が設定されます。値は変更しないで下さい。

- AWS：EMR Hbaseバックアップ成功後経過時間(分)

  説明 EMRのHbaseジョブフローにて、最後にバックアップが成功してからの経過時間を監視します。取得データは瞬間値となります。

  判定条件 取得されたEMRのHbaseジョブフローにて、最後にバックアップが成功してからの経過時間が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は分です。

パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
ジョブフローID	EMRジョブフローIDを指定します。省略可です。省略した場合はすべてのEMRジョブフローについて監視を行います。
追加オプション	バックアップが成功してからの経過時間の取得インターバルを指定します。固定値の6(分)が設定されます。値は変更しない

- AWS：S3 バケット使用量

  説明 S3バケットの使用量を監視します。取得データは瞬間値となります。

  判定条件 取得されたS3バケットの使用量が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はByteです。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効に
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定すること
リージョン	AWSリージョンを指定します。省略不可です。
ストレージタイプ,バケット名	ストレージタイプおよびS3バケット名をカンマ区切りで指定します。省略可です。省略した場合はすべてのS3バケ

  注釈

  データポイントの更新は日次ですが更新時刻が不定期のため、監視間隔を 2880分 (2日)に設定して下さい。

- AWS：S3 オブジェクト数

  説明 S3バケットのオブジェクト数を監視します。取得データは瞬間値となります。

  判定条件 取得されたS3バケットのオブジェクト数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効に
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定すること
リージョン	AWSリージョンを指定します。省略不可です。
ストレージタイプ,バケット名	ストレージタイプおよびS3バケット名をカンマ区切りで指定します。省略可です。省略した場合はすべてのS3バケ

  注釈

  データポイントの更新は日次ですが更新時刻が不定期のため、監視間隔を 2880分 (2日)に設定して下さい。

- AWS：S3 HTTP リクエスト総数

  説明 S3 バケットに対して行われた HTTP リクエストの総数を監視します。(タイプに関係なく)

  判定条件 取得されたS3バケットに対するHTTP リクエスト総数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になり
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはで
リージョン	AWSリージョンを指定します。省略不可です。
バケット名,フィルターID	S3バケット名およびフィルターIDをカンマ区切りで指定します。省略可です。省略した場合はすべてのS3バケットにつ

- AWS:AS インスタンス状態

  説明 オートスケーリンググループに関連するEC2インスタンスの状態を監視します。取得データは瞬間値となります。

  判定条件 取得されたオートスケーリンググループに関連するEC2インスタンスの状態が異常しきい値の文字列と異なる場合に異常とみなします。異常・警告しきい値には文字列のみ入力可能です。デフォルト値は"Healthy,N/A"です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定するこ
リージョン	AWSリージョンを指定します。省略不可です。
オートスケーリンググループ名	オートスケーリンググループ名を指定します。省略可です。省略した場合はすべてのEC2インスタンスについて監

- AWS:AS インスタンス数

  説明 オートスケーリンググループに関連するEC2インスタンス数を監視します。取得データは瞬間値となります。

  判定条件 取得されたオートスケーリンググループに関連するEC2インスタンス数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定するこ
リージョン	AWSリージョンを指定します。省略不可です。
オートスケーリンググループ名	オートスケーリンググループ名を指定します。省略可です。省略した場合はすべてのオートスケーリンググループ

- AWS:AS オートスケール処理時間(秒)

  説明 オートスケーリングの処理時間を監視します。取得データは瞬間値となります。

  判定条件 取得されたオートスケーリングの処理時間が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は秒です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定するこ
リージョン	AWSリージョンを指定します。省略不可です。
オートスケーリンググループ名	オートスケーリンググループ名を指定します。省略可です。省略した場合はすべてのオートスケーリンググループ

- AWS:AS オートスケール実行回数

  説明 オートスケーリングの実行回数を監視します。取得データは検査間隔期間内の発生数となります。

  判定条件 取得されたオートスケーリングの実行回数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定するこ
リージョン	AWSリージョンを指定します。省略不可です。
オートスケーリンググループ名	オートスケーリンググループ名を指定します。省略可です。省略した場合はすべてのオートスケーリンググループ

- AWS：AS オートスケール最終実行日時

  説明 オートスケーリング実行の最終日時を監視します。取得データは瞬間値となります。

  判定条件 取得されたオートスケーリング実行の最終日時は常に正常とみなします。しきい値には文字列のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定するこ
リージョン	AWSリージョンを指定します。省略不可です。
オートスケーリンググループ名	オートスケーリンググループ名を指定します。省略可です。省略した場合はすべてのオートスケーリンググループ

- AWS：AS インスタンス ライフサイクル状態

  説明 オートスケーリンググループに関連するEC2インスタンスのライフサイクル状態を監視します。取得データは瞬間値となります。

  判定条件 取得されたオートスケーリンググループに関連するEC2インスタンスのライフサイクル状態が異常しきい値の文字列を含む場合に異常とみなします。異常・警告しきい値には文字列のみ入力可能です。デフォルト値は"Terminating"です。
  ライフサイクル状態の出力する文字列は、以下の3つの状態になります。
  ・Pending
  ・InService
  ・Terminating:WaitまたはTerminating:Proceed

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定するこ
リージョン	AWSリージョンを指定します。省略不可です。
オートスケーリンググループ名	オートスケーリンググループ名を指定します。省略可です。省略した場合はすべてのEC2インスタンスについて監

- AWS：CW アラーム状態更新回数

  説明 CWアラームの状態更新回数を取得します。取得データは検査間隔期間内の発生数となります。

  判定条件 取得されたCWアラームの状態更新回数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
アラームネーム	CWアラームネームを指定します。省略可です。省略した場合はすべてのCWアラームについて監視を行います。

- AWS：CW アラーム状態

  説明 CWアラームの状態を監視します。取得データは瞬間値となります。

  判定条件 取得されたCWアラームの状態が異常しきい値の文字列と異なる場合に異常とみなします。異常・警告しきい値には文字列のみ入力可能です。デフォルト値は"OK"です。

パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
アラームネーム	CWアラームネームを指定します。省略可です。省略した場合はすべてのCWアラームについて監視を行います。

- AWS：CW アラーム状態最終更新日時

  説明 CWアラーム状態更新の最終日時を監視します。取得データは瞬間値となります。

  判定条件 取得されたCWアラーム状態更新の最終日時は常に正常とみなします。しきい値には文字列のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
アラームネーム	CWアラームネームを指定します。省略可です。省略した場合はすべてのCWアラームについて監視を行います。

- AWS：Billing 利用料金($)

  説明 AWSの利用料金を監視します。取得データは瞬間値となります。

  判定条件 取得されたAWSの利用料金が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
追加オプション	AWSの利用料金の取得インターバルを指定します。固定値の540(分)が設定されます。値は変更しないで下さい。

- AWS：CostExplorer 利用金額取得(メトリクス：BLENDED_COST)

  説明 AWSの利用金額を監視します(メトリクス：BLENDED_COST)。取得データは瞬間値となります。

  判定条件 取得された利用金額が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することは
タイプ	グループ化するタイプを指定します。タグでグループ化したい場合はタイプに「TAG」を指定し、キーにタグキーを指定
キー	グループ化するキーを指定します。タグでグループ化したい場合はタイプに「TAG」を指定し、キーにタグキーを指定
モード	モードを指定します。省略不可です。固定値の monitoringTask が設定されます。値は変更しないで下さい。
期間フラグ(day/month)	利用金額の取得範囲を昨日(day)か当月(month)か切り替えます。デフォルト値は昨日(day)となります。省略不

- AWS：CostExplorer 利用金額取得(メトリクス：UNBLENDED_COST)

  説明 AWSの利用金額を監視します(メトリクス：UNBLENDED_COST)。取得データは瞬間値となります。

  判定条件 取得された利用金額が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することは
タイプ	グループ化するタイプを指定します。タグでグループ化したい場合はタイプに「TAG」を指定し、キーにタグキーを指定
キー	グループ化するキーを指定します。タグでグループ化したい場合はタイプに「TAG」を指定し、キーにタグキーを指定
モード	モードを指定します。省略不可です。固定値の monitoringTask が設定されます。値は変更しないで下さい。
期間フラグ(day/month)	利用金額の取得範囲を昨日(day)か当月(month)か切り替えます。デフォルト値は昨日(day)となります。省略不

- AWS：CostExplorer 利用金額取得(メトリクス：AMORTIZED_COST)

  説明 AWSの利用金額を監視します(メトリクス：AMORTIZED_COST)。取得データは瞬間値となります。

  判定条件 取得された利用金額が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することは
タイプ	グループ化するタイプを指定します。タグでグループ化したい場合はタイプに「TAG」を指定し、キーにタグキーを指定
キー	グループ化するキーを指定します。タグでグループ化したい場合はタイプに「TAG」を指定し、キーにタグキーを指定
モード	モードを指定します。省略不可です。固定値の monitoringTask が設定されます。値は変更しないで下さい。
期間フラグ(day/month)	利用金額の取得範囲を昨日(day)か当月(month)か切り替えます。デフォルト値は昨日(day)となります。省略不

- AWS：CostExplorer 利用金額取得(メトリクス：NET_AMORTIZED_COST)

  説明 AWSの利用金額を監視します(メトリクス：NET_AMORTIZED_COST)。取得データは瞬間値となります。

  判定条件 取得された利用金額が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することは
タイプ	グループ化するタイプを指定します。タグでグループ化したい場合はタイプに「TAG」を指定し、キーにタグキーを指定
キー	グループ化するキーを指定します。タグでグループ化したい場合はタイプに「TAG」を指定し、キーにタグキーを指定
モード	モードを指定します。省略不可です。固定値の monitoringTask が設定されます。値は変更しないで下さい。
期間フラグ(day/month)	利用金額の取得範囲を昨日(day)か当月(month)か切り替えます。デフォルト値は昨日(day)となります。省略不

- AWS：CostExplorer 利用金額取得(メトリクス：NET_UNBLENDED_COST)

  説明 AWSの利用金額を監視します(メトリクス：NET_UNBLENDED_COST)。取得データは瞬間値となります。

  判定条件 取得された利用金額が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することは
タイプ	グループ化するタイプを指定します。タグでグループ化したい場合はタイプに「TAG」を指定し、キーにタグキーを指定
キー	グループ化するキーを指定します。タグでグループ化したい場合はタイプに「TAG」を指定し、キーにタグキーを指定
モード	モードを指定します。省略不可です。固定値の monitoringTask が設定されます。値は変更しないで下さい。
期間フラグ(day/month)	利用金額の取得範囲を昨日(day)か当月(month)か切り替えます。デフォルト値は昨日(day)となります。省略不

- AWS：CostExplorer 利用金額取得(メトリクス：USAGE_QUANTITY)

  説明 AWSの使用量を監視します(メトリクス：USAGE_QUANTITY)。取得データは瞬間値となります。

  判定条件 取得された使用量が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することは
タイプ	グループ化するタイプを指定します。タグでグループ化したい場合はタイプに「TAG」を指定し、キーにタグキーを指定
キー	グループ化するキーを指定します。タグでグループ化したい場合はタイプに「TAG」を指定し、キーにタグキーを指定
モード	モードを指定します。省略不可です。固定値の monitoringTask が設定されます。値は変更しないで下さい。
期間フラグ(day/month)	使用量の取得範囲を昨日(day)か当月(month)か切り替えます。デフォルト値は昨日(day)となります。省略不可

- AWS：CostExplorer 利用金額取得(メトリクス：NORMALIZED_USAGE_AMOUNT)

  説明 AWSのリザーブドインスタンスの正規化係数の合計を監視します(メトリクス：NORMALIZED_USAGE_AMOUNT)。取得データは瞬間値となります。

  判定条件 取得された合計値が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することは
タイプ	グループ化するタイプを指定します。タグでグループ化したい場合はタイプに「TAG」を指定し、キーにタグキーを指定
キー	グループ化するキーを指定します。タグでグループ化したい場合はタイプに「TAG」を指定し、キーにタグキーを指定
モード	モードを指定します。省略不可です。固定値の monitoringTask が設定されます。値は変更しないで下さい。
期間フラグ(day/month)	合計値の取得範囲を昨日(day)か当月(month)か切り替えます。デフォルト値は昨日(day)となります。省略不可

- AWS：CWL AWSログ情報取得

  説明 AWSのログ情報を監視します。取得データは成否となります。

  判定条件 ログ収集に失敗した場合、異常となります。ログの件数が多く、ログを取得し切れなかった場合、警告となります。異常・警告しきい値は変更しないで下さい。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
ロググループ名	ロググループ名を指定します。省略不可です。
ログフォーマット	取得したログの出力フォーマットをLTSVもしくはJSONに切り替えます。デフォルト値はLTSVとなります。省略可能です。
ログファイル	出力ログファイルのフルパスを指定します。省略可能です。

  備考 Amazon CloudWatch Logs連携機能については、Amazon CloudWatch Logs連携機能 を参照して下さい。

  注釈

  AWS：CWL AWSログ情報取得では、最後に取得したログのタイムスタンプよりlogBufferTimeに指定した分数遡ってログを取得します。監視タスクの新規作成時などの最後に取得したログが無い場合は「監視間隔＋logBufferTime＋5分」以内に発生したログを取得します。
  AWS Cloud Watch Log では、発生したログが AWS Cloud Watch Log 上に現れるまでに時間がかかる場合があります。その時間が監視間隔以上かかる場合、ログが取得されない状態となります。このような場合は、logBufferTimeを適切に設定して下さい。

- AWS：API Gateway API リクエスト合計数

説明 指定期間内の API リクエストの合計数を監視します。

判定条件 取得されたAPI リクエストの合計数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
API 名	API 名を指定します。省略可です。省略した場合はすべてのAPIについて監視を行います。

- AWS：CloudFront リクエスト数

説明 すべての HTTP メソッドと HTTP および HTTPS リクエストの両方のリクエストの数を監視します。

判定条件 取得されたCloudFrontに対するリクエスト数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.ini
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキー
リージョン	AWSリージョンを指定します。省略不可です。
リージョン,ディストリビューションの CloudFront ID	リージョンおよびディストリビューションの CloudFront IDをカンマ区切りで指定します。省
ゼロパブリッシュ	検査間隔内にデータポイントが無かった場合に取得データの値を「0」とする場合にONを

注釈

ゼロパブリッシュがONの場合は、監視間隔でデータポイントの有無に変化があると、監視結果の状態にかかわらずメッセージモニタにメッセージが通知されます。

- AWS：Events ターゲット呼び出し回数

説明 Eventsに反応してルールのターゲットが呼び出された回数を測定します。

判定条件 取得されたターゲット呼び出し回数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
ルール名	ルール名を指定します。省略可です。省略した場合はすべてのルールについて監視を行います。

- AWS：Logs ログイベント数

説明 CloudWatch Logs にアップロードされたログイベントの数を監視します。LogGroupName ディメンションと同時に使用すると、ロググループにアップロードされたログイベントの数になります。

判定条件 取得されたログイベント数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
ロググループ名	ロググループ名を指定します。省略可です。省略した場合はすべてのロググループについて監視を行います。

- AWS：DX 接続状態

  説明 接続の状態を監視します。0 は DOWN、1 は UP を示します。

  判定条件 取得されたDirect Connect接続の状態が 1 と異なる場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
接続ID	接続IDを指定します。省略可です。省略した場合はすべてのDirect Connectについて監視を行います。

- AWS：DynamoDB 読み取り容量ユニット数

  説明 指定の期間内に消費された読み取り容量ユニットの数を監視します。

  判定条件 取得された読み取り容量ユニットの数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aw
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同
リージョン	AWSリージョンを指定します。省略不可です。
テーブル名,グローバルセカンダリインデックス名	テーブル名およびグローバルセカンダリインデックス名をカンマ区切りで指定します。省略可です

- AWS：DynamoDB 書き込み容量ユニット数

  説明 指定の期間内に消費された書き込み容量ユニットの数を監視します。

  判定条件 取得された書き込み容量ユニットの数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aw
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同
リージョン	AWSリージョンを指定します。省略不可です。
テーブル名,グローバルセカンダリインデックス名	テーブル名およびグローバルセカンダリインデックス名をカンマ区切りで指定します。省略可です

- AWS：ECS CPU の割合

  説明 クラスターやサービスで使用されている CPU の割合を監視します。

  判定条件 取得されたクラスターのCPU使用率が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は%です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することは
リージョン	AWSリージョンを指定します。省略不可です。
サービス名,クラスター名	サービス名およびクラスター名をカンマ区切りで指定します。省略可です。省略した場合はすべてのクラスターについ

- AWS：ECS メモリの割合

  説明 クラスターやサービスで利用されるメモリの割合を監視します。

  判定条件 取得されたクラスターのメモリ使用率が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は%です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することは
リージョン	AWSリージョンを指定します。省略不可です。
サービス名,クラスター名	サービス名およびクラスター名をカンマ区切りで指定します。省略可です。省略した場合はすべてのクラスターについ

- AWS：EFS I/O制限数

  説明 ファイルシステムが汎用パフォーマンス モードの I/O 制限にどれだけ近づいているかを監視します。

  判定条件 取得されたファイルシステムのI/O使用率が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は%です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効に
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできま
リージョン	AWSリージョンを指定します。省略不可です。
ファイルシステムID	ファイルシステムIDを指定します。省略可です。省略した場合はすべての汎用パフォーマンスモードを使用したファイルシス

- AWS：Lambda 関数の呼び出し回数

  説明 イベントまたは API 呼び出しに応じて呼び出される関数の回数を測定します。

  判定条件 取得された関数の呼び出し回数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
関数名	関数名を指定します。省略可です。省略した場合はすべての関数について監視を行います。

- AWS：Lambda 関数の呼び出しエラー回数

  説明 関数 (応答コード 4XX) エラーが原因で失敗した呼び出しの数を測定します。

  判定条件 取得された失敗した関数の呼び出し回数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
関数名	関数名を指定します。省略可です。省略した場合はすべての関数について監視を行います。

- AWS：Lambda 関数の実行時間

  説明 呼び出しの結果として関数コードが実行を開始してから関数の実行が停止されるまでの実行時間を測定します。

  判定条件 取得された関数の実行時間が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はミリ秒です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
関数名	関数名を指定します。省略可です。省略した場合はすべての関数について監視を行います。

- AWS：Route53 ヘルスチェックエンドポイント状態

  説明 CloudWatch で確認しているヘルスチェックエンドポイントのステータスを監視します。[1] は正常を示し、[0] は異常を示します。HealthCheckStatus は、すべてのリージョンについてのみ確認できます (選択したリージョンについてのデータは表示できません)。

  判定条件 取得されたRoute53 ヘルスチェックエンドポイントの状態が 1 と異なる場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	省略不可です。この監視項目は、すべてのリージョンについてのみ確認できます (選択したリージョンについてのデータは表
ヘルスチェックID	ヘルスチェックIDを指定します。省略可です。省略した場合はすべてのRoute53 ヘルスチェックについて監視を行います。

- AWS：NATGateway アクティブTCP接続合計数

  説明 NATゲートウェイ経由の同時アクティブTCP接続の合計数を監視します

  判定条件 取得されたNATゲートウェイのアクティブTCP接続数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になりま
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはでき
リージョン	AWSリージョンを指定します。省略不可です。
NAT ゲートウェイID	NAT ゲートウェイIDを指定します。省略可です。省略した場合はすべてのNAT ゲートウェイについて監視を行います。

- AWS：VPN トンネル状態

  説明 トンネルの状態を監視します。0はDOWNを示し、1はUPを示します。

  判定条件 取得されたVPNのトンネル状態が 1 と異なる場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になり
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはで
リージョン	AWSリージョンを指定します。省略不可です。
トンネルの IP アドレス	トンネルの IP アドレスをカンマ区切りで指定します。省略可です。省略した場合はすべてのVPNについて監視を行い

- AWS：メトリクス監視

  説明 指定したメトリクスの情報を取得します

  判定条件 「計算式の変数の値」で指定した「ネームスペース:メトリクス」から取得したメトリクス値の判定条件を指定して下さい。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
ディメンション	ディメンションで指定したリソースだけ取得したい場合に指定します。【ディメンション名=値】の形式で指定して下さい。省略
タグキー	リソースを識別するタグのキーを指定します。省略可です。ディメンションと同時に指定することはできません。タグ値を省略
タグ値	リソースを識別するタグの値を指定します。省略可です。ディメンションと同時に指定することはできません。タグ値を指定す
ゼロパブリッシュ	検査間隔内にデータポイントが無かった場合に取得データの値を「0」とする場合にONを指定します。省略可能です。省略

- AWS：Health イベント情報取得

  説明 Health イベント情報を監視します。取得データは成否となります。

  判定条件 Health イベント情報収集に失敗した場合、異常となります。ログの件数が多く、ログを取得し切れなかった場合、警告となります。異常・警告しきい値は変更しないで下さい。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
モード	モードを指定します。省略可能です。更新日時(update)、作成日時(create)かを切り替えます。デフォルト値は更新日時
フィルター	フィルターを指定します。省略可能です。すべてのイベント(all)、影響のあるイベント(affected)かを切り替えます。デフォルト
ログフォーマット	取得したログの出力フォーマットをLTSVもしくはJSONに切り替えます。デフォルト値はLTSVとなります。省略可能です。
ログファイル	出力ログファイルのフルパスを指定します。省略可能です。

注釈

AWS：Health イベント情報取得では、最後に取得したログのタイムスタンプよりlogBufferTimeに指定した分数遡ってログを取得します。監視タスクの新規作成時などの最後に取得したログが無い場合は過去3ヶ月に発生したログを取得します。

- AWS：キャパシティ監視

  説明 指定した使用状況メトリクスのキャパシティ情報を取得します。取得データは瞬間値となります。

  判定条件 「計算式の変数の値」で指定した「ネームスペース:メトリクス」から取得したキャパシティ値の判定条件を指定して下さい。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効にな
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできませ
リージョン	AWSリージョンを指定します。省略不可です。
統計	取得するメトリクスの統計単位を候補「Average、Maximum、Minimum」から選択します。省略不可です。
ゼロパブリッシュ	検査間隔内にデータポイントが無かった場合に取得データの値を「0」とする場合にONを指定します。省略可能です。省略

- AWS：Athena ログ情報取得

  説明 Athenaのログ情報取得を監視します。取得データは成否となります。

  判定条件 ログ情報収集に失敗した場合、異常となります。ログの件数が多く、ログを取得し切れなかった場合、警告となります。異常・警告しきい値は変更しないで下さい。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になりま
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはで
リージョン	AWSリージョンを指定します。省略不可です。
ワークグループ名	取得対象のワークグループ名を指定します。省略不可です。
データベース名	取得対象のデータベース名を指定します。省略不可です。
タイムスタンプカラム名	クエリ対象のタイムスタンプカラム名を指定します。省略不可です。
クエリファイルパス	Athenaで実行したいクエリを記載したファイルのフルパスを指定します(※1)。省略不可です。
s3パス	クエリ実行結果が保存するS3のパスを指定します。省略不可です。
ログファイル	出力ログファイルのフルパスを指定します。省略可能です。
ログフォーマット	取得したログの出力フォーマットをLTSVもしくはJSONに切り替えます。デフォルト値はLTSVとなります。省略可能で

  備考 Amazon Athena連携機能については、Amazon Athena連携機能 を参照して下さい。

  ※1　クエリファイルのパスを指定し、このファイルには必ずタイムスタンプ条件付きのクエリを記載してください(下記の例ではWHERE timegenerated >= %ExtPack_LastTimeStamp%に該当します)。プログラムで実際のスタート時間を%ExtPack_LastTimeStamp%に置き換えます。
  例：SELECT * FROM dataTable WHERE timegenerated >= %ExtPack_LastTimeStamp% AND containerid = '964909d62941a14b3c8c174645d' ORDER BY computer DESC,timegenerated ASC;

  注釈

  AWS：Athena ログ情報取得では、最後に取得したログのタイムスタンプよりlogBufferTimeに指定した分数遡ってログを取得します。監視タスクの新規作成時などの最後に取得したログが無い場合は「監視間隔＋logBufferTime＋5分」以内に発生したログを取得します。
  AWS Athenaでは、発生したログが AWS Athena上に現れるまでに時間がかかる場合があります。その時間が監視間隔以上かかる場合、ログが取得されない状態となります。このような場合は、logBufferTimeを適切に設定して下さい。

- AWS：SQS メッセージ取得

  説明 Amazon SQSメッセージ情報を取得します。取得データは成否となります。

  判定条件 Amazon SQSメッセージ情報収集に失敗した場合、異常となります。ログの件数が多く、ログを取得し切れなかった場合、警告となります。異常・警告しきい値は変更しないで下さい。

  パラメータ

パラメータ名	説明
アクセスキー	AWS接続用のアクセスキーIDを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効になります。
シークレットキー	AWS接続用のシークレットアクセスキーを指定します。省略可です。省略した場合はsj_aws.iniで指定した値が有効に
プロファイル	AWS接続用のプロファイル名を指定します。省略可です。アクセスキー、シークレットキーと同時に指定することはできま
リージョン	接続先AWSのリージョンを指定します。省略不可です。
キューUrl	メッセージの受信元となるAmazon SQSキューのURLを指定します。省略不可です。
メッセージ属性名	メッセージ属性の名前を指定します。省略可能です。省略した場合はメッセージ属性を返しません。「All」または「.*」を
属性名	属性の名前を指定します。省略可能です。省略した場合は「SentTimestamp」以外の属性を返しません。「All」を指
ログフォーマット	取得したログの出力フォーマットをLTSVもしくはJSONに切り替えます。デフォルト値はLTSVとなります。省略可能です。
ログファイル	出力ログファイルのフルパスを指定します。省略可能です。

備考 ※1 「属性名」で指定できる属性：ApproximateFirstReceiveTimestamp、AverageReceiveCount、AWSTraceHeader、SenderId、SentTimestamp、SqsManagedSseEnabled、MessageDeduplicationId、MessageGroupId、SequenceNumber

2.8.1.2. Azure監視

注釈

監視項目によっては、監視間隔を10分未満に設定すると値が取得できないことがあります。その場合は監視間隔を10分以上に設定して下さい。

参考

各種パラメータの設定値が分からない場合は、Azure ポータルにて確認して下さい。

- Azure：Batch コア数

  説明 Batchアカウントの専用コアの合計数を監視します。取得データは瞬間値となります。

  判定条件 取得されたBatchアカウントの専用コアの合計数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式：A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure：Batch ノード数

  説明 Batchアカウントの専用ノードの合計数を監視します。取得データは瞬間値となります。

  判定条件 取得されたBatchアカウントの専用ノードの合計数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式：A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure：Batch 開始ノード数

  説明 Batchアカウントのタスクを開始したノード数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたBatchアカウントのタスクを開始したノード数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式：A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure：Batch 待機ノード数

  説明 Batchアカウントの開始したタスクの完了を待っているノード数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたBatchアカウントの開始したタスクの完了を待っているノード数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式：A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure：Batch 失敗ノード数

  説明 Batchアカウントの開始したタスクが失敗したノード数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたBatchアカウントの開始したタスクが失敗したノード数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式：A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure：Batch アイドルノード数

  説明 Batchアカウントのアイドル状態のノード数を監視します。取得データは瞬間値となります。

  判定条件 取得されたBatchアカウントのアイドル状態のノード数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式：A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure：Batch オフラインノード数

  説明 Batchアカウントのオフライン状態のノード数を監視します。取得データは瞬間値となります。

  判定条件 取得されたBatchアカウントのオフライン状態のノード数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Batch 再起動中ノード数

  説明 Batchアカウントの再起動中のノード数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたBatchアカウントの再起動中のノード数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Batch 再イメージ化中ノード数

  説明 Batchアカウントの再イメージ化中のノード数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたBatchアカウントの再イメージ化中のノード数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Batch 実行中ノード数

  説明 Batchアカウントのタスク実行中のノード数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたBatchアカウントのタスク実行中のノード数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Batch プール移動中ノード数

  説明 Batchアカウントのプールから移動中のノード数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたBatchアカウントのプールから移動中のノード数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Batch 使用不可ノード数

  説明 Batchアカウントの使用できないノード数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたBatchアカウントの使用できないノード数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Batch プール作成イベント数

  説明 Batchアカウントでプールの作成を開始したイベント数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたBatchアカウントでプールの作成を開始したイベント数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Batch プールサイズ変更開始イベント数

  説明 Batchアカウントでプールのサイズ変更を開始したイベント数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたBatchアカウントでプールのサイズ変更を開始したイベント数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Batch プールサイズ変更完了イベント数

  説明 Batchアカウントでプールのサイズ変更が完了したイベント数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたBatchアカウントでプールのサイズ変更が完了したイベント数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Batch プール削除開始イベント数

  説明 Batchアカウントでプール削除を開始したイベント数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたBatchアカウントでプール削除を開始したイベント数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Batch 作成ノード数

  説明 Batchアカウントで作成されたノード数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたBatchアカウントで作成されたノード数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Redis Cache 合計処理数

  説明 Redis Cacheでキャッシュサーバーによって処理されたコマンド数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたRedis Cacheでキャッシュサーバーによって処理されたコマンド数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
メトリック名	メトリック名を指定します。省略不可です。シャード全体の値を監視したい場合は、デフォルト値のままで監視タスクを作
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Redis Cache 接続クライアント数

  説明 Redis Cacheでキャッシュに接続されるクライアントの数を監視します。取得データは検査間隔の最大値となります。

  判定条件 取得されたRedis Cacheでキャッシュに接続されるクライアントの数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
メトリック名	メトリック名を指定します。省略不可です。シャード全体の値を監視したい場合は、デフォルト値のままで監視タスクを作
フィルター	ディメンションを指定します。省略可能です。(形式：A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure：Redis Cache キャッシュヒット数

  説明 Redis Cacheでキー検索に成功した数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたRedis Cacheでキー検索に成功した数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
メトリック名	メトリック名を指定します。省略不可です。シャード全体の値を監視したい場合は、デフォルト値のままで監視タスクを作
フィルター	ディメンションを指定します。省略可能です。(形式：A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure：Redis Cache キャッシュミス数

  説明 Redis Cacheでキー検索に失敗した数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたRedis Cacheでキー検索に失敗した数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
メトリック名	メトリック名を指定します。省略不可です。シャード全体の値を監視したい場合は、デフォルト値のままで監視タスクを作
フィルター	ディメンションを指定します。省略可能です。(形式：A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure：Redis Cache 取得数

  説明 Redis Cacheでキャッシュから実行された取得処理の数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたRedis Cacheでキャッシュから実行された取得処理の数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
メトリック名	メトリック名を指定します。省略不可です。シャード全体の値を監視したい場合は、デフォルト値のままで監視タスクを作
フィルター	ディメンションを指定します。省略可能です。(形式：A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure：Redis Cache 設定数

  説明 Redis Cacheでキャッシュから実行された設定処理の数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたRedis Cacheでキャッシュから実行された設定処理の数が異常しきい値より大きい場合に異常とみなします。異

常・警告しきい値には数値のみ入力可能です。

パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
メトリック名	メトリック名を指定します。省略不可です。シャード全体の値を監視したい場合は、デフォルト値のままで監視タスクを作
フィルター	ディメンションを指定します。省略可能です。(形式：A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure：Redis Cache 削除されたキー数

  説明 Redis Cacheでmaxmemoryの制限によってキャッシュから削除された項目の数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたRedis Cacheでmaxmemoryの制限によってキャッシュから削除された項目の数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
メトリック名	メトリック名を指定します。省略不可です。シャード全体の値を監視したい場合は、デフォルト値のままで監視タスクを作
フィルター	ディメンションを指定します。省略可能です。(形式：A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure：Redis Cache 合計キー数

  説明 Redis Cacheでキャッシュ内のキーの最大数を監視します。取得データは検査間隔の最大値となります。

  判定条件 取得されたRedis Cacheでキャッシュ内のキーの最大数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
メトリック名	メトリック名を指定します。省略不可です。シャード全体の値を監視したい場合は、デフォルト値のままで監視タスクを作
フィルター	ディメンションを指定します。省略可能です。(形式：A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure：Redis Cache 期限切れキー数

  説明 Redis Cacheで期限が切れたキャッシュの項目数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたRedis Cacheで期限が切れたキャッシュの項目数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
メトリック名	メトリック名を指定します。省略不可です。シャード全体の値を監視したい場合は、デフォルト値のままで監視タスクを作
フィルター	ディメンションを指定します。省略可能です。(形式：A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure：Redis Cache メモリ使用量(MB)

  説明 Redis Cacheでキャッシュ内のキー／値のペアで使用されるキャッシュメモリの量を監視します。取得データは検査間隔の最大値となります。

  判定条件 取得されたRedis Cacheでキャッシュ内のキー／値のペアで使用されるキャッシュメモリの量が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はMBです。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
メトリック名	メトリック名を指定します。省略不可です。シャード全体の値を監視したい場合は、デフォルト値のままで監視タスクを作
フィルター	ディメンションを指定します。省略可能です。(形式：A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure：Redis Cache RSSメモリ使用量(MB)

  説明 Redis Cacheで使用されるキャッシュメモリの量を監視します。取得データは検査間隔の最大値となります。

  判定条件 取得されたRedis Cacheで使用されるキャッシュメモリの量が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はMBです。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
メトリック名	メトリック名を指定します。省略不可です。シャード全体の値を監視したい場合は、デフォルト値のままで監視タスクを作
フィルター	ディメンションを指定します。省略可能です。(形式：A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure：Redis Cache サーバー利用率(%)

  説明 Redis Cacheでサーバー処理中であるサイクルの割合を監視します。取得データは検査間隔の最大値となります。

  判定条件 取得されたRedis Cacheでサーバー処理中であるサイクルの割合が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は%です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
メトリック名	メトリック名を指定します。省略不可です。シャード全体の値を監視したい場合は、デフォルト値のままで監視タスクを作
フィルター	ディメンションを指定します。省略可能です。(形式：A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure：Redis Cache キャッシュの書き込み(Byte/秒)

  説明 Redis Cacheでキャッシュから書き込まれたデータ量を監視します。取得データは検査間隔の最大値となります。

  判定条件 取得されたRedis Cacheでキャッシュから書き込まれたデータ量が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はByte/秒です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
メトリック名	メトリック名を指定します。省略不可です。シャード全体の値を監視したい場合は、デフォルト値のままで監視タスクを作
フィルター	ディメンションを指定します。省略可能です。(形式：A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure：Redis Cache キャッシュの読み取り(Byte/秒)

  説明 Redis Cacheでキャッシュから読み取られたデータ量を監視します。取得データは検査間隔の最大値となります。

  判定条件 取得されたRedis Cacheでキャッシュから読み取られたデータ量が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はByte/秒です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
メトリック名	メトリック名を指定します。省略不可です。シャード全体の値を監視したい場合は、デフォルト値のままで監視タスクを作
フィルター	ディメンションを指定します。省略可能です。(形式：A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure：Redis Cache CPU使用率(%)

  説明 Redis CacheでCPU使用率を監視します。取得データは検査間隔の最大値となります。

  判定条件 取得されたRedis CacheのCPU使用率が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は%です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
メトリック名	メトリック名を指定します。省略不可です。シャード全体の値を監視したい場合は、デフォルト値のままで監視タスクを作
フィルター	ディメンションを指定します。省略可能です。(形式：A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure：Compute CPU使用率(%)

  説明 仮想マシンのCPU使用率を監視します。取得データは検査間隔の平均値となります。

  判定条件 取得された仮想マシンのCPU使用率が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は%です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式：A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure：Compute ネットワーク受信バイト数(KB)

  説明 仮想マシンのすべてのネットワークインターフェイスで受信したデータ量を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得された仮想マシンのすべてのネットワークインターフェイスで受信したデータ量が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はKBです。

パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Compute ネットワーク送信バイト数(KB)

  説明 仮想マシンのすべてのネットワークインターフェイスで送信したデータ量を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得された仮想マシンのすべてのネットワークインターフェイスで送信したデータ量が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はKBです。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Compute ディスク読み取りバイト数(KB)

  説明 仮想マシンのディスク読み取りデータ量を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得された仮想マシンのディスク読み取りデータ量が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はKBです。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Compute ディスク書き込みバイト数(KB)

  説明 仮想マシンのディスク書き込みデータ量を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得された仮想マシンのディスク書き込みデータ量が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はKBです。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Compute ディスク読み取り処理数(/秒)

  説明 仮想マシンのディスク読み取りIOPSを監視します。取得データは検査間隔の平均値となります。

  判定条件 取得された仮想マシンのディスク読み取りIOPSが異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は/秒です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Compute ディスク書き込み処理数(/秒)

  説明 仮想マシンのディスク書き込みIOPSを監視します。取得データは検査間隔の平均値となります。

  判定条件 取得された仮想マシンのディスク書き込みIOPSが異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は/秒です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Compute 未使用CPU クレジット

  説明 バーストに使用できるクレジットの合計を監視します。

  判定条件 取得された仮想マシンの未使用CPU クレジット数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Compute データ ディスク読み取りバイト数/秒

  説明 監視期間中に 1 つのディスクから読み取られた合計バイト数/秒。

  判定条件 取得された仮想マシンのディスク読み取りバイト数/秒が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は/秒です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Compute データ ディスク書き込みバイト数/秒

  説明 監視期間中に 1 つのディスクに書き込まれた合計バイト数/秒。

  判定条件 取得された仮想マシンのディスク書き込みバイト数/秒が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は/秒です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Compute CPU使用率(%) [スケールセット]

  説明 スケールセットのCPU使用率を監視します。取得データは検査間隔の平均値となります。

  判定条件 取得されたスケールセットのCPU使用率が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は%です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Compute ネットワーク受信バイト数(KB) [スケールセット]

  説明 スケールセットのすべてのネットワークインターフェイスで受信したデータ量を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたスケールセットのすべてのネットワークインターフェイスで受信したデータ量が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はKBです。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Compute ネットワーク送信バイト数(KB) [スケールセット]

  説明 スケールセットのすべてのネットワークインターフェイスで送信したデータ量を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたスケールセットのすべてのネットワークインターフェイスで送信したデータ量が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はKBです。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Compute ディスク読み取りバイト数(KB) [スケールセット]

  説明 スケールセットのディスク読み取りデータ量を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたスケールセットのディスク読み取りデータ量が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はKBです。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Compute ディスク書き込みバイト数(KB) [スケールセット]

  説明 スケールセットのディスク書き込みデータ量を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたスケールセットのディスク書き込みデータ量が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はKBです。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Compute ディスク読み取り処理数(/秒) [スケールセット]

  説明 スケールセットのディスク読み取りIOPSを監視します。取得データは検査間隔の平均値となります。

  判定条件 取得されたスケールセットのディスク読み取りIOPSが異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は/秒です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Compute ディスク書き込み処理数(/秒) [スケールセット]

  説明 スケールセットのディスク書き込みIOPSを監視します。取得データは検査間隔の平均値となります。

  判定条件 取得されたスケールセットのディスク書き込みIOPSが異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は/秒です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Compute CPU使用率(%) [スケールセット/仮想マシン]

  説明 スケールセット内仮想マシンのCPU使用率を監視します。取得データは検査間隔の平均値となります。

  判定条件 取得されたスケールセット内仮想マシンのCPU使用率が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は%です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Compute ネットワーク受信バイト数(KB) [スケールセット/仮想マシン]

  説明 スケールセット内仮想マシンのすべてのネットワークインターフェイスで受信したデータ量を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたスケールセット内仮想マシンのすべてのネットワークインターフェイスで受信したデータ量が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はKBです。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Compute ネットワーク送信バイト数(KB) [スケールセット/仮想マシン]

  説明 スケールセット内仮想マシンのすべてのネットワークインターフェイスで送信したデータ量を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたスケールセット内仮想マシンのすべてのネットワークインターフェイスで送信したデータ量が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はKBです。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Compute ディスク読み取りバイト数(KB) [スケールセット/仮想マシン]

  説明 スケールセット内仮想マシンのディスク読み取りデータ量を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたスケールセット内仮想マシンのディスク読み取りデータ量が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はKBです。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Compute ディスク書き込みバイト数(KB) [スケールセット/仮想マシン]

  説明 スケールセット内仮想マシンのディスク書き込みデータ量を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたスケールセット内仮想マシンのディスク書き込みデータ量が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はKBです。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Compute ディスク読み取り処理数(/秒) [スケールセット/仮想マシン]

  説明 スケールセット内仮想マシンのディスク読み取りIOPSを監視します。取得データは検査間隔の平均値となります。

  判定条件 取得されたスケールセット内仮想マシンのディスク読み取りIOPSが異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は/秒です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Compute ディスク書き込み処理数(/秒) [スケールセット/仮想マシン]

  説明 スケールセット内仮想マシンのディスク書き込みIOPSを監視します。取得データは検査間隔の平均値となります。

  判定条件 取得されたスケールセット内仮想マシンのディスク書き込みIOPSが異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は/秒です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:IoT Hub 送信試行テレメトリメッセージ数

  説明 IoT Hubへの送信が試行されたDevice to Cloudテレメトリメッセージの数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたIoT Hubへの送信が試行されたDevice to Cloudテレメトリメッセージの数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:IoT Hub 送信済みテレメトリメッセージ数

  説明 IoT Hubに正常に送信されたDevice to Cloudテレメトリメッセージの数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたIoT Hubに正常に送信されたDevice to Cloudテレメトリメッセージの数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:IoT Hub 完了コマンド数

  説明 IoT Hubのデバイスで正常に完了したCloud to Deviceコマンドの数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたIoT Hubのデバイスで正常に完了したCloud to Deviceコマンドの数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:IoT Hub 中止コマンド数

  説明 IoT Hubのデバイスで中止されたCloud to Deviceコマンドの数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたIoT Hubのデバイスで中止されたCloud to Deviceコマンドの数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:IoT Hub 拒否コマンド数

  説明 IoT Hubのデバイスで拒否されたCloud to Deviceコマンドの数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたIoT Hubのデバイスで拒否されたCloud to Deviceコマンドの数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:IoT Hub 接続デバイス数

  説明 IoT Hubに接続されているデバイスの数を監視します。取得データは瞬間値となります。

  判定条件 取得されたIoT Hubに接続されているデバイスの数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:IoT Hub 合計デバイス数

  説明 IoT Hubに登録されているデバイスの数を監視します。取得データは瞬間値となります。

  判定条件 取得されたIoT Hubに登録されているデバイスの数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Event Hub 受信要求数

  説明 Event Hubの受信要求数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたEvent Hubの受信要求数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Event Hub 成功要求数

  説明 Event Hubの成功した要求数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたEvent Hubの成功した要求数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Event Hub 失敗要求数

  説明 Event Hubで失敗した要求数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたEvent Hubで失敗した要求数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Event Hub サーバービジーエラー数

  説明 Event Hubのサーバービジーエラー数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたEvent Hubのサーバービジーエラー数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Event Hub 内部サーバーエラー数

  説明 Event Hubの内部サーバーエラー数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたEvent Hubの内部サーバーエラー数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Event Hub その他のエラー数

  説明 Event Hubで発生したその他のエラー数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたvent Hubで発生したその他のエラー数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Event Hub 受信メッセージ数

  説明 Event Hubの受信メッセージ数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたEvent Hubの受信メッセージ数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Event Hub 送信メッセージ数

  説明 Event Hubの送信メッセージ数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたEvent Hubの送信メッセージ数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Event Hub 受信バイト数(KB)

  説明 Event Hubの受信バイト数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたEvent Hubの受信バイト数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はKBです。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Event Hub 送信バイト数(KB)

  説明 Event Hubの送信バイト数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたEvent Hubの送信バイト数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はKBです。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Event Hub アーカイブバックログメッセージ数

  説明 Event Hubのアーカイブバックログメッセージ数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたEvent Hubのアーカイブバックログメッセージ数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Event Hub アーカイブメッセージ数

  説明 Event Hubのアーカイブメッセージ数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたEvent Hubのアーカイブメッセージ数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Event Hub アーカイブメッセージスループット(KB)

  説明 Event Hubのアーカイブメッセージ処理データ量を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたEvent Hubのアーカイブメッセージ処理データ量が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はKBです。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Event Hub Cluster 受信要求数

  説明 Event Hub Clusterの受信要求数を監視します。

  判定条件 取得されたEvent Hub Clusterの受信要求数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Logic Apps 実行開始ワークフロー数

  説明 Logic Appsで実行を開始したワークフロー数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたLogic Appsで実行を開始したワークフロー数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Logic Apps 完了ワークフロー数

  説明 Logic Appsで完了したワークフロー数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたLogic Appsで完了したワークフロー数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Logic Apps 成功ワークフロー数

  説明 Logic Appsで実行に成功したワークフロー数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたLogic Appsで実行に成功したワークフロー数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Logic Apps 失敗ワークフロー数

  説明 Logic Appsで実行に失敗したワークフロー数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたLogic Appsで実行に失敗したワークフロー数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Logic Apps キャンセルワークフロー数

  説明 Logic Appsでキャンセルされたワークフロー数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたLogic Appsでキャンセルされたワークフロー数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Logic Apps スロットルイベント数

  説明 Logic Appsでワークフローアクションまたはトリガーのスロットルイベント数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたLogic Appsでワークフローアクションまたはトリガーのスロットルイベント数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Logic Apps 開始アクション数

  説明 Logic Appsで開始したワークフローアクション数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたLogic Appsで開始したワークフローアクション数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Logic Apps 完了アクション数

  説明 Logic Appsで完了したワークフローアクション数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたLogic Appsで完了したワークフローアクション数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Logic Apps 成功アクション数

  説明 Logic Appsで成功したワークフローアクション数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたLogic Appsで成功したワークフローアクション数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Logic Apps 失敗アクション数

  説明 Logic Appsで失敗したワークフローアクション数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたLogic Appsで失敗したワークフローアクション数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Logic Apps スキップアクション数

  説明 Logic Appsでスキップされたワークフローアクション数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたLogic Appsでスキップされたワークフローアクション数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Logic Apps アクションスロットルイベント数

  説明 Logic Appsでワークフローアクションのスロットルイベント数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたLogic Appsでワークフローアクションのスロットルイベント数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Logic Apps 開始トリガー数

  説明 Logic Appsで開始したワークフロートリガー数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたLogic Appsで開始したワークフロートリガー数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Logic Apps 完了トリガー数

  説明 Logic Appsで完了したワークフロートリガー数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたLogic Appsで完了したワークフロートリガー数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Logic Apps 成功トリガー数

  説明 Logic Appsで成功したワークフロートリガー数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたLogic Appsで成功したワークフロートリガー数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Logic Apps 失敗トリガー数

  説明 Logic Appsで失敗したワークフロートリガー数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたLogic Appsで失敗したワークフロートリガー数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Logic Apps スキップトリガー数

  説明 Logic Appsでスキップされたワークフロートリガー数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたLogic Appsでスキップされたワークフロートリガー数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Logic Apps 起動されたトリガー数

  説明 Logic Appsで起動されたワークフロートリガー数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたLogic Appsで起動されたワークフロートリガー数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Logic Apps トリガースロットルイベント数

  説明 Logic Appsでワークフロートリガーのスロットルイベント数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたLogic Appsでワークフロートリガーのスロットルイベント数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Search 検索待機時間(秒)

  説明 検索サービスが検索クエリを処理するために必要とした時間を監視します。取得データは検査間隔の平均値となります。

  判定条件 取得された検索サービスが検索クエリを処理するために必要とした時間が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は秒です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Search 検索クエリ数(/秒)

  説明 検索サービスで1秒間に受信した検索クエリの数を監視します。取得データは検査間隔の平均値となります。

  判定条件 取得された検索サービスで1秒間に受信した検索クエリの数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は/秒です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Search スロットルされた検索クエリの割合(%)

  説明 検索サービスでスロットルされた検索クエリの割合を監視します。取得データは検査間隔の平均値となります。

  判定条件 取得された検索サービスでスロットルされた検索クエリの割合が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は%です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:SQL Database CPU使用率(%)

  説明 DatabaseのCPU使用率を監視します。取得データは検査間隔の平均値となります。

  判定条件 取得されたDatabaseのCPU使用率が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は%です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:SQL Database データIOの割合(%)

  説明 DatabaseのすべてのIOに対するデータIOの割合を監視します。取得データは検査間隔の平均値となります。

  判定条件 取得されたDatabaseのすべてのIOに対するデータIOの割合が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は%です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:SQL Database ログIOの割合(%)

  説明 DatabaseのすべてのIOに対するログIOの割合を監視します。取得データは検査間隔の平均値となります。

  判定条件 取得されたDatabaseのすべてのIOに対するログIOの割合が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は%です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:SQL Database 接続成功数

  説明 Databaseへの接続に成功した回数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたDatabaseへの接続に成功した回数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:SQL Database 接続失敗数

  説明 Databaseへの接続に失敗した回数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたDatabaseへの接続に失敗した回数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:SQL Database ファイアウォールブロック数

  説明 Databaseでファイアウォールによってブロックされた回数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたDatabaseでファイアウォールによってブロックされた回数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:SQL Database デッドロック数

  説明 Databaseのデッドロック数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたDatabaseのデッドロック数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:SQL Database インメモリOLTPストレージの使用率(%)

  説明 Databaseでのインメモリ OLTPストレージの使用率を監視します。取得データは検査間隔の平均値となります。

  判定条件 取得されたDatabaseでのインメモリOLTPストレージの使用率が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は%です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:SQL Database ワーカー使用率(%)

  説明 Databaseの最大同時実行ワーカー数に対する実行ワーカー数の割合を監視します。取得データは検査間隔の平均値となります。

  判定条件 取得されたDatabaseの最大同時実行ワーカー数に対する実行ワーカー数の割合が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は%です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:SQL Database セッション使用率(%)

  説明 Databaseの最大同時セッション数に対するセッション数の割合を監視します。取得データは検査間隔の平均値となります。

  判定条件 取得されたDatabaseの最大同時セッション数に対するセッション数の割合が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は%です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:SQL Database DWU使用率(%)

  説明 Databaseで割り当てられたDWU(Data Warehouse Unit)の使用率を監視します。取得データは検査間隔の最大値となります。

  判定条件 取得されたDatabaseで割り当てられたDWU(Data Warehouse Unit)の使用率が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は%です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:SQL Database 使用済みDWU数

  説明 Databaseの使用済みDWU(Data Warehouse Unit)数を監視します。取得データは検査間隔の最大値となります。

  判定条件 取得されたDatabaseの使用済みDWU(Data Warehouse Unit)数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:SQL Elastic Pools ストレージの上限値(MB)

  説明 Elastic Poolsのストレージの上限値を監視します。取得データは検査間隔の平均値となります。

  判定条件 取得されたElastic Poolsのストレージの上限値が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はMBです。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:SQL Elastic Pools 使用済みストレージ(KB)

  説明 Elastic Poolsの使用済みストレージを監視します。取得データは検査間隔の平均値となります。

  判定条件 取得されたElastic Poolsの使用済みストレージが異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はMBです。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:SQL Elastic Pools CPU使用率(%)

  説明 Elastic PoolsのCPU使用率を監視します。取得データは検査間隔の平均値となります。

  判定条件 取得されたElastic PoolsのCPU使用率が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は%です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:SQL Elastic Pools データIOの割合(%)

  説明 Elastic PoolsのすべてのIOに対するデータIOの割合を監視します。取得データは検査間隔の平均値となります。

  判定条件 取得されたElastic PoolsのすべてのIOが異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は%です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:SQL Elastic Pools ログIOの割合(%)

  説明 Elastic PoolsのすべてのIOに対するログIOの割合を監視します。取得データは検査間隔の平均値となります。

  判定条件 取得されたElastic PoolsのすべてのIOに対するログIOの割合が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は%です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:SQL Elastic Pools ワーカー使用率(%)

  説明 Elastic Poolsの最大同時実行ワーカー数に対する実行ワーカー数の割合を監視します。取得データは検査間隔の平均値となります。

  判定条件 取得されたElastic Poolsの最大同時実行ワーカー数に対する実行ワーカー数の割合が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は%です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:SQL Elastic Pools セッション使用率(%)

  説明 Elastic Poolsの最大同時セッション数に対するセッション数の割合を監視します。取得データは検査間隔の平均値となります。

  判定条件 取得されたElastic Poolsの最大同時セッション数に対するセッション数の割合が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は%です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:SQL Managed Instance IO要求数

  説明 Managed InstanceのIO要求数を監視します。

  判定条件 取得されたManaged InstanceのIO要求数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Stream Analytics SU使用率(%)

  説明 Stream Analyticsのストリーミングユニット使用率を監視します。取得データは検査間隔の最大値となります。

  判定条件 取得されたStream Analyticsのストリーミングユニット使用率が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は%です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Stream Analytics 入力イベント数

  説明 Stream Analyticsへの入力イベント数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたStream Analyticsへの入力イベント数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Stream Analytics 入力イベントバイト数(KB)

  説明 Stream Analyticsへの入力イベントのデータ量を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたStream Analyticsへの入力イベントのデータ量が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はKBです。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Stream Analytics 入力イベント遅延数

  説明 Stream Analyticsへの遅延入力イベント数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたtream Analyticsへの遅延入力イベント数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Stream Analytics 出力イベント数

  説明 Stream Analyticsの出力イベント数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたStream Analyticsの出力イベント数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Stream Analytics データ変換エラー数

  説明 Stream Analyticsでのデータ変換エラー数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたStream Analyticsでのデータ変換エラー数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Stream Analytics 実行時エラー数

  説明 Stream Analyticsでアプリケーションのタスク実行時のエラー数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたStream Analyticsでアプリケーションのタスク実行時のエラー数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Stream Analytics 順不同のイベント数

  説明 Stream Analyticsに送信されたのと異なる順序で届いたイベント数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたStream Analyticsに送信されたのと異なる順序で届いたイベント数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:App Service プラン CPU使用率(%)

  説明 App Serviceプラン全体のCPU使用率を監視します。取得データは検査間隔の平均値となります。

  判定条件 取得されたApp Serviceプラン全体のCPU使用率が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は%です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:App Service プラン メモリ使用率(%)

  説明 App Serviceプラン全体のメモリ使用率を監視します。取得データは検査間隔の平均値となります。

  判定条件 取得されたApp Serviceプラン全体のメモリ使用率が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は%です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:App Service プラン ディスクキュー

  説明 App Serviceプランのストレージのキューに登録された読み取り要求と書き込み要求の数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたpp Serviceプランのストレージのキューに登録された読み取り要求と書き込み要求の数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:App Service プラン HTTPキュー

  説明 App Serviceプランの処理される前にキューで待つ必要があったHTTP要求の数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたApp Serviceプランの処理される前にキューで待つ必要があったHTTP要求の数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:App Service プラン 受信データバイト数(KB)

  説明 App Serviceプラン全体の受信データ量を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたApp Serviceプラン全体の受信データ量が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はKBです。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:App Service プラン 送信データバイト数(KB)

  説明 App Serviceプラン全体の送信データ量を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたApp Serviceプラン全体の送信データ量が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はKBです。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Web App CPU時間(秒)

  説明 Web Appで使用したCPU時間を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたWeb Appで使用したCPU時間が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は秒です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Web App HTTPリクエスト数

  説明 Web Appが受け付けた要求の合計数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたWeb Appが受け付けた要求の合計数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Web App 受信データバイト数(KB)

  説明 Web Appの受信データ量を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたWeb Appの受信データ量が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はKBです。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Web App 送信データバイト数(KB)

  説明 Web Appの送信データ量を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたWeb Appの送信データ量が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はKBです。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Web App Http2xx 発生数

  説明 Web Appで200以上300未満のHTTP状態コードを返した要求の数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたWeb Appで200以上300未満のHTTP状態コードを返した要求の数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Web App Http3xx 発生数

  説明 Web Appで300以上400未満のHTTP状態コードを返した要求の数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたWeb Appで300以上400未満のHTTP状態コードを返した要求の数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Web App Http401 発生数

  説明 Web AppでHTTP状態コード401を返した要求の数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたWeb AppでHTTP状態コード401を返した要求の数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Web App Http403 発生数

  説明 Web AppでHTTP状態コード403を返した要求の数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたWeb AppでHTTP状態コード403を返した要求の数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Web App Http404 発生数

  説明 Web AppでHTTP状態コード404を返した要求の数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたWeb AppでHTTP状態コード404を返した要求の数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Web App Http406 発生数

  説明 Web AppでHTTP状態コード406を返した要求の数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたWeb AppでHTTP状態コード406を返した要求の数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Web App Http4xx 発生数

  説明 Web Appで400以上500未満のHTTP状態コードを返した要求の数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたWeb Appで400以上500未満のHTTP状態コードを返した要求の数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Web App Http5xx 発生数

  説明 Web Appで500以上600未満のHTTP状態コードが返した要求の数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたWeb Appで500以上600未満のHTTP状態コードが返した要求の数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Web App メモリワーキングセット(MB)

  説明 Web Appの現在のメモリ使用量を監視します。取得データは瞬間値となります。

  判定条件 取得されたWeb Appの現在のメモリ使用量が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はMBです。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Web App 平均メモリワーキングセット(MB)

  説明 Web Appの平均メモリ使用量を監視します。取得データは検査間隔の平均値となります。

  判定条件 取得されたWeb Appの平均メモリ使用量が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はMBです。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Web App 平均応答時間(秒)

  説明 Web Appが要求に応答するのに要した時間を監視します。取得データは検査間隔の平均値となります。

  判定条件 取得されたWeb Appが要求に応答するのに要した時間が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は秒です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Web App 関数の実行単位

  説明 関数の実行単位を監視します。

  判定条件 取得された関数の実行単位が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Web App 関数の実行回数

  説明 関数の実行回数を監視します。

  判定条件 取得された関数の実行回数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Web App デプロイメント スロット CPU時間(秒)

  説明 デプロイメントスロットのアプリで使用したCPU時間を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたデプロイメントスロットのアプリで使用したCPU時間が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は秒です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Web App デプロイメント スロット 要求数

  説明 デプロイメントスロットのアプリが受け付けた要求の合計数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたデプロイメントスロットのアプリが受け付けた要求の合計数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Web App デプロイメント スロット 受信データバイト数(KB)

  説明 デプロイメントスロットのアプリの受信データ量を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたデプロイメントスロットのアプリの受信データ量が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はKBです。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Web App デプロイメント スロット 送信データバイト数(KB)

  説明 デプロイメントスロットのアプリの送信データ量を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたデプロイメントスロットのアプリの送信データ量が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はKBです。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Web App デプロイメント スロット Http2xx 発生数

  説明 デプロイメントスロットのアプリで200以上300未満のHTTP状態コードを返した要求の数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたデプロイメントスロットのアプリで200以上300未満のHTTP状態コードを返した要求の数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Web App デプロイメント スロット Http3xx 発生数

  説明 デプロイメントスロットのアプリで300以上400未満のHTTP状態コードを返した要求の数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたデプロイメントスロットのアプリで300以上400未満のHTTP状態コードを返した要求の数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Web App デプロイメント スロット Http401 発生数

  説明 デプロイメントスロットのアプリでHTTP状態コード401を返した要求の数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたデプロイメントスロットのアプリでHTTP状態コード401を返した要求の数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Web App デプロイメント スロット Http403 発生数

  説明 デプロイメントスロットのアプリでHTTP状態コード403を返した要求の数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたデプロイメントスロットのアプリでHTTP状態コード403を返した要求の数が異常しきい値より大きい場合に異常と

みなします。異常・警告しきい値には数値のみ入力可能です。

パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Web App デプロイメント スロット Http404 発生数

  説明 デプロイメントスロットのアプリでHTTP状態コード404を返した要求の数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたデプロイメントスロットのアプリでHTTP状態コード404を返した要求の数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Web App デプロイメント スロット Http406 発生数

  説明 デプロイメントスロットのアプリでHTTP状態コード406を返した要求の数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたデプロイメントスロットのアプリでHTTP状態コード406を返した要求の数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Web App デプロイメント スロット Http4xx 発生数

  説明 デプロイメントスロットのアプリで400以上500未満のHTTP状態コードを返した要求の数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたデプロイメントスロットのアプリで400以上500未満のHTTP状態コードを返した要求の数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Web App デプロイメント スロット Http5xx 発生数

  説明 デプロイメントスロットのアプリで500以上600未満のHTTP状態コードが返した要求の数を監視します。取得データは検査間隔の

合計値となります。

判定条件 取得されたデプロイメントスロットのアプリで500以上600未満のHTTP状態コードが返した要求の数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式：A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure：Web App デプロイメント スロット メモリワーキングセット(MB)

  説明 デプロイメントスロットのアプリの現在のメモリ使用量を監視します。取得データは瞬間値となります。

  判定条件 取得されたデプロイメントスロットのアプリの現在のメモリ使用量が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はMBです。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式：A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure：Web App デプロイメント スロット 平均メモリワーキングセット(MB)

  説明 デプロイメントスロットのアプリの平均メモリ使用量を監視します。取得データは検査間隔の平均値となります。

  判定条件 取得されたデプロイメントスロットのアプリの平均メモリ使用量が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はMBです。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式：A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure：Web App デプロイメント スロット 平均応答時間(秒)

  説明 デプロイメントスロットのアプリが要求に応答するのに要した時間を監視します。取得データは検査間隔の平均値となります。

  判定条件 取得されたデプロイメントスロットのアプリが要求に応答するのに要した時間が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は秒です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式：A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure：Log Analytics ログ情報取得[イベントログ]

  説明 Log Analyticsのログ情報[イベントログ]を監視します。取得ログ情報は監視実行ノード上にログファイルとして保存します。

判定条件 ログ情報取得が異常終了した場合、異常となります。ログの件数が多く、ログを取得し切れなかった場合、警告となります。値は変更しないで下さい。

パラメータ

パラメータ名	説明
リソースグループ名	ワークスペースが所属するリソースグループ名を指定します。省略不可です。
ワークスペース名	ワークスペース名を指定します。省略不可です。
クエリ	ログ情報取得するクエリ(※4)(※5)を指定します。省略不可です。
識別子	収集したログ情報の出力先ログファイル名に使用する識別子を指定します。任意の文字列が指定可能です。省略不
サブスクリプションID	サブスクリプションIDを指定します。省略不可です。
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し
ログ出力ファイル	収集したログ情報の出力先ログファイルを指定することが可能です。絶対パスでログ出力ファイル名を指定して下さい。
ログフォーマット	取得したログの出力フォーマットをLTSVもしくはJSONに切り替えます。デフォルト値はLTSVとなります。省略可能です

備考 Azure Log Analytics連携機能については、Azure Log Analytics連携機能 を参照して下さい。

※4 クエリを指定する際に、「｜」などの記号や「スペース」を含む場合は、「"」で囲む必要があります。また、「"」を含む場合は、「\」でエスケープする必要があります。
例: "Event | where EventLevelName == \"Information\""
クエリの記述方法は下記Microsoftのサイトをご参照下さい。
参考URL:https://docs.microsoft.com/ja-jp/azure/azure-monitor/log-query/log-query-overview (2019年8月現在)
※5 クエリにはイベントログ以外のテーブルも指定可能です。

注釈

Azure:Log Analytics ログ情報取得では、最後に取得したログのタイムスタンプよりlogBufferTimeに指定した分数遡ってログを取得します。監視タスクの新規作成時などの最後に取得したログが無い場合は「監視間隔＋logBufferTime＋5分」以内に発生したログを取得します。
Azure Log Analytics では、発生したログが Azure Log Analytics 上に現れるまでに時間がかかる場合があります。その時間が監視間隔以上かかる場合、ログが取得されない状態となります。このような場合は、logBufferTimeを適切に設定して下さい。

- Azure:Log Analytics ログ情報取得[SYSLOG]

  説明 Log Analyticsのログ情報[SYSLOG]を監視します。取得ログ情報は監視実行ノード上にログファイルとして保存します。

  判定条件 ログ情報取得が異常終了した場合、異常となります。ログの件数が多く、ログを取得し切れなかった場合、警告となります。値は変更しないで下さい。

  パラメータ

パラメータ名	説明
リソースグループ名	ワークスペースが所属するリソースグループ名を指定します。省略不可です。
ワークスペース名	ワークスペース名を指定します。省略不可です。
クエリ	ログ情報取得するクエリ(※4)(※5)を指定します。省略不可です。
識別子	収集したログ情報の出力先ログファイル名に使用する識別子を指定します。任意の文字列が指定可能です。省略不
サブスクリプションID	サブスクリプションIDを指定します。省略不可です。
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し
ログ出力ファイル	収集したログ情報の出力先ログファイルを指定することが可能です。絶対パスでログ出力ファイル名を指定して下さい。
ログフォーマット	取得したログの出力フォーマットをLTSVもしくはJSONに切り替えます。デフォルト値はLTSVとなります。省略可能です

  備考 Azure Log Analytics連携機能については、Azure Log Analytics連携機能 を参照して下さい。

  ※4 クエリを指定する際に、「｜」などの記号や「スペース」を含む場合は、「"」で囲む必要があります。また「"」を含む場合は、「\」でエスケープする必要があります。
  例: "Syslog | where Facility == \"authpriv\""
  クエリの記述方法は下記Microsoftのサイトをご参照下さい。
  参考URL:https://docs.microsoft.com/ja-jp/azure/azure-monitor/log-query/log-query-overview (2019年8月現在)
  ※5 クエリにはSYSLOG以外のテーブルも指定可能です。

  注釈

  Azure:Log Analytics ログ情報取得では、最後に取得したログのタイムスタンプよりlogBufferTimeに指定した分数遡ってログ

を取得します。監視タスクの新規作成時などの最後に取得したログが無い場合は「監視間隔＋logBufferTime＋5分」以内に発生したログを取得します。
Azure Log Analytics では、発生したログが Azure Log Analytics 上に現れるまでに時間がかかる場合があります。その時間が監視間隔以上かかる場合、ログが取得されない状態となります。このような場合は、logBufferTimeを適切に設定して下さい。

- Azure：Log Analytics ログ情報取得[AzureActivity]

  説明 Log Analyticsのログ情報[AzureActivity]を監視します。取得ログ情報は監視実行ノード上にログファイルとして保存します。

  判定条件 ログ情報取得が異常終了した場合、異常となります。ログの件数が多く、ログを取得し切れなかった場合、警告となります。値は変更しないで下さい。

  パラメータ

パラメータ名	説明
リソースグループ名	ワークスペースが所属するリソースグループ名を指定します。省略不可です。
ワークスペース名	ワークスペース名を指定します。省略不可です。
クエリ	ログ情報取得するクエリ（※4）（※5）を指定します。省略不可です。
識別子	収集したログ情報の出力先ログファイル名に使用する識別子を指定します。任意の文字列が指定可能です。省略不
サブスクリプションID	サブスクリプションIDを指定します。省略不可です。
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し
ログ出力ファイル	収集したログ情報の出力先ログファイルを指定することが可能です。絶対パスでログ出力ファイル名を指定して下さい。
ログフォーマット	取得したログの出力フォーマットをLTSVもしくはJSONに切り替えます。デフォルト値はLTSVとなります。省略可能です

  備考 Azure Log Analytics連携機能については、Azure Log Analytics連携機能 を参照して下さい。

  ※4　クエリを指定する際に、「｜」などの記号や「スペース」を含む場合は、「"」で囲む必要があります。また、「"」を含む場合は、「\」でエスケープする必要があります。
  例：　"AzureActivity | where Level == \"Informational\""
  クエリの記述方法は下記Microsoftのサイトをご参照下さい。
  参考URL：https://docs.microsoft.com/ja-jp/azure/azure-monitor/log-query/log-query-overview　(2019年8月現在)
  ※5　クエリにはAzureActivity以外のテーブルも指定可能です。

注釈

Azure：Log Analytics ログ情報取得では、最後に取得したログのタイムスタンプよりlogBufferTimeに指定した分数遡ってログを取得します。監視タスクの新規作成時などの最後に取得したログが無い場合は「監視間隔＋logBufferTime＋5分」以内に発生したログを取得します。
Azure Log Analytics では、発生したログが Azure Log Analytics 上に現れるまでに時間がかかる場合があります。その時間が監視間隔以上かかる場合、ログが取得されない状態となります。このような場合は、logBufferTimeを適切に設定して下さい。

- Azure：利用料金（当月）

  説明 当月分の利用料金を監視します。取得データは瞬間値となります。

  判定条件 取得された当月分の利用料金が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
先月/当月フラグ(P/T)	利用料金の取得範囲を先月(P)か当月(T)か切り替えます。デフォルト値は当月(T)となります。省略不可です。
リソースグループ名	特定のリソースグループの利用料金を監視したい場合に指定します。省略可です。省略した場合はすべてのリソー
タグ	タグ付けされたリソースの利用料金だけ取得したい場合に指定します。【タグ名:タグ値】の形式で指定して下さい。省
課金情報集計モード	取得した全リソースグループの利用料金の合計値で監視する場合に"TOTAL"を指定して下さい。省略可です。
サブスクリプションID	サブスクリプションIDを指定します。省略不可です。
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定

注釈

監視タスクに対するタグの指定は、リソースへタグ付けを行った翌日から有効となります。

注釈

Azureユーザー情報設定ファイルのclosingDateに"01"を指定することで、毎月1日の監視結果には前月1日から当日までの料金が報告され、毎月2日から月末までは当月1日から当日までの料金が報告されます。

- Azure：利用料金（昨日）

  説明 昨日分の利用料金を監視します。取得データは瞬間値となります。

  判定条件 取得された昨日分の利用料金が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	特定のリソースグループの利用料金を監視したい場合に指定します。省略可です。省略した場合はすべてのリソース
タグ	タグ付けされたリソースの利用料金だけ取得したい場合に指定します。"タグ名:タグ値"の形式で指定して下さい。省
課金情報集計モード	取得した全リソースグループの利用料金の合計値で監視する場合に"TOTAL"を指定して下さい。省略可です。
サブスクリプションID	サブスクリプションIDを指定します。省略不可です。
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定

注釈

監視タスクに対するタグの指定は、リソースへタグ付けを行った翌日から有効となります。

- Azure：API Management ゲートウェイ要求合計数

  説明 ゲートウェイ要求の数を監視します。

  判定条件 取得されたAPI Management ゲートウェイ要求合計数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式：A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure：Container Instances CPU 使用率

  説明 すべてのコアの CPU 使用率を監視します (ミリコア単位)。

  判定条件 取得されたContainer Instances CPU 使用率が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式：A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure：Container Instances メモリ使用量

  説明 合計メモリ使用量を監視します (バイト単位)。

  判定条件 取得されたContainer Instances メモリ使用量が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はBytesです。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Container Service 準備完了状態ポッド数

  説明 準備完了状態のポッドの数を監視します。

  判定条件 取得された準備完了状態ポッド数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Azure Database for PostgreSQL ストレージ割合

  説明 ストレージの割合を監視します。

  判定条件 取得されたストレージ使用率が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は%です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Azure Cosmos DB 要求合計数

  説明 行われた要求の数を監視します。

  判定条件 取得されたAzure Cosmos DBへ要求数のが異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Load balancers VIP 可用性

  説明 プローブの結果に基づく、VIP エンドポイントの可用性を監視します。

  判定条件 取得されたVIP エンドポイントの可用性が異常しきい値より小さい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Public IP DDoS 受信パケット数

  説明 DDoS 受信パケット数を監視します。

  判定条件 取得されたDDoS 受信パケット数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:ExpressRoute circuits 受信ビット数/秒

  説明 1 秒あたりの Azure へのイングレス ビット数を監視します。

  判定条件 取得された 1 秒あたりの Azure へのイングレス ビット数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は/秒です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:ExpressRoute circuits 送信ビット数/秒

  説明 1 秒あたりの Azure からのエグレス ビット数を監視します。

  判定条件 取得された 1 秒あたりの Azure からのエグレス ビット数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は/秒です。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Storage accounts blob イングレス データ量

  説明 イングレス データの量を監視します (バイト単位)。この値には、外部クライアントから Azure Storage へのイングレスおよび Azure 内でのイングレスが含まれます。

  判定条件 取得されたイングレス データ量が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はBytesです。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名として、<ストレージ名>/defaultのように、ストレージ名に続けて「/default」を付けて指定します。省
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:Storage accounts blob エグレス データ量

  説明 エグレス データの量を監視します (バイト単位)。この値には、外部クライアントから Azure Storage へのエグレスおよび Azure 内でのエグレスが含まれます。そのため、この値は課金対象のエグレスを反映しません。

  判定条件 取得されたエグレス データ量が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はBytesです。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名として、<ストレージ名>/defaultのように、ストレージ名に続けて「/default」を付けて指定します。省
リソースタイプ	リソースタイプを指定します。固定値です。変更は出来ません。
フィルター	ディメンションを指定します。省略可能です。(形式:A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し

- Azure:利用料金(EA)

  説明 マイクロソフトエンタープライズ契約(EA)での利用料金を監視します。取得データは瞬間値となります。

  判定条件 取得された利用料金が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
Billing/Usageフラグ(B/U)	固定値の利用料金(B)となります。変更は出来ません。
先月/当月フラグ(P/T)	利用料金の取得範囲を先月(P)か当月(T)か切り替えます。デフォルト値は当月(T)となります。省略不可です。
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を

- Azure:リソース使用量(EA)

  説明 マイクロソフトエンタープライズ契約(EA)でのリソース使用量を監視します。取得データは瞬間値となります。

  判定条件 取得されたリソース使用量が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
Billing/Usageフラグ(B/U)	固定値のリソース使用量(U)となります。変更は出来ません。
先月/当月フラグ(P/T)	利用料金の取得範囲を先月(P)か当月(T)か切り替えます。デフォルト値は当月(T)となります。省略不可です。
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を

- Azure:メトリクス監視

  説明 指定したメトリクスの情報を取得します

  判定条件 「計算式の変数の値」で指定した「リソースタイプ:メトリック」から取得したメトリクス値の判定条件を指定して下さい。

  パラメータ

パラメータ名	説明
リソースグループ名	監視するリソースが所属するリソースグループ名を指定します。省略不可です。
リソース名	監視するリソース名を指定します。省略不可です。
フィルター	ディメンションを指定します。省略可能です。(形式：A eq 'a1'、A eq 'a1' and(or) B eq 'b1')
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し
APIバージョン	監視するリソースタイプのリソースプロバイダーがサポートするAPIバージョンを指定します（例：2020-02-02）。省略した場
ゼロパブリッシュ	検査間隔内にデータポイントが無かった場合に取得データの値を「0」とする場合にONを指定します。省略可能です。省

注釈

APIバージョンの自動判別が行えない場合は、Azure ポータルのリソースエクスプローラーでリソースプロバイダーがサポートするAPIバージョンを確認しパラメータに設定して下さい。

- Azure：Service Health情報取得

  説明 Service Health情報を監視します。取得データは成否となります。

  判定条件 Service Health情報に失敗した場合、異常となります。異常・警告しきい値は変更しないで下さい。

  パラメータ

パラメータ名	説明
サブスクリプションID	サブスクリプションIDを指定します。省略不可です。
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指定し
モード	モードを指定します。省略可能です。更新日時(update)、作成日時(create)かを切り替えます。デフォルト値は更新日
ログフォーマット	取得したログの出力フォーマットをLTSVもしくはJSONに切り替えます。デフォルト値はLTSVとなります。省略可能です
ログ出力ファイル	収集したログ情報の出力先ログファイルを指定することが可能です。絶対パスでログ出力ファイル名を指定して下さい。

注釈

Azure：Service Health情報取得では、最後に取得したログのタイムスタンプよりlogBufferTimeに指定した分数遡ってログを取得します。監視タスクの新規作成時などの最後に取得したログが無い場合は過去6ヶ月に発生したログを取得します。

- Azure：DataExplorer ログ情報取得

  説明 Data Explorerのログ情報を監視します。取得ログ情報は監視実行ノード上にログファイルとして保存します。

  判定条件 ログ情報取得が異常終了した場合、異常となります。ログの件数が多く、ログを取得し切れなかった場合、警告となります。値は変更しないで下さい。

  パラメータ

パラメータ名	説明
認証ファイル	Azureユーザー情報設定ファイルを指定することが可能です。絶対パスでAzureユーザー情報設定ファイル名を指
ログ出力ファイル	収集したログ情報の出力先ログファイルを指定することが可能です。絶対パスでログ出力ファイル名を指定して下さ
エンドポイント	作成したクラスターのURIで、フォーマットの「https://クラスター名.リージョン.kusto.windows.net」を指定します。
データベース名	データベース名を指定します。省略不可です。
テーブル名	テーブル名を指定します。省略不可です。
タイムスタンプカラム名	タイムスタンプカラム名を指定します。省略不可です。
タイムパーティション名	タイムパーティション名を指定します。タイムパーティション範囲を指定するときは、タイムパーティション名は省略不可
タイムパーティション範囲	タイムパーティション範囲を指定します。タイムパーティション名を指定するときは、タイムパーティション範囲は省略不
ワークスペースカラム名	ワークスペースカラム名を指定します。ワークスペース名を指定するときは、ワークスペースカラム名は省略不可です
ワークスペース名	ワークスペース名を指定します。ワークスペースカラム名を指定するときは、ワークスペース名は省略不可です。
クエリ	ログ情報取得するクエリ(※1)(※2)(※3)を指定します。省略可能です。

  備考 Azure Data Explorer連携機能については、Azure Data Explorer連携機能 を参照して下さい。

  ※1　テーブル名に「"」を含む場合は、「\」でエスケープする必要があります。
  　例：external_table(\"abcTable\")
  ※2　テーブル名を自動的にクエリに追加するため、クエリパラメータでのテーブル名指定は不要です。
  　OK例：| search Timestamp >= datetime(2022-06-11 23:05:01.917)
  　NG例：testTable | search Timestamp >= datetime(2022-06-11 23:05:01.917)

指定方法の詳細は右のウェブサイトに参照してください。https://docs.microsoft.com/ja-jp/azure/data-explorer/kql-quick-reference(2022年8月現在)
※3　また、タイムスタンプを必ず先頭の項目とするため、「| project-reorder {tsColName}」を自動的にクエリに追加しています。

注釈

Azure：DataExplorerログ情報取得では、最後に取得したログのタイムスタンプよりlogBufferTimeに指定した分数遡ってログを取得します。監視タスクの新規作成時などの最後に取得したログが無い場合は「監視間隔＋logBufferTime＋5分」以内に発生したログを取得します。
Azure Data Explorer では、発生したログが Azure Data Explorer 上に現れるまでに時間がかかる場合があります。その時間が監視間隔以上かかる場合、ログが取得されない状態となります。このような場合は、logBufferTimeを適切に設定して下さい。

2.8.1.3. Google Cloud監視

注釈

監視項目によっては、監視間隔を15分未満に設定すると値が取得できないことがあります。その場合は監視間隔を15分以上に設定して下さい。

参考

各種パラメータの設定値が分からない場合は、Google Cloudより提供されているMetrics Explorerにて確認して下さい。
参考URL：https://console.cloud.google.com/monitoring (2020年4月現在)

- GCP：App Engine インスタンス数

  説明 App Engine の存在するインスタンスの数を監視します。取得データは検査間隔期間内の最大値となります。

  判定条件 取得されたApp Engine のインスタンス数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースタイプ	監視するリソースタイプです。固定値です。省略不可です。
メトリクスラベル	監視対象をフィルタする条件としてメトリクスラベルのstateを指定することが可能です。【項目名=値】で条件を指定し
リソースラベル	監視対象をフィルタする条件としてリソースラベルのzone、module_id、version_idを指定することが可能です。【項目
グループ名	監視対象をフィルタする条件としてStackdriverのグループ名を指定することが可能です。省略可能です。
ユーザーラベル	監視対象をフィルタする条件としてユーザーラベルを指定することが可能です。【ユーザーラベル名=値】の形式で指定
システムラベル	監視対象をフィルタする条件としてシステムラベルを指定することが可能です。【システムラベル名=値】の形式で指定し
タグ	監視対象をフィルタする条件としてタグを指定することが可能です。【タグ名=値】の形式で指定して下さい。省略可能
認証ファイル	サービスアカウントのAPIキーを指定することが可能です。絶対パスでAPIキー認証ファイル名を指定して下さい。省略
出力メトリクスラベル	監視結果の監視対象として表示するメトリクスラベルを指定します。省略可能です。
出力リソースラベル	監視結果の監視対象として表示するリソースラベルを指定します。省略可能です。

- GCP：BigQuery クエリ数

  説明 BigQuery の実行中のクエリの数を監視します。取得データは検査間隔期間内の最大値となります。

  判定条件 取得されたBigQuery の実行中のクエリ数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースタイプ	監視するリソースタイプです。固定値です。省略不可です。
メトリクスラベル	監視対象をフィルタする条件としてメトリクスラベルのpriorityを指定することが可能です。【項目名=値】で条件を指定
リソースラベル	監視対象をフィルタする条件としてリソースラベルを指定することが可能です。【項目名=値】で条件を指定して下さい。
グループ名	監視対象をフィルタする条件としてStackdriverのグループ名を指定することが可能です。省略可能です。
ユーザーラベル	監視対象をフィルタする条件としてユーザーラベルを指定することが可能です。【ユーザーラベル名=値】の形式で指定
システムラベル	監視対象をフィルタする条件としてシステムラベルを指定することが可能です。【システムラベル名=値】の形式で指定し
タグ	監視対象をフィルタする条件としてタグを指定することが可能です。【タグ名=値】の形式で指定して下さい。省略可能
認証ファイル	サービスアカウントのAPIキーを指定することが可能です。絶対パスでAPIキー認証ファイル名を指定して下さい。省略
出力メトリクスラベル	監視結果の監視対象として表示するメトリクスラベルを指定します。省略可能です。
出力リソースラベル	監視結果の監視対象として表示するリソースラベルを指定します。省略可能です。

- GCP：Cloud Functions 関数実行回数

  説明 Cloud Functions のステータス別の関数実行回数を監視します。取得データは検査間隔期間内の合計値となります。

  判定条件 取得されたCloud Functions のステータス別の関数実行回数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースタイプ	監視するリソースタイプです。固定値です。省略不可です。
メトリクスラベル	監視対象をフィルタする条件としてメトリクスラベルのmemory、status、trigger_typeを指定することが可能です。【項
リソースラベル	監視対象をフィルタする条件としてリソースラベルのfunction_name、regionを指定することが可能です。【項目名=値
グループ名	監視対象をフィルタする条件としてStackdriverのグループ名を指定することが可能です。省略可能です。
ユーザーラベル	監視対象をフィルタする条件としてユーザーラベルを指定することが可能です。【ユーザーラベル名=値】の形式で指定
システムラベル	監視対象をフィルタする条件としてシステムラベルを指定することが可能です。【システムラベル名=値】の形式で指定し
タグ	監視対象をフィルタする条件としてタグを指定することが可能です。【タグ名=値】の形式で指定して下さい。省略可能
認証ファイル	サービスアカウントのAPIキーを指定することが可能です。絶対パスでAPIキー認証ファイル名を指定して下さい。省略
出力メトリクスラベル	監視結果の監視対象として表示するメトリクスラベルを指定します。省略可能です。
出力リソースラベル	監視結果の監視対象として表示するリソースラベルを指定します。省略可能です。

- GCP：Cloud Functions 関数実行時間(ナノ秒)

  説明 Cloud Functions のステータス別の関数実行時間を監視します。取得データは監視間隔内の99パーセンタイルの実行時間となります。

  判定条件 取得されたCloud Functions のステータス別の関数実行時間が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はナノ秒です。

  パラメータ

パラメータ名	説明
リソースタイプ	監視するリソースタイプです。固定値です。省略不可です。
メトリクスラベル	監視対象をフィルタする条件としてメトリクスラベルのmemory、status、trigger_typeを指定することが可能です。【項
リソースラベル	監視対象をフィルタする条件としてリソースラベルのfunction_name、regionを指定することが可能です。【項目名=値
グループ名	監視対象をフィルタする条件としてStackdriverのグループ名を指定することが可能です。省略可能です。
ユーザーラベル	監視対象をフィルタする条件としてユーザーラベルを指定することが可能です。【ユーザーラベル名=値】の形式で指定
システムラベル	監視対象をフィルタする条件としてシステムラベルを指定することが可能です。【システムラベル名=値】の形式で指定し
タグ	監視対象をフィルタする条件としてタグを指定することが可能です。【タグ名=値】の形式で指定して下さい。省略可能
認証ファイル	サービスアカウントのAPIキーを指定することが可能です。絶対パスでAPIキー認証ファイル名を指定して下さい。省略
出力メトリクスラベル	監視結果の監視対象として表示するメトリクスラベルを指定します。省略可能です。
出力リソースラベル	監視結果の監視対象として表示するリソースラベルを指定します。省略可能です。

- GCP：Cloud SQL インスタンス配信状況

  説明 Cloud SQLインスタンスの現在の配信状況を監視します。取得データは瞬間値となります。

  判定条件 取得されたCloud SQLインスタンスの現在の配信状況がRUNNING、RUNNABLEと異なる場合に異常とみなします。異常・警告しきい値には文字列のみ入力可能です。

パラメータ

パラメータ名	説明
リソースタイプ	監視するリソースタイプです。固定値です。省略不可です。
メトリクスラベル	監視対象をフィルタする条件としてメトリクスラベルを指定することが可能です。【項目名=値】で条件を指定して下さい
リソースラベル	監視対象をフィルタする条件としてリソースラベルのdatabase_id、regionを指定することが可能です。【項目名=値】
グループ名	監視対象をフィルタする条件としてStackdriverのグループ名を指定することが可能です。省略可能です。
ユーザーラベル	監視対象をフィルタする条件としてユーザーラベルを指定することが可能です。【ユーザーラベル名=値】の形式で指定
システムラベル	監視対象をフィルタする条件としてシステムラベルを指定することが可能です。【システムラベル名=値】の形式で指定し
タグ	監視対象をフィルタする条件としてタグを指定することが可能です。【タグ名=値】の形式で指定して下さい。省略可能
認証ファイル	サービスアカウントのAPIキーを指定することが可能です。絶対パスでAPIキー認証ファイル名を指定して下さい。省略
出力メトリクスラベル	監視結果の監視対象として表示するメトリクスラベルを指定します。省略可能です。
出力リソースラベル	監視結果の監視対象として表示するリソースラベルを指定します。省略可能です。

- GCP：Stackdriver Trace 課金対象のトレーススパン

  説明 Stackdriver Trace の課金対象のトレーススパンを監視します。取得データは検査間隔内の合計値となります。

  判定条件 取得されたStackdriver Trace の課金対象のトレーススパンが異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースタイプ	監視するリソースタイプです。固定値です。省略不可です。
メトリクスラベル	監視対象をフィルタする条件としてメトリクスラベルにservice、chargeableを指定することが可能です。【項目名=値】
リソースラベル	監視対象をフィルタする条件としてリソースラベルを指定することが可能です。【項目名=値】で条件を指定して下さい。
グループ名	監視対象をフィルタする条件としてStackdriverのグループ名を指定することが可能です。省略可能です。
ユーザーラベル	監視対象をフィルタする条件としてユーザーラベルを指定することが可能です。【ユーザーラベル名=値】の形式で指定
システムラベル	監視対象をフィルタする条件としてシステムラベルを指定することが可能です。【システムラベル名=値】の形式で指定し
タグ	監視対象をフィルタする条件としてタグを指定することが可能です。【タグ名=値】の形式で指定して下さい。省略可能
認証ファイル	サービスアカウントのAPIキーを指定することが可能です。絶対パスでAPIキー認証ファイル名を指定して下さい。省略
出力メトリクスラベル	監視結果の監視対象として表示するメトリクスラベルを指定します。省略可能です。
出力リソースラベル	監視結果の監視対象として表示するリソースラベルを指定します。省略可能です。

- GCP：Compute Engine CPU使用率(%)

  説明 Compute Engine のCPU使用率を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたCompute Engine のCPU使用率が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は%です。

  パラメータ

パラメータ名	説明
リソースタイプ	監視するリソースタイプです。固定値です。省略不可です。
メトリクスラベル	監視対象をフィルタする条件としてメトリクスラベルにinstance_nameを指定することが可能です。【項目名=値】で条
リソースラベル	監視対象をフィルタする条件としてリソースラベルにinstance_id、zoneを指定することが可能です。【項目名=値】で条
グループ名	監視対象をフィルタする条件としてStackdriverのグループ名を指定することが可能です。省略可能です。
ユーザーラベル	監視対象をフィルタする条件としてユーザーラベルを指定することが可能です。【ユーザーラベル名=値】の形式で指定
システムラベル	監視対象をフィルタする条件としてシステムラベルを指定することが可能です。【システムラベル名=値】の形式で指定し
タグ	監視対象をフィルタする条件としてタグを指定することが可能です。【タグ名=値】の形式で指定して下さい。省略可能
認証ファイル	サービスアカウントのAPIキーを指定することが可能です。絶対パスでAPIキー認証ファイル名を指定して下さい。省略
出力メトリクスラベル	監視結果の監視対象として表示するメトリクスラベルを指定します。省略可能です。
出力リソースラベル	監視結果の監視対象として表示するリソースラベルを指定します。省略可能です。

- GCP：Kubernetes Engine ノード内プロセス数

  説明 Kubernetes Engine ノード内のプロセス数を監視します。取得データは検査間隔期間内の最大値となります。

  判定条件 取得されたKubernetes Engine ノード内のプロセス数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

パラメータ

パラメータ名	説明
リソースタイプ	監視するリソースタイプです。固定値です。省略不可です。
メトリクスラベル	監視対象をフィルタする条件としてメトリクスラベルを指定することが可能です。【項目名=値】で条件を指定して下さい
リソースラベル	監視対象をフィルタする条件としてリソースラベルにlocation、cluster_name、node_nameを指定することが可能です
グループ名	監視対象をフィルタする条件としてStackdriverのグループ名を指定することが可能です。省略可能です。
ユーザーラベル	監視対象をフィルタする条件としてユーザーラベルを指定することが可能です。【ユーザーラベル名=値】の形式で指定
システムラベル	監視対象をフィルタする条件としてシステムラベルを指定することが可能です。【システムラベル名=値】の形式で指定し
タグ	監視対象をフィルタする条件としてタグを指定することが可能です。【タグ名=値】の形式で指定して下さい。省略可能
認証ファイル	サービスアカウントのAPIキーを指定することが可能です。絶対パスでAPIキー認証ファイル名を指定して下さい。省略
出力メトリクスラベル	監視結果の監視対象として表示するメトリクスラベルを指定します。省略可能です。
出力リソースラベル	監視結果の監視対象として表示するリソースラベルを指定します。省略可能です。

- GCP：Cloud Datastore API呼び出し回数

  説明 Cloud Datastore のAPI呼び出し数を監視します。取得データは検査間隔期間内の最大値となります。

  判定条件 取得されたCloud Datastore のAPI呼び出し数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースタイプ	監視するリソースタイプです。固定値です。省略不可です。
メトリクスラベル	監視対象をフィルタする条件としてメトリクスラベルにapi_method、response_codeを指定することが可能です。【項
リソースラベル	監視対象をフィルタする条件としてリソースラベルにmodule_id、version_idを指定することが可能です。【項目名=値
グループ名	監視対象をフィルタする条件としてStackdriverのグループ名を指定することが可能です。省略可能です。
ユーザーラベル	監視対象をフィルタする条件としてユーザーラベルを指定することが可能です。【ユーザーラベル名=値】の形式で指定
システムラベル	監視対象をフィルタする条件としてシステムラベルを指定することが可能です。【システムラベル名=値】の形式で指定し
タグ	監視対象をフィルタする条件としてタグを指定することが可能です。【タグ名=値】の形式で指定して下さい。省略可能
認証ファイル	サービスアカウントのAPIキーを指定することが可能です。絶対パスでAPIキー認証ファイル名を指定して下さい。省略
出力メトリクスラベル	監視結果の監視対象として表示するメトリクスラベルを指定します。省略可能です。
出力リソースラベル	監視結果の監視対象として表示するリソースラベルを指定します。省略可能です。

- GCP：Cloud Datastore 読み込みエンティティのサイズ(Byte)

  説明 タイプごとの読み取りエンティティのサイズを監視します。取得データは監視間隔内の99パーセンタイルの値となります。

  判定条件 取得されたCloud Datastore の読み込みエンティティのサイズが異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はByteです。

  パラメータ

パラメータ名	説明
リソースタイプ	監視するリソースタイプです。固定値です。省略不可です。
メトリクスラベル	監視対象をフィルタする条件としてメトリクスラベルにtypeを指定することが可能です。【項目名=値】で条件を指定して
リソースラベル	監視対象をフィルタする条件としてリソースラベルにmodule_id、version_idを指定することが可能です。【項目名=値
グループ名	監視対象をフィルタする条件としてStackdriverのグループ名を指定することが可能です。省略可能です。
ユーザーラベル	監視対象をフィルタする条件としてユーザーラベルを指定することが可能です。【ユーザーラベル名=値】の形式で指定
システムラベル	監視対象をフィルタする条件としてシステムラベルを指定することが可能です。【システムラベル名=値】の形式で指定し
タグ	監視対象をフィルタする条件としてタグを指定することが可能です。【タグ名=値】の形式で指定して下さい。省略可能
認証ファイル	サービスアカウントのAPIキーを指定することが可能です。絶対パスでAPIキー認証ファイル名を指定して下さい。省略
出力メトリクスラベル	監視結果の監視対象として表示するメトリクスラベルを指定します。省略可能です。
出力リソースラベル	監視結果の監視対象として表示するリソースラベルを指定します。省略可能です。

- GCP：Cloud Datastore 書き込みエンティティのサイズ(Byte)

  説明 Opetation Type ごとの書き込みエンティティのサイズを監視します。取得データは監視間隔内の99パーセンタイルの値となります。

  判定条件 取得されたCloud Datastore の書き込みエンティティのサイズが異常しきい値より大きい場合に異常とみなします。異常・警

告しきい値には数値のみ入力可能です。単位はByteです。

パラメータ

パラメータ名	説明
リソースタイプ	監視するリソースタイプです。固定値です。省略不可です。
メトリクスラベル	監視対象をフィルタする条件としてメトリクスラベルにopを指定することが可能です。【項目名=値】で条件を指定して
リソースラベル	監視対象をフィルタする条件としてリソースラベルにmodule_id、version_idを指定することが可能です。【項目名=値
グループ名	監視対象をフィルタする条件としてStackdriverのグループ名を指定することが可能です。省略可能です。
ユーザーラベル	監視対象をフィルタする条件としてユーザーラベルを指定することが可能です。【ユーザーラベル名=値】の形式で指定
システムラベル	監視対象をフィルタする条件としてシステムラベルを指定することが可能です。【システムラベル名=値】の形式で指定し
タグ	監視対象をフィルタする条件としてタグを指定することが可能です。【タグ名=値】の形式で指定して下さい。省略可能
認証ファイル	サービスアカウントのAPIキーを指定することが可能です。絶対パスでAPIキー認証ファイル名を指定して下さい。省略
出力メトリクスラベル	監視結果の監視対象として表示するメトリクスラベルを指定します。省略可能です。
出力リソースラベル	監視結果の監視対象として表示するリソースラベルを指定します。省略可能です。

- GCP：Clould DNS レスポンス数

  説明 すべてのDNSレスポンス数を監視します。取得データは監視間隔内の平均値となります。

  判定条件 取得されたClould DNS のレスポンス数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースタイプ	監視するリソースタイプです。固定値です。省略不可です。
メトリクスラベル	監視対象をフィルタする条件としてメトリクスラベルにresponse_codeを指定することが可能です。【項目名=値】で条
リソースラベル	監視対象をフィルタする条件としてリソースラベルにtarget_name、target_type、source_typeを指定することが可能
グループ名	監視対象をフィルタする条件としてStackdriverのグループ名を指定することが可能です。省略可能です。
ユーザーラベル	監視対象をフィルタする条件としてユーザーラベルを指定することが可能です。【ユーザーラベル名=値】の形式で指定
システムラベル	監視対象をフィルタする条件としてシステムラベルを指定することが可能です。【システムラベル名=値】の形式で指定し
タグ	監視対象をフィルタする条件としてタグを指定することが可能です。【タグ名=値】の形式で指定して下さい。省略可能
認証ファイル	サービスアカウントのAPIキーを指定することが可能です。絶対パスでAPIキー認証ファイル名を指定して下さい。省略
出力メトリクスラベル	監視結果の監視対象として表示するメトリクスラベルを指定します。省略可能です。
出力リソースラベル	監視結果の監視対象として表示するリソースラベルを指定します。省略可能です。

- GCP：Cloud Load Balancing バックエンドレイテンシ(ミリ秒)

  説明 プロキシがバックエンドにリクエストを送信してからバックエンドからのレスポンスの最後のバイトを受信するまでのレイテンシを監視します。取得データは監視間隔内の99パーセンタイルの値となります。

  判定条件 取得されたCloud Load Balancing のバックエンドレイテンシが異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はミリ秒です。

  パラメータ

パラメータ名	説明
リソースタイプ	監視するリソースタイプです。固定値です。省略不可です。
メトリクスラベル	監視対象をフィルタする条件としてメトリクスラベルにprotocol、response_code、proxy_continent、client_countr
リソースラベル	監視対象をフィルタする条件としてリソースラベルにmatched_url_path_rule、backend_target_name、backend_t
グループ名	監視対象をフィルタする条件としてStackdriverのグループ名を指定することが可能です。省略可能です。
ユーザーラベル	監視対象をフィルタする条件としてユーザーラベルを指定することが可能です。【ユーザーラベル名=値】の形式で指定
システムラベル	監視対象をフィルタする条件としてシステムラベルを指定することが可能です。【システムラベル名=値】の形式で指定し
タグ	監視対象をフィルタする条件としてタグを指定することが可能です。【タグ名=値】の形式で指定して下さい。省略可能
認証ファイル	サービスアカウントのAPIキーを指定することが可能です。絶対パスでAPIキー認証ファイル名を指定して下さい。省略
出力メトリクスラベル	監視結果の監視対象として表示するメトリクスラベルを指定します。省略可能です。
出力リソースラベル	監視結果の監視対象として表示するリソースラベルを指定します。省略可能です。

- GCP：Stackdriver Logging ログエントリ数

  説明 Compute Engine のログエントリの数を監視します。取得データは検査間隔期間内の合計値となります。

判定条件 取得されたCompute Engine のログエントリの数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

パラメータ

パラメータ名	説明
リソースタイプ	監視するリソースタイプです。固定値です。省略不可です。
メトリクスラベル	監視対象をフィルタする条件としてメトリクスラベルにlog、severityを指定することが可能です。【項目名=値】で条件を
リソースラベル	監視対象をフィルタする条件としてリソースラベルにinstance_id、zoneを指定することが可能です。【項目名=値】で条
グループ名	監視対象をフィルタする条件としてStackdriverのグループ名を指定することが可能です。省略可能です。
ユーザーラベル	監視対象をフィルタする条件としてユーザーラベルを指定することが可能です。【ユーザーラベル名=値】の形式で指定
システムラベル	監視対象をフィルタする条件としてシステムラベルを指定することが可能です。【システムラベル名=値】の形式で指定し
タグ	監視対象をフィルタする条件としてタグを指定することが可能です。【タグ名=値】の形式で指定して下さい。省略可能
認証ファイル	サービスアカウントのAPIキーを指定することが可能です。絶対パスでAPIキー認証ファイル名を指定して下さい。省略
出力メトリクスラベル	監視結果の監視対象として表示するメトリクスラベルを指定します。省略可能です。
出力リソースラベル	監視結果の監視対象として表示するリソースラベルを指定します。省略可能です。

- GCP：Stackdriver Logging エラーログエントリ数

  説明 Compute Engine のエラーログエントリの数を監視します。取得データは検査間隔期間内の合計値となります。

  判定条件 取得されたCompute Engine のエラーログエントリの数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
リソースタイプ	監視するリソースタイプです。固定値です。省略不可です。
メトリクスラベル	監視対象をフィルタする条件としてメトリクスラベルにlogを指定することが可能です。【項目名=値】で条件を指定して
リソースラベル	監視対象をフィルタする条件としてリソースラベルにinstance_id、zoneを指定することが可能です。【項目名=値】で条
グループ名	監視対象をフィルタする条件としてStackdriverのグループ名を指定することが可能です。省略可能です。
ユーザーラベル	監視対象をフィルタする条件としてユーザーラベルを指定することが可能です。【ユーザーラベル名=値】の形式で指定
システムラベル	監視対象をフィルタする条件としてシステムラベルを指定することが可能です。【システムラベル名=値】の形式で指定し
タグ	監視対象をフィルタする条件としてタグを指定することが可能です。【タグ名=値】の形式で指定して下さい。省略可能
認証ファイル	サービスアカウントのAPIキーを指定することが可能です。絶対パスでAPIキー認証ファイル名を指定して下さい。省略
出力メトリクスラベル	監視結果の監視対象として表示するメトリクスラベルを指定します。省略可能です。
出力リソースラベル	監視結果の監視対象として表示するリソースラベルを指定します。省略可能です。

- GCP：Stackdriver Monitoring リソースチェック

  説明 Compute Engine の稼働時間チェックで不合格になった数を監視します。取得データは検査間隔期間内の合計値となります。

  判定条件 取得されたCompute Engine の稼働時間チェックで不合格になった数が0と異なる場合に異常とみなします。

  パラメータ

パラメータ名	説明
リソースタイプ	監視するリソースタイプです。固定値です。省略不可です。
メトリクスラベル	監視対象をフィルタする条件としてメトリクスラベルにcheck_id、checked_resource_id、checker_locationを指定
リソースラベル	監視対象をフィルタする条件としてリソースラベルにinstance_id、zoneを指定することが可能です。【項目名=値】で条
グループ名	監視対象をフィルタする条件としてStackdriverのグループ名を指定することが可能です。省略可能です。
ユーザーラベル	監視対象をフィルタする条件としてユーザーラベルを指定することが可能です。【ユーザーラベル名=値】の形式で指定
システムラベル	監視対象をフィルタする条件としてシステムラベルを指定することが可能です。【システムラベル名=値】の形式で指定し
タグ	監視対象をフィルタする条件としてタグを指定することが可能です。【タグ名=値】の形式で指定して下さい。省略可能
認証ファイル	サービスアカウントのAPIキーを指定することが可能です。絶対パスでAPIキー認証ファイル名を指定して下さい。省略
出力メトリクスラベル	監視結果の監視対象として表示するメトリクスラベルを指定します。省略可能です。
出力リソースラベル	監視結果の監視対象として表示するリソースラベルを指定します。省略可能です。

- GCP：Pub/Sub バックログメッセージの経過時間(/秒)

  説明 サブスクリプション内の最も古い未確認メッセージの経過時間を監視します。取得データは瞬間値となります。

判定条件 取得されたサブスクリプション内の最も古い未確認メッセージの経過時間が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は秒です。

パラメータ

パラメータ名	説明
リソースタイプ	監視するリソースタイプです。固定値です。省略不可です。
メトリクスラベル	監視対象をフィルタする条件としてメトリクスラベルを指定することが可能です。【項目名=値】で条件を指定して下さい
リソースラベル	監視対象をフィルタする条件としてリソースラベルにsubscription_idを指定することが可能です。【項目名=値】で条件
グループ名	監視対象をフィルタする条件としてStackdriverのグループ名を指定することが可能です。省略可能です。
ユーザーラベル	監視対象をフィルタする条件としてユーザーラベルを指定することが可能です。【ユーザーラベル名=値】の形式で指定
システムラベル	監視対象をフィルタする条件としてシステムラベルを指定することが可能です。【システムラベル名=値】の形式で指定し
タグ	監視対象をフィルタする条件としてタグを指定することが可能です。【タグ名=値】の形式で指定して下さい。省略可能
認証ファイル	サービスアカウントのAPIキーを指定することが可能です。絶対パスでAPIキー認証ファイル名を指定して下さい。省略
出力メトリクスラベル	監視結果の監視対象として表示するメトリクスラベルを指定します。省略可能です。
出力リソースラベル	監視結果の監視対象として表示するリソースラベルを指定します。省略可能です。

- GCP：Cloud Spanner APIリクエスト数(/秒)

  説明 1秒間の Cloud Spanner API のリクエスト数を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得された1秒間の Cloud Spanner API のリクエスト数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は/秒です。

  パラメータ

パラメータ名	説明
リソースタイプ	監視するリソースタイプです。固定値です。省略不可です。
メトリクスラベル	監視対象をフィルタする条件としてメトリクスラベルにdatabase、status、methodを指定することが可能です。【項目
リソースラベル	監視対象をフィルタする条件としてリソースラベルにinstance_id、location、instance_configを指定することが可能
グループ名	監視対象をフィルタする条件としてStackdriverのグループ名を指定することが可能です。省略可能です。
ユーザーラベル	監視対象をフィルタする条件としてユーザーラベルを指定することが可能です。【ユーザーラベル名=値】の形式で指定
システムラベル	監視対象をフィルタする条件としてシステムラベルを指定することが可能です。【システムラベル名=値】の形式で指定し
タグ	監視対象をフィルタする条件としてタグを指定することが可能です。【タグ名=値】の形式で指定して下さい。省略可能
認証ファイル	サービスアカウントのAPIキーを指定することが可能です。絶対パスでAPIキー認証ファイル名を指定して下さい。省略
出力メトリクスラベル	監視結果の監視対象として表示するメトリクスラベルを指定します。省略可能です。
出力リソースラベル	監視結果の監視対象として表示するリソースラベルを指定します。省略可能です。

- GCP：Cloud Spanner データベースサーバー要求待ち時間(秒)

  説明 データベースのサーバー要求待ち時間を監視します。取得データは監視間隔内の99パーセンタイルの値となります。

  判定条件 取得されたデータベースのサーバー要求待ち時間が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は秒です。

  パラメータ

パラメータ名	説明
リソースタイプ	監視するリソースタイプです。固定値です。省略不可です。
メトリクスラベル	監視対象をフィルタする条件としてメトリクスラベルにdatabase、methodを指定することが可能です。【項目名=値】て
リソースラベル	監視対象をフィルタする条件としてリソースラベルにinstance_id、location、instance_configを指定することが可能
グループ名	監視対象をフィルタする条件としてStackdriverのグループ名を指定することが可能です。省略可能です。
ユーザーラベル	監視対象をフィルタする条件としてユーザーラベルを指定することが可能です。【ユーザーラベル名=値】の形式で指定
システムラベル	監視対象をフィルタする条件としてシステムラベルを指定することが可能です。【システムラベル名=値】の形式で指定し
タグ	監視対象をフィルタする条件としてタグを指定することが可能です。【タグ名=値】の形式で指定して下さい。省略可能
認証ファイル	サービスアカウントのAPIキーを指定することが可能です。絶対パスでAPIキー認証ファイル名を指定して下さい。省略
出力メトリクスラベル	監視結果の監視対象として表示するメトリクスラベルを指定します。省略可能です。
出力リソースラベル	監視結果の監視対象として表示するリソースラベルを指定します。省略可能です。

- GCP：Cloud Storage ネットワーク受信バイト数(Byte)

  説明 GCS BUCKETのネットワーク経由で受信されたバイト数を監視します。取得データは検査間隔期間内の合計値となります。

判定条件 取得されたGCS BUCKETのネットワーク経由で受信されたバイト数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はByteです。

パラメータ

パラメータ名	説明
リソースタイプ	監視するリソースタイプです。固定値です。省略不可です。
メトリクスラベル	監視対象をフィルタする条件としてメトリクスラベルにresponse_code、methodを指定することが可能です。【項目名
リソースラベル	監視対象をフィルタする条件としてリソースラベルにbucket_name、locationを指定することが可能です。【項目名=値
グループ名	監視対象をフィルタする条件としてStackdriverのグループ名を指定することが可能です。省略可能です。
ユーザーラベル	監視対象をフィルタする条件としてユーザーラベルを指定することが可能です。【ユーザーラベル名=値】の形式で指定
システムラベル	監視対象をフィルタする条件としてシステムラベルを指定することが可能です。【システムラベル名=値】の形式で指定し
タグ	監視対象をフィルタする条件としてタグを指定することが可能です。【タグ名=値】の形式で指定して下さい。省略可能
認証ファイル	サービスアカウントのAPIキーを指定することが可能です。絶対パスでAPIキー認証ファイル名を指定して下さい。省略
出力メトリクスラベル	監視結果の監視対象として表示するメトリクスラベルを指定します。省略可能です。
出力リソースラベル	監視結果の監視対象として表示するリソースラベルを指定します。省略可能です。

- GCP：Cloud Storage ネットワーク送信バイト数(Byte)

  説明 GCS BUCKETのネットワーク経由で送信されたバイト数を監視します。取得データは検査間隔期間内の合計値となります。

  判定条件 取得されたGCS BUCKETのネットワーク経由で送信されたバイト数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はByteです。

  パラメータ

パラメータ名	説明
リソースタイプ	監視するリソースタイプです。固定値です。省略不可です。
メトリクスラベル	監視対象をフィルタする条件としてメトリクスラベルにresponse_code、methodを指定することが可能です。【項目名
リソースラベル	監視対象をフィルタする条件としてリソースラベルにbucket_name、locationを指定することが可能です。【項目名=値
グループ名	監視対象をフィルタする条件としてStackdriverのグループ名を指定することが可能です。省略可能です。
ユーザーラベル	監視対象をフィルタする条件としてユーザーラベルを指定することが可能です。【ユーザーラベル名=値】の形式で指定
システムラベル	監視対象をフィルタする条件としてシステムラベルを指定することが可能です。【システムラベル名=値】の形式で指定し
タグ	監視対象をフィルタする条件としてタグを指定することが可能です。【タグ名=値】の形式で指定して下さい。省略可能
認証ファイル	サービスアカウントのAPIキーを指定することが可能です。絶対パスでAPIキー認証ファイル名を指定して下さい。省略
出力メトリクスラベル	監視結果の監視対象として表示するメトリクスラベルを指定します。省略可能です。
出力リソースラベル	監視結果の監視対象として表示するリソースラベルを指定します。省略可能です。

- GCP：Cloud Storage バケット内オブジェクト合計サイズ(Byte)

  説明 GCS BUCKET内のすべてのオブジェクトの合計サイズを監視します。取得データは検査間隔期間内の合計値となります。

  判定条件 取得されたGCS BUCKET内のすべてのオブジェクトの合計サイズが異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はByteです。

  パラメータ

パラメータ名	説明
リソースタイプ	監視するリソースタイプです。固定値です。省略不可です。
メトリクスラベル	監視対象をフィルタする条件としてメトリクスラベルにstorage_classを指定することが可能です。【項目名=値】で条件
リソースラベル	監視対象をフィルタする条件としてリソースラベルにbucket_name、locationを指定することが可能です。【項目名=値
グループ名	監視対象をフィルタする条件としてStackdriverのグループ名を指定することが可能です。省略可能です。
ユーザーラベル	監視対象をフィルタする条件としてユーザーラベルを指定することが可能です。【ユーザーラベル名=値】の形式で指定
システムラベル	監視対象をフィルタする条件としてシステムラベルを指定することが可能です。【システムラベル名=値】の形式で指定し
タグ	監視対象をフィルタする条件としてタグを指定することが可能です。【タグ名=値】の形式で指定して下さい。省略可能
認証ファイル	サービスアカウントのAPIキーを指定することが可能です。絶対パスでAPIキー認証ファイル名を指定して下さい。省略
出力メトリクスラベル	監視結果の監視対象として表示するメトリクスラベルを指定します。省略可能です。
出力リソースラベル	監視結果の監視対象として表示するリソースラベルを指定します。省略可能です。

- GCP：Stackdriver ログ情報取得

  説明 Google Cloudのログ情報を監視します。取得データは成否となります。

判定条件 ログ情報取得が異常終了した場合、異常となります。ログの件数が多く、ログを取得し切れなかった場合、警告となります。値は変更しないで下さい。

パラメータ

パラメータ名	説明
認証ファイル	サービスアカウントのAPIキーを指定することが可能です。絶対パスでAPIキー認証ファイル名を指定して下さい。省略可能
リソースタイプ	監視するリソースタイプです。固定値です。省略不可です。
リソースラベル	監視対象をフィルタする条件としてリソースラベルを指定することが可能です。【項目名=値】で条件を指定して下さい。省
ログ名	取得するログ名を指定します。ログ名はURL エンコードした値を指定して下さい（例： cloudfunctions.googleapis.com
ログレベル	取得するログレベルを指定します。省略可能です。
ログフォーマット	取得したログの出力フォーマットをLTSVもしくはJSONに切り替えます。デフォルト値はLTSVとなります。省略可能です
ログ出力ファイル	収集したログ情報の出力先ログファイルを指定することが可能です。絶対パスでログ出力ファイル名を指定して下さい。省

備考 Cloud Logging連携機能については、Cloud Logging連携機能 を参照して下さい。

注釈

GCP：Stackdriver ログ情報取得では、最後に取得したログのタイムスタンプよりlogBufferTimeに指定した分数遡ってログを取得します。監視タスクの新規作成時などの最後に取得したログが無い場合は「監視間隔＋logBufferTime＋5分」以内に発生したログを取得します。
GCP Stackdriver では、発生したログが GCP Stackdriver 上に現れるまでに時間がかかる場合があります。その時間が監視間隔以上かかる場合、ログが取得されない状態となります。このような場合は、logBufferTimeを適切に設定して下さい。

- GCP：利用料金（当月）

  説明 当月分の利用料金を監視します。取得データは瞬間値となります。

  判定条件 取得された利用料金が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
認証ファイル	サービスアカウントのAPIキーを指定することが可能です。絶対パスでAPIキー認証ファイル名を指定して下さい。省略可能で
テーブル名	Cloud Billing データをエクスポートしたBigQueryのデータセットのテーブル名を「<プロジェクト名>.<データセット名>.<テーブ
モード	利用料金の取得範囲を当月(T)に指定します。省略不可です。
グループ	利用料金の合計の算出グループを全体(T)、サービス毎(S)か切り替えます。デフォルト値は全体(T)となります。省略可能で
サービス名	監視するサービス名を指定します。省略可能です。
ラベル(タグ)	監視対象をフィルタする条件としてタグを指定することが可能です。【タグ名=値】の形式で指定して下さい。省略可能です。

  備考 Cloud Billing データを BigQuery にエクスポートする方法、制限事項については、下記Googleのサイトをご参照下さい。
  参考URL：https://cloud.google.com/billing/docs/how-to/export-data-bigquery （2020年4月現在）

  注釈

  Google Cloud側で利用料金の反映に時間がかかるため取得されたデータとGoogle Cloudコンソールで確認した金額に差分が発生する可能性があります。

- GCP：利用料金（先月）

  説明 先月分の利用料金を監視します。取得データは瞬間値となります。

  判定条件 取得された利用料金が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
認証ファイル	サービスアカウントのAPIキーを指定することが可能です。絶対パスでAPIキー認証ファイル名を指定して下さい。省略可能で
テーブル名	Cloud Billing データをエクスポートしたBigQueryのデータセットのテーブル名を「<プロジェクト名>.<データセット名>.<テーブ
モード	利用料金の取得範囲を先月(P)に指定します。省略不可です。
グループ	利用料金の合計の算出グループを全体(T)、サービス毎(S)か切り替えます。デフォルト値は全体(T)となります。省略可能で
サービス名	監視するサービス名を指定します。省略可能です。
ラベル(タグ)	監視対象をフィルタする条件としてタグを指定することが可能です。【タグ名=値】の形式で指定して下さい。省略可能です。

備考 Cloud Billing データを BigQuery にエクスポートする方法、制限事項については、下記Googleのサイトをご参照下さい。
参考URL：https://cloud.google.com/billing/docs/how-to/export-data-bigquery （2020年4月現在）

注釈

Google Cloud側で利用料金の反映に時間がかかるため取得されたデータとGoogle Cloudコンソールで確認した金額に差分が発生する可能性があります。

- GCP：メトリクス監視

  説明 指定したメトリクスの情報を取得します

  判定条件 「計算式の変数の値」で指定した「リソースタイプ:メトリクスタイプ」から取得したメトリクス値の判定条件を指定して下さい。

  パラメータ

パラメータ名	説明
メトリクスラベル	監視対象をフィルタする条件としてメトリクスラベルを指定することが可能です。【項目名=値】で条件を指定して下さい
リソースラベル	監視対象をフィルタする条件としてリソースラベルを指定することが可能です。【項目名=値】で条件を指定して下さい。
グループ名	監視対象をフィルタする条件としてグループ名を指定することが可能です。省略可能です。
ユーザーラベル	監視対象をフィルタする条件としてユーザーラベルを指定することが可能です。【ユーザーラベル名=値】の形式で指定
システムラベル	監視対象をフィルタする条件としてシステムラベルを指定することが可能です。【システムラベル名=値】の形式で指定し
タグ	監視対象をフィルタする条件としてタグを指定することが可能です。【タグ名=値】の形式で指定して下さい。省略可能
認証ファイル	サービスアカウントのAPIキーを指定することが可能です。絶対パスでAPIキー認証ファイル名を指定して下さい。省略
出力メトリクスラベル	監視結果の監視対象として表示するメトリクスラベルを指定します。省略可能です。
出力リソースラベル	監視結果の監視対象として表示するリソースラベルを指定します。省略可能です。

2.8.1.4. OCI監視

注釈

監視項目によっては、監視間隔を15分未満に設定すると値が取得できないことがあります。その場合は監視間隔を15分以上に設定して下さい。

参考

各種パラメータの設定値が分からない場合は、Oracle Cloud Infrastructureより提供されているMetrics Explorerにて確認して下さい。
参考URL：https://console.us-ashburn-1.oraclecloud.com/monitoring/explore （2020年9月現在）

- OCI：Compute CPU使用率(%)

  説明 Compute インスタンスのCPU使用率を監視します。取得データは検査間隔期間内の平均値となります。インスタンス・プールの場合、値はプール内のすべてのインスタンスの平均値となります。

  判定条件 取得されたCompute インスタンスのCPU使用率が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
コンパートメント	監視するリソースが所属するコンパートメントIDまたはコンパートメント名を指定します。省略不可です。
ディメンション	監視対象をフィルタする条件としてディメンションを指定することが可能です。【項目名=値】で条件を指定して下さい。
フリーフォームタグ	監視対象をフィルタする条件としてフリーフォームタグを指定することが可能です。【タグ名=値】の形式で指定して下さ
定義済みタグ	監視対象をフィルタする条件として定義済みタグを指定することが可能です。【ネームスペース:タグ名=値】の形式で指
表示ディメンション名	監視結果の監視対象として表示する表示ディメンション名を指定します。省略可能です。
認証ファイル	ユーザーのAPIキーを指定することが可能です。絶対パスでAPIキー認証ファイル名を指定して下さい。省略可能です

  備考 ※1　サービス「computeagent」と「objectstorage」のみ対応しております。
  ※2　同じタグを複数指定した場合は後勝ちです。

- OCI：Block Volume ボリューム読み取りスループット(Byte)

  説明 Block Volumeの読み取りバイト数を監視します。取得データは検査間隔期間内の合計値となります。

  判定条件 取得されたBlock Volumeの読み取りバイト数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

パラメータ

パラメータ名	説明
コンパートメント	監視するリソースが所属するコンパートメントIDまたはコンパートメント名を指定します。省略不可です。
ディメンション	監視対象をフィルタする条件としてディメンションを指定することが可能です。【項目名=値】で条件を指定して下さい。
表示ディメンション名	監視結果の監視対象として表示する表示ディメンション名を指定します。省略可能です。
認証ファイル	ユーザーのAPIキーを指定することが可能です。絶対パスでAPIキー認証ファイル名を指定して下さい。省略可能です

- OCI: Block Volume ボリューム書き込みスループット(Byte)

  説明 Block Volumeの書き込みバイト数を監視します。取得データは検査間隔期間内の合計値となります。

  判定条件 取得されたBlock Volumeの書き込みバイト数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
コンパートメント	監視するリソースが所属するコンパートメントIDまたはコンパートメント名を指定します。省略不可です。
ディメンション	監視対象をフィルタする条件としてディメンションを指定することが可能です。【項目名=値】で条件を指定して下さい。
表示ディメンション名	監視結果の監視対象として表示する表示ディメンション名を指定します。省略可能です。
認証ファイル	ユーザーのAPIキーを指定することが可能です。絶対パスでAPIキー認証ファイル名を指定して下さい。省略可能です

- OCI: VNIC ネットワーク受信バイト数(Byte)

  説明 ネットワークからVNICに受信されたバイト数を監視します。取得データは検査間隔期間内の合計値となります。

  判定条件 取得されたネットワークからVNICに受信されたバイト数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
コンパートメント	監視するリソースが所属するコンパートメントIDまたはコンパートメント名を指定します。省略不可です。
ディメンション	監視対象をフィルタする条件としてディメンションを指定することが可能です。【項目名=値】で条件を指定して下さい。
表示ディメンション名	監視結果の監視対象として表示する表示ディメンション名を指定します。省略可能です。
認証ファイル	ユーザーのAPIキーを指定することが可能です。絶対パスでAPIキー認証ファイル名を指定して下さい。省略可能です

- OCI: VNIC ネットワーク送信バイト数(Byte)

  説明 VNICからネットワークに送信されたバイト数を監視します。取得データは検査間隔期間内の合計値となります。

  判定条件 取得されたVNICからネットワークに送信されたバイト数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
コンパートメント	監視するリソースが所属するコンパートメントIDまたはコンパートメント名を指定します。省略不可です。
ディメンション	監視対象をフィルタする条件としてディメンションを指定することが可能です。【項目名=値】で条件を指定して下さい。
表示ディメンション名	監視結果の監視対象として表示する表示ディメンション名を指定します。省略可能です。
認証ファイル	ユーザーのAPIキーを指定することが可能です。絶対パスでAPIキー認証ファイル名を指定して下さい。省略可能です

- OCI: Autonomous Database CPU使用率(%)

  説明 Autonomous DatabaseのCPU使用率を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたAutonomous DatabaseのCPU使用率が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
コンパートメント	監視するリソースが所属するコンパートメントIDまたはコンパートメント名を指定します。省略不可です。
ディメンション	監視対象をフィルタする条件としてディメンションを指定することが可能です。【項目名=値】で条件を指定して下さい。
表示ディメンション名	監視結果の監視対象として表示する表示ディメンション名を指定します。省略可能です。
認証ファイル	ユーザーのAPIキーを指定することが可能です。絶対パスでAPIキー認証ファイル名を指定して下さい。省略可能です

- OCI：Autonomous Database SQL実行数

  説明 Autonomous DatabaseのSQL文を実行したユーザー・コールおよび再帰コールの数を監視します。取得データは検査間隔期間内の合計値となります。

  判定条件 取得されたAutonomous DatabaseのSQL文を実行したユーザー・コールおよび再帰コールの数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
コンパートメント	監視するリソースが所属するコンパートメントIDまたはコンパートメント名を指定します。省略不可です。
ディメンション	監視対象をフィルタする条件としてディメンションを指定することが可能です。【項目名=値】で条件を指定して下さい。
表示ディメンション名	監視結果の監視対象として表示する表示ディメンション名を指定します。省略可能です。
認証ファイル	ユーザーのAPIキーを指定することが可能です。絶対パスでAPIキー認証ファイル名を指定して下さい。省略可能です

- OCI：Events 一致したイベント数

  説明 ルールに対して一致したイベントの合計数を監視します。取得データは検査間隔期間内の合計値となります。

  判定条件 取得されたルールに対して一致したイベントの合計数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
コンパートメント	監視するリソースが所属するコンパートメントIDまたはコンパートメント名を指定します。省略不可です。
ディメンション	監視対象をフィルタする条件としてディメンションを指定することが可能です。【項目名=値】で条件を指定して下さい。
表示ディメンション名	監視結果の監視対象として表示する表示ディメンション名を指定します。省略可能です。
認証ファイル	ユーザーのAPIキーを指定することが可能です。絶対パスでAPIキー認証ファイル名を指定して下さい。省略可能です
ゼロパブリッシュ	検査間隔内にデータポイントが無かった場合に取得データの値を「0」とする場合にONを指定します。省略可能です。

注釈

ゼロパブリッシュがONの場合は、監視間隔でデータポイントの有無に変化があると、監視結果の状態にかかわらずメッセージモニタにメッセージが通知されます。

- OCI：Load Balancing HTTP2xxレスポンス数

  説明 バックエンド・セットから受信されたHTTP 2xxレスポンスの数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたバックエンド・セットから受信されたHTTP 2xxレスポンスの数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
コンパートメント	監視するリソースが所属するコンパートメントIDまたはコンパートメント名を指定します。省略不可です。
ディメンション	監視対象をフィルタする条件としてディメンションを指定することが可能です。【項目名=値】で条件を指定して下さい。
表示ディメンション名	監視結果の監視対象として表示する表示ディメンション名を指定します。省略可能です。
認証ファイル	ユーザーのAPIキーを指定することが可能です。絶対パスでAPIキー認証ファイル名を指定して下さい。省略可能です

- OCI：Load Balancing HTTP3xxレスポンス数

  説明 バックエンド・セットから受信されたHTTP 3xxレスポンスの数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたバックエンド・セットから受信されたHTTP 3xxレスポンスの数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
コンパートメント	監視するリソースが所属するコンパートメントIDまたはコンパートメント名を指定します。省略不可です。
ディメンション	監視対象をフィルタする条件としてディメンションを指定することが可能です。【項目名=値】で条件を指定して下さい。
表示ディメンション名	監視結果の監視対象として表示する表示ディメンション名を指定します。省略可能です。
認証ファイル	ユーザーのAPIキーを指定することが可能です。絶対パスでAPIキー認証ファイル名を指定して下さい。省略可能です

- OCI:Load Balancing HTTP4xxレスポンス数

  説明 バックエンド・セットから受信されたHTTP 4xxレスポンスの数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたバックエンド・セットから受信されたHTTP 4xxレスポンスの数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
コンパートメント	監視するリソースが所属するコンパートメントIDまたはコンパートメント名を指定します。省略不可です。
ディメンション	監視対象をフィルタする条件としてディメンションを指定することが可能です。【項目名=値】で条件を指定して下さい。
表示ディメンション名	監視結果の監視対象として表示する表示ディメンション名を指定します。省略可能です。
認証ファイル	ユーザーのAPIキーを指定することが可能です。絶対パスでAPIキー認証ファイル名を指定して下さい。省略可能です

- OCI:Load Balancing HTTP5xxレスポンス数

  説明 バックエンド・セットから受信されたHTTP 5xxレスポンスの数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたバックエンド・セットから受信されたHTTP 5xxレスポンスの数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
コンパートメント	監視するリソースが所属するコンパートメントIDまたはコンパートメント名を指定します。省略不可です。
ディメンション	監視対象をフィルタする条件としてディメンションを指定することが可能です。【項目名=値】で条件を指定して下さい。
表示ディメンション名	監視結果の監視対象として表示する表示ディメンション名を指定します。省略可能です。
認証ファイル	ユーザーのAPIキーを指定することが可能です。絶対パスでAPIキー認証ファイル名を指定して下さい。省略可能です

- OCI:FastConnect 接続状態

  説明 FastConnect接続に停止(0)状態が検査間隔内に発生しているか監視します。

  判定条件 取得されたFastConnect接続に停止(0)状態が異常しきい値と等しい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
コンパートメント	監視するリソースが所属するコンパートメントIDまたはコンパートメント名を指定します。省略不可です。
ディメンション	監視対象をフィルタする条件としてディメンションを指定することが可能です。【項目名=値】で条件を指定して下さい。
表示ディメンション名	監視結果の監視対象として表示する表示ディメンション名を指定します。省略可能です。
認証ファイル	ユーザーのAPIキーを指定することが可能です。絶対パスでAPIキー認証ファイル名を指定して下さい。省略可能です

- OCI:VPN Connect IPSecトンネルの状態

  説明 VPN ConnectのIPSecトンネルに停止中(0)状態が検査間隔内に発生しているかを監視します。

  判定条件 取得されたVPN ConnectのIPSecトンネルに停止中(0)状態が異常しきい値と等しい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
コンパートメント	監視するリソースが所属するコンパートメントIDまたはコンパートメント名を指定します。省略不可です。
ディメンション	監視対象をフィルタする条件としてディメンションを指定することが可能です。【項目名=値】で条件を指定して下さい。
表示ディメンション名	監視結果の監視対象として表示する表示ディメンション名を指定します。省略可能です。
認証ファイル	ユーザーのAPIキーを指定することが可能です。絶対パスでAPIキー認証ファイル名を指定して下さい。省略可能です

- OCI:Notifications 配信メッセージ数

  説明 エンドポイントに正常に配信されたメッセージ数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたエンドポイントに正常に配信されたメッセージ数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
コンパートメント	監視するリソースが所属するコンパートメントIDまたはコンパートメント名を指定します。省略不可です。
ディメンション	監視対象をフィルタする条件としてディメンションを指定することが可能です。【項目名=値】で条件を指定して下さい。
表示ディメンション名	監視結果の監視対象として表示する表示ディメンション名を指定します。省略可能です。
認証ファイル	ユーザーのAPIキーを指定することが可能です。絶対パスでAPIキー認証ファイル名を指定して下さい。省略可能です
ゼロパブリッシュ	検査間隔内にデータポイントが無かった場合に取得データの値を「0」とする場合にONを指定します。省略可能です。

  注釈

  ゼロパブリッシュがONの場合は、監視間隔でデータポイントの有無に変化があると、監視結果の状態にかかわらずメッセージモニタにメッセージが通知されます。

- OCI:Notifications 失敗メッセージ数

  説明 エンドポイントに配信されなかったメッセージ数を監視します。取得データは検査間隔の合計値となります。

  判定条件 取得されたエンドポイントに配信されなかったメッセージ数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
コンパートメント	監視するリソースが所属するコンパートメントIDまたはコンパートメント名を指定します。省略不可です。
ディメンション	監視対象をフィルタする条件としてディメンションを指定することが可能です。【項目名=値】で条件を指定して下さい。
表示ディメンション名	監視結果の監視対象として表示する表示ディメンション名を指定します。省略可能です。
認証ファイル	ユーザーのAPIキーを指定することが可能です。絶対パスでAPIキー認証ファイル名を指定して下さい。省略可能です
ゼロパブリッシュ	検査間隔内にデータポイントが無かった場合に取得データの値を「0」とする場合にONを指定します。省略可能です。

  注釈

  ゼロパブリッシュがONの場合は、監視間隔でデータポイントの有無に変化があると、監視結果の状態にかかわらずメッセージモニタにメッセージが通知されます。

- OCI:Object Storage バケット・サイズ(Byte)

  説明 バケットのサイズを監視します。取得データは検査間隔期間内の最大値となります。

  判定条件 取得されたバケットのサイズが異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
コンパートメント	監視するリソースが所属するコンパートメントIDまたはコンパートメント名を指定します。省略不可です。
ディメンション	監視対象をフィルタする条件としてディメンションを指定することが可能です。【項目名=値】で条件を指定して下さい。
フリーフォームタグ	監視対象をフィルタする条件としてフリーフォームタグを指定することが可能です。【タグ名=値】の形式で指定して下さ
定義済みタグ	監視対象をフィルタする条件として定義済みタグを指定することが可能です。【ネームスペース:タグ名=値】の形式で指
表示ディメンション名	監視結果の監視対象として表示する表示ディメンション名を指定します。省略可能です。
認証ファイル	ユーザーのAPIキーを指定することが可能です。絶対パスでAPIキー認証ファイル名を指定して下さい。省略可能です

備考 ※1　サービス「computeagent」と「objectstorage」のみ対応しております。
※2　同じタグを複数指定した場合は後勝ちです。

注釈

監視間隔を60分未満に設定すると値が取得できないことがあります。その場合は監視間隔を60分以上に設定して下さい。

- OCI：Object Storage オブジェクト数

説明 バケット内のオブジェクトの数を監視します。取得データは検査間隔期間内の最大値となります。

判定条件 取得されたバケット内のオブジェクトの数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

パラメータ

パラメータ名	説明
コンパートメント	監視するリソースが所属するコンパートメントIDまたはコンパートメント名を指定します。省略不可です。
ディメンション	監視対象をフィルタする条件としてディメンションを指定することが可能です。【項目名=値】で条件を指定して下さい。
フリーフォームタグ	監視対象をフィルタする条件としてフリーフォームタグを指定することが可能です。【タグ名=値】の形式で指定して下さ
定義済みタグ	監視対象をフィルタする条件として定義済みタグを指定することが可能です。【ネームスペース:タグ名=値】の形式で指
表示ディメンション名	監視結果の監視対象として表示する表示ディメンション名を指定します。省略可能です。
認証ファイル	ユーザーのAPIキーを指定することが可能です。絶対パスでAPIキー認証ファイル名を指定して下さい。省略可能です

備考 ※1　サービス「computeagent」と「objectstorage」のみ対応しております。
※2　同じタグを複数指定した場合は後勝ちです。

注釈

監視間隔を60分未満に設定すると値が取得できないことがあります。その場合は監視間隔を60分以上に設定して下さい。

- OCI：Function ファンクションの合計実行時間(ミリ秒)

説明 ファンクションの合計実行時間を監視します。取得データは監視間隔内の合計時間になります。

判定条件 取得されたファンクションの合計実行時間が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

パラメータ

パラメータ名	説明
コンパートメント	監視するリソースが所属するコンパートメントIDまたはコンパートメント名を指定します。省略不可です。
ディメンション	監視対象をフィルタする条件としてディメンションを指定することが可能です。【項目名=値】で条件を指定して下さい。
表示ディメンション名	監視結果の監視対象として表示する表示ディメンション名を指定します。省略可能です。
認証ファイル	ユーザーのAPIキーを指定することが可能です。絶対パスでAPIキー認証ファイル名を指定して下さい。省略可能です
ゼロパブリッシュ	検査間隔内にデータポイントが無かった場合に取得データの値を「0」とする場合にONを指定します。省略可能です。

注釈

ゼロパブリッシュがONの場合は、監視間隔でデータポイントの有無に変化があると、監視結果の状態にかかわらずメッセージモニタにメッセージが通知されます。

- OCI：Function ファンクション呼出し回数

説明 ファンクションの呼出しの合計数を監視します。取得データは監視間隔内の合計数になります。

判定条件 取得されたファンクションの呼出しの合計数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

パラメータ

パラメータ名	説明
コンパートメント	監視するリソースが所属するコンパートメントIDまたはコンパートメント名を指定します。省略不可です。
ディメンション	監視対象をフィルタする条件としてディメンションを指定することが可能です。【項目名=値】で条件を指定して下さい。
表示ディメンション名	監視結果の監視対象として表示する表示ディメンション名を指定します。省略可能です。
認証ファイル	ユーザーのAPIキーを指定することが可能です。絶対パスでAPIキー認証ファイル名を指定して下さい。省略可能です
ゼロパブリッシュ	検査間隔内にデータポイントが無かった場合に取得データの値を「0」とする場合にONを指定します。省略可能です。

注釈

ゼロパブリッシュがONの場合は、監視間隔でデータポイントの有無に変化があると、監視結果の状態にかかわらずメッセージモニタにメッセージが通知されます。

- OCI:File Storage 読み取りスループット(Byte/秒)

  説明 ファイル・システムの1秒あたりの読み取りバイト数を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたファイル・システムの1秒あたりの読み取りバイト数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
コンパートメント	監視するリソースが所属するコンパートメントIDまたはコンパートメント名を指定します。省略不可です。
ディメンション	監視対象をフィルタする条件としてディメンションを指定することが可能です。【項目名=値】で条件を指定して下さい。
表示ディメンション名	監視結果の監視対象として表示する表示ディメンション名を指定します。省略可能です。
認証ファイル	ユーザーのAPIキーを指定することが可能です。絶対パスでAPIキー認証ファイル名を指定して下さい。省略可能です

- OCI:File Storage 書き込みスループット(Byte/秒)

  説明 ファイル・システムの1秒あたりの書き込みバイト数を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたファイル・システムの1秒あたりの書き込みバイト数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
コンパートメント	監視するリソースが所属するコンパートメントIDまたはコンパートメント名を指定します。省略不可です。
ディメンション	監視対象をフィルタする条件としてディメンションを指定することが可能です。【項目名=値】で条件を指定して下さい。
表示ディメンション名	監視結果の監視対象として表示する表示ディメンション名を指定します。省略可能です。
認証ファイル	ユーザーのAPIキーを指定することが可能です。絶対パスでAPIキー認証ファイル名を指定して下さい。省略可能です

- OCI:Audit ログ情報取得

  説明 OCIの監査ログ情報を監視します。取得データは成否となります。

  判定条件 ログ収集に失敗した場合、異常となります。異常・警告しきい値は変更しないで下さい。

  パラメータ

パラメータ名	説明
コンパートメント	監視するリソースが所属するコンパートメントIDまたはコンパートメント名を指定します。省略不可です。
認証ファイル	ユーザーのAPIキーを指定することが可能です。絶対パスでAPIキー認証ファイル名を指定して下さい。省略可能です。
ログサイクル	サイクル方式を日付(D)かサイズ(S)か切り替えます。デフォルト値はサイズ(S)となります。省略可能です。
ログフォーマット	取得したログの出力フォーマットをLTSVもしくはJSONに切り替えます。デフォルト値はLTSVとなります。省略可能です。
ログファイル	収集したログ情報の出力先ログファイルを指定することが可能です。絶対パスでログ出力ファイル名を指定して下さい。省略

注釈

- OCI:Audit ログ情報取得では、最後に取得したログのタイムスタンプよりlogBufferTimeに指定した分数遡ってログを取得します。監視タスクの新規作成時などの最後に取得したログが無い場合は「監視間隔＋logBufferTime＋5分」以内に発生したログを取得します。
  OCI Audit では、発生したログが OCI Audit 上に現れるまでに時間がかかる場合があります。その時間が監視間隔以上かかる場合、ログが取得されない状態となります。このような場合は、logBufferTimeを適切に設定して下さい。
- 監視間隔時間内で最新のログまで取得されなかった場合、メッセージモニタに警告メッセージ「OCI logs cannot get to the latest」が通知されます。
- OCI AuditのコンソールでEventIDまで差異のないログが複数出力されている場合、ログを取得するときには1件だけ出力されます。

- OCI:Budget 支出実績金額

  説明 予算の支出実績金額を監視します。取得データは瞬間値となります。

判定条件 取得された予算の支出実績金額が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

パラメータ

パラメータ名	説明
予算名	予算名を指定します。省略可です。
フリーフォームタグ	監視対象をフィルタする条件としてフリーフォームタグを指定することが可能です。【タグ名=値】の形式で指定して下さい。
定義済みタグ	監視対象をフィルタする条件として定義済みタグを指定することが可能です。【ネームスペース:タグ名=値】の形式で指定
認証ファイル	ユーザーのAPIキーを指定することが可能です。絶対パスでAPIキー認証ファイル名を指定して下さい。省略可能です。

備考 ※1　同じタグを複数指定した場合は後勝ちです。

- OCI:Budget 支出実績比率(%)

  説明 予算の支出実績金額の予算比率を監視します。取得データは瞬間値となります。

  判定条件 取得された予算の支出実績金額の予算比率が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
予算名	予算名を指定します。省略可です。
フリーフォームタグ	監視対象をフィルタする条件としてフリーフォームタグを指定することが可能です。【タグ名=値】の形式で指定して下さい。
定義済みタグ	監視対象をフィルタする条件として定義済みタグを指定することが可能です。【ネームスペース:タグ名=値】の形式で指定
認証ファイル	ユーザーのAPIキーを指定することが可能です。絶対パスでAPIキー認証ファイル名を指定して下さい。省略可能です。

  備考 ※1　同じタグを複数指定した場合は後勝ちです。

- OCI:Budget 支出予測金額

  説明 予算の支出予測金額を監視します。取得データは瞬間値となります。

  判定条件 取得された予算の支出予測金額が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
予算名	予算名を指定します。省略可です。
フリーフォームタグ	監視対象をフィルタする条件としてフリーフォームタグを指定することが可能です。【タグ名=値】の形式で指定して下さい。
定義済みタグ	監視対象をフィルタする条件として定義済みタグを指定することが可能です。【ネームスペース:タグ名=値】の形式で指定
認証ファイル	ユーザーのAPIキーを指定することが可能です。絶対パスでAPIキー認証ファイル名を指定して下さい。省略可能です。

  備考 ※1　同じタグを複数指定した場合は後勝ちです。

- OCI:Budget 支出予測比率(%)

  説明 予算の支出予測金額の予算比率を監視します。取得データは瞬間値となります。

  判定条件 取得された予算の支出予測金額の予算比率が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
予算名	予算名を指定します。省略可です。
フリーフォームタグ	監視対象をフィルタする条件としてフリーフォームタグを指定することが可能です。【タグ名=値】の形式で指定して下さい。
定義済みタグ	監視対象をフィルタする条件として定義済みタグを指定することが可能です。【ネームスペース:タグ名=値】の形式で指定
認証ファイル	ユーザーのAPIキーを指定することが可能です。絶対パスでAPIキー認証ファイル名を指定して下さい。省略可能です。

  備考 ※1　同じタグを複数指定した場合は後勝ちです。

- OCI:Log Analytics ログ情報取得

  説明 Log Analyticsのログ情報を監視します。取得データは成否となります。

判定条件 ログ収集に失敗した場合、異常となります。ログの件数が多く、ログを取得し切れなかった場合、警告となります。異常・警告しきい値は変更しないで下さい。

パラメータ

パラメータ名	説明
ネームスペース名	ログが所属するオブジェクト・ストレージ・ネームスペースを指定します。省略不可です。
コンパートメント	ログが所属するコンパートメントIDまたはコンパートメント名を指定します。省略不可です。
LogGroup名	ログが所属するLogGroup名を指定します。省略可能です。
LogSource名	ログが所属するLogSource名を指定します。省略可能です。
認証ファイル	ユーザーのAPIキーを指定することが可能です。絶対パスでAPIキー認証ファイル名を指定して下さい。省略可能です。
ログファイル	収集したログ情報の出力先ログファイルを指定することが可能です。絶対パスでログ出力ファイル名を指定して下さい。省
ログフォーマット	取得したログの出力フォーマットをLTSVもしくはJSONに切り替えます。デフォルト値はLTSVとなります。省略可能です。

備考 ネームスペース名について下記OCIのサイトをご参照下さい。
参考URL：https://docs.oracle.com/ja-jp/iaas/Content/Object/Tasks/understandingnamespaces.htm（2021年4月現在）

注釈

- OCI：Log Analytics ログ情報取得では、最後に取得したログのタイムスタンプよりlogBufferTimeに指定した分数遡ってログを取得します。監視タスクの新規作成時などの最後に取得したログが無い場合は「監視間隔＋logBufferTime＋5分」以内に発生したログを取得します。
  OCI Log Analytics では、発生したログが OCI Log Analytics 上に現れるまでに時間がかかる場合があります。その時間が監視間隔以上かかる場合、ログが取得されない状態となります。このような場合は、logBufferTimeを適切に設定して下さい。
- OCI Log Analyticsのコンソールで差異のないログが複数出力されている場合、ログを取得するときには1件だけ出力されます。

- OCI：アナウンス情報取得

  説明 アナウンス情報を監視します。取得データは成否となります。

  判定条件 アナウンス情報収集に失敗した場合、異常となります。異常・警告しきい値は変更しないで下さい。

  パラメータ

パラメータ名	説明
コンパートメント	ルート・コンパートメントIDまたはコンパートメント名を指定します。省略可能です。省略の場合、認証ファイルから取得しま
認証ファイル	ユーザーのAPIキーを指定することが可能です。絶対パスでAPIキー認証ファイル名を指定して下さい。省略可能です。
モード	モードを指定します。省略可能です。更新日時(update)、作成日時(create)か切り替えます。デフォルト値は更新日時(u
ログフォーマット	取得したログの出力フォーマットをLTSVもしくはJSONに切り替えます。デフォルト値はLTSVとなります。省略可能です。
ログファイル	収集したログ情報の出力先ログファイルを指定することが可能です。絶対パスでログ出力ファイル名を指定して下さい。省略

  注釈

  - OCI：アナウンス情報取得では、最後に取得したログのタイムスタンプよりlogBufferTimeに指定した分数遡ってログを取得します。監視タスクの新規作成時などの最後に取得したログが無い場合は直前2年前から発生したログを取得します。

- OCI：アラーム状態

  説明 アラームの状態を監視します。取得データは瞬間値となります。

  判定条件 取得されたアラームの状態が異常しきい値の文字列と異なる場合に正常とみなします。異常・警告しきい値には文字列のみ入力可能です。デフォルト値は"FIRING"です。

  パラメータ

パラメータ名	説明
コンパートメント	監視するリソースが所属するコンパートメントIDまたはコンパートメント名を指定します。省略可能です。省略の場合、認
定義名	アラーム定義名を指定します。省略可です。
フリーフォームタグ	監視対象をフィルタする条件としてフリーフォームタグを指定することが可能です。【タグ名=値】の形式で指定して下さい。
定義済みタグ	監視対象をフィルタする条件として定義済みタグを指定することが可能です。【ネームスペース:タグ名=値】の形式で指定
認証ファイル	ユーザーのAPIキーを指定することが可能です。絶対パスでAPIキー認証ファイル名を指定して下さい。省略可能です。

備考 ※1　同じタグを複数指定した場合は後勝ちです。

- OCI:メトリクス監視

  説明 指定したメトリクスの情報を取得します

  判定条件 「計算式の変数の値」で指定した「メトリックネームスペース:メトリック」から取得したメトリクス値の判定条件を指定して下さい。

  パラメータ

パラメータ名	説明
コンパートメント	監視するリソースが所属するコンパートメントIDまたはコンパートメント名を指定します。省略不可です。
統計	取得するメトリクスの統計を候補から選択します。「計算式の変数Aの値」と合わせた統計を指定して下さい。省略不
ディメンション	監視対象をフィルタする条件としてディメンションを指定することが可能です。【項目名=値】で条件を指定して下さい。
フリーフォームタグ	監視対象をフィルタする条件としてフリーフォームタグを指定することが可能です。【タグ名=値】の形式で指定して下さ
定義済みタグ	監視対象をフィルタする条件として定義済みタグを指定することが可能です。【ネームスペース:タグ名=値】の形式で指
表示ディメンション名	監視結果の監視対象として表示する表示ディメンション名を指定します。省略可能です。
認証ファイル	ユーザーのAPIキーを指定することが可能です。絶対パスでAPIキー認証ファイル名を指定して下さい。省略可能です
ゼロパブリッシュ	検査間隔内にデータポイントが無かった場合に取得データの値を「0」とする場合にONを指定します。省略可能です。

  備考 ※1　同じタグを複数指定した場合は後勝ちです。

  注釈

  ゼロパブリッシュがONの場合は、監視間隔でデータポイントの有無に変化があると、監視結果の状態にかかわらずメッセージモニタにメッセージが通知されます。

- OCI:Logging ログ情報取得

  説明 ロギングのログ情報を監視します。取得データは成否となります。

  判定条件 ログ収集に失敗した場合、異常となります。ログの件数が多く、ログを取得し切れなかった場合、警告となります。異常・警告しきい値は変更しないで下さい。

  パラメータ

パラメータ名	説明
コンパートメント	ログが所属するコンパートメントIDまたはコンパートメント名を指定します。省略不可です。
ロググループ	ログが所属するロググループIDまたはロググループ名を指定します。省略可能です。(ログIDが入力される場合、省略不可て
ログ	ログが所属するログIDまたはログ名を指定します。省略可能です。
フィルタ条件	where条件を指定します。省略可能です。(※1)
認証ファイル	ユーザーのAPIキーを指定することが可能です。絶対パスでAPIキー認証ファイル名を指定して下さい。省略可能です。
ログファイル	収集したログ情報の出力先ログファイルを指定することが可能です。絶対パスでログ出力ファイル名を指定して下さい。省略
ログフォーマット	取得したログの出力フォーマットをLTSVもしくはJSONに切り替えます。デフォルト値はLTSVとなります。省略可能です。

  備考 ※1　フィルタ条件には、サーチ対象となるLog Streamは指定不可です。where条件以降のみ指定可能です。例:
  "type='com.oraclecloud.logging.custom.linuxcustomlog'"
  また、「'」などの記号や「スペース」を含む場合は、「"」で囲む必要があります。「"」を含む場合は、「\」でエスケープする必要があります。
  記述方法は下記Oracleのサイトをご参照下さい。
  参考URL:https://docs.oracle.com/en-us/iaas/Content/Logging/Reference/query_language_specification.htm

  注釈

  - OCI:Logging ログ情報取得では、最後に取得したログのタイムスタンプよりlogBufferTimeに指定した分数遡ってログを取得します。監視タスクの新規作成時などの最後に取得したログが無い場合は「監視間隔＋logBufferTime＋5分」以内に発生したログを取得します。
    Oracle Cloud Infrastructure Logging では、発生したログが Oracle Cloud Infrastructure Logging 上に現れるまでに時間がかかる場合があります。その時間が監視間隔以上かかる場合、ログが取得されない状態となります。このような場合は、logBufferTimeを適切に設定して下さい。
  - Oracle Cloud Infrastructure Logging から取得可能なログは14日前までです。
  - 前回のログ取得が14日以前の場合、メッセージモニタに警告メッセージ「「Period between start time and end time cannot be more than 14 days」が通知されます。
  - 監視間隔時間内で最新のログまで取得されなかった場合、メッセージモニタに警告メッセージ「OCI logs cannot get to the latest」が通知されます。

- OCI:Streaming ログ情報取得

  説明 Streamingのログ情報を監視します。取得データは成否となります。

  判定条件 ログ収集に失敗した場合、異常となります。ログの件数が多く、ログを取得し切れなかった場合、警告となります。異常・警告しきい値は変更しないで下さい。

  パラメータ

パラメータ名	説明
ストリームID	ストリームIDを指定します。省略不可です。
エンドポイントリージョン	エンドポイントのリージョンを指定します。省略不可です。
認証ファイル	ユーザーのAPIキーを指定することが可能です。絶対パスでAPIキー認証ファイル名を指定して下さい。省略可能て
ログファイル	収集したログ情報の出力先ログファイルを指定することが可能です。絶対パスでログ出力ファイル名を指定して下さい
ログフォーマット	取得したログの出力フォーマットをLTSVもしくはJSONに切り替えます。デフォルト値はLTSVとなります。省略可能て

  注釈

  - OCI:Streaming ログ情報取得では、最後に取得したログのタイムスタンプよりlogBufferTimeに指定した分数遡ってログを取得します。監視タスクの新規作成時などの最後に取得したログが無い場合は「監視間隔＋logBufferTime＋5分」以内に発生したログを取得します。
    OCI Streaming では、発生したログが OCI Streaming 上に現れるまでに時間がかかる場合があります。その時間が監視間隔以上かかる場合、ログが取得されない状態となります。このような場合は、logBufferTimeを適切に設定して下さい。
  - 前回のログ取得が保存期間以前の場合、メッセージモニタに警告メッセージ「「Period between start time and end time cannot be more than retentionInHours」が通知されます。
  - 監視間隔時間内で最新のログまで取得されなかった場合、メッセージモニタに警告メッセージ「OCI streaming logs cannot get to the latest」が通知されます。

- OCI:Data Guard 適用ラグ(秒)

  説明 Data Guardの適用ラグを監視します。取得データは瞬間値となります。

  判定条件 取得されたOCI Data Guardの適用ラグが異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
データベースID	監視するData Guardのデータベースを指定します。省略不可です。
認証ファイル	ユーザーのAPIキーを指定することが可能です。絶対パスでAPIキー認証ファイル名を指定して下さい。省略可能です。

- OCI:Data Guard 適用レート(KB/秒)

  説明 Data Guardの適用レートを監視します。取得データは瞬間値となります。

  判定条件 取得されたOCI Data Guardの適用レートが異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
データベースID	監視するData Guardのデータベースを指定します。省略不可です。
認証ファイル	ユーザーのAPIキーを指定することが可能です。絶対パスでAPIキー認証ファイル名を指定して下さい。省略可能です。

- OCI:Data Guard ライフサイクル状態

  説明 Data Guardのライフサイクル状態を監視します。取得データは瞬間値となります。

  判定条件 取得されたData Guardのライフサイクル状態がAVAILABLE、UPDATINGと異なる場合に異常とみなします。異常・警告しきい値には文字列のみ入力可能です。
  ライフサイクル状態の出力する文字列は、以下の7つの状態になります。
  ・PROVISIONING
  ・AVAILABLE
  ・UPDATING
  ・TERMINATING
  ・TERMINATED

・FAILED
・UPGRADING

パラメータ

パラメータ名	説明
データベースID	監視するData Guardのデータベースを指定します。省略不可です。
認証ファイル	ユーザーのAPIキーを指定することが可能です。絶対パスでAPIキー認証ファイル名を指定して下さい。省略可能です。

- OCI:サービス制限監視

  説明 指定したサービス制限を監視します。取得データは瞬間値となります。

  判定条件 取得された使用率（使用量/サービス制限*100）の値が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
コンパートメントID(ルート)	サービス制限情報を監視したいルートのコンパートメントIDを指定します。省略不可です。
リージョン	サービス制限情報を監視したいリージョンを指定します。省略可能です。
認証ファイル	ユーザーのAPIキーを指定することが可能です。絶対パスでAPIキー認証ファイル名を指定して下さい。省略可能

- OCI:メトリクス監視(MQL)

  説明 MQLファイルで指定したメトリクスの情報を取得します。取得データは瞬間値となります。

  判定条件 取得されたメトリクス値が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
コンパートメント	監視するリソースが所属するコンパートメントIDまたはコンパートメント名を指定します。省略不可です。
ネームスペース	監視するメトリクスのネームスペースを指定します。省略不可です。
フリーフォームタグ	監視対象をフィルタする条件としてフリーフォームタグを指定することが可能です。【タグ名=値】の形式で指定して下さ
定義済みタグ	監視対象をフィルタする条件として定義済みタグを指定することが可能です。【ネームスペース:タグ名=値】の形式で指
表示ディメンション名	監視結果の監視対象として表示する表示ディメンション名を指定します。省略可能です。
認証ファイル	ユーザーのAPIキーを指定することが可能です。絶対パスでAPIキー認証ファイル名を指定して下さい。省略可能です
ゼロパブリッシュ	検査間隔内にデータポイントが無かった場合に取得データの値を「0」とする場合にONを指定します。省略可能です。
MQLファイル	Monitoring Query Language (MQL)式を記載したテキストファイル名を絶対パスで指定します。省略不可です。(※

  備考 ※1　同じタグを複数指定した場合は後勝ちです。
  　※2　MQLファイルにはMQL式のみを記載してください。間隔値は文字列「%SjISM_CheckINT%」で指定してください。MQLファイルの内容は一行書きにしてください。複数行記載した場合、一行目の内容だけ使用されます。
  記載例：　"DiskBytesWritten[%SjISM_CheckINT%].mean() + DiskBytesRead[%SjISM_CheckINT%].mean()"。

  注釈

  ゼロパブリッシュがONの場合は、監視間隔でデータポイントの有無に変化があると、監視結果の状態にかかわらずメッセージモニタにメッセージが通知されます。

- OCI:Analytics インスタンス状態

  説明 Analyticsインスタンス状態を取得します。取得データは瞬間値となります。

  判定条件 取得されたAnalyticsインスタンス状態がACTIVE、CREATING、UPDATINGと異なる場合に異常とみなします。異常・警告しきい値には文字列のみ入力可能です。
  インスタンス状態の出力する文字列は、以下の7つの状態になります。
  ・ACTIVE
  ・CREATING
  ・DELETED
  ・DELETING
  ・FAILED
  ・INACTIVE
  ・UPDATING

パラメータ

パラメータ名	説明
コンパートメント	監視するAnalyticsインスタンスが所属するコンパートメントIDまたはコンパートメント名を指定します。省略不可です。
インスタンス名	監視するAnalyticsインスタンス名を指定します。省略可能です。省略した場合はコンパートメント内すべてのインスタンス情
認証ファイル	ユーザーのAPIキーを指定することが可能です。絶対パスでAPIキー認証ファイル名を指定して下さい。省略可能です。

- OCI:リソース一覧取得

  説明 OCIリソース一覧を取得します。取得データは成否となります。

  判定条件 ログ収集に失敗した場合、異常となります。ログの件数が多く、ログを取得し切れなかった場合、警告となります。異常・警告しきい値は変更しないで下さい。

  パラメータ

パラメータ名	説明
region	取得先のリージョンを指定します。省略不可です。
フィールドネーム	クエリのフィールドネームをカンマ区切りで指定します。省略可能です。省略した場合は「displayName,resourceTyp
リソースタイプ	クエリのリソースタイプをカンマ区切りで指定します。省略可能です。省略した場合は「all」となります。
クエリ条件(Where)	クエリのwhere条件を指定します。省略可能です。where条件にはwhereキーも含めて指定してください。(例:where
ファイルフォーマット	取得したリソース情報の出力フォーマットをLTSVもしくはJSONに切り替えます。デフォルト値はLTSVとなります。省略
リソース一覧ファイル	収集したリソース情報の出力先ファイルを指定することが可能です。絶対パスで出力ファイル名を指定して下さい。省略
クエリファイル	クエリ文をファイル形式で指定することが可能です。絶対パスでクエリファイル名を指定して下さい。省略可能です。クエ
認証ファイル	ユーザーのAPIキーを指定することが可能です。絶対パスでAPIキー認証ファイル名を指定して下さい。省略可能です

  備考 ※1 クエリファイルで指定する場合、フィールドを絞りたい場合はクエリファイル内に書くのではなく、フィールドネームパラメータに指定してください。

  フィールドネームに指定可能な名称

番号	フィールド名
1	displayName
2	resourceType
3	identifier(リソースのOCID)
4	compartmentId
5	timeCreated
6	availabilityDomain
7	lifecycleState
8	freeformTags
9	definedTags
10	systemTags
11	searchContext
12	identityContext
13	additionalDetails

2.8.1.5. IBM Cloud監視

注釈

メトリクス監視項目の監視間隔は1分、10分、60分、1440分(1日)のみ指定可能です。

参考

各種パラメータの設定値が分からない場合は、IBM Cloudより提供されているIBM Cloud Monitoring Web UI にて確認して下さい。

- IBM Cloud:Virtual Servers 平均CPU使用率(%)

  説明 IBM Cloud Virtual Servers インスタンスの平均CPU使用率を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたIBM Cloud Virtual Servers インスタンスの平均CPU使用率が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は%です。

パラメータ

パラメータ名	説明
ラベル	監視結果の監視対象として表示するメトリクスラベルを指定します。省略不可です。
フィルター	監視対象をフィルタする条件としてラベルを指定することが可能です。【ラベル名=値】の形式で指定して下さい。省略可能
ゼロパブリッシュ	検査間隔内にデータポイントが無かった場合に取得データの値を「0」とする場合にONを指定します。省略可能です。省略
認証ファイルパス	ユーザーのAPIキーを指定することが可能です。絶対パスでIBM Cloud情報設定ファイル名を指定して下さい。省略可能

- IBM Cloud：Cloud Foundry アプリケーションCPU使用率(%)

  説明 Cloud Foundry アプリケーションのCPU 使用率を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたCloud Foundry アプリケーションのCPU 使用率が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は%です。

  パラメータ

パラメータ名	説明
ラベル	監視結果の監視対象として表示するメトリクスラベルを指定します。省略不可です。
フィルター	監視対象をフィルタする条件としてラベルを指定することが可能です。【ラベル名=値】の形式で指定して下さい。省略可能
ゼロパブリッシュ	検査間隔内にデータポイントが無かった場合に取得データの値を「0」とする場合にONを指定します。省略可能です。省略
認証ファイルパス	ユーザーのAPIキーを指定することが可能です。絶対パスでIBM Cloud情報設定ファイル名を指定して下さい。省略可能

- IBM Cloud：Cloudant レート制限された操作の数

  説明 IBM Cloudant のレート制限された操作の数を監視します。取得データは検査間隔期間内の最大値となります。

  判定条件 取得されたIBM Cloudant のレート制限された操作の数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
ラベル	監視結果の監視対象として表示するメトリクスラベルを指定します。省略不可です。
フィルター	監視対象をフィルタする条件としてラベルを指定することが可能です。【ラベル名=値】の形式で指定して下さい。省略可能
ゼロパブリッシュ	検査間隔内にデータポイントが無かった場合に取得データの値を「0」とする場合にONを指定します。省略可能です。省略
認証ファイルパス	ユーザーのAPIキーを指定することが可能です。絶対パスでIBM Cloud情報設定ファイル名を指定して下さい。省略可能

- IBM Cloud：Databases for PostgresSQL 5分間の平均入出力使用率(%)

  説明 Databases for PostgresSQL の入出力使用率を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたDatabases for PostgresSQL の入出力使用率が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は%です。

  パラメータ

パラメータ名	説明
ラベル	監視結果の監視対象として表示するメトリクスラベルを指定します。省略不可です。
フィルター	監視対象をフィルタする条件としてラベルを指定することが可能です。【ラベル名=値】の形式で指定して下さい。省略可能
ゼロパブリッシュ	検査間隔内にデータポイントが無かった場合に取得データの値を「0」とする場合にONを指定します。省略可能です。省略
認証ファイルパス	ユーザーのAPIキーを指定することが可能です。絶対パスでIBM Cloud情報設定ファイル名を指定して下さい。省略可能

- IBM Cloud：Databases for PostgresSQL インスタンスのCPU使用率(%)

  説明 Databases for PostgresSQL インスタンスのCPU使用率 (%) を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたDatabases for PostgresSQL インスタンスのCPU使用率が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は%です。

  パラメータ

パラメータ名	説明
ラベル	監視結果の監視対象として表示するメトリクスラベルを指定します。省略不可です。
フィルター	監視対象をフィルタする条件としてラベルを指定することが可能です。【ラベル名=値】の形式で指定して下さい。省略可能
ゼロパブリッシュ	検査間隔内にデータポイントが無かった場合に取得データの値を「0」とする場合にONを指定します。省略可能です。省略
認証ファイルパス	ユーザーのAPIキーを指定することが可能です。絶対パスでIBM Cloud情報設定ファイル名を指定して下さい。省略可能

- IBM Cloud：Databases for Redis 5分間の平均入出力使用率(%)

  説明 Databases for Redis の入出力平均使用率を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたDatabases for Redis の入出力平均使用率が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は%です。

  パラメータ

パラメータ名	説明
ラベル	監視結果の監視対象として表示するメトリクスラベルを指定します。省略不可です。
フィルター	監視対象をフィルタする条件としてラベルを指定することが可能です。【ラベル名=値】の形式で指定して下さい。省略可能
ゼロパブリッシュ	検査間隔内にデータポイントが無かった場合に取得データの値を「0」とする場合にONを指定します。省略可能です。省略
認証ファイルパス	ユーザーのAPIキーを指定することが可能です。絶対パスでIBM Cloud情報設定ファイル名を指定して下さい。省略可能

- IBM Cloud：Databases for Redis インスタンスのCPU使用率(%)

  説明 Databases for Redis インスタンスのCPU使用率 (%) を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたDatabases for Redis インスタンスのCPU使用率が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は%です。

  パラメータ

パラメータ名	説明
ラベル	監視結果の監視対象として表示するメトリクスラベルを指定します。省略不可です。
フィルター	監視対象をフィルタする条件としてラベルを指定することが可能です。【ラベル名=値】の形式で指定して下さい。省略可能
ゼロパブリッシュ	検査間隔内にデータポイントが無かった場合に取得データの値を「0」とする場合にONを指定します。省略可能です。省略
認証ファイルパス	ユーザーのAPIキーを指定することが可能です。絶対パスでIBM Cloud情報設定ファイル名を指定して下さい。省略可能

- IBM Cloud：Databases for etcd 5分間の平均入出力使用率(%)

  説明 Databases for etcd の入出力平均使用率を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたDatabases for etcd の入出力平均使用率が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は%です。

  パラメータ

パラメータ名	説明
ラベル	監視結果の監視対象として表示するメトリクスラベルを指定します。省略不可です。
フィルター	監視対象をフィルタする条件としてラベルを指定することが可能です。【ラベル名=値】の形式で指定して下さい。省略可能
ゼロパブリッシュ	検査間隔内にデータポイントが無かった場合に取得データの値を「0」とする場合にONを指定します。省略可能です。省略
認証ファイルパス	ユーザーのAPIキーを指定することが可能です。絶対パスでIBM Cloud情報設定ファイル名を指定して下さい。省略可能

- IBM Cloud：Databases for etcd インスタンスのCPU使用率(%)

  説明 Databases for etcd インスタンスのCPU使用率 (%) を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたDatabases for etcd インスタンスのCPU使用率が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は%です。

  パラメータ

パラメータ名	説明
ラベル	監視結果の監視対象として表示するメトリクスラベルを指定します。省略不可です。
フィルター	監視対象をフィルタする条件としてラベルを指定することが可能です。【ラベル名=値】の形式で指定して下さい。省略可能
ゼロパブリッシュ	検査間隔内にデータポイントが無かった場合に取得データの値を「0」とする場合にONを指定します。省略可能です。省略
認証ファイルパス	ユーザーのAPIキーを指定することが可能です。絶対パスでIBM Cloud情報設定ファイル名を指定して下さい。省略可能

- IBM Cloud：Databases for Elasticsearch 5分間の平均入出力使用率(%)

  説明 Databases for Elasticsearch の入出力平均使用率を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたDatabases for Elasticsearch の入出力平均使用率が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は%です。

  パラメータ

パラメータ名	説明
ラベル	監視結果の監視対象として表示するメトリクスラベルを指定します。省略不可です。
フィルター	監視対象をフィルタする条件としてラベルを指定することが可能です。【ラベル名=値】の形式で指定して下さい。省略可能
ゼロパブリッシュ	検査間隔内にデータポイントが無かった場合に取得データの値を「0」とする場合にONを指定します。省略可能です。省略
認証ファイルパス	ユーザーのAPIキーを指定することが可能です。絶対パスでIBM Cloud情報設定ファイル名を指定して下さい。省略可能

- IBM Cloud：Databases for Elasticsearch インスタンスのCPU使用率(%)

  説明 Databases for Elasticsearch インスタンスのCPU使用率 (%) を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたDatabases for Elasticsearch インスタンスのCPU使用率が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は%です。

  パラメータ

パラメータ名	説明
ラベル	監視結果の監視対象として表示するメトリクスラベルを指定します。省略不可です。
フィルター	監視対象をフィルタする条件としてラベルを指定することが可能です。【ラベル名=値】の形式で指定して下さい。省略可能
ゼロパブリッシュ	検査間隔内にデータポイントが無かった場合に取得データの値を「0」とする場合にONを指定します。省略可能です。省略
認証ファイルパス	ユーザーのAPIキーを指定することが可能です。絶対パスでIBM Cloud情報設定ファイル名を指定して下さい。省略可能

- IBM Cloud：Databases for MongoDB 5分間の平均入出力使用率(%)

  説明 Databases for MongoDB の入出力平均使用率を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたDatabases for MongoDB の入出力平均使用率が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は%です。

  パラメータ

パラメータ名	説明
ラベル	監視結果の監視対象として表示するメトリクスラベルを指定します。省略不可です。
フィルター	監視対象をフィルタする条件としてラベルを指定することが可能です。【ラベル名=値】の形式で指定して下さい。省略可能
ゼロパブリッシュ	検査間隔内にデータポイントが無かった場合に取得データの値を「0」とする場合にONを指定します。省略可能です。省略
認証ファイルパス	ユーザーのAPIキーを指定することが可能です。絶対パスでIBM Cloud情報設定ファイル名を指定して下さい。省略可能

- IBM Cloud：Databases for MongoDB インスタンスのCPU使用率(%)

  説明 Databases for MongoDB インスタンスのCPU使用率 (%) を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたDatabases for MongoDB インスタンスのCPU使用率が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は%です。

  パラメータ

パラメータ名	説明
ラベル	監視結果の監視対象として表示するメトリクスラベルを指定します。省略不可です。
フィルター	監視対象をフィルタする条件としてラベルを指定することが可能です。【ラベル名=値】の形式で指定して下さい。省略可能
ゼロパブリッシュ	検査間隔内にデータポイントが無かった場合に取得データの値を「0」とする場合にONを指定します。省略可能です。省略
認証ファイルパス	ユーザーのAPIキーを指定することが可能です。絶対パスでIBM Cloud情報設定ファイル名を指定して下さい。省略可能

- IBM Cloud：Messages for RabbitMQ 5分間の平均入出力使用率(%)

  説明 Messages for RabbitMQ の入出力平均使用率を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたMessages for RabbitMQ の入出力平均使用率が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は%です。

  パラメータ

パラメータ名	説明
ラベル	監視結果の監視対象として表示するメトリクスラベルを指定します。省略不可です。
フィルター	監視対象をフィルタする条件としてラベルを指定することが可能です。【ラベル名=値】の形式で指定して下さい。省略可能
ゼロパブリッシュ	検査間隔内にデータポイントが無かった場合に取得データの値を「0」とする場合にONを指定します。省略可能です。省略
認証ファイルパス	ユーザーのAPIキーを指定することが可能です。絶対パスでIBM Cloud情報設定ファイル名を指定して下さい。省略可能

- IBM Cloud：Messages for RabbitMQ インスタンスのCPU使用率(%)

  説明 Messages for RabbitMQ インスタンスのCPU使用率 (%) を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたMessages for RabbitMQ インスタンスのCPU使用率が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位は%です。

  パラメータ

パラメータ名	説明
ラベル	監視結果の監視対象として表示するメトリクスラベルを指定します。省略不可です。
フィルター	監視対象をフィルタする条件としてラベルを指定することが可能です。【ラベル名=値】の形式で指定して下さい。省略可能
ゼロパブリッシュ	検査間隔内にデータポイントが無かった場合に取得データの値を「0」とする場合にONを指定します。省略可能です。省略
認証ファイルパス	ユーザーのAPIキーを指定することが可能です。絶対パスでIBM Cloud情報設定ファイル名を指定して下さい。省略可能

- IBM Cloud：Event Streams 秒当たりのインスタンスへのバイト数(byte)

  説明 Event Streams インスタンスへの秒当たりにプロデュースされたバイト数を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたEvent Streams インスタンスへの秒当たりにプロデュースされたバイト数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はbyteです。

  パラメータ

パラメータ名	説明
ラベル	監視結果の監視対象として表示するメトリクスラベルを指定します。省略不可です。
フィルター	監視対象をフィルタする条件としてラベルを指定することが可能です。【ラベル名=値】の形式で指定して下さい。省略可能
ゼロパブリッシュ	検査間隔内にデータポイントが無かった場合に取得データの値を「0」とする場合にONを指定します。省略可能です。省略
認証ファイルパス	ユーザーのAPIキーを指定することが可能です。絶対パスでIBM Cloud情報設定ファイル名を指定して下さい。省略可能

- IBM Cloud：Event Streams 秒当たりのインスタンスからのバイト数(byte)

  説明 Event Streams インスタンスからの秒当たりにコンシュームされたバイト数を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたEvent Streams インスタンスからの秒当たりにコンシュームされたバイト数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はbyteです。

  パラメータ

パラメータ名	説明
ラベル	監視結果の監視対象として表示するメトリクスラベルを指定します。省略不可です。
フィルター	監視対象をフィルタする条件としてラベルを指定することが可能です。【ラベル名=値】の形式で指定して下さい。省略可能
ゼロパブリッシュ	検査間隔内にデータポイントが無かった場合に取得データの値を「0」とする場合にONを指定します。省略可能です。省略
認証ファイルパス	ユーザーのAPIキーを指定することが可能です。絶対パスでIBM Cloud情報設定ファイル名を指定して下さい。省略可能

- IBM Cloud：Load Balancer 接続率

  説明 Load Balancer 接続レートは、ご使用のロード・バランサーに対する 1 秒当たりの新規着信アクティブ接続の数を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたロード・バランサーに対する 1 秒当たりの新規着信アクティブ接続数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
ラベル	監視結果の監視対象として表示するメトリクスラベルを指定します。省略不可です。
フィルター	監視対象をフィルタする条件としてラベルを指定することが可能です。【ラベル名=値】の形式で指定して下さい。省略可能
ゼロパブリッシュ	検査間隔内にデータポイントが無かった場合に取得データの値を「0」とする場合にONを指定します。省略可能です。省略
認証ファイルパス	ユーザーのAPIキーを指定することが可能です。絶対パスでIBM Cloud情報設定ファイル名を指定して下さい。省略可能

- IBM Cloud：Load Balancer for VPC 接続率

  説明 Load Balancer for VPC 接続レートは、ご使用のロード・バランサーに対する 1 秒当たりの新規着信アクティブ接続の数を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたロード・バランサーに対する 1 秒当たりの新規着信アクティブ接続数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
ラベル	監視結果の監視対象として表示するメトリクスラベルを指定します。省略不可です。
フィルター	監視対象をフィルタする条件としてラベルを指定することが可能です。【ラベル名=値】の形式で指定して下さい。省略可能
ゼロパブリッシュ	検査間隔内にデータポイントが無かった場合に取得データの値を「0」とする場合にONを指定します。省略可能です。省略
認証ファイルパス	ユーザーのAPIキーを指定することが可能です。絶対パスでIBM Cloud情報設定ファイル名を指定して下さい。省略可能

- IBM Cloud：Object Storage 使用するバイト数

  説明 Object Storage の使用バイト数を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたObject Storage の使用バイト数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。単位はbyteです。

  パラメータ

パラメータ名	説明
ラベル	監視結果の監視対象として表示するメトリクスラベルを指定します。省略不可です。
フィルター	監視対象をフィルタする条件としてラベルを指定することが可能です。【ラベル名=値】の形式で指定して下さい。省略可能
ゼロパブリッシュ	検査間隔内にデータポイントが無かった場合に取得データの値を「0」とする場合にONを指定します。省略可能です。省略
認証ファイルパス	ユーザーのAPIキーを指定することが可能です。絶対パスでIBM Cloud情報設定ファイル名を指定して下さい。省略可能

- IBM Cloud：Object Storage オブジェクト数

  説明 Object Storage のオブジェクト数を監視します。取得データは検査間隔期間内の平均値となります。

  判定条件 取得されたObject Storage のオブジェクト数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
ラベル	監視結果の監視対象として表示するメトリクスラベルを指定します。省略不可です。
フィルター	監視対象をフィルタする条件としてラベルを指定することが可能です。【ラベル名=値】の形式で指定して下さい。省略可能
ゼロパブリッシュ	検査間隔内にデータポイントが無かった場合に取得データの値を「0」とする場合にONを指定します。省略可能です。省略
認証ファイルパス	ユーザーのAPIキーを指定することが可能です。絶対パスでIBM Cloud情報設定ファイル名を指定して下さい。省略可能

- IBM Cloud：VPN for VPC VPNゲートウェイ状況

  説明 VPN for VPC のゲートウェイ状況を監視します。1：使用可能、0：使用不可。検査間隔期間内に使用不可状態があった場合に異常と判定します。

  判定条件 取得されたVPN for VPC のゲートウェイ状況が1と異なる場合に異常とみなします。

  パラメータ

パラメータ名	説明
ラベル	監視結果の監視対象として表示するメトリクスラベルを指定します。省略不可です。
フィルター	監視対象をフィルタする条件としてラベルを指定することが可能です。【ラベル名=値】の形式で指定して下さい。省略可能
ゼロパブリッシュ	検査間隔内にデータポイントが無かった場合に取得データの値を「0」とする場合にONを指定します。省略可能です。省略
認証ファイルパス	ユーザーのAPIキーを指定することが可能です。絶対パスでIBM Cloud情報設定ファイル名を指定して下さい。省略可能

- IBM Cloud：Cloud Functions アプリケーションエラー アクティベーション数

  説明 Cloud Functions のアプリケーション・エラーに由来する失敗したアクティベーションの数を監視します。取得データは検査間隔期間内の合計値となります。

  判定条件 取得されたCloud Functions のアプリケーション・エラーに由来する失敗したアクティベーションの数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
ラベル	監視結果の監視対象として表示するメトリクスラベルを指定します。省略不可です。
フィルター	監視対象をフィルタする条件としてラベルを指定することが可能です。【ラベル名=値】の形式で指定して下さい。省略可能
ゼロパブリッシュ	検査間隔内にデータポイントが無かった場合に取得データの値を「0」とする場合にONを指定します。省略可能です。省略
認証ファイルパス	ユーザーのAPIキーを指定することが可能です。絶対パスでIBM Cloud情報設定ファイル名を指定して下さい。省略可能

- IBM Cloud：Cloud Functions デベロッパーエラー アクティベーション数

  説明 Cloud Functions の開発者に由来する失敗したアクティベーションの数を監視します。取得データは検査間隔期間内の合計値となります。

  判定条件 取得されたCloud Functions の開発者に由来する失敗したアクティベーションの数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
ラベル	監視結果の監視対象として表示するメトリクスラベルを指定します。省略不可です。
フィルター	監視対象をフィルタする条件としてラベルを指定することが可能です。【ラベル名=値】の形式で指定して下さい。省略可能
ゼロパブリッシュ	検査間隔内にデータポイントが無かった場合に取得データの値を「0」とする場合にONを指定します。省略可能です。省略
認証ファイルパス	ユーザーのAPIキーを指定することが可能です。絶対パスでIBM Cloud情報設定ファイル名を指定して下さい。省略可能

- IBM Cloud：Cloud Functions 内部エラー アクティベーション数

  説明 Cloud Functions の内部エラーに由来する失敗したアクティベーションの数を監視します。取得データは検査間隔期間内の合計値となります。

  判定条件 取得されたCloud Functions の内部エラーに由来する失敗したアクティベーションの数が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
ラベル	監視結果の監視対象として表示するメトリクスラベルを指定します。省略不可です。
フィルター	監視対象をフィルタする条件としてラベルを指定することが可能です。【ラベル名=値】の形式で指定して下さい。省略可能
ゼロパブリッシュ	検査間隔内にデータポイントが無かった場合に取得データの値を「0」とする場合にONを指定します。省略可能です。省略
認証ファイルパス	ユーザーのAPIキーを指定することが可能です。絶対パスでIBM Cloud情報設定ファイル名を指定して下さい。省略可能

- IBM Cloud：メトリクス監視

  説明 指定したメトリクスの情報を取得します

  判定条件 判定条件は自由に指定できます。

  パラメータ

パラメータ名	説明
ラベル	監視結果の監視対象として表示するメトリクスラベルを指定します。省略不可です。
統計	取得するメトリクスの統計を候補から選択します。「計算式の変数Aの値」と合わせた統計を指定して下さい。省略不可で
フィルター	監視対象をフィルタする条件としてラベルを指定することが可能です。【ラベル名=値】の形式で指定して下さい。省略可能
ゼロパブリッシュ	検査間隔内にデータポイントが無かった場合に取得データの値を「0」とする場合にONを指定します。省略可能です。省略
認証ファイルパス	ユーザーのAPIキーを指定することが可能です。絶対パスでIBM Cloud情報設定ファイル名を指定して下さい。省略可能

- IBM Cloud：Log Analysis ログ情報取得

  説明 Log Analysisのログ情報を監視します。取得データは成否となります。

  判定条件 ログ収集に失敗した場合、異常となります。異常・警告しきい値は変更しないで下さい。

  パラメータ

パラメータ名	説明
ホスト名	ログが所属するホストを指定します。省略可能です。(指定方式：host1，host2...)
アプリケーション名	ログが所属するアプリケーションを指定します。省略可能です。(指定方式：app1，app2...)
レベル	取得するログレベルを指定します。省略可能です。(指定方式：level1，level2...)
クエリ	ログ情報取得するクエリを指定します。省略可能です。
タグ	エージェントを識別するタグのキーを指定します。省略可能です。(指定方式：tag1，tag2...)
認証ファイル	絶対パスでIBM Cloudの認証ファイル名を指定して下さい。省略可能です。
ログ出力ファイル	収集したログ情報の出力先ログファイルを指定することが可能です。絶対パスでログ出力ファイル名を指定して下さい。省
ログフォーマット	取得したログの出力フォーマットをLTSVもしくはJSONに切り替えます。デフォルト値はLTSVとなります。省略可能です。

  備考 IBM Cloud Log Analysis連携機能については、IBM Cloud Log Analysis連携機能 を参照して下さい。
  クエリを指定する際にtag:k8s、host:[extlinunit,calico-node-xmldq]、host:extlinunit tag:mytagなどの指定方法があります。
  また、「｜」などの記号や「スペース」を含む場合は、「"」で囲む必要があります。「"」を含む場合は、「\」でエスケープする必要があります。
  クエリの記述方法はlogdnaのサイトをご参照下さい。参考URL：https://docs.logdna.com/docs/search

  注釈

  - IBM Cloud：Log Analysis ログ情報取得では、最後に取得したログのタイムスタンプよりlogBufferTimeに指定した分数遡ってログを取得します。監視タスクの新規作成時などの最後に取得したログが無い場合は「監視間隔＋logBufferTime＋5分」以内に発生したログを取得します。
    IBM Cloud Log Analysis では、発生したログが IBM Cloud Log Analysis 上に現れるまでに時間がかかる場合があります。その時間が監視間隔以上かかる場合、ログが取得されない状態となります。このような場合は、logBufferTimeを適切に設定して下さい。
  - 監視間隔時間内で最新のログまで取得されなかった場合、メッセージモニタに警告メッセージ「IBM Cloud logs cannot get to the latest」が通知されます。

- IBM Cloud：アカウント利用料金

  説明 アカウントの利用料金を監視します。取得データは瞬間値となります。

  判定条件 取得された利用料金が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
先月/当月フラグ(P/T)	利用料金の取得範囲を先月(P)か当月(T)か切り替えます。デフォルト値は当月(T)となります。省略不可です。
アカウントID	使用量を監視するアカウントIDを指定します。省略不可です。
認証ファイル	絶対パスでIBM Cloudの認証ファイル名を指定して下さい。省略可能です。

- IBM Cloud：サービス利用料金

  説明 サービスの利用料金を監視します。取得データは瞬間値となります。

  判定条件 取得された利用料金が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
先月/当月フラグ(P/T)	利用料金の取得範囲を先月(P)か当月(T)か切り替えます。デフォルト値は当月(T)となります。省略不可です。
アカウントID	使用量を監視するアカウントIDを指定します。省略不可です。
認証ファイル	絶対パスでIBM Cloudの認証ファイル名を指定して下さい。省略可能です。

- IBM Cloud：リソースグループ利用料金

  説明 リソースグループの利用料金を監視します。取得データは瞬間値となります。

  判定条件 取得された利用料金が異常しきい値より大きい場合に異常とみなします。異常・警告しきい値には数値のみ入力可能です。

  パラメータ

パラメータ名	説明
先月/当月フラグ(P/T)	利用料金の取得範囲を先月(P)か当月(T)か切り替えます。デフォルト値は当月(T)となります。省略不可です。
アカウントID	使用量を監視するアカウントIDを指定します。省略不可です。
リソースグループID	リソースグループIDを指定します。省略可能です。
認証ファイル	絶対パスでIBM Cloudの認証ファイル名を指定して下さい。省略可能です。

注釈

- デフォルトのタイムアウト時間で料金が取得できない場合、タイムアウト時間を延ばして下さい。
- 月初めに対象データが取得できなくてエラーが発生する可能性が有りますので、リトライ回数を延ばして下さい。
- タイムアウト時間、リトライ回数の設定方法については、IBM Cloud情報設定ファイル(sj_ibc_sys.json)の作成 を参照して下さい。

2.8.2. API利用状況

2.8.2.1. AWS

監視項目名	モジュール名	利用API
AWS：EC2 AWS：EBS AWS：ELB AWS：SQS AWS：RDS AWS：SNS AWS：EMR AWS：S3 AWS：CW AWS：Billing AWS：API Gateway AWS：CloudFront AWS：Events AWS：Logs AWS：DX AWS：DynamoDB AWS：ECS AWS：EFS AWS：Lambda AWS：Route 53 AWS：NATGateway AWS：VPN	sjANM_getAwsCWM	CloudWatchAPI.getMetricStatistics CloudWatchAPI.listMetrics EC2API.DescribeVolumes EC2API.DescribeInstances EC2API.DescribeRegions CloudWatchAPI.describeAlarms CloudWatchAPI.describeAlarmHistory AWSCredentials
AWS：EC2	sjANM_getAwsEC2	EC2API.describeInstances AWSCredentials
AWS：ELB	sjANM_getAwsELB	ELBAPI.describeLoadBalancers ELBAPI.describeInstanceHealth AWSCredentials
AWS：RDS	sjANM_getAwsRDS	RDSAPI.describeDBSnapshots RDSAPI.describeDBInstances RDSAPI.describeDBClusters RDSAPI.describeDBClusterSnapshots AWSCredentials
AWS：AS	sjANM_getAwsAS	AutoScalingAPI.describeAutoScalingGroups AutoScalingAPI.describeScalingActivities AWSCredentials
AWS：CE	sjANM_getAwsCE	CostExplorerAPI.getCostAndUsage AWSCredentials
AWS：CWL	sjANM_getAwsCWLog	CloudWatchLogsAPI.filterLogEvents AWSCredentials
AWS：Health	sjANM_getAwsHealthEvents	HealthAPI.describeEvents HealthAPI.describeEventDetails HealthAPI.describeAffectedEntities AWSCredentials
AWS：Capacity	sjANM_getAwsCapacity	CloudWatchAPI.GetMetricData AWSCredentials
AWS：Athena	sjANM_getAwsAthenaLog	AthenaAPI.StartQueryExecution AthenaAPI.GetQueryResults AWSCredentials
AWS：SQS Message	sjANM_getAwsSQSMessage	AmazonSQSAPI.ReceiveMessage AmazonSQSAPI.DeleteMessage AWSCredentials

2.8.2.2. Azure

監視項目名	モジュール名	利用API
Azure: Batch Azure: Redis Cache Azure: Compute Azure: IoT Hub Azure: Event Hub Azure: Logic Apps Azure: Search Azure: SQL Database Azure: SQL Elastic Pools Azure: SQL Managed Azure: Stream Analytics Azure: Web App Azure: API Management Azure: Container Instances Azure: Kubernetes Service Azure: Azure Database for PostgreSQL Azure: Cosmos DB Azure: Load balancers Azure: Public IP Azure: ExpressRoute Azure: Storage	sjANM_getAzureMetric	Azure Monitor REST API
Azure: Log Analytics	sjANM_getAzureLogAnalytics	Log Analytics REST API
Azure: Billing	sjANM_getAzureBillingMonth sjANM_getAzureBillingDay	Azure Consumption API
Azure: Billing(EA)	sjANM_getAzureEABillingAndUsage	Azure Consumption API
Azure: Service Health	sjANM_getAzureServiceHealth	Azure Resource health REST API
Azure: Data Explorer	sjANM_getAzureDataExplorer	Azure Data Explorer REST API

2.8.2.3. Google Cloud

監視項目名	モジュール名	利用API
GCP: App Engine GCP: BigQuery GCP: Cloud Functions GCP: Cloud SQL GCP: Stackdriver Trace GCP: Compute Engine GCP: Kubernetes Engine GCP: Cloud Datastore GCP: Clould DNS GCP: Cloud Load Balancing GCP: Stackdriver Logging GCP: Stackdriver Monitoring GCP: Pub/Sub GCP: Cloud Spanner GCP: Cloud Storage	sjANM_getGcpSDM	Cloud Monitoring API
GCP: Cloud Logging	sjANM_getGcpSDL	Cloud Logging API
GCP: 利用料金	sjANM_getGcpBilling	BigQuery API

2.8.2.4. OCI

監視項目名	モジュール名	利用API
OCI: Compute OCI: Block Volume OCI: VNIC OCI: Autonomous Database OCI: Events OCI: Load Balancing OCI: FastConnect OCI: VPN Connect OCI: Notifications OCI: Object Storage OCI: Function OCI: File Storage	sjANM_getOciMEM	Monitoring API(SummarizeMetricsData)
OCI: Audit	sjANM_getOciAuditLog	Audit API(ListEvents)
OCI: Budget	sjANM_getOciBilling	Budgets API(ListBudgets)
OCI: Announcements	sjANM_getOciAnnouncements	Announcements API(GetAnnouncement)
OCI: LogAnalytics	sjANM_getOciLogAnalytics	LogAnalytics API(Query)
OCI: Alarms	sjANM_getOciAlarms	Alarms API(ListAlarms、ListAlarmsStatus)
OCI: Logging	sjANM_getOciLogging	SearchLogs API(SearchLogs)
OCI: Streaming	sjANM_getOciStreaming	Streaming API(CreateCursor、GetMessages)
OCI: Data Guard	sjANM_getOciDataGuard	Data Guard API(ListDataGuardAssociations)
OCI: Service Limits	sjANM_getOciCapacity	Service Limits API(limitsClient.GetResourceAvailability、limitsClient.l
OCI: Analytics	sjANM_getOciAnalyticsInstance	Analytics API(ListAnalyticsInstances)
OCI: Resource List	sjANM_getOciResources	SearchResources API(SearchResources)

2.8.2.5. IBM Cloud

監視項目名	モジュール名	利用API
IBM Cloud: Monitoring	sjANM_getIbcMEM	Monitoring API
IBM Cloud: Log Analysis	sjANM_getIbcLogAnalysis	Log Analysis API
IBM Cloud: 利用料金	sjANM_getIbcBilling	Usage Reports API

2.8.3. 千手コマンドの使用法

2.8.3.1. sj_countDefExt－千手定義データの定義数と上限値の参照－

- 指定形式

  ```
  sj_countDefExt [-c]
  ```

- 目的

  千手システムに登録されているExtension Packライセンス情報の確認を行うコマンドです。コマンドを実行すると各構成要素の定義数、上限値を一覧表示します。

注釈

- 本コマンドは千手マネージャノードのみで利用可能です。

- オプション

  - -c
    - オプションが指定された場合は、csv形式で出力します。
    - オプションが省略された場合は、スペースパディングでカラム幅をあわせて出力します。

- 実行結果

  - (例1) サマリ表示

```
====================================
Monitoring Information (Extension Pack)
====================================
Item                                    Current Value  Limit  Decision
Details
Monitoring Task (AWS監視)                         100   1111  OK
Monitoring Task (Azure監視)                       100   2222  OK
Monitoring Task (GCP監視)                         100   3333  OK
Monitoring Task (OCI監視)                         100   4444  OK
Monitoring Task (IBM Cloud監視)                   100   5555  OK
Monitoring Task (Docker監視)                      100   2121  OK
Monitoring Task (Kubernetes監視)                  100   2222  OK
Monitoring Task (Podman監視)                      100   2323  OK
Monitoring Task (OpenShift監視)                   100   2424  OK
Monitoring Task (外形監視)                        100   4141  OK
```

- (例2) サマリ表示(CSV形式)

```
Subsystem,Item,Current Value,Limit,Decision,Details
Monitoring,Monitoring Task (AWS監視),100,1111,OK,
Monitoring,Monitoring Task (Azure監視),100,2222,OK,
Monitoring,Monitoring Task (GCP監視),100,3333,OK,
Monitoring,Monitoring Task (OCI監視),100,4444,OK,
Monitoring,Monitoring Task (IBM Cloud監視),100,5555,OK,
Monitoring,Monitoring Task (Docker監視),100,2121,OK,
Monitoring,Monitoring Task (Kubernetes監視),100,2222,OK,
Monitoring,Monitoring Task (Podman監視),100,2323,OK,
Monitoring,Monitoring Task (OpenShift監視),100,2424,OK,
Monitoring,Monitoring Task (外形監視),100,4141,OK,
```

- 出力されたカラムの内容
  - サブシステム

    カテゴリ名が表示されます。
  - 項目

    定義情報の項目名が表示されます。
  - 現在値

    定義されている数が表示されます。
  - 上限

    定義可能な上限値(ライセンス数による上限)が表示されます。
  - 判定

    「WARN」か「OK」が表示されます。構成要素の定義数が上限値の90%以上の場合に、「WARN」が表示されます。
  - 詳細

    項目の追記事項にあたる内容が":"区切りで表示されます。
- 出力項目内容

カテゴリ	項目	内容
	AWS監視	AWS監視ライセンスの情報が出力されます。現在値/上限値と出力されます。
	Azure監視	Azure監視ライセンスの情報が出力されます。現在値/上限値と出力されます。
	Kubernetes監視	Kubernetes監視ライセンスの情報が出力されます。現在値/上限値と出力されます。
	Dokcer監視	Dokcer監視ライセンスの情報が出力されます。現在値/上限値と出力されます。
	GCP監視	Google Cloud監視ライセンスの情報が出力されます。現在値/上限値と出力されます。
	OCI監視	OCI監視ライセンスの情報が出力されます。現在値/上限値と出力されます。
	IBM Cloud監視	IBM Cloud監視ライセンスの情報が出力されます。現在値/上限値と出力されます。
	Podman監視	Podman監視ライセンスの情報が出力されます。現在値/上限値と出力されます。
	OpenShift監視	OpenShift監視ライセンスの情報が出力されます。現在値/上限値と出力されます。
	外形監視	外形監視ライセンスの情報が出力されます。現在値/上限値と出力されます。

- 標準エラー出力
  - 「パラメータ指定エラー」「Usage：sj_countDefExt [-c]」

    入力パラメータエラー時に出力されます。
  - 「環境変数(SENJUHOME)の取得に失敗しました。」

千手の環境変数取得の失敗時に出力されます。

- 終了ステータス
    - 0：正常終了
    - 1：異常終了

2.8.4. Extension Packライセンスキーの変更

ここでは、千手システムのExtension Packライセンスキーの変更方法について説明します。

2.8.4.1. Extension Packライセンスキーについて

千手システムで使用することのできるExtension Pack機能、及び有効期限は、Extension Packライセンスキーによって設定されます。登録されているExtension Packライセンスキーの有効期限の確認は、以下のように行います。

千手ブラウザのツリービューで、ドメインのエンティティを右クリックして現れるコンテキストメニューの[プロパティ]を選択すると、下記の図のようなプロパティウィンドウが開きます。

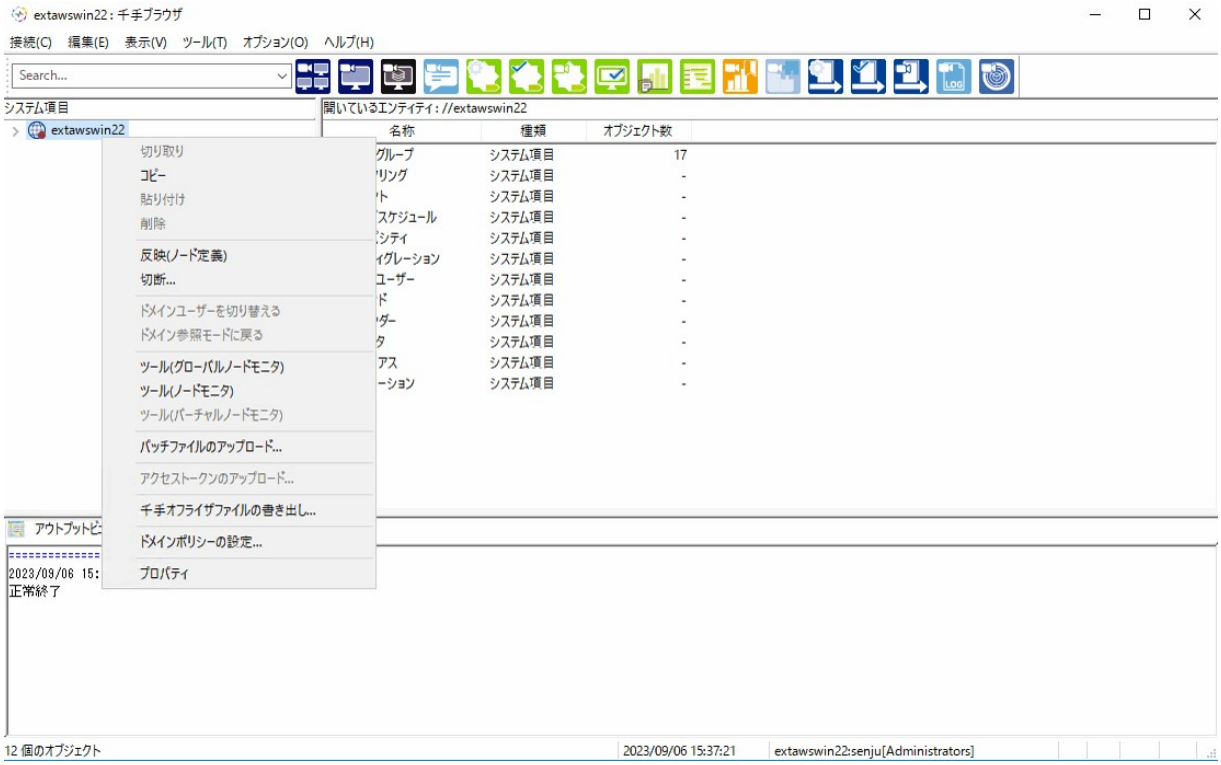


図 2.2 ドメインのコンテキストメニュー

図 2.3 ドメインのプロパティ

上記のプロパティ画面の「Extension Packライセンス情報」フレームの「ライセンス情報確認」ボタンを押すと、下記の図のようなライセンス情報ウィンドウが表示され、ドメイン名、ライセンスの期限、RefNo、登録されているライセンスキー、使用されている監視エクステンションを確認することができます。

(※)実際のウィンドウでは、「ライセンスキー」フィールドに、登録されているライセンスキーが表示されます。

(※)ライセンスキー変更を行うための、[ライセンスキー変更]ボタンは、AdministratorsもしくはManagersのユーザーグループに属するユーザーの場合のみ活性です。

図 2.4 Extension Packライセンス情報ウィンドウ

2.8.4.2. 千手ブラウザからのExtension Packライセンスキーの変更

千手システム販売元より取得したExtension Packライセンスキーファイル(sjKEY_<*千手ドメイン名*>)を千手ブラウザのインストールディレクトリ直下にコピーして下さい。

注釈

- **Extension Packライセンスキーファイルは、ファイル名を以下のように変更してください。**

  sjKEY_<*千手ドメイン名*>

警告

千手ドメイン名がExtension Packライセンスキーに登録されています。

千手システム販売元より取得したExtension Packライセンスキーファイルのホスト名と千手ドメイン名が大文字小文字も含め一致することを確認してください。
また、Extension Packライセンスキーに登録されている千手ドメイン名は、ライセンスキーを送付したメールの【ホスト名】に記載されています。
一致していない場合、千手システムは稼働しません。

ドメインのプロパティ画面の「Extension Packライセンス情報」フレームの[ライセンスキー変更]ボタンを押すと、下記の図のような画面が現れます。

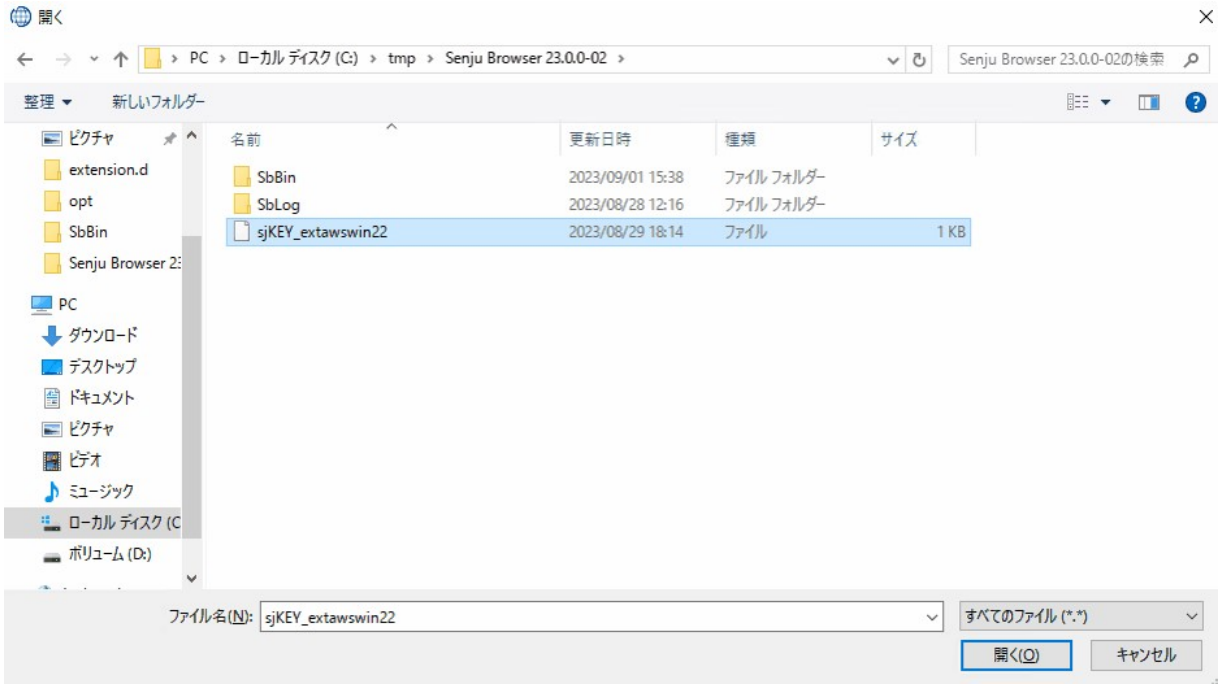


図 2.5 Extension Packライセンスキーファイルの指定画面

「ファイルの場所」にExtension Packライセンスキーファイルを格納したディレクトリを指定し、Extension Packライセンスキーファイルを開くと、下記の図のような確認ダイアログが現れます。

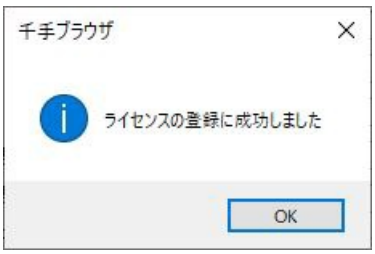


図 2.6 Extension Packライセンスキー登録確認ダイアログ

この画面で[OK]ボタンを押すことによりExtension Packライセンスキーの登録が完了します。

3. Cloud Job Scheduler

3.1. はじめに

3.1.1. 本章について

- Job Scheduler for Cloud 使用者の手引きは、Job Scheduler for Cloud の機能や使用方法について説明します。
- Job Scheduler for Cloud はAmazon Web Services(AWS)のElastic MapReduce、Lambda Functionの機能、AzureのDurable Functionsの機能、Google CloudのCloud Functionsの機能、Google CloudのCloud Composerの機能、Oracle Cloud Infrastructure(OCI)のCloud Functionsの機能、IBM CloudのFunctionsの機能とSenju/DCのジョブスケジュール機能を連携させることができます。この連携により、Senju/DCのジョブスケジュール機能からAWS/Elastic MapReduceのジョブフロー、Lambda Function、Azure/Durable Functions、Google Cloud Functions、Google Cloud Composer、OCI/Oracle Functions、IBM Cloud Functionsを実行および監視することができるようになります。
- 「Senju DevOperation Conductor」「Senju Operation Conductor」「Senju Enterprise Navigator」「eXsenju」「EX千手/EXSENJU」「千手/SENJU」「e-千手/e-SENJU」および「セキュア・キューブ/SecureCube」は（株）野村総合研究所の登録商標です。
- Amazon Web Services、“Powered by Amazon Web Services”ロゴ、[およびかかる資料で使用されるその他のAWS商標]は、米国その他の諸国における、Amazon.com, Inc.またはその関連会社の商標です。
- UNIXは、X/Open Company Limitedが独占的にライセンスしている米国ならびに他の国における登録商標です。
- Linuxは、Linus Torvalds氏の登録商標です。
- Windows、Windows Server、Azureは、米国Microsoft Corporationの米国及びその他の国における登録商標または商標です。
- Google、Google Cloud、Google Cloud Platform、および、GCP は、Google LLC の商標です。
- OracleとJavaは、Oracle Corporation 及びその子会社、関連会社の米国及びその他の国における登録商標です。文中の社名、商品名等は各社の商標または登録商標である場合があります。
- IBM、IBM ロゴ、および ibm.com は、世界の多くの国で登録された International Business Machines Corp. の商標です。他の製品名およびサービス名等は、それぞれ、IBM または各社の商標である場合があります。現時点での IBM商標リストについては、http://www.ibm.com/legal/copytrade.shtml の『Copyright and trademark information』をご覧ください。
- その他、本誌で引用の製品名・会社名はそれぞれの会社の商標、もしくは登録商標です。なお、本誌中では、™、® マークなどは明記していません

3.1.2. 読者の対象

本章はJob Scheduler for Cloud を利用して、Senju/DCのジョブスケジュール機能からAWS/Elastic MapReduceのジョブフロー、Lambda FunctionとAzure/Durable Functions、Google Cloud Functions、Google Cloud Composer、OCI/Oracle Functions、IBM Cloud Functionsを管理するシステム・アドミニストレータのためのものです。従って、本章の読者は以下のような概念に精通していることを前提にしています。

- Amazon Web Services（AWS）
- Microsoft Azure
- Google Cloud
- Oracle Cloud Infrastructure(OCI)
- IBM Cloud
- Senju/DCの各種コンポーネント（千手ブラウザ、千手マネージャ、千手エージェント）
- Senju/DCのジョブスケジュール機能
- オペレーティング・システムについての知識

3.1.3. 前提条件と関連資料

3.1.3.1. Amazon Web Servicesの利用について

Job Scheduler for Cloudの利用において、事前にAmazon Web Servicesアカウントの登録が必要です。

Amazon Web Servicesサイトよりアカウント登録を行って下さい。

3.1.3.2. Microsoft Azureの利用について

Job Scheduler for Cloudの利用において、事前にMicrosoft Azureアカウントの登録が必要です。

Microsoft Azureサイトよりアカウント登録を行って下さい。

3.1.3.3. Google Cloudの利用について

Job Scheduler for Cloudの利用において、事前にGoogle Cloudアカウントの登録が必要です。

Google Cloudサイトよりアカウント登録を行って下さい。

3.1.3.4. Oracle Cloud Infrastructureの利用について

Job Scheduler for Cloudの利用において、事前にOracle Cloud Infrastructureアカウントの登録が必要です。

Oracle Cloud Infrastructureサイトよりアカウント登録を行って下さい。

3.1.3.5. IBM Cloudの利用について

Job Scheduler for Cloudの利用において、事前にIBM Cloudアカウントの登録が必要です。

IBM Cloudサイトよりアカウント登録を行って下さい。

3.1.3.6. 関連資料

本章を参照するにあたっては、以下の各マニュアルなどを参照して下さい。

- 統合運用管理ツール「Senju DevOperation Conductor」リリースノート
- 統合運用管理ツール「Senju DevOperation Conductor」ユーザーズガイド
- Amazon Web Servicesドキュメント
- Microsoft Azureドキュメント
- Google Cloudドキュメント
- Oracle Cloud Infrastructureドキュメント
- IBM Cloudドキュメント

3.2. Job Scheduler for Cloudの概要

Job Scheduler for Cloudの機能を利用するためには、以下の設定が必要になります。

- ライセンスの購入とライセンスキーの入手
    - AWS監視
    - Azure監視
    - Google Cloud監視
    - OCI監視
- Senju DevOperation Conductor Extension Packの入手と適用

    運用管理サーバーおよび、Cloud連携ジョブを実行する管理対象ノードに Senju DevOperation Conductor Extension Pack の適用が必要です。
    - 運用管理サーバー（千手マネージャ）への適用（ジョブテンプレート項目の更新）
    - 管理対象ノード（千手エージェント(プローブノード)）への適用（ジョブ実行コマンドの更新）

参考

Senju DevOperation Conductor Extension Packの適用手順につきましては、Senju DevOperation Conductor Extension Pack の README をご参照下さい。

注釈

Senju DevOperation Conductor Extension Packの適用に際しては、千手システムの停止は不要ですが、関連する監視タスクの停止が必要です。

Job Scheduler for Cloudは、下記のジョブ群によって、Senju/DCのジョブスケジュールサブシステムよりAWS/S3、AWS/Elastic MapReduce、AWS/Lambda Function、Azure/Durable Functions、Google Cloud Functions、Google Cloud Composer、OCI/Oracle FunctionsおよびIBM Cloud Functionsの機能を利用します。

- AWS/S3ファイル取得ジョブ
- AWS/S3ファイル登録ジョブ
- AWS/S3ファイル削除ジョブ
- AWS/Elastic MapReduceジョブフロー実行ジョブ
- AWS/Lambda Function連携ジョブ
- Azure/Durable Functions連携ジョブ
- Google Cloud Functions連携ジョブ
- Google Cloud Composer連携コマンド
- OCI/Functions連携ジョブ
- IBM Cloud Functions連携ジョブ

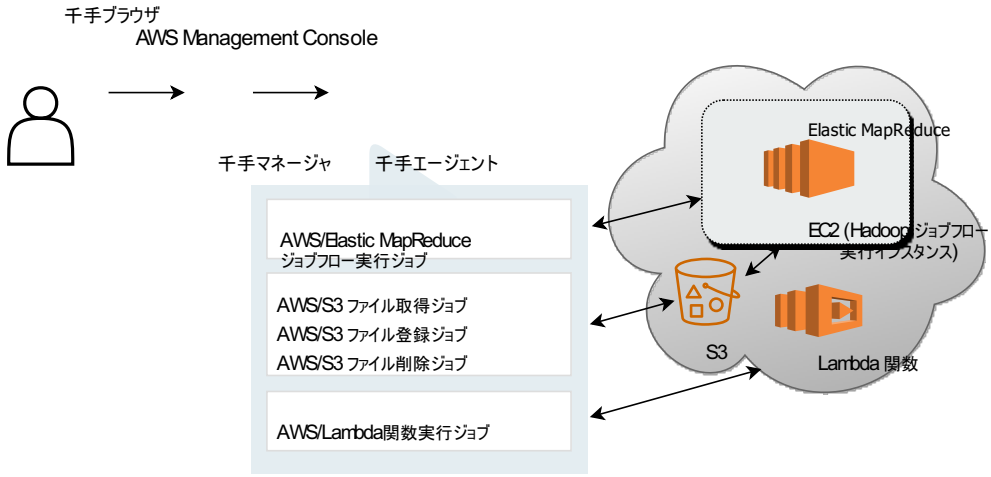


図 3.1 Senju/DCとAWSとの連携

Job Scheduler for CloudがAWSと接続する際、AWSに関する情報をsj_aws.iniファイルから取得します。そのため、Job Scheduler for Cloudを使用する前にsj_aws.iniファイルを設定しておく必要があります。

Senju/DCのジョブスケジュールサブシステムよりAWS/S3の機能を利用するためには、以下のジョブを使用します。

- AWS/S3ファイル取得ジョブ
- AWS/S3ファイル登録ジョブ
- AWS/S3ファイル削除ジョブ

Senju/DCのジョブスケジュールサブシステムよりAWS/Elastic MapReduceの機能を利用するためには、AWS/Elastic MapReduceジョブフロー実行ジョブを使用します。

Senju/DCのジョブスケジュールサブシステムよりAWS/Lambda Functionの機能を利用するためには、AWS/Lambda Function連携ジョブを使用します。

AWS上の操作はAWS Management Consoleを使用します。

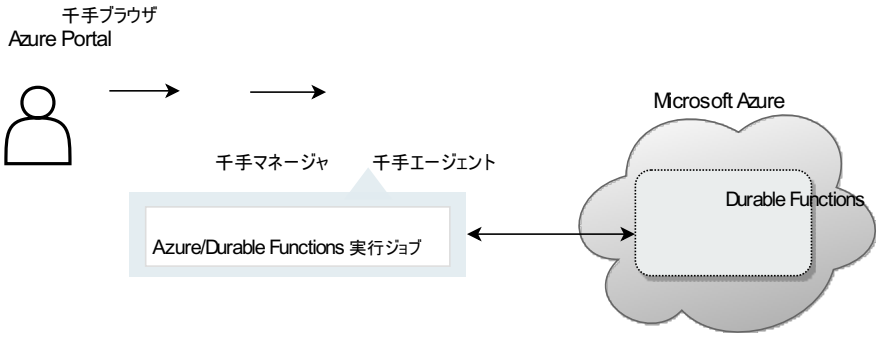


図 3.2 Senju/DCとAzureとの連携

Job Scheduler for CloudがAzureと接続する際、Azureに関する情報をsj_azure_user.confファイルから取得します。そのため、Job Scheduler for Cloudを使用する前にsj_azure_user.confファイルを設定しておく必要があります。

Senju/DCのジョブスケジュールサブシステムよりAzure/Durable Functionsの機能を利用するためには、Azure/Durable Functions連携ジョブを使用します。

Azure上の操作はAzure Portalを使用します。

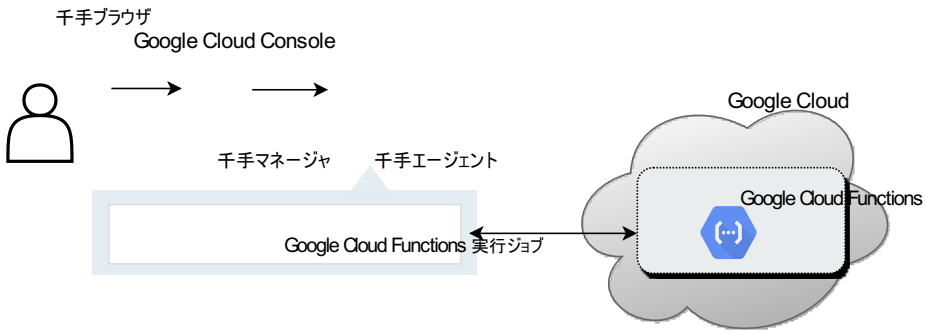


図 3.3 Senju/DCとGoogle Cloud Functionsとの連携

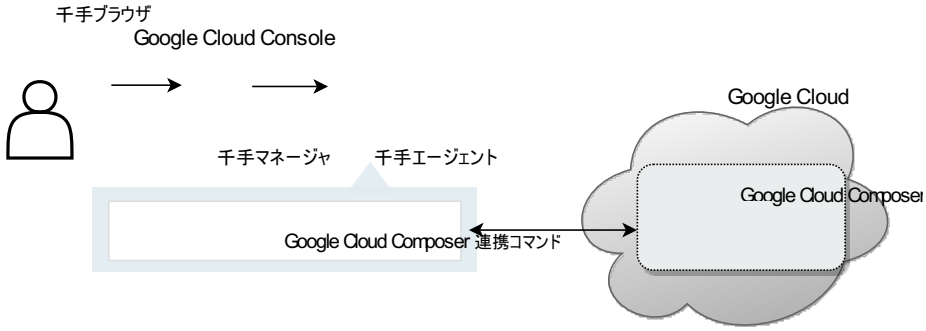


図 3.4 Senju/DCとGoogle Cloud Composerとの連携

Job Scheduler for CloudがGoogle Cloudと接続する際、Google Cloudに関する情報をsj_gcp_sys.jsonファイルから取得します。そのため、Job Scheduler for Cloudを使用する前にsj_gcp_sys.jsonファイルを設定しておく必要があります。

Senju/DCのジョブスケジュールサブシステムよりGoogle Cloud Functionsの機能を利用するためには、Google Cloud Functions連携ジョブを使用します。

Google Cloud Composerの機能を利用するためには、Google Cloud Composer連携コマンドを使用します。

Google Cloud上の操作はGoogle Cloud Consoleを使用します。

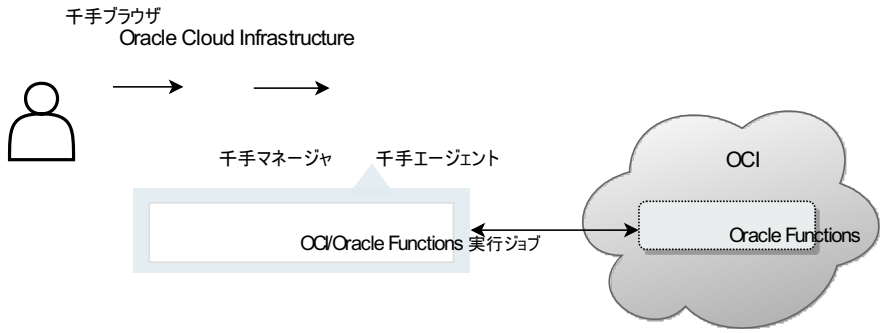


図 3.5 Senju/DCとOCIとの連携

Job Scheduler for CloudがOCIと接続する際、OCIに関する情報をsj_oci_sys.jsonファイルから取得します。そのため、Job Scheduler for Cloudを使用する前にsj_oci_sys.jsonファイルを設定しておく必要があります。

Senju/DCのジョブスケジュールサブシステムよりOCI/Oracle Functionsの機能を利用するためには、OCI/Functions連携ジョブを使用します。

OCI上の操作はOracle Cloud Infrastructureを使用します。

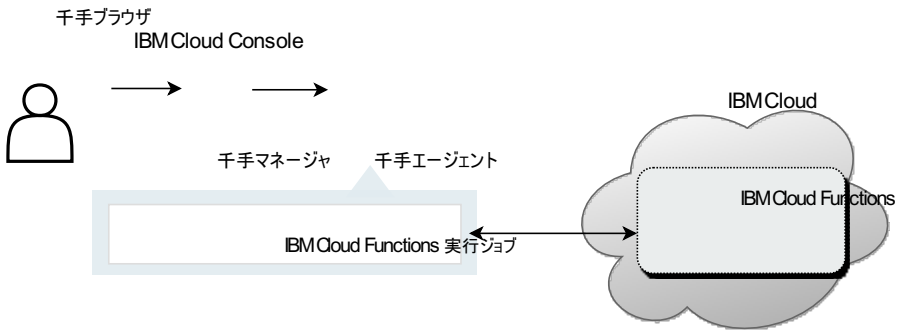


図 3.6 Senju/DCとIBM Cloudとの連携

Job Scheduler for CloudがIBM Cloudと接続する際、IBM Cloudに関する情報をsj_ibc_sys.jsonファイルから取得します。そのため、Job Scheduler for Cloudを使用する前にsj_ibc_sys.jsonファイルを設定しておく必要があります。

Senju/DCのジョブスケジュールサブシステムよりIBM Cloud Functionsの機能を利用するためには、IBM Cloud Functions連携ジョブを使用します。

IBM Cloud上の操作はIBM Cloud Consoleを使用します。

3.3. Job Scheduler for Cloud(AWS)の使い方

3.3.1. Job Scheduler for Cloud(AWS/S3)の使い方

3.3.1.1. Job Scheduler for Cloud(AWS/S3)の機能

Job Scheduler for Cloud(AWS/S3)とは、Senju/DCのジョブスケジュール機能と連携し、AWS/S3上のファイルの取得、登録および削除を行なう機能です。

3.3.1.2. ポリシーの作成

AWS/S3連携機能を使用するため、**「AWS/S3連携機能に必要なアクセス権限」**に示すポリシーを作成して、ユーザーにアクセス権限を付与します。

表 3.1 AWS/S3連携機能に必要なアクセス権限

ジョブ	必要なアクセス権
AWS/S3連携ジョブ	s3:listBuckets s3:putObject s3:getObject s3:deleteObject

3.3.1.3. sj_aws.iniの設定

sj_aws.iniファイルは、AWSに関する情報の設定ファイルで、Job Scheduler for Cloud(AWS/S3)ジョブはこのファイルを参照します。

設定方法については、**Cloud Monitoring の sj_setup_aws ― AWS情報設定ファイル更新 ―** を参照して下さい。

sj_aws.iniに、TABLEに示す内容を設定して下さい。

表 3.2 sj_aws.iniの記述内容

項目	省略	デフォルト	暗号化対象	説明
accessKey	可	―	○	AWS接続用のアクセスキーID
secretKey	可	―	○	AWS接続用のシークレットアクセスキー
bucket	可	―	×	AWS/S3のバケット
checkInterval	可	60	×	チェックインターバル(秒)[10-600]

- 省略可能な項目を省略した場合は、Job Scheduler for Cloud(AWS/S3)ジョブのオプションで指定する必要があります。デフォルトが存在するものに関しては、省略してもデフォルト値で動作します。
- 同じ項目を、sj_aws.iniとJob Scheduler for Cloud(AWS/S3)ジョブのオプションの両方で指定した場合は、Job Scheduler for Cloud(AWS/S3)ジョブのオプションで指定した値が有効になります。
- AWS接続用のアクセスキーIDおよびシークレットアクセスキーは、Amazon Web Servicesのサイトで確認して下さい
- 指定可能なAWSリージョン および EC2インスタンスタイプは、「4.5.1 Job Scheduler for Cloudの制限事項」を参照して下さい。

警告

Senju/DCジョブの起動コマンドには、文字数に制限があります。なるべく各項目は省略せずに、sj_aws.iniファイルに設定して下さい。

3.3.1.4. AWS/S3ファイル取得ジョブの利用方法

AWS/S3ファイル取得ジョブは、AWS/Elastic MapReduceジョブフロー実行ジョブやAWS Management Consoleなどによって登録、作成したファイルをAWS/S3上から取得します。

AWS/S3ファイル取得ジョブが起動されると、引数に指定された内容でファイルを取得し、結果を標準出力に出力します。

AWS/S3ファイル取得ジョブを起動する際に指定する引数には、以下に示す内容を指定して下さい。

```
sjPEX_CloudFunctions -m S3
        -get S3URI
        [-ak アクセスキーID] [-sk シークレットアクセスキー] [ -bk S3バケット名]
        [-i チェックインターバル]
```

オプション	省略	デフォルト	長さ	説明
get	不可	—	510	AWS/S3上のファイル名 （AWS/S3上のURIとローカルパスを' ,' で区切って指定。"AWS/S3上のURI,ローカルパス"。s3:///バケット名/を
ak	可	—	256	AWS接続用のアクセスキーID
-sk	可	—	256	AWS接続用のシークレットアクセスキー
bk	可	—	255	AWS/S3上のバケット
-i	可	60	4	チェックインターバル(秒) [10-600]

- Senju/DCジョブの起動コマンドの最大文字数は2048文字です。起動コマンドが最大文字数を超える場合は、sj_aws.iniに設定して下さい。
- 省略可能なオプションを省略した場合は、sj_aws.iniで指定した値が有効になります。
- AWS接続用のアクセスキーIDおよびシークレットアクセスキーは、Amazon Web Servicesのサイトで確認して下さい。

3.3.1.4.1. AWS/S3ファイル取得ジョブテンプレートの使い方

ジョブテンプレートとは、ジョブの起動コマンドシーケンスのみを持ち、パラメータ値が未決定であるエンティティです。ジョブテンプレートを用いることにより、ジョブの登録のたびにコマンドシーケンスを入力しなくても、必要なパラメータ値を入力するだけでジョブの作成が行えます。Job Scheduler for CloudをSenju/DCのジョブスケジュール機能と連携するために、Job Scheduler for Cloudジョブを、Senju/DCのジョブの起動コマンドとして設定します。

AWS/S3ファイル取得ジョブテンプレートを使用し、ジョブの起動コマンドとして利用するには、千手ブラウザのツリービューで、＜ドメイン＞→"ジョブスケジュール"→"ジョブ"を選択し、ジョブの新規作成を行います。

ジョブの新規作成プロパティウィンドで[ジョブテンプレートを使用]チェックボックスをチェックし、[ジョブテンプレート入力]ボタンを押して下さい。

ジョブテンプレート入力ウィンドでAWS/S3ファイル取得ジョブテンプレートを選択し、各パラメータ値を設定して下さい。

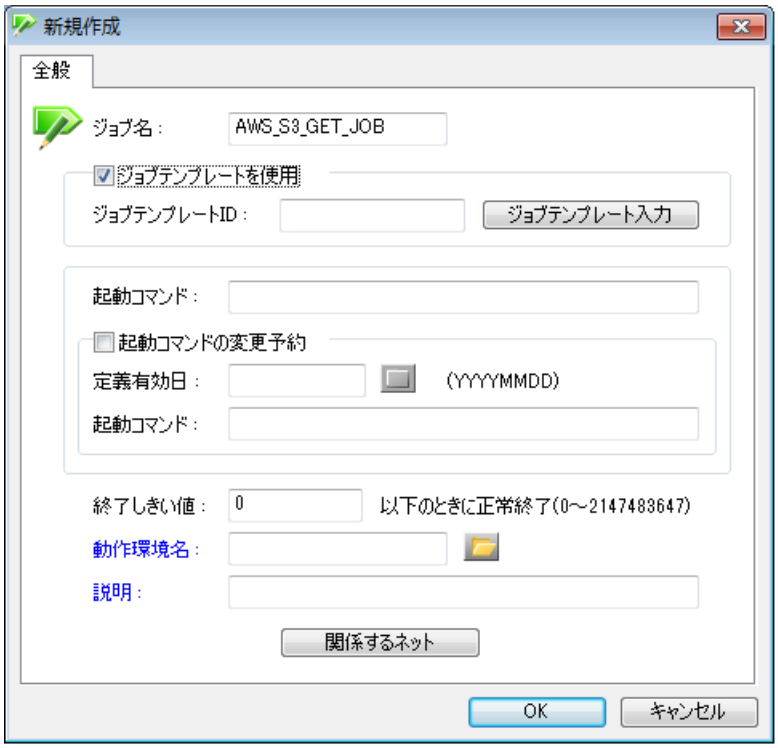


図 3.7 AWS/S3ファイル取得ジョブテンプレートの使用

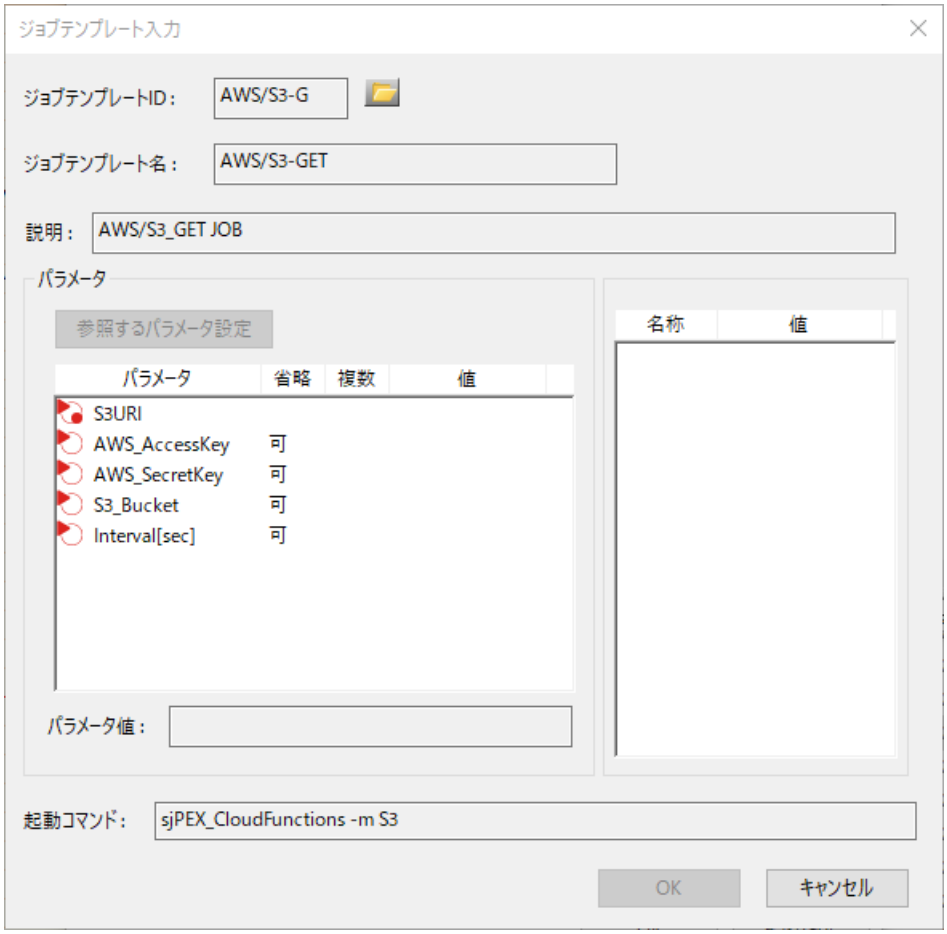


図 3.8 AWS/S3ファイル取得ジョブテンプレートの入力

表 3.3 AWS/S3ファイル取得ジョブテンプレートの入力

パラメータ	説明
S3URI	AWS/S3上のファイル名 （AWS/S3上のURIとローカルパスを' ,' で区切って指定。"AWS/S3上のURI,ローカルパス"。s3://バケット名/を外したファイル名ま
AWS_AccessKey	AWS接続用のアクセスキーID
AWS_SecretKey	AWS接続用のシークレットアクセスキー
S3_Bucket	AWS/S3上のバケット
Interval[sec]	チェックインターバル(秒) [10-600]

3.3.1.4.2. AWS/S3ファイル取得ジョブの処理の流れ(通常時)

AWS/S3ファイル取得ジョブがSenju/DCのジョブスケジュールで1つのジョブとして起動されると、**「図 3-4　AWS/S3ファイル取得ジョブの処理の流れ」**および**「TABLE 3-7　AWS/S3ファイル取得ジョブの処理の流れ」**に示す流れで動きます。

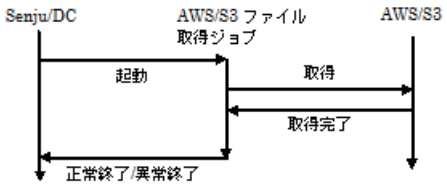


図 3.9 AWS/S3ファイル取得ジョブの処理の流れ

表 3.4 AWS/S3ファイル取得ジョブの処理の流れ

Senju/DC ジョブの状態	AWS/S3ファイル取得 ジョブの処理内容	メッセージモニタの出力
起動待ち	起動前の状態	
稼働中	起動	
稼働中	引数に従い、AWS/S3上のファイル取得	
正常終了	AWS/S3上のファイル取得に成功	!PEXC03 AWS/S3からのデータ取得に成功しました。
異常終了	AWS/S3上のファイル取得に失敗	!PEXC04 AWS/S3からのデータ取得に失敗しました。

1. AWS/S3ファイル取得ジョブが起動されると、引数に指定された内容でファイルを取得処理を実行します。
2. AWS/S3上のファイルを取得します。
3. 取得が正しく行なわれると、データ取得に成功した旨のメッセージを出力し、Senju/DCジョブは正常終了します。
4. 取得が何らかの理由で正しく行なわれないと、データ取得に失敗した旨のメッセージを出力し、Senju/DCジョブは異常終了します。

警告

データが正しく取得されたかは、引数に指定したローカルパス配下を確認して下さい。

3.3.1.5. AWS/S3ファイル登録ジョブの利用方法

AWS/S3ファイル登録ジョブは、ジョブの実行環境である該当ノード上に登録、作成したファイルをAWS/S3上へ登録します。

AWS/S3ファイル登録ジョブが起動されると、引数に指定された内容でファイルを登録し、結果を標準出力に出力します。

AWS/S3ファイル登録ジョブを起動する際に指定する引数には、以下に示す内容を指定して下さい。

```
sjPEX_CloudFunctions -m S3
        -put S3URI
        [-ak アクセスキーID] [-sk シークレットアクセスキー] [ -bk S3バケット名]
        [-i チェックインターバル]
```

オプション	省略	デフォルト	長さ	説明
-put	不可	—	510	AWS/S3上のファイル名 （AWS/S3上のURIとローカルパスを’,’で区切って指定。”AWS/S3上のURI,ローカルパス”。s3:///バケット名/を
-ak	可	—	256	AWS接続用のアクセスキーID
-sk	可	—	256	AWS接続用のシークレットアクセスキー
-bk	可	—	255	AWS/S3上のバケット
-i	可	60	4	チェックインターバル(秒) [10-600]

- Senju/DCジョブの起動コマンドの最大文字数は2048文字です。起動コマンドが最大文字数を超える場合は、sj_aws.iniに設定して下さい。
- 省略可能なオプションを省略した場合は、sj_aws.iniで指定した値が有効になります。
- AWS接続用のアクセスキーIDおよびシークレットアクセスキーは、Amazon Web Servicesのサイトで確認して下さい。

3.3.1.5.1. AWS/S3ファイル登録ジョブテンプレートの使い方

ジョブテンプレートとは、ジョブの起動コマンドシーケンスのみを持ち、パラメータ値が未決定であるエンティティです。ジョブテンプレートを用いることにより、ジョブの登録のたびにコマンドシーケンスを入力しなくても、必要なパラメータ値を入力するだけでジョブの作成が行えます。Job Scheduler for CloudをSenju/DCのジョブスケジュール機能と連携するために、Job Scheduler for Cloudジョブを、Senju/DCのジョブの起動コマンドとして設定します。

AWS/S3ファイル登録ジョブテンプレートを使用し、ジョブの起動コマンドとして利用するには、千手ブラウザのツリービューで、＜ドメイン＞→“ジョブスケジュール”→“ジョブ”を選択し、ジョブの新規作成から行います。

ジョブの新規作成プロパティウィンドで[ジョブテンプレートを使用]チェックボックスをチェックし、[ジョブテンプレート入力]ボタンを押して下さい。

ジョブテンプレート入力ウィンドでAWS/S3ファイル登録ジョブテンプレートを選択し、各パラメータ値を設定して下さい。

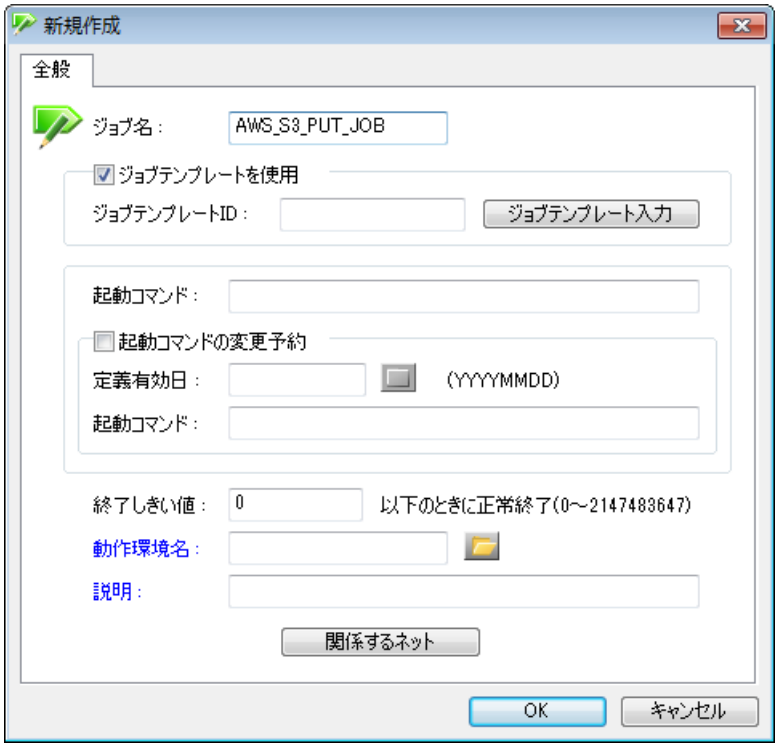


図 3.10 AWS/S3ファイル登録ジョブテンプレートの使用

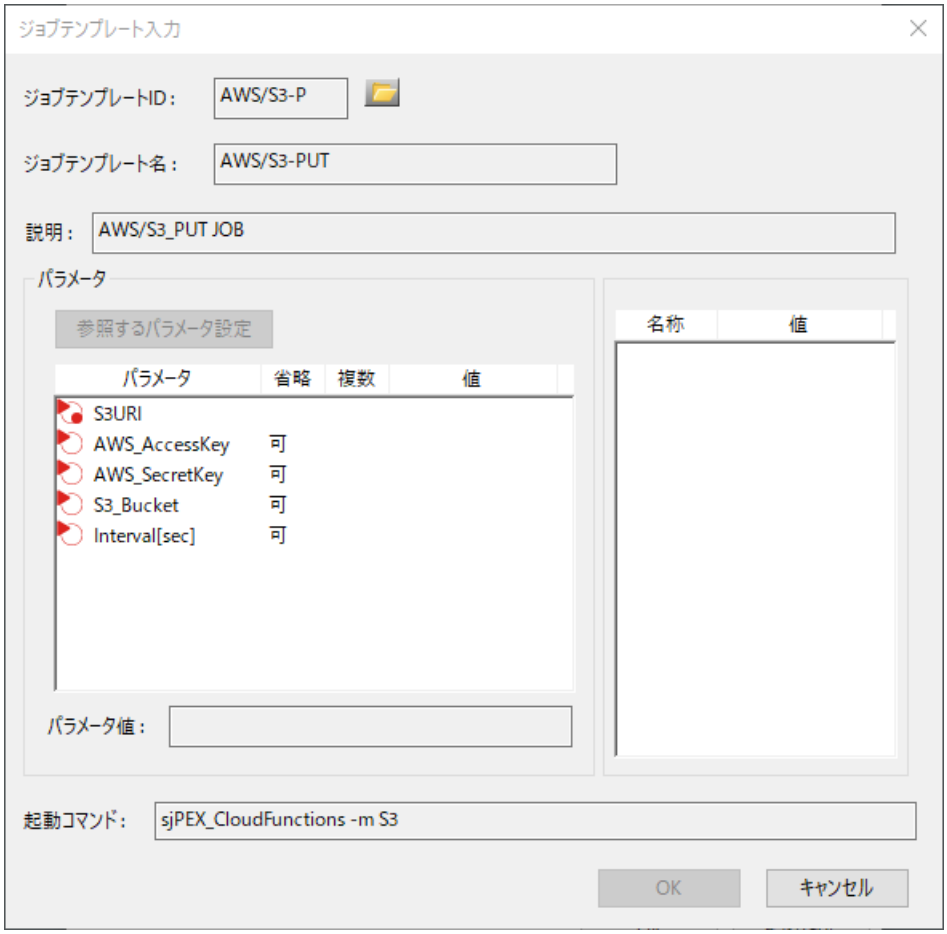


図 3.11 AWS/S3ファイル登録ジョブテンプレートの入力

表 3.5 AWS/S3ファイル登録ジョブテンプレートの入力

パラメータ	説明
S3URI	AWS/S3上のファイル名 （AWS/S3上のURIとローカルパスを' ,' で区切って指定。"AWS/S3上のURI,ローカルパス"。s3://バケット名/を外したファイル名ま
AWS_AccessKey	AWS接続用のアクセスキーID
AWS_SecretKey	AWS接続用のシークレットアクセスキー
S3_Bucket	AWS/S3上のバケット
Interval[sec]	チェックインターバル(秒) [10-600]

3.3.1.5.2. AWS/S3ファイル登録ジョブの処理の流れ(通常時)

AWS/S3ファイル登録ジョブがSenju/DCのジョブスケジュールで1つのジョブとして起動されると、**「図 3-7　AWS/S3ファイル登録ジョブの処理の流れ」**および**「TABLE 3-9　AWS/S3ファイル登録ジョブの処理の流れ」**に示す流れで動きます。

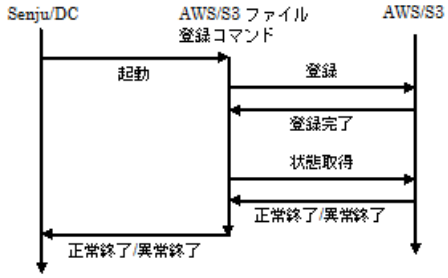


図 3.12 AWS/S3ファイル登録ジョブの処理の流れ

表 3.6 AWS/S3ファイル登録ジョブの処理の流れ

Senju/DC ジョブの状態	AWS/S3ファイル登録 ジョブの処理内容	メッセージモニタの出力
起動待ち	起動前の状態	
稼働中	起動	
稼働中	引数に従い、AWS/S3上のファイル登録	
稼働中	AWS/S3上のファイル登録状態を取得	
正常終了	AWS/S3上のファイル登録に成功	!PEXC05 AWS/S3へのデータ登録に成功しました。
異常終了	AWS/S3上のファイル登録に失敗	!PEXC06 AWS/S3へのデータ登録に失敗しました。

1. AWS/S3ファイル登録ジョブが起動されると、引数に指定された内容でファイル登録処理を実行します。
2. AWS/S3上へファイルを登録します。
3. 指定されたファイルがAWS/S3上へ登録されたか状態を取得します。
4. 登録が正しく行なわれると、成功した旨のメッセージを出力し、Senju/DCジョブは正常終了します。
5. 登録が何らかの理由で正しく行なわれないと、失敗した旨のメッセージを出力し、Senju/DCジョブは異常終了します。

3.3.1.6. AWS/S3ファイル削除ジョブの利用方法

AWS/S3ファイル削除ジョブは、AWS/Elastic MapReduceジョブフロー実行ジョブやAWS Management Consoleなどによって登録、作成したファイルをAWS/S3上から削除します。削除されたファイルの情報は一切残りませんので、本ジョブを実行する場合は細心の注意を払い行って下さい。

AWS/S3ファイル削除ジョブが起動されると、引数に指定された内容でファイルを削除し、結果を標準出力に出力します。

AWS/S3ファイル削除ジョブを起動する際に指定する引数には、以下に示す内容を指定して下さい。

```
sjPEX_CloudFunctions -m S3
        -del S3URI
        [-ak アクセスキーID] [-sk シークレットアクセスキー] [ -bk S3バケット名]
        [-i チェックインターバル]
```

オプション	省略	デフォルト	長さ	説明
-del	不可	—	510	AWS/S3上のファイル名（AWS/S3上のURI）
-ak	可	—	256	AWS接続用のアクセスキーID
-sk	可	—	256	AWS接続用のシークレットアクセスキー
-bk	可	—	255	AWS/S3上のバケット
-i	可	60	4	チェックインターバル(秒) [10-600]

- Senju/DCジョブの起動コマンドの最大文字数は2048文字です。起動コマンドが最大文字数を超える場合は、sj_aws.iniに設定して下さい。
- 省略可能なオプションを省略した場合は、sj_aws.iniで指定した値が有効になります。
- AWS接続用のアクセスキーIDおよびシークレットアクセスキーは、Amazon Web Servicesのサイトで確認して下さい。

3.3.1.6.1. AWS/S3ファイル削除ジョブテンプレートの使い方

ジョブテンプレートとは、ジョブの起動コマンドシーケンスのみを持ち、パラメータ値が未決定であるエンティティです。ジョブテンプレートを用いることにより、ジョブの登録のたびにコマンドシーケンスを入力しなくても、必要なパラメータ値を入力するだけでジョブの作成が行えます。Job Scheduler for CloudをSenju/DCのジョブスケジュール機能と連携するために、Job Scheduler for Cloudジョブを、Senju/DCのジョブの起動コマンドとして設定します。

AWS/S3ファイル削除ジョブテンプレートを使用し、ジョブの起動コマンドとして利用するには、千手ブラウザのツリービューで、＜ドメイン＞→“ジョブスケジュール”→“ジョブ”を選択し、ジョブの新規作成から行います。

ジョブの新規作成プロパティウィンドで[ジョブテンプレートを使用]チェックボックスをチェックし、[ジョブテンプレート入力]ボタンを押して下さい。

ジョブテンプレート入力ウィンドでAWS/S3ファイル削除ジョブテンプレートを選択し、各パラメータ値を設定して下さい。

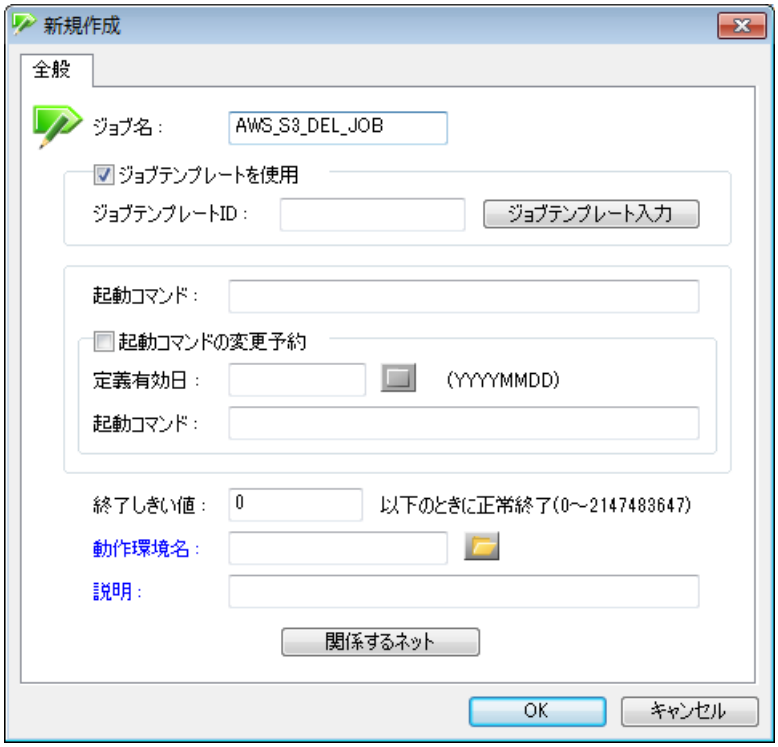


図 3.13 AWS/S3ファイル削除ジョブテンプレートの使用

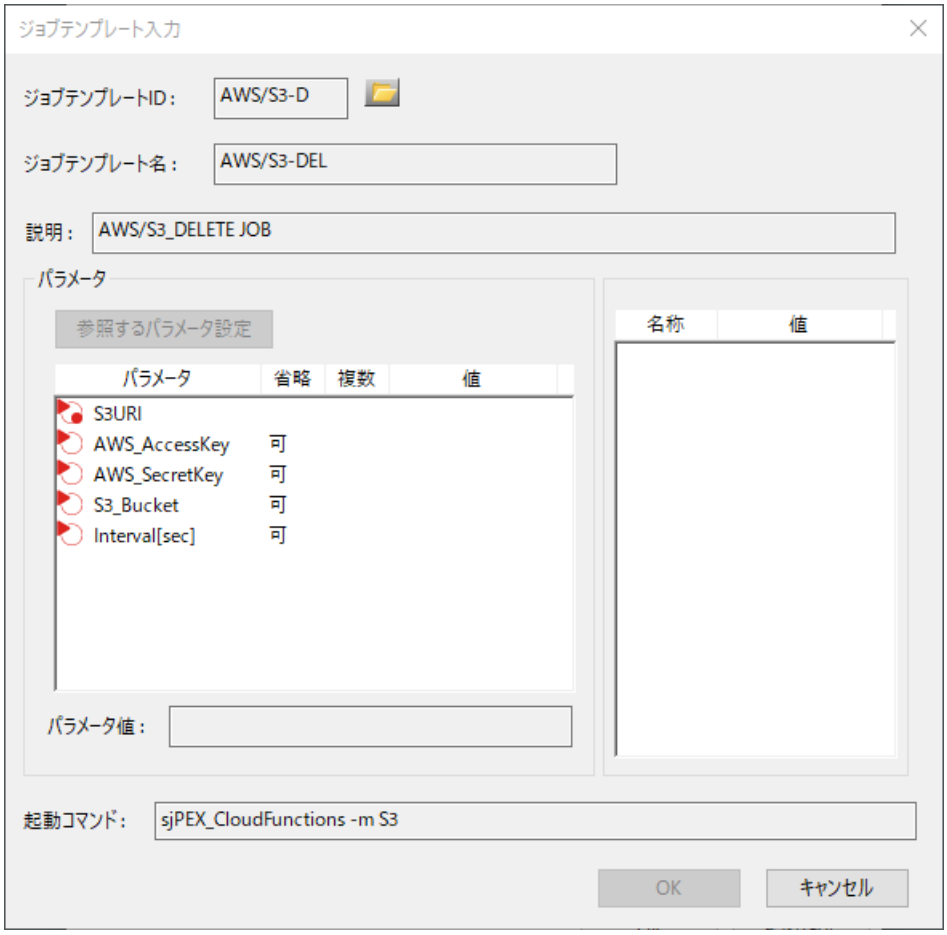


図 3.14 AWS/S3ファイル削除ジョブテンプレートの入力

表 3.7 AWS/S3ファイル削除ジョブテンプレートの入力

パラメータ	説明
S3URI	AWS/S3上のファイル名（AWS/S3上のURI）
AWS_AccessKey	AWS接続用のアクセスキーID
AWS_SecretKey	AWS接続用のシークレットアクセスキー
S3_Bucket	AWS/S3上のバケット
Interval[sec]	チェックインターバル(秒) [10-600]

3.3.1.6.2. AWS/S3ファイル削除ジョブの処理の流れ(通常時)

AWS/S3ファイル削除ジョブがSenju/DCのジョブスケジュールで1つのジョブとして起動されると、**「図 3-10　AWS/S3ファイル削除ジョブの処理の流れ」**および**「TABLE 3-11　AWS/S3ファイル削除ジョブの処理の流れ」**に示す流れで動きます。

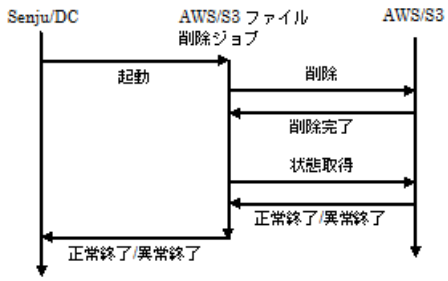


図 3.15 AWS/S3ファイル削除ジョブの処理の流れ

表 3.8 AWS/S3ファイル削除ジョブの処理の流れ

Senju/DC ジョブの状態	AWS/S3ファイル削除 ジョブの処理内容	メッセージモニタの出力
起動待ち	起動前の状態	
稼働中	起動	
稼働中	引数に従い、AWS/S3上のファイル削除	
稼働中	AWS/S3上のファイル削除 状態を取得	
正常終了	AWS/S3上のファイル削除に成功	!PEXC07 AWS/S3からのデータ削除に成功しました。
異常終了	AWS/S3上のファイル削除に失敗	!PEXC08 AWS/S3からのデータ削除に失敗しました。

1. AWS/S3ファイル削除ジョブが起動されると、引数に指定された内容でファイル削除処理を実行します。
2. AWS/S3上のファイルを削除します。
3. 指定されたファイルがAWS/S3上から削除されたか状態を取得します。
4. 削除が正しく行なわれると、成功した旨のメッセージを出力し、Senju/DCジョブは正常終了します。
5. 削除が何らかの理由で正しく行なわれないと、失敗した旨のメッセージを出力し、Senju/DCジョブは異常終了します。

3.3.2. Job Scheduler for Cloud(AWS/Elastic MapReduce)の使い方

3.3.2.1. Job Scheduler for Cloud(AWS/Elastic MapReduce)の機能

Job Scheduler for Cloud(AWS/Elastic MapReduce)とは、Senju/DCのジョブスケジュール機能と連携し、AWS/Elastic MapReduceのジョブフローの実行と、開始から終了まで監視を行なう機能です。

3.3.2.2. AWS/Elastic MapReduceジョブフロー実行の流れ

Job Scheduler for CloudでAWS/Elastic MapReduceのジョブフローを実行する際の流れを次に示します。

AWSに関する情報の設定を行い、Job Scheduler for Cloudジョブを Senju/DCのジョブに登録して、Elastic MapReduceジョブフローの入力ファイルの登録、ジョブフローの実行、出力ファイルの取得を行います。

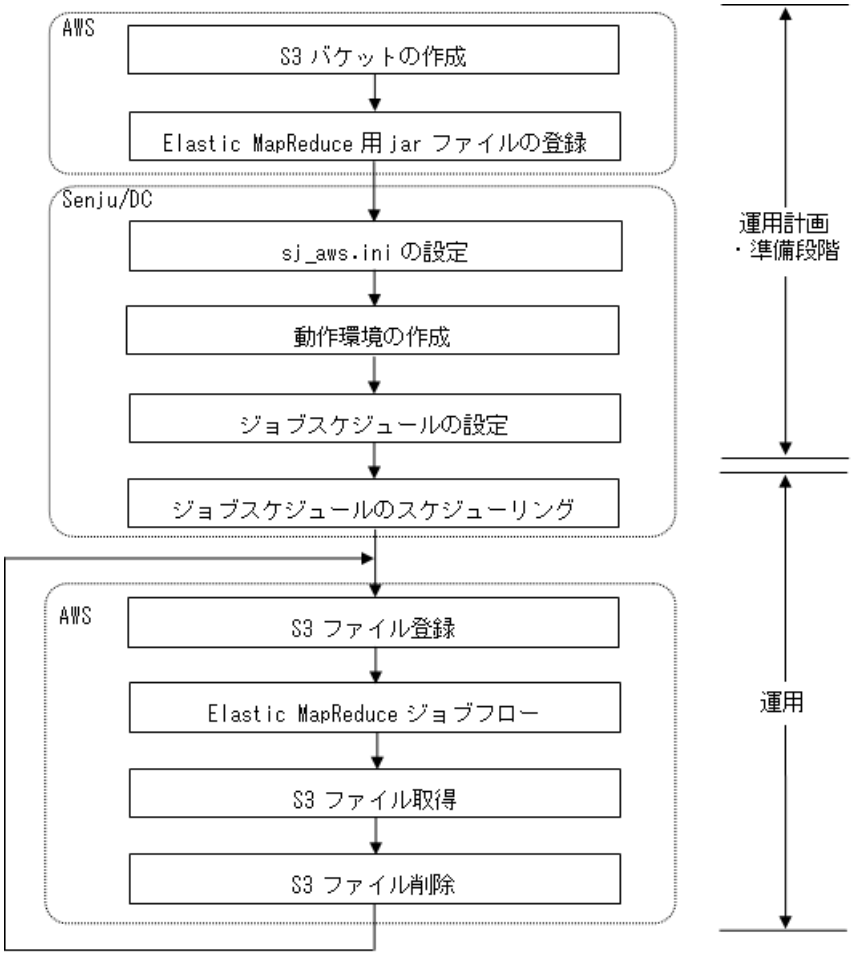


図 3.16 **AWS/Elastic MapReduceジョブフロー実行の流れ**

3.3.2.2.1. 運用計画・準備段階

- AWS/S3バケットの作成 [必須作業]

  Job Scheduler for Cloudジョブを実行するために、AWS/S3バケットを1つ以上作成します。作成はAWS Management Consoleなどから行なって下さい。

- Elastic MapReduce用jarファイルの登録 [必須作業]

  Job Scheduler for Cloud(Elastic MapReduce)で作成したクラスター内で実行するカスタムjarファイルを登録します。

  jarファイルは、AWS/S3ファイル登録ジョブやAWS Management ConsoleなどでAWS/S3上に登録して下さい。

参考

AWS/Elastic MapReduceで使用可能な jarファイルはAWS/Elastic MapReduceの仕様に依存します。詳細については、Amazon Web Servicesサイトよりご確認下さい。

- sj_aws.iniの設定 [必須作業]

  Job Scheduler for Cloudジョブを実行するために、AWSに関する情報を設定します。

  (「 sj_aws.iniの設定 (AWS/S3)」「 sj_aws.iniの設定 (AWS/Elastic MapReduce)」参照)

- 動作環境の作成 [必須作業]

  Senju/DCのジョブスケジュールで Job Scheduler for Cloudジョブを実行するために、動作環境を作成します。

  動作環境には、環境変数を設定することができます。

  (「 動作環境の環境変数の利用法」参照)

- ジョブスケジュールの設定 [必須作業]

  Senju/DCのジョブスケジュールで Job Scheduler for Cloudジョブを実行するために、以下の設定を行います。

- ジョブおよびネットの作成
- システムの作成とネットの登録

参考

ジョブスケジュール設定の詳細は**「ユーザーズガイド」**を参照して下さい。

3.3.2.2.2. 運用

- ジョブスケジュールのスケジューリング

  Senju/DCのジョブスケジュールを実行するために、以下の設定を行います。

  - フレーム登録によるスケジューリング
  - フレームの投入および日付変更

参考

スケジューリング設定の詳細は**「ユーザーズガイド」**を参照して下さい。

- AWS/S3ファイル登録

  AWS/S3ファイル登録ジョブを使用し、AWS/Elastic MapReduceで使用するファイルをコマンドの実行環境である該当ノード上からAWS/S3上へ登録します。

  （「 AWS/S3ファイル登録ジョブの利用方法」参照）

- AWS/Elastic MapReduceジョブフロー

  AWS/Elastic MapReduceジョブフロー実行ジョブは、AWS/Elastic MapReduceジョブフローの実行と、開始から終了までの監視を行ないます。

  （「 AWS/Elastic MapReduce ジョブフロー実行ジョブの利用方法」参照）

- AWS/S3ファイル取得

  AWS/S3ファイル取得ジョブを使用し、AWS/Elastic MapReduceジョブフロー実行ジョブによって作成されたファイルをAWS/S3上から取得します。

  （「 AWS/S3ファイル取得ジョブの利用方法」参照）

- AWS/S3ファイル削除

  AWS/S3ファイル削除ジョブを使用し、AWS/Elastic MapReduceジョブフロー実行後の不要になったファイルをAWS/S3上から削除します。

  （「 AWS/S3ファイル削除ジョブの利用方法」参照）

3.3.2.3. ポリシーの作成

AWS/Elastic MapReduce連携機能を使用するため、**「AWS/Elastic MapReduce連携機能に必要なアクセス権限」**に示すポリシーを作成して、ユーザーにアクセス権限を付与します。

表 3.9 AWS/Elastic MapReduce連携機能に必要なアクセス権限

ジョブ	必要なアクセス権
AWS/Elastic MapReduce連携ジョブ	iam:PassRole elasticmapreduce:ListSteps elasticmapreduce:DescribeCluster elasticmapreduce:AddJobFlowSteps elasticmapreduce:RunJobFlow elasticmapreduce:TerminateJobFlows

3.3.2.4. sj_aws.iniの設定

sj_aws.iniファイルは、AWSに関する情報の設定ファイルで、Job Scheduler for Cloud(AWS/Elastic MapReduce)ジョブはこのファイルを参照します。

設定方法については、**Cloud Monitoring** の **sj_setup_aws** ー **AWS情報設定ファイル更新** ー を参照して下さい。

sj_aws.iniに、**「TABLE 3-12　sj_aws.iniの記述内容」**に示す内容を設定して下さい。

表 3.10 sj_aws.iniの記述内容

項目	省略	デフォルト	暗号化対象	説明
accessKey	可	—	○	AWS接続用のアクセスキーID
secretKey	可	—	○	AWS接続用のシークレットアクセスキー
region	可	—	×	AWSの接続先リージョン
instanceCount	可	5	×	AWS/EC2インスタンス数
masterInstanceType	可	m1.small	×	AWS/EC2インスタンスタイプ（マスター）
slaveInstanceType	可	m1.small	×	AWS/EC2インスタンスタイプ（スレーブ）
mapreduceLogUri	可	—	×	AWS/Elastic MapReduceジョブフローのログ出力先URI
checkInterval	可	60	×	チェックインターバル(秒) [10-600]
hadoopVersion	可	1.0.3	×	hadoopバージョン

- 省略可能な項目を省略した場合は、Job Scheduler for Cloud(AWS/Elastic MapReduce)ジョブのオプションで指定する必要があります。デフォルトが存在するものに関しては、省略してもデフォルト値で動作します。
- 同じ項目を、sj_aws.iniとJob Scheduler for Cloud(AWS/Elastic MapReduce)ジョブのオプションの両方で指定した場合は、Job Scheduler for Cloud(AWS/Elastic MapReduce)ジョブのオプションで指定した値が有効になります。
- AWS接続用のアクセスキーIDおよびシークレットアクセスキーは、Amazon Web Servicesのサイトで確認して下さい。
- 指定可能なAWSリージョン および EC2インスタンスタイプは、「4.5.1 Job Scheduler for Cloudの制限事項」を参照して下さい。
- Amazon EMR の AMI バージョン 2.x および 3.x を対象にしているため、指定可能なhadoopバージョンは「2.4.0」、「2.2.0」、および「1.0.3」です。

警告

Senju/DCジョブの起動コマンドには、文字数に制限があります。なるべく各項目は省略せずに、sj_aws.iniファイルに設定して下さい。

3.3.2.5. AWS/Elastic MapReduce ジョブフロー実行ジョブの利用方法

AWS/Elastic MapReduceジョブフロー実行ジョブは、AWS/Elastic MapReduceのジョブフローを実行し、開始から終了までの監視を行います。

AWS/Elastic MapReduceジョブフロー実行ジョブが起動されると、引数に指定された内容でジョブフローを実行し、結果を標準出力に出力します。

AWS/Elastic MapReduceジョブフロー実行ジョブを起動する際に指定する引数には、以下に示す内容を指定して下さい。

```
sjPEX_CloudFunctions -m MR
        -juri S3URI
        [-ak アクセスキーID] [-sk シークレットアクセスキー] [ -reg AWSのリージョン]
        [-inc EC2インスタンス数] [-mit EC2マスタインスタンスタイプ]
        [-sit EC2スレーブインスタンスタイプ] [-luri S3URI]
        [-iuri S3URI] [-ouri S3URI] [-mc /Elastic MapReduceメインクラス]
        [-args /Elastic MapReduceパラメータ]
        [-i チェックインターバル]
```

オプション	省略	デフォルト	長さ	説明
-juri	不可	—	1024	JarファイルのURI（AWS/S3上のURI）
-ak	可	—	256	AWS接続用のアクセスキーID
-sk	可	—	256	AWS接続用のシークレットアクセスキー
-reg	可	—	32	AWSの接続先リージョン
-inc	可	5	3	AWS/EC2インスタンス数
-mit	可	m1.small	256	AWS/EC2インスタンスタイプ（マスター）
-sit	可	m1.small	256	AWS/EC2インスタンスタイプ（スレーブ）
-luri	可	—	1024	AWS/Elastic MapReduceジョブフローのログ出力先URI
-iuri	可	—	1024	AWS/Elastic MapReduceのインプットURI（AWS/S3上のURI）
-ouri	可	—	1024	AWS/Elastic MapReduceのアウトプットURI（AWS/S3上のURI）
-mc	可	—	128	AWS/Elastic MapReduceのメインクラス
-args	可	—	126	AWS/Elastic MapReduceのパラメータ
-i	可	60	4	チェックインターバル(秒) [10-600]

- Senju/DCジョブの起動コマンドの最大文字数は2048文字です。起動コマンドが最大文字数を超える場合は、sj_aws.iniまたは動作環境に設定して下さい。(動作環境については、「3.4.4.4 動作環境の環境変数の利用法」を参照して下さい。)
- 省略可能なオプションを省略した場合は、sj_aws.iniで指定した値が有効になります。
- AWS接続用のアクセスキーIDおよびシークレットアクセスキーは、Amazon Web Servicesのサイトで確認して下さい。
- 指定可能なAWSリージョン および EC2インスタンスタイプは、「4.5.1 Job Scheduler for Cloudの制限事項」を参照して下さい。

注釈

AWS/Elastic MapReduceのインプットURI、アウトプットURI、メインクラス、パラメータは、指定するjarファイルの仕様に依存します。

3.3.2.5.1. ジョブテンプレートの追加手順

AWS/Elastic MapReduce連携機能を利用する場合、Senju/DCシステムが提供する運用コマンドsjPEX_editTmpl(ジョブテンプレートの変更/追加/削除)を実行し、最初にジョブテンプレートの追加を行って下さい。なお、既に登録されている場合、新たに追加する必要はありません。

以下のコマンドを実行すると、ジョブテンプレートにAWS/Elastic MapReduceジョブフロー実行ジョブが追加されます。

コマンド実行は、千手稼働アカウントにてログインして行って下さい。

実行コマンド

```
% sjPEX_editTmpl -iAWS/EMR -nAWS/EMR_JobFlow -x"sjPEX_CloudFunctions -m MR" -p"-juri @EMRJarURI@ -ak
@@AWS_AccessKey@@ -sk @@AWS_SecretKey@@ -reg @@AWS_Region@@ -inc @@EC2_Instance@@ -mit
@@EC2_MasterInstance@@ -sit @@EC2_SlaveInstance@@ -luri @@EMR_LogURI@@ -iuri @@EMR_InputURI@@ -ouri
@@EMR_OutputURI@@ -mc @@EMR_MainClass@@ -args @@EMR_Parameter@@ -i @@Interval[sec]@@" -
c"AWS/EMR_JobFlow JOB"
```

オプション	値
テンプレートID	AWS/EMR
テンプレート名称	AWS/EMR_JobFlow
コマンド	sjPEX_CloudFunctions -m MR
パラメータ	-juri @EMRJarURI@ -ak @@AWS_AccessKey@@ -sk @@AWS_SecretKey@@ -reg @@AWS_Region@@ -inc @
説明	AWS/EMR_JobFlow JOB

警告

実行後は、千手ブラウザのツリービューで、<ドメイン>→"ジョブスケジュール"→"ジョブテンプレート"を選択し、AWS/Elastic MapReduce ジョブフロー実行ジョブテンプレートが追加されていることを確認して下さい。

参考

sjPEX_editTmplコマンドの詳細は**「開発者ガイド」**を参照して下さい。

3.3.2.5.2. AWS/Elastic MapReduceジョブフロー実行ジョブテンプレートの使い方

ジョブテンプレートとは、ジョブの起動コマンドシーケンスのみを持ち、パラメータ値が未決定であるエンティティです。ジョブテンプレートを用いることにより、ジョブの登録のたびにコマンドシーケンスを入力しなくても、必要なパラメータ値を入力するだけでジョブの作成が行えます。Job Scheduler for CloudをSenju/DCのジョブスケジュール機能と連携するために、Job Scheduler for Cloudジョブを、Senju/DCのジョブの起動コマンドとして設定します。

AWS/Elastic MapReduceジョブフロー実行ジョブテンプレートを使用し、ジョブの起動コマンドとして利用するには、千手ブラウザのツリービューで、<ドメイン>→"ジョブスケジュール"→"ジョブ"を選択し、ジョブの新規作成を行います。

ジョブの新規作成プロパティウィンドで[ジョブテンプレートを使用]チェックボックスをチェックし、[ジョブテンプレート入力]ボタンを押して下さい。

ジョブテンプレート入力ウィンドでAWS/Elastic MapReduceジョブフロー実行ジョブテンプレートを選択し、各パラメータ値を設定して下さい。

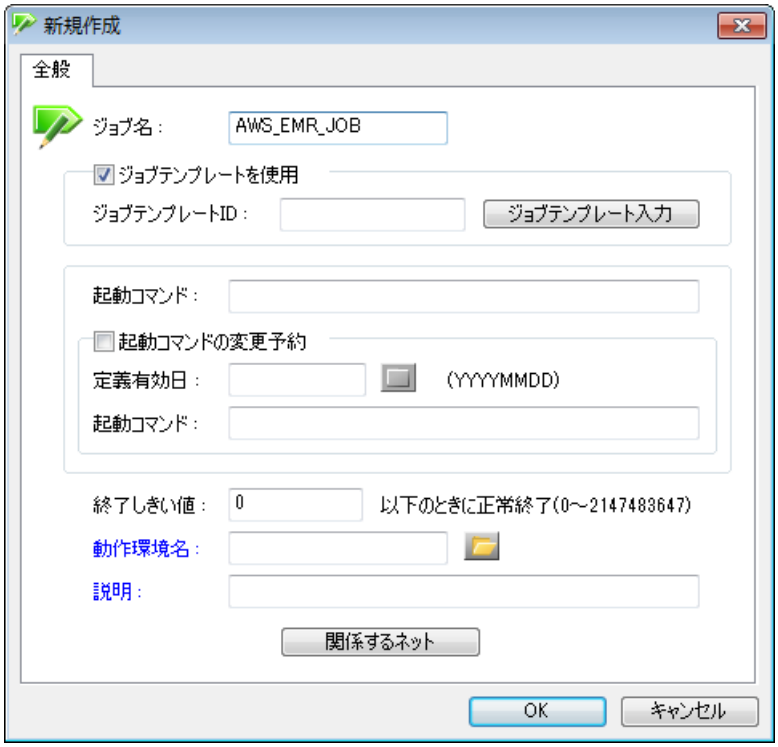


図 3.17 AWS/Elastic MapReduceジョブフロー実行ジョブテンプレートの使用

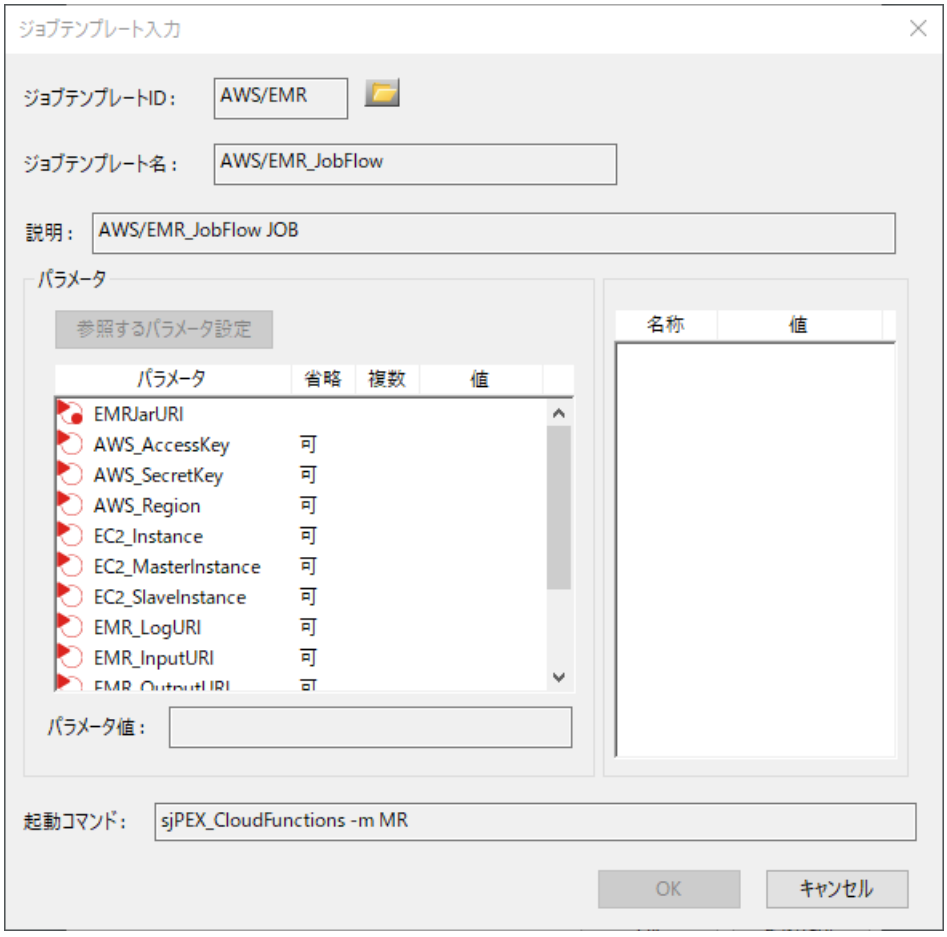


図 3.18 AWS/Elastic MapReduceジョブフロー実行ジョブテンプレートの入力

表 3.12 AWS/S3ファイル削除ジョブテンプレートの入力

パラメータ	説明
EMRJarURI	JarファイルのURI（AWS/S3上のURI）
AWS_AccessKey	AWS接続用のアクセスキーID
AWS_SecretKey	AWS接続用のシークレットアクセスキー
AWS_Region	AWSの接続先リージョン
EC2_Instance	AWS/EC2インスタンス数
EC2_MasterInstance	AWS/EC2インスタンスタイプ（マスター）
EC2_SlaveInstance	AWS/EC2インスタンスタイプ（スレーブ）
EMR_LogURI	AWS/Elastic MapReduceジョブフローのログ出力先URI
EMR_InputURI	AWS/Elastic MapReduceのインプットURI（AWS/S3上のURI）
EMR_OutputURI	AWS/Elastic MapReduceのアウトプットURI（AWS/S3上のURI）
EMR_MainClass	AWS/Elastic MapReduceのメインクラス
EMR_Parameter	AWS/Elastic MapReduceのパラメータ
Interval[sec]	チェックインターバル(秒) [10-600]

3.3.2.5.3. AWS/Elastic MapReduce ジョブフロー実行ジョブの流れ（通常時）

AWS/Elastic MapReduce ジョブフロー実行ジョブがSenju/DCのジョブスケジュールで1つのジョブとして起動されると、**「図 3-13　AWS/Elastic MapReduce ジョブフロー実行ジョブの処理の流れ」**および**「TABLE 3-14　AWS/Elastic MapReduce ジョブフロー実行ジョブの処理の流れ」**に示す流れで動きます。

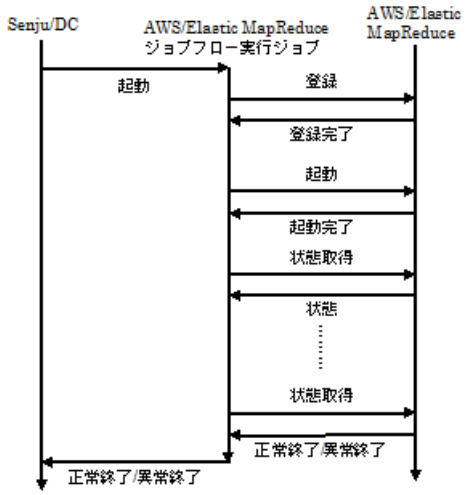


図 3.19 AWS/Elastic MapReduce ジョブフロー実行ジョブの処理の流れ

表 3.13 AWS/Elastic MapReduce ジョブフロー実行ジョブの処理の流れ

Senju/DC ジョブの状態	AWS/Elastic MapReduce ジョブフロー実行ジョブの処理内容	メッセージモニタの出力
起動待ち	起動前の状態	
稼働中	起動	
稼働中	引数に従い、AWS/Elastic MapReduceジョブフローを登録	
稼働中	登録したAWS/Elastic MapReduceジョブフローの状態を取得	
正常終了	登録したAWS/Elastic MapReduceジョブフローの実行に成功	!PEXC09 AWS/MRジョブフローの実行に成功しました。
異常終了	登録したAWS/Elastic MapReduceジョブフローの実行に失敗	!PEXC10 AWS/MRジョブフローの実行に失敗しました。

1. AWS/Elastic MapReduce ジョブフロー実行ジョブが起動されると、引数に指定された内容でAWS/Elastic MapReduce ジョブフローを登録します。
2. 登録したAWS/Elastic MapReduceジョブフローを起動します。
3. 起動したAWS/Elastic MapReduceジョブフローの状態を取得します。
4. AWS/Elastic MapReduceジョブフローが正常終了すると、実行に成功した旨のメッセージを出力し、Senju/DCジョブは正常終了します。
5. AWS/Elastic MapReduceジョブフローが何らかの理由で異常終了すると、実行に失敗した旨のメッセージを出力し、Senju/DCジョブは異常終了します。

   （異常終了時の復旧手順については「3.4.5 AWS/Elastic MapReduceジョブフロー異常終了時の復旧手順」を参照して下さい。）

3.3.2.5.4. AWS/Elastic MapReduce ジョブフロー実行ジョブの流れ（強制停止時）

AWS/Elastic MapReduce ジョブフロー実行ジョブは、他のSenju/DCのジョブと同じく強制停止させることができます。AWS/Elastic MapReduce ジョブフロー実行ジョブに対し、Senju/DCのジョブスケジュールより強制停止が行なわれると、**「図 3-14　AWS/Elastic MapReduce ジョブフロー実行ジョブの強制停止の流れ」**に示す流れで動きます。

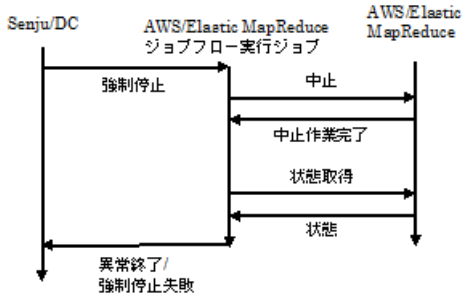


図 3.20 AWS/Elastic MapReduce ジョブフロー実行ジョブの強制停止の流れ

1. Senju/DC より、AWS/Elastic MapReduce ジョブフロー実行ジョブに強制停止をすると、AWS/Elastic MapReduceに対し、ジョブフローを中止するように依頼します。

   この段階では、AWS/Elastic MapReduce ジョブフローはまだ終了していませんが、Senju/DCのジョブスケジュールでは、ジョブの状態は異常終了となります。

3.3.2.5.5. 動作環境の環境変数の利用法

AWS/Elastic MapReduceジョブフロー実行ジョブを実行する際、該当ノードの動作環境には、以下に示す環境変数を使用できます。

環境変数に設定した値は、SJ_AWS_ARG01からSJ_AWS_ARG10までを順につなげた形で、AWS/Elastic MapRedue上で稼働するジョブフローの引数として渡されます。

環境変数	長さ	説明
SJ_AWS_ARG01	126	AWS/Elastic MapReduceのパラメータ
SJ_AWS_ARG02	126	AWS/Elastic MapReduceのパラメータ
SJ_AWS_ARG03	126	AWS/Elastic MapReduceのパラメータ
SJ_AWS_ARG04	126	AWS/Elastic MapReduceのパラメータ
SJ_AWS_ARG05	126	AWS/Elastic MapReduceのパラメータ
SJ_AWS_ARG06	126	AWS/Elastic MapReduceのパラメータ
SJ_AWS_ARG07	126	AWS/Elastic MapReduceのパラメータ
SJ_AWS_ARG08	126	AWS/Elastic MapReduceのパラメータ
SJ_AWS_ARG09	126	AWS/Elastic MapReduceのパラメータ
SJ_AWS_ARG10	126	AWS/Elastic MapReduceのパラメータ

1.上記の環境変数にはAWS/Elastic MapReduceのパラメータを一つずつ設定して下さい。

2.上記の環境変数の値には、以下の環境変数が使用できます。

```
・ SENJUHOME      :       千手ホームディレクトリ
・ SJ_PEX_DATE    :       Senju/DCジョブの運用日付
・ SJ_PEX_FRAME   :       Senju/DCジョブの所属するフレーム名
・ SJ_PEX_NET     :       Senju/DCジョブの上位ネット名
・ SJ_PEX_JOB     :       Senju/DCジョブのジョブ名
```

注釈

環境変数に設定するパラメータは、それぞれ126文字以内で設定して下さい。

3.3.2.6. AWS/Elastic MapReduceジョブフロー異常終了時の復旧手順

AWS/Elastic MapReduceジョブが異常終了した場合（「PEXC10」メッセージが出力された場合）のSenju/DCのジョブスケジュールの復旧手順を説明します。

- 手順1：ジョブフローIDの確認

  AWS/Elastic MapReduceジョブのジョブログファイルを参照し、ジョブフローIDを確認します。ジョブフローID は、ジョブログのレコードの5カラム目に出力されます。
- 手順2：AWS (Elastic MapReduce)のジョブフローを停止

  WEBブラウザからAWS Management Consoleを開き「手順1」で取得したジョブフローIDに該当するジョブフローを停止します。

  AWS/Elastic MapReduceジョブが異常終了となった状況によっては、ジョブフローIDが出力されない場合があります。
- 手順3：該当ジョブをスキップ指定

  千手ブラウザのジョブモニタから該当ジョブに対しスキップ指定を行います。
- 手順4：再ラン

  千手ブラウザのジョブモニタから該当ジョブに対し再ランを行います。上記手順を実行することにより、該当のジョブがスキップ終了となり後続のジョブが稼働します。

参考

! AWS/Elastic MapReduceジョブのジョブログの詳細は「4.3.2 Job Scheduler for Cloud(AWS/Elastic MapReduce)のジョブログファイル」を参照して下さい。

警告

AWS Management Consoleの使用方法は、Amazon Web Servicesサイトよりご確認下さい。

3.3.3. Job Scheduler for Cloud(AWS/Lambda Function)の使い方

3.3.3.1. Job Scheduler for Cloud(AWS/Lambda Function)の機能

Job Scheduler for Cloud(AWS/Lambda Function)とは、Senju/DCのジョブスケジュール機能と連携し、AWS/Lambda Functionを実行する機能です。

3.3.3.2. ポリシーの作成

AWS/Lambda Function連携機能を使用するため、**「AWS/Lambda Function連携機能に必要なアクセス権限」**に示すポリシーを作成して、ユーザーにアクセス権限を付与します。

表 3.14 AWS/Lambda Function連携機能に必要なアクセス権限

ジョブ	必要なアクセス権
AWS/Lambda Function連携ジョブ	lambda:InvokeAsync lambda:InvokeFunction

3.3.3.3. sj_aws.iniの設定

sj_aws.iniファイルは、AWSに関する情報の設定ファイルで、Job Scheduler for Cloud(AWS/Lambda Function)ジョブはこのファイルを参照します。

設定方法については、**Cloud Monitoring の sj_setup_aws ― AWS情報設定ファイル更新 ―** を参照して下さい。

sj_aws.iniに、**「TABLE 3-15　sj_aws.iniの記述内容」**に示す内容を設定して下さい。

表 3.15 sj_aws.iniの記述内容

項目	省略	デフォルト	暗号化対象	説明
accessKey	可	―	○	AWS接続用のアクセスキーID
secretKey	可	―	○	AWS接続用のシークレットアクセスキー

- 省略可能な項目を省略した場合は、Job Scheduler for Cloud(AWS/Lambda Function)ジョブのオプションで指定する必要があります。デフォルトが存在するものに関しては、省略してもデフォルト値で動作します。
- 同じ項目を、sj_aws.iniとJob Scheduler for Cloud(AWS/Lambda Function)ジョブのオプションの両方で指定した場合は、Job Scheduler for Cloud(AWS/Lambda Function)ジョブのオプションで指定した値が有効になります。
- AWS接続用のアクセスキーIDおよびシークレットアクセスキーは、Amazon Web Servicesのサイトで確認して下さい

警告

Senju/DCジョブの起動コマンドには、文字数に制限があります。なるべく各項目は省略せずに、sj_aws.iniファイルに設定して下さい。

3.3.3.4. AWS/Lambda Function連携ジョブの利用方法

AWS/Lambda Function連携ジョブは、AWS Management Consoleなどによって作成したAWS/Lambda Functionを実行します。

AWS/Lambda Function連携ジョブが起動されると、引数に指定された内容でAWS/Lambda Functionを実行し、実行結果を標準出力に出力します。

AWS/Lambda Function連携ジョブを起動する際に指定する引数には、以下に示す内容を指定して下さい。

```
sjPEX_CloudFunctions -m LS
        -fnm Lambdaファンクション名
        -lreg AWSリージョン
        [-ak アクセスキーID] [-sk シークレットアクセスキー]
        [-cctf ファンクションパラメータ(JSONファイル名)]
        [-p プロファイル名] [-ar ロールARN] [-ei AWS外部ID]
```

オプション	省略	デフォルト	長さ	説明
-fnm	不可	―	255	Lambdaファンクション名
-lreg	不可	―	32	AWSリージョン
-ak	可	―	256	AWS接続用のアクセスキーID
-sk	可	―	256	AWS接続用のシークレットアクセスキー
-cctf	可	―	255	ファンクションパラメータ(JSONファイル名)
-p	可	―	255	プロファイル名
-ar	可	―	1024	ロールARN
-ei	可	―	128	AWS外部ID

- Senju/DCジョブの起動コマンドの最大文字数は2048文字です。起動コマンドが最大文字数を超える場合は、sj_aws.iniに設定して下さい。
- 省略可能なオプションを省略した場合は、sj_aws.iniで指定した値が有効になります。
- AWS接続用のアクセスキーIDおよびシークレットアクセスキーは、Amazon Web Servicesのサイトで確認して下さい。

3.3.3.4.1. AWS/Lambda Function連携ジョブテンプレートの使い方

ジョブテンプレートとは、ジョブの起動コマンドシーケンスのみを持ち、パラメータ値が未決定であるエンティティです。ジョブテンプレートを用いることにより、ジョブの登録のたびにコマンドシーケンスを入力しなくても、必要なパラメータ値を入力するだけでジョブの作成が行えます。Job Scheduler for CloudをSenju/DCのジョブスケジュール機能と連携するために、Job Scheduler for Cloudジョブを、Senju/DCのジョブの起動コマンドとして設定します。

AWS/Lambda Function連携ジョブテンプレートを使用し、ジョブの起動コマンドとして利用するには、千手ブラウザのツリービューで、＜ドメイン＞

→“ジョブスケジュール”→“ジョブ”を選択し、ジョブの新規作成を行います。

ジョブの新規作成プロパティウィンドで[ジョブテンプレートを使用]チェックボックスをチェックし、[ジョブテンプレート入力]ボタンを押して下さい。

ジョブテンプレート入力ウィンドでAWS/Lambda Function連携ジョブテンプレートを選択し、各パラメータ値を設定して下さい。

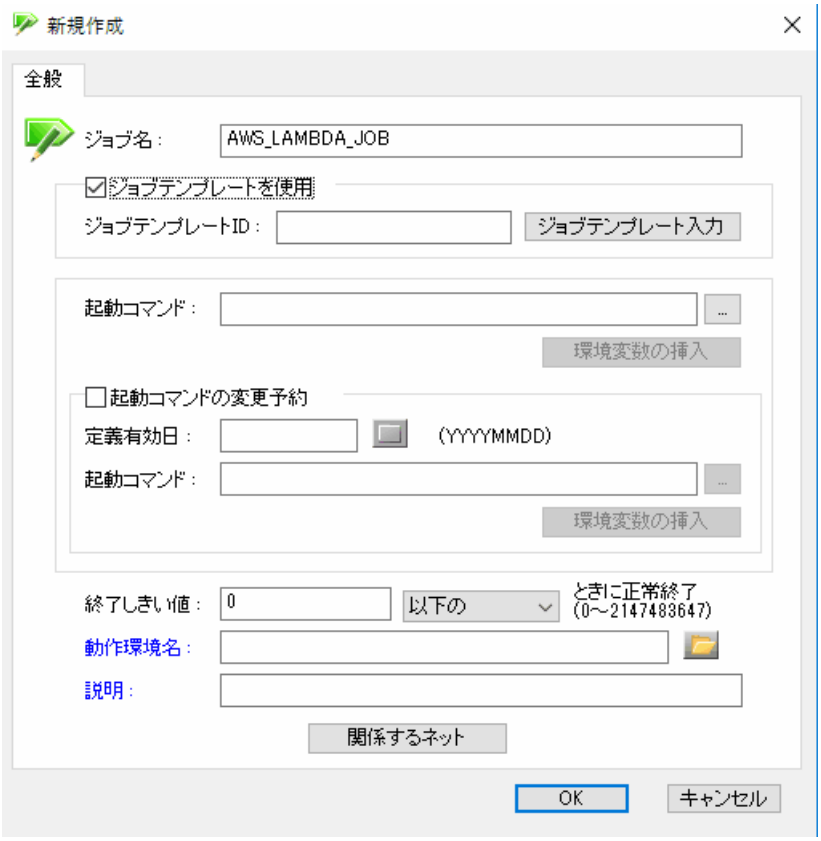


図 3.21 AWS/Lambda Function連携ジョブテンプレートの使用

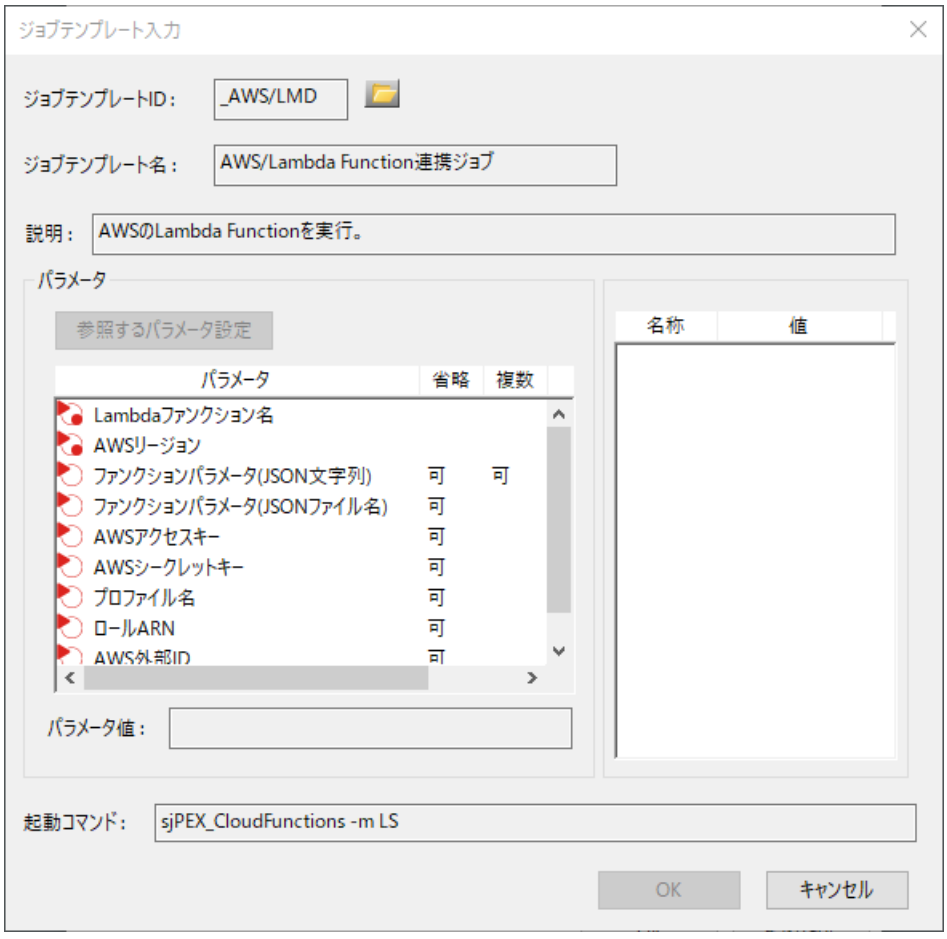


図 3.22 AWS/Lambda Function連携ジョブテンプレートの入力

表 3.16 AWS/Lambda Function連携ジョブテンプレートの入力

パラメータ	説明
Lambdaファンクション名	Lambda Function名を指定します。省略不可です。
AWSリージョン	AWS/Lambda Function所属のリージョンを指定します。省略不可です。
アクセスキーID	AWS接続用のアクセスキーIDを指定します。sj_aws.iniで指定している場合は、省略可能です。
シークレットアクセスキー	AWS接続用のシークレットアクセスキーを指定します。sj_aws.iniで指定している場合は、省略可能です。
ファンクションパラメータ(JSONファイル名)	Lambda Functionへ渡すイベントデータを記載したJSONファイル名を指定します。省略可能です。
プロファイル名	ロール認証に使用されるプロファイルを指定します。省略可能です。
ロールARN	ロール認証に使用されるロールARNを指定します。省略可能です。
AWS外部ID	ロール認証に使用される外部IDを指定します。省略可能です。

3.3.3.4.2. AWS/Lambda Function連携ジョブの処理の流れ(通常時)

AWS/Lambda Function連携ジョブがSenju/DCのジョブスケジュールで1つのジョブとして起動されると、**「図 3-17　AWS/Lambda Function連携ジョブの処理の流れ」**および**「TABLE 3-18　AWS/Lambda Function連携ジョブの処理の流れ」**に示す流れで動きます。

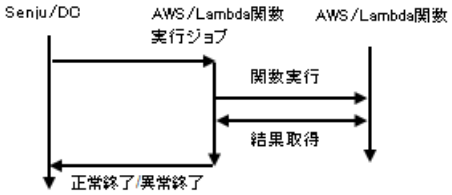


図 3.23 AWS/Lambda Function連携ジョブの処理の流れ

表 3.17 AWS/Lambda Function連携ジョブの処理の流れ

Senju/DC ジョブの状態	AWS/Lambda Function実行 ジョブの処理内容	メッセージモニタの出力
起動待ち	起動前の状態	
稼働中	起動	
稼働中	引数に従い、AWS/Lambda上の関数実行	
正常終了	AWS/Lambda上の関数実行に成功	!PEXC13 AWS/Lambda上の関数実行に成功しました。
異常終了	AWS/Lambda上の関数実行に失敗	!PEXC14 AWS/Lambda上の関数実行に失敗しました。

1. AWS/Lambda Function連携ジョブが起動されると、引数に指定された内容でAWS/Lambda Functionを実行します。
2. AWS/Lambda上の関数を実行します。
3. AWS/Lambda Functionが正しく実行されると、関数実行に成功した旨のメッセージを出力し、Senju/DCジョブは正常終了します。
4. AWS/Lambda Functionが何らかの理由で正しく実行されないと、失敗した旨のメッセージを出力し、Senju/DCジョブは異常終了します。

3.3.3.4.3. AWS/Lambda Function連携ジョブの処理の流れ（強制停止時）

AWS/Lambda Function連携ジョブは、他のSenju/DCのジョブと同じく強制停止させることができます。

Senju/DCのジョブスケジュールより、AWS/Lambda Function連携ジョブを強制停止しても、関数実行中のAWS/Lambda Functionは実行されたままとなります。

Senju/DCのジョブスケジュールでは、強制停止されたジョブの状態は異常終了となります。

3.3.4. Job Scheduler for Cloud(AWS/Step Functions)の使い方

3.3.4.1. Job Scheduler for Cloud(AWS/Step Functions)の機能

Job Scheduler for Cloud(AWS/Step Functions)とは、Senju/DCのジョブスケジュール機能と連携し、AWS/Step Functionsを実行する機能です。

3.3.4.2. ポリシーの作成

AWS/Step Functions連携機能を使用するため、**「AWS/Step Functions連携機能に必要なアクセス権限」**に示すポリシーを作成して、ユーザーにアクセス権限を付与します。

表 3.18 AWS/Step Functions連携機能に必要なアクセス権限

ジョブ	必要なアクセス権
AWS/Step Functions連携ジョブ	states:DescribeExecution states:StartExecution states:StopExecution states:StartSyncExecution

3.3.4.3. sj_aws.iniの設定

sj_aws.iniファイルは、AWSに関する情報の設定ファイルで、Job Scheduler for Cloud(AWS/Step Functions)ジョブはこのファイルを参照します。

設定方法については、**Cloud Monitoring** の **sj_setup_aws** ― **AWS情報設定ファイル更新** ― を参照して下さい。

sj_aws.iniに、**「TABLE 3-19　sj_aws.iniの記述内容」**に示す内容を設定して下さい。

表 3.19 sj_aws.iniの記述内容

項目	省略	デフォルト	暗号化対象	説明
accessKey	可	―	○	AWS接続用のアクセスキーID
secretKey	可	―	○	AWS接続用のシークレットアクセスキー
region	不可	―	○	AWS接続用のリージョン

- 省略可能な項目を省略した場合は、Job Scheduler for Cloud(AWS/Step Functions)ジョブのオプションで指定する必要があります。デフォルトが存在するものに関しては、省略してもデフォルト値で動作します。
- 同じ項目を、sj_aws.iniとJob Scheduler for Cloud(AWS/Step Functions)ジョブのオプションの両方で指定した場合は、Job Scheduler for Cloud(AWS/Step Functions)ジョブのオプションで指定した値が有効になります。
- AWS接続用のアクセスキーIDおよびシークレットアクセスキーは、Amazon Web Servicesのサイトで確認して下さい

警告

Senju/DCジョブの起動コマンドには、文字数に制限があります。なるべく各項目は省略せずに、sj_aws.iniファイルに設定して下さい。

3.3.4.4. AWS/Step Functions連携ジョブの利用方法

AWS/Step Functions連携ジョブは、AWS Management Consoleなどによって作成したAWS/Step Functionsを実行します。

AWS/Step Functions連携ジョブが起動されると、引数に指定された内容でAWS/Step Functionsを実行し、実行結果を標準出力に出力します。

AWS/Step Functions連携ジョブを起動する際に指定する引数には、以下に示す内容を指定して下さい。

```
sjPEX_CloudFunctions -m SF
        -smn ステートマシンARN
        [-ak アクセスキーID] [-sk シークレットアクセスキー]
        [-exn 実行名] [-sync]
        [-cctf ファンクションパラメータ(JSONファイル名)]
        [-i チェックインターバル]
```

オプション	省略	デフォルト	長さ	説明
-smn	不可	—	255	ステートマシンARN
-ak	可	—	256	AWS接続用のアクセスキーID
-sk	可	—	256	AWS接続用のシークレットアクセスキー
-exn	可	—	255	実行名
-sync	可	—	—	同期開始指定オプション
-cctf	可	—	255	ファンクションパラメータ(JSONファイル名)
-i	可	60	4	チェックインターバル(秒) [10-600]

- Senju/DCジョブの起動コマンドの最大文字数は2048文字です。起動コマンドが最大文字数を超える場合は、sj_aws.iniに設定して下さい。
- アクセスキーID、シークレットアクセスキーを省略した場合は、sj_aws.iniで指定した値が有効になります。
- AWS接続用のアクセスキーIDおよびシークレットアクセスキーは、Amazon Web Servicesのサイトで確認して下さい。

3.3.4.4.1. AWS/Step Functions連携ジョブテンプレートの使い方

ジョブテンプレートとは、ジョブの起動コマンドシーケンスのみを持ち、パラメータ値が未決定であるエンティティです。ジョブテンプレートを用いることにより、ジョブの登録のたびにコマンドシーケンスを入力しなくても、必要なパラメータ値を入力するだけでジョブの作成が行えます。Job Scheduler for CloudをSenju/DCのジョブスケジュール機能と連携するために、Job Scheduler for Cloudジョブを、Senju/DCのジョブの起動コマンドとして設定します。

AWS/Step Functions連携ジョブテンプレートを使用し、ジョブの起動コマンドとして利用するには、千手ブラウザのツリービューで、＜ドメイン＞→“ジョブスケジュール”→“ジョブ”を選択し、ジョブの新規作成を行います。

ジョブの新規作成プロパティウィンドで[ジョブテンプレートを使用]チェックボックスをチェックし、[ジョブテンプレート入力]ボタンを押して下さい。

ジョブテンプレート入力ウィンドでAWS/Step Functions連携ジョブテンプレートを選択し、各パラメータ値を設定して下さい。

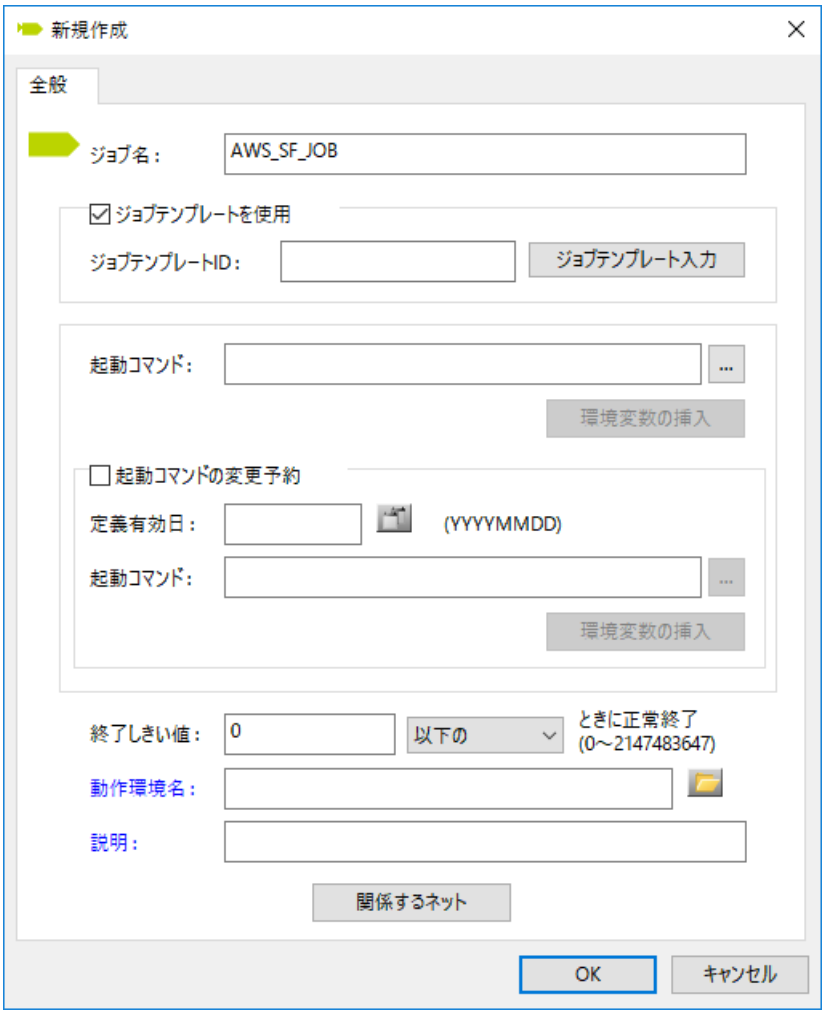


図 3.24 AWS/Step Functions連携ジョブテンプレートの使用

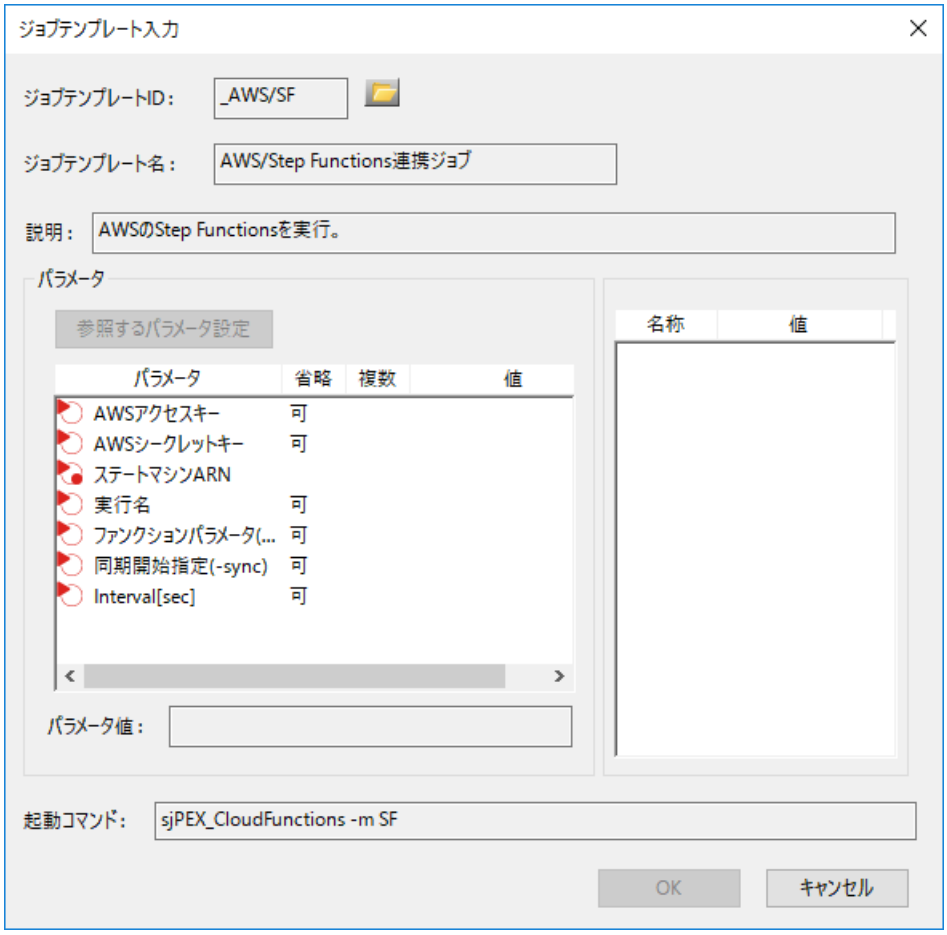


図 3.25 AWS/Step Functions連携ジョブテンプレートの入力

表 3.20 AWS/Step Functions連携ジョブテンプレートの入力

パラメータ	説明
アクセスキーID	AWS接続用のアクセスキーIDを指定します。sj_aws.iniで指定している場合は、省略可能です。
シークレットアクセスキー	AWS接続用のシークレットアクセスキーを指定します。sj_aws.iniで指定している場合は、省略可能です。
ステートマシンARN	ステートマシンのARNを指定します。省略不可です。
実行名	ステートマシンの実行名を指定します。省略可能です。
ファンクションパラメータ(JSONファイル名)	ステートマシンへ渡すパラメータを記載したJSONファイル名を指定します。マルチバイトを含む場合、エンコードは
同期開始指定(-sync)	Expressワークフローの結果ステータスを取得したい場合に指定します。省略可能です。
interval[sec]	ワークフローの実行状態取得のチェック間隔[sec]を指定します。省略可能です。

3.3.4.4.2. AWS/Step Functions連携ジョブの処理の流れ(通常時)

AWS/Step Functions連携ジョブがSenju/DCのジョブスケジュールで1つのジョブとして起動されると、**「図 3-20　AWS/Setp Functions連携ジョブの処理の流れ」**および**「TABLE 3-21　AWS/Step Functions連携ジョブの処理の流れ」**に示す流れで動きます。

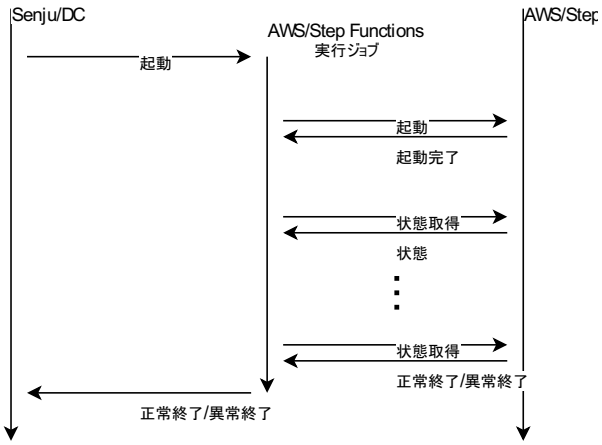


図 3.26 AWS/Step Functions連携ジョブの処理の流れ

表 3.21 AWS/Step Functions連携ジョブの処理の流れ

Senju/DC ジョブの状態	AWS/Step Functions実行 ジョブの処理内容	メッセージモニタの出力
起動待ち	起動前の状態	
稼働中	起動	
稼働中	引数に従い、AWS/Step Functionsステートマシンを実行	
正常終了	AWS/Step Functionsステートマシンの実行に成功	!PEXC23 AWS/Step Functionsの実行に成功しました。
異常終了	AWS/Step Functionsステートマシンの実行に失敗	!PEXC24 AWS/Step Functionsの実行に失敗しました。

1. AWS/Step Functions連携ジョブが起動されると、引数に指定された内容でAWS/Step Functionsを実行します。
2. AWS/Step Functionsステートマシンを実行します。
3. AWS/Step Functionsステートマシンが正常終了すると、実行に成功した旨のメッセージを出力し、Senju/DCジョブは正常終了します。
4. AWS/Step Functionsステートマシンが何らかの理由で異常終了すると、実行に失敗した旨のメッセージを出力し、Senju/DCジョブは異常終了します。

3.3.4.4.3. AWS/Step Functions連携ジョブの処理の流れ（強制停止時）

AWS/Step Functions連携ジョブは、他のSenju/DCのジョブと同じく強制停止させることができます。

Senju/DCのジョブスケジュールより、AWS/Step Functions連携ジョブを強制停止しても、実行中のAWS/Step Functionsステートマシンは実行されたままとなります。

Senju/DCのジョブスケジュールでは、強制停止されたジョブの状態は異常終了となります。

3.4. Job Scheduler for Cloud(Azure)の使い方

3.4.1. Job Scheduler for Cloud(Azure/Durable Functions)の使い方

3.4.1.1. Job Scheduler for Cloud(Azure/Durable Functions)の機能

Job Scheduler for Cloud(Azure/Durable Functions)とは、Senju/DCのジョブスケジュール機能と連携し、Azure/Durable Functionsを実行する機能です。

3.4.1.2. Azure/Durable Functions連携ジョブの利用方法

Azure/Durable Functions連携ジョブは、Azure Portalなどによって作成したDurable Functionsを実行します。

Azure/Durable Functions連携ジョブが起動されると、引数に指定された内容でDurable Functionsを実行し、実行結果を標準出力に出力します。

Azure/Durable Functions連携ジョブを起動する際に指定する引数には、以下に示す内容を指定して下さい。

```
sjPEX_CloudFunctions -m DF
        -furl ファンクションURL
        -ofnm Orchestratorファンクション名
```

オプション	省略	デフォルト	長さ	説明
-furl	不可	—	1024	ファンクションURL
-ofnm	不可	—	255	Orchestratorファンクション名

- Senju/DCジョブの起動コマンドの最大文字数は2048文字です。
- ファンクションURLおよびOrchestratorファンクション名は、Microsoft Azureサイトで確認して下さい。

3.4.1.2.1. Azure/Durable Functions連携ジョブテンプレートの使い方

ジョブテンプレートとは、ジョブの起動コマンドシーケンスのみを持ち、パラメータ値が未決定であるエンティティです。ジョブテンプレートを用いることにより、ジョブの登録のたびにコマンドシーケンスを入力しなくても、必要なパラメータ値を入力するだけでジョブの作成が行えます。Job Scheduler for CloudをSenju/DCのジョブスケジュール機能と連携するために、Job Scheduler for Cloudジョブを、Senju/DCのジョブの起動コマンドとして設定します。

Azure/Durable Functions連携ジョブテンプレートを使用し、ジョブの起動コマンドとして利用するには、千手ブラウザのツリービューで、＜ドメイン＞→“ジョブスケジュール”→“ジョブ”を選択し、ジョブの新規作成を行います。

ジョブの新規作成プロパティウィンドで[ジョブテンプレートを使用]チェックボックスをチェックし、[ジョブテンプレート入力]ボタンを押して下さい。

ジョブテンプレート入力ウィンドでAzure/Durable Functions連携ジョブテンプレートを選択し、各パラメータ値を設定して下さい。

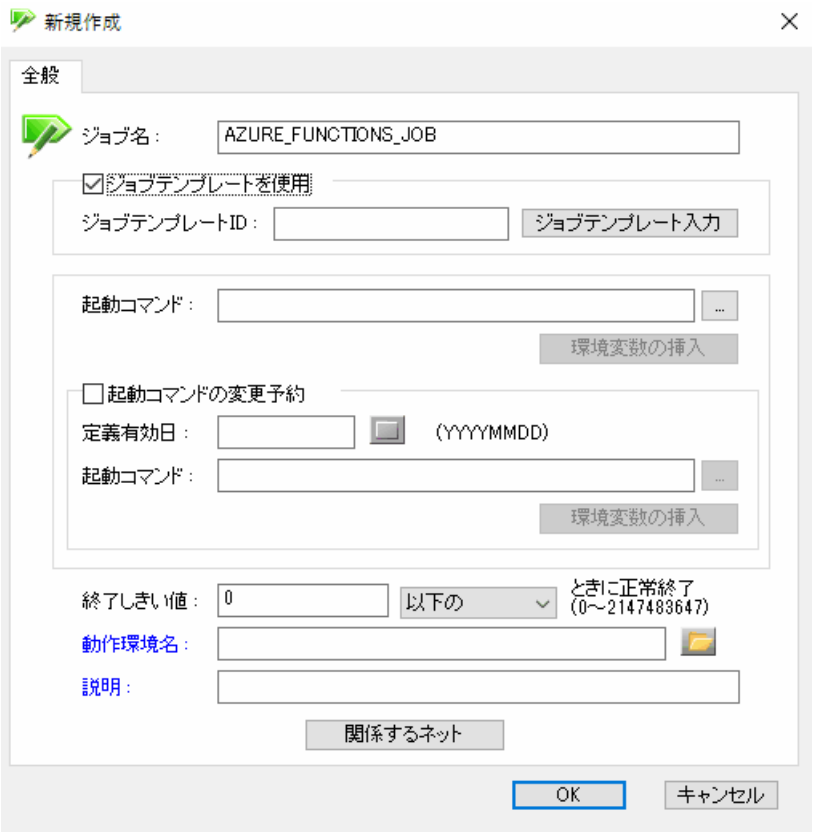


図 3.27 Azure/Durable Functions連携ジョブテンプレートの使用

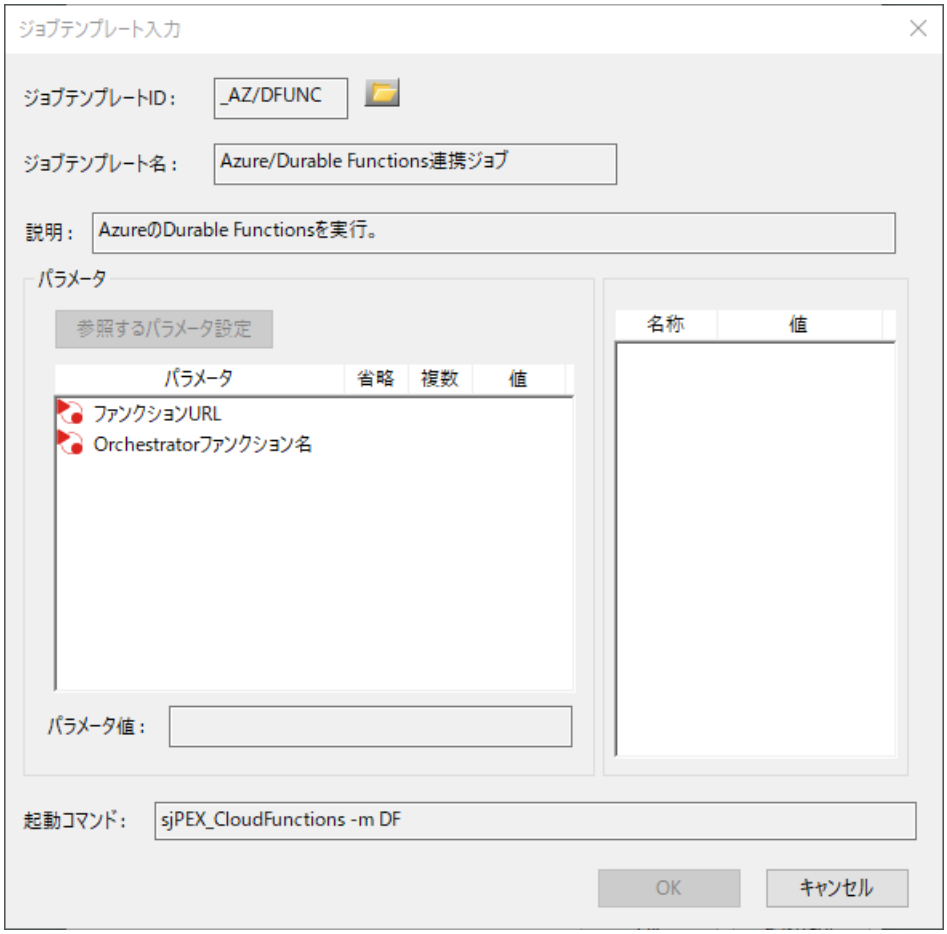


図 3.28 Azure/Durable Functions連携ジョブテンプレートの入力

表 3.22 Azure/Durable Functions連携ジョブテンプレートの入力

パラメータ	説明
ファンクションURL	Durable FunctionsのURLを指定します。省略不可です。
Orchestratorファンクション名	Durable FunctionsのOrchestratorファンクション名を指定します。省略不可です。

3.4.1.2.2. Azure/Durable Functions連携ジョブの処理の流れ(通常時)

Azure/Durable Functions連携ジョブがSenju/DCのジョブスケジュールで1つのジョブとして起動されると、**「図 4-3　Azure/Durable Functions連携ジョブの処理の流れ」**および**「TABLE 4-3　Azure/Durable Functions連携ジョブの処理の流れ」**に示す流れで動きます。

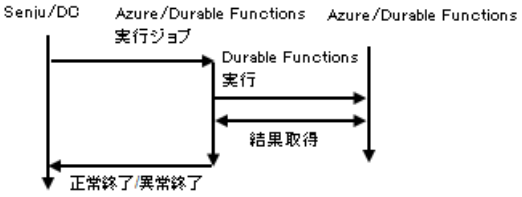


図 3.29 Azure/Durable Functions連携ジョブの処理の流れ

表 3.23 Azure/Durable Functions連携ジョブの処理の流れ

Senju/DC ジョブの状態	Azure/Durable Functions実行 ジョブの処理内容	メッセージモニタの出力
起動待ち	起動前の状態	
稼働中	起動	
稼働中	引数に従い、Azure/Durable Functions上の関数実行	
正常終了	Azure/Durable Functions実行に成功	!PEXC15 Azure/Functionsの関数実行に成功しました。
異常終了	Azure/Durable Functions実行に失敗	!PEXC16 Azure/Functionsの関数実行に失敗しました。

1. Azure/Durable Functions連携ジョブが起動されると、引数に指定された内容でAzure/Durable Functionsを実行します。
2. Azure/Durable Functionsを実行します。
3. Durable Functionsが正しく実行されると、成功した旨のメッセージを出力し、Senju/DCジョブは正常終了します。
4. Durable Functionsが何らかの理由で正しく実行されないと、失敗した旨のメッセージを出力し、Senju/DCジョブは異常終了します。

3.4.1.2.3. Azure/Durable Functions連携ジョブの処理の流れ（強制停止時）

Azure/Durable Functions連携ジョブは、他のSenju/DCのジョブと同じく強制停止させることができます。

Senju/DCのジョブスケジュールより、Azure/Durable Functions連携ジョブを強制停止しても、関数実行中のAzure/Durable Functionsは実行されたままとなります。

Senju/DCのジョブスケジュールでは、強制停止されたジョブの状態は異常終了となります。

3.5. Job Scheduler for Cloud(Google Cloud)の使い方

3.5.1. Job Scheduler for Cloud(Google Cloud Functions)の使い方

3.5.1.1. Job Scheduler for Cloud(Google Cloud Functions)の機能

Job Scheduler for Cloud(Google Cloud Functions)とは、Senju/DCのジョブスケジュール機能と連携し、Google Cloud Functionsを実行する機能です。

3.5.1.2. Google Cloud連携機能の設定

- **説明**

  ジョブスケジュールサブシステムを用いてGoogle Cloud Functions連携機能を使用するための設定を行います。

- **設定手順**

  Google Cloud Functions連携機能を設定するには以下の手順が必要です。

  - Google Cloudアカウントの登録
  - 認証設定
  - Google Cloud情報設定ファイルの作成

3.5.1.2.1. Google Cloudアカウントの登録

Google Cloud Functions連携機能の利用において、事前にGoogle Cloud サービスアカウントの登録が必要です。Google Cloudサイトよりアカウント登録を行って下さい。

3.5.1.2.1.1. ロールの作成

Google Cloud Functions連携機能を使用するため、**「Google Cloud Functions連携機能に必要なアクセス権限」**に示すアクセス権限を付与したロールを作成して下さい。

表 3.24 Google Cloud Functions連携機能に必要なアクセス権限

ジョブ	必要なアクセス権
Google Cloud Functions連携ジョブ	cloudfunctions.functions.call

3.5.1.2.1.2. サービスアカウントの作成

Google Cloud Functions連携機能を使用するためにはサービスアカウントによる認証が必要となります。Google Cloudサイトよりサービスアカウントの作成を行って下さい。サービスアカウントの作成時に、ロールの作成 で作成したロールを割り当てて下さい。

3.5.1.2.2. 認証設定

3.5.1.2.2.1. Compute Engineにサービスアカウントを設定し認証する

Google Cloud内のエージェントからGoogle Cloud Functions連携機能を実行する場合は、エージェントとなるCompute Engineにサービスアカウントを割り当てて認証します。Google CloudサイトよりCompute Engineのインスタンスにサービスアカウントを関連付けて下さい。また、Google Cloud情報設定ファイル(sj_gcp_sys.json)の作成 でGoogle Cloud情報設定ファイルにプロジェクトIDを設定して下さい。

3.5.1.2.2.2. APIキーで認証する

Google Cloud外のエージェントからGoogle Cloud Functions連携機能を実行する場合は、エージェントからサービスアカウントで作成したAPIキーの認証ファイルを利用して認証します。Google CloudサイトよりサービスアカウントからAPIキーを作成し、APIキー認証ファイルをダウンロードして下さ

い。ダウンロードしたAPIキー認証ファイルをエージェントの千手稼働アカウントでアクセスできる位置に配置し、Google Cloud情報設定ファイル(sj_gcp_sys.json)の作成 でGoogle Cloud情報設定ファイルにAPIキー認証ファイルのパスを設定して下さい。

3.5.1.2.3. Google Cloud情報設定ファイル(sj_gcp_sys.json)の作成

sj_gcp_sys.jsonファイルは、Google Cloudに関する情報の設定ファイルです。sj_gcp_sys.jsonとGoogle Cloud Functions連携ジョブのパラメータの両方でAPIキー認証ファイルを指定した場合は、Google Cloud Functions連携ジョブのパラメータで指定した値が有効になります。

設定方法については、**Cloud Monitoring** の **sj_setup_gcp** ー **Google Cloud情報設定ファイル更新** ー を参照して下さい。

Google Cloud情報設定ファイル(dat/opt/sj_gcp_sys.json)を作成し、以下の項目を設定して下さい。

表 3.25 sj_gcp_sys.jsonの記述内容

項目	省略	デフォルト	暗号化対象	説明
proxyURL	可	—	×	Google Cloud接続時に経由するプロキシサーバー。(次の形式で記載して下さい "<プロトコル
proxyUsername	可	—	×	プロキシサーバーアクセス用ユーザーID
proxyPassword	可	—	○	プロキシサーバーアクセス用パスワード(暗号化後のパスワード)
project_id	可	—	×	Compute Engineにサービスアカウントを割り当てた場合の認証用プロジェクトID
accountFilePath	可	—	×	サービスアカウントのAPIキー認証ファイルの絶対パス

- project_idはCompute Engineにサービスアカウントを割り当てた場合に指定して下さい。
- accountFilePathは、APIキーによる認証を行う場合に指定して下さい。
- proxyUsernameおよびproxyPasswordの両方を指定しなかった場合、プロキシサーバーの認証に利用しません。

3.5.1.3. Google Cloud Functions連携ジョブの利用方法

Google Cloud Functions連携ジョブは、Google Cloud Consoleなどによって作成したGoogle Cloud Functionsを実行します。

Google Cloud Functions連携ジョブが起動されると、引数に指定された内容でGoogle Cloud Functionsを実行し、実行結果を標準出力に出力します。

Google Cloud Functions連携ジョブを起動する際に指定する引数には、以下に示す内容を指定して下さい。

```
sjPEX_CloudFunctions -m GF
        -gfnm Google Cloudファンクション名
        -gfr Google Cloudリージョン
        -gfdf ファンクションパラメータ(JSONファイル名)
        -gaf Google Cloudの認証ファイル
```

オプション	省略	デフォルト	長さ	説明
-gfnm	不可	—	—	Google Cloudファンクション名
-gfr	不可	—	—	Google Cloudリージョン
-gfdf	可	—	—	ファンクションパラメータ(JSONファイル名)
-gaf	可	—	—	Google CloudのAPIキー認証ファイル

- Senju/DCジョブの起動コマンドの最大文字数は2048文字です。
- Google Cloudファンクション名およびGoogle Cloudリージョンは、Google Cloudサイトで確認して下さい。

3.5.1.3.1. Google Cloud Functions連携ジョブテンプレートの使い方

ジョブテンプレートとは、ジョブの起動コマンドシーケンスのみを持ち、パラメータ値が未決定であるエンティティです。ジョブテンプレートを用いることにより、ジョブの登録のたびにコマンドシーケンスを入力しなくても、必要なパラメータ値を入力するだけでジョブの作成が行えます。Job Scheduler for CloudをSenju/DCのジョブスケジュール機能と連携するために、Job Scheduler for Cloudジョブを、Senju/DCのジョブの起動コマンドとして設定します。

Google Cloud Functions連携ジョブテンプレートを使用し、ジョブの起動コマンドとして利用するには、千手ブラウザのツリービューで、<ドメイン>→“ジョブスケジュール”→“ジョブ”を選択し、ジョブの新規作成を行います。

ジョブの新規作成プロパティウィンドで[ジョブテンプレートを使用]チェックボックスをチェックし、[ジョブテンプレート入力]ボタンを押して下さい。

ジョブテンプレート入力ウィンドでGoogle Cloud Functions連携ジョブテンプレートを選択し、各パラメータ値を設定して下さい。

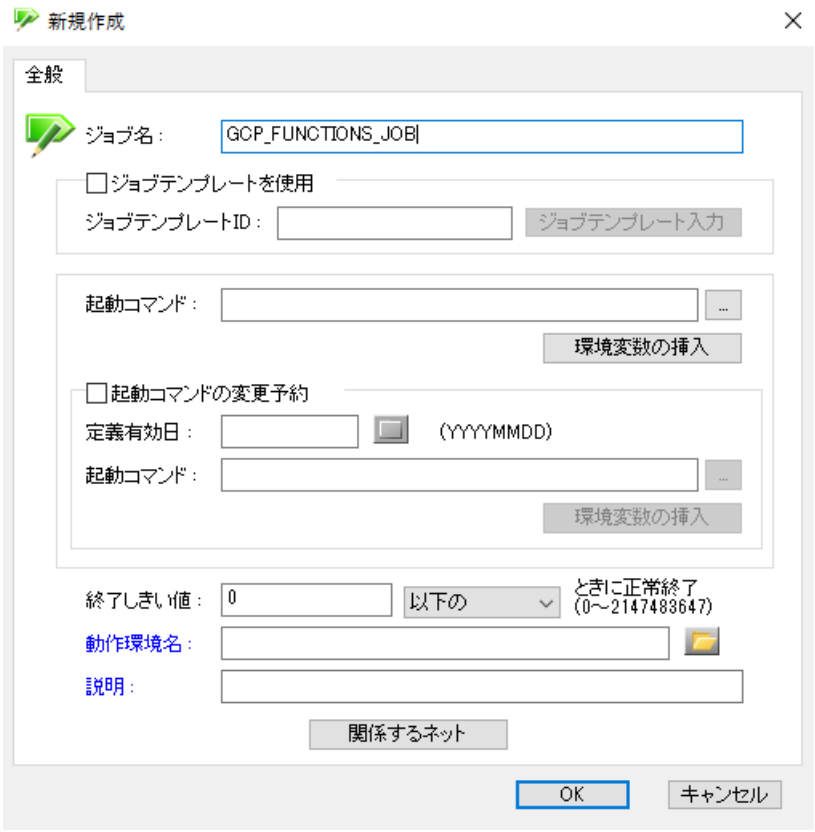


図 3.30 Google Cloud Functions連携ジョブテンプレートの使用

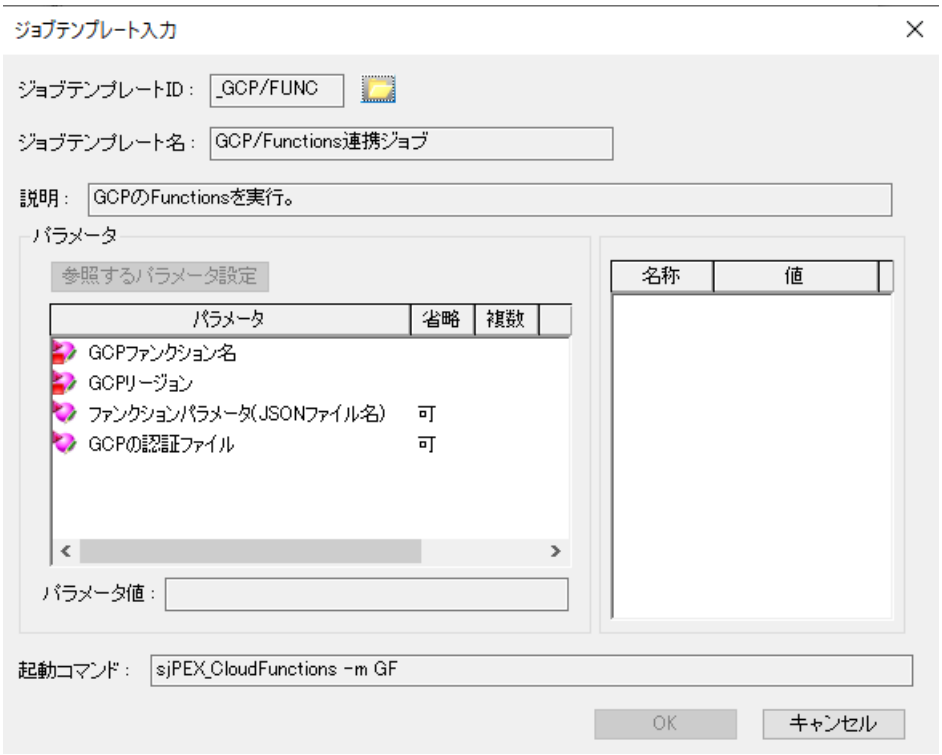


図 3.31 Google Cloud Functions連携ジョブテンプレートの入力

表 3.26 Google Cloud Functions連携

パラメータ	説明
GCPファンクション名	Google Cloud Functionsの名前を指定します。省略不可です。
GCPリージョン	Google Cloud Functionsが存在するリージョンを指定します。省略不可です。
ファンクションパラメータ（JSONファイル名）	Google Cloud Functionsへ渡す引数が記載されたJSONファイルを絶対パスで指定します。必要ない場合
GCPの認証ファイル	Google CloudのAPIキー認証ファイルを絶対パスで指定します。sj_gcp_sys.json で指定した場合、または

3.5.1.3.2. Google Cloud Functions連携ジョブの処理の流れ(通常時)

Google Cloud Functions連携ジョブがSenju/DCのジョブスケジュールで1つのジョブとして起動されると、**「図 5-3　Google Cloud Functions連携ジョブの処理の流れ」**および**「TABLE 5-5　Google Cloud Functions連携ジョブの処理の流れ」**に示す流れで動きます。

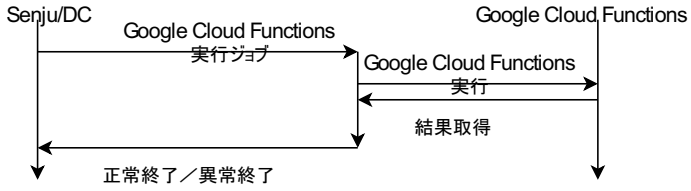


図 3.32 Google Cloud Functions連携ジョブの処理の流れ

表 3.27 Google Cloud Functions連携ジョブの処理の流れ

Senju/DC ジョブの状態	Google Cloud Functions実行 ジョブの処理内容	メッセージモニタの出力
起動待ち	起動前の状態	
稼働中	起動	
稼働中	引数に従い、Google Cloud Functions上の関数実行	
正常終了	Google Cloud Functions実行に成功	!PEXC17 Google Cloud Functionsの関数実行に成功しました。
異常終了	Google Cloud Functions実行に失敗	!PEXC18 Google Cloud Functionsの関数実行に失敗しました。

1. Google Cloud Functions連携ジョブが起動されると、引数に指定された内容でGoogle Cloud Functionsを実行します。
2. Google Cloud Functionsを実行します。
3. Google Cloud Functionsが正しく実行されると、成功した旨のメッセージを出力し、Senju/DCジョブは正常終了します。
4. Google Cloud Functionsが何らかの理由で正しく実行されないと、失敗した旨のメッセージを出力し、Senju/DCジョブは異常終了します。

3.5.1.3.3. Google Cloud Functions連携ジョブの処理の流れ（強制停止時）

Google Cloud Functions連携ジョブは、他のSenju/DCのジョブと同じく強制停止させることができます。

Senju/DCのジョブスケジュールより、Google Cloud Functions連携ジョブを強制停止しても、関数実行中のGoogle Cloud Functionsは実行されたままとなります。

Senju/DCのジョブスケジュールでは、強制停止されたジョブの状態は異常終了となります。

3.5.2. Job Scheduler for Cloud(Google Cloud Composer)の使い方

3.5.2.1. Job Scheduler for Cloud(Google Cloud Composer)の機能

Job Scheduler for Cloud(Google Cloud Composer)とは、ユーザコマンド機能と連携し、Google Cloud ComposerのDAGに対し各種操作

を行う機能です。

3.5.2.2. Google Cloud Composer連携機能の設定

- **説明**

  Google Cloud Composer連携機能を使用するための設定を行います。

- **設定手順**

  Google Cloud Composer連携機能を設定するには以下の手順が必要です。

  - Google Cloudアカウントの登録
  - 認証設定
  - Google Cloud情報設定ファイルの作成
  - Google Cloud Composer APIの設定
  - Google Cloud SDK、Python、Kubectlのインストール

3.5.2.2.1. Google Cloudアカウントの登録

Google Cloud Composer連携機能の利用において、事前にGoogle Cloud サービスアカウントの登録が必要です。Google Cloudサイトよりアカウント登録を行って下さい。

3.5.2.2.1.1. ロールの作成

Google Cloud Composer連携機能を使用するため、**「Google Cloud Composer連携機能に必要なアクセス権限」**に示すアクセス権限を付与したロールを作成して下さい。

表 3.28 Google Cloud Composer連携機能に必要なアクセス権限

コマンド	必要なアクセス権
Google Cloud Composer	storage.objects.* composer.environments.get container.clusters.get container.clusters.list container.clusters.getCredentials container.namespaces.list container.namespaces.get container.pods.list container.pods.get container.pods.exec

3.5.2.2.1.2. サービスアカウントの作成

Google Cloud Composer連携機能を使用するためにはサービスアカウントによる認証が必要となります。Google Cloudサイトよりサービスアカウントの作成を行って下さい。サービスアカウントの作成時に、ロールの作成 で作成したロールを割り当てて下さい。

3.5.2.2.2. 認証設定

3.5.2.2.2.1. Compute Engineにサービスアカウントを設定し認証する

Google Cloud内のエージェントからGoogle Cloud Composer連携機能を実行する場合は、エージェントとなるCompute Engineにサービスアカウントを割り当てて認証します。Google CloudサイトよりCompute Engineのインスタンスにサービスアカウントを関連付けて下さい。また、Google Cloud情報設定ファイル(sj_gcp_sys.json)の作成 でGoogle Cloud情報設定ファイルにプロジェクトIDを設定して下さい。

3.5.2.2.2.2. APIキーで認証する

Google Cloud外のエージェントからGoogle Cloud Composer連携機能を実行する場合は、エージェントからサービスアカウントで作成したAPIキーの認証ファイルを利用して認証します。Google CloudサイトよりサービスアカウントからAPIキーを作成し、APIキー認証ファイルをダウンロードして下さい。ダウンロードしたAPIキー認証ファイルをエージェントの千手稼働アカウントでアクセスできる位置に配置し、Google Cloud情報設定ファイル(sj_gcp_sys.json)の作成 でGoogle Cloud情報設定ファイルにAPIキー認証ファイルのパスを設定して下さい。

3.5.2.2.3. Google Cloud情報設定ファイル(sj_gcp_sys.json)の作成

sj_gcp_sys.jsonファイルは、Google Cloudに関する情報の設定ファイルです。sj_gcp_sys.jsonとGoogle Cloud Composer連携コマンドのパラメータの両方でAPIキー認証ファイルを指定した場合は、Google Cloud Composer連携コマンドのパラメータで指定した値が有効になります。

設定方法については、**Cloud Monitoring** の **sj_setup_gcp** ー **Google Cloud情報設定ファイル更新** ー を参照して下さい。

Google Cloud情報設定ファイル(dat/opt/sj_gcp_sys.json)を作成し、以下の項目を設定して下さい。

表 3.29 sj_gcp_sys.jsonの記述内容

項目	省略	デフォルト	暗号化対象	説明
proxyURL	可	—	×	Google Cloud接続時に経由するプロキシサーバー。(次の形式で記載して下さい "<プロトコル
proxyUsername	可	—	×	プロキシサーバーアクセス用ユーザーID
proxyPassword	可	—	○	プロキシサーバーアクセス用パスワード(暗号化後のパスワード)
project_id	可	—	×	Compute Engineにサービスアカウントを割り当てた場合の認証用プロジェクトID
accountFilePath	可	—	×	サービスアカウントのAPIキー認証ファイルの絶対パス

- project_idはCompute Engineにサービスアカウントを割り当てた場合に指定して下さい。
- accountFilePathは、APIキーによる認証を行う場合に指定して下さい。
- proxyUsernameおよびproxyPasswordの両方を指定しなかった場合、プロキシサーバーの認証に利用しません。

3.5.2.2.4. Google Cloud Composer APIの設定

Google Cloud Composer連携機能の利用において、事前にGoogle Cloud Composer APIを有効にします。

設定方法については、https://cloud.google.com/composer/docs/composer-2/access-airflow-api?hl=ja をご覧ください。

3.5.2.2.5. Google Cloud SDK、Python、Kubectlのインストール

- Google Cloud SDKをインストールします。

  ※手順については、https://cloud.google.com/sdk/docs/install をご覧ください。

- Google Cloud SDKをインストール時にバンドされているPython もインストールします。

  単独でインストールする場合、下記コマンドを利用できます。

  ※インストール用のコマンド:

  gcloud components install app-engine-python (sudo yum install google-cloud-cli-app-engine-python)

- Google Cloud SDKからkubectlをインストールします。

  ※インストール用のコマンド:

  gcloud components install kubectl (sudo yum install kubectl)

- $SENJUHOME/dat/opt/sjusershrcの変更

  ※モジュール適用対象ノードにGoogle Cloud SDKがインストール済みだった場合、以下の手順は不要です。

  インストールした際に追加された$SENJUHOME/.bashrcの内容を、$SENJUHOME/dat/opt/sjusershrcに追加します。

  (記載例)

```
# The next line updates PATH for the Google Cloud SDK.
if [ -f '/home/senju/google-cloud-sdk/path.bash.inc' ]; then . '/home/senju/google-cloud-
sdk/path.bash.inc'; fi
# The next line enables shell command completion for gcloud.
if [ -f '/home/senju/google-cloud-sdk/completion.bash.inc' ]; then . '/home/senju/google-
cloud-sdk/completion.bash.inc'; fi
```

3.5.2.3. Google Cloud Composer連携コマンドの利用方法

Google Cloud Composer連携コマンドは、ユーザーが自由にユーザコマンドを登録することができます。

ユーザコマンドからGoogle Cloud ComposerのDAGに対し各種操作を行います。

注釈

起動シーケンスにコマンド「remsh」を記載していますが、Windowsの場合、sj_remshe.exeに変更して下さい。
起動シーケンスに[\"]を記載していますが、Windowsの場合、[\\\"]変更して下さい。

3.5.2.3.1. タスクのクリア・起動

- タスクのクリア・起動コマンドの登録

起動シーケンス:

```
remsh "@ノード名@" -l "@ユーザ名@" sjPEX_GCPCloudComposer -m ctk -pj \"@projectId@\" -env
\"@environment@\" -loc \"@location@\" -did \"@DAGID@\" -tr \"@@taskRegex@@\" -us
\"@@upstream@@\" -ds \"@@downstream@@\" -of \"@@onlyFailed@@\" -sd \"##開始日付##\" -ed \"##終了
日付##\" -gaf \"@@認証ファイル@@\"
```

- タスクのクリア・起動コマンドの使用

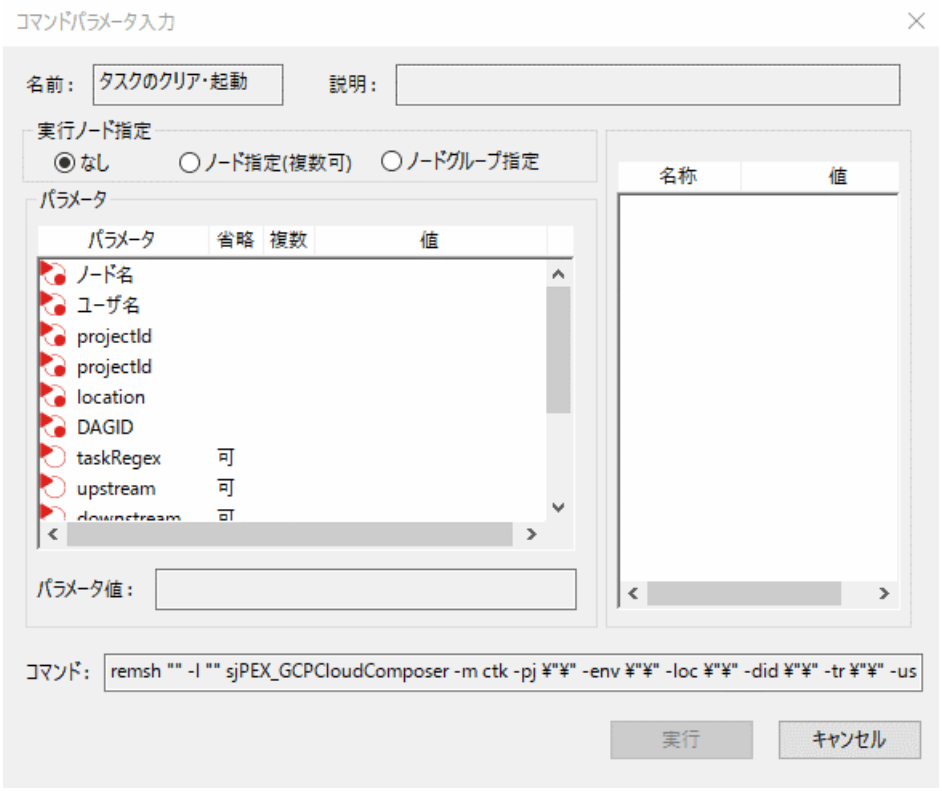


図 3.33 タスクのクリア・起動コマンドの使用

表 3.30 タスクのクリア・起動コマンドの入力

パラメータ名	タイプ	省略	デフォルト	概要
projectId	文字列	不可	_	composer環境が所属するプロジェクトIDを指定します。
environment	文字列	不可	_	composer環境の名称を指定します。
location	文字列	不可	_	composer環境のlocationを指定します。
DAGID	文字列	不可	_	DAGIDを指定します。
taskRegex	文字列	可	(空)	タスク正規表現を指定します。
upstream	文字列	可	true	false:指定したタスクのみクリア; true:upstreamタスクもクリアします。
downstream	文字列	可	true	false:指定したタスクのみクリア; true:downstreamタスクもクリアします。
onlyFailed	文字列	可	true	false:条件を満たすタスクをクリア; true:Failedのタスクのみクリアします。
start-date	文字列	可	(空)	開始日付(UTC)を指定します。(YYYY-MM-DD;YYYY-MM-DDT00:0
end-date	文字列	可	(空)	終了日付(UTC)を指定します。(YYYY-MM-DD;YYYY-MM-DDT00:0
認証ファイル	文字列	可	Google Cloud情報設定ファイルから取得	認証Jsonファイルを指定します。

3.5.2.3.2. タスクのMark Failed

- タスクのMark Failedコマンドの登録

起動シーケンス:

```
remsh "@ノード名@" -l "@ユーザ名@" sjPEX_GCPCloudComposer -m mf -url \"@airflowWebUi@\" -did
\"@DAGID@\" -tid \"@タスクID@\" -exed \"#実行日付#\" -us \"@@upstream@@\" -ds \"@@downstream@@\" -
gaf \"@@認証ファイル@@\"
```

- タスクのMark Failedコマンドの使用

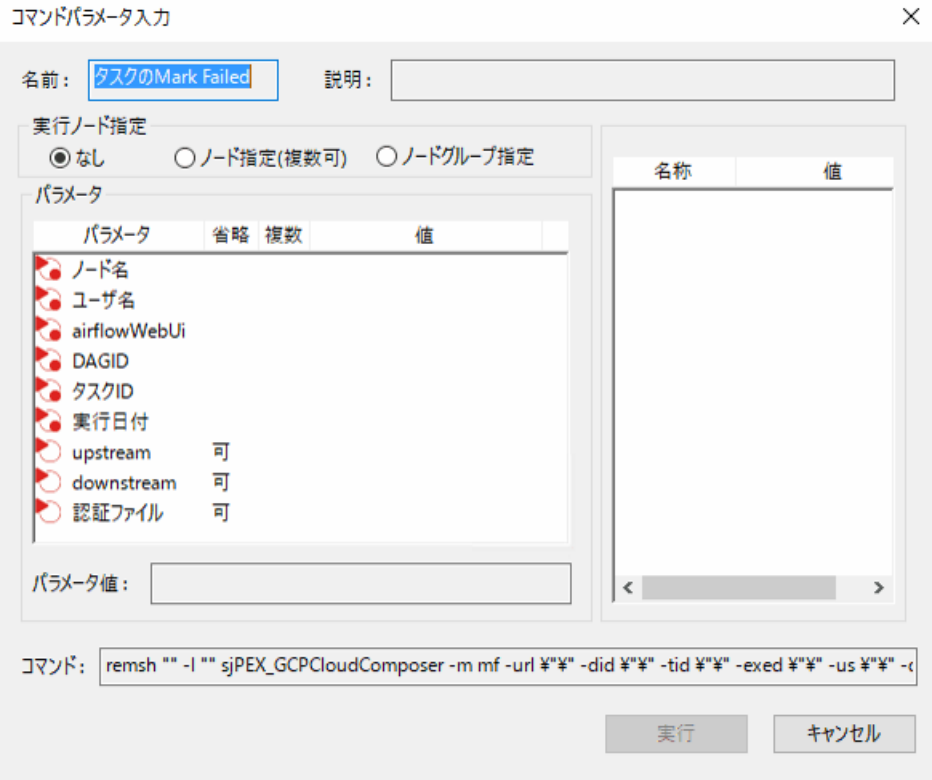


図 3.34 タスクのMark Failedコマンドの使用

表 3.31 タスクのMark Failedコマンドの入力

パラメータ名	タイプ	省略	デフォルト	概要
airflowWebUi	文字列	不可	_	composer環境のairflowWebUiを指定します。
DAGID	文字列	不可	_	DAGIDを指定します。
タスクID	文字列	不可	_	タスクIDを指定します。
実行日付	文字列	不可	_	executionDateを指定します。
upstream	文字列	可	true	false:指定したタスクのみ実施;true:upstreamタスクも実施します。
downstream	文字列	可	true	false:指定したタスクのみ実施;true:downstreamタスクも実施します。
認証ファイル	文字列	可	GoogleCloud情報設定ファイルから取得	認証Jsonファイルを指定します。

3.5.2.3.3. DAGのMark Failed

- DAGのMark Failedコマンドの登録

起動シーケンス:

```
remsh "@ノード名@" -l "@ユーザ名@" sjPEX_GCPCloudComposer -m dmf -url \"@airflowWebUi@\" -did
\"@DAGID@\" -eid \"@実行ID@\" -gaf \"@@認証ファイル@@\"
```

- DAGのMark Failedコマンドの使用

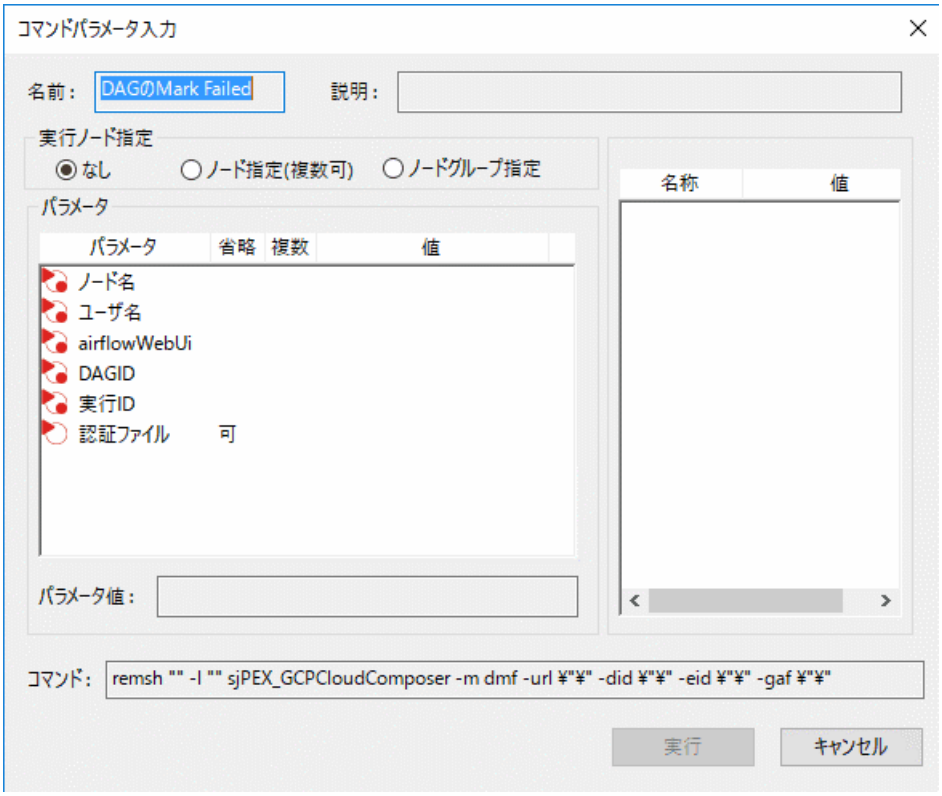


図 3.35 DAGのMark Failedコマンドの使用

表 3.32 DAGのMark Failedコマンドの入力

パラメータ名	タイプ	省略	デフォルト	概要
airflowWebUi	文字列	不可	_	composer環境のairflowWebUiを指定します。
DAGID	文字列	不可	_	DAGIDを指定します。
実行ID	文字列	不可	_	実行IDを指定します。
認証ファイル	文字列	可	GoogleCloud情報設定ファイルから取得	認証Jsonファイルを指定します。

3.5.2.3.4. タスクの強制起動

- タスクの強制起動コマンドの登録

起動シーケンス:

```
remsh "@ノード名@" -l "@ユーザ名@" sjPEX_GCPCloudComposer -m trk -pj \"@projectId@\" -env
\"@environment@\" -loc \"@location@\" -did \"@DAGID@\" -tid \"@タスクID@\" -eid \"@実行ID@\" -igd
\"@@ignoreDependencies@@\" -f \"@@force@@\" -gaf \"@@認証ファイル@@\"
```

- タスクの強制起動コマンドの使用

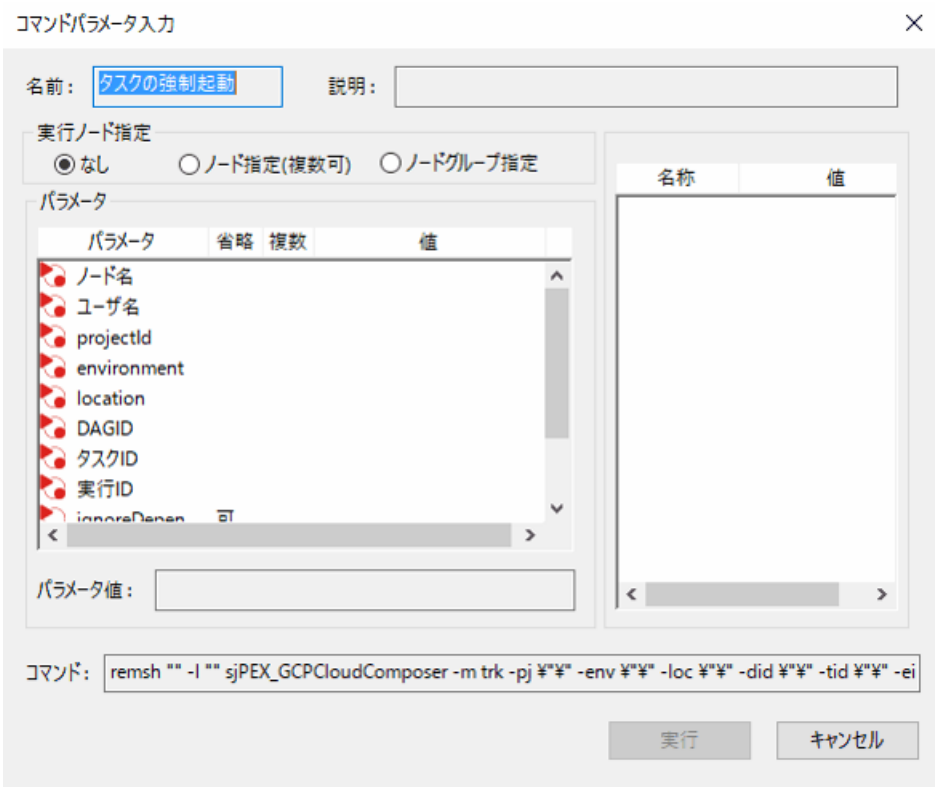


図 3.36 タスクの強制起動コマンドの使用

表 3.33 タスクの強制起動コマンドの入力

パラメータ名	タイプ	省略	デフォルト	概要
projectId	文字列	不可	_	composer環境が所属するプロジェクトIDを指定します。
environment	文字列	不可	_	composer環境の名称を指定します。
location	文字列	不可	_	composer環境のlocationを指定します。
DAGID	文字列	不可	_	DAGIDを指定します。
タスクID	文字列	不可	_	タスクIDを指定します。
実行ID(実行日付)	文字列	不可	_	実行ID(実行日付)を指定します。(日付例：2022-09-24T12:51
ignoreDependencies	文字列	可	true	false:先行が終わらないと実施しない;true:先行が終わらなくても
force	文字列	可	true	false:Success済みは実施しない;true:Success済みでも実施
認証ファイル	文字列	可	GoogleCloud情報設定ファイルから取得	認証Jsonファイルを指定します。

注釈

パラメータ「実行ID(実行日付)」はairflow Version2.2.0以下の場合、実行日付のみサポートします。

3.5.2.3.5. DAGの強制起動

- DAGの強制起動コマンドの登録

起動シーケンス：

```
remsh "@ノード名@" -l "@ユーザ名@" sjPEX_GCPCloudComposer -m dr -url \"@airflowWebUi@\" -did
\"@DAGID@\" -eid \"@@実行ID@@\" -ld \"@@logicalDate@@\" -df \"@@DAGパラメータ(JSONファイル名)@@\" -gaf
\"@@認証ファイル@@\"
```

- DAGの強制起動コマンドの使用

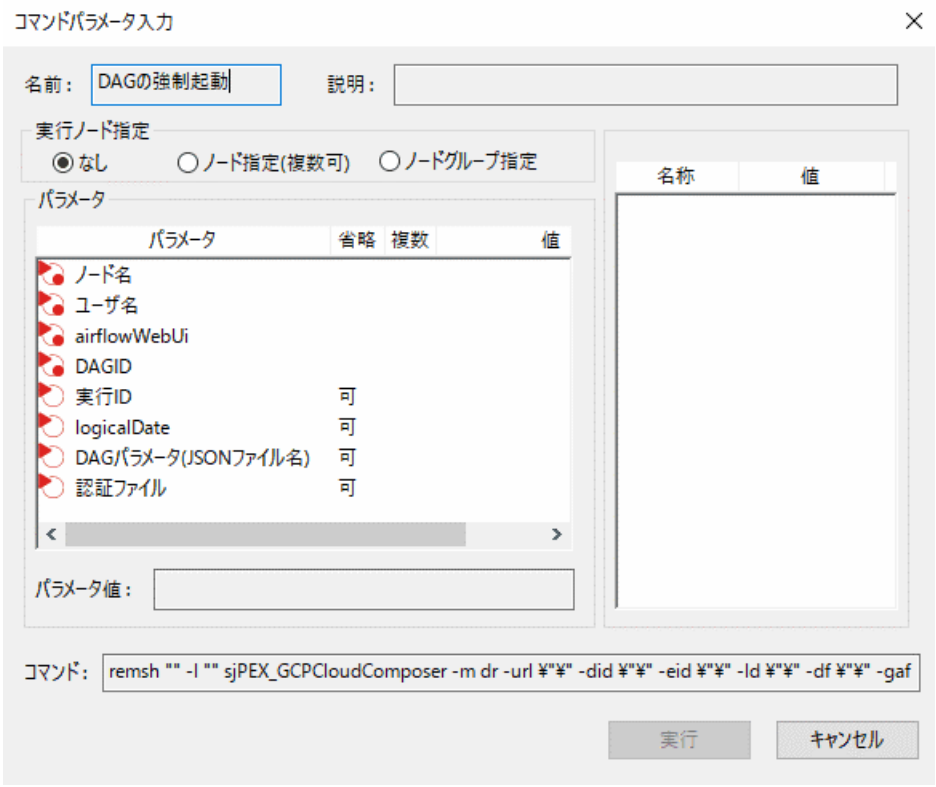


図 3.37 DAGの強制起動コマンドの使用

表 3.34 DAGの強制起動コマンドの入力

パラメータ名	タイプ	省略	デフォルト	概要
airflowWebUi	文字列	不可	_	composer環境のairflowWebUiを指定します。
DAGID	文字列	不可	_	DAGIDを指定します。
実行ID	文字列	可	(空)	実行IDを指定します。(未指定の場合、GCPにより自
logicalDate	文字列	可	(空)	logicalDateを指定します。(日付例：2023-02-07T09
DAGパラメータ(JSONファイル名)	文字列	可	(空)	jsonファイルで「DAGへ渡すパラメータ」を指定します。
認証ファイル	文字列	可	GoogleCloud情報設定ファイルから取得	認証Jsonファイルを指定します。

3.5.2.3.6. DAGをPauseにする

- DAGをPauseにするコマンドの登録

起動シーケンス：

```
remsh "@ノード名@" -l "@ユーザ名@" sjPEX_GCPCloudComposer -m p -url \"@airflowWebUi@\" -did
\"@DAGID@\" -gaf \"@@認証ファイル@@\"
```

- DAGをPauseにするコマンドの使用

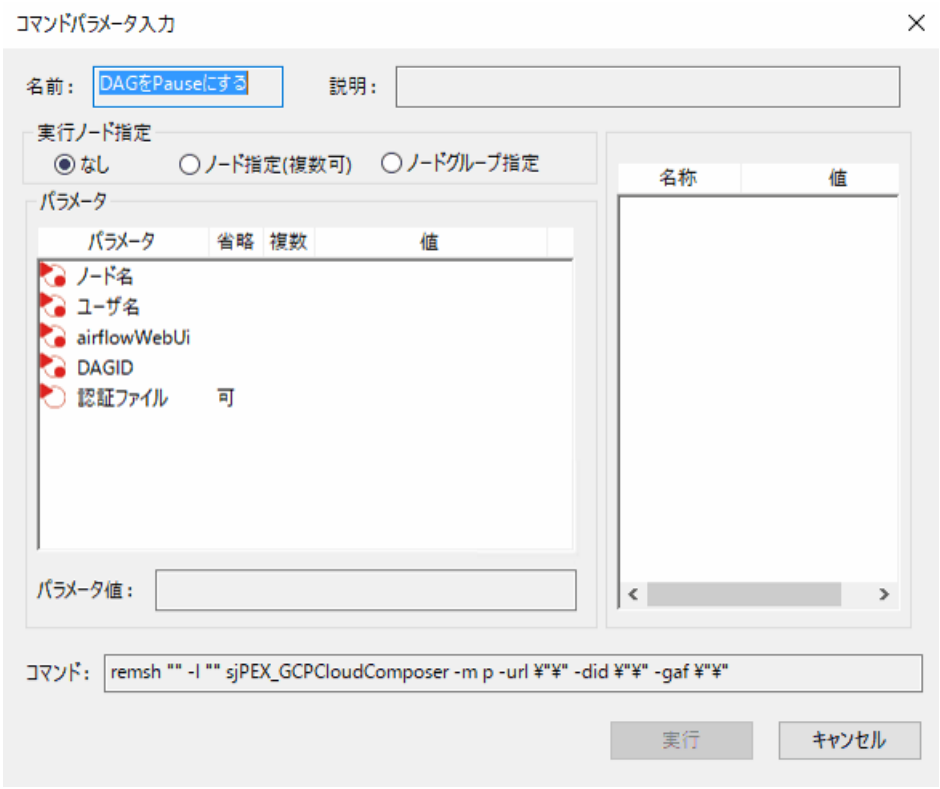


図 3.38 DAGをPauseにするコマンドの使用

表 3.35 DAGをPauseにするコマンドの入力

パラメータ名	タイプ	省略	デフォルト	概要
airflowWebUi	文字列	不可	_	composer環境のairflowWebUiを指定します。
DAGID	文字列	不可	_	DAGIDを指定します。
認証ファイル	文字列	可	GoogleCloud情報設定ファイルから取得	認証Jsonファイルを指定します。

3.5.2.3.7. DAGをUnpauseにする

- DAGをUnpauseにするコマンドの登録

起動シーケンス:

```
remsh "@ノード名@" -l "@ユーザ名@" sjPEX_GCPCloudComposer -m up -url \"@airflowWebUi@\" -did
\"@DAGID@\" -gaf \"@@認証ファイル@@\"
```

- DAGをUnpauseにするコマンドの使用

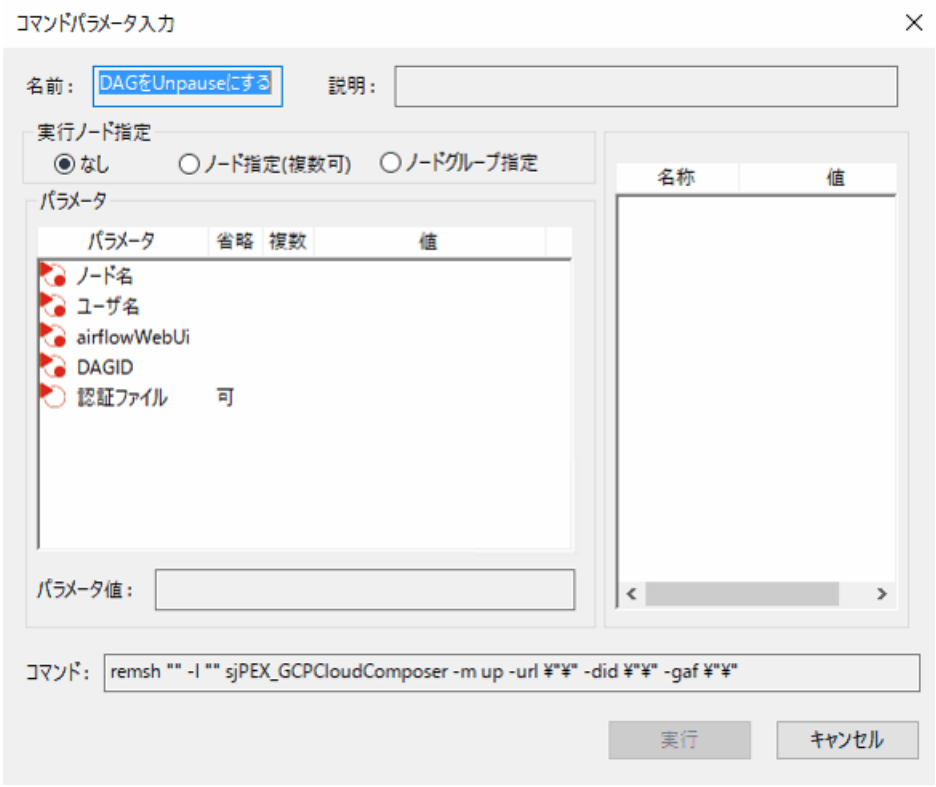


図 3.39 DAGをUnpauseにするコマンドの使用

表 3.36 DAGをUnpauseにするコマンドの入力

パラメータ名	タイプ	省略	デフォルト	概要
airflowWebUi	文字列	不可	_	composer環境のairflowWebUiを指定します。
DAGID	文字列	不可	_	DAGIDを指定します。
認証ファイル	文字列	可	GoogleCloud情報設定ファイルから取得	認証Jsonファイルを指定します。

3.5.2.3.8. タスクのMark Success

- タスクのMark Successコマンドの登録

起動シーケンス:

```
remsh "@ノード名@" -l "@ユーザ名@" sjPEX_GCPCloudComposer -m ms -url \"@airflowWebUi@\" -did
\"@DAGID@\" -tid \"@タスクID@\" -exed \"#実行日付#\" -us \"@@upstream@@\" -ds \"@@downstream@@\" -
gaf \"@@認証ファイル@@\
```

- タスクのMark Successコマンドの使用

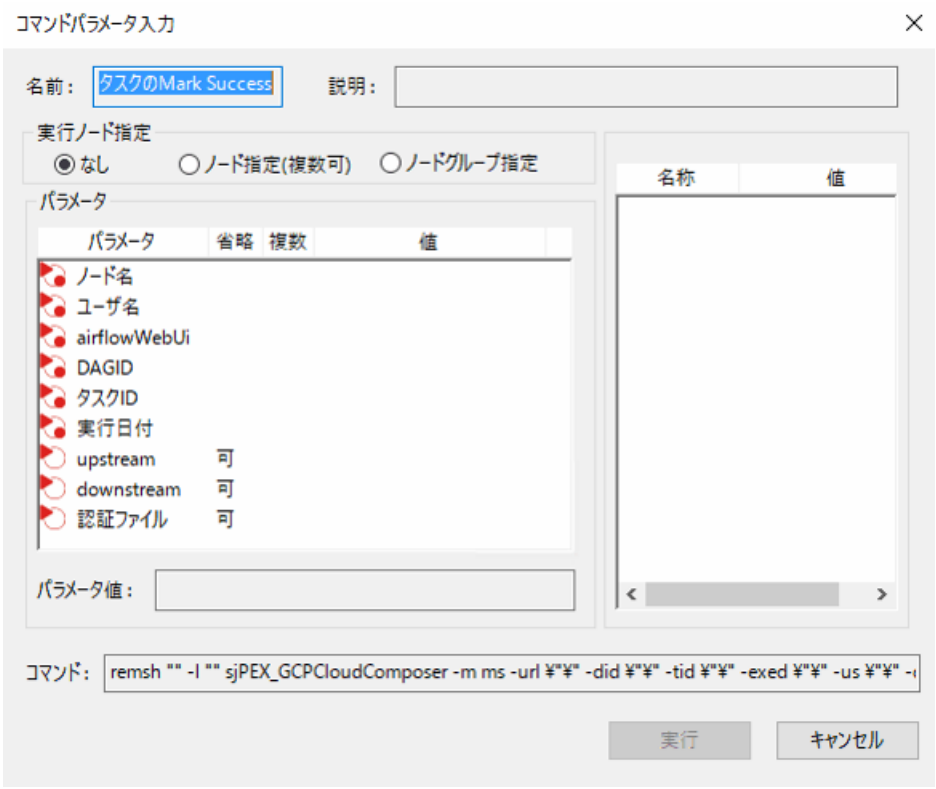


図 3.40 タスクのMark Successコマンドの使用

表 3.37 タスクのMark Successコマンドの入力

パラメータ名	タイプ	省略	デフォルト	概要
airflowWebUi	文字列	不可	_	composer環境のairflowWebUiを指定します。
DAGID	文字列	不可	_	DAGIDを指定します。
タスクID	文字列	不可	_	タスクIDを指定します。
実行日付	文字列	不可	_	executionDateを指定します。
upstream	文字列	可	true	false:指定したタスクのみ実施;true:upstreamタスクも実施します。
downstream	文字列	可	true	false:指定したタスクのみ実施;true:downstreamタスクも実施します。
認証ファイル	文字列	可	GoogleCloud情報設定ファイルから取得	認証Jsonファイルを指定します。

3.5.2.3.9. DAGのMark Success

- DAGのMark Successコマンドの登録

起動シーケンス:

```
remsh "@ノード名@" -l "@ユーザ名@" sjPEX_GCPCloudComposer -m dms -url \"@airflowWebUi@\" -did
\"@DAGID@\" -eid \"@実行ID@\" -gaf \"@@認証ファイル@@\"
```

- DAGのMark Successコマンドの使用

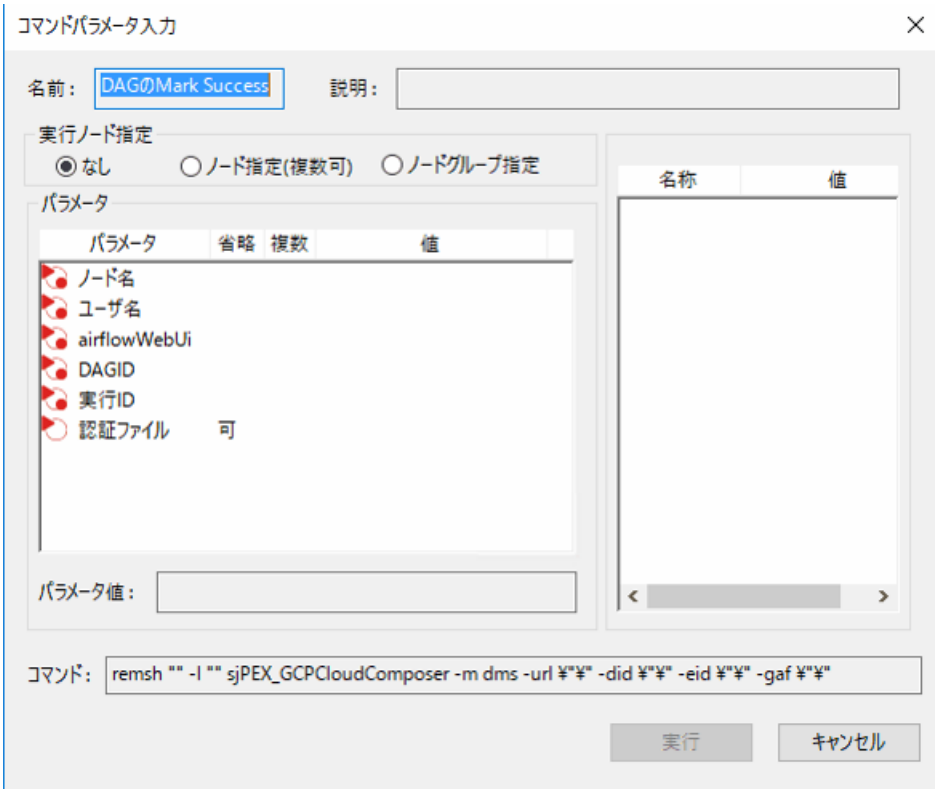


図 3.41 DAGのMark Successコマンドの使用

表 3.38 DAGのMark Successコマンドの入力

パラメータ名	タイプ	省略	デフォルト
airflowWebUi	文字列	不可	_
DAGID	文字列	不可	_
実行ID	文字列	不可	_
認証ファイル	文字列	可	GoogleCloud情報設定ファイルから取

※ DAGのMark Successを利用するために、airflow Version2.2.0以上が必要となります。

3.5.2.3.10. 環境変数を設定_追加

- 環境変数を設定_追加コマンドの登録

起動シーケンス:

```
remsh "@ノード名@" -l "@ユーザ名@" sjPEX_GCPCloudComposer -m av -url \"@airflowWebUi@\" -k \"@key@\"
-v \"@value@\" -gaf \"@@認証ファイル@@\"
```

- 環境変数を設定_追加コマンドの使用

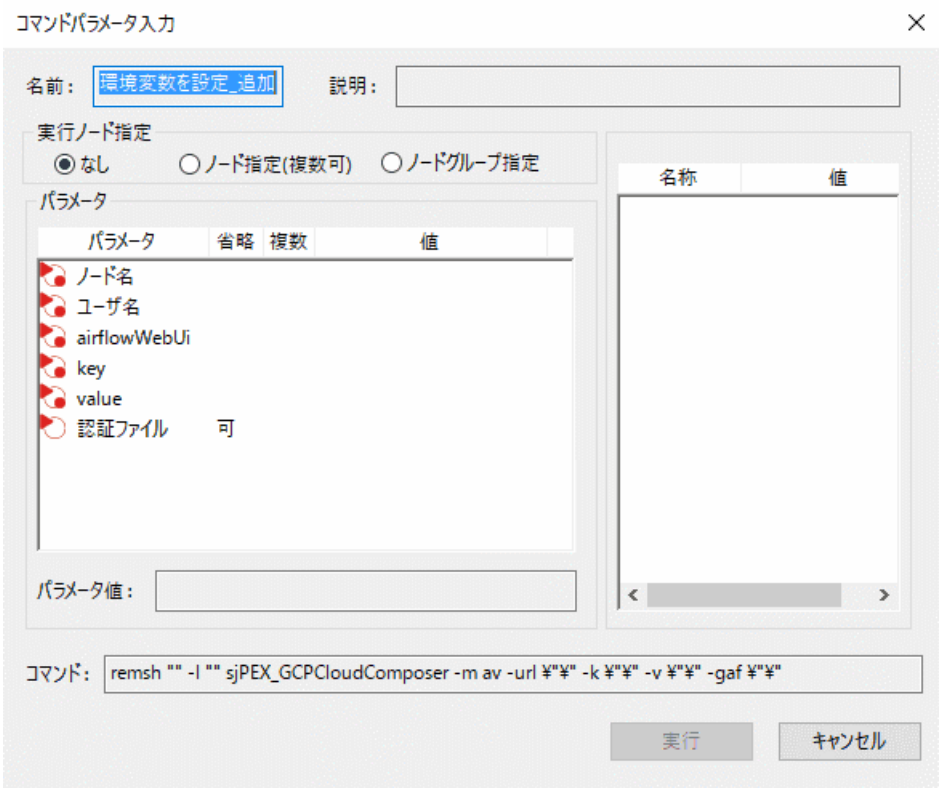


図 3.42 環境変数を設定_追加コマンドの使用

表 3.39 環境変数を設定_追加コマンドの入力

パラメータ名	タイプ	省略	デフォルト	概要
airflowWebUi	文字列	不可	_	composer環境のairflowWebUiを指定します。
key	文字列	不可	_	variableKeyを指定します。
value	文字列	不可	_	追加したいValueを指定します。([]で囲む。例:[a1][a2][a3]。Linuxの場
認証ファイル	文字列	可	GoogleCloud情報設定ファイルから取得	認証Jsonファイルを指定します。

3.5.2.3.11. 環境変数を設定_削除

- 環境変数を設定_削除コマンドの登録

起動シーケンス:

```
remsh "@ノード名@" -l "@ユーザ名@" sjPEX_GCPCloudComposer -m dv -url \"@airflowWebUi@\" -k \"@key@\"
-v \"@value@\" -gaf \"@@認証ファイル@@\"
```

- 環境変数を設定_削除コマンドの使用

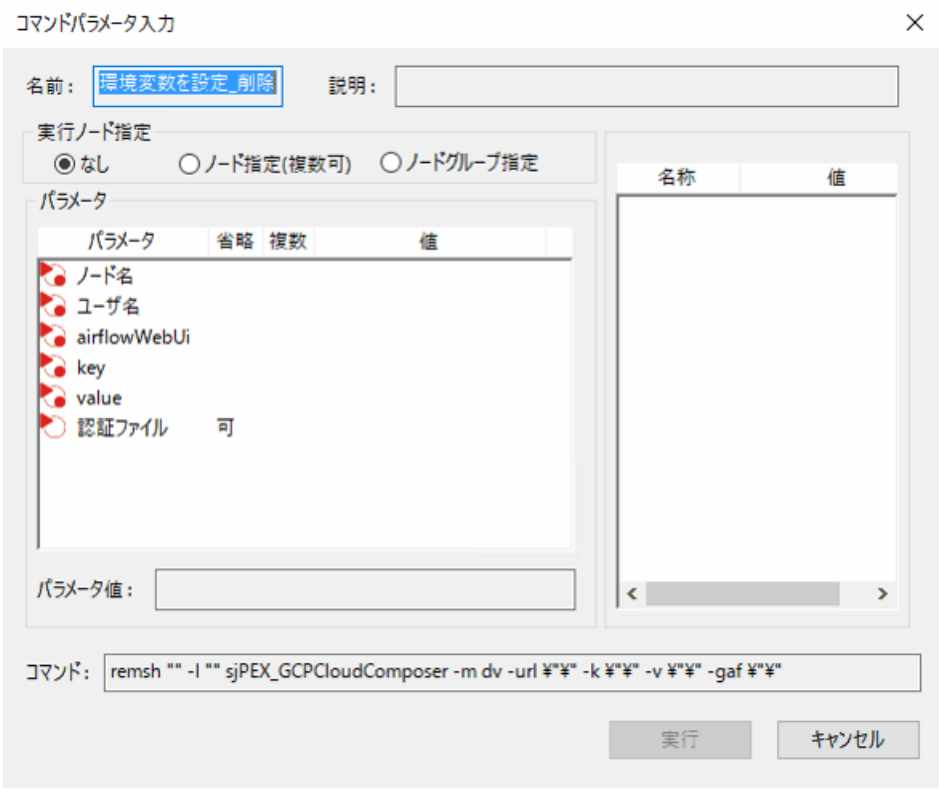


図 3.43 環境変数を設定_削除コマンドの使用

表 3.40 環境変数を設定_削除コマンドの入力

パラメータ名	タイプ	省略	デフォルト	概要
airflowWebUi	文字列	不可	_	composer環境のairflowWebUiを指定します。
key	文字列	不可	_	variableKeyを指定します。
value	文字列	不可	_	削除したいValueを指定します。([]で囲む。例:[a1][a2][a3]。Linuxの場
認証ファイル	文字列	可	GoogleCloud情報設定ファイルから取得	認証Jsonファイルを指定します。

3.5.2.3.12. DAGの状態一覧を取得

- DAGの状態一覧を取得コマンドの登録

起動シーケンス:

```
remsh "@ノード名@" -l "@ユーザ名@" sjPEX_GCPCloudComposer -m ld -url \"@airflowWebUi@\" -did
\"@DAGID@\" -l \"@@limit@@\" -s \"@@ソート順@@\" -edg \"##開始日付##\" -edl \"##終了日付##\" -gaf
\"@@認証ファイル@@\"
```

- DAGの状態一覧を取得コマンドの使用

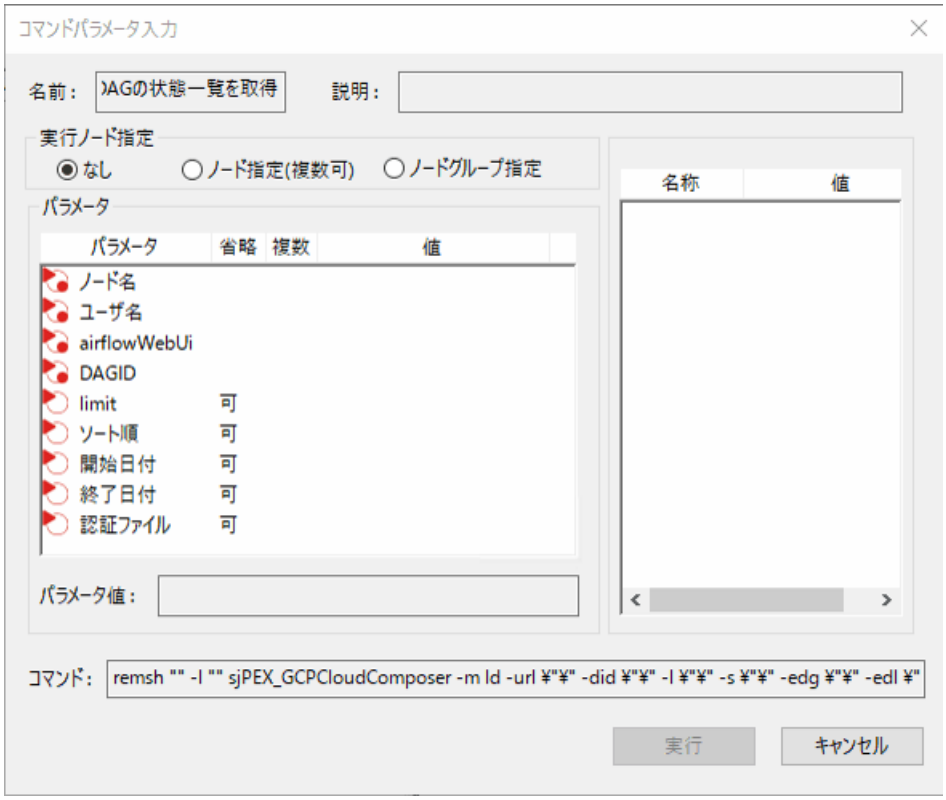


図 3.44 DAGの状態一覧を取得コマンドの使用

表 3.41 DAGの状態一覧を取得コマンドの入力

パラメータ名	タイプ	省略	デフォルト	概要
airflowWebUi	文字列	不可	_	composer環境のairflowWebUiを指定します。
DAGID	文字列	不可	_	DAGIDを指定します。
limit	文字列	可	100	取得の上限件数を指定します。(最大100件まで)
ソート順	文字列	可	-execution_date	ソート条件を指定します。(execution_date: 昇順;-execution_date:降
開始日付	文字列	可	(空)	取得するexecutionDate範囲の開始日付を指定します。
終了日付	文字列	可	(空)	取得するexecutionDate範囲の終了日付を指定します。
認証ファイル	文字列	可	GoogleCloud情報設定ファイルから取得	認証Jsonファイルを指定します。

3.5.2.3.13. 起動したタスクの情報取得

- 起動したタスクの情報取得コマンドの登録

起動シーケンス:

```
remsh "@ノード名@" -l "@ユーザ名@" sjPEX_GCPCloudComposer -m gt -url \"@airflowWebUi@\" -did
\"@DAGID@\" -eid \"@実行ID@\" -tid \"@タスクID@\" -gaf \"@@認証ファイル@@\"
```

- 起動したタスクの情報取得コマンドの使用

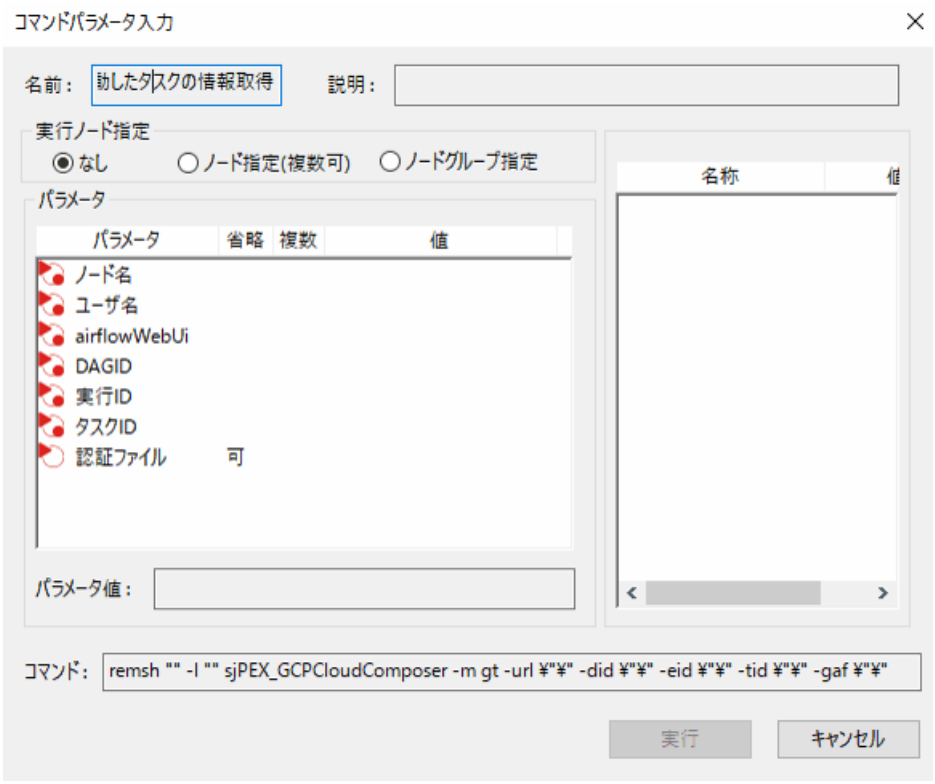


図 3.45 起動したタスクの情報取得コマンドの使用

表 3.42 起動したタスクの情報取得コマンドの入力

パラメータ名	タイプ	省略	デフォルト	概要
airflowWebUi	文字列	不可	_	composer環境のairflowWebUiを指定します。
DAGID	文字列	不可	_	DAGIDを指定します。
実行ID	文字列	不可	_	実行IDを指定します。
タスクID	文字列	不可	_	タスクIDを指定します。
認証ファイル	文字列	可	GoogleCloud情報設定ファイルから取得	認証Jsonファイルを指定します。

3.5.2.3.14. DAGの基本情報取得

- DAGの基本情報取得コマンドの登録

起動シーケンス:

```
remsh "@ノード名@" -l "@ユーザ名@" sjPEX_GCPCloudComposer -m gd -url \"@airflowWebUi@\" -did
\"@DAGID@\" -gaf \"@@認証ファイル@@\"
```

- DAGの基本情報取得コマンドの使用

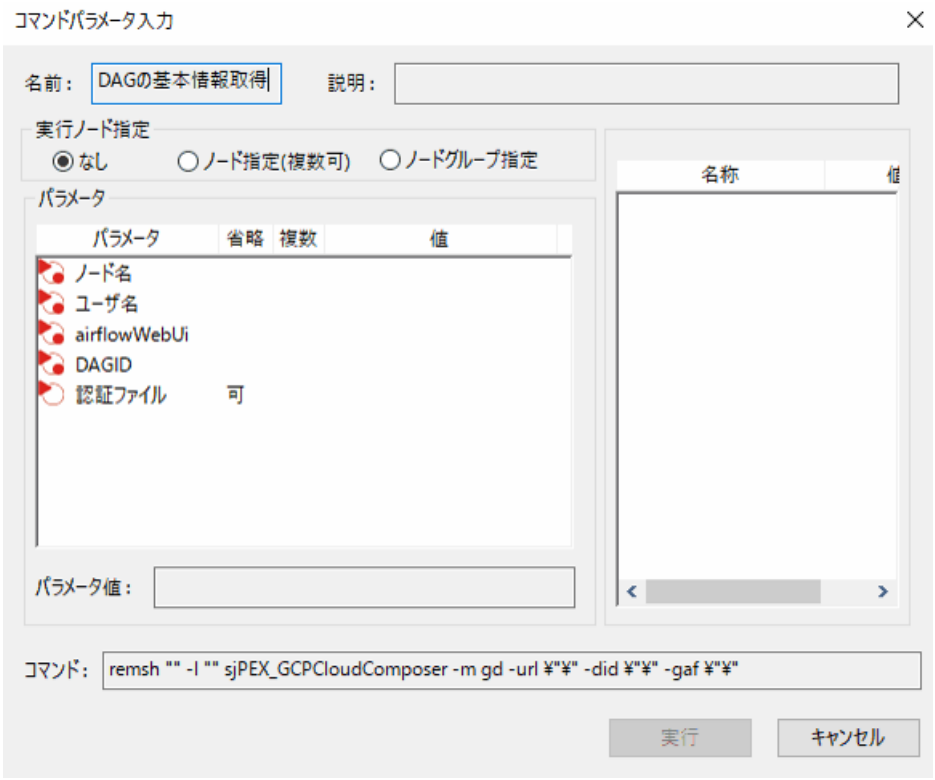


図 3.46 DAGの基本情報取得コマンドの使用

表 3.43 DAGの基本情報取得コマンドの入力

パラメータ名	タイプ	省略	デフォルト	概要
airflowWebUi	文字列	不可	_	composer環境のairflowWebUiを指定します。
DAGID	文字列	不可	_	DAGIDを指定します。
認証ファイル	文字列	可	GoogleCloud情報設定ファイルから取得	認証Jsonファイルを指定します。

3.6. Job Scheduler for Cloud(OCI)の使い方

3.6.1. Job Scheduler for Cloud(OCI/Functions)の使い方

3.6.1.1. Job Scheduler for Cloud(OCI/Functions)の機能

Job Scheduler for Cloud(OCI/Functions)とは、Senju/DCのジョブスケジュール機能と連携し、OCI/Oracle Functionsを実行する機能です。

3.6.1.2. OCI連携機能の設定

- **説明**

  ジョブスケジュールサブシステムを用いてOCI/Functions連携機能を使用するための設定を行います。

- **設定手順**

  OCI/Functions連携機能を設定するには以下の手順が必要です。

  - Oracle Cloud Infrastructureユーザーの登録
  - 認証方式設定
  - OCI情報設定ファイルの作成

3.6.1.2.1. Oracle Cloud Infrastructureユーザーの登録

OCI/Functions連携機能の利用において、事前にOracle Cloud Infrastructure ユーザーの登録が必要です。Oracle Cloud Infrastructureサイトよりユーザー登録を行って下さい。

3.6.1.2.1.1. ポリシーの作成

OCI/Functions連携機能を使用するため、**「OCI/Functions連携機能に必要なアクセス権限」**に示すポリシーを作成して、ユーザーグループにアクセス権限を付与します。

表 3.44 OCI/Functions連携機能に必要なアクセス権限

ジョブ	必要なアクセス権
OCI/Functions連携ジョブ	Allow group <group-name> to inspect fn-app in compartment <compartment-name> Allow group <group-name> to inspect fn-function in compartment <compartment-name> Allow group <group-name> to use fn-invocation in compartment <compartment-name>

3.6.1.2.2. 認証設定

3.6.1.2.2.1. インスタンス許可で認証する

OCI内のエージェントからOCI/Functions連携機能を実行する場合は、インスタンスを認可する方法で認証します。Oracle Cloud Infrastructureサイトより動的グループを作成し、インスタンスを動的グループのメンバーとして追加します。その後、OCIサービスへのAPIコールを許可するポリシーを作成して下さい。

表 3.45 動的グループに必要なアクセス権限

ジョブ	必要なアクセス権
OCI/Functions連携ジョブ	Allow dynamic-group <group-name> to inspect fn-app in compartment <compartment-name> Allow dynamic-group <group-name> to inspect fn-function in compartment <compartment-name> Allow dynamic-group <group-name> to use fn-invocation in compartment <compartment-name>

3.6.1.2.2.2. APIキーで認証する

OCI外のエージェントからOCI/Functions連携機能を実行する場合は、ユーザーで作成したユーザー設定ファイルを利用して認証します。Oracle

Cloud InfrastructureサイトよりAPIキー、フィンガープリント、テナンシのOCID、ユーザーのOCID、リージョンを取得し、ユーザー設定ファイルの作成 で作成して下さい。作成したユーザー設定ファイルをエージェントの千手稼働アカウントでアクセスできる位置に配置し、OCI情報設定ファイル(sj_oci_sys.json)の作成 でOCI情報設定ファイルにユーザー設定ファイルのパスを設定して下さい。

参照URL：https://docs.cloud.oracle.com/ja-jp/iaas/Content/API/Concepts/apisigningkey.htm

3.6.1.2.3. ユーザー設定ファイルの作成

ユーザー設定ファイルは、OCIに関する認証情報の設定ファイルです。dat/opt/sj_oci_user.json.sample をコピーして以下の項目を設定して下さい。

表 3.46 ユーザー設定ファイルの記述内容

項目	省略	説明
tenantOCID	不可	テナンシのOCID
userOCID	不可	ユーザーのOCID
region	不可	リージョン
fingerprint	不可	APIキーのフィンガープリント
privateKeyLocation	不可	秘密キー・ファイルの絶対パス
privateKeyPassphrase	可	秘密キーを生成する時、設定したパスフレーズ

3.6.1.2.4. OCI情報設定ファイル(sj_oci_sys.json)の作成

sj_oci_sys.jsonファイルは、OCIに関する情報の設定ファイルです。sj_oci_sys.jsonとOCI/Functions連携ジョブのパラメータの両方でユーザー設定ファイルを指定した場合は、OCI/Functions連携ジョブのパラメータで指定した値が有効になります。

設定方法については、**Cloud Monitoring の sj_setup_oci ― OCI情報設定ファイル更新 ―** を参照して下さい。

OCI情報設定ファイル(dat/opt/sj_oci_sys.json)を作成し、以下の項目を設定して下さい。

表 3.47 sj_oci_sys.jsonの記述内容

項目	省略	デフォルト	暗号化対象	説明
proxyURL	可	—	×	OCI接続時に経由するプロキシサーバー。（次の形式で記載して下さい "<プロトコル>://<ipアド
proxyUsername	可	—	×	プロキシサーバーアクセス用ユーザーID
proxyPassword	可	—	○	プロキシサーバーアクセス用パスワード(暗号化後のパスワード)
userFilePath	可	—	×	ユーザー設定ファイルの絶対パス

- userFilePathは、APIキーによる認証を行う場合に指定して下さい。
- proxyUsernameおよびproxyPasswordの両方を指定しなかった場合、プロキシサーバーの認証に利用しません。

3.6.1.3. OCI/Functions連携ジョブの利用方法

OCI/Functions連携ジョブは、Oracle Cloud Infrastructure Consoleなどによって作成したOracle Functionsを実行します。

OCI/Functions連携ジョブが起動されると、引数に指定された内容でOracle Functionsを実行し、実行結果を標準出力に出力します。

OCI/Functions連携ジョブを起動する際に指定する引数には、以下に示す内容を指定して下さい。

```
sjPEX_CloudFunctions -m OF
        -ofc OCIコンパートメント名
        -ofa OCIアプリケーション名
        -ofn OCIファンクション名
        -ofpf ファンクションパラメータ（JSONファイル名）
        -ouf OCIのユーザー設定ファイル
```

オプション	省略	デフォルト	長さ	説明
-ofc	不可	—	—	OCIコンパートメント名
-ofa	不可	—	—	OCIアプリケーション名
-ofn	不可	—	—	OCIファンクション名
-ofpf	可	—	—	ファンクションパラメータ（JSONファイル名）
-ouf	可	—	—	OCIのユーザー設定ファイル

- Senju/DCジョブの起動コマンドの最大文字数は2048文字です。
- OCIコンパートメント名、OCIアプリケーション名およびOCIファンクション名は、Oracle Cloud Infrastructureサイトで確認して下さい。

3.6.1.3.1. OCI/Functions連携ジョブテンプレートの使い方

ジョブテンプレートとは、ジョブの起動コマンドシーケンスのみを持ち、パラメータ値が未決定であるエンティティです。ジョブテンプレートを用いることにより、ジョブの登録のたびにコマンドシーケンスを入力しなくても、必要なパラメータ値を入力するだけでジョブの作成が行えます。Job Scheduler for CloudをSenju/DCのジョブスケジュール機能と連携するために、Job Scheduler for Cloudジョブを、Senju/DCのジョブの起動コマンドとして設定します。

OCI/Functions連携ジョブテンプレートを使用し、ジョブの起動コマンドとして利用するには、千手ブラウザのツリービューで、＜ドメイン＞→“ジョブスケジュール”→“ジョブ”を選択し、ジョブの新規作成を行います。

ジョブの新規作成プロパティウィンドで[ジョブテンプレートを使用]チェックボックスをチェックし、[ジョブテンプレート入力]ボタンを押して下さい。

ジョブテンプレート入力ウィンドでOCI/Functions連携ジョブテンプレートを選択し、各パラメータ値を設定して下さい。

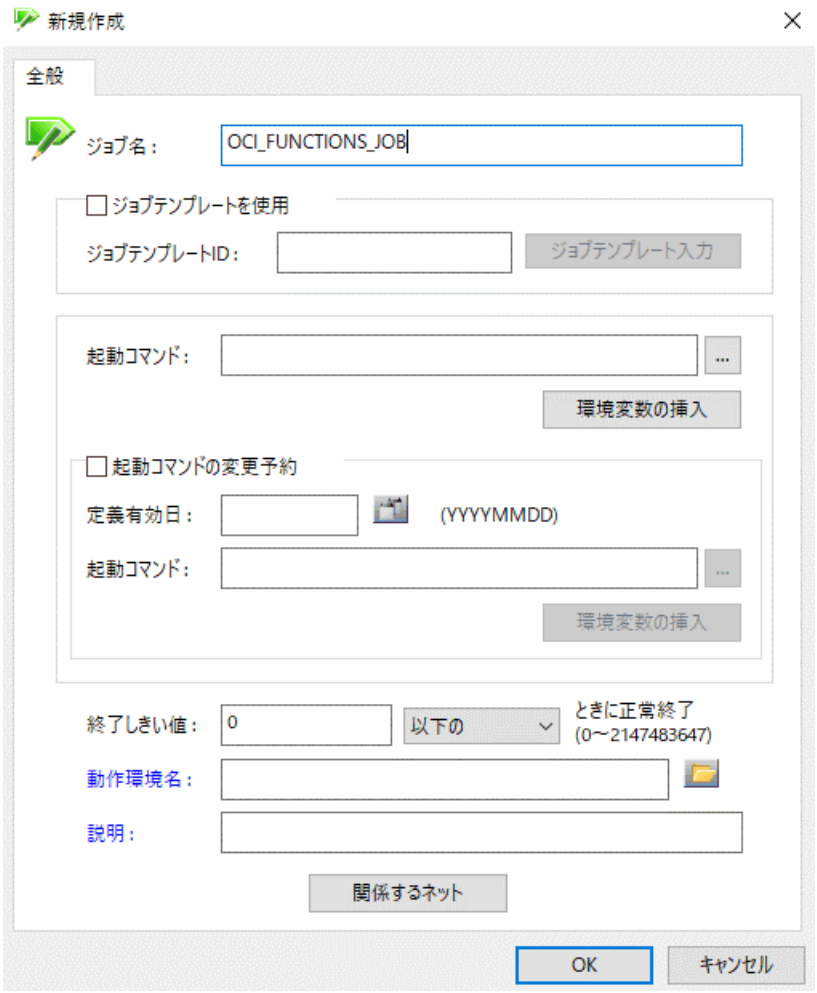


図 3.47 OCI/Functions連携ジョブテンプレートの使用

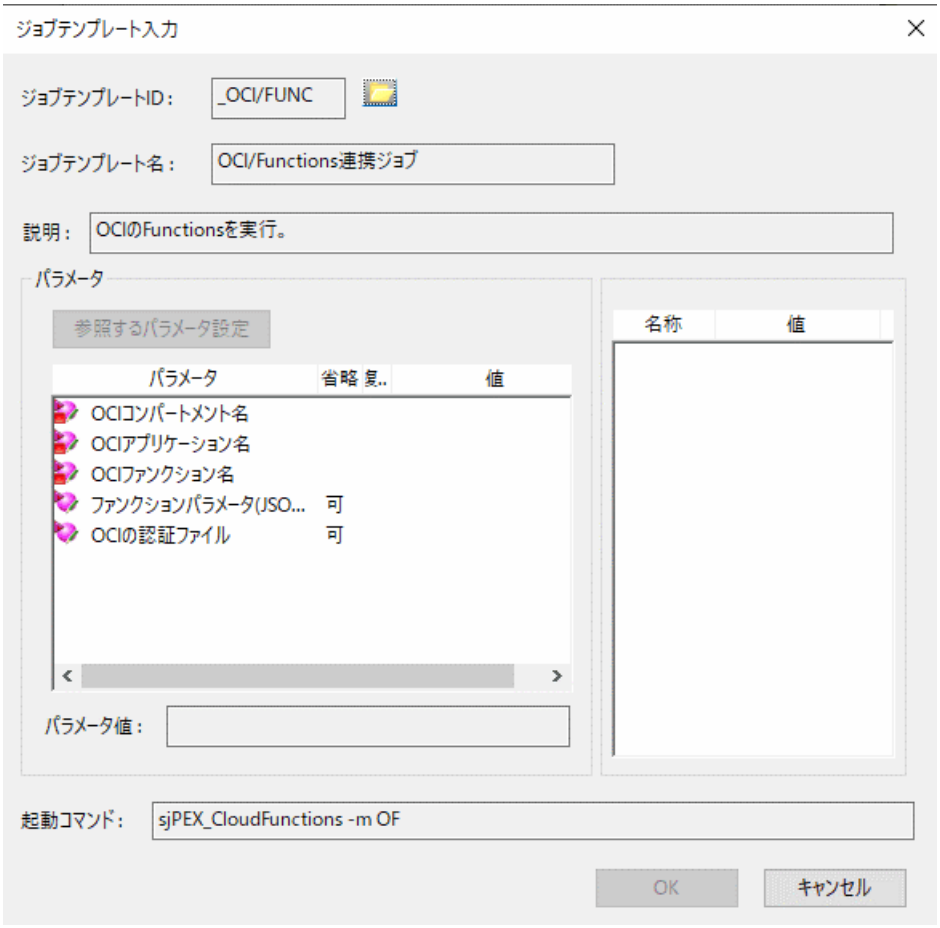


図 3.48 OCI/Functions連携ジョブテンプレートの入力

表 3.48 OCI/Functions連携ジョブテンプレートの入力

パラメータ	説明
OCIコンパートメント名	Cloud コンパートメントの名前を指定します。省略不可です。
OCIアプリケーション名	Cloud アプリケーションの名前を指定します。省略不可です。
OCIファンクション名	Oracle Functionの名前を指定します。省略不可です。
ファンクションパラメータ（JSONファイル名）	Oracle Functionsへ渡す引数が記載されたJSONファイルを絶対パスで指定します。必要ない場合は省略
OCIの認証ファイル	OCIのユーザー設定ファイルを絶対パスで指定します。sj_oci_sys.json で指定した場合、またはインスタンス

3.6.1.3.2. OCI/Functions連携ジョブの処理の流れ(通常時)

OCI/Functions連携ジョブがSenju/DCのジョブスケジュールで1つのジョブとして起動されると、**「図 6-3　OCI/Functions連携ジョブの処理の流れ」**および**「TABLE 6-7　OCI/Functions連携ジョブの処理の流れ」**に示す流れで動きます。

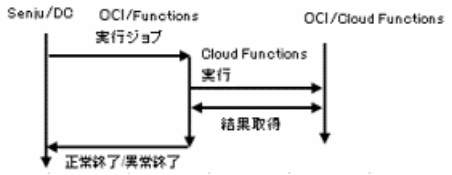


図 3.49 OCI/Functions連携ジョブの処理の流れ

表 3.49 OCI/Functions連携ジョブの処理の流れ

Senju/DC ジョブの状態	OCI/Functions実行 ジョブの処理内容	メッセージモニタの出力
起動待ち	起動前の状態	
稼働中	起動	
稼働中	引数に従い、OCI/Clound Functions上の関数実行	
正常終了	OCI/Functions実行に成功	!PEXC19 OCI/Functionsの関数実行に成功しました。
異常終了	OCI/Functions実行に失敗	!PEXC20 OCI/Functionsの関数実行に失敗しました。

1. OCI/Functions連携ジョブが起動されると、引数に指定された内容でOCI/Functionsを実行します。
2. OCI/Functionsを実行します。
3. OCI/Functionsが正しく実行されると、成功した旨のメッセージを出力し、Senju/DCジョブは正常終了します。
4. OCI/Functionsが何らかの理由で正しく実行されないと、失敗した旨のメッセージを出力し、Senju/DCジョブは異常終了します。

3.6.1.3.3. OCI/Functions連携ジョブの処理の流れ（強制停止時）

OCI/Functions連携ジョブは、他のSenju/DCのジョブと同じく強制停止させることができます。

Senju/DCのジョブスケジュールより、OCI/Functions連携ジョブを強制停止しても、関数実行中のOCI/Functionsは実行されたままとなります。

Senju/DCのジョブスケジュールでは、強制停止されたジョブの状態は異常終了となります。

3.7. Job Scheduler for Cloud(IBM Cloud)の使い方

3.7.1. Job Scheduler for Cloud(IBM Cloud Functions)の使い方

3.7.1.1. Job Scheduler for Cloud(IBM Cloud Functions)の機能

Job Scheduler for Cloud(IBM Cloud Functions)とは、Senju/DCのジョブスケジュール機能と連携し、IBM Cloud Functionsを実行する機能です。

3.7.1.2. IBM Cloud連携機能の設定

- **説明**

  ジョブスケジュールサブシステムを用いてIBM Cloud Functions連携機能を使用するための設定を行います。

- **設定手順**

  IBM Cloud Functions連携機能を設定するには以下の手順が必要です。

  - IBM Cloudユーザーの登録
  - 認証設定
  - IBM Cloud情報設定ファイルの作成

3.7.1.2.1. IBM Cloudユーザーの登録

IBM Cloud Functions連携機能の利用において、事前にIBM Cloudユーザーの登録が必要です。IBM Cloudサイトよりユーザー登録を行って下さい。

3.7.1.2.2. 認証設定

3.7.1.2.2.1. APIキーで認証する

エージェントからIBM Cloud Functions連携機能を実行する場合は、IBM Cloudユーザーまたはサービスに結び付いたAPIキーを使って認証します。IBM Cloudサイトより、IBM Cloudユーザーまたはサービスに IBM Cloud Functionsへのアクセスを許可するアクセスポリシーを設定して下さい。IBM Cloudユーザーまたはサービスに のAPIキーを取得し、IBM Cloud情報設定ファイル(sj_ibc_sys.json)の作成 で、APIキーを暗号化した値をapiKeyの値に設定して下さい

表 3.50 サービスIDのAPIキーで認証に必要なアクセス権限

項目名	設定値
サービス	Functions
アクセス権限の範囲指定	すべてのリソース
プラットフォームアクセス	未指定
サービス・アクセス	リーダー

3.7.1.2.3. IBM Cloud情報設定ファイル(sj_ibc_sys.json)の作成

sj_ibc_sys.jsonファイルは、IBM Cloudに関する情報の設定ファイルです。IBM Cloud Functions連携ジョブのパラメータで指定した場合は、指定したファイルが有効になります。

設定方法については、**Cloud Monitoring** の **sj_setup_ibc ー IBM Cloud情報設定ファイル更新 ー** を参照して下さい。

IBM Cloud情報設定ファイル(dat/opt/sj_ibc_sys.json)を作成し、以下の項目を設定して下さい。

表 3.51 sj_ibc_sys.jsonの記述内容

項目	省略	デフォルト	暗号化対象	説明
proxyURL	可	—	×	IBM接続時に経由するプロキシサーバー。(次の形式で記載して下さい "<プロトコル>://<ipア
proxyUsername	可	—	×	プロキシサーバーアクセス用ユーザーID
proxyPassword	可	—	○	プロキシサーバーアクセス用パスワード(暗号化後のパスワード)
apiKey	不可	—	○	APIキー
region	不可	—	×	エンドポイント設定用リージョン

- APIキーは、ユーザーのAPIキーとサービスIDのAPIキー両方をサポートします。
- proxyUsernameおよびproxyPasswordの両方を指定しなかった場合、プロキシサーバーの認証に利用しません。

3.7.1.3. IBM Cloud Functions連携ジョブの利用方法

IBM Cloud Functions連携ジョブは、IBM Cloud Consoleなどによって作成したIBM Cloud Functionsを実行します。

IBM Cloud Functions連携ジョブが起動されると、引数に指定された内容でIBM Cloud Functionsを実行し、実行結果を標準出力に出力します。

IBM Cloud Functions連携ジョブを起動する際に指定する引数には、以下に示す内容を指定して下さい。

```
sjPEX_CloudFunctions -m IF
        -ins ネームスペースのID
        -ifn IBM Cloudファンクション名
        -ifdf ファンクションパラメータ(JSONファイル名)
        -iuf IBM Cloudの認証ファイル
```

オプション	省略	デフォルト	長さ	説明
-ins	不可	—	—	ファンクションが所属するネームスペースのID
-ifn	不可	—	—	IBM Cloudファンクション名
-ifdf	可	—	—	ファンクションパラメータ(JSONファイル名)
-iuf	可	—	—	IBM Cloudの認証ファイル

- Senju/DCジョブの起動コマンドの最大文字数は2048文字です。
- IBM Cloudファンクション名およびIBM CloudネームスペースのIDは、IBM Cloudサイトで確認して下さい。

3.7.1.3.1. IBM Cloud Functions連携ジョブテンプレートの使い方

ジョブテンプレートとは、ジョブの起動コマンドシーケンスのみを持ち、パラメータ値が未決定であるエンティティです。ジョブテンプレートを用いることにより、ジョブの登録のたびにコマンドシーケンスを入力しなくても、必要なパラメータ値を入力するだけでジョブの作成が行えます。Job Scheduler for CloudをSenju/DCのジョブスケジュール機能と連携するために、Job Scheduler for Cloudジョブを、Senju/DCのジョブの起動コマンドとして設定します。

IBM Cloud Functions連携ジョブテンプレートを使用し、ジョブの起動コマンドとして利用するには、千手ブラウザのツリービューで、<ドメイン>→“ジョブスケジュール”→“ジョブ”を選択し、ジョブの新規作成を行います。

ジョブの新規作成プロパティウィンドで[ジョブテンプレートを使用]チェックボックスをチェックし、[ジョブテンプレート入力]ボタンを押して下さい。

ジョブテンプレート入力ウィンドでIBM Cloud Functions連携ジョブテンプレートを選択し、各パラメータ値を設定して下さい。

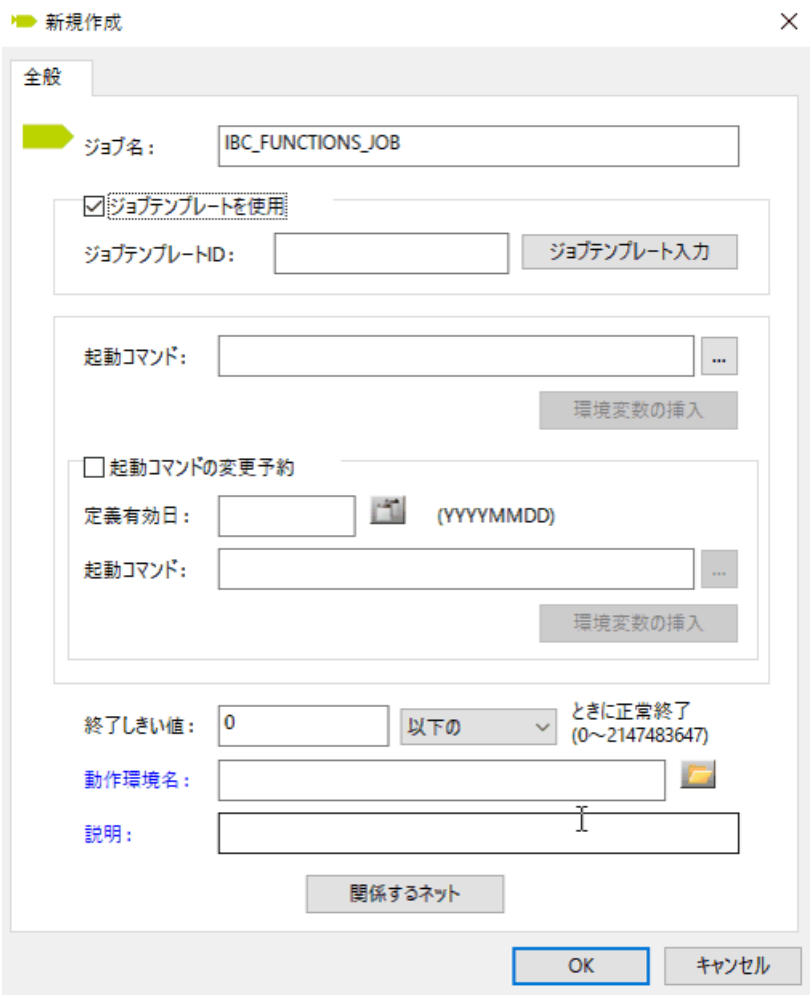


図 3.50 IBM Cloud Functions連携ジョブテンプレートの使用

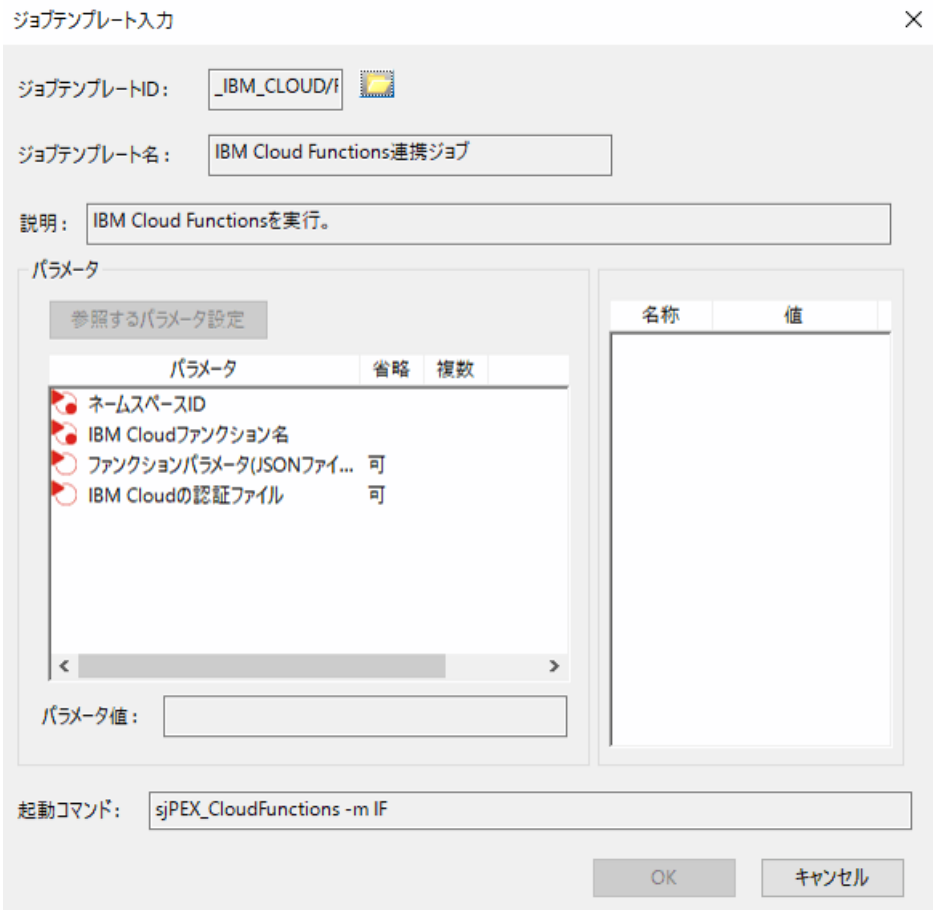


図 3.51 IBM Cloud Functions連携ジョブテンプレートの入力

表 3.52 IBM Cloud Functions連携ジョブテンプレートの入力

パラメータ	説明
ネームスペースID	IBM Cloud Functionsが所属するネームスペースのIDを指定します。省略不可です。
IBM Cloudファンクション名	IBM Cloud Functionsの名前を指定します。省略不可です。
ファンクションパラメータ（JSONファイル名）	IBM Cloud Functionsへ渡す引数が記載されたJSONファイルを絶対パスで指定します。必要ない場合は省
IBM Cloudの認証ファイル	IBM Cloudの認証ファイルを絶対パスで指定します。省略可能です。指定した場合はパラメータで指定した内

3.7.1.3.2. IBM Cloud Functions連携ジョブの処理の流れ(通常時)

IBM Cloud Functions連携ジョブがSenju/DCのジョブスケジュールで1つのジョブとして起動されると、**「図 7-3　IBM Cloud Functions連携ジョブの処理の流れ」**および**「TABLE 7-6　IBM Cloud Functions連携ジョブの処理の流れ」**に示す流れで動きます。

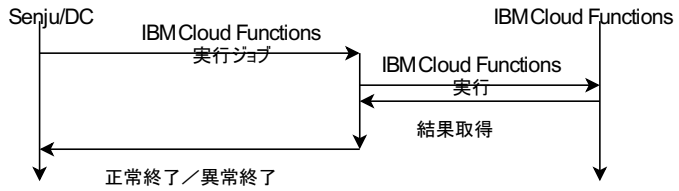


図 3.52 IBM Cloud Functions連携ジョブの処理の流れ

表 3.53 IBM Cloud Functions連携ジョブの処理の流れ

Senju/DC ジョブの状態	IBM Cloud Functions実行 ジョブの処理内容	メッセージモニタの出力
起動待ち	起動前の状態	
稼働中	起動	
稼働中	引数に従い、IBM Cloud Functions上の関数実行	
正常終了	IBM Cloud Functions実行に成功	!PEXC21 IBM Cloud Functionsの関数実行に成功しました。
異常終了	IBM Cloud Functions実行に失敗	!PEXC22 IBM Cloud Functionsの関数実行に失敗しました。

1. IBM Cloud Functions連携ジョブが起動されると、引数に指定された内容でIBM Cloud Functionsを実行します。
2. IBM Cloud Functionsを実行します。
3. IBM Cloud Functionsが正しく実行されると、成功した旨のメッセージを出力し、Senju/DCジョブは正常終了します。
4. IBM Cloud Functionsが何らかの理由で正しく実行されないと、失敗した旨のメッセージを出力し、Senju/DCジョブは異常終了します。

3.7.1.3.3. IBM Cloud Functions連携ジョブの処理の流れ（強制停止時）

IBM Cloud Functions連携ジョブは、他のSenju/DCのジョブと同じく強制停止させることができます。

Senju/DCのジョブスケジュールより、IBM Cloud Functions連携ジョブを強制停止しても、関数実行中のIBM Cloud Functionsは実行されたままとなります。

Senju/DCのジョブスケジュールでは、強制停止されたジョブの状態は異常終了となります。

3.8. 付録

3.8.1. メッセージ一覧

ID	レベル	表示	警報	メッセージ内容	原因・内容
!PEXC01	E	2	ON	クラウドジョブスケジュールコマンドの起動に失敗しました。	クラウドジョブスケジュールコマンドの起動に失敗しました。
!PEXC02	E	2	ON	クラウドジョブスケジュールコマンドの起動に失敗しました。	クラウドジョブスケジュールコマンドの起動に失敗しました。
!PEXC03	I	1	OFF	AWS/S3からのデータ取得に成功しました。	AWS/S3からのデータ取得に成功しました
!PEXC04	E	1	ON	AWS/S3からのデータ取得に失敗しました。	AWS/S3からのデータ取得に失敗しました。
!PEXC05	I	1	OFF	AWS/S3へのデータ登録に成功しました。	AWS/S3へのデータ登録に成功しました。
!PEXC06	E	1	ON	AWS/S3へのデータ登録に失敗しました。	AWS/S3へのデータ登録に失敗しました。
!PEXC07	I	1	OFF	AWS/S3上のデータ削除に成功しました。	AWS/S3からのデータ削除に成功しました。
!PEXC08	E	1	ON	AWS/S3上のデータ削除に失敗しました。	AWS/S3からのデータ削除に失敗しました。
!PEXC09	I	1	OFF	AWS/MRジョブフローの実行に成功しました。	AWS/MRジョブフローの実行に成功しました。
!PEXC10	E	1	ON	AWS/MRジョブフローの実行に失敗しました。	AWS/MRジョブフローの実行に失敗しました。
!PEXC11	I	1	OFF	クラウドジョブスケジュールコマンドを強制停止します。	クラウドジョブスケジュールコマンドを強制停止します。
!PEXC12	E	1	ON	クラウドジョブスケジュールコマンドが異常終了しました。	クラウドジョブスケジュールコマンドが異常終了しました。
!PEXC13	I	1	OFF	AWS/Lambda上の関数実行に成功しました。	AWS/Lambda上の関数実行に成功しました。
!PEXC14	E	1	ON	AWS/Lambda上の関数実行に失敗しました。	AWS/Lambda上の関数実行に失敗しました。
!PEXC15	I	1	OFF	Azure/Functionsの関数実行に成功しました。	Azure/Functionsの関数実行に成功しました。
!PEXC16	E	1	ON	Azure/Functionsの関数実行に失敗しました。	Azure/Functionsの関数実行に失敗しました。
!PEXC17	I	1	OFF	GCP/Functionsの関数実行に成功しました。	GCP/Functionsの関数実行に成功しました。
!PEXC18	E	1	ON	GCP/Functionsの関数実行に失敗しました。	GCP/Functionsの関数実行に失敗しました。
!PEXC19	I	1	OFF	OCI/Functionsの関数実行に成功しました。	OCI/Functionsの関数実行に成功しました。
!PEXC20	E	1	ON	OCI/Functionsの関数実行に失敗しました。	OCI/Functionsの関数実行に失敗しました。
!PEXC21	I	1	OFF	IBM Cloud Functionsの関数実行に成功しました。	IBM Cloud Functionsの関数実行に成功しました。
!PEXC22	E	1	ON	IBM Cloud Functionsの関数実行に失敗しました。	IBM Cloud Functionsの関数実行に失敗しました。
!PEXC23	I	1	OFF	AWS/Step Functionsの実行に成功しました。	AWS/Step Functionsの実行に成功しました。
!PEXC24	E	1	ON	AWS/Step Functionsの実行に失敗しました。	AWS/Step Functionsの実行に失敗しました。

3.8.2. エラーメッセージとその対処方法

3.8.2.1. Job Scheduler for Cloud(AWS/S3)

Job Scheduler for Cloud(AWS/S3)の実行中にエラーが起きると、エラーメッセージがメッセージモニタに表示されます。

メッセージID	エラー内容	終了値	対処方法
!PEXC01	duplicate *****option (func:***,line:***)	5	オプション
	-m can not take S3 or MR or LS or LA or DF or GF or OF or IF or SF("***" is error) (func:***,line:***)	5	-mオプショ
	*****has no filepath (func:***,line:***)	5	指定した
	-t can take 0,1,2,3("***" is error) (func:***,line:***)	5	-tオプション
	-i can take 10-600("***" is error) (func:***,line:***)	5	-iオプション
	"***" is Unrecognized option (func:***,line:***)	5	不明なオ
	*****option not found (func:***,line:***)	5	必須オプ
	file("***") open fail(***) (func:***,line:***)	5	指定した
	chdir("******") fail(***)	14	Senju/DC
	SENJUHOME("******") is too long	15	Senju/DC
	memory allocate error (func:***,line:***)	16	コマンドが
!PEXC02	child process start failed (***) (func:***,line:***)	9	子プロセス
!PEXC04	*****(func:***,line:***)	45	出力内容
!PEXC06	*****(func:***,line:***)	41	出力内容
!PEXC08	*****(func:***,line:***)	43	出力内容
!PEXC12	child killed by SIGNAL (***) (func:***,line:***)	8	子プロセス
	wait error (***) (func:***,line:***)	10	子プロセス
	child:parent not exist (func:***,line:***)	13	親プロセス

3.8.2.2. Job Scheduler for Cloud(AWS/Elastic MapReduce)

Job Scheduler for Cloud(AWS/Elastic MapReduce)の実行中にエラーが起きると、エラーメッセージがメッセージモニタに表示されます。

メッセージID	エラー内容	終了値	対処方法
!PEXC01	duplicate *****option (func:***,line:***)	5	オプション
	-m can not take S3 or MR or LS or LA or DF or GF or OF or IF or SF("***" is error)(func:***,line:***)	5	-mオプショ
	*****has no filepath (func:***,line:***)	5	指定した
	-inc can take 1 over("***" is error)(func:***,line:***)	5	-incオプシ
	-t can take 0,1,2,3("***" is error) (func:***,line:***)	5	-tオプション
	-i can take 10-600("***" is error) (func:***,line:***)	5	-iオプション
	"***" is Unrecognized option (func:***,line:***)	5	不明なオプ
	*****option not found (func:***,line:***)	5	必須オプシ
	file("***") open fail (***) (func:***,line:***)	5	指定した
	chdir("******") fail(***)	14	Senju/DC
	SENJUHOME("******") is too long	15	Senju/DC
	memory allocate error (func:***,line:***)	16	コマンドが移
!PEXC02	child process start failed (***) (func:***,line:***)	9	子プロセス
!PEXC10	*****(func:***,line:***)	47	出力内容
!PEXC12	child killed by SIGNAL (***) (func:***,line:***)	8	子プロセス
	wait error (***) (func:***,line:***)	10	子プロセス
	child:parent not exist (func:***,line:***)	13	親プロセス

3.8.2.3. Job Scheduler for Cloud(AWS/Lambda Function)

Job Scheduler for Cloud(AWS/Lambda Function)の実行中にエラーが起きると、エラーメッセージがメッセージモニタに表示されます。

メッセージID	エラー内容	終了値	対処方法
!PEXC01	duplicate *****option (func:***,line:***)	5	オプション
	-m can not take S3 or MR or LS or LA or DF or GF or OF or IF or SF("****" is error) (func:***,line:***)	5	-mオプショ
	"****" is Unrecognized option (func:***,line:***)	5	不明なオ
	*****option not found (func:***,line:***)	5	必須オプ
	chdir("******") fail(***)	14	Senju/DC
	SENJUHOME("******") is too long	15	Senju/DC
	memory allocate error (func:***,line:***)	16	コマンドが
!PEXC02	child process start failed (***) (func:***,line:***)	9	子プロセス
!PEXC12	child killed by SIGNAL (***) (func:***,line:***)	8	子プロセス
	wait error (***) (func:***,line:***)	10	子プロセス
	child:parent not exist (func:***,line:***)	13	親プロセス
!PEXC14	*****(func:***,line:***)	49	出力内容

3.8.2.4. Job Scheduler for Cloud(AWS/Step Functions)

Job Scheduler for Cloud(AWS/Step Functions)の実行中にエラーが起きると、エラーメッセージがメッセージモニタに表示されます。

メッセージID	エラー内容	終了値	対処方法
!PEXC01	duplicate *****option (func:***,line:***)	5	オプション
	-m can not take S3 or MR or LS or LA or DF or GF or OF or IF or SF("****" is error) (func:***,line:***)	5	-mオプショ
	"****" is Unrecognized option (func:***,line:***)	5	不明なオ
	*****option not found (func:***,line:***)	5	必須オプ
	chdir("******") fail(***)	14	Senju/DC
	SENJUHOME("******") is too long	15	Senju/DC
	memory allocate error (func:***,line:***)	16	コマンドが
!PEXC02	child process start failed (***) (func:***,line:***)	9	子プロセス
!PEXC12	child killed by SIGNAL (***) (func:***,line:***)	8	子プロセス
	wait error (***) (func:***,line:***)	10	子プロセス
	child:parent not exist (func:***,line:***)	13	親プロセス
!PEXC24	*****(Date:***,Frame:***,Net:***,Job:***)	59	出力内容

3.8.2.5. Job Scheduler for Cloud(Azure/Durable Functions)

Job Scheduler for Cloud(Azure/Durable Functions)の実行中にエラーが起きると、エラーメッセージがメッセージモニタに表示されます。

メッセージID	エラー内容	終了値	対処方法
!PEXC01	duplicate *****option (func:***,line:***)	5	オプション
	-m can not take S3 or MR or LS or LA or DF or GF or OF or IFor SF("****" is error) (func:***,line:***)	5	-mオプショ
	"****" is Unrecognized option (func:***,line:***)	5	不明なオ
	*****option not found (func:***,line:***)	5	必須オプ
	chdir("******") fail(***)	14	Senju/DC
	SENJUHOME("******") is too long	15	Senju/DC
	memory allocate error (func:***,line:***)	16	コマンドが
!PEXC02	child process start failed (***) (func:***,line:***)	9	子プロセス
!PEXC12	child killed by SIGNAL (***) (func:***,line:***)	8	子プロセス
	wait error (***) (func:***,line:***)	10	子プロセス
!PEXC16	*****(func:***,line:***)	51	出力内容

3.8.2.6. Job Scheduler for Cloud(Google Cloud Functions)

Job Scheduler for Cloud(Google Cloud Functions)の実行中にエラーが起きると、エラーメッセージがメッセージモニタに表示されます。

メッセージID	エラー内容	終了値	対処方法
!PEXC01	duplicate *****option (func:***,line:***)	5	オプション
	-m can not take S3 or MR or LS or LA or DF or GF or OF or IF or SF("****" is error) (func:***,line:***)	5	-mオプショ
	"****" is Unrecognized option (func:***,line:***)	5	不明なオ
	*****option not found (func:***,line:***)	5	必須オプ
	chdir("******") fail(***)	14	Senju/DC
	SENJUHOME("******") is too long	15	Senju/DC
	memory allocate error (func:***,line:***)	16	コマンドが
!PEXC02	child process start failed (***) (func:***,line:***)	9	子プロセス
!PEXC12	child killed by SIGNAL (***) (func:***,line:***)	8	子プロセス
	wait error (***) (func:***,line:***)	10	子プロセス
!PEXC18	*****(func:***,line:***)	53	出力内容

3.8.2.7. Job Scheduler for Cloud(OCI/Functions)

Job Scheduler for Cloud(OCI/Functions)の実行中にエラーが起きると、エラーメッセージがメッセージモニタに表示されます。

メッセージID	エラー内容	終了値	対処方法
!PEXC01	duplicate *****option (func:***,line:***)	5	オプション
	-m can not take S3 or MR or LS or LA or DF or GF or OF or IF or SF("****" is error) (func:***,line:***)	5	-mオプショ
	"****" is Unrecognized option (func:***,line:***)	5	不明なオ
	*****option not found (func:***,line:***)	5	必須オプ
	chdir("******") fail(***)	14	Senju/DC
	SENJUHOME("******") is too long	15	Senju/DC
	memory allocate error (func:***,line:***)	16	コマンドが
!PEXC02	child process start failed (***) (func:***,line:***)	9	子プロセス
!PEXC12	child killed by SIGNAL (***) (func:***,line:***)	8	子プロセス
	wait error (***) (func:***,line:***)	10	子プロセス
!PEXC20	*****(func:***,line:***)	55	出力内容

3.8.2.8. Job Scheduler for Cloud(IBM Cloud Functions)

Job Scheduler for Cloud(IBM Cloud Functions)の実行中にエラーが起きると、エラーメッセージがメッセージモニタに表示されます。

メッセージID	エラー内容	終了値	対処方法
!PEXC01	duplicate *****option (func:***,line:***)	5	オプション
	-m can not take S3 or MR or LS or LA or DF or GF or OF or IF or SF("****" is error) (func:***,line:***)	5	-mオプショ
	"****" is Unrecognized option (func:***,line:***)	5	不明なオ
	*****option not found (func:***,line:***)	5	必須オプ
	chdir("******") fail(***)	14	Senju/DC
	SENJUHOME("******") is too long	15	Senju/DC
	memory allocate error (func:***,line:***)	16	コマンドが
!PEXC02	child process start failed (***) (func:***,line:***)	9	子プロセス
!PEXC12	child killed by SIGNAL (***) (func:***,line:***)	8	子プロセス
	wait error (***) (func:***,line:***)	10	子プロセス
!PEXC22	*****(func:***,line:***)	57	出力内容

3.8.3. Job Scheduler for Cloudのジョブログファイル

Senju/DCのジョブスケジュール機能を連携し、Job Scheduler for Cloudを実行すると、Job Scheduler for Cloudジョブの稼働情報が書かれたジョブログファイルが作成されます。

UNIX／Linuxの場合はJob Scheduler for Cloudが稼働するノード上の$SENJUHOME/dat/pex/aws ディレクトリ、Windowsの場合はJob

Scheduler for Cloudが稼働するノード上の%SENJUHOME%\dat\pex\awsディレクトリに、以下のファイル名で作成されます。

- UNIX／Linux:
  `"(運用日付)_(フレーム名)"/"(ネット名).(ジョブ名)"`
- Windows:
  `"(運用日付)_(フレーム名)"\"(ネット名).(ジョブ名)"`

3.8.3.1. Job Scheduler for Cloud(AWS/S3)のジョブログファイル

ジョブログファイルは、以下のフォーマットで出力されます。

`(日時)<TAB>(モード:アクション)<TAB>(ステータス)<TAB>(終了コード)<TAB>(バケット)<TAB>(AWS/S3のURI)<TAB>(ローカルパス)<TAB>(ステータス要因)`

各カラムの意味を以下に示します。

カラム	内容
日時	ファイルに書き込まれた日時が表示されます。
モード:アクション	Job Scheduler for Cloudの実行モードとアクションが表示されます。
ステータス	Job Scheduler for Cloudの実行ステータスが表示されます。
終了コード	Job Scheduler for Cloudの終了コードが表示されます。
バケット	処理の対象となるバケット名が表示されます。
AWS/S3のURI	処理の対象となるAWS/S3のURIが表示されます。
ローカルファイルパス	処理の対象となるローカルファイルパスが表示されます。
ステータス要因	Job Scheduler for Cloudのエラー要因を表示します。

3.8.3.2. Job Scheduler for Cloud(AWS/Elastic MapReduce)のジョブログファイル

ジョブログファイルは、以下のフォーマットで出力されます。

`(日時)<TAB>(モード:アクション)<TAB>(ステータス)<TAB>(終了コード)<TAB>(ジョブフローID)<TAB>(ジョブフロー名)<TAB>(ジョブステップ名)<TAB>(ステータス要因)`

各カラムの意味を以下に示します。

カラム	内容
日時	ファイルに書き込まれた日時が表示されます。
モード:アクション	Job Scheduler for Cloudの実行モードとアクションが表示されます。
ステータス	Job Scheduler for Cloudの実行ステータスが表示されます。
終了コード	Job Scheduler for Cloudの終了コードが表示されます。
ジョブフローID	AWS/ Elastic MapReduceのジョブフローIDが表示されます。
ジョブフロー名	AWS/ Elastic MapReduceのジョブフロー名が表示されます。
ジョブステップ名	AWS/ Elastic MapReduceのジョブステップ名が表示されます。
ステータス要因	Job Scheduler for Cloudのエラー要因を表示します。

3.8.3.3. Job Scheduler for Cloud(AWS/Lambda Function)のジョブログファイル

ジョブログファイルは、以下のフォーマットで出力されます。

`(日時)<TAB>(モード)<TAB>(ステータス)<TAB>(終了コード)<TAB>(リクエストID)<TAB>(未使用)<TAB>(関数名)<TAB>(ステータス要因)`

各カラムの意味を以下に示します。

カラム	内容
日時	ファイルに書き込まれた日時が表示されます。
モード	AWS連携コマンドの実行モード(LS/LA)が表示されます。
ステータス	Job Scheduler for Cloudの実行ステータスが表示されます。
終了コード	Job Scheduler for Cloudの終了コードが表示されます。
リクエストID	Lambda Functionが実行された時のリクエストIDが表示されます。非同期実行の際には取得されません。
(未使用)	
関数名	実行されたLambda関数名が表示されます。
ステータス要因	Job Scheduler for Cloudのエラー要因を表示します。

3.8.3.4. Job Scheduler for Cloud(AWS/Step Functions)のジョブログファイル

ジョブログファイルは、以下のフォーマットで出力されます。

(日時)<TAB>(モード:アクション)<TAB>(ステータス)<TAB>(終了コード)<TAB>(ステートマシン名)<TAB>(実行ARN)<TAB>(開始時刻 - 終了時刻)<TAB>(ステータス要因)

各カラムの意味を以下に示します。

カラム	内容
日時	ファイルに書き込まれた日時が表示されます。
モード:アクション	Job Scheduler for Cloudの実行モード(SF)とアクション(RUN/CHK)が表示されます。
ステータス	Job Scheduler for Cloudの実行ステータスが表示されます。
終了コード	Job Scheduler for Cloudの終了コードが表示されます。
ステートマシン名	開始したステートマシン名が表示されます。
実行ARN	開始したステートマシンの実行名(実行ARN)が表示されます。
開始時刻 - 終了時刻	開始したステートマシンの開始時刻と終了時刻が表示されます。
ステータス要因	Job Scheduler for Cloudのステータス要因を表示します。

3.8.3.5. Job Scheduler for Cloud(Azure/Durable Functions)のジョブログファイル

ジョブログファイルは、以下のフォーマットで出力されます。

(日時)<TAB>(モード)<TAB>(ステータス)<TAB>(終了コード)<TAB>(instanceId)<TAB>(statusQueryGetUri)<TAB>(orchestrator関数名)<TAB>(ステータス要因)

各カラムの意味を以下に示します。

カラム	内容
日時	ファイルに書き込まれた日時が表示されます。
モード	Azure連携コマンドの実行モード(DF)が表示されます。
ステータス	Job Scheduler for Cloudの実行ステータスが表示されます。
終了コード	Job Scheduler for Cloudの終了コードが表示されます。
instanceId	Durable Functionsが実行された時のinstanceIdが表示されます。
statusQueryGetUri	Durable Functionsが実行された時のstatusQueryGetUriが表示されます。
orchestrator関数名	実行されたorchestrator関数名が表示されます。
ステータス要因	Job Scheduler for Cloudのエラー要因を表示します。

3.8.3.6. Job Scheduler for Cloud(Google Cloud Functions)のジョブログファイル

ジョブログファイルは、以下のフォーマットで出力されます。

(日時)<TAB>(モード)<TAB>(ステータス)<TAB>(終了コード)<TAB>(ProjectID)<TAB>(ExecutionID)<TAB>(関数名)<TAB>(ステータス要因)

各カラムの意味を以下に示します。

カラム	内容
日時	ファイルに書き込まれた日時が表示されます。
モード	クラウドジョブスケジュールコマンドの実行モード(GF)が表示されます。
ステータス	Job Scheduler for Cloudの実行ステータスが表示されます。
終了コード	Job Scheduler for Cloudの終了コードが表示されます。
ProjectID	Cloud Functionsが実行された時のプロジェクトIDが表示されます。
ExecutionID	Cloud Functionsが実行された時のExecutionIDが表示されます。
関数名	Cloud Functions名が表示されます。
ステータス要因	Job Scheduler for Cloudのエラー要因を表示します。

3.8.3.7. Job Scheduler for Cloud(OCI/Functions)のジョブログファイル

ジョブログファイルは、以下のフォーマットで出力されます。

(日時) <TAB> (モード) <TAB> (ステータス) <TAB> (終了コード) <TAB> (リクエストID) <TAB> (アプリケーション名) <TAB> (関数名) <TAB> (ステータス要因)

各カラムの意味を以下に示します。

カラム	内容
日時	ファイルに書き込まれた日時が表示されます。
モード	クラウドジョブスケジュールコマンドの実行モード(OF)が表示されます。
ステータス	Job Scheduler for Cloudの実行ステータスが表示されます。
終了コード	Job Scheduler for Cloudの終了コードが表示されます。
リクエストID	Cloud Functionsが実行された時のリクエストIDが表示されます。
アプリケーション名	関数が所属するアプリケーション名が表示されます。
関数名	Cloud Functions名が表示されます。
ステータス要因	Job Scheduler for Cloudのエラー要因を表示します。

3.8.3.8. Job Scheduler for Cloud(IBM Cloud Functions)のジョブログファイル

ジョブログファイルは、以下のフォーマットで出力されます。

(日時) <TAB> (モード) <TAB> (ステータス) <TAB> (終了コード) <TAB> (リクエストID) <TAB> (ネームスペースID) <TAB> (関数名) <TAB> (ステータス要因)

各カラムの意味を以下に示します。

カラム	内容
日時	ファイルに書き込まれた日時が表示されます。
モード	クラウドジョブスケジュールコマンドの実行モード(IF)が表示されます。
ステータス	Job Scheduler for Cloudの実行ステータスが表示されます。
終了コード	Job Scheduler for Cloudの終了コードが表示されます。
リクエストID	Cloud Functionsが実行された時のリクエストIDが表示されます。
ネームスペースID	Cloud Functionsが所属するネームスペースIDが表示されます。
関数名	Cloud Functions名が表示されます。
ステータス要因	Job Scheduler for Cloudのエラー要因を表示します。

3.8.4. Job Scheduler for Cloudのコマンド一覧

Job Scheduler for Cloudで提供するコマンドの文法について説明します。Senju/DCのジョブスケジュール機能からの実行のほか、コマンドラインから実行することでAWSの操作を行うことができます。

3.8.4.1. AWS/S3 操作

3.8.4.1.1. AWS/S3データ取得

- 指定形式

  `sjPEX_AWSFunctions -m S3 -get S3URI -ak アクセスキーID -sk シークレットアクセスキー -bk S3バケット名`

- 目的

  AWS/S3上からデータの取得を行います。

- オプション

  - S3URI

    AWS/S3上のURIと取得先のローカルパスを','(カンマ)で区切って指定します。URIには s3:///バケット名/を外したファイル名までを指定します。省略不可です。

  - アクセスキーID

    AWS接続用のアクセスキーIDを指定します。

  - シークレットアクセスキー

    AWS接続用のシークレットアクセスキーを指定します。

  - S3バケット名

    AWS/S3上のバケットを指定します。

- 実行結果

  - (例)

    ```
    $ sjPEX_AWSFunctions -m S3 -get output.txt,/home/senju/tmpout/output.txt -bk aws-bucket
    S3:GET  OK      0       aws-bucket      output.txt      /home/senju/tmpout/output.txt
    ```

- 終了ステータス
  - 0 :正常終了
  - 11:システムエラー
  - 12:環境変数の取得に失敗
  - 13:ローカルパスが存在しない
  - 14:ローカルパスがファイルでない
  - 15:ファイルのオープンに失敗
  - 16:ファイルの書込みに失敗
  - 17:ファイルの読込みに失敗
  - 18:パラメータ解析に失敗
  - 30:AWSサービスエラー
  - 31:AWSクライアントエラー
  - 32:AWS/S3上に指定バケットが存在しない
  - 33:AWS/S3上に指定URIが存在しない
  - 36:取得ファイルサイズが上限を超えている

3.8.4.1.2. AWS/S3データ登録

- 指定形式

  `sjPEX_AWSFunctions -m S3 -put S3URI -ak アクセスキーID -sk シークレットアクセスキー -bk S3バケット名`

- 目的

  AWS/S3上へのデータの登録を行います。

- オプション

  - S3URI

    AWS/S3上のURIと対象データのローカルパスを','(カンマ)で区切って指定します。URIには s3:///バケット名/を外したファイル名までを指定します。省略不可です。

  - アクセスキーID

    AWS接続用のアクセスキーIDを指定します。sj_aws.iniで指定している場合は、省略可能です。

  - シークレットアクセスキー

AWS接続用のシークレットアクセスキーを指定します。sj_aws.iniで指定している場合は、省略可能です。

- S3バケット名

  AWS/S3上のバケットを指定します。sj_aws.iniで指定している場合は、省略可能です。

- 実行結果
  - (例)

```
$ sjPEX_AWSFunctions -m S3 -put put/input.txt,/home/senju/tmpout/input.txt -bk
aws-bucket
S3:PUT  OK      0       aws-bucket      put/input.txt
/home/senju/tmpout/input.txt
```

- 終了ステータス
  - 0 :正常終了
  - 11:システムエラー
  - 12:環境変数の取得に失敗
  - 13:ローカルパスが存在しない
  - 14:ローカルパスがファイルでない
  - 15:ファイルのオープンに失敗
  - 16:ファイルの書込みに失敗
  - 17:ファイルの読込みに失敗
  - 18:パラメータ解析に失敗
  - 30:AWSサービスエラー
  - 31:AWSクライアントエラー
  - 32:AWS/S3上に指定バケットが存在しない
  - 33:AWS/S3上に指定URIが存在しない

3.8.4.1.3. AWS/S3データ削除

- 指定形式

  `sjPEX_AWSFunctions -m S3 -del S3URI -ak アクセスキーID -sk シークレットアクセスキー -bk S3バケット名`

- 目的

  AWS/S3上からデータの削除を行います。

- オプション

  - S3URI

    AWS/S3上のURIを指定します。s3:///バケット名/を外したファイル名までを指定します。省略不可です。

  - アクセスキーID

    AWS接続用のアクセスキーIDを指定します。

    sj_aws.iniで指定している場合は、省略可能です。

  - シークレットアクセスキー

    AWS接続用のシークレットアクセスキーを指定します。

    sj_aws.iniで指定している場合は、省略可能です。

  - S3バケット名

    AWS/S3上のバケットを指定します。

    sj_aws.iniで指定している場合は、省略可能です。

- 実行結果
  - (例)

```
$ sjPEX_AWSFunctions -m S3 -del del/output.txt -bk aws-bucket
S3:DEL  OK      0       aws-bucket      del/output.txt
```

- 終了ステータス

- 0 :正常終了
- 11:システムエラー
- 12:環境変数の取得に失敗
- 13:ローカルパスが存在しない
- 14:ローカルパスがファイルでない
- 15:ファイルのオープンに失敗
- 16:ファイルの書込みに失敗
- 17:ファイルの読込みに失敗
- 18:パラメータ解析に失敗
- 30:AWSサービスエラー
- 31:AWSクライアントエラー
- 32:AWS/S3上に指定バケットが存在しない
- 33:AWS/S3上に指定URIが存在しない

3.8.4.1.4. AWS/S3データ確認

- 指定形式

  `sjPEX_AWSFunctions -m S3 -chk S3URI -ak アクセスキーID -sk シークレットアクセスキー -bk S3バケット名`

- 目的

  AWS/S3上からデータの確認を行います。

- オプション

  - S3URI

    AWS/S3上のURIを指定します。s3:///バケット名/を外したファイル名までを指定します。省略不可です。

  - アクセスキーID

    AWS接続用のアクセスキーIDを指定します。

    sj_aws.iniで指定している場合は、省略可能です。

  - シークレットアクセスキー

    AWS接続用のシークレットアクセスキーを指定します。

    sj_aws.iniで指定している場合は、省略可能です。

  - S3バケット名

    AWS/S3上のバケットを指定します。

    sj_aws.iniで指定している場合は、省略可能です。

- 実行結果

  - (例)

    ```
    $ sjPEX_AWSFunctions -m S3 -chk chk/input.txt -bk aws-bucket
    S3:CHK  OK      0       aws-bucket      chk/input.txt
    ```

- 終了ステータス
  - 0 :正常終了
  - 11:システムエラー
  - 12:環境変数の取得に失敗
  - 13:ローカルパスが存在しない
  - 14:ローカルパスがファイルでない
  - 15:ファイルのオープンに失敗
  - 16:ファイルの書込みに失敗
  - 17:ファイルの読込みに失敗
  - 18:パラメータ解析に失敗
  - 30:AWSサービスエラー
  - 31:AWSクライアントエラー
  - 32:AWS/S3上に指定バケットが存在しない

- 33：AWS/S3上に指定URIが存在しない

3.8.4.2. AWS/Elastic MapReduce 操作

3.8.4.2.1. AWS/MapReduceジョブフロー登録

- 指定形式

  `sjPEX_AWSFunctions -m MR -exec crt -ak アクセスキーID -sk シークレットアクセスキー -reg AWSリージョン -inc EC2インスタンス数 -mit EC2マスタインスタンスタイプ -sit EC2スレーブインスタンスタイプ -jfnジョブフロー名 -vpc サブネットID -luri ジョブフロー稼働ログ出力先URI`

- 目的

  AWS/Elastic MapReduceジョブフローの登録を行います。ジョブフローの登録に成功した場合、AWS/Elastic MapReduceサービスからジョブフローIDが割り当てられます。

- オプション

  - アクセスキーID

    AWS接続用のアクセスキーIDを指定します。
    sj_aws.iniで指定している場合は、省略可能です。

  - シークレットアクセスキー

    AWS接続用のシークレットアクセスキーを指定します。
    sj_aws.iniで指定している場合は、省略可能です。

  - AWSリージョン

    AWSの接続先リージョンを指定します。
    sj_aws.iniで指定している場合は、省略可能です。

  - EC2インスタンス数

    AWS/MRジョブフローを実行するEC2インスタンス数を指定します。
    sj_aws.iniで指定している場合は、省略可能です。省略した場合は、デフォルト値が設定されます。

  - EC2マスタインスタンスタイプ

    AWS/MRジョブフローを実行するEC2インスタンスタイプを指定します。
    sj_aws.iniで指定している場合は、省略可能です。省略した場合は、デフォルト値が設定されます。

  - EC2スレーブインスタンスタイプ

    AWS/MRジョブフローを実行するEC2インスタンスタイプを指定します。
    sj_aws.iniで指定している場合は、省略可能です。省略した場合は、デフォルト値が設定されます。

  - サブネットID

    クラスターを起動するVPCのサブネットIDを指定します。
    省略した場合は、デフォルトVPCのサブネットにてクラスターが起動します。

  - AWS/MapReduceジョブフローログ出力URI

    AWS/MapReduceジョブフローの稼働ログのURIを指定します。
    sj_aws.iniで指定している場合は、省略可能です。

- 標準出力

  - (例)

    ```
    $ sjPEX_AWSFunctions -m MR -exec crt -reg ap-northeast-1 -inc 3 -mit m1.medium -
    sit m1.medium -jfn emr-test -luri s3://aws-bucket/emr
    MR:CRT  OK      0       j-35E23QEM6JNWG emr-test
    ```

- 終了ステータス

- 0：正常終了
- 11：システムエラー
- 12：環境変数の取得に失敗
- 18：パラメータ解析に失敗
- 30：AWSサービスエラー
- 31：AWSクライアントエラー
- 34：AWS/Elastic MapReduce上に指定したジョブフローIDが存在しない
- 35：AWS/Elastic MapReduce上のジョブフローが既に終了している

3.8.4.2.2. AWS/MapReduceジョブフローステータスチェック

- 指定形式

  `sjPEX_AWSFunctions -m MR -exec chkj -ak アクセスキーID -sk シークレットアクセスキー -reg AWSリージョン -jid ジョブフローID`

- 目的

  AWS/Elastic MapReduceジョブフローのステータスチェックを行います。

- オプション

  - アクセスキーID

    AWS接続用のアクセスキーIDを指定します。
    sj_aws.iniで指定している場合は、省略可能です。

  - シークレットアクセスキー

    AWS接続用のシークレットアクセスキーを指定します。
    sj_aws.iniで指定している場合は、省略可能です。

  - AWSリージョン

    AWSの接続先リージョンを指定します。
    sj_aws.iniで指定している場合は、省略可能です。

  - ジョブフローID

    AWS/MRジョブフローのジョブフローIDを指定します。
    ジョブフローIDは、「AWS/MapReduceジョブフロー登録」で割り当てられた値を指定して下さい。

- 実行結果

  - (例)

```
$ sjPEX_AWSFunctions -m MR -exec chkj -reg ap-northeast-1 -jid j-35E23QEM6JXXX
MR:CHK  STARTING        0       j-35E23QEM6JXXX emr-test        Configuring
cluster software
```

- 終了ステータス
  - 0：正常終了
  - 11：システムエラー
  - 12：環境変数の取得に失敗
  - 18：パラメータ解析に失敗
  - 30：AWSサービスエラー
  - 31：AWSクライアントエラー
  - 34：AWS/Elastic MapReduce上に指定したジョブフローIDが存在しない
  - 35：AWS/Elastic MapReduce上のジョブフローが既に終了している

3.8.4.2.3. AWS/MapReduceジョブステップ追加・実行

- 指定形式

  `sjPEX_AWSFunctions -m MR -exec run -ak アクセスキーID -sk シークレットアクセスキー -reg AWSリージョン -jidジョブフローID -juri JarURI -mc Jarメインクラス -iuri Jarインプットプット URI -orui Jarアプトプット URI -args Jarパラメータ`

- 目的

  既に登録されているAWS/Elastic MapReduceジョブフローにカスタムjarジョブステップの追加・実行を行います。

- オプション

  - アクセスキーID

    AWS接続用のアクセスキーIDを指定します。

    sj_aws.iniで指定している場合は、省略可能です。

  - シークレットアクセスキー

    AWS接続用のシークレットアクセスキーを指定します。

    sj_aws.iniで指定している場合は、省略可能です。

  - AWSリージョン

    AWSの接続先リージョンを指定します。

    sj_aws.iniで指定している場合は、省略可能です。

  - ジョブフローID

    AWS/MRジョブフローのジョブフローIDを指定します。

    ジョブフローIDは、「AWS/MapReduceジョブフロー登録」で割り当てられた値を指定して下さい。

- 実行結果

  - (例)

```
$ sjPEX_AWSFunctions -m MR -exec run -reg ap-northeast-1 -jid j-35E23QEM6JNWG -
juri s3://aws-bucket/emr/emr-customjar.jar -mc main -jsn Step1 -iuri s3://aws-
bucket/emr/in -ouri s3://aws-bucket/emr/out -args arg1,arg2,arg3
MR:RUN  OK      0       j-35E23QEM6JNWG emr-test        Step1
```

- 終了ステータス
  - 0 : 正常終了
  - 11 : システムエラー
  - 12 : 環境変数の取得に失敗
  - 18 : パラメータ解析に失敗
  - 30 : AWSサービスエラー
  - 31 : AWSクライアントエラー
  - 34 : AWS/Elastic MapReduce上に指定したジョブフローIDが存在しない
  - 35 : AWS/Elastic MapReduce上のジョブフローが既に終了している

3.8.4.2.4. AWS/MapReduceジョブステップステータスチェック

- 指定形式

  `sjPEX_AWSFunctions -m MR -exec chks -ak アクセスキーID -sk シークレットアクセスキー -reg AWSリージョン -jid ジョブフローID`

- 目的

  AWS/Elastic MapReduceジョブステップのステータスチェックを行います。

- オプション

  - アクセスキーID

    AWS接続用のアクセスキーIDを指定します。

    sj_aws.iniで指定している場合は、省略可能です。

  - シークレットアクセスキー

    AWS接続用のシークレットアクセスキーを指定します。

    sj_aws.iniで指定している場合は、省略可能です。

  - AWSリージョン

AWSの接続先リージョンを指定します。
sj_aws.iniで指定している場合は、省略可能です。

- ジョブフローID

AWS/MRジョブフローのジョブフローIDを指定します。
ジョブフローIDは、「AWS/MapReduceジョブフロー登録」で割り当てられた値を指定して下さい。

- 実行結果
  - (例1)

```
$ sjPEX_AWSFunctions -m MR -exec chks -reg ap-northeast-1 -jid j-35E23QEM6JNWG
MR:CHK  RUNNING 0       j-35E23QEM6JNWG emr-test        Step1   Running step
```

- 終了ステータス
  - 0 :正常終了
  - 11:システムエラー
  - 12:環境変数の取得に失敗
  - 18:パラメータ解析に失敗
  - 30:AWSサービスエラー
  - 31:AWSクライアントエラー
  - 34:AWS/Elastic MapReduce上に指定したジョブフローIDが存在しない
  - 35:AWS/Elastic MapReduce上のジョブフローが既に終了している

3.8.4.2.5. AWS/MapReduceジョブフロー停止

- 指定形式

`sjPEX_AWSFunctions -m MR -exec trm -ak アクセスキーID -sk シークレットアクセスキー -reg AWSリージョン -jid ジョブフローID`

- 目的

既に登録されているAWS/Elastic MapReduceジョブフローの停止を行います。

- オプション
  - アクセスキーID

AWS接続用のアクセスキーIDを指定します。
sj_aws.iniで指定している場合は、省略可能です。

  - シークレットアクセスキー

AWS接続用のシークレットアクセスキーを指定します。
sj_aws.iniで指定している場合は、省略可能です。

  - AWSリージョン

AWSの接続先リージョンを指定します。
sj_aws.iniで指定している場合は、省略可能です。

  - ジョブフローID

AWS/MRジョブフローのジョブフローIDを指定します。
ジョブフローIDは、「AWS/MapReduceジョブフロー登録」で割り当てられた値を指定して下さい。

- 実行結果
  - (例)

```
$ sjPEX_AWSFunctions -m MR -exec trm -reg ap-northeast-1 -jid j-35E23QEM6JNWG
MR:TRM  OK      0       j-35E23QEM6JNWG emr-test
```

- 終了ステータス
  - 0 :正常終了
  - 11:システムエラー

- 12:環境変数の取得に失敗
- 18:パラメータ解析に失敗
- 30:AWSサービスエラー
- 31:AWSクライアントエラー
- 34:AWS/Elastic MapReduce上に指定したジョブフローIDが存在しない
- 35:AWS/Elastic MapReduce上のジョブフローが既に終了している

3.8.4.3. AWS/Lambda Function 操作

3.8.4.3.1. AWS/Lambda Functionの実行

- 指定形式

  `sjPEX_AWSFunctions -m LS -fnm Lambdaファンクション名 -lreg AWSリージョン -ak アクセスキーID -sk シークレットアクセスキー -cctf ファンクションパラメータ(JSONファイル名) -p プロファイル名 -ar ロールARN -ei AWS外部ID`

- 目的

  引数に指定された内容でAWS/Lambda Functionを実行し、実行結果を出力します。

- オプション

  - Lambdaファンクション名

    Lambda Function名を指定します。省略不可です。

  - AWSリージョン

    Lambda Function所属のリージョンを指定します。省略不可です。

  - アクセスキーID

    AWS接続用のアクセスキーIDを指定します。sj_aws.iniで指定している場合またはロール認証する場合は、省略可能です。

  - シークレットアクセスキー

    AWS接続用のシークレットアクセスキーを指定します。sj_aws.iniで指定している場合またはロール認証する場合は、省略可能です。

  - ファンクションパラメータ(JSONファイル名)

    Lambda Functionへ渡すJSONファイル名を指定します。省略可能です。

  - プロファイル名

    ロール認証に使用されるプロファイルを指定します。省略可能です。

  - ロールARN

    ロール認証に使用されるロールARNを指定します。省略可能です。

  - AWS外部ID

    ロール認証に使用される外部IDを指定します。省略可能です。

- 実行結果

  - (例)

    ```
    $ sjPEX_AWSFunctions -m LS -fnm FunctionTest -lreg ap-northeast-1 -cctf
    /home/senju/tmpout/cct.json -p myprofile
    LS      OK      0       ae89055c-3006-47be-8db4-3dbb008b2a3a    FunctionTest
    StatusCode:200, Duration: 14016.09 ms Billed Duration: 14017 ms Memory Size: 512
    MB Max Memory Used: 36 MB Init Duration: 114.35 ms
    ```

- 終了ステータス
  - 0 :正常終了
  - 11:システムエラー
  - 12:環境変数の取得に失敗
  - 15:ファイルオープンエラー
  - 17:ファイル読み取りエラー
  - 18:パラメータ解析に失敗

- 30：AWSサービスエラー
- 31：AWSクライアントエラー
- 40：Lambda Function実行エラー

3.8.4.4. AWS/Step Functions 操作

3.8.4.4.1. AWS/Step Functionsの実行

- 指定形式

  `sjPEX_AWSFunctions -m SF -exec run -ak アクセスキーID -sk シークレットアクセスキー -smn ステートマシンARN -exn 実行名 -sync -cctf ファンクションパラメータ(JSONファイル名)`

- 目的

  引数に指定された内容でAWS/Step Functionsを実行します。

- オプション

  - アクセスキーID

    AWS接続用のアクセスキーIDを指定します。sj_aws.iniで指定している場合は、省略可能です。

  - シークレットアクセスキー

    AWS接続用のシークレットアクセスキーを指定します。sj_aws.iniで指定している場合は、省略可能です。

  - ステートマシンARN

    AWS/Step Functions上のステートマシンARNを指定します。省略不可です。

  - 実行名

    AWS/Step Functions上のステートマシン実行時の識別名を指定します。省略可能です。

  - sync

    ワークフローの実行開始時の同期開始指定(-sync)。Expressワークフローで実行結果を取得したい場合に指定してください。省略可能です。

  - ファンクションパラメータ(JSONファイル名)

    ステートマシンへ渡すパラメータを記述したJSONファイル名を指定します。省略可能です。

- 実行結果

  - (例1)

    ```
    $ sjPEX_AWSFunctions -m SF -exec run -smn arn:aws:states:ap-northeast-
    1:181889877882:stateMachine:SFTest -exn test -cctf /home/senju/tmpout/cct.json
    SF:RUN  OK      0       SFTest  arn:aws:states:ap-northeast-
    1:181889877882:execution:SFTest:test        20220826-152425 -       STARTED
    ```

  - (例2)

    ```
    $ sjPEX_AWSFunctions -m SF -exec run -smn arn:aws:states:ap-northeast-
    1:181889877882:stateMachine:ExpressTest -exn test -sync -cctf
    /home/senju/tmpout/cct.json
    SF:RUN  OK      0       ExpressTest     arn:aws:states:ap-northeast-
    1:181889877882:express:ExpressTest:test:f34499a3-cd5c-4540-b745-c2de2583dffe
    20220826-135451 - 20220826-135451       SUCCEEDED
    ```

- 終了ステータス
  - 0 ：正常終了
  - 11：システムエラー
  - 12：環境変数の取得に失敗
  - 15：ファイルオープンエラー
  - 16：ファイル書き込みエラー
  - 17：ファイル読み取りエラー
  - 18：パラメータ解析に失敗
  - 30：AWSサービスエラー
  - 31：AWSクライアントエラー

3.8.4.4.2. AWS/Step Functionsのステータスチェック

- 指定形式

  `sjPEX_AWSFunctions -m SF -exec chk -ak アクセスキーID -sk シークレットアクセスキー -exn 実行ARN`

- 目的

  実行されたAWS/Step Functionsステートマシンの現在の状態を確認します。

- オプション

  - アクセスキーID

    AWS接続用のアクセスキーIDを指定します。sj_aws.iniで指定している場合は、省略可能です。

  - シークレットアクセスキー

    AWS接続用のシークレットアクセスキーを指定します。sj_aws.iniで指定している場合は、省略可能です。

  - 実行ARN

    AWS/Step Functionsステートマシンの実行ARNを指定します。省略不可です。

    標準タイプのステートマシンの実行ARNを指定して下さい。Expressタイプの状態は取得できません。

- 実行結果

  - (例)

```
$ sjPEX_AWSFunctions -m SF -exec chk -exn arn:aws:states:ap-northeast-
1:181889877882:execution:SFTest:test
SF:CHK  OK      0       SFTest  arn:aws:states:ap-northeast-
1:181889877882:execution:SFTest:test        20220826-144738 -       RUNNING
```

- 終了ステータス
  - 0 : 正常終了
  - 11 : システムエラー
  - 12 : 環境変数の取得に失敗
  - 15 : ファイルオープンエラー
  - 16 : ファイル書き込みエラー
  - 17 : ファイル読み取りエラー
  - 18 : パラメータ解析に失敗
  - 30 : AWSサービスエラー
  - 31 : AWSクライアントエラー

3.8.4.4.3. AWS/Step Functionsの停止

- 指定形式

  `sjPEX_AWSFunctions -m SF -exec trm -ak アクセスキーID -sk シークレットアクセスキー -exn 実行ARN -cause 停止理由`

- 目的

  既に実行されているAWS/Step Functionsステートマシンの停止を行います。

- オプション

  - アクセスキーID

    AWS接続用のアクセスキーIDを指定します。sj_aws.iniで指定している場合は、省略可能です。

  - シークレットアクセスキー

    AWS接続用のシークレットアクセスキーを指定します。sj_aws.iniで指定している場合は、省略可能です。

  - 実行ARN

    AWS/Step Functionsステートマシンの実行ARNを指定します。省略不可です。

    標準タイプのステートマシンの実行ARNを指定して下さい。Expressタイプは停止できません。

  - 停止理由

AWS/Step Functionsステートマシンを強制停止する理由を指定します。省略可能です。
省略した場合、Causeには"Forced stop"が設定されます。

- 実行結果
  - (例1)

```
$ sjPEX_AWSFunctions -m SF -exec trm -exn arn:aws:states:ap-northeast-
1:181889877882:execution:SFTest:test -cause stop
SF:TRM  OK      0       arn:aws:states:ap-northeast-
1:181889877882:execution:HelloWorld:stoptest06       - 20220826-152437
```

  - (例2)

```
$ sjPEX_AWSFunctions -m SF -exec trm -exn arn:aws:states:ap-northeast-
1:181889877882:express:ExpressTest:test:f34499a3-cd5c-4540-b745-c2de2583dffe
SF:TRM  OK      0       arn:aws:states:ap-northeast-
1:181889877882:express:ExpressTest:test:f34499a3-cd5c-4540-b745-c2de2583dffe
-      NOT SUPPORTED
```

- 終了ステータス
  - 0 :正常終了
  - 11:システムエラー
  - 12:環境変数の取得に失敗
  - 15:ファイルオープンエラー
  - 16:ファイル書き込みエラー
  - 17:ファイル読み取りエラー
  - 18:パラメータ解析に失敗
  - 30:AWSサービスエラー
  - 31:AWSクライアントエラー

3.8.4.5. Azure/Durable Functions 操作

3.8.4.5.1. Azure/Durable Functionsの実行

- 指定形式

  `sjPEX_AzureFunctions -furl ファンクションURL -ofnm Orchestratorファンクション名`

- 目的

  引数に指定された内容でAzure/Durable Functionsを実行し、実行結果を出力します。

- オプション

  - ファンクションURL

    Durable FunctionsのURLを指定します。省略不可です。

  - Orchestratorファンクション名

    Durable FunctionsのOrchestratorファンクション名を指定します。省略不可です。

- 実行結果
  - (例)

```
2019/09/10 14:32:54     DF      OK      0       b25fc5bdf8a94b35814530e2b17d18dd
https://functionapphmc.azurewebsites.net/runtime/webhooks/durabletask/instances/b2
5fc5bdf8a94b35814530e2b17d18dd?
taskHub=DurableFunctionsHub&connection=Storage&code=R4ad/aGzl7i0usBMq8xu0HnTLBgWet
yHaxzknlIldJNITnCrjaUZaQ==   DurableFunctionsOrchestrator1   [Hello Tokyo! Hello
Seattle! Hello London!]
```

- 終了ステータス
  - 0 :正常終了
  - 11:システムエラー
  - 15:ファイルオープンエラー
  - 17:ファイル読み取りエラー
  - 18:パラメータ解析に失敗

- 41：Durable Functions実行エラー

3.8.4.6. Google Cloud Functions 操作

3.8.4.6.1. Google Cloud Functionsの実行

- 指定形式

  `sjPEX_GCPFunctions -gfnm Google Cloudファンクション名 -gfr Google Cloudリージョン -gfdf ファンクションパラメータ(JSONファイル名) -gaf Google Cloudの認証ファイル`

- 目的

  引数に指定された内容でGoogle Cloud Functionsを実行し、実行結果を出力します。

- オプション

  - Google Cloudファンクション名

    Cloud Functionsの名前を指定します。省略不可です。

  - Google Cloudリージョン

    Cloud Functionsが存在するリージョンを指定します。省略不可です。

  - ファンクションパラメータ(JSONファイル名)

    Cloud Functionsへ渡す引数が記載されたJSONファイルを絶対パスで指定します。必要ない場合は省略可能です。

  - Google Cloudの認証ファイル

    Google CloudのAPIキー認証ファイルを絶対パスで指定します。省略可能です。

- 実行結果

  - (例)

    ```
    2020/03/03 09:02:28     GF      OK      0       test-develop    lj0n7yjr9hfx
    myFunctionTest  hello world
    ```

- 終了ステータス
  - 0 ：正常終了
  - 11：システムエラー
  - 15：ファイルオープンエラー
  - 17：ファイル読み取りエラー
  - 18：パラメータ解析に失敗
  - 42：Cloud Functions実行エラー

3.8.4.7. Google Cloud Composer 操作

3.8.4.7.1. タスクのクリア・起動コマンドの実行

- 指定形式

  `sjPEX_GCPCloudComposer -m ctk -pj projectId -env environment -loc location -did DAGID -tr taskRegex -us upstream -ds downstream -of onlyFailed -sd 開始日付 -ed 終了日付 -gaf 認証ファイル`

- 目的

  引数に指定された内容でタスクのクリア・起動を行い、実行結果を出力します。

- オプション

  - モード

    ctkで指定します。省略不可です。

  - projectId

    composer環境が所属するプロジェクトIDを指定します。省略不可です。

- environment
  composer環境の名称を指定します。省略不可です。
- location
  composer環境のlocationを指定します。省略不可です。
- DAGID
  DAGIDを指定します。省略不可です。
- taskRegex
  タスク正規表現を指定します。省略可能です。
- upstream
  false:指定したタスクのみクリア; true:upstreamタスクもクリアします。省略可能です。
- downstream
  false:指定したタスクのみクリア; true:downstreamタスクもクリアします。省略可能です。
- onlyFailed
  false:条件を満たすタスクをクリア; true:Failedのタスクのみクリアします。省略可能です。
- 開始日付
  開始日付(UTC)を指定します。(YYYY-MM-DD;YYYY-MM-DDT00:00:00.949358+00:00)。省略可能です。
- 終了日付
  終了日付(UTC)を指定します。(YYYY-MM-DD;YYYY-MM-DDT00:00:00.949358+00:00)。省略可能です。
- Google Cloudの認証ファイル
  Google CloudのAPIキー認証ファイルを絶対パスで指定します。省略可能です。

- 実行結果
  - (例)

```
$ sjPEX_GCPCloudComposer -m ctk -env environment -loc location -did DAGID -tr
taskRegex -sd 開始日付 -ed 終了日付 -gaf 認証ファイル
clearTask was successfully executed.
```

- 終了ステータス
  - 0 :正常終了
  - 11:システムエラー
  - 15:ファイルオープンエラー
  - 17:ファイル読み取りエラー
  - 18:パラメータ解析に失敗
  - 67:clearTask実行エラー

3.8.4.7.2. タスクのMark Failedコマンドの実行

- 指定形式
  `sjPEX_GCPCloudComposer -m mf -url airflowWebUi -did DAGID -tid タスクID -exed 実行日付 -us upstream -ds downstream -gaf 認証ファイル`
- 目的
  引数に指定された内容でタスクのMark Failedを行い、実行結果を出力します。
- オプション
  - モード
    mfで指定します。省略不可です。
  - airflowWebUi
    composer環境のairflowWebUiを指定します。省略不可です。
  - DAGID

DAGIDを指定します。省略不可です。

- タスクID
  タスクIDを指定します。省略不可です。
- 実行日付
  executionDateを指定します。省略不可です。
- upstream
  false:指定したタスクのみ実施;true:upstreamタスクも実施します。省略可能です。
- downstream
  false:指定したタスクのみ実施;true:downstreamタスクも実施します。省略可能です。
- Google Cloudの認証ファイル
  Google CloudのAPIキー認証ファイルを絶対パスで指定します。省略可能です。

- 実行結果
  - (例)

```
$ sjPEX_GCPCloudComposer -m mf -url airflowWebUi -did DAGID -tid タスクID -exed 実行日付 -gaf 認証ファイル
markFailed was successfully executed.
```

- 終了ステータス
  - 0 :正常終了
  - 11:システムエラー
  - 15:ファイルオープンエラー
  - 17:ファイル読み取りエラー
  - 18:パラメータ解析に失敗
  - 68:markFailed実行エラー

3.8.4.7.3. DAGのMark Failedコマンドの実行

- 指定形式

```
sjPEX_GCPCloudComposer -m dmf -url airflowWebUi -did DAGID -eid 実行ID -gaf 認証ファイル
```

- 目的
  引数に指定された内容でDAGのMark Failedを行い、実行結果を出力します。
- オプション
  - モード
    dmfで指定します。省略不可です。
  - airflowWebUi
    composer環境のairflowWebUiを指定します。省略不可です。
  - DAGID
    DAGIDを指定します。省略不可です。
  - 実行ID
    実行IDを指定します。省略不可です。
  - Google Cloudの認証ファイル
    Google CloudのAPIキー認証ファイルを絶対パスで指定します。省略可能です。
- 実行結果
  - (例)

```
$ sjPEX_GCPCloudComposer -m dmf -url airflowWebUi -did DAGID -eid 実行ID -gaf 認証ファイル
dagMarkFailed was successfully executed.
```

- 終了ステータス
    - 0 :正常終了
    - 11:システムエラー
    - 15:ファイルオープンエラー
    - 17:ファイル読み取りエラー
    - 18:パラメータ解析に失敗
    - 74:dagMarkFailed実行エラー

3.8.4.7.4. タスクの強制起動コマンドの実行

- 指定形式

  `sjPEX_GCPCloudComposer -m trk -pj projectId -env environment -loc location -did DAGID -tid タスクID -eid 実行ID(実行日付) -igd ignoreDependencies -f force -gaf 認証ファイル`

- 目的

  引数に指定された内容でタスクの強制起動を実施し、実行結果を出力します。

- オプション

    - モード

      trkで指定します。省略不可です。

    - projectId

      composer環境が所属するプロジェクトIDを指定します。省略不可です。

    - environment

      composer環境の名称を指定します。省略不可です。

    - location

      composer環境のlocationを指定します。省略不可です。

    - DAGID

      DAGIDを指定します。省略不可です。

    - タスクID

      タスクIDを指定します。省略不可です。

    - 実行ID(実行日付)

      実行ID(実行日付)を指定します。(日付例:2022-09-24T12:51:13.063238+00:00)。省略不可です。

    - ignoreDependencies

      false:先行が終わらないと実施しない;true:先行が終わらなくても実施します。省略可能です。

    - force

      false:Success済みは実施しない;true:Success済みでも実施します。省略可能です。

    - Google Cloudの認証ファイル

      Google CloudのAPIキー認証ファイルを絶対パスで指定します。省略可能です。

- 実行結果

    - (例)

      ```
      $ sjPEX_GCPCloudComposer -m trk -pj projectId -env environment -loc location -did
      DAGID -tid タスクID -eid 実行ID(実行日付) -igd ignoreDependencies -f force -gaf 認証
      ファイル
      taskRun was successfully executed.
      ```

- 終了ステータス
    - 0 :正常終了
    - 11:システムエラー
    - 15:ファイルオープンエラー
    - 17:ファイル読み取りエラー
    - 18:パラメータ解析に失敗

- 70：taskRun実行エラー

3.8.4.7.5. DAGの強制起動コマンドの実行

- 指定形式

  `sjPEX_GCPCloudComposer -m dr -url airflowWebUi -did DAGID -eid 実行ID -ld logicalDate -df DAGパラメータ(JSONファイル名) -gaf 認証ファイル`

- 目的

  引数に指定された内容でDAGの強制起動を実施し、実行結果を出力します。

- オプション

  - モード

    drで指定します。省略不可です。

  - airflowWebUi

    composer環境が所属するプロジェクトIDを指定します。省略不可です。

  - DAGID

    DAGIDを指定します。省略不可です。

  - 実行ID

    実行IDを指定します。(未指定の場合、GCPにより自動採番)。省略可能です。

  - logicalDate

    logicalDateを指定します。(日付例：2023-02-07T09:15:00+00:00)。省略可能です。

  - DAGパラメータ(JSONファイル名)

    jsonファイルで「DAGへ渡すパラメータ」を指定します。省略可能です。

  - Google Cloudの認証ファイル

    Google CloudのAPIキー認証ファイルを絶対パスで指定します。省略可能です。

- 実行結果

  - (例)

    ```
    $ sjPEX_GCPCloudComposer -m dr -url airflowWebUi -did DAGID -eid 実行ID -ld
    logicalDate -df JSONファイル名 -gaf 認証ファイル
    dagRun was successfully executed.
    ```

- 終了ステータス
  - 0 ：正常終了
  - 11：システムエラー
  - 15：ファイルオープンエラー
  - 17：ファイル読み取りエラー
  - 18：パラメータ解析に失敗
  - 76：dagRun実行エラー

3.8.4.7.6. DAGをPauseにするコマンドの実行

- 指定形式

  `sjPEX_GCPCloudComposer -m p -url airflowWebUi -did DAGID -gaf 認証ファイル`

- 目的

  引数に指定された内容で対象DAGをPauseにし、実行結果を出力します。

- オプション

  - モード

    pで指定します。省略不可です。

  - airflowWebUi

composer環境が所属するプロジェクトIDを指定します。省略不可です。

- DAGID

  DAGIDを指定します。省略不可です。

- Google Cloudの認証ファイル

  Google CloudのAPIキー認証ファイルを絶対パスで指定します。省略可能です。

- 実行結果

  - (例)

```
$ sjPEX_GCPCloudComposer -m p -url airflowWebUi -did DAGID -gaf 認証ファイル
pause was successfully executed.
```

- 終了ステータス
  - 0 : 正常終了
  - 11 : システムエラー
  - 15 : ファイルオープンエラー
  - 17 : ファイル読み取りエラー
  - 18 : パラメータ解析に失敗
  - 71 : pause実行エラー

3.8.4.7.7. DAGをUnpauseにするコマンドの実行

- 指定形式

  `sjPEX_GCPCloudComposer -m up -url airflowWebUi -did DAGID -gaf 認証ファイル`

- 目的

  引数に指定された内容で対象DAGをUnpauseにし、実行結果を出力します。

- オプション

  - モード

    upで指定します。省略不可です。

  - airflowWebUi

    composer環境が所属するプロジェクトIDを指定します。省略不可です。

  - DAGID

    DAGIDを指定します。省略不可です。

  - Google Cloudの認証ファイル

    Google CloudのAPIキー認証ファイルを絶対パスで指定します。省略可能です。

- 実行結果

  - (例)

```
$ sjPEX_GCPCloudComposer -m up -url airflowWebUi -did DAGID -gaf 認証ファイル
unPause was successfully executed.
```

- 終了ステータス
  - 0 : 正常終了
  - 11 : システムエラー
  - 15 : ファイルオープンエラー
  - 17 : ファイル読み取りエラー
  - 18 : パラメータ解析に失敗
  - 72 : unPause実行エラー

3.8.4.7.8. タスクのMark Successコマンドの実行

- 指定形式

`sjPEX_GCPCloudComposer -m ms -url airflowWebUi -did DAGID -tid タスクID -exed 実行日付 -us upstream -ds downstream -gaf 認証ファイル`

- 目的

  引数に指定された内容でタスクのMark Successを行い、実行結果を出力します。

- オプション

  - モード

    msで指定します。省略不可です。

  - airflowWebUi

    composer環境が所属するプロジェクトIDを指定します。省略不可です。

  - DAGID

    DAGIDを指定します。省略不可です。

  - タスクID

    タスクIDを指定します。省略不可です。

  - 実行日付

    executionDateを指定します。省略不可です。

  - upstream

    false:指定したタスクのみ実施;true:upstreamタスクも実施します。省略可能です。

  - downstream

    false:指定したタスクのみ実施;true:downstreamタスクも実施します。省略可能です。

  - Google Cloudの認証ファイル

    Google CloudのAPIキー認証ファイルを絶対パスで指定します。省略可能です。

- 実行結果

  - (例)

```
$ sjPEX_GCPCloudComposer -m ms -url airflowWebUi -did DAGID -tid タスクID  -exed 実行日付 -us false -gaf 認証ファイル
markSuccess was successfully executed.
```

- 終了ステータス
  - 0 :正常終了
  - 11:システムエラー
  - 15:ファイルオープンエラー
  - 17:ファイル読み取りエラー
  - 18:パラメータ解析に失敗
  - 69:markSuccess実行エラー

3.8.4.7.9. DAGのMark Successコマンドの実行

- 指定形式

  `sjPEX_GCPCloudComposer -m dms -url airflowWebUi -did DAGID -eid 実行ID -gaf 認証ファイル`

- 目的

  引数に指定された内容でDAGのMark Successを行い、実行結果を出力します。

- オプション

  - モード

    dmsで指定します。省略不可です。

  - airflowWebUi

    composer環境のairflowWebUiを指定します。省略不可です。

  - DAGID

DAGIDを指定します。省略不可です。

- 実行ID

  実行IDを指定します。省略不可です。

- Google Cloudの認証ファイル

  Google CloudのAPIキー認証ファイルを絶対パスで指定します。省略可能です。

- 実行結果

  - (例)

```
$ sjPEX_GCPCloudComposer -m dms -url airflowWebUi -did DAGID -eid 実行ID -gaf 認証
ファイル
dagMarkSuccess was successfully executed.
```

- 終了ステータス
  - 0 :正常終了
  - 11:システムエラー
  - 15:ファイルオープンエラー
  - 17:ファイル読み取りエラー
  - 18:パラメータ解析に失敗
  - 75:dagMarkSuccess実行エラー

3.8.4.7.10. 環境変数を設定_追加コマンドの実行

- 指定形式

  `sjPEX_GCPCloudComposer -m av -url airflowWebUi -k key -v value -gaf 認証ファイル`

- 目的

  引数に指定された内容で環境変数に値を追加し、実行結果を出力します。

- オプション

  - モード

    avで指定します。省略不可です。

  - airflowWebUi

    composer環境が所属するプロジェクトIDを指定します。省略不可です。

  - key

    variableKeyを指定します。省略不可です。

  - value

    追加したいValueを指定します。([]で囲む。例:[a1][a2][a3]。Linuxの場合、"["、"]"の前にを付ける必要あり)。省略不可です。

  - Google Cloudの認証ファイル

    Google CloudのAPIキー認証ファイルを絶対パスで指定します。省略可能です。

- 実行結果

  - (例)

```
$ sjPEX_GCPCloudComposer -m av -url airflowWebUi -k skip_dag_list -v [a1][a3] -gaf
認証ファイル
addVariable was successfully executed.
Create a new key "skip_dag_list" because the specified key does not exist.
key: skip_dag_list addValue: [a1][a3]
```

- 終了ステータス
  - 0 :正常終了
  - 11:システムエラー
  - 15:ファイルオープンエラー
  - 17:ファイル読み取りエラー
  - 18:パラメータ解析に失敗

- 77addVariable実行エラー

3.8.4.7.11. 環境変数を設定_削除コマンドの実行

- 指定形式

  `sjPEX_GCPCloudComposer -m dv -url airflowWebUi -k key -v value -gaf 認証ファイル`

- 目的

  引数に指定された内容で環境変数から値を削除し、実行結果を出力します。

- オプション

  - モード

    dvで指定します。省略不可です。

  - airflowWebUi

    composer環境が所属するプロジェクトIDを指定します。省略不可です。

  - key

    variableKeyを指定します。省略不可です。

  - value

    削除したいValueを指定します。([]で囲む。例:[a1][a2][a3]。Linuxの場合、"["、"]"の前にを付ける必要あり)。省略不可です。

  - Google Cloudの認証ファイル

    Google CloudのAPIキー認証ファイルを絶対パスで指定します。省略可能です。

- 実行結果

  - (例)

    ```
    $ sjPEX_GCPCloudComposer -m dv -url airflowWebUi -k skip_dag_list -v [a2][a3][a4]
    -gaf 認証ファイル
    delVariable was successfully executed.
    key: skip_dag_list delValue: [a2][a3]
    key: skip_dag_list skipValue: [a4]
    ```

- 終了ステータス
  - 0 :正常終了
  - 11:システムエラー
  - 15:ファイルオープンエラー
  - 17:ファイル読み取りエラー
  - 18:パラメータ解析に失敗
  - 78:delVariable実行エラー

3.8.4.7.12. DAGの状態一覧を取得コマンドの実行

- 指定形式

  `sjPEX_GCPCloudComposer -m ld -url airflowWebUi -did DAGID -l limit -s ソート順 -edg 開始日付 -edl 終了日付 -gaf 認証ファイル`

- 目的

  引数に指定された内容でDAGの状態一覧を取得し、実行結果を出力します。

- オプション

  - モード

    ldで指定します。省略不可です。

  - airflowWebUi

    composer環境が所属するプロジェクトIDを指定します。省略不可です。

  - DAGID

DAGIDを指定します。省略不可です。

- limit

  取得の上限件数を指定します。(最大100件まで)。省略可能です。

- ソート順

  ソート条件を指定します。(execution_date:昇順;-execution_date:降順)。省略可能です。

- 開始日付

  取得範囲の開始日付を指定します。省略可能です。

- 終了日付

  取得範囲の終了日付を指定します。省略可能です。

- Google Cloudの認証ファイル

  Google CloudのAPIキー認証ファイルを絶対パスで指定します。省略可能です。

- 実行結果

  - (例)

```
$ sjPEX_GCPCloudComposer -m ld -url airflowWebUi -did DAGID -l limit -s ソート順 -
edg 開始日付 -edl 終了日付 -gaf 認証ファイル
listDAG was successfully executed.
{
  "dag_runs": [
    {
      "conf": {},
      "dag_id": "composer_quickstart",
      "dag_run_id": "scheduled__2022-05-16T08:31:04.518480+00:00",
      "end_date": "2022-05-17T08:31:09.974760+00:00",
      "execution_date": "2022-05-16T08:31:04.518480+00:00",
      "external_trigger": false,
      "logical_date": "2022-05-16T08:31:04.518480+00:00",
      "start_date": "2022-05-17T08:31:05.805751+00:00",
      "state": "success"
    },
    {
      "conf": {},
      "dag_id": "composer_quickstart",
      "dag_run_id": "manual__2022-05-17T10:41:53.513645+00:00",
      "end_date": "2022-05-17T10:42:00.798525+00:00",
      "execution_date": "2022-05-17T10:41:53.513645+00:00",
      "external_trigger": true,
      "logical_date": "2022-05-17T10:41:53.513645+00:00",
      "start_date": "2022-05-17T10:41:54.902172+00:00",
      "state": "success"
    },
    ...
    ...
    ...
  ],
  "total_entries": 112
}
```

- 終了ステータス
  - 0 :正常終了
  - 11:システムエラー
  - 15:ファイルオープンエラー
  - 17:ファイル読み取りエラー
  - 18:パラメータ解析に失敗
  - 73:listDag実行エラー

3.8.4.7.13. 起動したタスクの情報取得コマンドの実行

- 指定形式

  `sjPEX_GCPCloudComposer -m gt -url airflowWebUi -did DAGID -eid 実行ID -tid タスクID -gaf 認証ファイル`

- 目的

  引数に指定された内容で起動したタスク情報を取得し、実行結果を出力します。

- オプション
    - モード
        gtで指定します。省略不可です。
    - airflowWebUi
        composer環境が所属するプロジェクトIDを指定します。省略不可です。
    - DAGID
        DAGIDを指定します。省略不可です。
    - 実行ID
        実行IDを指定します。省略不可です。
    - タスクID
        タスクIDを指定します。省略不可です。
    - Google Cloudの認証ファイル
        Google CloudのAPIキー認証ファイルを絶対パスで指定します。省略可能です。
- 実行結果
    - (例)

```
$ sjPEX_GCPCloudComposer -m gt -url airflowWebUi -did DAGID -eid 実行ID -tid タスク
ID -gaf 認証ファイル
getTask was successfully executed.
{
  "dag_id": "composer_quickstart_230814",
  "duration": 31.619697,
  "end_date": "2023-08-14T06:03:20.679962+00:00",
  "execution_date": "2023-08-14T06:02:22.577503+00:00",
  "executor_config": "{}",
  "hostname": "airflow-worker-pmnjs",
  "max_tries": 1,
  "operator": "BashOperator",
  "pid": 6781,
  "pool": "default_pool",
  "pool_slots": 1,
  "priority_weight": 2,
  "queue": "default",
  "queued_when": "2023-08-14T06:02:47.480766+00:00",
  "sla_miss": null,
  "start_date": "2023-08-14T06:02:49.060265+00:00",
  "state": "success",
  "task_id": "composer_quickstart_task_230814_bye2",
  "try_number": 1,
  "unixname": "airflow"
}
```

- 終了ステータス
    - 0 : 正常終了
    - 11 : システムエラー
    - 15 : ファイルオープンエラー
    - 17 : ファイル読み取りエラー
    - 18 : パラメータ解析に失敗
    - 79 : getTask実行エラー

3.8.4.7.14. DAGの基本情報取得コマンドの実行

- 指定形式
    `sjPEX_GCPCloudComposer -m gd -url airflowWebUi -did DAGID -gaf 認証ファイル`
- 目的
    引数に指定された内容でDAGの基本情報を取得し、実行結果を出力します。
- オプション
    - モード
        gdで指定します。省略不可です。

- airflowWebUi

  composer環境が所属するプロジェクトIDを指定します。省略不可です。

- DAGID

  DAGIDを指定します。省略不可です。

- Google Cloudの認証ファイル

  Google CloudのAPIキー認証ファイルを絶対パスで指定します。省略可能です。

- 実行結果

  - (例)

```
$ sjPEX_GCPCloudComposer -m gd -url airflowWebUi -did DAGID -gaf 認証ファイル
getDag was successfully executed.
{
  "dag_id": "composer_quickstart_230814",
  "description": null,
  "file_token":
"Ii9ob21lL2FpcmZsb3cvZ2NzL2RhZ3MvY29tcG9zZXJfcXVpY2tzdGFydF8yMzA5MTQucHki.aKo3bDkE
0S5ZyfrSN1agiw41wvA",
  "fileloc": "/home/airflow/gcs/dags/composer_quickstart_230914.py",
  "is_active": true,
  "is_paused": false,
  "is_subdag": false,
  "owners": [
    "Composer test1"
  ],
  "root_dag_id": null,
  "schedule_interval": {
    "__type": "TimeDelta",
    "days": 1,
    "microseconds": 0,
    "seconds": 0
  },
  "tags": []
}
```

- 終了ステータス
  - 0 :正常終了
  - 11:システムエラー
  - 15:ファイルオープンエラー
  - 17:ファイル読み取りエラー
  - 18:パラメータ解析に失敗
  - 80:getDag実行エラー

3.8.4.8. OCI/Functions 操作

3.8.4.8.1. OCI/Functionsの実行

- 指定形式

  `sjPEX_OCIFunctions -ofc OCIコンパートメント名 -ofa OCIアプリケーション名 -ofn OCIファンクション名 -ofpf ファンクションパラメータ(JSONファイル名) -ouf OCIの認証ファイル`

- 目的

  引数に指定された内容でOCI/Functionsを実行し、実行結果を出力します。

- オプション

  - OCIコンパートメント名

    Cloud コンパートメントの名前を指定します。省略不可です。

  - OCIアプリケーション名

    Cloud アプリケーションの名前を指定します。省略不可です。

  - OCIファンクション名

    Oracle Functionsの名前を指定します。省略不可です。

  - ファンクションパラメータ(JSONファイル名)

Oracle Functionsへ渡す引数が記載されたJSONファイルを絶対パスで指定します。必要ない場合は省略可能です。

- OCIの認証ファイル

  OCIのAPIキー認証ファイルを絶対パスで指定します。省略可能です。

- 実行結果
  - (例)

```
2020/07/28 09:02:28     OF      OK      0
d7be37df9c83ea9aa0b3294041bc1f60/01EG7W79QS1BT0S3RZJ004K3CE/01EG7W79QS1BT0S3RZJ004
K3CF  helloworld-app  functions-func  hello world
```

- 終了ステータス
  - 0 :正常終了
  - 11:システムエラー
  - 15:ファイルオープンエラー
  - 17:ファイル読み取りエラー
  - 18:パラメータ解析に失敗
  - 46:Cloud Functions実行エラー

3.8.4.9. IBM Cloud Functions 操作

3.8.4.9.1. IBM Cloud Functionsの実行

- 指定形式

  `sjPEX_IBCFunctions -ins ネームスペースID -ifn IBM Cloudファンクション名 -ifdf ファンクションパラメータ(JSONファイル名) -iuf IBM Cloudの認証ファイル`

- 目的

  引数に指定された内容でIBM Cloud Functionsを実行し、実行結果を出力します。

- オプション
  - ネームスペースID

    ファンクションが所属するネームスペースIDを指定します。省略不可です。

  - IBM Cloudファンクション名

    Cloud Functionsの名前を指定します。省略不可です。

  - ファンクションパラメータ(JSONファイル名)

    Cloud Functionsへ渡す引数が記載されたJSONファイルを絶対パスで指定します。必要ない場合は省略可能です。

  - IBM Cloudの認証ファイル

    IBM Cloudの認証ファイルを絶対パスで指定します。省略可能です。

- 実行結果
  - (例)

```
2020/03/03 09:02:28     IF      OK      0       e98dee346eac54354545ef1 we323wew-
1dc4-4567-453b-2w3e4r5t6ytr    testFunc        {"message","hello world"}
```

- 終了ステータス
  - 0 :正常終了
  - 11:システムエラー
  - 15:ファイルオープンエラー
  - 17:ファイル読み取りエラー
  - 18:パラメータ解析に失敗
  - 57:Cloud Functions実行エラー

3.8.5. 制限事項

3.8.5.1. Job Scheduler for Cloudの制限事項

- Job Scheduler for Cloudで利用する、AWS/Azure/Google Cloud/OCI/IBM Cloudの各サービスは利用状況により料金が発生します。詳細についてはAmazon Web Services/Microsoft Azure/Google Cloud/Oracle Cloud Infrastructure/IBM Cloudよりご確認下さい。
- Job Scheduler for Cloudを利用する該当ノードのマシン時刻を未来に進めた状態でAWS/Azure/Google Cloud/OCI/IBM Cloudにアクセスすると通信エラーが発生する場合があります。

- sj_aws.iniおよびAWS/Elastic MapReduceジョブフロー実行ジョブに設定可能なAWSリージョンはAWSがElastic MapReduceサービスを提供しているリージョンに依存します。

  以下に、AWSリージョンと設定する値の例を示します。詳細についてはAmazon Web Servicesよりご確認下さい。

AWSリージョン	値
米国東部（バージニア）	us-east-1
米国西部（カルフォルニア）	us-west-1
米国西部（オレゴン）	us-west-2
EU（アイルランド）	eu-west-1
アジアパフィック（シンガポール）	ap-southeast-1
アジアパフィック（東京）	ap-northeast-1

- sj_aws.iniおよびAWS/Elastic MapReduce AWSジョブフロー実行ジョブに設定可能なEC2インスタンスタイプはAWS/EC2で利用可能なインスタンスタイプに依存します。

  以下に、インスタンスタイプと設定する値の例を示します。詳細についてはAmazon Web Servicesよりご確認下さい。

インスタンスタイプ	値
スモール インスタンス	m1.small
ラージ インスタンス	m1.large
エクストララージ インスタンス	m1.xlarge
マイクロインスタンス	t1.micro
ハイメモリ エクストララージ インスタンス	m2.xlarge
ハイメモリ ダブルエクストララージ インスタンス	m2.2xlarge
ハイメモリ クアドラプル エクストララージ インスタンス	m2.4xlarge
ハイ CPU ミディアム インスタンス	c1.medium
ハイ CPU エクストララージ インスタンス	c1.xlarge
クラスタコンピュート クアドラプル エクストララージ インスタンス	cc1.4xlarge
クラスタ GPU コンピュート クアドラプル エクストララージ インスタンス	cg1.4xlarge

- AWS/S3データ取得ジョブジョブで取得可能な最大ファイルサイズは300MByteです。

  300MByteを超えたファイルを指定した場合はエラーとなります。

- AWS/S3データ登録ジョブでファイルの転送中に対象ファイルに書込みが行われた場合はエラーとなります。
- AWS/S3のバケット名に使用可能な文字の種類はリージョンにより異なります。詳細については、Amazon Web Servicesサイトよりご確認下さい。
- AWS(Elastic MapReduce)ジョブで指定可能なEC2インスタンス数の上限は、既定では1つのリージョンで20が上限となります。EC2インスタンス数上限を拡張する場合、Amazon Web Serviceの専用フォームから上限緩和の申請を行う必要があります。詳しくはAmazon Web Servicにお問い合わせ下さい。
- Google Cloud Composer連携コマンドはairflow Version2.2.5までサポートします。
- DAGの状態一覧を取得コマンドのパラメータ「limit」はAPIの仕様が上限100件までのため、1~100の値で指定可能です。
- DAGのMark Successコマンドを利用するために、airflow Version2.2.0以上が必要となります。

4. Container Monitoring

4.1. はじめに

4.1.1. 本章について

- 本章では、コンテナ監視(Docker/Kubernetes/Podman/OpenShift)エクステンション の機能や使用方法について説明します。
- コンテナ監視(Docker/Kubernetes/Podman/OpenShift)エクステンション は Docker、Kubenetes、Podman および OpenShift などのコンテナ運用基盤について、Senju DevOperation Conductor のモニタリング機能を連携させることができます。この連携により、Senju DevOperation Conductorのモニタリング機能からDocker、Kubernetes、PodmanおよびOpenShiftを監視することができるようになります。
- 「Senju DevOperation Conductor」は（株）野村総合研究所の登録商標です。
- Dockerは、Docker,Inc.の米国およびその他の国における登録商標または商標です。
- Kubernetesは、The Linux Foundationの米国およびその他の国における登録商標または商標です。
- OpenShiftは、Red Hat, Inc.の米国およびその他の国における登録商標または商標です。
- Linuxは、Linus Torvalds氏の登録商標です。
- Windows、Windows Serverは、米国Microsoft Corporationの米国及びその他の国における登録商標または商標です。
- 本章では、CC-BY-4.0 適用ソフトウェアである Kubernetes Icons Set を使用しています。
- その他、本誌で引用の製品名・会社名はそれぞれの会社の商標、もしくは登録商標です。なお、本誌中では、™、® マークなどは明記していません。

4.1.2. 読者の対象

本章は Senju DevOperation Conductorのモニタリング機能からDocker、Kubenetes、PodmanおよびOpenShiftを監視するシステム・アドミニストレータのためのものです。従って、本章の読者は以下のような概念に精通していることを前提にしています。

- Docker、Kubenetes、PodmanおよびOpenShiftによるコンテナ運用
- Senju DevOperation Conductorの各種コンポーネント（千手ブラウザ、千手マネージャ、千手エージェント）
- Senju DevOperation Conductorのモニタリング機能
- オペレーティング・システムについての知識

4.1.3. 前提条件と関連資料

本章を参照するにあたっては、以下の各マニュアルなどを参照して下さい。

- 統合運用管理ツール「Senju DevOperation Conductor」リリースノート
- 統合運用管理ツール「Senju DevOperation Conductor」ユーザーズガイド
- Docker Documentation (https://docs.docker.com/)
- Kubernetes Documentaion (https://kubernetes.io/docs/home/)
- Podman Documentation (https://docs.podman.io/en/latest/)
- OpenShift Documentation (https://docs.openshift.com/)

4.2. コンテナ監視(Docker/Kubernetes/Podman/OpenShift)の概要

コンテナ監視(Docker/Kubernetes/Podman/OpenShift)機能では、Docker、Kubernetes、PodmanおよびOpenShiftと連携し、コンテナ運用基盤を監視するために、以下の機能を提供します。

- Dockerの各種メトリクス取得
- Kubernetesの各種メトリクス取得

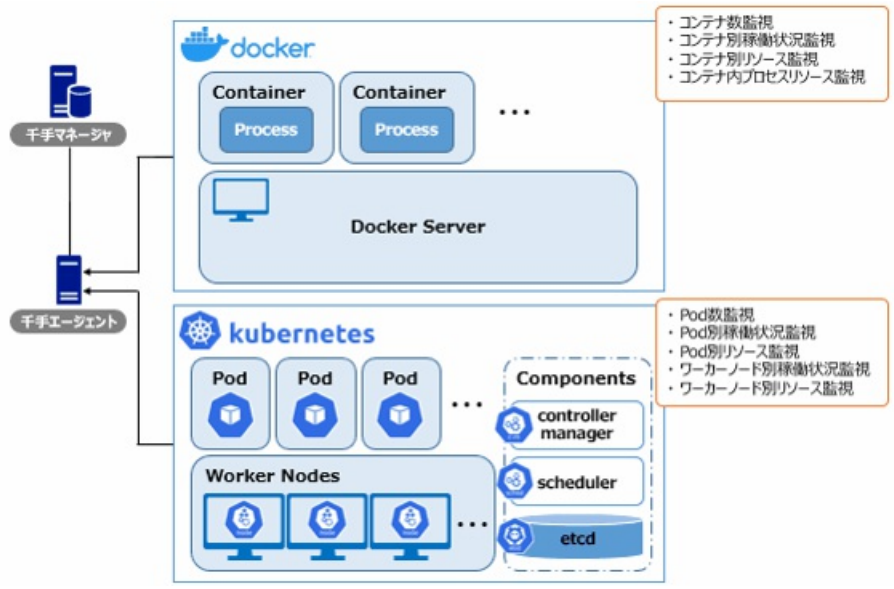


図 4.1 Senju DevOperation Conductorと Docker/Kubernetes との連携

- Podmanの各種メトリクス取得
- OpenShiftの各種メトリクス取得

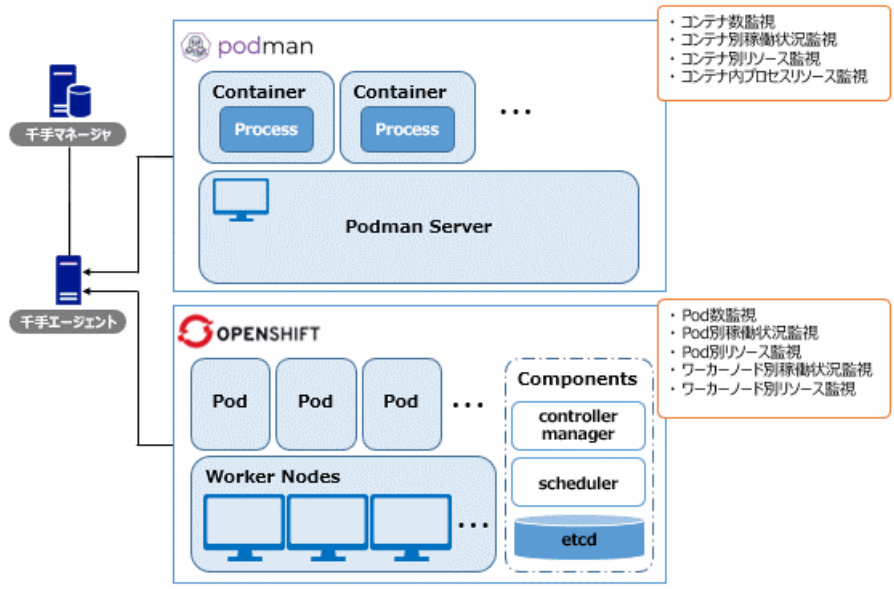


図 4.2 Senju DevOperation Conductorと Podman/OpenShift との連携

各種メトリクス取得機能では、Senju DevOperation Conductorモニタリング機能を使用して、Docker/Kubernetes/Podman/OpenShiftに対して定期的にデータ取得を行い、しきい値監視することが出来ます。（モニタリング機能については、**ユーザーズガイド「4．モニタリング」**を参照して下さい。）

以下の2パターンによる監視構成を取ることができます。

- 千手エージェント機能によるコンテナ監視

- 千手センサー機能によるコンテナ監視

4.2.1. Docker監視機能の概要

Dockerから情報取得する際には、**dockerコマンド** を実行して取得を行います。そのため、千手エージェントまたは千手センサー上で docker コマンドを実行可能にする必要があります。また、千手センサーの場合は、プローブノードに対してSSHでの接続ができる必要があります。

取得可能な項目については、Docker 監視項目一覧 を参照してください。

4.2.2. Kubernetes監視機能の概要

Kubernetesから情報を取得する際には、**kubectlコマンド** を実行して取得を行います。そのため、千手エージェントまたは千手センサー上で kubectl コマンドを実行可能にする必要があります。また、千手センサーの場合は、プローブノードに対してSSHでの接続ができる必要があります。

取得可能な項目については、Kubernetes 監視項目一覧 を参照してください。

4.2.3. Podman監視機能の概要

Podmanから情報取得する際には、**podmanコマンド** を実行して取得を行います。そのため、千手エージェントまたは千手センサー上で podman コマンドを実行可能にする必要があります。また、千手センサーの場合は、プローブノードからSSHでの接続ができる必要があります。

取得可能な項目については、Podman 監視項目一覧 を参照してください。

4.2.4. OpenShift監視機能の概要

OpenShiftから情報を取得する際には、**ocコマンド** を実行して取得を行います。そのため、千手エージェントまたは千手センサー上で oc コマンドを実行可能にする必要があります。また、千手センサーの場合は、プローブノードに対してSSHでの接続ができる必要があります。

取得可能な項目については、OpenShift 監視項目一覧 を参照してください。

4.3. コンテナ監視(Docker/Kubernetes/Podman/OpenShift)監視設定手順

Docker/Kubernetes/Podman/OpenShift監視設定を行う際には、以下の設定が必要になります。

- ライセンスの購入とライセンスキーの入手
    - Docker監視
    - Kubernetes監視
    - Podman監視
    - OpenShift監視

注釈

監視対象コンテナ/Pod数に応じて内容が異なります。

- Senju DevOperation Conductor Extension Packの入手と適用

  運用管理サーバーおよび、コンテナ監視を行う管理対象ノードに、同一バージョンの Senju DevOperation Conductor Extension Pack の適用が必要です。
    - 運用管理サーバー(千手マネージャ)への適用(監視項目の更新)
    - 管理対象ノード(千手エージェント(プローブノード))への適用(情報取得コマンドの更新)

警告

適用可能な Senju DevOperation Conductor のバージョンやパッチ状況に制限がある場合があります。詳しくは、Senju DevOperation Conductor Extension Pack の README をご参照下さい。

参考

Senju DevOperation Conductor Extension Packの適用手順につきましては、Senju DevOperation Conductor Extension Pack の README をご参照ください。

注釈

Senju DevOperation Conductor Extension Packの適用に際しては、千手システムの停止は不要ですが、関連する監視タスクの停止が必要です。

4.3.1. Kubernetes監視の設定ファイル

4.3.1.1. Kubernetesユーザー設定ファイルの作成

Kubernetesユーザー設定ファイルは、監視項目のパラメータ「設定ファイル」に指定するファイルです。

Kubernetesユーザー設定ファイル(xxx.json)のパスおよびファイル名は任意に指定することが可能です。

dat/opt/sj_k8s_user.json.sample をコピーしてKubernetesユーザー設定ファイル(xxx.json)を作成し、以下の項目を設定して下さい。

表 4.1 Kubernetesユーザー設定ファイルの記述内容

項目	省略	デフォルト	暗号化対象	説明
CMD_PATH	可	kubectl	×	監視で利用するkubectlコマンドの絶対パスを指定します。
OUTPUT_FORMAT	可	LTSV	×	取得ログの出力フォーマットです。LTSVまたはJSONが指定可能です。以下の監視項目で • Kubernetes:イベント監視 • Kubernetes:コンテナログ監視

- Kubernetesユーザー設定ファイル(xxx.json)とKubernetesの監視タスクのパラメータの両方で指定可能な項目については、Kubernetesの監視タスクのパラメータで指定した値が有効になります。

4.3.1.2. Kubernetesシステム設定ファイル(sj_k8s_sys.json)の作成

Kubernetesシステム設定ファイル(sj_k8s_sys.json)は、Kubernetesの全監視項目で共通の設定ファイルです。

dat/opt/sj_k8s_sys.json.sample をコピーしてKubernetesシステム設定ファイル(dat/opt/sj_k8s_sys.json)を作成し、以下の項目を設定して下さい。

表 4.2 Kubernetesシステム設定ファイル(sj_k8s_sys.json)の記述内容

項目	省略	デフォルト	暗号化対象	説明
MON_CACHE_INTERVAL	可	60	×	キャッシュ有効期間(秒)
ROTATE_COUNT	可	7	×	出力するログファイルの世代数。以下の監視項目で有効となります。 • Kubernetes：イベント監視 • Kubernetes：コンテナログ監視
ROTATE_SIZE	可	10485760	×	出力するログファイルの最大サイズ(Byte)。以下の監視項目で有効となりま • Kubernetes：イベント監視 • Kubernetes：コンテナログ監視
CMD_RETRY_INTERVAL	可	1	×	情報取得コマンド実行のリトライ間隔(秒)。以下の監視項目で有効となりま • Kubernetes：コンテナログ監視
CMD_RETRY_LIMIT	可	5	×	情報取得コマンド実行のリトライ回数。以下の監視項目で有効となります。 • Kubernetes：コンテナログ監視
CMD_PATH	可	kubectl	×	監視で利用するkubectlコマンドの絶対パスを指定します。
LOG_BUFFER_TIME	可	5	×	前回取得した最後のログより遡る時間(分)。以下の監視項目で有効となり • Kubernetes：イベント監視 • Kubernetes：コンテナログ監視
OUTPUT_FORMAT	可	LTSV	×	取得ログの出力フォーマットです。LTSVまたはJSONが指定可能です。以 • Kubernetes：イベント監視 • Kubernetes：コンテナログ監視
RESOURCE_METRICS_PREFIX	可	container	×	Podのリソース状況取得メトリクスのプレフィックス（{container|pod}）。以下 • Kubernetes：Pod別CPU使用率(%) • Kubernetes：Pod別CPUミリコア使用量(millicores) • Kubernetes：Pod別メモリ使用量(KB) • Kubernetes：Pod別メモリ使用量(MB) • Kubernetes：デプロイメント別CPU使用率(%) • Kubernetes：レプリカセット別CPU使用率(%) • Kubernetes：デーモンセット別CPU使用率(%)

- Kubernetesシステム設定ファイル(sj_k8s_sys.json)とKubernetesの監視タスクのパラメータの両方で指定可能な項目については、Kubernetesの監視タスクのパラメータで指定した値が有効になります。
- Kubernetesシステム設定ファイル(sj_k8s_sys.json)とKubernetesユーザー設定ファイルの両方で指定可能な項目については、ユーザー設定ファイルで指定した値が有効になります。
- 一回以上ログを取得している状態でLOG_BUFFER_TIMEを現在よりも大きい値に変更した場合、変更後の1回目の実行で過去に取得したログを重複して取得する場合があります。ご注意ください。

- Kubernetesシステム設定ファイル(sj_k8s_sys.json) の記載例

```
{
        "MON_CACHE_INTERVAL": "60",
        "ROTATE_COUNT": "7",
        "ROTATE_SIZE": "10485760",
        "CMD_RETRY_INTERVAL": "1",
        "CMD_RETRY_LIMIT": "5",
        "LOG_BUFFER_TIME": "5",
        "OUTPUT_FORMAT": "LTSV",
        "RESOURCE_METRICS_PREFIX": "container",
        "CMD_PATH": "kubectl"
}
```

注釈

デフォルトの設定値を変更する必要がない場合は、Kubernetesシステム設定ファイル(sj_k8s_sys.json)を作成する必要はありません。

4.3.2. OpenShift監視の認証設定

4.3.2.1. oc loginコマンドの初回実行

千手環境でOpenShift監視コマンドを実行するためには~/.kube/configファイルが必要です。~/.kube/configファイルを作成するには、oc loginコマンドを実行してください。マネージドサービスを利用している場合は、その仕様に従ってAPIキー等を指定して下さい。

- 実行コマンド

```
% oc login -u ユーザ -p パスワード --server サーバー
```

表 4.3 oc loginコマンドオプションの設定内容

オプション	説明
ユーザ	ocログイン用のユーザを指定します。
パスワード	ocログイン用のパスワードを指定します。
サーバー	OpenShift Container Platform サーバー URLを指定します。

- oc loginコマンドの記載例

```
oc login -u apikey -p I7XXIqavfFXQ28yV3DEF19KPeJv6WWE6qWrBL4DWEUjb --server https://c100-
e.jp-tok.containers.cloud.ibm.com:xxxxx
```

4.3.3. OpenShift監視の設定ファイル

4.3.3.1. OpenShiftユーザー設定ファイルの作成

OpenShiftユーザー設定ファイルは、監視項目のパラメータ「設定ファイル」に指定するファイルです。

OpenShiftユーザー設定ファイル(xxx.json)のパスおよびファイル名は任意に指定することが可能です。

後述のOpenShift情報設定ファイル更新コマンド(sj_setup_ops ー OpenShift情報設定ファイル更新 ー)を利用してOpenShiftユーザー設定ファイルを作成し、以下の項目を設定して下さい。

表 4.4 OpenShiftユーザー設定ファイルの記述内容

項目	省略	デフォルト	暗号化対象	説明
OC_USER	可	-	×	ocログイン用のユーザを指定します。
OC_PASSWORD	可	-	○	ocログイン用のパスワードを指定します。
CMD_PATH	可	oc	×	監視で利用するocコマンドの絶対パスを指定します。
OUTPUT_FORMAT	可	LTSV	×	取得ログの出力フォーマットです。LTSVまたはJSONが指定可能です。以下の監視項目で • OpenShift：イベント監視 • OpenShift：コンテナログ監視

- OpenShiftユーザー設定ファイルとOpenShiftの監視タスクのパラメータの両方で指定可能な項目については、OpenShiftの監視タスクのパラメータで指定した値が有効になります。

4.3.3.2. OpenShiftシステム設定ファイル(sj_ops_sys.json)の作成

OpenShiftシステム設定ファイル(sj_ops_sys.json)は、OpenShiftの全監視項目で共通の設定ファイルです。

後述のOpenShift情報設定ファイル更新コマンド(sj_setup_ops － OpenShift情報設定ファイル更新 －)を利用してOpenShiftシステム設定ファイル(dat/opt/sj_ops_sys.json)を作成し、以下の項目を設定して下さい。

表 4.5 OpenShiftシステム設定ファイル(sj_ops_sys.json)の記述内容

項目	省略	デフォルト	暗号化対象	説明
OC_USER	可	-	×	ocログイン用のユーザーを指定します。
OC_PASSWORD	可	-	○	ocログイン用のパスワードを指定します。
CMD_PATH	可	oc	×	監視で利用するocコマンドの絶対パスを指定します。
OUTPUT_FORMAT	可	LTSV	×	取得ログの出力フォーマットです。LTSVまたはJSONが指定可能です。以 • OpenShift：イベント監視 • OpenShift：コンテナログ監視
MON_CACHE_INTERVAL	可	60	×	キャッシュ有効期間(秒)
ROTATE_COUNT	可	7	×	出力するログファイルの世代数。以下の監視項目で有効となります。 • OpenShift：イベント監視 • OpenShift：コンテナログ監視
ROTATE_SIZE	可	10485760	×	出力するログファイルの最大サイズ(Byte)。以下の監視項目で有効となりま • OpenShift：イベント監視 • OpenShift：コンテナログ監視
CMD_RETRY_INTERVAL	可	1	×	情報取得コマンド実行のリトライ間隔(秒)。以下の監視項目で有効となりま • OpenShift：コンテナログ監視
CMD_RETRY_LIMIT	可	5	×	情報取得コマンド実行のリトライ回数。以下の監視項目で有効となります。 • OpenShift：コンテナログ監視
LOG_BUFFER_TIME	可	5	×	前回取得した最後のログより遡る時間(分)。以下の監視項目で有効となり • OpenShift：イベント監視 • OpenShift：コンテナログ監視
RESOURCE_METRICS_PREFIX	可	container	×	Podのリソース状況取得メトリクスのプレフィックス（{container|pod}）。以下 • OpenShift：Pod別CPU使用率(%) • OpenShift：Pod別CPUミリコア使用量(millicores) • OpenShift：Pod別メモリ使用量(KB) • OpenShift：Pod別メモリ使用量(MB) • OpenShift：デプロイメント別CPU使用率(%) • OpenShift：レプリカセット別CPU使用率(%) • OpenShift：デーモンセット別CPU使用率(%)

- OpenShiftシステム設定ファイル(sj_ops_sys.json)とOpenShiftの監視タスクのパラメータの両方で指定可能な項目については、OpenShiftの監視タスクのパラメータで指定した値が有効になります。
- OpenShiftシステム設定ファイル(sj_ops_sys.json)とOpenShiftユーザー設定ファイルの両方で指定可能な項目については、OpenShiftユーザー設定ファイルで指定した値が有効になります。
- 一回以上ログを取得している状態でLOG_BUFFER_TIMEを現在よりも大きい値に変更した場合、変更後の1回目の実行で過去に取得したログを重複して取得する場合があります。ご注意ください。

- OpenShiftシステム設定ファイル(sj_ops_sys.json) の記載例

```
{
        "CMD_PATH": "oc",
        "CMD_RETRY_INTERVAL": "",
        "CMD_RETRY_LIMIT": "",
        "LOG_BUFFER_TIME": "",
        "MON_CACHE_INTERVAL": "100",
        "OC_PASSWORD":
"=Ad28Ls5cRv45dSNWSTz45GFzdYxqKdFNo8A5dWzu3HdXzjvd5Ljj+W9waYdNj93dwA==",
        "OC_USER": "apikey",
        "OUTPUT_FORMAT": "json",
        "RESOURCE_METRICS_PREFIX": "",
        "ROTATE_COUNT": "",
        "ROTATE_SIZE": ""
}
```

注釈

OC_USER・OC_PASSWORDは、必ずOpenShiftシステム設定ファイル(sj_ops_sys.json)またはOpenShiftユーザー設定ファイルのいずれかで指定する必要があります。

4.3.3.3. sj_setup_ops ー OpenShift情報設定ファイル更新 ー

- 指定形式
    - [参照]

      ```
      sj_setup_ops
      ```

    - [作成＆更新]

      ```
      sj_setup_ops
        [-ci[Cache expiration interval]]
        [-mlc[Maximum count of output OpenShift log]]
        [-mls[Maximum size(B) of output OpenShift log]]
        [-ri[Retry interval(seconds) for executing command]]
        [-rc[Retry count for executing command]]
        [-lbt[BufferTime of log file output by log monitoring]]
        [-lf[Format of log file output by log monitoring]]
        [-mp[Metrics prefix for getting resource information]]
        [-cp[OpenShift command(oc) path]]
        [-ocuser[oc login user]]
        [-ocpswd[oc login password]]
        [-cf[Configuration file]]
      ```

- 目的

  OpenShiftユーザー設定ファイル・OpenShiftシステム設定ファイルの現在値の参照、作成と更新を行います。

- オプション
    - -cf

      現在値の参照、作成と更新を行う任意のOpenShiftユーザー設定ファイルを絶対パスで指定して下さい。
      値を省略した場合はOpenShiftシステム設定ファイルの参照、作成と更新を行います。

    - -ci

      キャッシュの有効期間(MON_CACHE_INTERVAL)に設定する値を指定して下さい。単位は秒です。
      値を省略するとOpenShiftシステム設定ファイルに設定されている値を削除します。
      OpenShiftシステム設定ファイルの操作時のみ有効です。

    - -mlc

      ログ監視によって出力されるログファイルのローテーション最大個数(ROTATE_COUNT)に設定する値を指定して下さい。
      値を省略するとOpenShiftシステム設定ファイルに設定されている値を削除します。
      OpenShiftシステム設定ファイルの操作時のみ有効です。

    - -mls

ログ監視によって出力されるログファイルの最大サイズ(ROTATE_SIZE)に設定する値を指定して下さい。
値を省略するとOpenShiftシステム設定ファイルに設定されている値を削除します。
OpenShiftシステム設定ファイルの操作時のみ有効です。

- -ri

  情報取得コマンド実行のリトライ間隔(CMD_RETRY_INTERVAL)に設定する値を指定して下さい。単位は秒です。
  値を省略するとOpenShiftシステム設定ファイルに設定されている値を削除します。
  OpenShiftシステム設定ファイルの操作時のみ有効です。

- -rc

  情報取得コマンド実行のリトライ回数(CMD_RETRY_LIMIT)に設定する値を指定して下さい。
  値を省略するとOpenShiftシステム設定ファイルに設定されている値を削除します。
  OpenShiftシステム設定ファイルの操作時のみ有効です。

- -lbt

  最後に取得したログより遡る時間(LOG_BUFFER_TIME)に設定する値を指定して下さい。
  値を省略するとOpenShiftシステム設定ファイルに設定されている値を削除します。
  OpenShiftシステム設定ファイルの操作時のみ有効です。

- -lf

  ログ監視によって出力されるログフォーマット(OUTPUT_FORMAT)に設定する値を指定して下さい。
  値を省略するとOpenShiftシステム/ユーザー設定ファイルに設定されている値を削除します。

- -mp

  Podのリソース状況取得メトリクスのプレフィックス(RESOURCE_METRICS_PREFIX)に設定する値を指定して下さい。
  値を省略するとOpenShiftシステム設定ファイルに設定されている値を削除します。
  OpenShiftシステム設定ファイルの操作時のみ有効です。

- -cp

  ocコマンドの格納パス(CMD_PATH)に設定する値を指定して下さい。
  値を省略するとOpenShiftシステム/ユーザー設定ファイルに設定されている値を削除します。

- -ocuser

  ocログイン用のユーザー(OC_USER)に設定する値を指定して下さい。
  値を省略するとOpenShiftシステム/ユーザー設定ファイルに設定されている値を削除します。

- -ocpswd

  ocログイン用のパスワード(OC_PASSWORD)に設定する値を指定して下さい。
  値を省略するとOpenShiftシステム/ユーザー設定ファイルに設定されている値を削除します。

- 実行結果

  - (例1.1)現在の設定値参照(OpenShiftシステム設定ファイル)

```
% sj_setup_ops
{
        "CMD_PATH": "",
        "CMD_RETRY_INTERVAL": "100",
        "CMD_RETRY_LIMIT": "",
        "LOG_BUFFER_TIME": "",
        "MON_CACHE_INTERVAL": "",
        "OC_PASSWORD": "**********",
        "OC_USER": "apikey",
        "OUTPUT_FORMAT": "json",
        "RESOURCE_METRICS_PREFIX": "",
        "ROTATE_COUNT": "",
        "ROTATE_SIZE": ""
}
```

  - (例1.2)現在の設定値参照(OpenShiftユーザー設定ファイル)

```
% sj_setup_ops -cf/home/senju/dat/opt/sj_ops_user.json
{
        "CMD_PATH": "/usr/local/bin/oc",
        "OC_PASSWORD": "**********",
        "OC_USER": "apikey",
        "OUTPUT_FORMAT": ""
}
```

- (例2)OC_USERとOC_PASSWORDを設定

```
% sj_setup_ops -ocuserXXXX-XXXX -ocpswd
Please enter the value.
        "OC_PASSWORD":

The value of OC_USER has changed from (ABCD) to (XXXX-XXXX).
The value of OC_PASSWORD has changed from (**********) to (**********).
The update is complete.
% sj_setup_ops
{
        "CMD_PATH": "",
        "CMD_RETRY_INTERVAL": "",
        "CMD_RETRY_LIMIT": "",
        "LOG_BUFFER_TIME": "",
        "MON_CACHE_INTERVAL": "",
        "OC_PASSWORD": "**********",
        "OC_USER": "XXXX-XXXX",
        "OUTPUT_FORMAT": "",
        "RESOURCE_METRICS_PREFIX": "",
        "ROTATE_COUNT": "",
        "ROTATE_SIZE": ""
}
```

- (例3)設定を削除

```
% sj_setup_ops -ocuser -ocpswd
Please enter the value.
        "OC_PASSWORD":

The value of OC_USER has changed from (XXXX-XXXX) to ().
The value of OC_PASSWORD has changed from (**********) to (**********).
The update is complete.
% sj_setup_ops
{
        "CMD_PATH": "",
        "CMD_RETRY_INTERVAL": "",
        "CMD_RETRY_LIMIT": "",
        "LOG_BUFFER_TIME": "",
        "MON_CACHE_INTERVAL": "",
        "OC_PASSWORD": "**********",
        "OC_USER": "",
        "OUTPUT_FORMAT": "",
        "RESOURCE_METRICS_PREFIX": "",
        "ROTATE_COUNT": "",
        "ROTATE_SIZE": ""
}
```

注釈

- 暗号化対象項目の標準出力への表示は全てアスタリスクでマスクされます。
- 暗号化対象項目の値の設定は、キーボードからの入力が一切表示されません。コピー＆ペーストで入力することをお勧めします。
- 暗号化対象項目の値を削除する場合、何も入力せずにリターンキーを押下して下さい。

- 標準エラー出力
  - Failed to acquire Senju home directory
  - The openshift configuration file does not exist.
  - Invalid data have been set in this file.
  - Failed to update the openshift configuration file.
  - File update failed.
- 終了ステータス
  - 0 : 正常終了
  - 1 : 異常終了

4.3.3.4. OpenShift情報設定ファイル更新コマンドの登録

OpenShift情報設定ファイルの現在値の参照、作成と更新を行うため、OpenShift情報設定ファイル更新コマンドを千手ブラウザからユーザーコマンドに登録します。詳細な手順については、ユーザーズガイド**「2.3.2.1 ユーザーコマンド」**を参照して下さい。

- ユーザーコマンドグループの作成

  OpenShift情報設定ファイル更新コマンドを登録するユーザーコマンドグループを千手ブラウザから登録して下さい。

- OpenShift情報設定ファイル更新コマンドの登録(OpenShiftシステム設定ファイル)

  作成したユーザーコマンドグループに、以下に示す起動シーケンスを指定してコマンドを登録して下さい。

  - 現在値の参照

```
sj_remshe "@ノード名@" -l "@ユーザ名@" sj_setup_ops
```

  - 作成と更新

```
sj_remshe "@ノード名@" -l "@ユーザ名@" sj_setup_ops "-ci@@キャッシュ有効期間@@" "-mlc@@ログファイルのローテーション最大個数@@" "-mls@@ログファイルの最大サイズ@@" "-ri@@コマンドのリトライ間隔@@" "-rc@@コマンドのリトライ上限@@" "-lbt@@最後に取得したログより遡る時間@@" "-lf@@ログフォーマット@@" "-mp@@Podのリソース状況取得メトリクスのプレフィックス@@" "-cp@@ocコマンドパス@@" "-ocuser@@ocログイン用のユーザ@@" "-ocpswd@@ocログイン用のパスワード@@"
```

注釈

上記の起動シーケンスは項目を全て変更する仕様となっています。項目別に変更を行いたい場合は、起動シーケンスから任意の「**-オプション@@パラメータ名@@**」を指定したユーザーコマンドを別途登録して下さい。

（例）sj_remshe "@ノード名@" -l "@ユーザ名@" sj_setup_ops "-ocuser@@ocログイン用のユーザ@@"

- OpenShift情報設定ファイル更新コマンドの登録(OpenShiftユーザー設定ファイル)

  作成したユーザーコマンドグループに、以下に示す起動シーケンスを指定してコマンドを登録して下さい。

  - 現在値の参照

```
sj_remshe "@ノード名@" -l "@ユーザ名@" sj_setup_ops "-cf@ユーザ設定ファイル@"
```

  - 作成と更新

```
sj_remshe "@ノード名@" -l "@ユーザ名@" sj_setup_ops "-cf@ユーザ設定ファイル@" "-lf@@ログフォーマット@@" "-cp@@ocコマンドパス@@" "-ocuser@@ocログイン用のユーザ@@" "-ocpswd@@ocログイン用のパスワード@@"
```

注釈

上記の起動シーケンスは変更可能な項目を全て変更する仕様となっています。項目別に変更を行いたい場合は、起動シーケンスから任意の「**-オプション@@パラメータ名@@**」を指定したユーザーコマンドを別途登録して下さい。

（例）sj_remshe "@ノード名@" -l "@ユーザ名@" sj_setup_ops "-cf@ユーザ設定ファイル@" "-ocuser@@ocログイン用のユーザ@@"

4.4. コンテナ監視(Docker/Kubernetes/Podman/OpenShift)の使い方

4.4.1. Dockerメトリクス監視機能

dockerコマンド経由で情報を取得し、Senju DevOperation Conductorのモニタリング機能を使って、監視することができます。

監視定義を千手ブラウザより登録し、監視を実施します。監視結果は、各種モニタ画面（グローバルノードモニタ／ノードモニタ）にてその監視状況を表示できます。予め設定したしきい値により障害を検知した場合は、メッセージモニタにメッセージが通知されます。（モニタリング機能については、ユーザーズガイド「 **4．モニタリング** 」を参照して下さい。）

4.4.2. Dockerコンテナログ監視機能

監視項目「Docker：コンテナログ監視」では Docker から取得したログをログファイルに蓄積します。このログファイルを監視することでDockerのコンテナログを検知することが可能です。

4.4.2.1. ログファイル

監視項目「Docker：コンテナログ監視」で取得したログファイルは次のファイルに出力されます。
ただし、ファイル名に使用できない記号と「=」(イコール)、「,」(カンマ)は「-」(半角ハイフン)に置き換えます。

- ログフォーマットがLTSVの場合：

表 4.6 ログファイル名(LTSV)

項目	内容
ログディレクトリ名	`~/log/container.d/`
ログファイル名(通常)	`~/log/container.d/dkr_container_{nodeid}_{containername}.log`
ログファイル名(センサー)	`~/log/container.d/dkr_container_{user}@{nodeid}_{containername}.log`

- ログフォーマットがJSONの場合：

表 4.7 ログファイル名(JSON)

項目	内容
ログディレクトリ名	`~/log/container.d/`
ログファイル名(通常)	`~/log/container.d/dkr_container_{nodeid}_{containername}.json`
ログファイル名(センサー)	`~/log/container.d/dkr_container_{user}@{nodeid}_{containername}.json`

4.4.2.2. ログフォーマット

以下にDockerコンテナログ監視で取得したログファイルのレコード形式について説明します。デフォルトのレコードフォーマットは LTSV形式で、項目間はタブ区切りとなります。

【Dockerコンテナログファイル　レコード形式】

- ログフォーマットがLTSVの場合：

最新のタイムスタンプ　コンテナ名　メッセージ

表 4.8 コンテナログ監視レコード形式(LTSV)

No.	項目	キー:	説明
1	タイムスタンプ	TimeStamp:	取得したコンテナログが記録された時刻。フォーマット: YYYY-MM-DDThh:mm:ddZ(例: 2020-03-13T07:0
2	コンテナ名	Container:	取得したコンテナ名
4	メッセージ	Message:	取得したコンテナログのメッセージ

- ログフォーマットがJSONの場合：

イベント内容

表 4.9 コンテナログ監視レコード形式(JSON)

No.	項目	説明
1	コンテナログ内容	取得したコンテナログの内容が入ります。コンテナログの内容はJSONの形式で出力されます。

4.4.3. Kubernetesメトリクス監視機能

kubectlコマンド経由で情報を取得し、Senju DevOperation Conductorのモニタリング機能を使って、監視することができます。

監視定義を千手ブラウザより登録し、監視を実施します。監視結果は、各種モニタ画面（グローバルノードモニタ／ノードモニタ）にてその監視状況を表示できます。予め設定したしきい値により障害を検知した場合は、メッセージモニタにメッセージが通知されます。（モニタリング機能については、ユーザーズガイド「 **4．モニタリング** 」を参照して下さい。）

4.4.4. Kubernetesイベント監視機能

監視項目「Kubernetes：イベント監視」では Kubernetes から取得したログをログファイルに蓄積します。このログファイルを監視することでKubernetesのイベントを検知することが可能です。

4.4.4.1. ログファイル

監視項目「Kubernetes：イベント監視」で取得したログファイルは次のファイルに出力されます。ただし、ファイル名に使用できない記号は「-」(半角ハイフン)に置き換えます。

- ログフォーマットがLTSVの場合：

表 4.10 ログファイル名(LTSV)

項目	内容
ログディレクトリ名	`~/log/container.d/`
ログファイル名(通常)	`~/log/container.d/k8s_events_{nodeid}_default.log`
ログファイル名(通常+ネームスペース指定)	`~/log/container.d/k8s_events_{nodeid}_default_{namespace}.log`
ログファイル名(通常+コンテキスト指定)	`~/log/container.d/k8s_events_{nodeid}_{context}.log`
ログファイル名(通常+コンテキスト+ネームスペース指定)	`~/log/container.d/k8s_events_{nodeid}_{context}_{namespace}.lo`
ログファイル名(センサー)	`~/log/container.d/k8s_events_{user}@{nodeid}_default.log`
ログファイル名(センサー+ネームスペース指定)	`~/log/container.d/k8s_events_{user}@{nodeid}_default_{namespac`
ログファイル名(センサー+コンテキスト指定)	`~/log/container.d/k8s_events_{user}@{nodeid}_{context}.log`
ログファイル名(センサー+コンテキスト+ネームスペース指定)	`~/log/container.d/k8s_events_{user}@{nodeid}_{context}_{namesp`

- ログフォーマットがJSONの場合：

表 4.11 ログファイル名(JSON)

項目	内容
ログディレクトリ名	`~/log/container.d/`
ログファイル名(通常)	`~/log/container.d/k8s_events_{nodeid}_default.json`
ログファイル名(通常+ネームスペース指定)	`~/log/container.d/k8s_events_{nodeid}_default_{namespace}.json`
ログファイル名(通常+コンテキスト指定)	`~/log/container.d/k8s_events_{nodeid}_{context}.json`
ログファイル名(通常+コンテキスト+ネームスペース指定)	`~/log/container.d/k8s_events_{nodeid}_{context}_{namespace}.js`
ログファイル名(センサー)	`~/log/container.d/k8s_events_{user}@{nodeid}_default.json`
ログファイル名(センサー+ネームスペース指定)	`~/log/container.d/k8s_events_{user}@{nodeid}_default_{namespac`
ログファイル名(センサー+コンテキスト指定)	`~/log/container.d/k8s_events_{user}@{nodeid}_{context}.json`
ログファイル名(センサー+コンテキスト+ネームスペース指定)	`~/log/container.d/k8s_events_{user}@{nodeid}_{context}_{namesp`

4.4.4.2. ログフォーマット

以下にKubernetesイベント監視で取得したログファイルのレコード形式について説明します。デフォルトのレコードフォーマットは LTSV形式で、項目間はタブ区切りとなります。

【Kubernetesイベントログファイル　レコード形式】

- ログフォーマットがLTSVの場合：

最新のタイムスタンプ　ノードID　名前空間　タイプ（通常、警告）　理由　オブジェクト　サブオブジェクト　発生環境　メッセージ　最初のタイムスタンプ　回数　名前

表 4.12 イベント監視レコード形式(LTSV)

No.	項目	キー：	説明
1	最新のタイムスタンプ	LastTimeStamp:	取得したイベントが記録された最新時刻。存在しない場合は、FirstTimeStampの値を利用しま フォーマット：YYYY-MM-DDThh:mm:ddZ(例：2020-03-13T07:09:06Z)
2	ノードID	NodeId:	ノードID名
3	名前空間	Namespace:	名前空間
4	タイプ(通常、警告)	Type:	イベントタイプ(Normal/Warning)
5	理由	Reason:	イベントオブジェクトのステータス理由。
6	オブジェクト	Object:	イベントに関連するオブジェクト
7	サブオブジェクト	SubObject:	イベントに関連するサブオブジェクト
8	発生環境	Source:	取得したイベントの発生環境
9	メッセージ	Message:	取得したイベントのメッセージ
10	最初のタイムスタンプ	FirstTimeStamp:	取得したイベントが最初に記録された時刻。存在しない場合は、eventTimeの値を利用します。 フォーマット：YYYY-MM-DDThh:mm:ddZ(例：2020-03-13T07:09:06Z)
11	回数	Count:	取得イベントの発生回数
12	名前	Name:	取得したPod名

- ログフォーマットがJSONの場合：

イベント内容

表 4.13 イベント監視レコード形式(JSON)

No.	項目	説明
1	イベント内容	取得したイベント内容が入ります。イベント内容はJSONの形式で出力されます。

4.4.5. Kubernetesコンテナログ監視機能

監視項目「Kubernetes：コンテナログ監視」では Kubernetes から取得したログをログファイルに蓄積します。このログファイルを監視することでKubernetesのコンテナログを検知することが可能です。

4.4.5.1. ログファイル

監視項目「Kubernetes：コンテナログ監視」で取得したログファイルは次のファイルに出力されます。
ただし、ファイル名に使用できない記号と「=」(イコール)、「,」(カンマ)は「-」(半角ハイフン)に置き換えます。

- ログフォーマットがLTSVの場合：

表 4.14 ログファイル名(LTSV)

項目	内容
ログディレクトリ名	~/log/container.d/
ログファイル名(通常)	~/log/container.d/k8s_container_{nodeid}_{selector}_default.lo
ログファイル名(通常+ネームスペース指定)	~/log/container.d/k8s_container_{nodeid}_{selector}_default_{n
ログファイル名(通常+コンテキスト指定)	~/log/container.d/k8s_container_{nodeid}_{selector}_{context}.
ログファイル名(通常+コンテキスト+ネームスペース指定)	~/log/container.d/k8s_container_{nodeid}_{selector}_{context}_
ログファイル名(センサー)	~/log/container.d/k8s_container_{user}@{nodeid}_{selector}_def
ログファイル名(センサー+ネームスペース指定)	~/log/container.d/k8s_container_{user}@{nodeid}_{selector}_def
ログファイル名(センサー+コンテキスト指定)	~/log/container.d/k8s_container_{user}@{nodeid}_{selector}_{co
ログファイル名(センサー+コンテキスト+ネームスペース指定)	~/log/container.d/k8s_container_{user}@{nodeid}_{selector}_{co

- ログフォーマットがJSONの場合:

表 4.15 ログファイル名(JSON)

項目	内容
ログディレクトリ名	~/log/container.d/
ログファイル名(通常)	~/log/container.d/k8s_container_{nodeid}_{selector}_default.js
ログファイル名(通常+ネームスペース指定)	~/log/container.d/k8s_container_{nodeid}_{selector}_default_{n
ログファイル名(通常+コンテキスト指定)	~/log/container.d/k8s_container_{nodeid}_{selector}_{context}.
ログファイル名(通常+コンテキスト+ネームスペース指定)	~/log/container.d/k8s_container_{nodeid}_{selector}_{context}_
ログファイル名(センサー)	~/log/container.d/k8s_container_{user}@{nodeid}_{selector}_def
ログファイル名(センサー+ネームスペース指定)	~/log/container.d/k8s_container_{user}@{nodeid}_{selector}_def
ログファイル名(センサー+コンテキスト指定)	~/log/container.d/k8s_container_{user}@{nodeid}_{selector}_{co
ログファイル名(センサー+コンテキスト+ネームスペース指定)	~/log/container.d/k8s_container_{user}@{nodeid}_{selector}_{co

4.4.5.2. ログフォーマット

以下にKubernetesコンテナログ監視で取得したログファイルのレコード形式について説明します。デフォルトのレコードフォーマットは LTSV形式で、項目間はタブ区切りとなります。

【Kubernetesコンテナログファイル　レコード形式】

- ログフォーマットがLTSVの場合:

最新のタイムスタンプ　Pod名　コンテナ名　メッセージ

表 4.16 コンテナログ監視レコード形式(LTSV)

No.	項目	キー:	説明
1	タイムスタンプ	TimeStamp:	取得したコンテナログが記録された時刻。フォーマット: YYYY-MM-DDThh:mm:ddZ(例: 2020-03-13T07:0
2	Pod名	Pod:	取得したPod名
3	コンテナ名	Container:	取得したコンテナ名
4	メッセージ	Message:	取得したコンテナログのメッセージ

- ログフォーマットがJSONの場合:

イベント内容

表 4.17 コンテナログ監視レコード形式(JSON)

No.	項目	説明
1	コンテナログ内容	取得したコンテナログの内容が入ります。コンテナログの内容はJSONの形式で出力されます。

4.4.6. Podmanメトリクス監視機能

podmanコマンド経由で情報を取得し、Senju DevOperation Conductorのモニタリング機能を使って、監視することができます。

監視定義を千手ブラウザより登録し、監視を実施します。監視結果は、各種モニタ画面（グローバルノードモニタ／ノードモニタ）にてその監視状況を表示できます。予め設定したしきい値により障害を検知した場合は、メッセージモニタにメッセージが通知されます。（モニタリング機能については、ユーザーズガイド「 **4．モニタリング** 」を参照して下さい。）

4.4.7. OpenShiftメトリクス監視機能

ocコマンド経由で情報を取得し、Senju DevOperation Conductorのモニタリング機能を使って、監視することができます。

監視定義を千手ブラウザより登録し、監視を実施します。監視結果は、各種モニタ画面（グローバルノードモニタ／ノードモニタ）にてその監視状況を表示できます。予め設定したしきい値により障害を検知した場合は、メッセージモニタにメッセージが通知されます。（モニタリング機能については、ユーザーズガイド「 **4．モニタリング** 」を参照して下さい。）

4.4.8. OpenShiftイベント監視機能

監視項目「OpenShift：イベント監視」では OpenShift から取得したログをログファイルに蓄積します。このログファイルを監視することでOpenShiftのイベントを検知することが可能です。

4.4.8.1. ログファイル

監視項目「OpenShift：イベント監視」で取得したログファイルは次のファイルに出力されます。ただし、ファイル名に使用できない記号は「-」(半角ハイフン)に置き換えます。

- ログフォーマットがLTSVの場合：

表 4.18 ログファイル名(LTSV)

項目	内容
ログディレクトリ名	`~/log/container.d/`
ログファイル名(通常)	`~/log/container.d/ops_events_{nodeid}_default.log`
ログファイル名(通常+コンテキスト指定)	`~/log/container.d/ops_events_{nodeid}_{context}.log`
ログファイル名(センサー)	`~/log/container.d/ops_events_{user}@{nodeid}_default.log`
ログファイル名(センサー+コンテキスト指定時)	`~/log/container.d/ops_events_{user}@{nodeid}_{context}.log`

- ログフォーマットがJSONの場合：

表 4.19 ログファイル名(JSON)

項目	内容
ログディレクトリ名	`~/log/container.d/`
ログファイル名(通常)	`~/log/container.d/ops_events_{nodeid}_default.json`
ログファイル名(通常+コンテキスト指定)	`~/log/container.d/ops_events_{nodeid}_{context}.json`
ログファイル名(センサー)	`~/log/container.d/ops_events_{user}@{nodeid}_default.json`
ログファイル名(センサー+コンテキスト指定時)	`~/log/container.d/ops_events_{user}@{nodeid}_{context}.json`

4.4.8.2. ログフォーマット

以下にOpenShiftイベント監視で取得したログファイルのレコード形式について説明します。デフォルトのレコードフォーマットは LTSV形式で、項目間はタブ区切りとなります。

【OpenShiftイベントログファイル　レコード形式】

- ログフォーマットがLTSVの場合：

最新のタイムスタンプ　ノードID　名前空間　タイプ（通常、警告）　理由　オブジェクト　サブオブジェクト　発生環境　メッセージ　最初のタイムスタンプ　回数　名前

表 4.20 イベント監視レコード形式(LTSV)

No.	項目	キー:	説明
1	最新のタイムスタンプ	LastTimeStamp:	取得したイベントが記録された最新時刻。存在しない場合は、FirstTimeStampの値を利用しま フォーマット: YYYY-MM-DDThh:mm:ddZ(例 : 2020-03-13T07:09:06Z)
2	ノードID	NodeId:	ノードID名
3	名前空間	Namespace:	名前空間
4	タイプ(通常、警告)	Type:	イベントタイプ(Normal/Warning)
5	理由	Reason:	イベントオブジェクトのステータス理由。
6	オブジェクト	Object:	イベントに関連するオブジェクト
7	サブオブジェクト	SubObject:	イベントに関連するサブオブジェクト
8	発生環境	Source:	取得したイベントの発生環境
9	メッセージ	Message:	取得したイベントのメッセージ
10	最初のタイムスタンプ	FirstTimeStamp:	取得したイベントが最初に記録された時刻。存在しない場合は、eventTimeの値を利用します。 フォーマット: YYYY-MM-DDThh:mm:ddZ(例 : 2020-03-13T07:09:06Z)
11	回数	Count:	取得イベントの発生回数
12	名前	Name:	取得したPod名

- ログフォーマットがJSONの場合 :

イベント内容

表 4.21 イベント監視レコード形式(JSON)

No.	項目	説明
1	イベント内容	取得したイベント内容が入ります。イベント内容はJSONの形式で出力されます。

4.4.9. OpenShiftコンテナログ監視機能

監視項目「OpenShift : コンテナログ監視」では OpenShift から取得したログをログファイルに蓄積します。このログファイルを監視することで OpenShiftのコンテナログを検知することが可能です。

4.4.9.1. ログファイル

監視項目「OpenShift : コンテナログ監視」で取得したログファイルは次のファイルに出力されます。
ただし、ファイル名に使用できない記号と「=」(イコール)、「,」(カンマ)は「-」(半角ハイフン)に置き換えます。

- ログフォーマットがLTSVの場合 :

表 4.22 ログファイル名(LTSV)

項目	内容
ログディレクトリ名	`~/log/container.d/`
ログファイル名(通常)	`~/log/container.d/ops_container_{nodeid}_{selector}_default.log`
ログファイル名(通常+コンテキスト指定)	`~/log/container.d/ops_container_{nodeid}_{selector}_{context}.log`
ログファイル名(センサー)	`~/log/container.d/ops_container_{user}@{nodeid}_{selector}_default.log`
ログファイル名(センサー+コンテキスト指定時)	`~/log/container.d/ops_container_{user}@{nodeid}_{selector}_{context}.log`

- ログフォーマットがJSONの場合 :

表 4.23 ログファイル名(JSON)

項目	内容
ログディレクトリ名	`~/log/container.d/`
ログファイル名(通常)	`~/log/container.d/ops_container_{nodeid}_{selector}_default.json`
ログファイル名(通常+コンテキスト指定)	`~/log/container.d/ops_container_{nodeid}_{selector}_{context}.json`
ログファイル名(センサー)	`~/log/container.d/ops_container_{user}@{nodeid}_{selector}_default.json`
ログファイル名(センサー+コンテキスト指定時)	`~/log/container.d/ops_container_{user}@{nodeid}_{selector}_{context}.jso`

4.4.9.2. ログフォーマット

以下にOpenShiftコンテナログ監視で取得したログファイルのレコード形式について説明します。デフォルトのレコードフォーマットは LTSV形式で、項目間はタブ区切りとなります。

【OpenShiftコンテナログファイル　レコード形式】

- ログフォーマットがLTSVの場合：

最新のタイムスタンプ　Pod名　コンテナ名　メッセージ

表 4.24 コンテナログ監視レコード形式(LTSV)

No.	項目	キー:	説明
1	タイムスタンプ	TimeStamp:	取得したコンテナログが記録された時刻。フォーマット: YYYY-MM-DDThh:mm:ddZ(例: 2020-03-13T07:0
2	Pod名	Pod:	取得したPod名
3	コンテナ名	Container:	取得したコンテナ名
4	メッセージ	Message:	取得したコンテナログのメッセージ

- ログフォーマットがJSONの場合：

イベント内容

表 4.25 コンテナログ監視レコード形式(JSON)

No.	項目	説明
1	コンテナログ内容	取得したコンテナログの内容が入ります。コンテナログの内容はJSONの形式で出力されます。

4.4.10. テキストログ監視の設定方法

以下にSenju DevOperation Conductorのテキストログ監視を利用して、Kubernetesイベントログ監視/Kubernetesコンテナログ監視/OpenShiftイベント監視で取得したログメッセージを監視する運用例を示します。この例では、ログメッセージにキーワードが発生時にメッセージモニタに通知されるようにログフィルタを登録し、監視する場合について説明します。

＜ログフィルタの登録＞
千手ブラウザのツリービューで＜ドメイン＞→“フィルタ”→“ログフィルタ”を選択します。ログフィルタのエンティティでリストビューの何も表示されていない部分でマウスの右ボタンを押してコンテキストメニューを表示し、[新規作成]メニューを選択します。ログフィルタのプロパティが表示されます。ログフィルタ名などの各項目を入力し[OK]ボタンを押下します。これにより、ログフィルタの登録が完了します。

＜フィルタ監視項目の追加＞
千手ブラウザのツリービューの＜ドメイン＞→“フィルタ”→“ログフィルタ”→＜ログフィルタ＞でフィルタ監視項目を登録するログフィルタを選択し、リストビューの何も表示されていない部分でマウスの右ボタンを押してコンテキストメニューを表示し、[新規作成]メニューを選択します。フィルタ監視項目のプロパティが表示されますので、指定フィールドを検知するキーワードで監視設定し、通知したいメッセージIDを登録します。

＜テキストログ監視の設定＞
OpenShiftイベントログファイルのテキストログ監視を行うには、千手ブラウザのツリービューで、＜ドメイン＞→“ノードグループ”→＜ノードグループ＞を選択し、そのリストビューからOpenShiftイベント監視のプローブとして設定したノードを選択し、マウスの右ボタンをクリックしコンテキストメニューを表示し、[プロパティ]メニューを選択します。ノードのプロパティウィンドウが表示されますので、[ログ監視]タブを選択します。ノードのプロパティ（[ログ監視]タブ）にて、監視対象のパス名とファイル名にOpenShiftログファイルを指定し、監視方法に先に作成したログフィルタを指定します。ログ監視を登録した後に、登録したノードに対して[反映(監視属性)]を実行することにより、ログファイルの監視を開始します。

以上で、テキストログ監視の設定方法は完了です。この設定によりKubernetesイベントログファイル/Kubernetesコンテナログファイル/OpenShiftイベントログファイルにキーワードが出力された場合、メッセージモニタに通知されます。

警告

管理対象ノードにおいて千手が起動していない状態で、[反映(監視属性)]を行うと失敗しますので、注意して下さい。

4.4.11. 使用上の制限事項

- Docker監視項目、Kubernetes監視項目、Podman監視項目およびOpenShift監視項目のパラメータにスペース、メタキャラクタを含む値を指定することはできません。
- OpenShift監視項目のセンサー監視では「コンテキスト」パラメータの値に「#」が含まれる場合、センサーのログインシェルの種類により「#」をバックスラッシュ「\」でエスケープする必要があります。

表 4.26 エスケープ有無の表

シェル種類	エスケープ有無	指定例
csh	有	default/xxxx-xxx:nnnn/IAM\\\#xxxxx@nri.co.jp
bash	無	default/xxxx-xxx:nnnn/IAM#xxxxx@nri.co.jp
dash	無	default/xxxx-xxx:nnnn/IAM#xxxxx@nri.co.jp

- 「Podman：コンテナ別」で始まる監視項目は、一部podman statsコマンドで取得していますが、podman statsコマンドはPodman、cgroupのバージョンとrootlessモードの状態により、サポートされないことがあります。詳細については下記の表に示します。

表 4.27 Podman stats実行可否結果表

	Podman V2		Podman V3	
	cgroup v1	cgroup v2	cgroup v1	cgroup v2
rootless有効	×	×	×	△
rootless無効	○	○	○	○

○：実行可能
×：実行不可
△：一部項目取得可能

- OpenShift監視での監視先がRed Hat OpenShift Service on AWS (ROSA)の場合、以下の監視項目は利用できません。
    - OpenShift：Pod別CPU使用率(%)
    - OpenShift：Pod別CPUミリコア使用量(millicores)
    - OpenShift：Pod別メモリ使用量(KB)
    - OpenShift：Pod別メモリ使用量(MB)
    - OpenShift：ワーカーノード別CPU使用率(%)
    - OpenShift：ワーカーノード別CPUミリコア使用量(millicores)
    - OpenShift：ワーカーノード別メモリ使用率(%)
    - OpenShift：ワーカーノード別メモリ使用量(MB)
    - OpenShift：デプロイメント別CPU使用率(%)
    - OpenShift：レプリカセット別CPU使用率(%)
    - OpenShift：デーモンセット別CPU使用率(%)

4.5. 付録

4.5.1. Docker 監視項目一覧

- **Docker：全体コンテナ数**

  説明 Dockerの全体コンテナ数を監視します。取得データは瞬間値となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし

- **Docker：稼働コンテナ数**

  説明 Dockerの稼働コンテナ数を監視します。取得データは瞬間値となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし

- **Docker：一時停止コンテナ数**

  説明 Dockerの一時停止コンテナ数を監視します。取得データは瞬間値となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし

- **Docker：停止コンテナ数**

  説明 Dockerの停止コンテナ数を監視します。取得データは瞬間値となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし

- **Docker：コンテナ別稼働状況**

  説明 Dockerコンテナの稼働状態を監視します。取得データは瞬間値となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
検索方法	監視対象のコンテナIDもしくはコンテナ名の検索方法（完全一致：complete、部分一致：part
コンテナID/コンテナ名	監視対象コンテナのコンテナIDもしくはコンテナ名を指定します。省略可です。省略した場合は

- **Docker：コンテナ別CPU使用率(%)**

  説明 DockerコンテナのCPU負荷状態を監視します。取得データは瞬間値の平均となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
検索方法	監視対象のコンテナIDもしくはコンテナ名の検索方法（完全一致：complete、部分一致：part
コンテナID/コンテナ名	監視対象コンテナのコンテナIDもしくはコンテナ名を指定します。省略可です。省略した場合は

- **Docker：コンテナ別メモリ使用率(%)**

  説明 Dockerコンテナの物理メモリの使用率を監視します。取得データは瞬間値となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
検索方法	監視対象のコンテナIDもしくはコンテナ名の検索方法（完全一致：complete、部分一致：part
コンテナID/コンテナ名	監視対象コンテナのコンテナIDもしくはコンテナ名を指定します。省略可です。省略した場合は

- **Docker：コンテナ別メモリ使用量(KB)**

  説明 Dockerコンテナの物理メモリの使用量を監視します。取得データは瞬間値となります。

パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
検索方法	監視対象のコンテナIDもしくはコンテナ名の検索方法(完全一致:complete、部分一致:par
コンテナID/コンテナ名	監視対象コンテナのコンテナIDもしくはコンテナ名を指定します。省略可です。省略した場合は

- **Docker:コンテナ別メモリ使用量(MB)**

  説明 Dockerコンテナの物理メモリの使用量を監視します。取得データは瞬間値となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
検索方法	監視対象のコンテナIDもしくはコンテナ名の検索方法(完全一致:complete、部分一致:par
コンテナID/コンテナ名	監視対象コンテナのコンテナIDもしくはコンテナ名を指定します。省略可です。省略した場合は

- **Docker:コンテナ別ネットワーク受信バイト数(kBps)**

  説明 Dockerコンテナのインターフェースが受信したデータ数を監視します。取得データは検査間隔期間内の平均値となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
検索方法	監視対象のコンテナIDもしくはコンテナ名の検索方法(完全一致:complete、部分一致:par
コンテナID/コンテナ名	監視対象コンテナのコンテナIDもしくはコンテナ名を指定します。省略可です。省略した場合は

- **Docker:コンテナ別ネットワーク送信バイト数(kBps)**

  説明 Dockerコンテナのインターフェースが送信したデータ数を監視します。取得データは検査間隔期間内の平均値となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
検索方法	監視対象のコンテナIDもしくはコンテナ名の検索方法(完全一致:complete、部分一致:par
コンテナID/コンテナ名	監視対象コンテナのコンテナIDもしくはコンテナ名を指定します。省略可です。省略した場合は

- **Docker：コンテナ内プロセスCPU使用率(%)**

  説明 Dockerコンテナ内のプロセスのCPU負荷状態を監視します。取得データは瞬間値となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
コンテナID/コンテナ名	監視対象コンテナのコンテナIDもしくはコンテナ名を指定します。

- **Docker：コンテナ内プロセス仮想メモリ使用量(KB)**

  説明 Dockerコンテナ内プロセスの仮想メモリ使用量を監視します。取得データは瞬間値となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
コンテナID/コンテナ名	監視対象コンテナのコンテナIDもしくはコンテナ名を指定します。

- **Docker：コンテナ内プロセス仮想メモリ使用量(MB)**

  説明 Dockerコンテナ内プロセスの仮想メモリ使用量を監視します。取得データは瞬間値となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
コンテナID/コンテナ名	監視対象コンテナのコンテナIDもしくはコンテナ名を指定します。

- **Docker：コンテナ内プロセス物理メモリ使用量(KB)**

  説明 Dockerコンテナ内プロセスの物理メモリ使用量を監視します。取得データは瞬間値となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
コンテナID/コンテナ名	監視対象コンテナのコンテナIDもしくはコンテナ名を指定します。

- **Docker：コンテナ内プロセス物理メモリ使用量(MB)**

説明 Dockerコンテナ内プロセスの物理メモリ使用量を監視します。取得データは瞬間値となります。

パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
コンテナID/コンテナ名	監視対象コンテナのコンテナIDもしくはコンテナ名を指定します。

- **Docker：コンテナログ監視**

  説明 Dockerのコンテナログ情報を監視します。取得データは成否となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
コンテナID/コンテナ名	監視対象コンテナのコンテナIDもしくはコンテナ名を指定します。
ログフォーマット	取得したログの出力フォーマットをLTSVもしくはJSONに切り替えます。省略可です。省略した

注釈

- 監視間隔内で監視対象コンテナが再起動した場合、当該コンテナの再起動前のログを取得することはできません。
- コンテナログ監視では、最後に取得したログから5分間遡ってログを取得します。

4.5.2. Kubernetes 監視項目一覧

- **Kubernetes：全体Pod数**

  説明 Kubernetesの全体Pod数を監視します。取得データは瞬間値となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
セレクター	監視対象とするPodをセレクターで指定します。省略可です。省略した場合は全てのPodを監 セレクターは `<key>=<value>` の形式で指定してください。(例) app=nginx
コンテキスト	Kubernetesクラスタへの接続に利用するコンテキストを指定します。省略可です。省略した場
ネームスペース	監視対象とするネームスペースを指定します。省略可です。省略した場合はデフォルトのネーム
設定ファイル	絶対パスで監視用の設定ファイルを指定します。省略可です。

- **Kubernetes：稼働Pod数**

  説明 Kubernetesの稼働Pod数を監視します。取得データは瞬間値となります。

パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
セレクター	監視対象とするPodをセレクターで指定します。省略可です。省略した場合は全てのPodを監 セレクターは `<key>=<value>` の形式で指定してください。(例) app=nginx
コンテキスト	Kubernetesクラスタへの接続に利用するコンテキストを指定します。省略可です。省略した場
ネームスペース	監視対象とするネームスペースを指定します。省略可です。省略した場合はデフォルトのネーム
設定ファイル	絶対パスで監視用の設定ファイルを指定します。省略可です。

- **Kubernetes：非稼働Pod数**

  説明 Kubernetesの非稼働Pod数を監視します。取得データは瞬間値となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
セレクター	監視対象とするPodをセレクターで指定します。省略可です。省略した場合は全てのPodを監 セレクターは `<key>=<value>` の形式で指定してください。(例) app=nginx
コンテキスト	Kubernetesクラスタへの接続に利用するコンテキストを指定します。省略可です。省略した場
ネームスペース	監視対象とするネームスペースを指定します。省略可です。省略した場合はデフォルトのネーム
設定ファイル	絶対パスで監視用の設定ファイルを指定します。省略可です。

- **Kubernetes：Pod別稼働状況**

  説明 KubernetesのPod別稼働状態を監視します。取得データは瞬間値となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
Pod名	監視対象とするPodのPod名を指定します。省略可です。省略した場合は全てのPodを監視
セレクター	監視対象とするPodをセレクターで指定します。省略可です。省略した場合は全てのPodを監 セレクターは `<key>=<value>` の形式で指定してください。(例) app=nginx
コンテキスト	Kubernetesクラスタへの接続に利用するコンテキストを指定します。省略可です。省略した場
ネームスペース	監視対象とするネームスペースを指定します。省略可です。省略した場合はデフォルトのネーム
設定ファイル	絶対パスで監視用の設定ファイルを指定します。省略可です。

- **Kubernetes：Pod別再起動状況**

説明 KubernetesのPod別再起動状況を監視します。前回取得した値の差分を返します。取得データは検査間隔内の瞬間値となります。

パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
Pod名	監視対象とするPodのPod名を指定します。省略可です。省略した場合は全てのPodを監視
セレクター	監視対象とするPodをセレクターで指定します。省略可です。省略した場合は全てのPodを監 セレクターは `<key>=<value>` の形式で指定してください。(例) app=nginx
コンテキスト	Kubernetesクラスタへの接続に利用するコンテキストを指定します。省略可です。省略した場
ネームスペース	監視対象とするネームスペースを指定します。省略可です。省略した場合はデフォルトのネーム
設定ファイル	絶対パスで監視用の設定ファイルを指定します。省略可です。

- **Kubernetes：Pod別CPU使用率(%)**

  説明 KubernetesのPod別CPU使用率を監視します。取得データはPodの検査間隔期間内のCPUミリコア使用量をCPU制限値で割った値となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
Pod名	監視対象とするPodのPod名を指定します。省略可です。省略した場合は全てのPodを監視
セレクター	監視対象とするPodをセレクターで指定します。省略可です。省略した場合は全てのPodを監 セレクターは `<key>=<value>` の形式で指定してください。(例) app=nginx
コンテキスト	Kubernetesクラスタへの接続に利用するコンテキストを指定します。省略可です。省略した場
ネームスペース	監視対象とするネームスペースを指定します。省略可です。省略した場合はデフォルトのネーム
設定ファイル	絶対パスで監視用の設定ファイルを指定します。省略可です。

- **Kubernetes：Pod別CPUミリコア使用量(millicores)**

  説明 KubernetesのPod別CPUミリコア値を監視します。取得データは平均値となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
Pod名	監視対象とするPodのPod名を指定します。省略可です。省略した場合は全てのPodを監視
セレクター	監視対象とするPodをセレクターで指定します。省略可です。省略した場合は全てのPodを監 セレクターは `<key>=<value>` の形式で指定してください。(例) app=nginx
コンテキスト	Kubernetesクラスタへの接続に利用するコンテキストを指定します。省略可です。省略した場
ネームスペース	監視対象とするネームスペースを指定します。省略可です。省略した場合はデフォルトのネーム
設定ファイル	絶対パスで監視用の設定ファイルを指定します。省略可です。

- **Kubernetes：Pod別メモリ使用量(KB)**

  説明 KubernetesのPod別物理メモリの使用量を監視します。取得データは瞬間値となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
Pod名	監視対象とするPodのPod名を指定します。省略可です。省略した場合は全てのPodを監視
セレクター	監視対象とするPodをセレクターで指定します。省略可です。省略した場合は全てのPodを監 セレクターは `<key>=<value>` の形式で指定してください。(例) app=nginx
コンテキスト	Kubernetesクラスタへの接続に利用するコンテキストを指定します。省略可です。省略した場
ネームスペース	監視対象とするネームスペースを指定します。省略可です。省略した場合はデフォルトのネーム
設定ファイル	絶対パスで監視用の設定ファイルを指定します。省略可です。

- **Kubernetes：Pod別メモリ使用量(MB)**

  説明 KubernetesのPod別物理メモリの使用量を監視します。取得データは瞬間値となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
Pod名	監視対象とするPodのPod名を指定します。省略可です。省略した場合は全てのPodを監視
セレクター	監視対象とするPodをセレクターで指定します。省略可です。省略した場合は全てのPodを監 セレクターは `<key>=<value>` の形式で指定してください。(例) app=nginx
コンテキスト	Kubernetesクラスタへの接続に利用するコンテキストを指定します。省略可です。省略した場
ネームスペース	監視対象とするネームスペースを指定します。省略可です。省略した場合はデフォルトのネーム
設定ファイル	絶対パスで監視用の設定ファイルを指定します。省略可です。

- **Kubernetes：ワーカーノード別稼働状況**

  説明 Kubernetesのワーカーノード別稼働状況を監視します。取得データは瞬間値となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
ワーカーノード名	監視対象ワーカーノードのワーカーノード名を指定します。省略可です。省略した場合は全ての
セレクター	監視対象とするワーカーノードをセレクターで指定します。省略可です。省略した場合は全ての セレクターは `<key>=<value>` の形式で指定してください。(例) app=nginx
コンテキスト	Kubernetesクラスタへの接続に利用するコンテキストを指定します。省略可です。省略した場
設定ファイル	絶対パスで監視用の設定ファイルを指定します。省略可です。

- **Kubernetes：ワーカーノード別稼働Pod数**

  説明 Kubernetesのワーカーノード別稼働Pod数を監視します。取得データは瞬間値となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
ワーカーノード名	監視対象ワーカーノードのワーカーノード名を指定します。省略可です。省略した場合は全ての
セレクター	監視対象とするワーカーノードをセレクターで指定します。省略可です。省略した場合は全ての セレクターは `<key>=<value>` の形式で指定してください。(例) app=nginx
コンテキスト	Kubernetesクラスタへの接続に利用するコンテキストを指定します。省略可です。省略した場
ネームスペース	監視対象とするネームスペースを指定します。省略可です。省略した場合はデフォルトのネーム
設定ファイル	絶対パスで監視用の設定ファイルを指定します。省略可です。

- **Kubernetes：ワーカーノード別CPU使用率(%)**

  説明 Kubernetesのワーカーノード別物理CPU使用率を監視します。取得データは平均値となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
ワーカーノード名	監視対象ワーカーノードのワーカーノード名を指定します。省略可です。省略した場合は全ての
セレクター	監視対象とするワーカーノードをセレクターで指定します。省略可です。省略した場合は全ての セレクターは `<key>=<value>` の形式で指定してください。(例) app=nginx
コンテキスト	Kubernetesクラスタへの接続に利用するコンテキストを指定します。省略可です。省略した場
設定ファイル	絶対パスで監視用の設定ファイルを指定します。省略可です。

- **Kubernetes：ワーカーノード別CPUミリコア使用量(millicores)**

  説明 Kubernetesのワーカーノード別物理CPUミリコア値を監視します。取得データは平均値となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
ワーカーノード名	監視対象ワーカーノードのワーカーノード名を指定します。省略可です。省略した場合は全ての
セレクター	監視対象とするワーカーノードをセレクターで指定します。省略可です。省略した場合は全ての セレクターは `<key>=<value>` の形式で指定してください。(例) app=nginx
コンテキスト	Kubernetesクラスタへの接続に利用するコンテキストを指定します。省略可です。省略した場
設定ファイル	絶対パスで監視用の設定ファイルを指定します。省略可です。

- **Kubernetes：ワーカーノード別メモリ使用率(%)**

  説明 Kubernetesのワーカーノード別物理メモリの使用率を監視します。取得データは瞬間値となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
ワーカーノード名	監視対象ワーカーノードのワーカーノード名を指定します。省略可です。省略した場合は全ての
セレクター	監視対象とするワーカーノードをセレクターで指定します。省略可です。省略した場合は全ての セレクターは `<key>=<value>` の形式で指定してください。(例) app=nginx
コンテキスト	Kubernetesクラスタへの接続に利用するコンテキストを指定します。省略可です。省略した場
設定ファイル	絶対パスで監視用の設定ファイルを指定します。省略可です。

- **Kubernetes：ワーカーノード別メモリ使用量(MB)**

  説明 Kubernetesのワーカーノード別物理メモリの使用量を監視します。取得データは瞬間値となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
ワーカーノード名	監視対象ワーカーノードのワーカーノード名を指定します。省略可です。省略した場合は全ての
セレクター	監視対象とするワーカーノードをセレクターで指定します。省略可です。省略した場合は全ての セレクターは `<key>=<value>` の形式で指定してください。(例) app=nginx
コンテキスト	Kubernetesクラスタへの接続に利用するコンテキストを指定します。省略可です。省略した場
設定ファイル	絶対パスで監視用の設定ファイルを指定します。省略可です。

- **Kubernetes：イベント監視**

  説明 Kubernetesのイベント情報を監視します。取得データは成否となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
コンテキスト	Kubernetesクラスタへの接続に利用するコンテキストを指定します。省略可です。省略した場
ログフォーマット	取得したログの出力フォーマットをLTSVもしくはJSONに切り替えます。省略可です。省略した
ネームスペース	監視対象とするネームスペースを指定します。省略可です。省略した場合はデフォルトのネーム
設定ファイル	絶対パスで監視用の設定ファイルを指定します。省略可です。

- **Kubernetes：デプロイメント監視**

  説明 Kubernetesのデプロイメント情報を監視します。取得データは瞬間値となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
Deployment名	監視対象とするデプロイメントのデプロイメント名を指定します。省略可です。省略した場合は全
セレクター	監視対象とするデプロイメントをセレクターで指定します。省略可です。省略した場合は全ての セレクターは `<key>=<value>` の形式で指定してください。(例) app=nginx
コンテキスト	Kubernetesクラスタへの接続に利用するコンテキストを指定します。省略可です。省略した場
ネームスペース	監視対象とするネームスペースを指定します。省略可です。省略した場合はデフォルトのネーム
設定ファイル	絶対パスで監視用の設定ファイルを指定します。省略可です。

- **Kubernetes：デプロイメント別CPU使用率(%)**

  説明 Kubernetesのデプロイメント別CPU使用率を監視します。取得データはデプロイメントが持つ各Podの検査間隔期間内のCPUミリコア使用量の合計を各PodのCPU制限値の合計で割った値となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
Deployment名	監視対象とするデプロイメントのデプロイメント名を指定します。省略可です。省略した場合は全
セレクター	監視対象とするデプロイメントをセレクターで指定します。省略可です。省略した場合は全ての セレクターは `<key>=<value>` の形式で指定してください。(例) app=nginx
コンテキスト	Kubernetesクラスタへの接続に利用するコンテキストを指定します。省略可です。省略した場
ネームスペース	監視対象とするネームスペースを指定します。省略可です。省略した場合はデフォルトのネーム
設定ファイル	絶対パスで監視用の設定ファイルを指定します。省略可です。

- **Kubernetes：レプリカセット監視**

  説明 Kubernetesのレプリカセット情報を監視します。取得データは瞬間値となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
ReplicaSet名	監視対象とするレプリカセットのレプリカセット名を指定します。省略可です。省略した場合は全
セレクター	監視対象とするレプリカセットをセレクターで指定します。省略可です。省略した場合は全てのし セレクターは `<key>=<value>` の形式で指定してください。(例) app=nginx
コンテキスト	Kubernetesクラスタへの接続に利用するコンテキストを指定します。省略可です。省略した場
ネームスペース	監視対象とするネームスペースを指定します。省略可です。省略した場合はデフォルトのネーム
設定ファイル	絶対パスで監視用の設定ファイルを指定します。省略可です。

- **Kubernetes：レプリカセット別CPU使用率(%)**

  説明 Kubernetesのレプリカセット別CPU使用率を監視します。取得データはレプリカセットが持つ各Podの検査間隔期間内のCPUミリコア使用量の合計を各PodのCPU制限値の合計で割った値となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
ReplicaSet名	監視対象とするレプリカセットのレプリカセット名を指定します。省略可です。省略した場合は全
セレクター	監視対象とするレプリカセットをセレクターで指定します。省略可です。省略した場合は全てのし セレクターは `<key>=<value>` の形式で指定してください。(例) app=nginx
コンテキスト	Kubernetesクラスタへの接続に利用するコンテキストを指定します。省略可です。省略した場
ネームスペース	監視対象とするネームスペースを指定します。省略可です。省略した場合はデフォルトのネーム
設定ファイル	絶対パスで監視用の設定ファイルを指定します。省略可です。

- **Kubernetes：デーモンセット監視**

  説明 Kubernetesのデーモンセット情報を監視します。取得データは瞬間値となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
DaemonSet名	監視対象とするデーモンセットのデーモンセット名を指定します。省略可です。省略した場合は
セレクター	監視対象とするデーモンセットをセレクターで指定します。省略可です。省略した場合は全ての セレクターは `<key>=<value>` の形式で指定してください。(例) app=nginx
コンテキスト	Kubernetesクラスタへの接続に利用するコンテキストを指定します。省略可です。省略した場
ネームスペース	監視対象とするネームスペースを指定します。省略可です。省略した場合はデフォルトのネーム
設定ファイル	絶対パスで監視用の設定ファイルを指定します。省略可です。

- **Kubernetes：デーモンセット別CPU使用率(%)**

  説明 Kubernetesのデーモンセット別CPU使用率を監視します。取得データはデーモンセットが持つ各Podの検査間隔期間内のCPUミリコア使用量の合計を各PodのCPU制限値の合計で割った値となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
DaemonSet名	監視対象とするデーモンセットのデーモンセット名を指定します。省略可です。省略した場合は
セレクター	監視対象とするデーモンセットをセレクターで指定します。省略可です。省略した場合は全ての セレクターは `<key>=<value>` の形式で指定してください。(例) app=nginx
コンテキスト	Kubernetesクラスタへの接続に利用するコンテキストを指定します。省略可です。省略した場
ネームスペース	監視対象とするネームスペースを指定します。省略可です。省略した場合はデフォルトのネーム
設定ファイル	絶対パスで監視用の設定ファイルを指定します。省略可です。

- **Kubernetes：コンテナログ監視**

  説明 Kubernetesのコンテナログ情報を監視します。取得データは成否となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
セレクター	監視対象とするPodをセレクターで指定します。省略不可です。 セレクターは `<key>=<value>` の形式で指定してください。(例) app=nginx
コンテキスト	Kubernetesクラスタへの接続に利用するコンテキストを指定します。省略可です。省略した場
ログフォーマット	取得したログの出力フォーマットをLTSVもしくはJSONに切り替えます。省略可です。省略した
ネームスペース	監視対象とするネームスペースを指定します。省略可です。省略した場合はデフォルトのネーム
設定ファイル	絶対パスで監視用の設定ファイルを指定します。省略可です。

注釈

- コンテナログ監視を利用する場合、対象のPodにラベルを設定する必要があります。
- 監視間隔内で監視対象Podに含まれるコンテナが再起動した場合、当該コンテナの再起動前のログを取得することはできません。
- コンテナログ監視では、最後に取得したログから5分間遡ってログを取得します。

警告

- 指定されたラベルセレクターの対象となるPodが存在しない場合、監視結果は正常となります。

4.5.3. Podman 監視項目一覧

- **Podman：全体コンテナ数**

  説明 Podmanの全体コンテナ数を監視します。取得データは瞬間値となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし

- **Podman：稼働コンテナ数**

  説明 Podmanの稼働コンテナ数を監視します。取得データは瞬間値となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし

- **Podman：一時停止コンテナ数**

  説明 Podmanの一時停止コンテナ数を監視します。取得データは瞬間値となります。

パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし

- **Podman：停止コンテナ数**

  説明 Podmanの停止コンテナ数を監視します。取得データは瞬間値となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし

- **Podman：コンテナ別稼働状況**

  説明 Podmanコンテナの稼働状態を監視します。取得データは瞬間値となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
検索方法	監視対象のコンテナIDもしくはコンテナ名の検索方法（完全一致：complete、部分一致：part
コンテナID/コンテナ名	監視対象コンテナのコンテナIDもしくはコンテナ名を指定します。省略可です。省略した場合は

注釈

「Podman：コンテナ別」で始まる監視項目は、一部podman statsコマンドで取得していますが、podman statsコマンドはPodman、cgroupのバージョンとrootlessモードの状態により、サポートされないことがあります。詳細については、使用上の制限事項 を参照して下さい。

- **Podman：コンテナ別CPU使用率(%)**

  説明 PodmanコンテナのCPU負荷状態を監視します。取得データは瞬間値の平均となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
検索方法	監視対象のコンテナIDもしくはコンテナ名の検索方法(完全一致:complete、部分一致:part
コンテナID/コンテナ名	監視対象コンテナのコンテナIDもしくはコンテナ名を指定します。省略可です。省略した場合は

注釈

「Podman:コンテナ別」で始まる監視項目は、一部podman statsコマンドで取得していますが、podman statsコマンドはPodman、cgroupのバージョンとrootlessモードの状態により、サポートされないことがあります。詳細については、使用上の制限事項 を参照して下さい。

- **Podman:コンテナ別メモリ使用率(%)**

  説明 Podmanコンテナの物理メモリの使用率を監視します。取得データは瞬間値となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
検索方法	監視対象のコンテナIDもしくはコンテナ名の検索方法(完全一致:complete、部分一致:part
コンテナID/コンテナ名	監視対象コンテナのコンテナIDもしくはコンテナ名を指定します。省略可です。省略した場合は

注釈

「Podman:コンテナ別」で始まる監視項目は、一部podman statsコマンドで取得していますが、podman statsコマンドはPodman、cgroupのバージョンとrootlessモードの状態により、サポートされないことがあります。詳細については、使用上の制限事項 を参照して下さい。

- **Podman:コンテナ別メモリ使用量(KB)**

  説明 Podmanコンテナの物理メモリの使用量を監視します。取得データは瞬間値となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
検索方法	監視対象のコンテナIDもしくはコンテナ名の検索方法(完全一致:complete、部分一致:part
コンテナID/コンテナ名	監視対象コンテナのコンテナIDもしくはコンテナ名を指定します。省略可です。省略した場合は

注釈

「Podman:コンテナ別」で始まる監視項目は、一部podman statsコマンドで取得していますが、podman statsコマンドはPodman、cgroupのバージョンとrootlessモードの状態により、サポートされないことがあります。詳細については、使用上の制限事項 を参照して下さい。

- **Podman:コンテナ別メモリ使用量(MB)**

説明 Podmanコンテナの物理メモリの使用量を監視します。取得データは瞬間値となります。

パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
検索方法	監視対象のコンテナIDもしくはコンテナ名の検索方法（完全一致：complete、部分一致：part
コンテナID/コンテナ名	監視対象コンテナのコンテナIDもしくはコンテナ名を指定します。省略可です。省略した場合は

注釈

「Podman：コンテナ別」で始まる監視項目は、一部podman statsコマンドで取得していますが、podman statsコマンドはPodman、cgroupのバージョンとrootlessモードの状態により、サポートされないことがあります。詳細については、使用上の制限事項 を参照して下さい。

- **Podman：コンテナ別ネットワーク受信バイト数(kBps)**

  説明 Podmanコンテナのインターフェースが受信したデータ数を監視します。取得データは検査間隔期間内の平均値となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
検索方法	監視対象のコンテナIDもしくはコンテナ名の検索方法（完全一致：complete、部分一致：part
コンテナID/コンテナ名	監視対象コンテナのコンテナIDもしくはコンテナ名を指定します。省略可です。省略した場合は

注釈

「Podman：コンテナ別」で始まる監視項目は、一部podman statsコマンドで取得していますが、podman statsコマンドはPodman、cgroupのバージョンとrootlessモードの状態により、サポートされないことがあります。詳細については、使用上の制限事項 を参照して下さい。

- **Podman：コンテナ別ネットワーク送信バイト数(kBps)**

  説明 Podmanコンテナのインターフェースが送信したデータ数を監視します。取得データは検査間隔期間内の平均値となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
検索方法	監視対象のコンテナIDもしくはコンテナ名の検索方法（完全一致：complete、部分一致：part
コンテナID/コンテナ名	監視対象コンテナのコンテナIDもしくはコンテナ名を指定します。省略可です。省略した場合は

注釈

「Podman：コンテナ別」で始まる監視項目は、一部podman statsコマンドで取得していますが、podman statsコマンドは

Podman、cgroupのバージョンとrootlessモードの状態により、サポートされないことがあります。詳細については、使用上の制限事項 を参照して下さい。

- **Podman：コンテナ内プロセスCPU使用率(%)**

  説明 Podmanコンテナ内のプロセスのCPU負荷状態を監視します。取得データは瞬間値となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
コンテナID/コンテナ名	監視対象コンテナのコンテナIDもしくはコンテナ名を指定します。

- **Podman：コンテナ内プロセス仮想メモリ使用量(KB)**

  説明 Podmanコンテナ内プロセスの仮想メモリ使用量を監視します。取得データは瞬間値となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
コンテナID/コンテナ名	監視対象コンテナのコンテナIDもしくはコンテナ名を指定します。

- **Podman：コンテナ内プロセス仮想メモリ使用量(MB)**

  説明 Podmanコンテナ内プロセスの仮想メモリ使用量を監視します。取得データは瞬間値となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
コンテナID/コンテナ名	監視対象コンテナのコンテナIDもしくはコンテナ名を指定します。

4.5.4. OpenShift 監視項目一覧

- **OpenShift：全体Pod数**

  説明 OpenShiftの全体Pod数を監視します。取得データは瞬間値となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
設定ファイル	絶対パスで監視用の設定ファイルを指定します。省略可です。
セレクター	監視対象とするPodをセレクターで指定します。省略可です。省略した場合は全てのPodを監 セレクターは `<key>=<value>` の形式で指定してください。(例) app=nginx
コンテキスト	OpenShiftクラスタへの接続に利用するコンテキストを指定します。省略可です。省略した場合

- **OpenShift：稼働Pod数**

  説明 OpenShiftの稼働Pod数を監視します。取得データは瞬間値となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
設定ファイル	絶対パスで監視用の設定ファイルを指定します。省略可です。
セレクター	監視対象とするPodをセレクターで指定します。省略可です。省略した場合は全てのPodを監 セレクターは `<key>=<value>` の形式で指定してください。(例) app=nginx
コンテキスト	OpenShiftクラスタへの接続に利用するコンテキストを指定します。省略可です。省略した場合

- **OpenShift：非稼働Pod数**

  説明 OpenShiftの非稼働Pod数を監視します。取得データは瞬間値となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
設定ファイル	絶対パスで監視用の設定ファイルを指定します。省略可です。
セレクター	監視対象とするPodをセレクターで指定します。省略可です。省略した場合は全てのPodを監 セレクターは `<key>=<value>` の形式で指定してください。(例) app=nginx
コンテキスト	OpenShiftクラスタへの接続に利用するコンテキストを指定します。省略可です。省略した場合

- **OpenShift：Pod別稼働状況**

  説明 OpenShiftのPod別稼働状態を監視します。取得データは瞬間値となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
設定ファイル	絶対パスで監視用の設定ファイルを指定します。省略可です。
Pod名	監視対象とするPodのPod名を指定します。省略可です。省略した場合は全てのPodを監視
セレクター	監視対象とするPodをセレクターで指定します。省略可です。省略した場合は全てのPodを監 セレクターは `<key>=<value>` の形式で指定してください。(例) app=nginx
コンテキスト	OpenShiftクラスタへの接続に利用するコンテキストを指定します。省略可です。省略した場合

- **OpenShift: Pod別再起動状況**

  説明 OpenShiftのPod別再起動状況を監視します。前回取得した値の差分を返します。取得データは検査間隔内の瞬間値となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
設定ファイル	絶対パスで監視用の設定ファイルを指定します。省略可です。
Pod名	監視対象とするPodのPod名を指定します。省略可です。省略した場合は全てのPodを監視
セレクター	監視対象とするPodをセレクターで指定します。省略可です。省略した場合は全てのPodを監 セレクターは `<key>=<value>` の形式で指定してください。(例) app=nginx
コンテキスト	OpenShiftクラスタへの接続に利用するコンテキストを指定します。省略可です。省略した場合

- **OpenShift: Pod別CPU使用率(%)**

  説明 OpenShiftのPod別CPU使用率を監視します。取得データはPodの検査間隔期間内のCPUミリコア使用量をCPU制限値で割った値となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
設定ファイル	絶対パスで監視用の設定ファイルを指定します。省略可です。
Pod名	監視対象とするPodのPod名を指定します。省略可です。省略した場合は全てのPodを監視
セレクター	監視対象とするPodをセレクターで指定します。省略可です。省略した場合は全てのPodを監 セレクターは `<key>=<value>` の形式で指定してください。(例) app=nginx
コンテキスト	OpenShiftクラスタへの接続に利用するコンテキストを指定します。省略可です。省略した場合

- **OpenShift: Pod別CPUミリコア使用量(millicores)**

説明 OpenShiftのPod別CPUミリコア値を監視します。取得データは平均値となります。

パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
設定ファイル	絶対パスで監視用の設定ファイルを指定します。省略可です。
Pod名	監視対象とするPodのPod名を指定します。省略可です。省略した場合は全てのPodを監視
セレクター	監視対象とするPodをセレクターで指定します。省略可です。省略した場合は全てのPodを監 セレクターは `<key>=<value>` の形式で指定してください。(例) app=nginx
コンテキスト	OpenShiftクラスタへの接続に利用するコンテキストを指定します。省略可です。省略した場合

- **OpenShift：Pod別メモリ使用量(KB)**

  説明 OpenShiftのPod別物理メモリの使用量を監視します。取得データは瞬間値となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
設定ファイル	絶対パスで監視用の設定ファイルを指定します。省略可です。
Pod名	監視対象とするPodのPod名を指定します。省略可です。省略した場合は全てのPodを監視
セレクター	監視対象とするPodをセレクターで指定します。省略可です。省略した場合は全てのPodを監 セレクターは `<key>=<value>` の形式で指定してください。(例) app=nginx
コンテキスト	OpenShiftクラスタへの接続に利用するコンテキストを指定します。省略可です。省略した場合

- **OpenShift：Pod別メモリ使用量(MB)**

  説明 OpenShiftのPod別物理メモリの使用量を監視します。取得データは瞬間値となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
設定ファイル	絶対パスで監視用の設定ファイルを指定します。省略可です。
Pod名	監視対象とするPodのPod名を指定します。省略可です。省略した場合は全てのPodを監視
セレクター	監視対象とするPodをセレクターで指定します。省略可です。省略した場合は全てのPodを監 セレクターは `<key>=<value>` の形式で指定してください。(例) app=nginx
コンテキスト	OpenShiftクラスタへの接続に利用するコンテキストを指定します。省略可です。省略した場合

- **OpenShift：ワーカーノード別稼働状況**

説明 OpenShiftのワーカーノード別稼働状況を監視します。取得データは瞬間値となります。

パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
設定ファイル	絶対パスで監視用の設定ファイルを指定します。省略可です。
ワーカーノード名	監視対象ワーカーノードのワーカーノード名を指定します。省略可です。省略した場合は全ての
セレクター	監視対象とするワーカーノードをセレクターで指定します。省略可です。省略した場合は全ての セレクターは `<key>=<value>` の形式で指定してください。(例) app=nginx
コンテキスト	OpenShiftクラスタへの接続に利用するコンテキストを指定します。省略可です。省略した場合

- **OpenShift：ワーカーノード別稼働Pod数**

  説明 OpenShiftのワーカーノード別稼働Pod数を監視します。取得データは瞬間値となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
設定ファイル	絶対パスで監視用の設定ファイルを指定します。省略可です。
ワーカーノード名	監視対象ワーカーノードのワーカーノード名を指定します。省略可です。省略した場合は全ての
セレクター	監視対象とするワーカーノードをセレクターで指定します。省略可です。省略した場合は全ての セレクターは `<key>=<value>` の形式で指定してください。(例) app=nginx
コンテキスト	OpenShiftクラスタへの接続に利用するコンテキストを指定します。省略可です。省略した場合

- **OpenShift：ワーカーノード別CPU使用率(%)**

  説明 OpenShiftのワーカーノード別物理CPU使用率を監視します。取得データは平均値となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
設定ファイル	絶対パスで監視用の設定ファイルを指定します。省略可です。
ワーカーノード名	監視対象ワーカーノードのワーカーノード名を指定します。省略可です。省略した場合は全ての
セレクター	監視対象とするワーカーノードをセレクターで指定します。省略可です。省略した場合は全ての セレクターは `<key>=<value>` の形式で指定してください。(例) app=nginx
コンテキスト	OpenShiftクラスタへの接続に利用するコンテキストを指定します。省略可です。省略した場合

- **OpenShift：ワーカーノード別CPUミリコア使用量(millicores)**

  説明 OpenShiftのワーカーノード別物理CPUミリコア値を監視します。取得データは平均値となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
設定ファイル	絶対パスで監視用の設定ファイルを指定します。省略可です。
ワーカーノード名	監視対象ワーカーノードのワーカーノード名を指定します。省略可です。省略した場合は全ての
セレクター	監視対象とするワーカーノードをセレクターで指定します。省略可です。省略した場合は全ての セレクターは `<key>=<value>` の形式で指定してください。(例) app=nginx
コンテキスト	OpenShiftクラスタへの接続に利用するコンテキストを指定します。省略可です。省略した場合

- **OpenShift：ワーカーノード別メモリ使用率(%)**

  説明 OpenShiftのワーカーノード別物理メモリの使用率を監視します。取得データは瞬間値となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
設定ファイル	絶対パスで監視用の設定ファイルを指定します。省略可です。
ワーカーノード名	監視対象ワーカーノードのワーカーノード名を指定します。省略可です。省略した場合は全ての
セレクター	監視対象とするワーカーノードをセレクターで指定します。省略可です。省略した場合は全ての セレクターは `<key>=<value>` の形式で指定してください。(例) app=nginx
コンテキスト	OpenShiftクラスタへの接続に利用するコンテキストを指定します。省略可です。省略した場合

- **OpenShift：ワーカーノード別メモリ使用量(MB)**

  説明 OpenShiftのワーカーノード別物理メモリの使用量を監視します。取得データは瞬間値となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
設定ファイル	絶対パスで監視用の設定ファイルを指定します。省略可です。
ワーカーノード名	監視対象ワーカーノードのワーカーノード名を指定します。省略可です。省略した場合は全ての
セレクター	監視対象とするワーカーノードをセレクターで指定します。省略可です。省略した場合は全ての セレクターは `<key>=<value>` の形式で指定してください。(例) app=nginx
コンテキスト	OpenShiftクラスタへの接続に利用するコンテキストを指定します。省略可です。省略した場合

- **OpenShift：イベント監視**

  説明 OpenShiftのイベント情報を監視します。取得データは成否となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
設定ファイル	絶対パスで監視用の設定ファイルを指定します。省略可です。
コンテキスト	OpenShiftクラスタへの接続に利用するコンテキストを指定します。省略可です。省略した場合
ログフォーマット	取得したログの出力フォーマットをLTSVもしくはJSONに切り替えます。省略可です。省略した

- **OpenShift：デプロイメント監視**

  説明 OpenShiftのデプロイメント情報を監視します。取得データは瞬間値となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
設定ファイル	絶対パスで監視用の設定ファイルを指定します。省略可です。
Deployment名	監視対象とするデプロイメントのデプロイメント名を指定します。省略可です。省略した場合は全
セレクター	監視対象とするデプロイメントをセレクターで指定します。省略可です。省略した場合は全ての セレクターは `<key>=<value>` の形式で指定してください。(例) app=nginx
コンテキスト	OpenShiftクラスタへの接続に利用するコンテキストを指定します。省略可です。省略した場合

- **OpenShift：デプロイメント別CPU使用率(%)**

  説明 OpenShiftのデプロイメント別CPU使用率を監視します。取得データはデプロイメントが持つ各Podの検査間隔期間内のCPUミリコア使用量の合計を各PodのCPU制限値の合計で割った値となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
設定ファイル	絶対パスで監視用の設定ファイルを指定します。省略可です。
Deployment名	監視対象とするデプロイメントのデプロイメント名を指定します。省略可です。省略した場合は全
セレクター	監視対象とするデプロイメントをセレクターで指定します。省略可です。省略した場合は全ての セレクターは `<key>=<value>` の形式で指定してください。(例) app=nginx
コンテキスト	OpenShiftクラスタへの接続に利用するコンテキストを指定します。省略可です。省略した場合

- **OpenShift：レプリカセット監視**

  説明 OpenShiftのレプリカセット情報を監視します。取得データは瞬間値となります。

パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
設定ファイル	絶対パスで監視用の設定ファイルを指定します。省略可です。
ReplicaSet名	監視対象とするレプリカセットのレプリカセット名を指定します。省略可です。省略した場合は全
セレクター	監視対象とするレプリカセットをセレクターで指定します。省略可です。省略した場合は全てのし セレクターは `<key>=<value>` の形式で指定してください。(例) app=nginx
コンテキスト	OpenShiftクラスタへの接続に利用するコンテキストを指定します。省略可です。省略した場合

- **OpenShift：レプリカセット別CPU使用率(%)**

  説明 OpenShiftのレプリカセット別CPU使用率を監視します。取得データはレプリカセットが持つ各Podの検査間隔期間内のCPUミリコア使用量の合計を各PodのCPU制限値の合計で割った値となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
設定ファイル	絶対パスで監視用の設定ファイルを指定します。省略可です。
ReplicaSet名	監視対象とするレプリカセットのレプリカセット名を指定します。省略可です。省略した場合は全
セレクター	監視対象とするレプリカセットをセレクターで指定します。省略可です。省略した場合は全てのし セレクターは `<key>=<value>` の形式で指定してください。(例) app=nginx
コンテキスト	OpenShiftクラスタへの接続に利用するコンテキストを指定します。省略可です。省略した場合

- **OpenShift：デーモンセット監視**

  説明 OpenShiftのデーモンセット情報を監視します。取得データは瞬間値となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
設定ファイル	絶対パスで監視用の設定ファイルを指定します。省略可です。
DaemonSet名	監視対象とするデーモンセットのデーモンセット名を指定します。省略可です。省略した場合は
セレクター	監視対象とするデーモンセットをセレクターで指定します。省略可です。省略した場合は全ての セレクターは `<key>=<value>` の形式で指定してください。(例) app=nginx
コンテキスト	OpenShiftクラスタへの接続に利用するコンテキストを指定します。省略可です。省略した場合

- **OpenShift：デーモンセット別CPU使用率(%)**

  説明 OpenShiftのデーモンセット別CPU使用率を監視します。取得データはデーモンセットが持つ各Podの検査間隔期間内のCPUミリコア使用量の合計を各PodのCPU制限値の合計で割った値となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
設定ファイル	絶対パスで監視用の設定ファイルを指定します。省略可です。
DaemonSet名	監視対象とするデーモンセットのデーモンセット名を指定します。省略可です。省略した場合は
セレクター	監視対象とするデーモンセットをセレクターで指定します。省略可です。省略した場合は全ての セレクターは `<key>=<value>` の形式で指定してください。(例) app=nginx
コンテキスト	OpenShiftクラスタへの接続に利用するコンテキストを指定します。省略可です。省略した場合

- **OpenShift：コンテナログ監視**

  説明 OpenShiftのコンテナログ情報を監視します。取得データは成否となります。

  パラメータ

パラメータ名	説明
◦ SSHアカウント ◦ SSHパスワード ◦ SSHポート番号 ◦ SSH認証方式 ◦ SSHパスフレーズ(公開鍵認証) ◦ SSH秘密鍵ファイル(公開鍵認証)	SSH接続による千手センサー監視を行う場合に使用します。パラメータの使用方法につきまし
設定ファイル	絶対パスで監視用の設定ファイルを指定します。省略可です。
セレクター	監視対象とするPodをセレクターで指定します。省略不可です。 セレクターは `<key>=<value>` の形式で指定してください。(例) app=nginx
コンテキスト	OpenShiftクラスタへの接続に利用するコンテキストを指定します。省略可です。省略した場合
ログフォーマット	取得したログの出力フォーマットをLTSVもしくはJSONに切り替えます。省略可です。省略した

注釈

- コンテナログ監視を利用する場合、対象のPodにラベルを設定する必要があります。
- 監視間隔内で監視対象Podに含まれるコンテナが再起動した場合、当該コンテナの再起動前のログを取得することはできません。
- コンテナログ監視では、最後に取得したログから5分間遡ってログを取得します。

警告

- 指定されたラベルセレクターの対象となるPodが存在しない場合、監視結果は正常となります。

5. Web Monitoring

5.1. はじめに

5.1.1. 本章について

- 本章では、Web監視(URL/外形監視)エクステンション の機能や使用方法について説明します。
- 「Senju DevOperation Conductor」は（株）野村総合研究所の登録商標です。
- Windows、Windows Server は、米国Microsoft Corporationの米国及びその他の国における登録商標または商標です。
- Linuxは、Linus Torvalds氏の登録商標です。
- Playwright は、米国Microsoft Corporationの米国及びその他の国における登録商標または商標です。
- その他、本誌で引用の製品名・会社名はそれぞれの会社の商標、もしくは登録商標です。なお、本誌中では、™、® マークなどは明記していません

5.1.2. 読者の対象

本章は Senju DevOperation Conductorのモニタリング機能からWebサービスを監視するシステム・アドミニストレータのためのものです。従って、本章の読者は以下のような概念に精通していることを前提にしています。

- Playwrightを利用したシナリオテスト実行
- Senju DevOperation Conductorの各種コンポーネント（千手ブラウザ、千手マネージャ、千手エージェント）
- Senju DevOperation Conductorのモニタリング機能
- オペレーティング・システムについての知識

5.1.3. 前提条件と関連資料

本章を参照するにあたっては、以下の各マニュアルなどを参照して下さい。

- 統合運用管理ツール「Senju DevOperation Conductor」リリースノート
- 統合運用管理ツール「Senju DevOperation Conductor」ユーザーズガイド
- Playwright Documentation(https://playwright.dev/docs/intro)

5.2. Web監視(URL/外形監視)の概要

Web監視(URL/外形監視)機能では、Webサイト・サービスを監視するために、以下の機能を提供します。

- HTTPリクエストに対するレスポンスボディの監視

図 5.1 Web監視(URL)の概要

- Webサイトへのアクセス時のレスポンスタイムおよび異常有無の監視

図 5.2 Web監視(外形監視)の概要

各種情報取得機能では、Senju DevOperation Conductorモニタリング機能を使用して、Webサーバー・サービスに対して定期的にデータ取得を行い、しきい値監視することが出来ます。（モニタリング機能については、**ユーザーズガイド「4．モニタリング」**を参照して下さい。）

また、Webサイトへのアクセス時のレスポンスタイムおよび異常有無の監視では、Playwrightを利用したテストスクリプトの実行結果を用いて監視を行います。

5.2.1. URL監視機能の概要

URL監視機能では、HTTPリクエストを送信してレスポンスボディを取得します。そのため、エージェント(プローブ)から対象のURLにアクセスできる必要があります。

取得可能な項目については、URL監視項目一覧 を参照してください。

5.2.2. 外形監視機能の概要

外形監視機能では、Playwrightのテストランナーを用いてテストスクリプトを実行し、その結果を取得します。そのため、エージェント(プローブ)にPlaywrightをインストールしている必要があります。

取得可能な項目については、外形監視項目一覧 を参照してください。

5.3. Web監視(URL)監視設定手順と使い方

URL監視設定を行う際には、以下の設定が必要になります。

- Senju DevOperation Conductor Extension Packの入手と適用

  運用管理サーバーおよび、レスポンスボディ監視を行う管理対象ノードに、同一バージョンの Senju DevOperation Conductor Extension Pack の適用が必要です
  - 運用管理サーバー(千手マネージャ)への適用(監視項目の更新)
  - 管理対象ノード(千手エージェント(プローブノード))への適用(情報取得コマンドの更新)

警告

適用可能な Senju DevOperation Conductor のバージョンやパッチ状況に制限がある場合があります。詳しくは、Senju DevOperation Conductor Extension Pack の README をご参照下さい。

参考

Senju DevOperation Conductor Extension Packの適用手順につきましては、Senju DevOperation Conductor Extension Pack の README をご参照下さい。

注釈

Senju DevOperation Conductor Extension Packの適用に際しては、千手システムの停止は不要ですが、関連する監視タスクの停止が必要です。

5.3.1. 設定

- **説明**

  モニタリングサブシステムを用いてURL監視項目を使用するための設定を行います。

- **設定手順**

  URL監視にてデフォルトの設定を変更するには以下の手順が必要です。
  - HTTPクライアント情報設定ファイルの作成

5.3.1.1. HTTPクライアント情報設定ファイル(sj_httpClient_conf.json)の作成

sj_httpClient_conf.jsonファイルは、HTTPクライアントに関する情報の設定ファイルです。

sj_httpClient_conf.jsonは「千手ホームディレクトリ/dat/opt/sj_httpClient_conf.json」に作成されます。

設定方法については、sj_setup_httpClient ー HTTPクライアント情報設定ファイル更新 ー を参照して下さい。

表 5.1 sj_httpClient_conf.jsonの記述内容

項目	省略	デフォルト	暗号化対象	説明
proxyURL	可	—	×	HTTPリクエスト送信時に経由するプロキシサーバー(次の形式で記載して下さい "<プロトコル>
proxyUsername	可	—	×	プロキシサーバーアクセス用ユーザーID
proxyPassword	可	—	○	プロキシサーバーアクセス用パスワード(暗号化後のパスワード)
retryCount	可	3	×	HTTPリクエストエラー時のリトライ回数
waitTime	可	30	×	HTTPリクエストのタイムアウト時間

- proxyURLを省略した場合、プロキシサーバーを利用しません。
- プロキシサーバーアクセス用ユーザーIDおよびパスワードの両方を指定しなかった場合、プロキシサーバーの認証に利用しません。

- sj_httpClient_conf.json の記載例

```
{
        "proxyURL": "http://ipアドレス:ポート番号",
        "proxyUsername": "",
        "proxyPassword": "",
        "retryCount": "",
        "waitTime": ""
}
```

5.3.1.1.1. sj_setup_httpClient ー HTTPクライアント情報設定ファイル更新 ー

- 指定形式
    - [参照]

      `sj_setup_httpClient`

    - [作成＆更新]

      ```
      sj_setup_httpClient
         [-purl[Proxy server via when connecting to http server]]
         [-puser[User ID for proxy server access]]
         [-ppswd[Password for proxy server access]]
         [-rc[number of retries when http request fails]]
         [-wt[wait time(seconds) when sending http request]]
      ```

- 目的

  HTTPクライアント情報設定ファイル(/dat/opt/sj_httpClient_conf.json) の現在値の参照、作成と更新を行います。

- オプション
    - -purl

      HTTPリクエスト送信時に経由するプロキシサーバー（proxyURL）に設定する値を指定して下さい。
      値を省略するとHTTPクライアント情報設定ファイルに設定されている値を削除します。

    - -puser

      プロキシサーバーのユーザー（proxyUsername）に設定する値を指定して下さい。
      値を省略するとHTTPクライアント情報設定ファイルに設定されている値を削除します。

    - -ppswd

      プロキシサーバーのパスワード（proxyPassword）に設定する値を指定して下さい。
      設定値の指定は対話形式で行われます。
      この項目は暗号化した値がHTTPクライアント情報設定ファイルに書き込まれます。

    - -rc

      HTTPリクエストエラー時のリトライ回数（retryCount）に設定する値を指定して下さい。
      値を省略するとHTTPクライアント情報設定ファイルに設定されている値を削除します。

    - -wt

      HTTPリクエストのタイムアウト時間（waitTime）に設定する値を指定して下さい。
      値を省略するとHTTPクライアント情報設定ファイルに設定されている値を削除します。

- 実行結果
    - (例1)現在の設定値参照

      ```
      % sj_setup_httpClient
      {
              "proxyURL": "",
              "proxyUsername": "",
              "proxyPassword": "",
              "retryCount": "",
              "waitTime": ""
      }
      ```

    - (例2)プロキシサーバーとユーザー、パスワードを設定

```
% sj_setup_httpClient -purlhttp://test.local:88 -pusersenju -ppswd
Please enter the value.
        "proxyPassword":

The value of proxyURL has changed from () to (http://test.local:88).
The value of proxyUsername has changed from () to (senju).
The value of proxyPassword has changed from (**********) to (**********).
The update is complete.

% sj_setup_httpClient
{
        "proxyURL": "http://test.local:88",
        "proxyUsername": "senju",
        "proxyPassword": "**********",
        "retryCount": "",
        "waitTime": ""
}
```

- (例3)設定を削除

```
% sj_setup_httpClient -purl -puser -ppswd
Please enter the value.
        "proxyPassword":

The value of proxyURL has changed from (http://test.local:88) to ().
The value of proxyUsername has changed from (senju) to ().
The value of proxyPassword has changed from (**********) to (**********).
The update is complete.

% sj_setup_httpClient
{
        "proxyURL": "",
        "proxyUsername": "",
        "proxyPassword": "",
        "retryCount": "",
        "waitTime": ""
}
```

注釈

- 暗号化対象項目の標準出力への表示は全てアスタリスクでマスクされます。
- 暗号化対象項目の値の設定は、キーボードからの入力が一切表示されません。コピー＆ペーストで入力することをお勧めします。
- 暗号化対象項目の値を削除する場合、何も入力せずにリターンキーを押下して下さい。

- エラー出力
  - Failed to acquire Senju home directory.
  - The http client configuration file does not exist.
  - Invalid data have been set in this file.
  - Failed to update the http client configuration file.
- 終了ステータス
  - 0：正常終了
  - 1：異常終了

5.3.2. 使い方

5.3.2.1. Webサイトコンテンツ監視機能

指定されたWebサイトに対してHTTPリクエストを送信し、得られたレスポンスボディからXPathで指定した値を取得し、Senju DevOperation Conductorのモニタリング機能を使って、監視することができます。

監視定義を千手ブラウザより登録し、監視を実施します。監視結果は、各種モニタ画面（グローバルノードモニタ／ノードモニタ）にてその監視状況を表示できます。予め設定したしきい値により障害を検知した場合は、メッセージモニタにメッセージが通知されます。
（モニタリング機能については、ユーザーズガイド「 **4．モニタリング** 」を参照して下さい。）

5.3.2.2. WebAPI応答監視機能

指定されたWebAPIサーバーに対してHTTPリクエストを送信し、得られた応答からJSONPathで指定した値を取得し、Senju DevOperation Conductorのモニタリング機能を使って、監視することができます。

監視定義を千手ブラウザより登録し、監視を実施します。監視結果は、各種モニタ画面（グローバルノードモニタ／ノードモニタ）にてその監視状況を表示できます。予め設定したしきい値により障害を検知した場合は、メッセージモニタにメッセージが通知されます。
（モニタリング機能については、ユーザーズガイド「 **4．モニタリング** 」を参照して下さい。）

5.3.2.3. 使用上の制限事項

- Webサイトコンテンツ監視にて、指定したXPathで取得可能な値が複数存在する場合は、最初の1件のみ出力します。
- WebAPI応答監視にて、指定したJSONPathで取得した値が文字列型の場合、ダブルクォート(")で囲まれた値が取得結果となります。
- データタイプに `x-www-form-urlencoded` を指定した場合、リクエストデータファイルには以下のフォーマットのファイルを指定してください。

```
key1=value1
key2=value2
```

- UNIX/Linuxの場合、XPath/JSONPathに指定するパラメータがスペース/ハイフンを含んでいない場合は、パラメータをダブルクォート(")で囲ってください。

5.4. Web監視(外形監視)監視設定手順と使い方

外形監視設定を行う際には、以下の設定が必要になります。

- Senju DevOperation Conductor Extension Packの入手と適用

  運用管理サーバーおよび、外形監視を行う管理対象ノードに、同一バージョンの Senju DevOperation Conductor Extension Pack の適用が必要です

  - 運用管理サーバー(千手マネージャ)への適用(監視項目の更新)
  - 管理対象ノード(千手エージェント(プローブノード))への適用(情報取得コマンドの更新)

警告

適用可能な Senju DevOperation Conductor のバージョンやパッチ状況に制限がある場合があります。詳しくは、Senju DevOperation Conductor Extension Pack の README をご参照下さい。

参考

Senju DevOperation Conductor Extension Packの適用手順につきましては、Senju DevOperation Conductor Extension Pack の README をご参照下さい。

注釈

Senju DevOperation Conductor Extension Packの適用に際しては、千手システムの停止は不要ですが、関連する監視タスクの停止が必要です。

5.4.1. 設定

- **説明**

  モニタリングサブシステムを用いて外形監視項目を使用するための設定を行います。

- **設定手順**

  外形監視を設定をするには以下の手順が必要です。

  - Playwrightの導入
  - 外形監視用千手設定ファイル(sj_synthetics_conf.json)の作成

5.4.1.1. Playwrightの導入

以下の手順はNode.jsがインストールされた環境で実施して下さい。Playwrightの稼働にはNode.js 14以降が必要です。

5.4.1.1.1. インストール

1. ログイン

   外形監視の設定を行うノードに、千手稼働アカウントでログインします。

2. Playwrightインストール

   Playwrightをインストールする任意のディレクトリに移動し、Playwrightをインストールします。

   以下は `D:\path\to\playwright` にPlaywrightをインストールする場合の例です。

   ```
   cd D:\path\to\playwright
   npm install @playwright/test@X.XX.X
   ```

   注釈

   XXXXには千手がサポートするPlaywrightのバージョンを指定して下さい。Playwrightのサポートバージョンについては、リリースノートに記載されている外形監視の稼働環境をご確認下さい。

3. Webブラウザインストール

以下コマンドにより、Playwrightで利用するWebブラウザをインストールします。

```
# chromium・firefox・webkitの3つをインストールする場合
npx playwright install

# chromiumのみをインストールする場合
npx playwright install chromium
```

4. 依存モジュールのインストール

以下コマンドにより、Playwrightの依存モジュールをインストールします。

```
# chromium・firefox・webkitの3つの依存モジュールをインストールする場合
npx playwright install-deps

# chromiumのみの依存モジュールをインストールする場合
npx playwright install-deps chromium
```

5.4.1.1.2. Playwright設定ファイル(playwright.config)の作成

Playwrightのテストランナー実行時にデフォルトで参照される設定ファイルを作成します。Playwrightの公式ドキュメントを参考に、設定ファイルを作成して下さい。

以下に、基本的な設定ファイル例(TypeScript)を記載します。

```
import { defineConfig, devices } from '@playwright/test';

export default defineConfig({
  // テストスクリプトの格納先ディレクトリ
  testDir: 'tests',

  // 全テストのパラレル実行
  fullyParallel: true,

  // Webブラウザごとのプロジェクト
  projects: [
    {
      name: 'chromium',
      use: { ...devices['Desktop Chrome'] },
    },
    {
      name: 'firefox',
      use: {
        ...devices['Desktop Firefox'],
      },
    },
    {
      name: 'webkit',
      use: {
        ...devices['Desktop Safari'],
      },
    },
  ],
});
```

注釈

- `projects` は必ず設定して下さい。監視タスクで指定するプロジェクト情報として参照されます。
- 作成した設定ファイルは、利用するテストスクリプトのスクリプトの種類に応じて、`playwright.config.ts` / `playwright.config.js` / `playwright.config.mjs` のいずれかのファイル名でPlaywrightをインストールしたプロジェクトディレクトリ下に格納して下さい。

参考

Playwright公式ドキュメント URL: https://playwright.dev/docs/test-configuration

5.4.1.1.3. テストスクリプトの準備

外形監視では、ユーザーが作成したテストスクリプトを実行することで監視を行います。

そのため、事前にテストスクリプトを手動で作成する必要があります。

Playwrightの公式ドキュメントを参考に、テストスクリプトを準備して下さい。

注釈

- テストスクリプトの作成には、Playwrightのコードジェネレータを利用することも可能です。
- 作成したテストスクリプトは、Playwright設定ファイル(playwright.config)の作成 で指定したテストディレクトリに格納して下さい。

参考

- Playwright公式ドキュメント URL: https://playwright.dev/docs/writing-tests
- Playwright CodeGen URL: https://playwright.dev/docs/codegen-intro

5.4.1.2. 外形監視用千手設定ファイル(sj_synthetics_conf.json)の作成

sj_synthetics_conf.jsonファイルは、千手での外形監視のための情報を設定するファイルです。外形監視の利用前に **必ず作成** して下さい。

sj_synthetics_conf.jsonは「千手ホームディレクトリ/dat/opt/sj_synthetics_conf.json」に作成します。

表 5.2 sj_synthetics_conf.jsonの記述内容

項目	省略	デフォルト	暗号化対象	説明
projectDir	不可	—	×	Playwrightをインストールしたプロジェクトディレクトリパス
trace.successGeneration	可	3	×	シナリオ実行成功時のtraceファイル保存世代数
trace.failedGeneration	可	10	×	シナリオ実行失敗時のtraceファイル保存世代数

- sj_synthetics_conf.json の記載例

```
{
  "projectDir": "D:\\path\\to\\playwright",
  "trace": {
    "successGeneration": 3,
    "failedGeneration": 10
  }
}
```

5.4.2. 使い方

5.4.2.1. 外形監視機能

Playwrightを利用したテストスクリプトの実行結果から、各ステップ・テストのレスポンスタイムやステータスを取得し、Senju DevOperation Conductorのモニタリング機能を使って、監視することができます。

監視定義を千手ブラウザより登録し、監視を実施します。監視結果は、各種モニタ画面（グローバルノードモニタ／ノードモニタ）にてその監視状況を表示できます。予め設定したしきい値により障害を検知した場合は、メッセージモニタにメッセージが通知されます。
（モニタリング機能については、ユーザーズガイド「 **4．モニタリング** 」を参照して下さい。）

5.4.2.1.1. トレースファイル

Playwrightにより作成されたトレースファイルは次の場所に保存されます。

保存世代数については、設定で変更可能です。詳細については 外形監視用千手設定ファイル(sj_synthetics_conf.json)の作成 を参照して下さい。

項目	内容
ディレクトリ名	`~/log/extension.d/synthetics/taskID_{監視タスクID}/`
ファイル名(テスト実行成功時)	`~/log/extension.d/synthetics/taskID_{監視タスクID}/success/YYYYMMDD-hhmmss/{テストスクリプト名}-{テ`
ファイル名(テスト実行失敗時)	`~/log/extension.d/synthetics/taskID_{監視タスクID}/fail/YYYYMMDD-hhmmss/{テストスクリプト名}-{テスト`

5.4.2.2. 使用上の制限事項

- Windowsでの監視の場合、プロキシサーバーを経由した監視を行うにはchromiumブラウザを利用する必要があります。
- 以下の動作は非対応です。
    - playwright.configでのテストのリトライ設定
    - 複数Webブラウザでの同時テスト

    - 実行対象テストスクリプトの複数指定

- LinuxノードでWebブラウザにwebkitを指定して監視を行う場合、Webブラウザのcoreファイルが作成されることがあります。
- サポート対象となるWebブラウザのバージョンについては、Playwrightのリリースノートを参照してください。
    - URL: https://playwright.dev/docs/release-notes

5.5. 付録

5.5.1. 監視項目

5.5.1.1. URL監視項目一覧

- **Webサイトコンテンツ監視(文字列)**

  説明 URLのレスポンスボディ(DOM)を監視します。閾値判定は文字列として行います。XPathで指定した対象を監視します。

  パラメータ

パラメータ名	説明
URL	監視対象となるWebサイトのURLを指定します。省略不可です。
HTTPメソッド	HTTPリクエスト送信時のメソッド(GET/POST)を指定します。省略可です。省略した場合はGETが有効になりま
認証用ヘッダー	認証用のヘッダーを利用する場合に指定します。省略可です。指定する場合は、ヘッダー名も含めて指定して下
リクエストヘッダーファイル	任意のHTTPリクエストヘッダーを利用する場合に指定します。省略可です。指定する場合は、JSONフォーマット
データタイプ	HTTPメソッドにPOSTを指定した場合のリクエストデータの送信方式(raw/x-www-form-urlencoded)を指定しま
リクエストデータファイル	HTTPメソッドにPOSTを指定した場合に送信するリクエストデータを指定します。省略可です。
基本認証ユーザー名	Webサイトへのアクセスに基本認証を利用する場合はユーザー名を指定します。省略可です。
基本認証パスワード	Webサイトへのアクセスに基本認証を利用する場合はパスワードを指定します。省略可です。
XPath	レスポンスボディから取得する対象のXPathを指定します。省略不可です。

  注釈

  - Webサイトコンテンツ監視(文字列)は、URLに指定されたWebページのみの取得を行います。フレームやリンク先、ページ内の画像などの取得は行いません。
  - 取得データのcharsetの値により文字コードを判断します。UTF-8のほか、Shift_JIS、EUC-JPに対応しています。
  - データタイプにrawを指定した場合、リクエストデータファイルの内容をそのままリクエストデータとして送信します。
  - データタイプにx-www-form-urlencodedを指定した場合、リクエストデータファイルのキー・バリュー型のデータをURLエンコードして送信します。指定フォーマットについては、 使用上の制限事項 を参照して下さい。

- **Webサイトコンテンツ監視(数値)**

  説明 URLのレスポンスボディ(DOM)を監視します。閾値判定は数値として行います。XPathで指定した対象を監視します。

  パラメータ

パラメータ名	説明
URL	監視対象となるWebサイトのURLを指定します。省略不可です。
HTTPメソッド	HTTPリクエスト送信時のメソッド(GET/POST)を指定します。省略可です。省略した場合はGETが有効になりま
認証用ヘッダー	認証用のヘッダーを利用する場合に指定します。省略可です。指定する場合は、ヘッダー名も含めて指定して下
リクエストヘッダーファイル	任意のHTTPリクエストヘッダーを利用する場合に指定します。省略可です。指定する場合は、JSONフォーマット
データタイプ	HTTPメソッドにPOSTを指定した場合のリクエストデータの送信方式(raw/x-www-form-urlencoded)を指定しま
リクエストデータファイル	HTTPメソッドにPOSTを指定した場合に送信するリクエストデータを指定します。省略可です。
基本認証ユーザー名	Webサイトへのアクセスに基本認証を利用する場合はユーザー名を指定します。省略可です。
基本認証パスワード	Webサイトへのアクセスに基本認証を利用する場合はパスワードを指定します。省略可です。
XPath	レスポンスボディから取得する対象のXPathを指定します。省略不可です。

  注釈

  - Webサイトコンテンツ監視(数値)は、URLに指定されたWebページのみの取得を行います。フレームやリンク先、ページ内の画像などの取得は行いません。
  - データタイプにrawを指定した場合、リクエストデータファイルの内容をそのままリクエストデータとして送信します。
  - データタイプにx-www-form-urlencodedを指定した場合、リクエストデータファイルのキー・バリュー型のデータをURLエ

ンコードして送信します。指定フォーマットについては、使用上の制限事項 を参照して下さい。

- 取得データのうち、カンマは除去されます。

警告

- 取得結果が数値でない場合、監視結果は異常となります。

- **WebAPI応答監視(文字列)**

  説明 URLのレスポンスボディ(JSON)を監視します。閾値判定は文字列として行います。JSONPathで指定した対象を監視します。

  パラメータ

パラメータ名	説明
URL	監視対象となるWebAPIエンドポイントを指定します。省略不可です。
HTTPメソッド	HTTPリクエスト送信時のメソッド(GET/POST)を指定します。省略可です。省略した場合はGETが有効になりま
認証用ヘッダー	認証用のヘッダーを利用する場合に指定します。省略可です。指定する場合は、ヘッダー名も含めて指定して下
リクエストヘッダーファイル	任意のHTTPリクエストヘッダーを利用する場合に指定します。省略可です。指定する場合は、JSONフォーマット
データタイプ	HTTPメソッドにPOSTを指定した場合のリクエストデータの送信方式(raw/x-www-form-urlencoded)を指定しま
リクエストデータファイル	HTTPメソッドにPOSTを指定した場合に送信するリクエストデータを指定します。省略可です。
基本認証ユーザー名	WebAPIサーバーへのアクセスに基本認証を利用する場合はユーザー名を指定します。省略可です。
基本認証パスワード	WebAPIサーバーへのアクセスに基本認証を利用する場合はパスワードを指定します。省略可です。
JSONPath	レスポンスボディから取得する対象のJSONPathを指定します。省略不可です。

注釈

- 取得データのcharsetの値により文字コードを判断します。UTF-8のほか、Shift_JIS、EUC-JPに対応しています。
- データタイプにrawを指定した場合、リクエストデータファイルの内容をそのままリクエストデータとして送信します。
- データタイプにx-www-form-urlencodedを指定した場合、リクエストデータファイルのキー・バリュー型のデータをURLエンコードして送信します。指定フォーマットについては、使用上の制限事項 を参照して下さい。

- **WebAPI応答監視(数値)**

  説明 URLのレスポンスボディ(JSON)を監視します。閾値判定は数値として行います。JSONPathで指定した対象を監視します。

  パラメータ

パラメータ名	説明
URL	監視対象となるWebAPIエンドポイントを指定します。省略不可です。
HTTPメソッド	HTTPリクエスト送信時のメソッド(GET/POST)を指定します。省略可です。省略した場合はGETが有効になりま
認証用ヘッダー	認証用のヘッダーを利用する場合に指定します。省略可です。指定する場合は、ヘッダー名も含めて指定して下
リクエストヘッダーファイル	任意のHTTPリクエストヘッダーを利用する場合に指定します。省略可です。指定する場合は、JSONフォーマット
データタイプ	HTTPメソッドにPOSTを指定した場合のリクエストデータの送信方式(raw/x-www-form-urlencoded)を指定しま
リクエストデータファイル	HTTPメソッドにPOSTを指定した場合に送信するリクエストデータを指定します。省略可です。
基本認証ユーザー名	WebAPIサーバーへのアクセスに基本認証を利用する場合はユーザー名を指定します。省略可です。
基本認証パスワード	WebAPIサーバーへのアクセスに基本認証を利用する場合はパスワードを指定します。省略可です。
JSONPath	レスポンスボディから取得する対象のJSONPathを指定します。省略不可です。

注釈

- データタイプにrawを指定した場合、リクエストデータファイルの内容をそのままリクエストデータとして送信します。
- データタイプにx-www-form-urlencodedを指定した場合、リクエストデータファイルのキー・バリュー型のデータをURLエンコードして送信します。指定フォーマットについては、使用上の制限事項 を参照して下さい。

警告

- 取得結果が数値でない場合、監視結果は異常となります。

5.5.1.2. 外形監視項目一覧

- **Synthetics:ステップ別レスポンスタイム**

  説明 シナリオの各ステップの実行時間を監視します。単位はミリ秒です。

パラメータ

パラメータ名	説明
テストフィルタ	実行するテストスクリプトをファイル名で指定します。省略不可です。指定例：sample.spec.ts
プロジェクト名	Playwrightのプロジェクトを指定します。省略不可です。
設定ファイル	Playwrightの設定ファイルをファイル名で指定します。省略可です。省略した場合、デフォルトの設定ファイルを利用します。
テスト名	テストスクリプト内のテスト名を指定します。省略可です。省略した場合、テストスクリプト内の全てのテストを実行します。
行番号	監視結果として取得するステップをテストスクリプトの行番号で指定します。省略可です。

注釈

- テストフィルタは テストスクリプトの準備 で格納したものを指定して下さい。
- 指定する設定ファイルは 外形監視用千手設定ファイル(sj_synthetics_conf.json)の作成 で指定したプロジェクトディレクトリ下に配置されている必要があります。

- **Synthetics：テスト別レスポンスタイム**

  説明 シナリオの各テストの実行時間を監視します。単位は秒です。

  パラメータ

パラメータ名	説明
テストフィルタ	実行するテストスクリプトをファイル名で指定します。省略不可です。指定例：sample.spec.ts
プロジェクト名	Playwrightのプロジェクトを指定します。省略不可です。
設定ファイル	Playwrightの設定ファイルをファイル名で指定します。省略可です。省略した場合、デフォルトの設定ファイルを利用します。
テスト名	テストスクリプト内のテスト名を指定します。省略可です。省略した場合、テストスクリプト内の全てのテストを実行します。
行番号	監視結果として取得するステップをテストスクリプトの行番号で指定します。省略可です。

注釈

- テストフィルタは テストスクリプトの準備 で格納したものを指定して下さい。
- 指定する設定ファイルは 外形監視用千手設定ファイル(sj_synthetics_conf.json)の作成 で指定したプロジェクトディレクトリ下に配置されている必要があります。

- **Synthetics：シナリオテストコンプリート**

  説明 シナリオの各テストを実行した時のステータスを監視します。

  パラメータ

パラメータ名	説明
テストフィルタ	実行するテストスクリプトをファイル名で指定します。省略不可です。指定例：sample.spec.ts
プロジェクト名	Playwrightのプロジェクトを指定します。省略不可です。
設定ファイル	Playwrightの設定ファイルをファイル名で指定します。省略可です。省略した場合、デフォルトの設定ファイルを利用します。
テスト名	テストスクリプト内のテスト名を指定します。省略可です。省略した場合、テストスクリプト内の全てのテストを実行します。
行番号	監視結果として取得するステップをテストスクリプトの行番号で指定します。省略可です。

注釈

- テストフィルタは テストスクリプトの準備 で格納したものを指定して下さい。
- 指定する設定ファイルは 外形監視用千手設定ファイル(sj_synthetics_conf.json)の作成 で指定したプロジェクトディレクトリ下に配置されている必要があります。

6. CCMS Monitoring for mySAP

6.1. はじめに

6.1.1. 本章について

- CCMS Monitoring for mySAP 使用者の手引きは、CCMS Monitoring for mySAP の機能や使用方法について説明します。
- CCMS Monitoring for mySAP はmySAPシステムのCCMS機能とSenju DevOperation Conductorのモニタリング機能を連携させることができます。この連携により、Senju DevOperation Conductorのモニタリング機能からmySAPシステムを監視することができるようになります。
- 「Senju DevOperation Conductor」「Senju Operation Conductor」「Senju Enterprise Navigator」「eXsenju」「EX千手/EXSENJU」「千手/SENJU」「e-千手/e-SENJU」および「セキュア・キューブ/SecureCube」は（株）野村総合研究所の登録商標です。
- SAP、R/3、mySAP、ABAPは、SAP AGのドイツ及びその他の国における登録商標または商標です。
- UNIXは、X/Open Company Limitedが独占的にライセンスしている米国ならびに他の国における登録商標です。
- Linuxは、Linus Torvalds氏の登録商標です。
- Windows、Windows Serverは、米国Microsoft Corporationの米国及びその他の国における登録商標または商標です。
- その他、本誌で引用の製品名・会社名はそれぞれの会社の商標、もしくは登録商標です。なお、本誌中では、™、® マークなどは明記していません。

6.1.2. 読者の対象

本章はCCMS Monitoring for mySAP を利用して、Senju DevOperation Conductorのモニタリング機能からmySAP システムを監視するシステム・アドミニストレータのためのものです。従って、本章の読者は以下のような概念に精通していることを前提にしています。

- mySAPシステム CCMS（Computing Center Management System）
- Senju DevOperation Conductorの各種コンポーネント（千手ブラウザ、千手マネージャ、千手エージェント）
- Senju DevOperation Conductorのモニタリング機能
- オペレーティング・システムについての知識

6.1.3. 前提条件と関連資料

本章を参照するにあたっては、以下の各マニュアルなどを参照して下さい。

- 統合運用管理ツール「Senju DevOperation Conductor」リリースノート
- 統合運用管理ツール「Senju DevOperation Conductor」ユーザーズマニュアル
- ERP（管理業務統合）ソフト「mySAP ERP」

6.2. CCMS Monitoring for mySAPの概要

CCMS Monitoring for mySAP 機能では、mySAPシステム上のCCMSと連携し、mySAPシステムを監視するために、以下の機能を提供します。

- アラート取得／確認
- パフォーマンスデータ監視

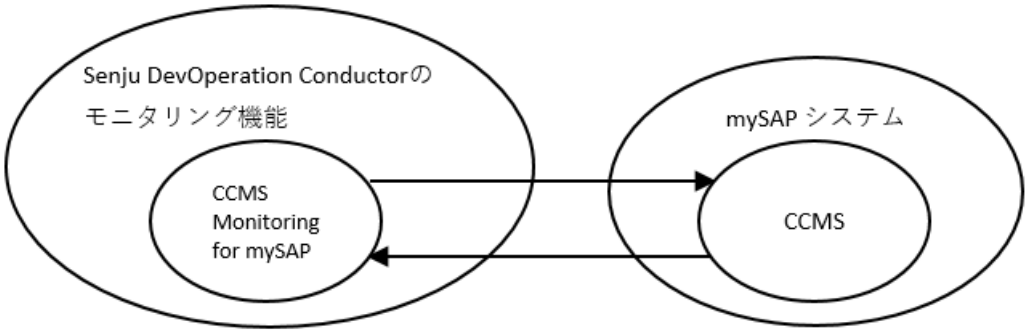


図 6.1 Senju DevOperation ConductorとmySAPシステム CCMS との連携

アラート取得機能では、接続したmySAPシステムのデスティネーション上で発生した全てのアラートを取得し、ログファイルにテキスト形式で蓄積します。また、Senju DevOperation Conductorのテキストログ監視を利用して、mySAPシステム上で発生したアラートをメッセージモニタに表示させる事が出来ます。発生したアラートは、Senju DevOperation Conductor側より、mySAPシステムに対し、確認することも出来ます。

パフォーマンスデータ監視機能では、Senju DevOperation Conductorモニタリング機能を使用して、定期的にデータ取得を行い、しきい値監視することが出来ます。（モニタリング機能については、**ユーザーズマニュアル「４．モニタリング」**を参照して下さい。）

CCMS Monitoring for mySAP機能は、mySAPシステムと接続する際、mySAPシステムに関する情報をsaprfc.iniファイルから取得します。そのため、CCMS Monitoring for mySAP機能を使用する前にsaprfc.iniファイルを設定しておく必要があります。（saprfc.iniについては、「saprfc.iniの設定」を参照して下さい。）

また、CCMS Monitoring for mySAP機能を使用するためには、千手エージェント（プローブ）上にて、「mySAPシステム監視設定」を行う必要があります。（mySAPシステム監視用設定については、「mySAPシステム監視設定」を参照して下さい。）

6.3. mySAPシステム監視設定手順

6.3.1. saprfc.iniの設定

saprfc.iniファイルは、mySAPシステムに関する情報が書かれたファイルで、CCMS Monitoring for mySAP機能はこのファイルを参照します。
saprfc.iniファイルは、UNIXの場合は、稼働するエージェント上の$SENJUHOME/dat/pex/sapディレクトリ、Windowsの場合は、%SENJUHOME%\dat\pex\sapディレクトリに存在する必要があります。(初期インストール時には saprfc.iniファイルのひな型(saprfc.ini.sample)を置いてあります。)saprfc.iniに、表 6.1 saprfc.iniの記述内容 に示す内容を記述して下さい。
(項目の詳細内容は、お客様の環境のmySAPシステム管理者にお尋ね下さい。)

表 6.1 saprfc.iniの記述内容

項目	例	説明
DEST=	R3SRV1	デスティネーション
TYPE=	A	Senju DevOperation Conductorシステムではパラメータに'A'を指定して下さい
ASHOST=	r3server1	TYPEが'A'のとき、接続するmySAPシステム名
SYSNR=	00	TYPEが'A'のとき、システム番号[00-99]
GWSERV=	3300	TYPEが'A'のとき、サービスのポート番号(※)
RFC_TRACE=	0	Senju DevOperation Conductorシステムではパラメータに'0'を指定して下さい

- デスティネーションには、大文字のアルファベットと数字を組み合わせて32文字までで自由な名前をつけることができます。ここで指定したデスティネーションを、mySAPシステム監視設定で指定します。

注釈

サービスのポート番号の上2桁は"33"で、下2桁はシステム番号になります。(例) SYSNR=02のとき、GWSERV=3302

(例)

- DEST=R3SRV1
- TYPE=A
- ASHOST=r3server1
- SYSNR=00
- GWSERV=3300
- RFC_TRACE=0

(例)

- DEST=R3SRV2
- TYPE=A
- ASHOST=r3server2
- SYSNR=02
- GWSERV=3302
- RFC_TRACE=0

6.3.2. mySAPシステム監視設定

mySAPシステム監視の為の設定を行います。
設定された値は、アラート取得や確認、パフォーマンスデータ監視にて、デフォルト値として使用します。

6.3.2.1. sj_setup_ccms コマンドの起動

千手エージェントに千手稼働アカウントでログインして下さい。
Unix の場合は、"sj_setup_ccms.com"と入力して下さい。

Windows の場合は、コマンドプロンプトを起動し、”sj_setup_ccms.cmd”と入力して下さい。
本コマンドは、日本語メッセージを出力しますので、日本語環境から実行して下さい。
以下のような「mySAPシステム監視用設定メインメニュー」画面が出てきます。

```
----- mySAPシステム監視用設定メインメニュー -----
1  mySAPシステム監視用設定情報 [現在値の参照]
2  監視する デスティネーションの設定
3  接続する mySAP ユーザ名の設定
4  接続する mySAP パスワードの設定
5  接続する mySAP ログイン言語の設定
6  接続する mySAP クライアント番号の設定
7  接続する mySAP XMI 監視レベルの設定

9  終了(設定結果反映)

番号を入力して下さい >>
```

警告

この設定コマンドは、同時に実行しないようにして下さい。
正しく設定出来ない可能性があります。

6.3.2.2. 監視する デスティネーションの設定

インメニューで、”2”入力をして、監視する デスティネーションを設定します。

```
----- 監視する デスティネーションの設定 -----

監視する デスティネーションの設定(現在値) : 未設定


 監視する デスティネーションを入力して下さい (省略不可) >> SAMPLE

監視する デスティネーション = SAMPLE

 よろしいですか?(y/n) >> y

SAMPLE を監視する デスティネーションとして設定しました。
```

「監視する デスティネーションの設定」画面が出てきますので、デスティネーションを入力して設定し、正しい場合は「y」を入力して下さい。

注釈

デスティネーションは、saprfc.iniに記述されているデスティネーションを指定して下さい。(saprfc.iniについては、「saprfc.iniの設定」を参照して下さい。)

6.3.2.3. 接続する mySAP ユーザ名の設定

メインメニューで、”3”入力をして、接続する mySAP ユーザ名を設定します。

```
----- 接続する mySAP ユーザ名の設定 -----

接続する mySAP ユーザ名の設定(現在値) : 未設定


 接続する mySAP ユーザ名を入力して下さい (省略不可) >> senju

接続する mySAP ユーザ名 = senju

 よろしいですか?(y/n) >> y

senjuを接続する mySAP ユーザ名として設定しました。
```

「接続する mySAP ユーザ名の設定」画面が出てきますので、ユーザ名を入力して設定し、正しい場合は「y」を入力して下さい。

6.3.2.4. 接続する mySAP パスワードの設定

メインメニューで、”4”入力をして、接続する mySAP パスワードを設定します。

```
----- 接続する mySAP パスワードの設定 -----
接続する mySAP パスワードの設定(現在値) : 未設定

 接続する mySAP パスワードを入力して下さい (省略不可) >> senju99
接続する mySAP パスワード = senju99
 よろしいですか？(y/n) >> y
senju99 を接続する mySAP パスワードとして設定しました。
```

「接続する mySAP パスワードの設定」画面が出てきますので、パスワードを入力して設定し、正しい場合は「y」を入力して下さい。

注釈

SAP ERP(RFC SDK 7.20)用監視機能に限り、指定可能なパスワード文字列長は40です。これにより、SAP NetWeaver6.40以降のSAPサーバーに接続できます。

6.3.2.5. 接続する mySAP ログイン言語の設定

メインメニューで、"5"入力をして、mySAP ログイン言語を設定します。

```
----- 接続する mySAP ログイン言語の設定 -----
接続する mySAP ログイン言語の設定(現在値) : 未設定

 接続する mySAP ログイン言語(J:日本語,E:英語,D:独語)を入力して下さい (省略可:E) >> E
接続する mySAP ログイン言語 = E
 よろしいですか？(y/n) >> y
E を接続する mySAP ログイン言語として設定しました。
```

「接続する mySAP ログイン言語の設定」画面が出てきますでmySAP ログイン言語(J:日本語,E:英語,D:独語)を入力して設定し、正しい場合は「y」を入力して下さい。

6.3.2.6. 接続するクライアント番号の設定

メインメニューで、"6"入力をして、mySAPクライアント番号を設定します。

```
----- 接続する mySAP クライアント番号の設定 -----
接続する mySAP クライアント番号の設定(現在値) : 未設定

 接続する mySAP クライアント番号(000 ～ 999)を入力して下さい (省略不可) >> 800
接続する mySAP クライアント番号 = 800
 よろしいですか？(y/n) >> y
800 を接続する mySAP クライアント番号として設定しました。
```

「接続する mySAPクライアント番号の設定」画面が出てきますでmySAPクライアント番号(000～999)を入力して設定し、正しい場合は「y」を入力して下さい。

警告

ユーザ名、パスワード、ログイン言語、クライアント番号については、mySAPシステムにログオンする際、入力する内容と同じものを指定して下さい。

6.3.2.7. 接続するXMI 監視レベルの設定

メインメニューで、"7"入力をして、mySAP XMI 監視レベルを設定します。

```
----- 接続する mySAP XMI 監視レベルの設定 -----

接続する mySAP XMI 監視レベル号の設定(現在値) : 未設定

 接続する mySAP XMI 監視レベル(0-3)を入力して下さい (省略可:0) >> 0

接続する mySAP XMI 監視レベル = 0

 よろしいですか？(y/n) >> y

0 を接続する mySAP XMI 監視レベルとして設定しました。
```

「接続する mySAP XMI 監視レベルの設定」画面が出てきますのでmySAP XMI 監視レベル(0-3)を入力して設定し、正しい場合は「y」を入力して下さい。

注釈

XMIとは、SAP Application Serverとサードベンダのアプリケーションが通信を行う上での通信レイヤのことです。

XMI監視レベルは0から3の4つのうちから選択可能です。大きな数字を設定するに従い、より詳細なログが出力され出力量が増大します。

0:データを変更するAPIを実行するときに出力されるレベル

1:読みとりを行うAPIの実行に失敗したときに出力されるレベル

2:読みとりを行うAPIを実行するときに出力されるのレベル

3:APIの開始時/APIの終了時に出力されるレベル

負荷を軽減する場合には、0を設定してください。

6.3.2.8. 設定結果反映

メインメニューで、"9"入力をして、設定結果を反映します。

```
----- mySAPシステム監視用設定メインメニュー -----
1  mySAPシステム監視用設定情報 [現在値の参照]
2  監視する デスティネーションの設定
3  接続する mySAP ユーザ名の設定
4  接続する mySAP パスワードの設定
5  接続する mySAP ログイン言語の設定
6  接続する mySAP クライアント番号の設定
7  接続する mySAP XMI 監視レベルの設定

9  終了(設定結果反映)

番号を入力して下さい >> 9

設定結果をファイルに反映しました。
```

設定結果が反映され、終了します。

6.3.2.9. 設定後の作業

千手を再起動します。
mySAP監視の為の設定は、以上で終了です。

6.4. CCMS Monitoring for mySAPの使い方

6.4.1. アラート取得機能

アラート取得機能は、アラート取得デーモンプロセスにて、mySAPシステム CCMS上に発生したアラートを定期的に取得し、ログファイルへの蓄積を行います。 収集したアラートを解析または監視することにより、mySAPシステムの状況を把握することができます。

6.4.1.1. アラートログファイル

取得したアラートは、千手エージェント（プローブ）上の次のログファイルに、テキスト形式で蓄積されます。

- 【UNIX/Linux】

  ```
  $SENJUHOME/log/sjANM_ccmsAlert.log
  ```

- 【Windows】

  ```
  %SENJUHOME%\log\sjANM_ccmsAlert.log
  ```

このファイルは、2MB を超えると、自動的に切り替えられ、新しいログ情報ファイルが作成されます。

古いログ情報ファイルは、”sjANM_ccmsAlert.log.1”のファイル名で保存されます。以降、”sjANM_ccmsAlert.log.2”、”sjANM_ccmsAlert.log.3・・・”へ保存され、最大”sjANM_ccmsAlert.log.7”まで7 世代分のファイルが保存されます。7 世代より前のファイルは順次削除されます。

6.4.1.2. アラート情報

以下に、1 アラート情報のレコード形式について説明します。レコードの各項目間はスペース、コロンで区切られています。

【アラートログファイル レコード形式】
取得日付 取得時刻 : アラート発生日付 アラート発生時刻 レベル AID[AID(Alert ID)] TID[TID(MTE ID)] Severity[重要度] Status[ステータス] : メッセージ (Set:モニタセット名)(Name:モニタ名)

表 6.2 アラートログレコード形式

カラム位置	項目	説明
1,2	取得日付 取得時刻	プローブ上で、アラートを受信した日付、時刻です。
3,4	アラート発生日付 アラート発生時刻	mySAPシステム上の、アラートが発生した日付、時刻です。 アラート確認コマンドにて、指定します。
5	レベル	アラートレベルで、以下のように対応しています。 ・ERR = エラー ・WRN = ワーニング
6	AID	アラートのIDです。 アラート確認コマンドにて、指定します。
7	TID	アラートが発生したMTEのIDです。
8	重要度	アラートの重要度を示す値です
9	ステータス	アラートの重要度を示す値です
10	メッセージ	アラートの内容を示すメッセージです。
11	モニタセット名	アラートを取得したモニタセット名です。
12	モニタ名	アラートを取得したモニタ名です。

6.4.1.3. アラート監視運用例

以下にSenju DevOperation Conductorのテキストログ監視を利用して、mySAPシステムのアラート発生を監視する運用例を示します。この例では、エラー及びワーニングの発生時にメッセージモニタに通知されるようにログフィルタを登録し、監視する場合について説明します。

＜ログフィルタの登録＞
千手ブラウザのツリービューで＜ドメイン＞→“フィルタ”→“ログフィルタ”を選択します。ログフィルタのエンティティでリストビューの何も表示されていない部分でマウスの右ボタンを押してコンテキストメニューを表示し、[新規作成]メニューを選択します。ログフィルタのプロパティが表示されます。

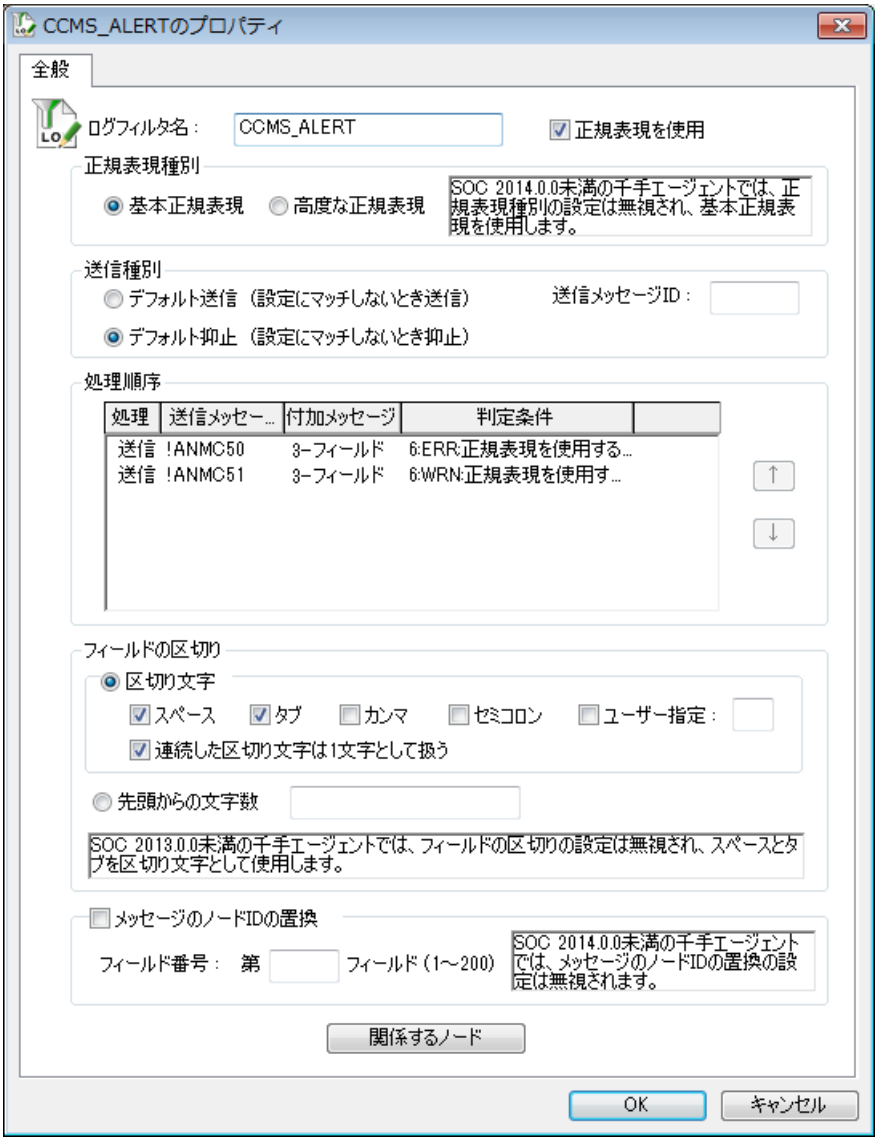


図 6.2 ログフィルタのプロパティ

ログフィルタ名などの各項目を入力し[OK]ボタンを押下します。これにより、ログフィルタの登録が完了します。

＜フィルタ監視項目の追加＞

千手ブラウザのツリービューの＜ドメイン＞→“フィルタ”→“ログフィルタ”→＜ログフィルタ＞でフィルタ監視項目を登録するログフィルタを選択し、リストビューの何も表示されていない部分でマウスの右ボタンを押してコンテキストメニューを表示し、[新規作成]メニューを選択します。フィルタ監視項目のプロパティが表示されますので、エラーとワーニング発生を監視するためフィールド6番目を文字列”ERR”と”WRN”で監視設定し、通知したいメッセージIDを登録します。

アラート（エラー）には、メッセージID“!ANMC50”、アラート（ワーニング）には、メッセージID“!ANMC51”を使用してください。また、付加メッセージには、3フィールド以降を設定してください。

以下はログフィルタの登録後のフィルタ監視項目です。

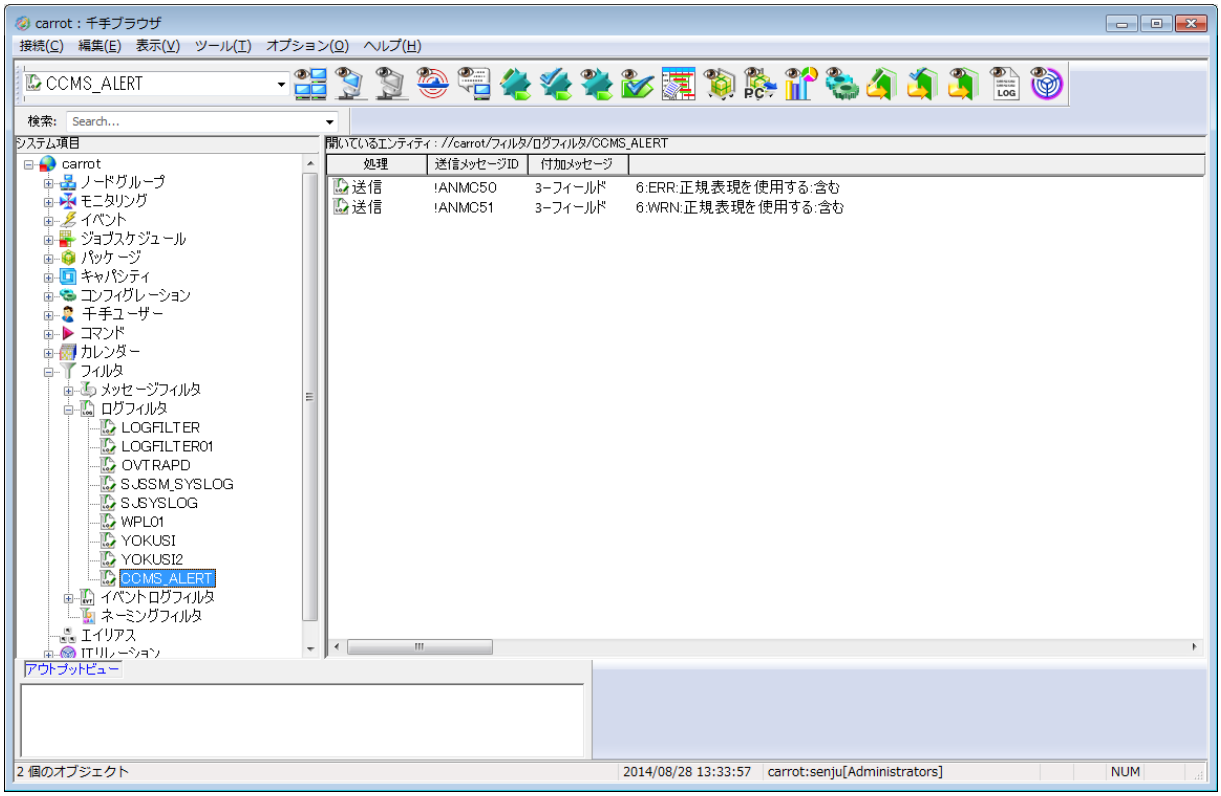


図 6.3 ログフィルタ登録例

＜テキストログ監視の設定＞

アラートファイルのテキストログ監視を行うには、千手ブラウザのツリービューで、＜ドメイン＞→“ノードグループ”→＜ノードグループ＞を選択し、そのリストビューからmySAP監視のプローブとして設定したノードを選択し、マウスの右ボタンをクリックしコンテキストメニューを表示し、[プロパティ]メニューを選択します。ノードのプロパティウィンドウが表示されますので、[ログ監視]タブを選択します。

ノードのプロパティ（[ログ監視]タブ）にて、監視対象のパス名とファイル名にアラートログファイルを指定し、監視方法に先に作成したログフィルタを指定します。以下はログ監視を登録した後の、ノードのプロパティ（[ログ監視]タブ）です。

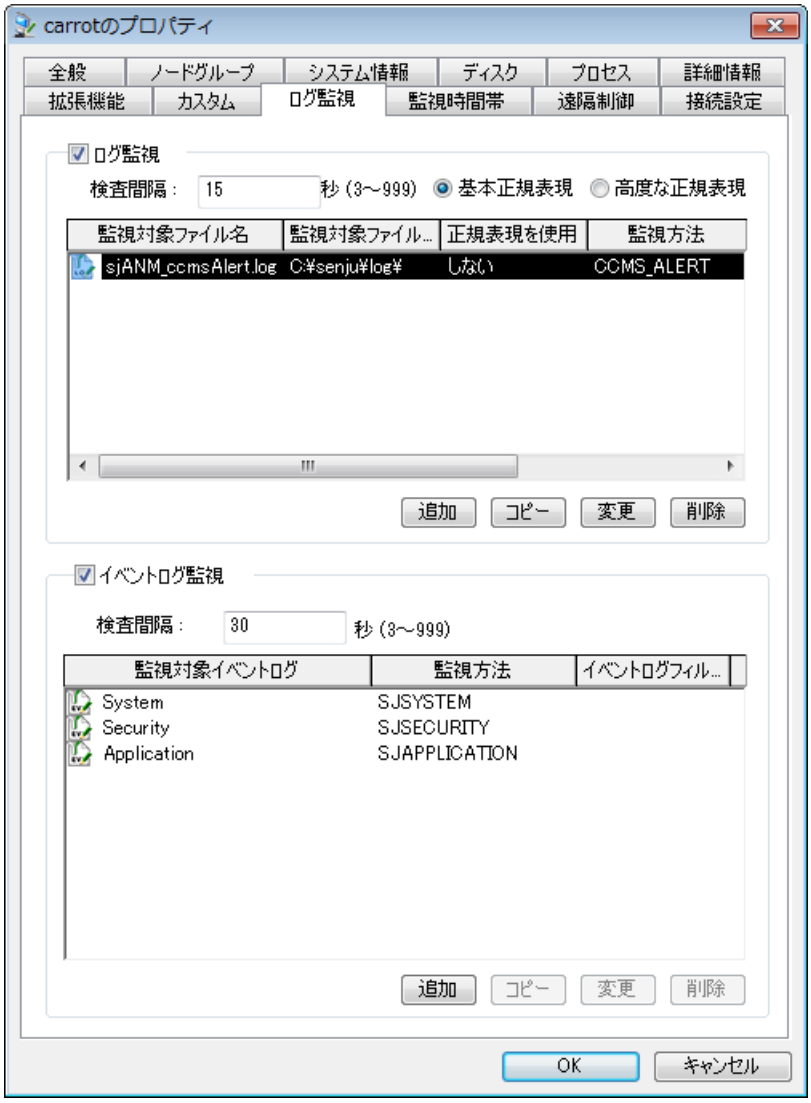


図 6.4 ログ監視登録例

ログ監視を登録した後に、登録したノードに対して[反映(監視属性)]を実行することにより、ログファイルの監視を開始します。
以上で、ログ監視を用いたmySAPシステム アラート監視の設定は完了です。この設定によりmySAPシステムにアラートが発生した場合、メッセージモニタに通知されます。

警告

管理対象ノードにおいて千手が起動していない状態で、[反映(監視属性)]を行うと失敗しますので、注意して下さい。

6.4.1.4. 取得アラートの制限

次のファイルパスのモニタセット名を記述したテキストファイルを作成することで、取得するアラートをモニタセット単位で制限することができます。

- 【UNIX/Linux】

  ```
  $SENJUHOME/dat/mon/sap/sjANM_ccmsAlrtMonSet.def
  ```

- 【Windows】

  ```
  %SENJUHOME%\\dat\\mon\\sap\\sjANM_ccmsAlrtMonSet.def
  ```

sjANM_ccmsAlrtMonSet.defをテキストエディタで開き、例のようにモニタセット名を1行ずつ記述して指定します。(最大100個まで指定できます。)

（例）
モニタセットA
モニタセットB
モニタセットC

警告

sjANM_ccmsAlrtMonSet.defに同じモニタを持つ異なる名前のモニタセットを設定しても、重複したアラートは取得されません。重複したアラートを取得する場合は、次のsjANM_ccms.defファイルをテキストエディタで開き、「FILTER=ALL」と記述されている部分を「FILTER=FILTERD」に書き換えて下さい。

- **【UNIX/Linux】**

```
$SENJUHOME/dat/mon/sap/sjANM_ccms.def
```

- **【Windows】**

```
%SENJUHOME%\\dat\\mon\\sap\\sjANM_ccms.def
```

6.4.2. アラート確認機能

mySAPシステム上で発生したアラートを、Senju DevOperation Conductor側より、確認することが出来ます。

6.4.2.1. アラート確認コマンド実行

千手ブラウザのツリービューの＜ドメイン＞→“コマンド”→“千手コマンド”→“モニタリング”より、「mySAPアラートメッセージ確認」コマンドを選択して実行します。（千手コマンドについては、ユーザーズマニュアル「 **千手コマンド** 」を参照して下さい。）

- アラート日付には、メッセージモニタに表示されたアラート発生日付を、アラート時刻には、アラート発生時刻を、アラートIDには、AID(Alert ID)を指定し、実行してください。
- デスティネーション、クライアント、mySAPユーザー名、mySAPパスワードは、省略可能です。

  省略時には、mySAPシステム監視設定で設定した値を使用します。（mySAPシステム監視用設定については、「mySAPシステム監視設定」を参照して下さい。）

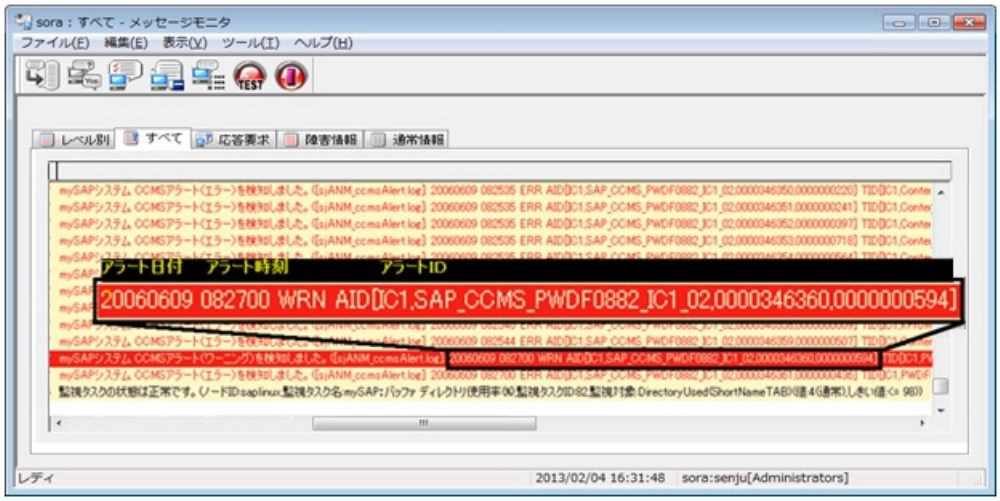


図 6.5 アラートメッセージ表示例

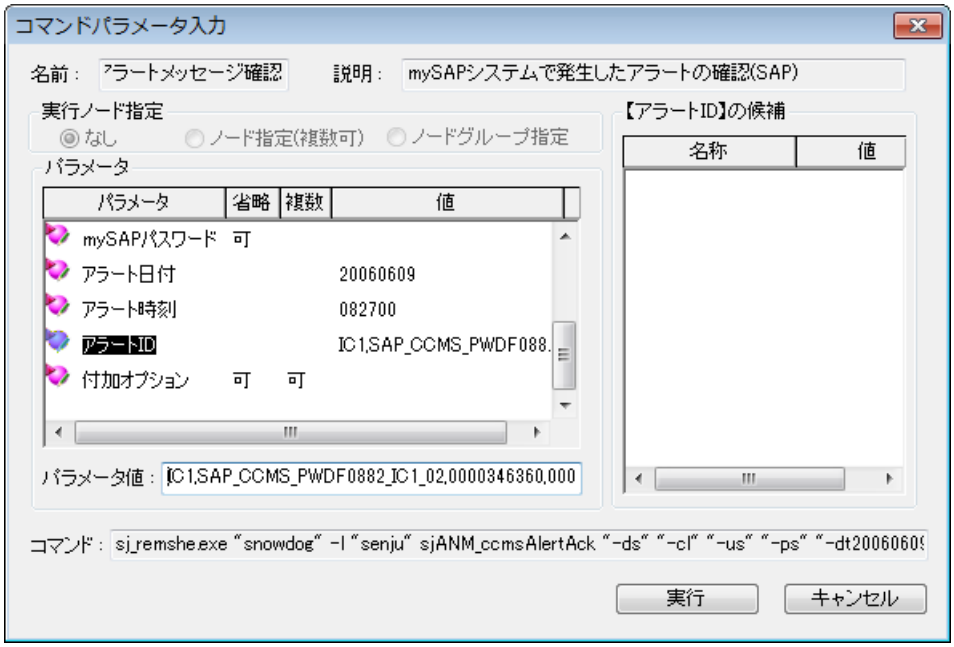


図 6.6 アラート確認コマンドパラメータ設定例

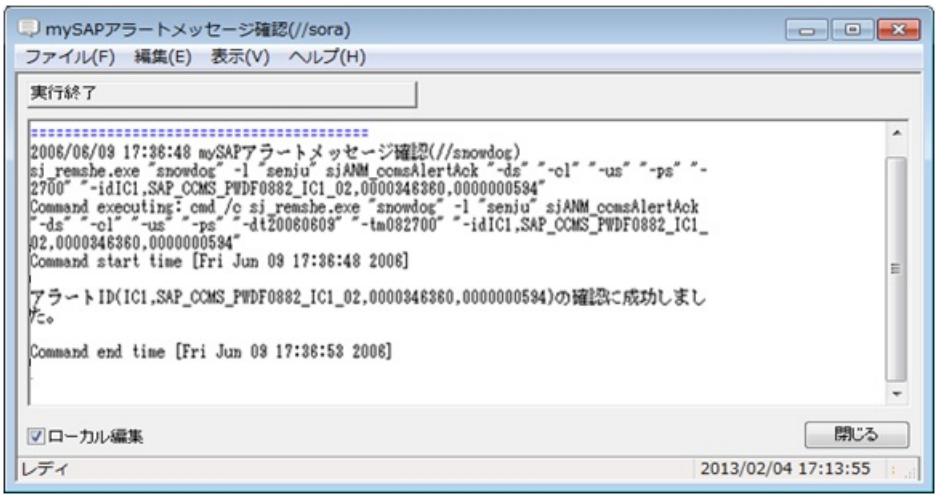


図 6.7 アラート確認実行結果例

6.4.3. パフォーマンスデータ監視機能

mySAPシステム CCMS上にて保持されているパフォーマンスデータを取得し、Senju DevOperation Conductorのモニタリング機能を使って、監視することが出来ます。

監視定義を千手ブラウザより登録し、監視を実施します。監視結果は、各種モニタ画面（グローバルノードモニタ／ノードモニタ）にてその監視状況を表示できます。予め設定したしきい値により障害を検知した場合は、メッセージモニタにメッセージが通知されます。（モニタリング機能については、ユーザーズマニュアル「 **4. モニタリング** 」を参照して下さい。）

6.4.3.1. 監視対象候補一覧表示

監視定義を作成する際に指定する監視対象候補の表示コマンドについて説明します。

千手ブラウザのツリービューの＜ドメイン＞→“コマンド”→“千手コマンド”→“モニタリング”より、「mySAP監視対象候補表示」コマンドを選択して実行します。（千手コマンドについては、ユーザーズマニュアル「 **千手コマンド** 」を参照して下さい。）

- 監視対称候補を表示するためには、監視対象が存在する、モニタセット名、モニタ名を指定する必要があります。
    - モニタセットの一覧を表示するには、モニタセット名、モニタ名、共に省略します。
    - モニタセット名を指定し、モニタ名を省略することで、そのモニタセットに存在するモニタの一覧を表示することが出来ます。

- モニタセット名、モニタ名、共に指定することで、監視対象候補に関する情報が表示されます。

- デスティネーション、クライアント、mySAPユーザー名、mySAPパスワードは、省略可能です。
  省略時には、mySAPシステム監視設定で設定した値を使用します。（mySAPシステム監視用設定については、「mySAPシステム監視設定」を参照して下さい。）

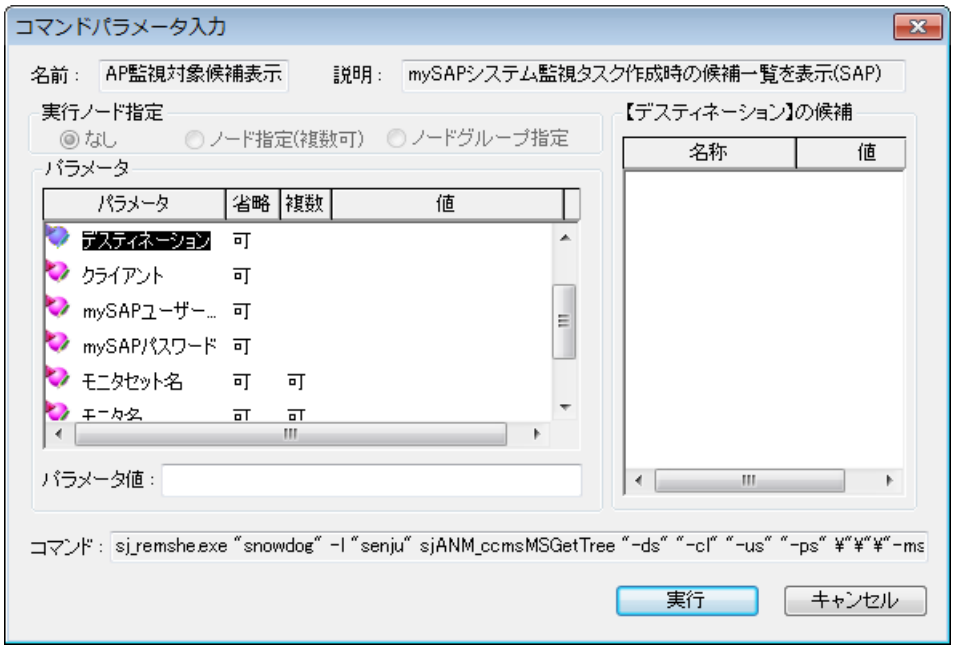


図 6.8 モニタセット表示時例

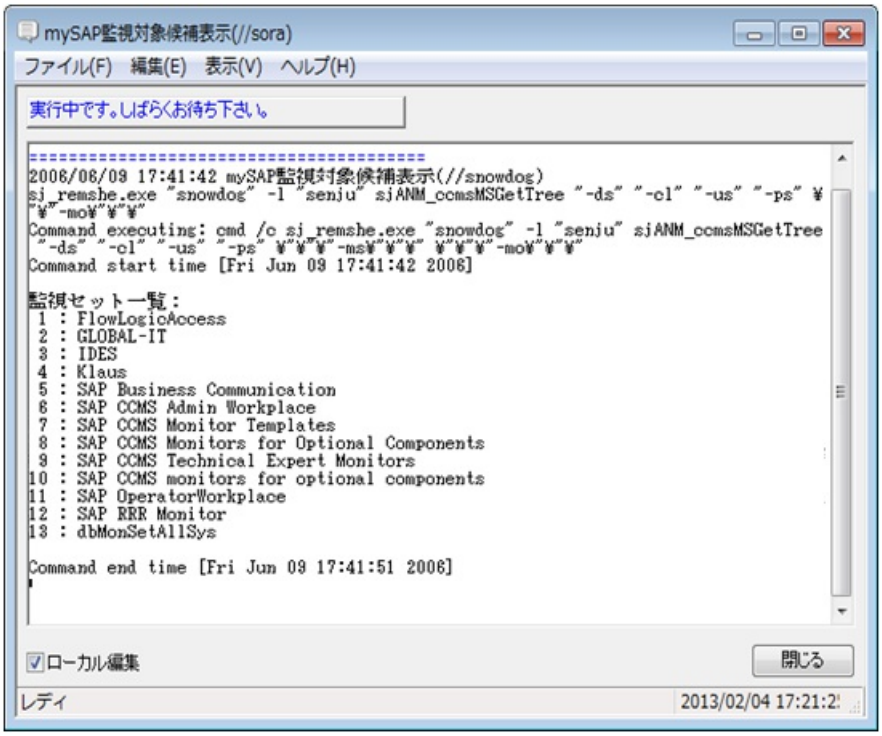


図 6.9 モニタセット表示　実行結果例

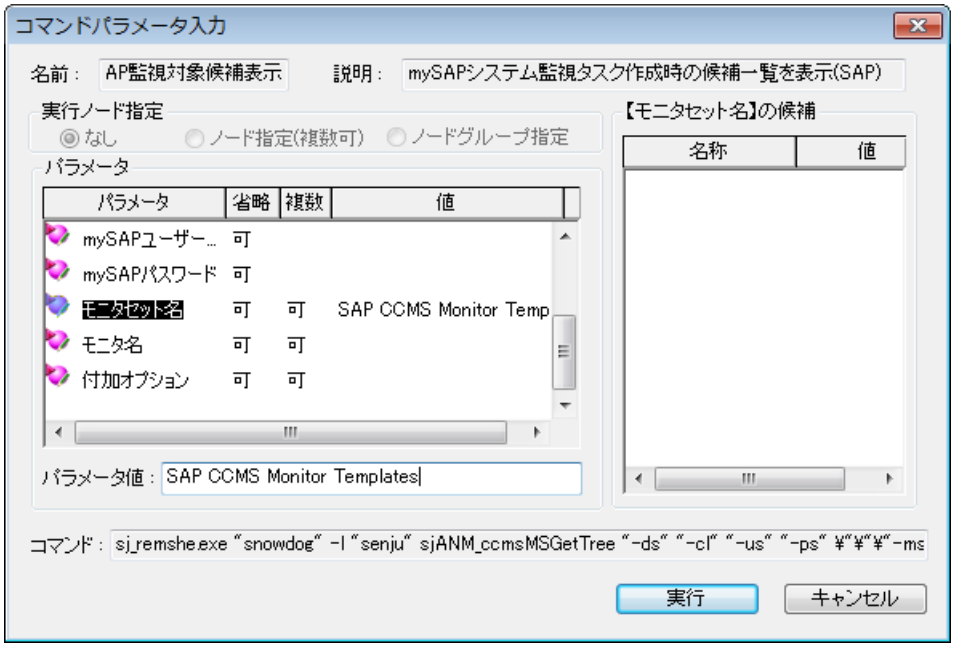


図 6.10 モニタ表示時例

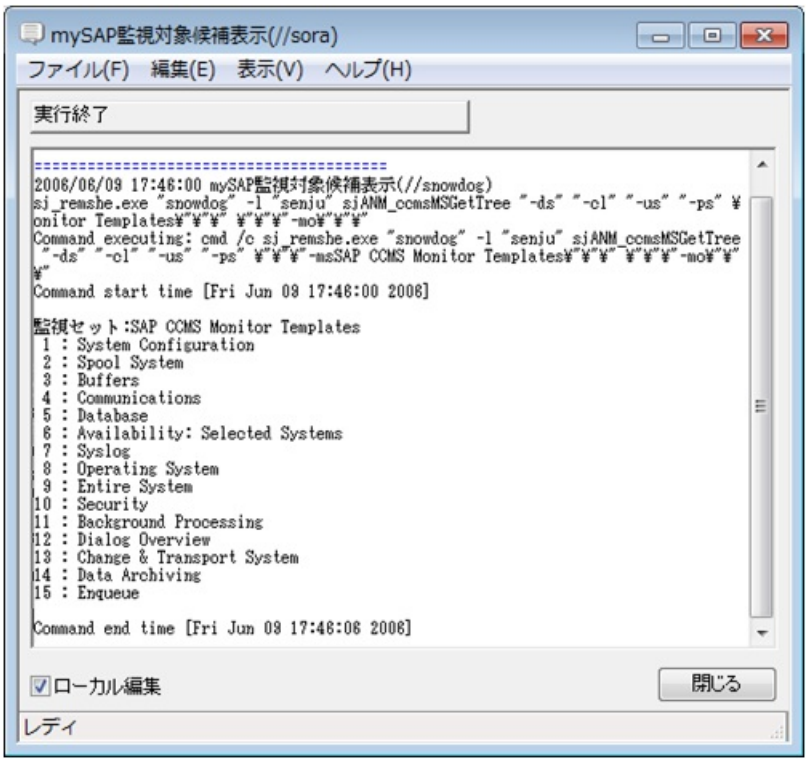


図 6.11 モニタ表示　実行結果例

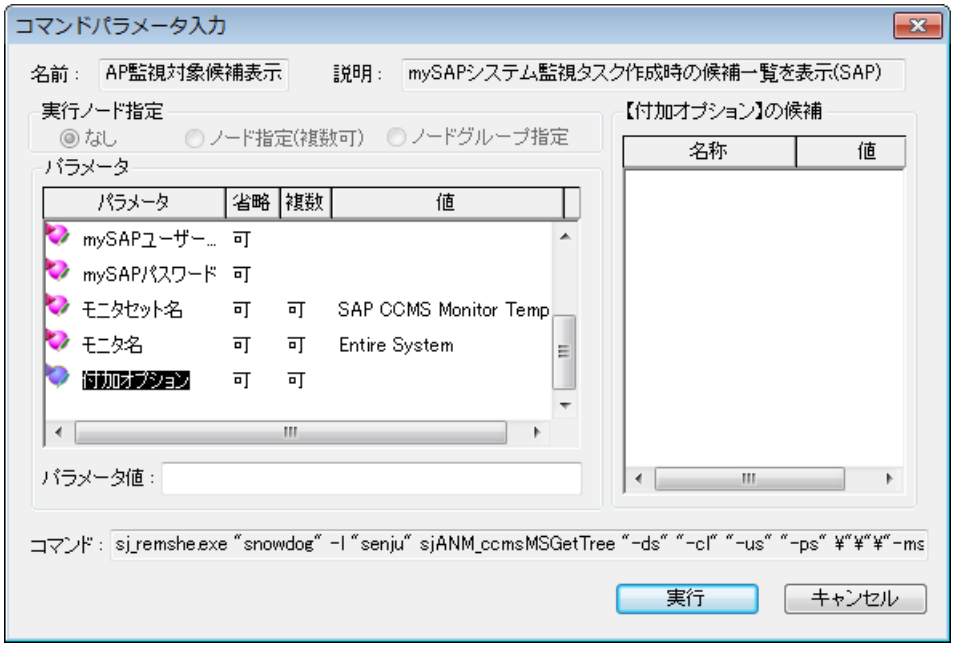


図 6.12 監視対象候補表示時例

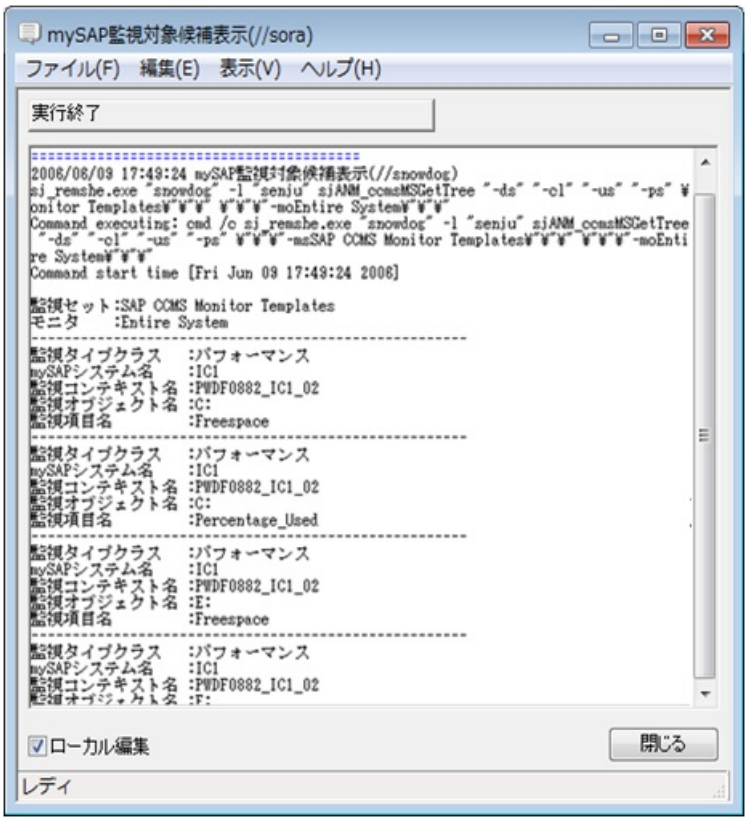


図 6.13 監視対象候補表示　実行結果例

6.5. 付録

6.5.1. メッセージ一覧

mySAP監視にて表示されるメッセージは以下になります。

ID	レベル	表示	警報	メッセージ内容	原因・内容
!ANMC01	E	2	ON	mySAPシステムとの通信ができません。	プローブの環境設定に誤りがあるか、サー
!ANMC02	I	2	OFF	mySAPシステムとの通信が復旧しました。	mySAPシステムとの通信が復旧しました。
!ANMC03	E	2	ON	mySAPシステム CCMSからのアラート取得に失敗しました。	プローブの環境設定に誤りがあるか、サー
!ANMC04	E	2	ON	メモリの確保に失敗しました。	メモリが不足しているため、処理が行えませ
!ANMC05	E	2	ON	mySAPシステム CCMSアラートファイルの書き込みに失敗しました。	CCMSアラートファイルの書き込みに失敗
!ANMC06	E	2	ON	mySAPシステム CCMSアラートファイルの読み込みに失敗しました。	CCMSアラートファイルの読み込みに失敗
!ANMC07	E	2	ON	mySAPシステム CCMSアラートファイルフォーマットエラーです。	CCMSアラートファイルフォーマットエラーで

7. SAP Job Scheduler

7.1. はじめに

7.1.1. 本章について

- Job Scheduler for R/3 使用者の手引きは、Job Scheduler for R/3 の機能や使用方法について説明します。
- Job Scheduler for R/3 はSAP R/3のバックグラウンドジョブの機能とSenju DevOperation Conductorのジョブスケジュール機能を連携させることができます。この連携により、Senju DevOperation Conductorのジョブスケジュール機能からSAP R/3のバックグラウンドジョブを実行および監視することができるようになります。
- 「Senju DevOperation Conductor」「Senju Operation Conductor」「Senju Enterprise Navigator」「eXsenju」「EX千手/EXSENJU」「千手/SENJU」「e-千手/e-SENJU」および「セキュア・キューブ/SecureCube」は（株）野村総合研究所の登録商標です。
- SAP、R/3、mySAP、ABAPは、SAP AGのドイツ及びその他の国における登録商標または商標です。
- UNIXは、X/Open Company Limitedが独占的にライセンスしている米国ならびに他の国における登録商標です。
- Linuxは、Linus Torvalds氏の登録商標です。
- Windows、Windows Serverは、米国Microsoft Corporationの米国及びその他の国における登録商標または商標です。
- その他、本誌で引用の製品名・会社名はそれぞれの会社の商標、もしくは登録商標です。なお、本誌中では、™、® マークなどは明記していません。

7.1.2. 読者の対象

本章はJob Scheduler for R/3 を利用して、Senju DevOperation Conductorのジョブスケジュール機能からSAP R/3のバックグラウンドジョブを管理するシステム・アドミニストレータのためのものです。従って、本章の読者は以下のような概念に精通していることを前提にしています。

- SAP R/3(ABAP/4プログラム・バリアントの定義登録)
- Senju DevOperation Conductorの各種コンポーネント（千手ブラウザ、千手マネージャ、千手エージェント）
- Senju DevOperation Conductorのジョブスケジュール機能
- オペレーティング・システムについての知識

7.1.3. 前提条件と関連資料

本章を参照するにあたっては、以下の各マニュアルなどを参照して下さい。

- 統合運用管理ツール「Senju DevOperation Conductor」リリースノート
- 統合運用管理ツール「Senju DevOperation Conductor」ユーザーズマニュアル
- ERP（管理業務統合）ソフト「SAP R/3」「mySAP ERP」

7.2. Job Scheduler for R/3の概要

下記の23個のJob Scheduler for R/3コマンド群は、Senju DevOperation Conductorのジョブスケジュールサブシステムよりの機能を利用するものです。

- R/3ジョブスケジュールコマンド(sjPEX_r3job)
- R/3ジョブ定義取得コマンド(sjPEX_r3job_defget)
- R/3ジョブログ取得コマンド(sjPEX_r3job_logget)
- R/3ジョブ状態確認コマンド(sjPEX_r3job_check)
- R/3ジョブバリアント取得コマンド(sjPEX_r3job_variant)
- R/3ジョブログ設定コマンド(sjPEX_r3job_logset)
- R/3ジョブ削除コマンド(sjPEX_r3job_delete)
- R/3ジョブ起動コマンド(sjPEX_r3job_start)
- R/3ジョブ検索コマンド(sjPEX_r3job_select)
- R/3ジョブ管理情報照会コマンド(sjPEX_r3job_confprint)
- R/3ジョブコピーコマンド(sjPEX_r3job_copy)（＊）
- R/3ジョブ強制停止コマンド(sjPEX_r3job_stop)（＊）
- R/3ジョブ子ジョブ取得コマンド(sjPEX_r3job_listChildJobs)（＊）
- R/3ジョブスプール取得コマンド(sjPEX_r3job_listSpool)（＊）
- R/3イベント送信コマンド(sjPEX_r3job_sendEvent)（＊）
- R/3プリンター覧コマンド(sjPEX_r3job_listOutputDevice)（＊）
- R/3 ABAPレポート一覧コマンド(sjPEX_r3job_listABAPReport)（＊）
- R/3ジョブバリアント変更コマンド(sjPEX_r3job_variantChange)（＊）
- BWプロセスチェーン検索コマンド(sjPEX_bwChain_select)（＊）
- BWプロセスチェーン起動コマンド(sjPEX_bwChain_start)（＊）
- BWプロセスチェーン状態確認コマンド(sjPEX_bwChain_check)（＊）
- BWプロセスチェーンログ取得コマンド(sjPEX_bwChain_logget)（＊）
- BWプロセスチェーンプロセス一覧コマンド(sjPEX_bwChain_processList)（＊）
- BWプロセスチェーンプロセスログ取得コマンド(sjPEX_bwChain_processLog)（＊）

注釈

＊：SAP ERP用R/3ジョブ連携コマンドのみ対応しています。

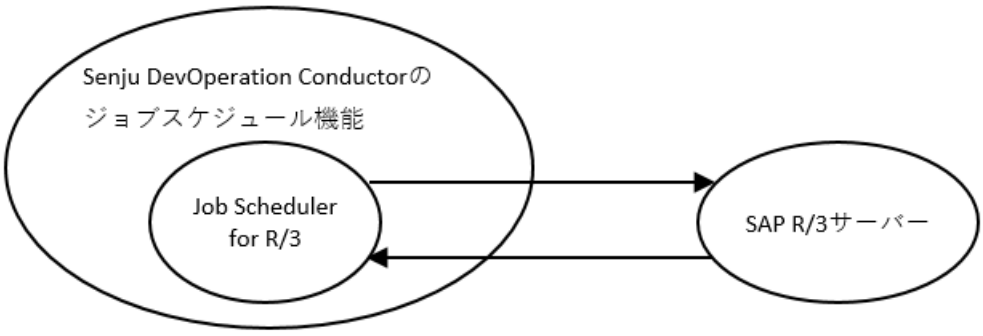


図 7.1 Senju DevOperation ConductorとSAP R/3との連携

Job Scheduler for R/3コマンドがSAP R/3サーバーと接続する際、SAP R/3サーバーに関する情報をsaprfc.iniファイルから取得します。そのため、Job Scheduler for R/3コマンドを使用する前にsaprfc.iniファイルを設定しておく必要があります。

Senju DevOperation Conductorのジョブスケジュールサブシステムよりの機能を利用するためには、まずR/3ジョブスケジュールコマンド(sjPEX_r3job)を使用します。

R/3ジョブスケジュールコマンドは起動されると、コマンドの引数に指定された内容でSAP R/3サーバーに対してR/3のジョブを登録・起動・監視します。

R/3ジョブスケジュールコマンドは、Senju DevOperation Conductorのジョブスケジュールサブシステムでジョブとして登録して利用して下さい。

R/3ジョブスケジュールコマンドは、R/3のジョブと1対1で対応します。このとき、R/3のジョブ名には、R/3ジョブスケジュールコマンドを起動した時のSenju DevOperation Conductorのジョブ名を使用します。

すなわち、Senju DevOperation Conductorのジョブ名とR/3のジョブ名は同一名称になります。

次に、必要に応じて以下のコマンドを利用することで、R/3サーバーで実行したジョブの、状況確認や起動、削除、コピー、強制停止を行うことができます。

- R/3ジョブ定義取得コマンド(sjPEX_r3job_defget)
- R/3ジョブログ取得コマンド(sjPEX_r3job_logget)
- R/3ジョブ状態確認コマンド(sjPEX_r3job_check)
- R/3ジョブ削除コマンド(sjPEX_r3job_delete)
- R/3ジョブコピーコマンド(sjPEX_r3job_copy)
- R/3ジョブ検索コマンド(sjPEX_r3job_select)
- R/3ジョブ起動コマンド(sjPEX_r3job_start)
- R/3ジョブ強制停止コマンド(sjPEX_r3job_stop)
- R/3ジョブ子ジョブ取得コマンド(sjPEX_r3job_listChildJobs)
- R/3ジョブスプール取得コマンド(sjPEX_r3job_listSpool)

R/3ジョブバリアント取得コマンド(sjPEX_r3job_variant)は、Senju DevOperation ConductorのジョブスケジュールサブシステムでR/3ジョブスケジュールコマンドをジョブとして登録する前に、指定したいABAP/4プログラムに対して定義済みのバリアントを確認することができます。

また、R/3ジョブバリアント変更コマンド(sjPEX_r3job_variantChange)は、定義済みのバリアントにパラメータや選択オプションが存在する場合に、それらのパラメータや選択オプションを変更することができます。

R/3プリンター覧コマンド(sjPEX_r3job_listOutputDevice)は、Senju DevOperation ConductorのジョブスケジュールサブシステムでR/3ジョブスケジュールコマンドをジョブとして登録する前に、指定したいプリンタを表示することができます。

R/3 ABAPレポート一覧コマンド(sjPEX_r3job_listABAPReport)は、Senju DevOperation ConductorのジョブスケジュールサブシステムでR/3ジョブスケジュールコマンドをジョブとして登録する前に、指定したいABAP/4プログラムを検索することができます。

R/3ジョブ管理情報照会コマンド(sjPEX_r3job_confprint)は、R/3で実行したジョブの情報（ジョブ名とジョブカウント）を基に、Senju DevOperation Conductorの管理情報（運用日付、フレーム名、ネット名）を表示することができます。

R/3イベント送信コマンド(sjPEX_r3job_sendEvent)は、R/3で起動条件にイベントを指定して登録済みのR/3ジョブに対し、イベントを送信してR/3ジョブを起動させることができます。

BWプロセスチェーン検索コマンド(sjPEX_bwChain_select)は、プロセスチェーンを起動する前に、指定したいプロセスチェーンを検索することができます。
BWプロセスチェーン起動コマンド(sjPEX_bwChain_start)は、プロセスチェーンを起動することができます。
必要に応じて以下のコマンドを利用することで、SAPサーバーで実行したプロセスチェーンの、状況確認やログ取得を行うことができます。

- BWプロセスチェーン状態確認コマンド(sjPEX_bwChain_check)
- BWプロセスチェーンログ取得コマンド(sjPEX_bwChain_logget)
- BWプロセスチェーンプロセス一覧コマンド(sjPEX_bwChain_processList)
- BWプロセスチェーンプロセスログ取得コマンド(sjPEX_bwChain_processLog)

7.3. Job Scheduler for R/3の使い方

7.3.1. saprfc.iniの設定

saprfc.iniファイルは、SAP R/3サーバーに関する情報が書かれたファイルで、Job Scheduler for R/3コマンド群はこのファイルを参照します。
saprfc.iniファイルは、UNIXの場合は Job Scheduler for R/3コマンド群が稼働するエージェント上の$SENJUHOME/dat/pex/sapディレクトリ、Windowsの場合はJob Scheduler for R/3コマンド群が稼働するエージェント上の%SENJUHOME%\dat\pex\sapディレクトリに必要です。初期インストール時には saprfc.iniファイルのひな型（saprfc.ini.sample）を置いてあります。

saprfc.iniに、「saprfc.iniの記述内容(TYPE=A)」に示す内容を記述して下さい。
負荷分散機能を利用する場合は「saprfc.iniの記述内容(TYPE=B)」に示す内容を記述して下さい。
（項目の詳細内容は、お客様の環境のSAP R/3の管理者にお尋ね下さい。）

表 7.1 saprfc.iniの記述内容(TYPE=A)

項目	例	説明
DEST=	R3SRV1	デスティネーション
TYPE=	A	通常（負荷分散機能を利用しない場合）パラメータに'A'を指定して下さい
ASHOST=	r3server1	TYPEが'A'のとき、接続するSAP R/3サーバー名
SYSNR=	00	TYPEが'A'のとき、システム番号[00-99]
GWSERV=	3300	TYPEが'A'のとき、サービスのポート番号(＊)
RFC_TRACE=	0	Senju DevOperation Conductorシステムではパラメータに'0'を指定して下さい

- デスティネーションには、大文字のアルファベットと数字を組み合わせて32文字までで自由な名前をつけることができます。ここで付けたデスティネーションを、SAP R/3連携コマンドの「-d」オプションに指定します。
- saprfc.iniの記述例(TYPE=A)

```
DEST=R3SRV1
TYPE=A
ASHOST=r3server1
SYSNR=00
GWSERV=3300
RFC_TRACE=0
```

注釈

＊：サービスのポート番号の上2桁は"33"で、下2桁はシステム番号になります。

(例) SYSNR=02のとき、GWSERV=3302

- saprfc.iniの記述例(TYPE=A で SYSNR=02のとき)

```
DEST=R3SRV2
TYPE=A
ASHOST=r3server2
SYSNR=02
GWSERV=3302
RFC_TRACE=0
```

負荷分散機能を利用する場合

表 7.2 saprfc.iniの記述内容(TYPE=B)

項目	例	説明
DEST=	R3SRV1	デスティネーション
TYPE=	B	負荷分散機能を使用する場合は'B'を指定してください
R3NAME=	R3SRV1	SAP システムの名称　オプション; デフォルト: 宛先
MSHOST=	sapgroup	メッセージサーバのホスト名
GROUP=	PUBLIC	アプリケーションサーバのグループ名　オプション; デフォルト: PUBLIC
RFC_TRACE=	0	Senju DevOperation Conductorシステムではパラメータに'0'を指定して下さい

- デスティネーションには、大文字のアルファベットと数字を組み合わせて32文字までで自由な名前をつけることができます。ここで付けたデスティネーションを、SAP R/3連携コマンドの「-d」オプションに指定します。

- 説明に「オプション；デフォルト」と記載している項目は **saprfc.ini** に記載しなくてもデフォルト値が適用されます。
- saprfc.iniの記述例(TYPE=B)

```
DEST=R3SRV1
TYPE=B
R3NAME=R3SRV1
MSHOST=sapgroup
GROUP=PUBLIC
RFC_TRACE=0
ABAP_DEBUG=0
```

7.3.2. R/3バックグラウンドジョブとの連携方法

7.3.2.1. R/3ジョブスケジュールコマンドを登録

R/3ジョブスケジュールコマンド(sjPEX_r3job)は、Senju DevOperation Conductorのジョブスケジュールサブシステムからの SAP R/3のバックグラウンドジョブの機能を利用するための中核のコマンドです。

R/3ジョブスケジュールコマンドは起動されると、コマンドの引数に指定された内容でSAP R/3サーバーに対してR/3のジョブを登録し、起動し、R/3のジョブが終了するまで監視し続けます。

R/3ジョブスケジュールコマンドは、Senju DevOperation Conductorのジョブスケジュールサブシステムでジョブとして登録し利用します。

R/3ジョブスケジュールコマンドをSenju DevOperation Conductorのジョブスケジュールサブシステムでジョブとして登録／利用する方法は、Senju DevOperation Conductorのユーザーズマニュアル「**5 ジョブスケジュール**」の「**5.2 ジョブスケジュールの使い方**」「**5.5.5 ジョブテンプレート**」及び「R/3ジョブスケジュールコマンドをジョブとして登録」、「R/3ジョブスケジュールコマンドをジョブとして利用」を参照して下さい。

R/3ジョブスケジュールコマンドをジョブとして登録する際に指定する引数には、以下に示す内容を指定して下さい。

警告

引数を指定する場合、アルファベットの大文字と小文字を絶対に間違えないようにして下さい。

```
sjPEX_r3job
      -cl クライアント -u R/3ユーザー名 -p パスワード -d デスティネーション
      [-l 言語] [-lv XMI監視レベル]
      [-jh R/3ジョブの対象ホスト名 | ジョブサーバグループ名] [-i インターバル] [-s] [-jclass 優先度]
      [-w稼働猶予時間(HH:MM)] [-k 打ち切り時間(HH:MM)]
      [-pDev 出力デバイス] [-pCopies 部数]
      [-pForm 書式] [-pRow 行数] [-pCol 列数]
      [-pName 名称] [-pTitle タイトル] [-pAuth 権限]
      [-pCover] [-pUser 受信者] [-pDepart 部署コード]
      [-pDel] [-pPeriod スプール保存期間] [-pNotNew] [-pPri 印刷優先度]
      { {-a ABAP/4プログラム名 [-v ABAP/4バリアント名]} | {-c 外部プログラム -h ホスト名} }
      [ { {-a [-v]} | {-c -h} } ] ..
      [ -recName 受信者アドレス -recType 受信者種別 [-gaCopy] [-gaBlind] [-gaExpress] [-gaNForward] ]
```

オプション	省略	デフォルト	長さ	説明
-cl	不可		3	クライアント
-u	不可		12	R/3ユーザー名
-p	不可(※1)		8(※2)	パスワード
-d	不可		32	デスティネーション
-l	可	E	1	言語[J/E/D/1](J:日本語、E:英語、D:独語、1:中国語)
-lv	可	0	1	XMI監視レベル[0-3]
-jh	可	R/3サーバーに依存	32	R/3ジョブの対象ホスト名／ジョブサーバグループ名
-i	可	60	3	ステータスチェックインターバル[10-300]
-s	可	R/3サーバーに依存	0	即時実行かどうか
-jclass	可	C	1	優先度[A/B/C]
-w	可		5	稼働猶予時間(HH:MM)
-k	可		5	打ち切り時間(HH:MM)
-pDev	可		4	出力デバイス
-pCopies	可	1	3	部数
-pForm	可		16	書式
-pRow	可		10	行数
-pCol	可		10	列数
-pName	可		12	名称
-pTitle	可		68	表題
-pAuth	可		12	権限
-pCover	可		0	選択カバーシート
-pUser	可		12	受信者
-pDepart	可		12	部署コード
-pDel	可		0	印刷後削除
-pPeriod	可		1	スプール保存期間[0-8]
-pNotNew	可		0	新規スプール依頼
-pPri	可		1	印刷優先度[1-9](1:高～9:低)
-a	不可		40	ABAP/4プログラム名
-v	可		14	ABAP/4バリアント名
-c	不可		384	外部プログラム
-h	不可		32	ホスト名
-recName	可		241	受信者アドレス
-recType	可		1	受信者種別、設定値は下記参照
-gaCopy	可		0	コピー
-gaBlind	可		0	ブラインドコピー
-gaExpress	可		0	緊急
-gaNForward	可		0	転送不可

- クライアント、R/3ユーザー名、パスワード、言語には、R/3ログオン画面 で入力する内容と同じものを指定して下さい（言語は省略すると'E'(英語)になります）。
- デスティネーションには、saprfc.iniのデスティネーションを指定して下さい（saprfc.iniについては、「saprfc.iniの設定」を参照して下さい）。
- R/3ジョブの対象ホスト名／ジョブサーバグループ名には、R/3ジョブの定義画面 で入力する内容と同じホスト名を指定して下さい。
- インターバルには、R/3ジョブスケジュールコマンドがR/3ジョブの監視を行う間隔(秒)を指定して下さい（インターバルは省略すると60(秒)になります）。
- -sオプションを指定すると、R/3のジョブのスケジュールをR/3のサーバーに任せずに、即時に起動します（すぐに起動できなかった場合は、R/3ジョブスケジュールコマンドは異常終了します）。
- ABAP/4プログラム名、ABAP/4バリアント名、外部プログラム、ホスト名には、R/3ジョブステップの定義画面 で入力する内容と同じ物を指定して下さい。1つのR/3のジョブに複数のステップを登録する場合は、これをステップ数だけ繰り返して下さい。
- ABAP/4バリアント名の省略は、ABAP/4プログラムでバリアントの定義を必要としない場合のみ可能です
- 受信者アドレスと受信者種別は同時に指定する指定してください。
- 「-ga～」の4つのオプションは受信者アドレス/受信者種別と同時に指定してください。
- **-gaCopy** と **-gaBlind** を同時に指定した場合、**-gaCopy** が有効となります。

注釈

(※1) SAP ERP(RFC SDK 7.20)用R/3ジョブ連携コマンドに限り、設定を行うことで-pオプションを省略できます。設定方法については、

「パスワード指定の省略方法」を参照して下さい。

(※2) SAP ERP(RFC SDK 7.20)用R/3ジョブ連携コマンドに限り、指定可能なパスワードの文字列長は40です。これにより、SAP NetWeaver6.40以降のSAPサーバーに接続できます。

- 受信者種別一覧

受信者種別	備考
P	Private distribution list
C	Shared distribution list
O	SAPoffice user
B	SAP user
U	Internet address
X	X.400 address
R	SAP user in another SAP System
A	External address
F	Fax number
D	X.500 Address
L	Telex number
H	Organizational unit/position
J	SAP object
G	Organization object/ID
K	Pager/SMS
1	Other Recipient Types

- (例)

```
クライアント            : 500
R/3ユーザー名             : ABC
パスワード               : pass
デスティネーション       : R3SRV1
```

```
R/3ジョブ
step 1 :         ABAP/4プログラム名    : CALC
step 2 :         ABAP/4プログラム名    : CALC2
                 ABAP/4バリアント名    : CALC_VAR2
step 3 :         外部プログラム         : multi_printout -u 10
                 ホスト名              : exserver
step 4 :         ABAP/4プログラム名    : CLEAR
```

- コマンドライン

```
sjPEX_r3job -cl 500 -u ABC -p pass -d R3SRV1 -a CALC -a CALC2 -v CAL_VAR2
 -c "multi_printout -u 10" -h exserver -a CLEAR
```

- 実行結果

  sjPEX_r3jobコマンドの実行結果はすべて千手ブラウザのメッセージモニタに表示されます。

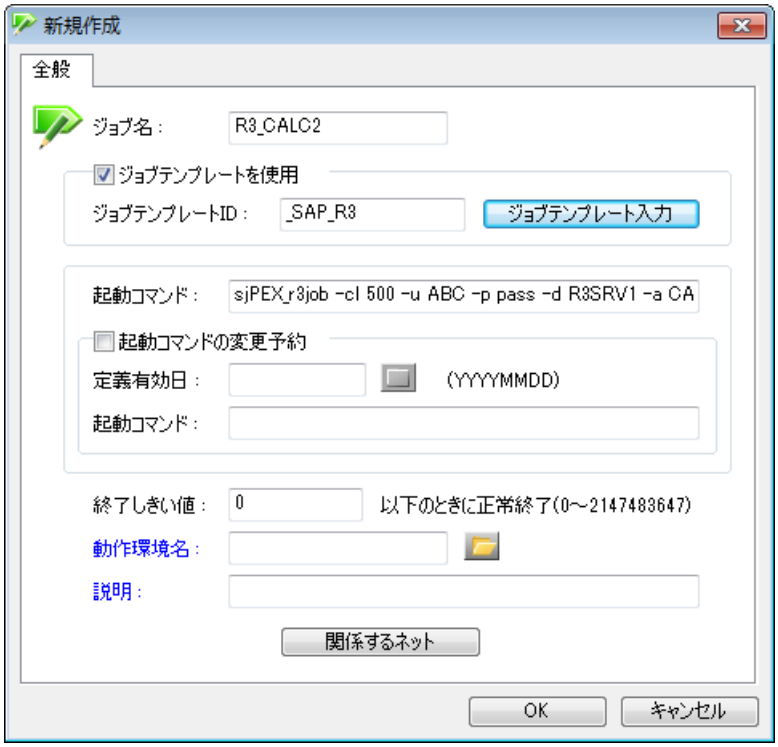


図 7.2 R/3ジョブスケジュールコマンドをジョブとして登録

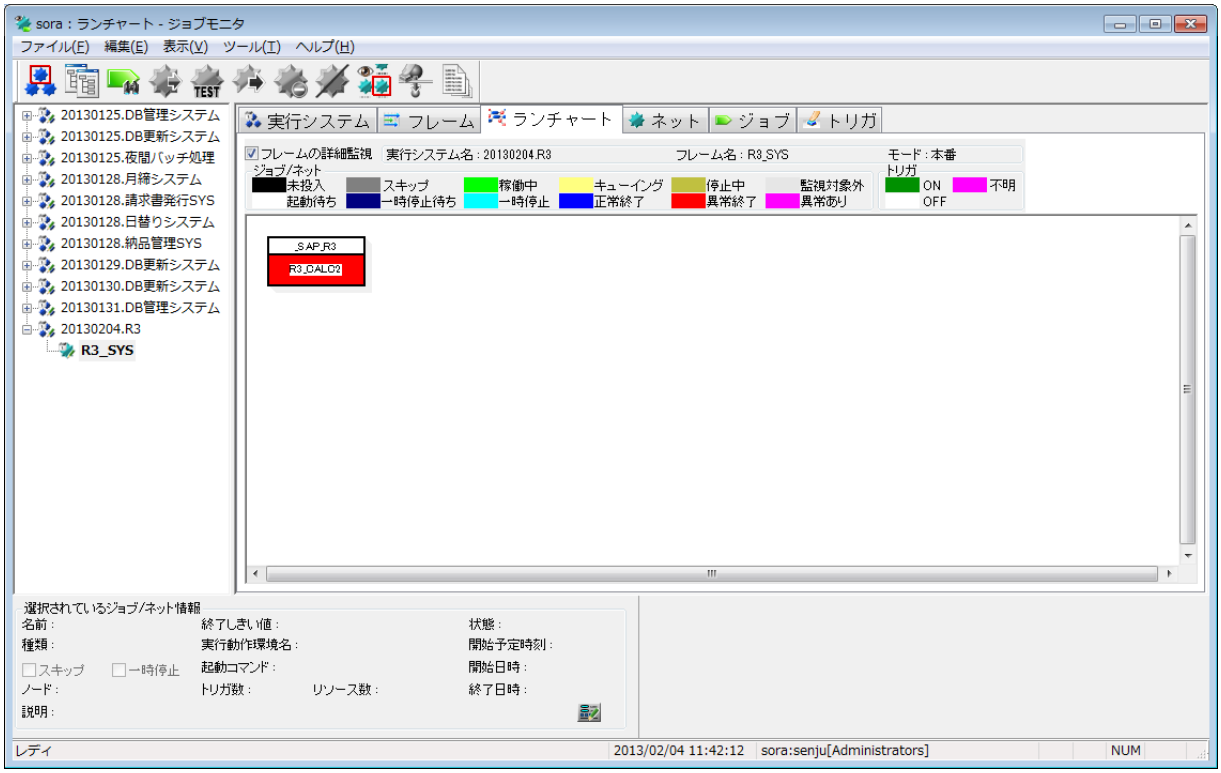


図 7.3 R/3ジョブスケジュールコマンドをジョブとして利用

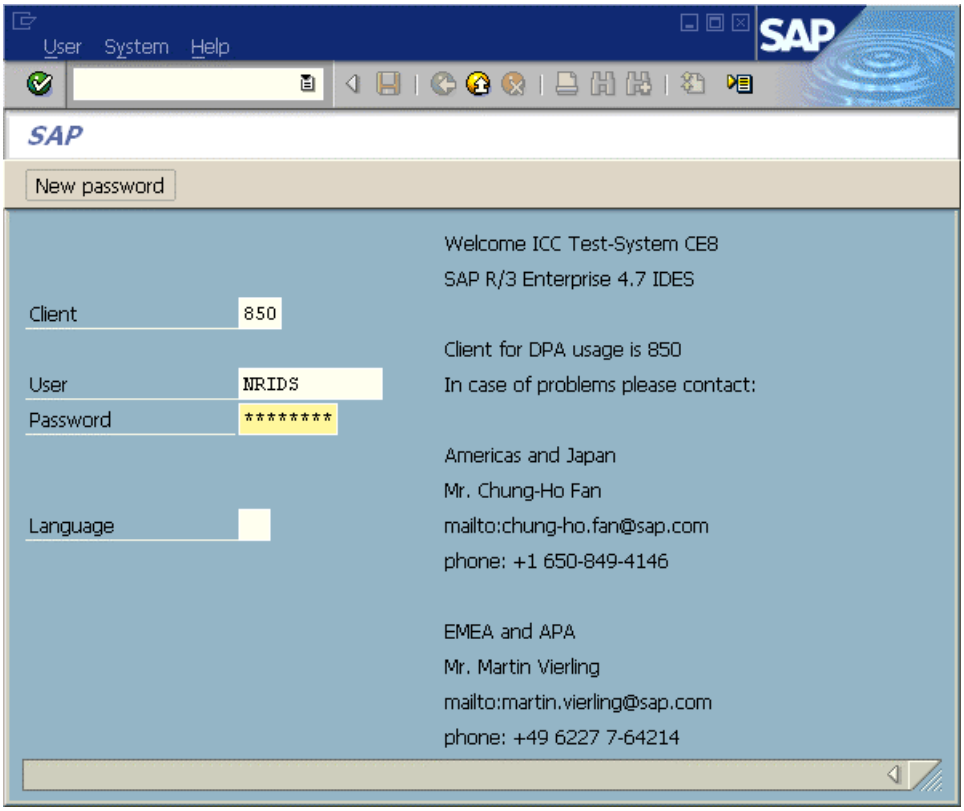


図 7.4 R/3ログオン画面

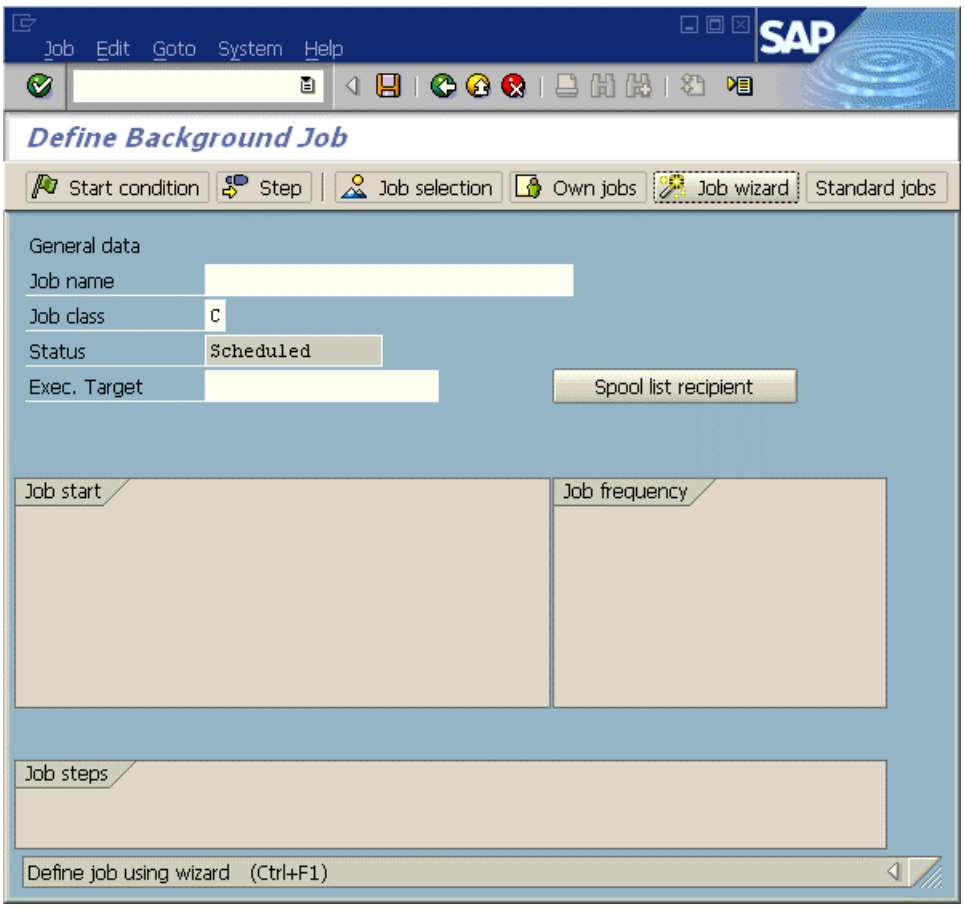


図 7.5 R/3ジョブの定義画面

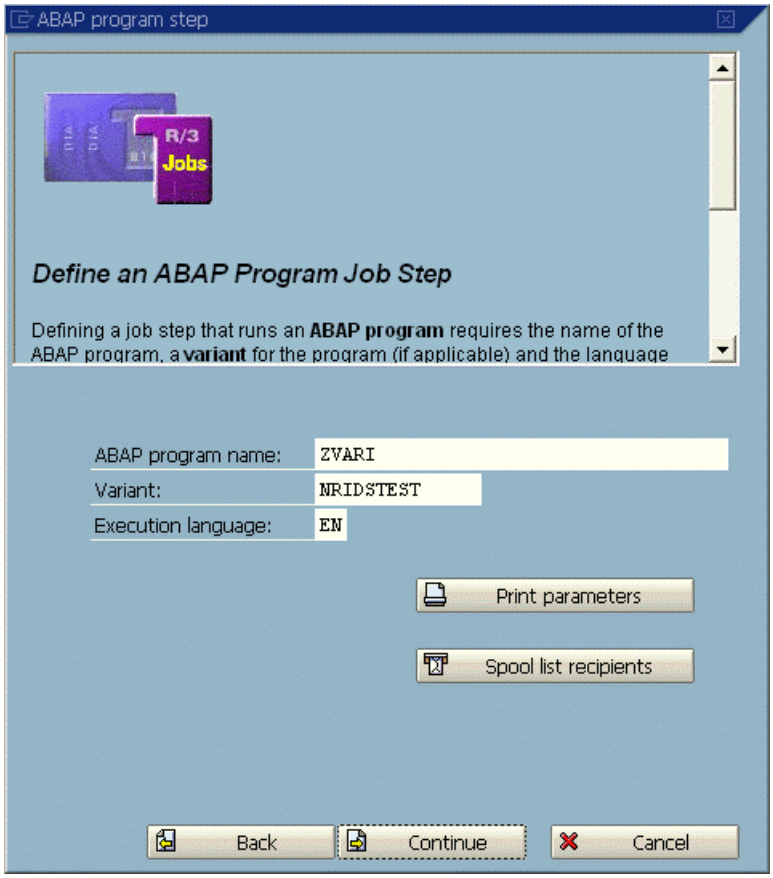


図 7.6 R/3ジョブステップの定義画面

7.3.2.2. R/3ジョブスケジュールコマンドを実行

R/3ジョブスケジュールコマンド(sjPEX_r3job)は、Senju DevOperation Conductorのジョブスケジュールサブシステムで1つのジョブとして登録し、利用します。

R/3ジョブスケジュールコマンドをSenju DevOperation Conductorのジョブスケジュールサブシステムでジョブとして登録／利用する方法は、Senju DevOperation Conductorのユーザーズマニュアル「**5 ジョブスケジュール**」の「**5.2 ジョブスケジュールの使い方**」などを参照して下さい。

R/3ジョブスケジュールコマンドは、R/3にてジョブを登録すると即時に起動をかけるため、ジョブの起動時刻などのスケジューリングはSenju DevOperation Conductorのジョブスケジュールサブシステムにて行って下さい。

7.3.2.2.1. R/3ジョブスケジュールコマンドの処理の流れ（通常時）

R/3ジョブスケジュールコマンドがSenju DevOperation Conductorのジョブスケジュールで1つのジョブとして起動されると、「図 7.7 R/3ジョブスケジュールコマンドの処理の流れ」及び「表 7.3 R/3ジョブスケジュールコマンドの処理の流れ」に示す流れで動きます。

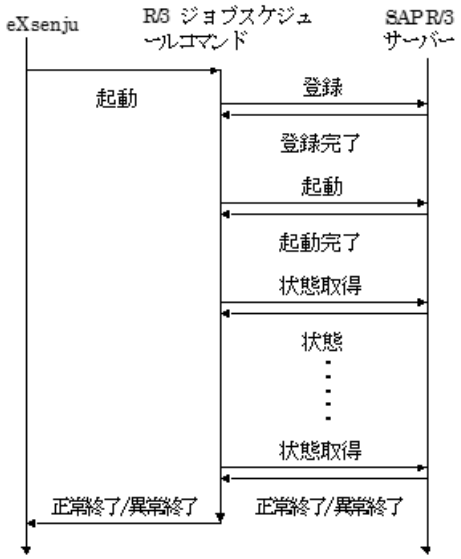


図 7.7 R/3ジョブスケジュールコマンドの処理の流れ

表 7.3 R/3ジョブスケジュールコマンドの処理の流れ

Senju DevOperation Conductorジョブの状態	R/3ジョブスケジュールコマンドの処理内容	R/3ジョブの状態	メッセージモニタ
起動待ち	起動前の状態	-(未登録)	
稼働中	起動	-(未登録)	
稼働中	引数に従い、R/3のジョブを登録	'P':予定済(scheduled)	!PEX504: R/3ジョブ
稼働中	登録したR/3ジョブを起動	'S':リリース済(released)	
稼働中	登録したR/3ジョブの状態を監視	'Y':待機中(ready)	
稼働中	登録したR/3ジョブの状態を監視	'R':実行中(active)	!PEX506: R/3ジョブ
正常終了	登録したR/3ジョブの状態を監視 → 正常終了	'F':終了(finished)	!PEX514: R/3ジョブ
異常終了	登録したR/3ジョブの状態を監視 → 異常終了	'A':中止(terminated)	!PEX513: R/3ジョブ

1. R/3ジョブスケジュールコマンドが起動されると、引数に指定された内容でR/3のジョブを登録し、R/3のジョブを登録した旨のメッセージを出力します。(R/3のジョブ名にはSenju DevOperation Conductorのジョブ名を使用します。)
2. 登録したR/3のジョブを起動します。
3. 起動したR/3のジョブの状態を指定されたインターバルでR/3サーバーに尋ねます。(初めて状態が'R':実行中になったときに、R/3のジョブが起動した旨のメッセージを出力します。)
4. R/3のジョブが正常終了すると、正常終了した旨のメッセージを出力し、R/3ジョブスケジュールコマンドも正常終了します。
5. R/3のジョブが異常終了すると、異常終了した旨のメッセージを出力し、R/3ジョブスケジュールコマンドも異常終了します。

7.3.2.2.2. R/3ジョブスケジュールコマンドの処理の流れ(強制停止時)

R/3ジョブスケジュールコマンドは、他のSenju DevOperation Conductorのジョブと同じく強制停止させることができます。
R/3ジョブスケジュールコマンドに対し、Senju DevOperation Conductorのジョブスケジュールより強制停止が行われると、「R/3ジョブスケジュールコマンドの強制停止の流れ」に示す流れで動きます。

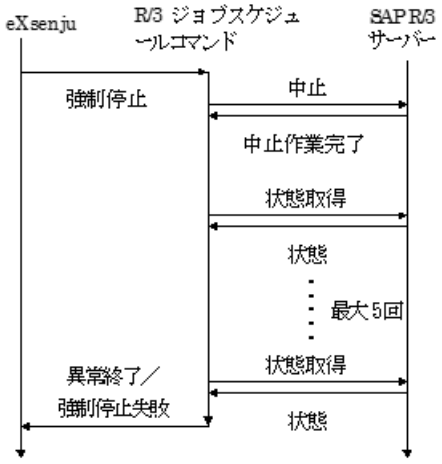


図 7.8 R/3ジョブスケジュールコマンドの強制停止の流れ

1. Senju DevOperation Conductorより、R/3ジョブスケジュールコマンドに強制停止の命令がくると、R/3サーバーに対し、R/3のジョブを中止するように依頼します。この段階では、まだR/3のジョブは終了していませんが、Senju DevOperation Conductorのジョブスケジュールの仕様では、*ジョブはこの時点で異常終了として扱います。*
2. 中止を依頼したR/3のジョブの状態を一定間隔（引数で指定されたインターバルの半分のインターバル（ただし、10秒より小さくはなりません））でR/3サーバーに尋ねます。
3. R/3のジョブが正常終了すると、正常終了した旨のメッセージと、強制停止が失敗した旨のメッセージを出力し、R/3ジョブスケジュールコマンドも正常終了します（ただし、Senju DevOperation Conductorのジョブは異常終了のままです）。
4. R/3のジョブが異常終了すると、異常終了した旨のメッセージを出力し、R/3ジョブスケジュールコマンドも異常終了します。
5. 5回状態を取得しても、正常終了または異常終了にならなかった場合には、強制停止が失敗した旨のメッセージを出力し、R/3ジョブスケジュールコマンドは異常終了します。

注釈

R/3ジョブスケジュールコマンドに対して強制停止を行った場合は、R/3のジョブが完全に終了する前にSenju DevOperation Conductorのジョブスケジュールコマンドは異常終了となるため、必要に応じてR/3のメッセージモニタをご覧下さい。

7.3.3. BWプロセスチェーンとの連携方法

BWプロセスチェーン起動コマンド(sjPEX_bwChain_start)とBWプロセスチェーン状態確認コマンド(sjPEX_bwChain_check)を使用することで、BWプロセスチェーンと連携する方法を述べます。

警告

BWプロセスチェーン起動コマンド(sjPEX_bwChain_start)は、R/3ジョブスケジュールコマンド(sjPEX_r3job)とは異なり、SAPサーバーでBWのプロセスチェーンを起動させるだけで、終了するまで監視しつづけるということは行いません。
別途BWプロセスチェーン状態確認コマンド(sjPEX_bwChain_check)を実行し、状態を確認して下さい。

7.3.3.1. BWプロセスチェーンを起動

BWのプロセスチェーンを起動させるために、BWプロセスチェーン起動コマンド(sjPEX_bwChain_start)コマンドを使用します。
BWプロセスチェーン起動コマンドが起動されると「BWプロセスチェーン起動コマンドの処理の流れ」に示すような流れで動作し、引数に指定された内容でBWのプロセスチェーンを起動して結果を標準出力に出力します。

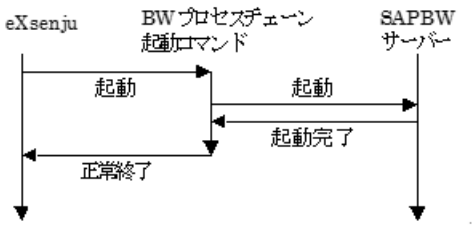


図 7.9 BWプロセスチェーン起動コマンドの処理の流れ

警告

BWプロセスチェーン起動コマンド(sjPEX_bwChain_start)は、R/3ジョブスケジュールコマンド(sjPEX_r3job)とは異なり、SAPサーバーでBWのプロセスチェーンを起動させるだけで、終了するまで監視しつづけるということは行いません。
別途BWプロセスチェーン状態確認コマンド(sjPEX_bwChain_check)を実行し、状態を確認して下さい。

BWプロセスチェーン起動コマンド(sjPEX_bwChain_start)の詳しい使用方法については、「BWプロセスチェーン起動コマンド(sjPEX_bwChain_start)の利用方法」を参照して下さい。

7.3.3.2. BWプロセスチェーンの状態を確認

BWプロセスチェーン起動コマンドで起動させたBWのプロセスチェーンの状態を確認するために、BWプロセスチェーン状態確認コマンド(sjPEX_bwChain_check)を使用します。
BWプロセスチェーン状態確認コマンドが起動されると「BWプロセスチェーン状態確認コマンドの処理の流れ」に示すような流れで動作し、引数に指定された内容でBWのプロセスチェーンの状態を確認して結果を標準出力に出力します。

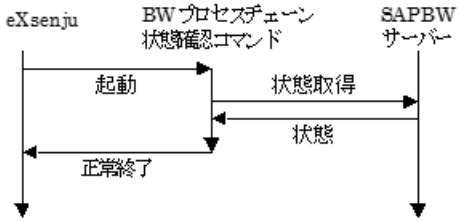


図 7.10 BWプロセスチェーン状態確認コマンドの処理の流れ

表 7.4 プロセスチェーンの状態一覧

プロセスチェーンの状態
‘A’ : (active)
‘G’ : (green)
‘R’ : (red)
‘X : (aborted)

BWプロセスチェーン状態確認コマンド(sjPEX_bwChain_check)の詳しい使用方法については、「BWプロセスチェーン状態確認コマンド(sjPEX_bwChain_check)の利用方法」を参照して下さい。

7.3.4. 他のJob Scheduler for R/3コマンド群の利用方法

Job Scheduler for R/3コマンド群で、R/3ジョブスケジュールコマンド(sjPEX_r3job)以外に、以下に示す22個のコマンドがあります。

- R/3ジョブ定義取得コマンド(sjPEX_r3job_defget)
- R/3ジョブログ取得コマンド(sjPEX_r3job_logget)
- R/3ジョブ状態確認コマンド(sjPEX_r3job_check)
- R/3ジョブバリアント取得コマンド(sjPEX_r3job_variant)
- R/3ジョブログ設定コマンド(sjPEX_r3job_logset)
- R/3ジョブ削除コマンド(sjPEX_r3job_delete)
- R/3ジョブ起動コマンド(sjPEX_r3job_start)
- R/3ジョブ検索コマンド(sjPEX_r3job_select)
- R/3ジョブ管理情報照会コマンド(sjPEX_r3job_confprint)
- R/3ジョブコピーコマンド(sjPEX_r3job_copy)（＊注）
- R/3ジョブ強制停止コマンド(sjPEX_r3job_stop)（＊注）
- R/3ジョブ子ジョブ取得コマンド(sjPEX_r3job_listChildJobs)（＊注）
- R/3ジョブスプール取得コマンド(sjPEX_r3job_listSpool)（＊注）
- R/3イベント送信コマンド(sjPEX_r3job_sendEvent)（＊注）
- R/3プリンター覧コマンド(sjPEX_r3job_listOutputDevice)（＊注）
- R/3 ABAPレポート一覧コマンド(sjPEX_r3job_listABAPReport)（＊注）
- R/3ジョブバリアント変更コマンド(sjPEX_r3job_variantChange)（＊注）
- BWプロセスチェーン検索コマンド(sjPEX_bwChain_select)（＊注）
- BWプロセスチェーン起動コマンド(sjPEX_bwChain_start)（＊注）
- BWプロセスチェーン状態確認コマンド(sjPEX_bwChain_check)（＊注）
- BWプロセスチェーンログ取得コマンド(sjPEX_bwChain_logget)（＊注）
- BWプロセスチェーンプロセス一覧コマンド(sjPEX_bwChain_processList)（＊注）
- BWプロセスチェーンプロセスログ取得コマンド(sjPEX_bwChain_processLog)（＊注）

注釈

＊：SAP ERP用R/3ジョブ連携コマンドのみ対応しています。

7.3.4.1. R/3ジョブ定義取得コマンド(sjPEX_r3job_defget)の利用方法

R/3ジョブ定義取得コマンド(sjPEX_r3job_defget)は、以前に稼働させたR/3ジョブスケジュールコマンド(sjPEX_r3job)によって登録、実行されたR/3ジョブやR/3サーバーで直接定義されたジョブの定義内容を表示するコマンドです。
R/3ジョブ定義取得コマンドが起動されると、引数に指定された内容でR/3のジョブの定義を取得し、結果を標準出力に出力します。
R/3ジョブ定義取得コマンドを起動する際に指定する引数には、以下に示す内容を指定して下さい。

警告

引数を指定する場合、アルファベットの大文字と小文字を絶対に間違えないようにして下さい。

```
sjPEX_r3job_defget
        -cl クライアント -u R/3ユーザー名 -p パスワード -d デスティネーション
        { ●Senju DevOperation Conductorジョブ指定 | ●R/3ジョブ指定 }
        [-l 言語] [-lv XMI監視レベル]
   ● Senju DevOperation Conductorジョブ指定(＊注):
        -date 運用日付 -f フレーム名 -n ネット名 -j Senju DevOperation Conductorジョブ名 [-jn ジョブ番号 | -
all]
   ● R/3ジョブ指定:
        -j R/3ジョブ名 [-jc ジョブカウント | -all]
```

注釈

＊：Senju DevOperation Conductorジョブ指定のオプションを指定する場合は、R/3ジョブスケジュールコマンド(sjPEX_r3job)を稼働させたエージェント上で実行して下さい。

オプション	省略	デフォルト	長さ	説明
-cl	不可		3	クライアント
-u	不可		12	R/3ユーザー名
-p	不可		8	パスワード
-d	不可		32	デスティネーション
-j	不可		32	Senju DevOperation Conductorジョブ名
-l	可	E	1	言語[J/E/D](J:日本語、E:英語、D:独語)
-lv	可	0	1	XMI監視レベル[0-3]
-date	可		8	運用日付
-f	可		32	フレーム名
-n	可		32	ネット名
-all	可	最新のジョブ	0	同一ジョブ名すべての定義内容を出力
-jc	可	最新のジョブ	8	ジョブカウント(R/3)
-jn	可	最新のジョブ	8	ジョブ番号(Senju DevOperation Conductor)

- クライアント、R/3ユーザー名、パスワード、言語には、「R/3ログオン画面」で入力する内容と同じものを指定して下さい。(言語は省略すると'E'になります。)
- デスティネーションには、saprfc.iniのデスティネーションを指定して下さい。(saprfc.iniについては、「saprfc.iniの設定」を参照して下さい。)
- -jc(ジョブカウント)はR/3上の管理情報です。同一ジョブ名を区別するために使用されます。R/3ジョブ検索コマンド(sjPEX_r3job_select)及びSAPGUI等で確認することができます。
- -jn(ジョブ番号)はSenju DevOperation Conductor上の管理情報です。同一運用日付、同一フレーム、同一ネット、同一ジョブをR/3ジョブスケジュールコマンド(sjPEX_r3job)で複数回稼働させた場合に昇順に付加されます。R/3ジョブ管理情報照会コマンド(sjPEX_r3job_confprint)で確認することができます。
- Senju DevOperation Conductorジョブ名で指定する場合、R/3ジョブスケジュールコマンド(sjPEX_r3job)を稼働させた運用日付、フレーム名、ネット名、ジョブ名で指定して下さい。
- R/3ジョブ名で指定する場合、R/3ジョブ検索コマンド(sjPEX_r3job_select)やSAPGUI等で ジョブカウントを確認の上、そのジョブカウントを指定して下さい。
- -jn及び-jcの代わりに-allを指定した場合、同一ジョブ名のすべての定義情報を表示します。
- -jn,--jc,-allすべてを省略した場合、指定したジョブの最新(最後に登録された)の定義情報を表示します。

【実行例】

- 設定

クライアント	500
R/3ユーザー名	ABC
パスワード	pass
デスティネーション	R3SRV1
運用日付	19980801
フレーム名	R3_FRM1
ネット名	R3_NET2
ジョブ名	R3_CALC

- コマンドライン:

```
sjPEX_r3job_defget -cl 500 -u ABC -p pass -d R3SRV1 -date 19980801 -f R3_FRM1
-n R3_NET2 -j R3_CALC
```

- 実行結果:

```
Job[R3_CALC] Count[09573501] definition
Job Header ====================
JOBNAME    : R3_CALC
JOBCOUNT   : 09573501
JOBGROUP   :
INTREPORT  : %NEWSTEP
STEPCOUNT  : 1
SDLSTRTDT  : 19980908
SDLSTRTTM  : 172452

（中略）

EOMCORRECT : 0
CALCORRECT : 0

Job Step :  1 ====================
PROGRAM    : CALC
TYP        : A
PARAMETER  :
AUTHCKNAM  : ABC
LISTIDENT  :
XPGID      :
XPGTGTSYS  :
   :
（以下略）
```

7.3.4.2. R/3ジョブログ取得コマンド(sjPEX_r3job_logget)の利用方法

R/3ジョブログ取得コマンド(sjPEX_r3job_logget)は、以前に稼働させたR/3ジョブスケジュールコマンド(sjPEX_r3job)によって登録、実行されたR/3ジョブのジョブログを表示するコマンドです。
R/3ジョブログ取得コマンドが起動されると、引数に指定された内容でR/3のジョブのジョブログを取得し、結果を標準出力に出力します。
R/3ジョブログ取得コマンドを起動する際に指定する引数には、以下に示す内容を指定して下さい。

警告

引数を指定する場合、アルファベットの大文字と小文字を絶対に間違えないようにして下さい。

```
sjPEX_r3job_logget
        -cl クライアント -u R/3ユーザー名 -p パスワード -d デスティネーション
        { ●Senju DevOperation Conductorジョブ指定 | ●R/3ジョブ指定 }
        [-l 言語] [-lv XMI監視レベル] { [-detail] | [-new] }
  ● Senju DevOperation Conductorジョブ指定(＊注):
        -date 運用日付 -f フレーム名 -n ネット名 -j Senju DevOperation Conductorジョブ名 [-jn ジョブ番号 | -
all]
  ● R/3ジョブ指定:
        -j R/3ジョブ名 [-jc ジョブカウント | -all]
```

注釈

＊:Senju DevOperation Conductorジョブ指定のオプションを指定する場合は、R/3ジョブスケジュールコマンド(sjPEX_r3job)を稼働させたエージェント上で実行して下さい。

オプション	省略	デフォルト	長さ	説明
-cl	不可		3	クライアント
-u	不可		12	R/3ユーザー名
-p	不可(※1)		8(※2)	パスワード
-d	不可		32	デスティネーション
-j	不可		32	Senju DevOperation Conductorジョブ名
-l	可	E	1	言語[J/E/D](J:日本語、E:英語、D:独語)
-lv	可	0	1	XMI監視レベル[0-3]
-date	可		8	運用日付
-f	可		32	フレーム名
-n	可		32	ネット名
-all	可	最新のジョブ	0	同一ジョブ名すべての定義内容を出力
-jc	可	最新のジョブ	8	ジョブカウント(R/3)
-jn	可	最新のジョブ	8	ジョブ番号(Senju DevOperation Conductor)
-detail	可	簡易表示	0	詳細表示を行う
-new	可	旧形式表示	0	簡易表示時、メッセージIDを付加し表示する

- クライアント、R/3ユーザー名、パスワード、言語には、「R/3ログオン画面」で入力する内容と同じものを指定して下さい(言語は省略すると'E'になります)。
- デスティネーションには、saprfc.iniのデスティネーションを指定して下さい(saprfc.iniについては、「saprfc.iniの設定」を参照して下さい)。
- -jc(ジョブカウント)はR/3上の管理情報です。同一ジョブ名を区別するために使用されます。R/3ジョブ検索コマンド(sjPEX_r3job_select)及びSAPGUI等で確認することができます。
- -jn(ジョブ番号)はSenju DevOperation Conductor上の管理情報です。同一運用日付、同一フレーム、同一ネット、同一ジョブをR/3ジョブスケジュールコマンド(sjPEX_r3job)で複数回稼働させた場合に昇順に付加されます。R/3ジョブ管理情報照会コマンド(sjPEX_r3job_confprint)で確認することができます。
- Senju DevOperation Conductorジョブ名で指定する場合、R/3ジョブスケジュールコマンド(sjPEX_r3job)を稼働させた運用日付、フレーム名、ネット名、ジョブ名で指定して下さい。
- R/3ジョブ名で指定する場合、R/3ジョブ検索コマンド(sjPEX_r3job_select)やSAPGUI等で ジョブカウントを確認の上、そのジョブカウントを指定して下さい。
- -jn及び-jcの代わりに-allを指定した場合、同一ジョブ名のすべてのジョブログを表示します。
- -jn,-jc,-allすべてを省略した場合、指定したジョブの最新(最後に登録された)のジョブログを表示します。

注釈

(※1) SAP ERP(RFC SDK 7.20)用R/3ジョブ連携コマンドに限り、設定を行うことで-pオプションを省略できます。設定方法については、「 パスワード指定の省略方法 」を参照して下さい。

(※2) SAP ERP(RFC SDK 7.20)用R/3ジョブ連携コマンドに限り、指定可能なパスワードの文字列長は40です。これにより、SAP NetWeaver6.40以降のSAPサーバーに接続できます。

【実行例】

- 設定

クライアント	500
R/3ユーザー名	ABC
パスワード	pass
デスティネーション	R3SRV1
運用日付	19980801
フレーム名	R3_FRM1
ネット名	R3_NET2
ジョブ名	R3_CALC

1. 言語が英語の場合("-l"オプションを付けなかった場合)
    - コマンドライン:

```
 sjPEX_r3job_logget -cl 500 -u ABC -p pass -d R3SRV1 -date 19980801 -f R3_FRM1
-n R3_NET2 -j R3_CALC
```

    - 実行結果:

```
Job[R3_CALC] Count[09573501] joblog
DATE     TIME   CODE  TEXT
--------|------|-----|----------------------
19980908 172453 00516 Job started
19980908 172453 00550 Step 001 started (program CALC, variant , username ABC,
language E)
19980908 172453 00550 Step 002 started (program CALC2, variant CALC_VAR2, user
name ABC, language E)
19980908 172454 00517 Job finished
```

2. 言語が日本語の場合("-l J"オプションを付けた場合)
    - コマンドライン:

```
 sjPEX_r3job_logget -cl 500 -u ABC -p pass -d R3SRV1 -date 19980801 -f R3_FRM1
-n R3_NET2 -j R3_CALC -l J
```

    - 実行結果:

```
Job[R3_CALC] Count[09573501] joblog
DATE     TIME   CODE  TEXT
--------|------|-----|----------------------
19980908 172453 00516 ジョブを開始しました
19980908 172453 00550 ステップ 001 を開始しました(プログラム CALC、バリアント 、ユーザー名 ABC 言語 E)
19980908 172453 00550 ステップ 002 を開始しました(プログラムCALC2、バリアントCALC_VAR2、ユーザー名 ABC 言語 E)
19980908 172454 00517 ジョブを終了しました
```

3. 簡易表示形式でメッセージ付加形式の場合(“-new”オプションを付けた場合)

    - コマンドライン:

```
 sjPEX_r3job_logget -cl 500 -u ABC -p pass -d R3SRV1 -date 19980801 -f R3_FRM1
-n R3_NET2 -j R3_CALC -l J -new
```

    - 実行結果:

```
Job[R3_CALC] Count[09573501] joblog
DATE     TIME   MSGID               CODE  TEXT
--------|------|-------------------|-----|----------------------
19980908 172453 MSG00001            00516 ジョブを開始しました
19980908 172453 MSG00002            00550 ステップ 001 を開始しました(プログラム CALC、バリアント 、ユーザー名 ABC 言語 E)
19980908 172453 MSG00003            00550 ステップ 002 を開始しました(プログラムCALC2、バリアントCALC_VAR2、ユーザー名 ABC 言語 E)
19980908 172454 MSG00004            00517 ジョブを終了しました
```

7.3.4.3. R/3ジョブ状態確認コマンド(sjPEX_r3job_check)の利用方法

R/3ジョブ状態確認コマンド(sjPEX_r3job_check)は、以前に稼働させたR/3ジョブスケジュールコマンド(sjPEX_r3job)によって登録、実行されたR/3ジョブの状態を確認するコマンドです。
R/3ジョブ状態確認コマンドが起動されると、引数に指定された内容でR/3のジョブの状態を確認し、結果を標準出力に出力します。
このコマンドは、ごくまれにR/3サーバー上のR/3ジョブの状態と、R/3のDB上のR/3ジョブの状態が異なることがあるため用意されています。もし、すでに正常終了しているはずのR/3ジョブの状態がまだ稼働中になっているといったようなことがありましたら、このコマンドを使用してみて下さい。
R/3ジョブ状態確認コマンドを起動する際に指定する引数には、以下に示す内容を指定して下さい。

警告

引数を指定する場合、アルファベットの大文字と小文字を絶対に間違えないようにして下さい。

```
sjPEX_r3job_check
        -cl クライアント -u R/3ユーザー名 -p パスワード -d デスティネーション
        { ●Senju DevOperation Conductorジョブ指定 | ●R/3ジョブ指定 }
        [-child] [-l 言語] [-lv XMI監視レベル]
  ● Senju DevOperation Conductorジョブ指定(＊注):
        -date 運用日付 -f フレーム名 -n ネット名 -j Senju DevOperation Conductorジョブ名 [-jn ジョブ番号 | -all]
  ● R/3ジョブ指定:
        -j R/3ジョブ名 [-jc ジョブカウント | -all]
```

注釈

＊:Senju DevOperation Conductorジョブ指定のオプションを指定する場合は、R/3ジョブスケジュールコマンド(sjPEX_r3job)を稼働させたエージェント上で実行して下さい。

オプション	省略	デフォルト	長さ	説明
-cl	不可		3	クライアント
-u	不可		12	R/3ユーザー名
-p	不可		8	パスワード
-d	不可		32	デスティネーション
-j	不可		32	Senju DevOperation Conductorジョブ名
-child	可	指定R/3ジョブのみ表示	0	指定R/3ジョブおよび子ジョブを表示
-l	可	E	1	言語[J/E/D](J:日本語、E:英語、D:独語)
-lv	可	0	1	XMI監視レベル[0-3]
-date	可		8	運用日付
-f	可		32	フレーム名
-n	可		32	ネット名
-all	可	最新のジョブ	0	同一ジョブ名すべての定義内容を出力
-jc	可	最新のジョブ	8	ジョブカウント(R/3)
-jn	可	最新のジョブ	8	ジョブ番号(Senju DevOperation Conductor)

- クライアント、R/3ユーザー名、パスワード、言語には、「R/3ログオン画面」で入力する内容と同じものを指定して下さい(言語は省略すると'E'になります)。
- デスティネーションには、saprfc.iniのデスティネーションを指定して下さい(saprfc.iniについては、「saprfc.iniの設定」を参照して下さい)。
- jc(ジョブカウント)はR/3上の管理情報です。同一ジョブ名を区別するために使用されます。R/3ジョブ検索コマンド(sjPEX_r3job_select)及びSAPGUI等で確認することができます。
- -jn(ジョブ番号)はSenju DevOperation Conductor上の管理情報です。同一運用日付、同一フレーム、同一ネット、同一ジョブをR/3ジョブスケジュールコマンド(sjPEX_r3job)で複数回稼働させた場合に昇順に付加されます。R/3ジョブ管理情報照会コマンド(sjPEX_r3job_confprint)で確認することができます。
- Senju DevOperation Conductorジョブ名で指定する場合、R/3ジョブスケジュールコマンド(sjPEX_r3job)を稼働させた運用日付、フレーム名、ネット名、ジョブ名で指定して下さい。
- R/3ジョブ名で指定する場合、R/3ジョブ検索コマンド(sjPEX_r3job_select)やSAPGUI等で ジョブカウントを確認の上、そのジョブカウントを指定して下さい。
- -jn及び-jcの代わりに-allを指定した場合、同一ジョブ名のすべてのジョブの状態を表示します。
- -jn,-jc,-allすべてを省略した場合、指定したジョブの最新(最後に登録された)のジョブの状態を表示します。

【実行例】

- 設定

クライアント	500
R/3ユーザー名	ABC
パスワード	pass
デスティネーション	R3SRV1
運用日付	19980801
フレーム名	R3_FRM1
ネット名	R3_NET2
ジョブ名	R3_CALC

1. 指定R/3ジョブのみ表示する場合("-child"オプションを付けなかった場合)
    - コマンドライン:

```
 sjPEX_r3job_check -cl 500 -u ABC -p pass -d R3SRV1 -date 19980801 -f R3_FRM1
-n R3_NET2 -j R3_CALC
```

    - 実行結果:

```
Job[R3_CALC] Count[09573501] status
status : F (finished)      (DB status : F)
```

注釈

- 左のstatusが正しい状態で、右のDB statusがDB上での状態になります。
- statusの見方は、「R/3ジョブスケジュールコマンドの処理の流れ」を参照して下さい。

2. 指定R/3ジョブおよび子ジョブを表示する場合(“-child”オプションを付けた場合)

    - コマンドライン:

```
 sjPEX_r3job_check -cl 500 -u ABC -p pass -d R3SRV1 -date 19980801 -f R3_FRM1
-n R3_NET2 -j R3_CALC -child
```

    - 実行結果:

```
 1 : Job[R3_CALC] Count[09573501] status
status   : F (finished)
HasChild : P (parent)

 2 : Job[CHILD_3] Count[09594801] status
status   : S (released)
HasChild : C (child)

 3 : Job[CHILD_1] Count[09594801] status
status   : S (released)
HasChild : C (child)

 4 : Job[CHILD_2] Count[09594801] status
status   : S (released)
HasChild : C (child)
```

7.3.4.4. R/3ジョブバリアント取得コマンド(sjPEX_r3job_variant)の利用方法

R/3ジョブバリアント取得コマンド(sjPEX_r3job_variant)は、ABAP/4プログラムで使用できる定義済みのバリアントを表示するコマンドです。
R/3ジョブバリアント取得コマンドが起動されると、引数に指定された内容でABAP/4プログラムで使用できる定義済みのバリアントを取得し、結果を標準出力に出力します。
R/3ジョブバリアント取得コマンドを起動する際に指定する引数には、以下に示す内容を指定して下さい。

警告

引数を指定する場合、アルファベットの大文字と小文字を絶対に間違えないようにして下さい。

```
sjPEX_r3job_variant
        -cl クライアント -u R/3ユーザー名 -p パスワード -d デスティネーション
        -a ABAP/4プログラム名 [-v ABAP/4バリアント名] [-detail]
        [-l 言語] [-lv XMI監視レベル]
```

オプション	省略	デフォルト	長さ	説明
-cl	不可		3	クライアント
-u	不可		12	R/3ユーザー名
-p	不可		8	パスワード
-d	不可		32	デスティネーション
-a	不可		40	ABAP/4プログラム名
-v	可		14	ABAP/4バリアント名
-detail	可	簡易表示	0	詳細表示を行う
-l	可	E	1	言語[J/E/D](J:日本語、E:英語、D:独語)
-lv	可	0	1	XMI監視レベル[0-3]

- クライアント、R/3ユーザー名、パスワード、言語には、「R/3ログオン画面」で入力する内容と同じものを指定して下さい(言語は省略すると'E'になります)。
- デスティネーションには、saprfc.iniのデスティネーションを指定して下さい(saprfc.iniについては、「saprfc.iniの設定」を参照して下さい)。
- ABAP/4プログラム名には、使用できる定義済みのバリアントを表示したいABAP/4プログラム名を指定して下さい。

【実行例】

- 設定

クライアント	500
R/3ユーザー名	ABC
パスワード	pass
デスティネーション	R3SRV1
ABAP/4プログラム名	CALC2

1. バリアントの一覧のみ取得する場合(“-detail”オプションを付けなかった場合)
    - コマンドライン:
    ```
    sjPEX_r3job_variant -cl 500 -u ABC -p pass -d R3SRV1 -a CALC2
    ```
    - 実行結果:
    ```
    "CALC2" has 2 VARIANT
     1 : REPORT : CALC2     VARIANT : CALC_VAR2
     2 : REPORT : CALC2     VARIANT : CALC_VAR2B
    ```
2. バリアントのパラメータや選択オプションも取得する場合(“-detail”オプションを付けた場合)
    - コマンドライン:
    ```
    sjPEX_r3job_variant -cl 500 -u ABC -p pass -d R3SRV1 -a CALC2 -detail
    ```
    - 実行結果:
    ```
    "CALC2" has 2 VARIANT
     1 : REPORT : CALC2     VARIANT : CALC_VAR2   TEXT : CALC variant2
          1 : Parameter     : X_VAL       Value : 15
          2 : Parameter     : X_VAL       Value : 15

     2 : REPORT : CALC2     VARIANT : CALC_VAR2B  TEXT : CALC variant2B
          1 : Parameter     : X_VAL       Value : 30
          2 : Parameter     : X_VAL       Value : 30
    ```

7.3.4.5. R/3ジョブログレベル設定コマンド(sjPEX_r3job_logset) の利用方法

R/3ジョブログレベル設定コマンド(sjPEX_r3job_logset)は、R/3ジョブスケジュールコマンド(sjPEX_r3job)によって登録、実行されるR/3ジョブのジョブログのレベルを設定するコマンドです。
R/3ジョブログレベル設定コマンドが起動されると、引数に指定された内容でR/3のジョブログレベルを設定し、結果を標準出力に出力します。
R/3ジョブログレベル設定コマンドを起動する際に指定する引数には、以下に示す内容を指定して下さい。

警告

引数を指定する場合、アルファベットの大文字と小文字を絶対に間違えないようにして下さい。

```
jPEX_r3job_logset
        -cl クライアント -u R/3ユーザー名 -p パスワード -d デスティネーション
        [-l 言語] -lv R/3ログレベル
```

オプション	省略	デフォルト	長さ	説明
-cl	不可		3	クライアント
-u	不可		12	R/3ユーザー名
-p	不可		8	パスワード
-d	不可		32	デスティネーション
-lv	不可	0	1	R/3 ログレベル[0-3]
-l	可	E	1	言語[J/E/D](J:日本語、E:英語、D:独語)

- クライアント、R/3ユーザー名、パスワード、言語には、「R/3ログオン画面」で入力する内容と同じものを指定して下さい(言語は省略すると'E'になります)。
- デスティネーションには、saprfc.iniのデスティネーションを指定して下さい(saprfc.iniについては、「saprfc.iniの設定」を参照して下さい)。

【実行例】

- 設定

クライアント	500
R/3ユーザー名	ABC
パスワード	pass
デスティネーション	R3SRV1

- コマンドライン:

```
sjPEX_r3job_logset -cl 500 -u ABC -p pass -d R3SRV1 -lv 3
```

- 実行結果:

```
sjPEX_r3job_logset : loglevel set to 3
```

7.3.4.6. R/3ジョブ削除コマンド(sjPEX_r3job_delete) の利用方法

R/3ジョブ削除コマンド(sjPEX_r3job_delete)は、Senju DevOperation ConductorまたはSAPGUIなどから登録、実行したR/3ジョブをR/3上から削除します。削除されたジョブの情報は一切残りませんので本コマンドを実行する場合は細心の注意を払うようにして下さい。
R/3ジョブ削除コマンドが起動されると、引数に指定された内容でR/3ジョブを削除し、結果を標準出力に出力します。
R/3ジョブ削除コマンドを起動する際に指定する引数には、以下に示す内容を指定して下さい。

警告

引数を指定する場合、アルファベットの大文字と小文字を絶対に間違えないようにして下さい。

```
sjPEX_r3job_delete
        -cl クライアント -u R/3ユーザー名 -p パスワード -d デスティネーション
        { ●Senju DevOperation Conductorジョブ指定 | ●R/3ジョブ指定 }
        [-l 言語] [-lv XMI監視レベル] [-q]
  ● Senju DevOperation Conductorジョブ指定(＊注):
        -date 運用日付 -f フレーム名 -n ネット名 -j Senju DevOperation Conductorジョブ名 [-jn ジョブ番号 | -
all]
  ● R/3ジョブ指定:
        -j R/3ジョブ名 [-jc ジョブカウント | -all]
```

注釈

＊:Senju DevOperation Conductorジョブ指定のオプションを指定する場合は、R/3ジョブスケジュールコマンド(sjPEX_r3job)を稼働させたエージェント上で実行して下さい。

オプション	省略	デフォルト	長さ	説明
-cl	不可		3	クライアント
-u	不可		12	R/3ユーザー名
-p	不可		8	パスワード
-d	不可		32	デスティネーション
-j	不可		32	Senju DevOperation Conductorジョブ名
-l	可	E	1	言語[J/E/D](J:日本語、E:英語、D:独語)
-lv	可	0	1	XMI監視レベル[0-3]
-date	可		8	運用日付
-f	可		32	フレーム名
-n	可		32	ネット名
-all	可	最新のジョブ	0	同一ジョブ名すべての定義内容を出力
-jc	可	最新のジョブ	8	ジョブカウント(R/3)
-jn	可	最新のジョブ	8	ジョブ番号(Senju DevOperation Conductor)
-q	可	問合せなし	0	削除時問合せ要求の有無

- クライアント、R/3ユーザー名、パスワード、言語には、「R/3ログオン画面」で入力する内容と同じものを指定して下さい(言語は省略すると'E'になります)。
- デスティネーションには、saprfc.iniのデスティネーションを指定して下さい(saprfc.iniについては、「saprfc.iniの設定」を参照して下さい)。
- -jc(ジョブカウント)はR/3上の管理情報です。同一ジョブ名を区別するために使用されます。R/3ジョブ検索コマンド(sjPEX_r3job_select)及びSAPGUI等で確認することができます。
- -jn(ジョブ番号)はSenju DevOperation Conductor上の管理情報です。同一運用日付、同一フレーム、同一ネット、同一ジョブをR/3ジョブスケジュールコマンド(sjPEX_r3job)で複数回稼働させた場合に昇順に付加されます。R/3ジョブ管理情報照会コマンド(sjPEX_r3job_confprint)で確認することができます。

- Senju DevOperation Conductorジョブ名で指定する場合、R/3ジョブスケジュールコマンド(sjPEX_r3job)を稼働させた運用日付、フレーム名、ネット名、ジョブ名で指定して下さい。
- R/3ジョブ名で指定する場合、R/3ジョブ検索コマンド(sjPEX_r3job_select)やSAPGUI等で ジョブカウントを確認の上、そのジョブカウントを指定して下さい。
- -jn及び-jcの代わりに-allを指定した場合、同一ジョブ名のすべてのジョブを削除します。
- -jn,-jc,-allすべてを省略した場合、指定したジョブの最新(最後に登録された)のジョブを削除します。
- -qオプションは削除時に削除確認問い合わせ要求をさせたいときに指定して下さい。
- XMI監視レベルを2以上(-lv 2)にしないと本機能のXMIログは保存されません。

【実行例】

- 設定

クライアント	500
R/3ユーザー名	ABC
パスワード	pass
デスティネーション	R3SRV1
運用日付	19980801
フレーム名	R3_FRM1
ネット名	R3_NET2
ジョブ名	R3_CALC

1. 問合せ要求を指定していない場合
    - コマンドライン:
    ```
     sjPEX_r3job_delete -cl 500 -u ABC -p pass -d R3SRV1 -date 19980801 -f R3_FRM1
    -n R3_NET2 -j R3_CALC
    ```
    - 実行結果:
    ```
    Job[R3_CALC] Count[09573501] delete
    delete ok
    ```
2. 全てのジョブを対象として問合せ要求を指定した場合
    - コマンドライン:
    ```
     sjPEX_r3job_delete -cl 500 -u ABC -p pass -d R3SRV1 -date 19980801 -f R3_FRM1
    -n R3_NET2 -j R3_CALC -all -q
    ```
    - 実行結果:
    ```
    R/3[Job: R3_CALC Count: 20153001] delete OK(Y/N)?
    Y     ･･･要求応答
    delete ok

    R/3[Job: R3_CALC Count: 20231001] delete OK(Y/N)?
    N     ･･･要求応答
     ...Not delete.

    R/3[Job: R3_CALC Count: 20553001] delete OK(Y/N)?
    Y     ･･･要求応答
    delete ok
    ```

7.3.4.7. R/3ジョブ起動コマンド(sjPEX_r3job_start) の利用方法

R/3ジョブ起動コマンド(sjPEX_r3job_start)は、既にR/3上に定義済みのR/3ジョブを起動し、終了するまでの間、監視を行ないます。

R/3ジョブ起動コマンドは、Senju DevOperation Conductorのジョブスケジュールサブシステムでジョブとして登録実行させる方法と、千手コマンドとして実行させる方法の二つの方法で実行が可能です。しかし、ジョブモニタ上で監視を行なう場合は必ず、前者の方法を選択して下さい。

R/3ジョブスケジュールコマンドをSenju DevOperation Conductorのジョブスケジュールサブシステムでジョブとして登録／利用する方法は、Senju DevOperation Conductorのマニュアル「**5 ジョブスケジュール**」の「**5.2 ジョブスケジュールの使い方**」及び「R/3ジョブスケジュールコマンドをジョブとして登録」、「R/3ジョブスケジュールコマンドをジョブとして利用」を参照して下さい。

R/3ジョブスケジュール起動コマンドを登録あるいは設定定義する際に指定する引数には、以下に示す内容を指定して下さい。

警告

- 引数を指定する場合、アルファベットの大文字と小文字を絶対に間違えないようにして下さい。
- SAP ERP(RFC SDK 7.20)用のR/3ジョブ起動コマンドはWindowsエージェントのみで使用可能です。

```
sjPEX_r3job_start
        -cl クライアント -u R/3ユーザー名 -p パスワード -d デスティネーション
        [-l 言語] [-lv XMI監視レベル]
        [-jh R/3ジョブの対象ホスト名 | ジョブサーバグループ名] [-i インターバル] [-s]
        -j R/3ジョブ名 [-jc ジョブカウント]
```

オプション	省略	デフォルト	長さ	説明
-cl	不可		3	クライアント
-u	不可		12	R/3ユーザー名
-p	不可		8	パスワード
-d	不可		32	デスティネーション
-j	不可		32	Senju DevOperation Conductorジョブ名
-l	可	E	1	言語[J/E/D](J:日本語、E:英語、D:独語)
-lv	可	0	1	XMI監視レベル[0-3]
-i	可	60	3	ステータスチェックインターバル[10-900]
-s	可	R/3サーバーに依存	0	即時実行
-jh	可	R/3サーバーに依存	32	R/3ジョブの対象ホスト名／ジョブサーバグループ名
-jc	可	最新のジョブ	8	ジョブカウント

- クライアント、R/3ユーザー名、パスワード、言語には、「R/3ログオン画面」で入力する内容と同じものを指定して下さい（言語は省略すると'E'になります）。
- デスティネーションには、saprfc.iniのデスティネーションを指定して下さい（saprfc.iniについては、「saprfc.iniの設定」を参照して下さい）。
- -jc(ジョブカウント)はR/3上の管理情報です。同一ジョブ名を区別するために使用されます。R/3ジョブ検索コマンド(sjPEX_r3job_select)及びSAPGUI等で確認することができます。
- R/3ジョブ名を指定する場合、R/3ジョブ検索コマンド(sjPEX_r3job_select)やSAPGUI等で ジョブカウントを確認の上、そのジョブカウントを指定して下さい。
- -jcを省略した場合、指定したジョブの最新(最後に登録された)のジョブを起動します。
- インターバルには、R/3ジョブスケジュールコマンドがR/3ジョブの監視を行う間隔(秒)を指定して下さい（インターバルは省略すると60(秒)になります）。
- -sオプションを指定すると、R/3のジョブのスケジュールをR/3のサーバーに任せずに、即時に起動します（すぐに起動できなかった場合は、R/3ジョブスケジュールコマンドは異常終了します）。

【実行例】

- 設定

クライアント	500
R/3ユーザー名	ABC
パスワード	pass
デスティネーション	R3SRV1
R/3ジョブ名	JOB1

- コマンドライン:

```
sjPEX_r3job_check -cl 500 -u ABC -p pass -d R3SRV1 -j JOB1
```

- 実行結果:

```
sjPEX_r3job_startコマンドの実行結果はすべて千手ブラウザのメッセージモニタに表示されます。
```

7.3.4.8. R/3ジョブ検索コマンド(sjPEX_r3job_select)の利用方法

R/3ジョブ検索コマンド(sjPEX_r3job_select)は、R/3サーバーに定義される全てのジョブを対象として、引数で指定する条件に一致するジョブとジョ

ブカウントを抽出し表示するコマンドです。
R/3ジョブ検索コマンドが起動されると、引数に指定された内容でR/3ジョブを検索し、結果を標準出力に出力します。
R/3ジョブ検索コマンドを起動する際に指定する引数には、以下に示す内容を指定して下さい。

警告

- 引数を指定する場合、アルファベットの大文字と小文字を絶対に間違えないようにして下さい。
- コマンドを実行し取得した情報が膨大である場合には、コマンド実行時のメッセージを表示するウインドウでは、全ての情報を表示できない場合があるので、アウトプットビューを参照して下さい。

```
sjPEX_r3job_select
        -cl クライアント -u R/3ユーザー名 -p パスワード -d デスティネーション
        [-l 言語] [-lv XMI監視レベル]
        [-ju R/3ジョブユーザー名] [-j R/3ジョブ名] [-jc ジョブカウント]
        [-sdate 検索開始日付] [-stime 検索開始時刻]
        [-edate 検索終了日付] [-etime 検索終了時刻]
        [-nodate] [-withpred] [-eid イベントID] [-eparm イベントパラメータ]
        [-status R/3ジョブの状態]
        [-status R/3ジョブの状態] ..
```

オプション	省略	デフォルト	長さ	説明
-cl	不可		3	クライアント
-u	不可		12	R/3ユーザー名
-p	不可		8	パスワード
-d	不可		32	デスティネーション
-j	不可		32	Senju DevOperation Conductorジョブ名
-l	可	E	1	言語[J/E/D](J:日本語、E:英語、D:独語)
-lv	可	0	1	XMI監視レベル[0-3]
-ju	可		12	R/3ジョブユーザー名（ワイルドカード指定可能）
-j	可		32	R/3ジョブ名（ワイルドカード指定可能）
-jc	可		8	ジョブカウント
-sdate	可		8	検索開始日付[yyyymmdd]
-stime	可		6	検索開始時刻[hhmmss]
-edate	可		8	検索終了日付[yyyymmdd]
-etime	可		6	検索終了時刻[hhmmss]
-nodate	可		0	開始条件なしで定義されたジョブ
-withpred	可		0	先行ジョブの実行を待つジョブ
-eid	可		32	イベントID（ワイルドカード指定可能）
-eparam	可		64	イベントパラメータ（ワイルドカード指定可能）
-status	可		1	R/3ジョブの状態 [P、S、Y、R、F、A]

- クライアント、R/3ユーザー名、パスワード、言語には、「R/3ログオン画面」で入力する内容と同じものを指定して下さい（言語は省略すると'E'になります）。
- デスティネーションには、saprfc.iniのデスティネーションを指定して下さい（saprfc.iniについては、「saprfc.iniの設定」を参照して下さい）。
- `R/3ジョブ名、R/3ジョブユーザー名、イベントID、イベントパラメータはワイルドカードを用いて指定することができます。その場合はジョブ名等を'’で囲んで下さい。（例：'JOB*' 及び '*SENJU'等）`
- Senju DevOperation Conductorからスケジュールしたジョブのみを検索対象にする場合は-uオプションで指定したR/3ユーザー名を-juオプションでも指定して下さい。
- -statusオプションで指定可能なジョブの状態はP（登録済み）、S（リリース済み）、W（起動待ち）、R（稼働中）、E（正常終了）、A（異常終了）です。なお、複数の状態を検索する場合は繰り返して指定して下さい。また、省略した場合はすべての状態のジョブを検索します。
- R/3ジョブが登録された日付(時刻)で検索する場合は検索開始日付(時刻)、検索終了日付(時刻)で範囲指定して下さい。尚、日付は8桁の西暦で入力して下さい。（例：2000年7月31日なら20000731）。時刻は6桁で入力して下さい。（例：15時5分30秒なら150530）
- 開始条件を指定せずに定義されたジョブ(ジョブ開始日付及び時刻未設定等)を検索する場合は-nodateを指定して下さい。
- 先行ジョブの実行を待つように定義されたジョブを検索する場合は-withpredを指定して下さい。
- イベントIDが定義されているジョブのみを検索する場合は-eidオプションでその定義内容を指定して下さい。
- イベントパラメータが定義されているジョブのみを検索する場合は-eparmオプションでその定義内容を指定して下さい。
- XMI監視レベルを2以上(-lv 2)にしないと本機能のXMIログは保存されません。

【実行例】

- 設定

クライアント	500
R/3ユーザー名	ABC
パスワード	pass
デスティネーション	R3SRV1

1. ユーザー名(USER*)とジョブ名(JOB*)を指定

    - コマンドライン:

```
sjPEX_r3job_select -cl 500 -u ABC -p pass -d R3SRV1 -ju 'USER*' -j 'JOB*'
```

    - 実行結果:

```
SELECTED:  1 ====================
JOBNAME:  JOBaltair-B
JOBCOUNT: 11522601
SELECTED:  2 ====================
JOBNAME:  JOBaltair-A
JOBCOUNT: 13212701
```

2. 開始日時(2000年8月18日 12:00:00)、終了日時(2000年8月18日 23:00:00)を指定

    - コマンドライン:

```
 sjPEX_r3job_select -cl 500 -u ABC -p pass -d R3SRV1 -sdate 20000818 -stime 120000
-edate 20000818 -etime 230000
```

    - 実行結果:

```
SELECTED:  1 ====================
JOBNAME:  altair-B
JOBCOUNT: 13212701
SELECTED:  2 ====================
JOBNAME:  R3_DEF_A01
JOBCOUNT: 19222601
SELECTED:  3 ====================
JOBNAME:  R3_DEF_AE11
JOBCOUNT: 22222701
```

7.3.4.9. R/3ジョブ管理情報照会コマンド(sjPEX_r3job_confprint)の利用方法

R/3ジョブ管理情報照会コマンド(sjPEX_r3job_confprint)は、Senju DevOperation ConductorからR/3サーバーに登録したジョブを対象として、R/3の管理情報(ジョブ名とジョブカウント)からSenju DevOperation Conductorでの管理情報(運用日付、フレーム名、ネット名)を抽出し表示するコマンドです。
R/3ジョブ管理情報照会コマンドを起動する際に指定する引数には、以下に示す内容を指定して下さい。

警告

引数を指定する場合、アルファベットの大文字と小文字を絶対に間違えないようにして下さい。

```
sjPEX_r3job_confprint
        -j ジョブ名 [-jc ジョブカウント]
```

オプション	省略	デフォルト	長さ	説明
-j	不可		14	R/3ジョブ名
-jc	可	全て	8	R/3ジョブカウント

- ジョブ名は、情報照会したいR/3ジョブ名を指定して下さい。
- ジョブカウントは、情報照会したいR/3ジョブのジョブカウントを指定して下さい。

【実行例】

1. ジョブ名(R3_JOB)を指定

    - コマンドライン:

```
sjPEX_r3job_confprint -j R3_JOB
```

- 実行結果:

```
*************************************************************************
JobName  :  R3_JOB
-------------------------------------------------------------------------
  > Date.Frame : 20000801.SAP_FRAME_01
      |---> Net: SAP_NET_01   JobName:R3_JOB / JobCount:12345600
      |---> Net: SAP_NET_02   JobName:R3_JOB / JobCount:23451000
      |---> Net: SAP_NET_05   JobName:R3_JOB / JobCount:16451200
       +----------------------------------------------------------------
```

2. ジョブ名(R3_JOB)とジョブカウント(12345600)を指定

- コマンドライン:

```
sjPEX_r3job_confprint -j R3_JOB -jc 12345600
```

- 実行結果:

```
*************************************************************************
JobName  :  R3_JOB / JobCount :  12345600
-------------------------------------------------------------------------
  > Date.Frame : 20000801.SAP_FRAME_01
      |---> Net: SAP_NET_01   JobName:R3_JOB / JobCount:12345600
       +----------------------------------------------------------------
```

7.3.4.10. R/3ジョブコピーコマンド(sjPEX_r3job_copy) の利用方法

R/3ジョブコピーコマンド(sjPEX_r3job_copy)は、Senju DevOperation ConductorまたはSAPGUIなどから登録実行したR/3ジョブをR/3上でコピーします。コピー先のR/3ジョブの状態は「'P':予定済(scheduled)」になります。
R/3ジョブコピーコマンドが起動されると、引数に指定された内容でR/3ジョブをコピーし、結果を標準出力に出力します。
R/3ジョブコピーコマンドを起動する際に指定する引数には、以下に示す内容を指定して下さい。

警告

引数を指定する場合、アルファベットの大文字と小文字を絶対に間違えないようにして下さい。

```
sjPEX_r3job_copy
        -cl クライアント -u R/3ユーザー名 -p パスワード -d デスティネーション
        { ●Senju DevOperation Conductorジョブ指定 | ●R/3ジョブ指定 }
        [-jcopy 新R/3ジョブ名]
        [-l 言語] [-lv XMI監視レベル] [-q]
  ● Senju DevOperation Conductorジョブ指定(＊注):
        -date 運用日付 -f フレーム名 -n ネット名 -j Senju DevOperation Conductorジョブ名 [-jn ジョブ番号 | -
all]
  ● R/3ジョブ指定:
        -j R/3ジョブ名 [-jc ジョブカウント | -all]
```

注釈

＊:Senju DevOperation Conductorジョブ指定のオプションを指定する場合は、R/3ジョブスケジュールコマンド(sjPEX_r3job)を稼働させたエージェント上で実行して下さい。

オプション	省略	デフォルト	長さ	説明
-cl	不可		3	クライアント
-u	不可		12	R/3ユーザー名
-p	不可		8	パスワード
-d	不可		32	デスティネーション
-j	不可		32	Senju DevOperation Conductorジョブ名
-l	可	E	1	言語[J/E/D](J:日本語、E:英語、D:独語)
-lv	可	0	1	XMI監視レベル[0-3]
-date	可		8	運用日付
-f	可		32	フレーム名
-n	可		32	ネット名
-all	可	最新のジョブ	0	同一ジョブ名すべての定義内容を出力
-jc	可	最新のジョブ	8	ジョブカウント(R/3)
-jn	可	最新のジョブ	8	ジョブ番号(Senju DevOperation Conductor)
-jcopy	可	コピー元と同名	32	コピー先のR/3ジョブ名
-q	可	問合せなし	0	コピー時問合せ要求の有無

- クライアント、R/3ユーザー名、パスワード、言語には、「R/3ログオン画面」で入力する内容と同じものを指定して下さい(言語は省略すると'E'になります)。
- デスティネーションには、saprfc.iniのデスティネーションを指定して下さい(saprfc.iniについては、「saprfc.iniの設定」を参照して下さい)。
- -jc(ジョブカウント)はR/3上の管理情報です。同一ジョブ名を区別するために使用されます。R/3ジョブ検索コマンド(sjPEX_r3job_select)及びSAPGUI等で確認することができます。
- -jn(ジョブ番号)はSenju DevOperation Conductor上の管理情報です。同一運用日付、同一フレーム、同一ネット、同一ジョブをR/3ジョブスケジュールコマンド(sjPEX_r3job)で複数回稼働させた場合に昇順に付加されます。R/3ジョブ管理情報照会コマンド(sjPEX_r3job_confprint)で確認することができます。
- Senju DevOperation Conductorジョブ名で指定する場合、R/3ジョブスケジュールコマンド(sjPEX_r3job)を稼働させた運用日付、フレーム名、ネット名、ジョブ名で指定して下さい。
- R/3ジョブ名で指定する場合、R/3ジョブ検索コマンド(sjPEX_r3job_select)やSAPGUI等で ジョブカウントを確認の上、そのジョブカウントを指定して下さい。
- -jn及び-jcの代わりに-allを指定した場合、同一ジョブ名のすべてのジョブをコピーします。
- -jn,-jc,-allすべてを省略した場合、指定したジョブの最新(最後に登録された)のジョブをコピーします。
- -qオプションはコピー時にコピー確認問い合わせ要求をさせたいときに指定して下さい。
- XMI監視レベルを2以上(-lv 2)にしないと本機能のXMIログは保存されません。

【実行例】

- 設定

クライアント	500
R/3ユーザー名	ABC
パスワード	pass
デスティネーション	R3SRV1
運用日付	19980801
フレーム名	R3_FRM1
ネット名	R3_NET2
ジョブ名	R3_CALC

1. 問合せ要求を指定していない場合
    - コマンドライン:

```
 sjPEX_r3job_copy -cl 500 -u ABC -p pass -d R3SRV1 -date 19980801 -f R3_FRM1
-n R3_NET2 -j R3_CALC
```

    - 実行結果:

```
Job[R3_CALC] Count[09573501] copy
copy ok New count[21734001]
```

2. 全てのジョブを対象として問合せ要求を指定した場合

- コマンドライン:

```
 sjPEX_r3job_copy -cl 500 -u ABC -p pass -d R3SRV1 -date 19980801 -f R3_FRM1
-n R3_NET2 -j R3_CALC -all -q
```

- 実行結果:

```
R/3[Job: R3_CALC Count: 20153001] copy OK(Y/N)?
Y     ･･･要求応答
copy ok New count[21735001]

R/3[Job: R3_CALC Count: 20231001] copy OK(Y/N)?
N     ･･･要求応答
 ...Not copy.

R/3[Job: R3_CALC Count: 20553001] copy OK(Y/N)?
Y     ･･･要求応答
copy ok New count[21755001]
```

7.3.4.11. R/3ジョブ強制停止コマンド(sjPEX_r3job_stop) の利用方法

R/3ジョブ強制停止コマンド(sjPEX_r3job_stop)は、Senju DevOperation ConductorまたはSAPGUIなどから登録、実行したR/3ジョブを強制停止します。強制停止されたジョブの状態は「'A':中止(terminated)」になります。
R/3ジョブ強制停止コマンドが起動されると、引数に指定された内容でR/3ジョブを強制停止し、結果を標準出力に出力します。
R/3ジョブ強制停止コマンドを起動する際に指定する引数には、以下に示す内容を指定して下さい。

警告

引数を指定する場合、アルファベットの大文字と小文字を絶対に間違えないようにして下さい。

```
sjPEX_r3job_stop
        -cl クライアント -u R/3ユーザー名 -p パスワード -d デスティネーション
        { ●Senju DevOperation Conductorジョブ指定 | ●R/3ジョブ指定 }
        [-l 言語] [-lv XMI監視レベル]
  ● Senju DevOperation Conductorジョブ指定(＊注①):
        -date 運用日付 -f フレーム名 -n ネット名 -j Senju DevOperation Conductorジョブ名 [-jn ジョブ番号 | -
all]
  ● R/3ジョブ指定:
        -j R/3ジョブ名 [-jc ジョブカウント | -all]
```

注釈

注①: Senju DevOperation Conductorジョブ指定のオプションを指定する場合は、R/3ジョブスケジュールコマンド(sjPEX_r3job)を稼働させたエージェント上で実行して下さい。

オプション	省略	デフォルト	長さ	説明
-cl	不可		3	クライアント
-u	不可		12	R/3ユーザー名
-p	不可		8	パスワード
-d	不可		32	デスティネーション
-j	不可		32	Senju DevOperation Conductorジョブ名
-l	可	E	1	言語[J/E/D](J:日本語、E:英語、D:独語)
-lv	可	0	1	XMI監視レベル[0-3]
-date	可		8	運用日付
-f	可		32	フレーム名
-n	可		32	ネット名
-all	可	最新のジョブ	0	同一ジョブ名すべての定義内容を出力
-jc	可	最新のジョブ	8	ジョブカウント(R/3)
-jn	可	最新のジョブ	8	ジョブ番号(Senju DevOperation Conductor)

- クライアント、R/3ユーザー名、パスワード、言語には、「R/3ログオン画面」で入力する内容と同じものを指定して下さい(言語は省略すると'E'になります)。
- デスティネーションには、saprfc.iniのデスティネーションを指定して下さい(saprfc.iniについては、「saprfc.iniの設定」を参照して下さい)。
- -jc(ジョブカウント)はR/3上の管理情報です。同一ジョブ名を区別するために使用されます。R/3ジョブ検索コマンド(sjPEX_r3job_select)及びSAPGUI等で確認することができます。
- -jn(ジョブ番号)はSenju DevOperation Conductor上の管理情報です。同一運用日付、同一フレーム、同一ネット、同一ジョブをR/3ジョ

ブスケジュールコマンド(sjPEX_r3job)で複数回稼働させた場合に昇順に付加されます。R/3ジョブ管理情報照会コマンド(sjPEX_r3job_confprint)で確認することができます。

- Senju DevOperation Conductorジョブ名で指定する場合、R/3ジョブスケジュールコマンド(sjPEX_r3job)を稼働させた運用日付、フレーム名、ネット名、ジョブ名で指定して下さい。
- R/3ジョブ名で指定する場合、R/3ジョブ検索コマンド(sjPEX_r3job_select)やSAPGUI等で ジョブカウントを確認の上、そのジョブカウントを指定して下さい。
- -jn及び-jcの代わりに-allを指定した場合、同一ジョブ名のすべてのジョブを強制停止します。
- -jn,-jc,-allすべてを省略した場合、指定したジョブの最新(最後に登録された)のジョブを強制停止します。
- XMI監視レベルを2以上(-lv 2)にしないと本機能のXMIログは保存されません。

【実行例】

- 設定

クライアント	500
R/3ユーザー名	ABC
パスワード	pass
デスティネーション	R3SRV1
運用日付	19980801
フレーム名	R3_FRM1
ネット名	R3_NET2
ジョブ名	R3_CALC

- コマンドライン:

```
 sjPEX_r3job_stop -cl 500 -u ABC -p pass -d R3SRV1 -date 19980801 -f R3_FRM1
-n R3_NET2 -j R3_CALC
```

- 実行結果:

```
Job[R3_CALC] Count[09573501] job stop
stop ok
```

7.3.4.12. R/3ジョブ子ジョブ取得コマンド(sjPEX_r3job_listChildJobs) の利用方法

R/3ジョブ子ジョブ取得コマンド(sjPEX_r3job_listChildJobs)は、Senju DevOperation ConductorまたはSAPGUIなどから登録、実行したR/3ジョブの子ジョブを表示します。
R/3ジョブ子ジョブ取得コマンドが起動されると、引数に指定された内容でR/3ジョブの子ジョブを取得し、結果を標準出力に出力します。
R/3ジョブ子ジョブ取得コマンドを起動する際に指定する引数には、以下に示す内容を指定して下さい。

警告

引数を指定する場合、アルファベットの大文字と小文字を絶対に間違えないようにして下さい。

```
sjPEX_r3job_listChildJobs
        -cl クライアント -u R/3ユーザー名 -p パスワード -d デスティネーション
        { ●Senju DevOperation Conductorジョブ指定 | ●R/3ジョブ指定 }
        [-l 言語] [-lv XMI監視レベル]
  ● Senju DevOperation Conductorジョブ指定(＊注):
        -date 運用日付 -f フレーム名 -n ネット名 -j Senju DevOperation Conductorジョブ名 [-jn ジョブ番号 | -
all]
  ● R/3ジョブ指定:
        -j R/3ジョブ名 [-jc ジョブカウント | -all]
```

注釈

＊:Senju DevOperation Conductorジョブ指定のオプションを指定する場合は、R/3ジョブスケジュールコマンド(sjPEX_r3job)を稼働させたエージェント上で実行して下さい。

オプション	省略	デフォルト	長さ	説明
-cl	不可		3	クライアント
-u	不可		12	R/3ユーザー名
-p	不可		8	パスワード
-d	不可		32	デスティネーション
-j	不可		32	Senju DevOperation Conductorジョブ名
-l	可	E	1	言語[J/E/D](J:日本語、E:英語、D:独語)
-lv	可	0	1	XMI監視レベル[0-3]
-date	可		8	運用日付
-f	可		32	フレーム名
-n	可		32	ネット名
-all	可	最新のジョブ	0	同一ジョブ名すべての定義内容を出力
-jc	可	最新のジョブ	8	ジョブカウント(R/3)
-jn	可	最新のジョブ	8	ジョブ番号(Senju DevOperation Conductor)

- クライアント、R/3ユーザー名、パスワード、言語には、「R/3ログオン画面」で入力する内容と同じものを指定して下さい（言語は省略すると'E'になります）。
- デスティネーションには、saprfc.iniのデスティネーションを指定して下さい（saprfc.iniについては、「saprfc.iniの設定」を参照して下さい）。
- -jc(ジョブカウント)はR/3上の管理情報です。同一ジョブ名を区別するために使用されます。R/3ジョブ検索コマンド(sjPEX_r3job_select)及びSAPGUI等で確認することができます。
- -jn(ジョブ番号)はSenju DevOperation Conductor上の管理情報です。同一運用日付、同一フレーム、同一ネット、同一ジョブをR/3ジョブスケジュールコマンド(sjPEX_r3job)で複数回稼働させた場合に昇順に付加されます。R/3ジョブ管理情報照会コマンド(sjPEX_r3job_confprint)で確認することができます。
- Senju DevOperation Conductorジョブ名で指定する場合、R/3ジョブスケジュールコマンド(sjPEX_r3job)を稼働させた運用日付、フレーム名、ネット名、ジョブ名で指定して下さい。
- R/3ジョブ名で指定する場合、R/3ジョブ検索コマンド(sjPEX_r3job_select)やSAPGUI等で ジョブカウントを確認の上、そのジョブカウントを指定して下さい。
- -jn及び-jcの代わりに-allを指定した場合、同一ジョブ名のすべてのジョブを強制停止します。
- -jn,-jc,-allすべてを省略した場合、指定したジョブの最新(最後に登録された)のジョブを強制停止します。
- XMI監視レベルを2以上(-lv 2)にしないと本機能のXMIログは保存されませ

【実行例】

- 設定

クライアント	500
R/3ユーザー名	ABC
パスワード	pass
デスティネーション	R3SRV1
運用日付	19980801
フレーム名	R3_FRM1
ネット名	R3_NET2
ジョブ名	R3_CALC

- コマンドライン:

```
 sjPEX_r3job_listChildJobs -cl 500 -u ABC -p pass -d R3SRV1 -date 19980801 -f R3_FRM1
-n R3_NET2 -j R3_CALC
```

- 実行結果:

```
Job[R3_CALC] Count[09573501] child jobs
 1 : JOBNAME : CHILD_4  JOBCOUNT : 09573801
 2 : JOBNAME : CHILD_2  JOBCOUNT : 09573701
 3 : JOBNAME : CHILD_3  JOBCOUNT : 09573801
 4 : JOBNAME : CHILD_1  JOBCOUNT : 09573701
```

7.3.4.13. R/3ジョブスプール取得コマンド(sjPEX_r3job_listSpool) の利用方法

R/3ジョブスプール取得コマンド(sjPEX_r3job_listSpool)は、Senju DevOperation ConductorまたはSAPGUIなどから登録、実行したR/3ジョブのスプールを表示します。
R/3ジョブスプール取得コマンドが起動されると、引数に指定された内容でR/3ジョブのスプールを取得し、結果を標準出力に出力します。
R/3ジョブスプール取得コマンドを起動する際に指定する引数には、以下に示す内容を指定して下さい。

警告

引数を指定する場合、アルファベットの大文字と小文字を絶対に間違えないようにして下さい。

```
sjPEX_r3job_listSpool
        -cl クライアント -u R/3ユーザー名 -p パスワード -d デスティネーション
        { ●Senju DevOperation Conductorジョブ指定 | ●R/3ジョブ指定 }
        [-step ステップ番号]
        [-l 言語] [-lv XMI監視レベル]
  ● Senju DevOperation Conductorジョブ指定(＊注①):
        -date 運用日付 -f フレーム名 -n ネット名 -j Senju DevOperation Conductorジョブ名 [-jn ジョブ番号 | -
all]
  ● R/3ジョブ指定:
        -j R/3ジョブ名 [-jc ジョブカウント | -all]
```

注釈

注①: Senju DevOperation Conductorジョブ指定のオプションを指定する場合は、R/3ジョブスケジュールコマンド(sjPEX_r3job)を稼働させたエージェント上で実行して下さい。

オプション	省略	デフォルト	長さ	説明
-cl	不可		3	クライアント
-u	不可		12	R/3ユーザー名
-p	不可		8	パスワード
-d	不可		32	デスティネーション
-j	不可		32	Senju DevOperation Conductorジョブ名
-l	可	E	1	言語[J/E/D](J:日本語、E:英語、D:独語)
-lv	可	0	1	XMI監視レベル[0-3]
-date	可		8	運用日付
-f	可		32	フレーム名
-n	可		32	ネット名
-all	可	最新のジョブ	0	同一ジョブ名すべての定義内容を出力
-jc	可	最新のジョブ	8	ジョブカウント(R/3)
-jn	可	最新のジョブ	8	ジョブ番号(Senju DevOperation Conductor)
-step	可	1	8	ステップ番号(R/3)

- クライアント、R/3ユーザー名、パスワード、言語には、「R/3ログオン画面」で入力する内容と同じものを指定して下さい(言語は省略すると'E'になります)。
- デスティネーションには、saprfc.iniのデスティネーションを指定して下さい(saprfc.iniについては、「saprfc.iniの設定」を参照して下さい)。
- -jc(ジョブカウント)はR/3上の管理情報です。同一ジョブ名を区別するために使用されます。R/3ジョブ検索コマンド(sjPEX_r3job_select)及びSAPGUI等で確認することができます。
- -jn(ジョブ番号)はSenju DevOperation Conductor上の管理情報です。同一運用日付、同一フレーム、同一ネット、同一ジョブをR/3ジョブスケジュールコマンド(sjPEX_r3job)で複数回稼働させた場合に昇順に付加されます。R/3ジョブ管理情報照会コマンド(sjPEX_r3job_confprint)で確認することができます。
- Senju DevOperation Conductorジョブ名で指定する場合、R/3ジョブスケジュールコマンド(sjPEX_r3job)を稼働させた運用日付、フレーム名、ネット名、ジョブ名で指定して下さい。
- R/3ジョブ名で指定する場合、R/3ジョブ検索コマンド(sjPEX_r3job_select)やSAPGUI等で ジョブカウントを確認の上、そのジョブカウントを指定して下さい。
- -jn及び-jcの代わりに-allを指定した場合、同一ジョブ名のすべてのジョブを強制停止します。
- -jn,-jc,-allすべてを省略した場合、指定したジョブの最新(最後に登録された)のジョブを強制停止します。
- XMI監視レベルを2以上(-lv 2)にしないと本機能のXMIログは保存されません。

【実行例】

- 設定

クライアント	500
R/3ユーザー名	ABC
パスワード	pass
デスティネーション	R3SRV1
運用日付	19980801
フレーム名	R3_FRM1
ネット名	R3_NET2
ジョブ名	R3_CALC

- コマンドライン:

```
 sjPEX_r3job_listSpool -cl 500 -u ABC -p pass -d R3SRV1 -date 19980801 -f R3_FRM1
-n R3_NET2 -j R3_CALC
```

- 実行結果:

```
Job[R3_CALC] Count[09573501] Step[1] spool list
 1 : 08.09.1998       R/3 CALC Job    1
 2 : --------------------------------------------------------------------------------
 3 : Start: 08.09.1998 17:24:53
 4 : End  : 08.09.1998 17:24:54
```

7.3.4.14. R/3イベント送信コマンド(sjPEX_r3job_sendEvent) の利用方法

R/3イベント送信コマンド(sjPEX_r3job_sendEvent)は、SAPGUIから起動条件にイベントを指定して登録したR/3ジョブを起動させるために、R/3のイベントを送信するコマンドです。
R/3イベント送信コマンドが起動されると、引数に指定された内容でR/3のイベントを送信し、結果を標準出力に出力します。
R/3イベント送信コマンドを起動する際に指定する引数には、以下に示す内容を指定して下さい。

警告

引数を指定する場合、アルファベットの大文字と小文字を絶対に間違えないようにして下さい。

```
sjPEX_r3job_sendEvent
        -cl クライアント -u R/3ユーザー名 -p パスワード -d デスティネーション
        -eid イベントID [-eparm イベントパラメータ]
        [-l 言語] [-lv XMI監視レベル]
```

オプション	省略	デフォルト	長さ	説明
-cl	不可		3	クライアント
-u	不可		12	R/3ユーザー名
-p	不可		8	パスワード
-d	不可		32	デスティネーション
-eid	不可		32	イベントID
-eparm	可		64	イベントパラメータ
-l	可	E	1	言語[J/E/D](J:日本語、E:英語、D:独語)
-lv	可	0	1	XMI監視レベル[0-3]

- クライアント、R/3ユーザー名、パスワード、言語には、「R/3ログオン画面」で入力する内容と同じものを指定して下さい(言語は省略すると'E'になります)。
- デスティネーションには、saprfc.iniのデスティネーションを指定して下さい(saprfc.iniについては、「saprfc.iniの設定」を参照して下さい)。

【実行例】

- 設定

クライアント	500
R/3ユーザー名	ABC
パスワード	pass
デスティネーション	R3SRV1
イベントID	R3_CALC_EVENT
イベントパラメータ	CALC1

- コマンドライン:

```
sjPEX_r3job_sendEvent -cl 500 -u ABC -p pass -d R3SRV1 -eid R3_CALC_EVENT -eparm CALC1
```

- 実行結果:

```
EventID[R3_CALC_EVENT] Param[CALC1]
send ok
```

7.3.4.15. R/3プリンター覧コマンド(sjPEX_r3job_listOutputDevice) の利用方法

R/3プリンター覧コマンド(sjPEX_r3job_listOutputDevice)は、R/3のプリンター覧を取得するコマンドです。
R/3プリンター覧コマンドが起動されると、引数に指定された内容でR/3のプリンタを取得し、結果を標準出力に出力します。
R/3プリンター覧コマンドを起動する際に指定する引数には、以下に示す内容を指定して下さい。

警告

引数を指定する場合、アルファベットの大文字と小文字を絶対に間違えないようにして下さい。

```
sjPEX_r3job_listOutputDevice
        -cl クライアント -u R/3ユーザー名 -p パスワード -d デスティネーション
        [-l 言語] [-lv XMI監視レベル]
```

オプション	省略	デフォルト	長さ	説明
-cl	不可		3	クライアント
-u	不可		12	R/3ユーザー名
-p	不可		8	パスワード
-d	不可		32	デスティネーション
-l	可	E	1	言語[J/E/D](J:日本語、E:英語、D:独語)
-lv	可	0	1	XMI監視レベル[0-3]

- クライアント、R/3ユーザー名、パスワード、言語には、「R/3ログオン画面」で入力する内容と同じものを指定して下さい(言語は省略すると'E'になります)。
- デスティネーションには、saprfc.iniのデスティネーションを指定して下さい(saprfc.iniについては、「saprfc.iniの設定」を参照して下さい)。

【実行例】

- 設定

クライアント	500
R/3ユーザー名	ABC
パスワード	pass
デスティネーション	R3SRV1

- コマンドライン:

```
sjPEX_r3job_listOutputDevice -cl 500 -u ABC -p pass -d R3SRV1
```

- 実行結果:

```
 1 ====================
DEVICE    : CARL
DEVICETYPE: ASCIIPRI
LAYOUT    :
 2 ====================
DEVICE    : DCC6
DEVICETYPE: SWIN
LAYOUT    :
 3 ====================
DEVICE    : POST
DEVICETYPE: POST2
LAYOUT    :
 4 ====================
DEVICE    : FS
DEVICETYPE: SAPGOF
LAYOUT    :
 5 ====================
DEVICE    : FSA
DEVICETYPE: PLAIN
LAYOUT    :
 6 ====================
DEVICE    : FS 0
DEVICETYPE: PDF1
LAYOUT    :
 7 ====================
DEVICE    : FSX
DEVICETYPE: XSF
LAYOUT    :
 8 ====================
DEVICE    : LOCL
DEVICETYPE: SAPWIN
LAYOUT    :
 9 ====================
DEVICE    : LP01
DEVICETYPE: JPASCII
LAYOUT    :
10 ====================
DEVICE    : LP02
DEVICETYPE: JPPOST
LAYOUT    :
11 ====================
DEVICE    : LP03
DEVICETYPE: JPSAPWIN
LAYOUT    :
12 ====================
DEVICE    : LP04
DEVICETYPE: JPEXPOST
LAYOUT    :
```

7.3.4.16. R/3ABAPレポート一覧コマンド(sjPEX_r3job_listABAPReport)の利用方法

R/3 ABAPレポート一覧コマンド(sjPEX_r3job_listABAPReport)は、R/3のABAPレポート一覧を取得するコマンドです。
R/3 ABAPレポート一覧コマンドが起動されると、引数に指定された内容でR/3のABAPレポートを取得し、結果を標準出力に出力します。
R/3 ABAPレポート一覧コマンドを起動する際に指定する引数には、以下に示す内容を指定して下さい。

警告

引数を指定する場合、アルファベットの大文字と小文字を絶対に間違えないようにして下さい。

```
sjPEX_r3job_listABAPReport
        -cl クライアント -u R/3ユーザー名 -p パスワード -d デスティネーション
        [-a ABAP/4プログラム名]
        [-l 言語] [-lv XMI監視レベル]
```

オプション	省略	デフォルト	長さ	説明
-cl	不可		3	クライアント
-u	不可		12	R/3ユーザー名
-p	不可		8	パスワード
-d	不可		32	デスティネーション
-a	可		40	ABAP/4プログラム名（ワイルドカード指定可能）
-l	可	E	1	言語[J/E/D](J:日本語、E:英語、D:独語)
-lv	可	0	1	XMI監視レベル[0-3]

- クライアント、R/3ユーザー名、パスワード、言語には、「R/3ログオン画面」で入力する内容と同じものを指定して下さい（言語は省略すると'E'になります）。

- デスティネーションには、saprfc.iniのデスティネーションを指定して下さい(saprfc.iniについては、「saprfc.iniの設定」を参照して下さい)。
- ABAP/4プログラム名はワイルドカードを用いて指定することができます。その場合はABAP/4プログラム名を''で囲んで下さい。(例:'JOB*' 及び '*SENJU'等)

【実行例】

- 設定

クライアント	500
R/3ユーザー名	ABC
パスワード	pass
デスティネーション	R3SRV1

1. ABAP/4プログラム名(CALC2)を指定
    - コマンドライン:

```
sjPEX_r3job_listABAPReport -cl 500 -u ABC -p pass -d R3SRV1 -a CALC2
```

    - 実行結果:

```
 1 ====================
ABAPNAME: CALC2
REPORT  : R/3 CALC Job 2
```

2. ABAP/4プログラム名(SAP*TYPE)を指定
    - コマンドライン:

```
sjPEX_r3job_listABAPReport -cl 500 -u ABC -p pass -d R3SRV1 -a 'SAP*TYPE'
```

    - 実行結果:

```
 1 ====================
ABAPNAME: SAPLH99_PRIMARYWAGETYPE
REPORT  :
 2 ====================
ABAPNAME: SAPLH99_WAGETYPE
REPORT  :
 3 ====================
ABAPNAME: SAPLPAK_UTILS_FOR_OBJTYPE
REPORT  :
 4 ====================
ABAPNAME: SAPLPAK_UTILS_FOR_TYPE
REPORT  :
 5 ====================
ABAPNAME: SAPLSEU_DEPTYPE
REPORT  :
 6 ====================
ABAPNAME: SAPLSU_SYSTEMTYPE
REPORT  :
 7 ====================
ABAPNAME: SAPLTMW_TDTYPE
REPORT  :
 8 ====================
ABAPNAME: SAPLW3_DEVTYPE
REPORT  :
 9 ====================
ABAPNAME: SAPRCKM_PRMT_RUN_TYPE
REPORT  : Maintenance of Future Prices with Date and Costing Run Profile
   :
(以下略)
```

7.3.4.17. R/3ジョブバリアント変更コマンド(sjPEX_r3job_variantChange)の利用方法

R/3ジョブバリアント変更コマンド(sjPEX_r3job_variantChange)は、定義済みのバリアントにパラメータや選択オプションが存在する場合に、それらのパラメータや選択オプションを変更するコマンドです。
R/3ジョブバリアント変更コマンドが起動されると、引数に指定された内容でABAP/4プログラムで使用できる定義済みのバリアントを取得し、結果を標準出力に出力します。
R/3ジョブバリアント変更コマンドを起動する際に指定する引数には、以下に示す内容を指定して下さい。

警告

引数を指定する場合、アルファベットの大文字と小文字を絶対に間違えないようにして下さい。

```
sjPEX_r3job_variantChange
        -cl クライアント -u R/3ユーザー名 -p パスワード -d デスティネーション
        -a ABAP/4プログラム名 -v ABAP/4バリアント名 [-vtext 説明]
        [-l 言語] [-lv XMI監視レベル]
        { {-vpParam パラメータ名 -vpLow パラメータの値} |
                {-vpSelect 選択オプション名 -vpOp選択オプションの演算子
                -vpLow 選択オプションの下限値 [-vpHigh 選択オプションの上限値]} }
        [ { {-vpParam -vpLow} | {-vpSelect -vpOp -vpLow [-vpHigh]} } ] ..
```

オプション	省略	デフォルト	長さ	説明
-cl	不可		3	クライアント
-u	不可		12	R/3ユーザー名
-p	不可		8	パスワード
-d	不可		32	デスティネーション
-a	不可		40	ABAP/4プログラム名
-v	不可		14	ABAP/4バリアント名
-vtext	可		30	説明
-vpParam	不可		8	パラメータ名
-vpLow	不可		45	パラメータの値または選択オプションの下限値
-vpSelect	不可		8	選択オプション名
-vpOp	不可		2	選択オプションの演算子(EQ、NE、LT、GT、LE、GE、BT、NB、CP、NP)
-vpHigh	可		45	選択オプションの上限値
-l	可	E	1	言語[J/E/D](J:日本語、E:英語、D:独語)
-lv	可	0	1	XMI監視レベル[0-3]

- クライアント、R/3ユーザー名、パスワード、言語には、「R/3ログオン画面」で入力する内容と同じものを指定して下さい(言語は省略すると'E'になります)。
- デスティネーションには、saprfc.iniのデスティネーションを指定して下さい(saprfc.iniについては、「saprfc.iniの設定」を参照して下さい)。
- ABAP/4プログラム名には、使用できる定義済みのバリアントを表示したいABAP/4プログラム名を指定して下さい。

【実行例】

- 設定

クライアント	500
R/3ユーザー名	ABC
パスワード	pass
デスティネーション	R3SRV1
ABAP/4プログラム名	CALC2
ABAP/4バリアント名	CALC_VAR2

- コマンドライン:

```
sjPEX_r3job_variantChange -cl 500 -u ABC -p pass -d R3SRV1 -a CALC2 -v CALC_VAR2
-vpParam X_VAL -vpLow 10 -vpParam Y_VAL -vpLow 20
```

- 実行結果:

```
ABAP[CALC2] Variant[CALC_VAR2]
 1 : Parameter[X_VAL] Value[10]
 2 : Parameter[Y_VAL] Value[20]
change ok
```

7.3.4.18. BWプロセスチェーン検索コマンド(sjPEX_bwChain_select)の利用方法

BWプロセスチェーン検索コマンド(sjPEX_bwChain_select)は、BWのプロセスチェーンを取得するコマンドです。
BWプロセスチェーン検索コマンドが起動されると、引数に指定された内容でBWのプロセスチェーンを取得し、結果を標準出力に出力します。
BWプロセスチェーン検索コマンドを起動する際に指定する引数には、以下に示す内容を指定して下さい。

警告

引数を指定する場合、アルファベットの大文字と小文字を絶対に間違えないようにして下さい。

```
sjPEX_bwChain_select
        -cl クライアント -u R/3ユーザー名 -p パスワード -d デスティネーション
        [-chain プロセスチェーン名]
        [-l 言語]
```

オプション	省略	デフォルト	長さ	説明
-cl	不可		3	クライアント
-u	不可		12	R/3ユーザー名
-p	不可		8	パスワード
-d	不可		32	デスティネーション
-chain	可		25	プロセスチェーン名
-l	可	E	1	言語[J/E/D](J:日本語、E:英語、D:独語)

- クライアント、R/3ユーザー名、パスワード、言語には、「R/3ログオン画面」で入力する内容と同じものを指定して下さい(言語は省略すると'E'になります)。
- デスティネーションには、saprfc.iniのデスティネーションを指定して下さい(saprfc.iniについては、「saprfc.iniの設定」を参照して下さい)。

【実行例】

- 設定

クライアント	500
R/3ユーザー名	ABC
パスワード	pass
デスティネーション	R3SRV1

1. プロセスチェーン名(MASTER_DATA)を指定
    - コマンドライン:

```
sjPEX_bwChain_select -cl 500 -u ABC -p pass -d R3SRV1 -chain MASTER_DATA
```

    - 実行結果:

```
SELECTED:  1 ====================
CHAIN_ID: MASTER_DATA
LANGU   : D
OBJVERS : M
TXTLG   : Master Data Reorganization
```

2. プロセスチェーン名を省略
    - コマンドライン:

```
sjPEX_bwChain_select -cl 500 -u ABC -p pass -d R3SRV1
```

    - 実行結果:

```
SELECTED:  1 ====================
CHAIN_ID: 0UCMA_PC01
LANGU   : E
OBJVERS : M
TXTLG   : Load and Update Marketing-Relevant Data (Data Init.)
SELECTED:  2 ====================
CHAIN_ID: COH_ATTR
LANGU   : E
OBJVERS : M
TXTLG   : COH_ATTR
   :
(以下略)
```

7.3.4.19. BWプロセスチェーン起動コマンド(sjPEX_bwChain_start)の利用方法

BWプロセスチェーン起動コマンド(sjPEX_bwChain_start)は、BWのプロセスチェーンを起動するコマンドです。
BWプロセスチェーン起動コマンドが起動されると、引数に指定された内容でBWのプロセスチェーンを起動し、結果を標準出力に出力します。
BWプロセスチェーン起動コマンドを起動する際に指定する引数には、以下に示す内容を指定して下さい。

警告

引数を指定する場合、アルファベットの大文字と小文字を絶対に間違えないようにして下さい。

```
sjPEX_bwChain_start
        -cl クライアント -u R/3ユーザー名 -p パスワード -d デスティネーション
        -chain プロセスチェーン名
        [-l 言語]
```

オプション	省略	デフォルト	長さ	説明
-cl	不可		3	クライアント
-u	不可		12	R/3ユーザー名
-p	不可(※1)		8(※2)	パスワード
-d	不可		32	デスティネーション
-chain	不可		25	プロセスチェーン名
-l	可	E	1	言語[J/E/D](J:日本語、E:英語、D:独語)

- クライアント、R/3ユーザー名、パスワード、言語には、「R/3ログオン画面」で入力する内容と同じものを指定して下さい(言語は省略すると'E'になります)。
- デスティネーションには、saprfc.iniのデスティネーションを指定して下さい(saprfc.iniについては、「saprfc.iniの設定」を参照して下さい)。

注釈

(※1) SAP ERP(RFC SDK 7.20)用R/3ジョブ連携コマンドに限り、設定を行うことで-pオプションを省略できます。設定方法については、「パスワード指定の省略方法」を参照して下さい。

(※2) SAP ERP(RFC SDK 7.20)用R/3ジョブ連携コマンドに限り、指定可能なパスワードの文字列長は40です。これにより、SAP NetWeaver6.40以降のSAPサーバーに接続できます。

【実行例】

- 設定

クライアント	500
R/3ユーザー名	ABC
パスワード	pass
デスティネーション	R3SRV1
プロセスチェーン名	MASTER_DATA

- コマンドライン:

```
sjPEX_bwChain_start -cl 500 -u ABC -p pass -d R3SRV1 -chain MASTER_DATA
```

- 実行結果:

```
ChainID[MASTER_DATA] start
LOG_ID : CPBHTQ3NFGSHGO2152HM2FLJA
```

7.3.4.20. BWプロセスチェーン状態確認コマンド(sjPEX_bwChain_check)の利用方法

BWプロセスチェーン状態確認コマンド(sjPEX_bwChain_check)は、BWのプロセスチェーンの状態を確認するコマンドです。
BWプロセスチェーン状態確認コマンドが起動されると、引数に指定された内容でBWのプロセスチェーンの状態を確認し、結果を標準出力に出力します。
BWプロセスチェーン状態確認コマンドを起動する際に指定する引数には、以下に示す内容を指定して下さい。

警告

引数を指定する場合、アルファベットの大文字と小文字を絶対に間違えないようにして下さい。

```
sjPEX_bwChain_check
        -cl クライアント -u R/3ユーザー名 -p パスワード -d デスティネーション
        -chain プロセスチェーン名 -clogid ログID
        [-l 言語]
```

オプション	省略	デフォルト	長さ	説明
-cl	不可		3	クライアント
-u	不可		12	R/3ユーザー名
-p	不可(※1)		8(※2)	パスワード
-d	不可		32	デスティネーション
-chain	不可		25	プロセスチェーン名
-clogid	不可		25	ログID
-l	可	E	1	言語[J/E/D](J:日本語、E:英語、D:独語)

- クライアント、R/3ユーザー名、パスワード、言語には、「R/3ログオン画面」で入力する内容と同じものを指定して下さい(言語は省略すると'E'になります)。
- デスティネーションには、saprfc.iniのデスティネーションを指定して下さい(saprfc.iniについては、「saprfc.iniの設定」を参照して下さい)。
- ログIDには、BWプロセスチェーン起動コマンド(sjPEX_bwChain_start)で出力されたものを指定して下さい。

注釈

(※1) SAP ERP(RFC SDK 7.20)用R/3ジョブ連携コマンドに限り、設定を行うことで-pオプションを省略できます。設定方法については、「パスワード指定の省略方法」を参照して下さい。

(※2) SAP ERP(RFC SDK 7.20)用R/3ジョブ連携コマンドに限り、指定可能なパスワードの文字列長は40です。これにより、SAP NetWeaver6.40以降のSAPサーバーに接続できます。

表 7.5 出力ステータス

status	説明
A (active)	Active
G (green)	Completed successfully
R (red)	Completed but errors occurred
X (aborted)	Canceled

【実行例】

- 設定

クライアント	500
R/3ユーザー名	ABC
パスワード	pass
デスティネーション	R3SRV1
プロセスチェーン名	MASTER_DATA
ログID	CPBHTQ3NFGSHGO2152HM2FLJA

- コマンドライン:

```
 sjPEX_bwChain_check -cl 500 -u ABC -p pass -d R3SRV1 -chain MASTER_DATA
-clogid CPBHTQ3NFGSHGO2152HM2FLJA
```

- 実行結果:

```
ChainID[MASTER_DATA] LogID[CPBHTQ3NFGSHGO2152HM2FLJA] status
status : G (green)
```

7.3.4.21. BWプロセスチェーンログ取得コマンド(sjPEX_bwChain_logget)の利用方法

BWプロセスチェーンログ取得コマンド(sjPEX_bwChain_logget)は、BWのプロセスチェーンのログを取得するコマンドです。
BWプロセスチェーンログ取得コマンドが起動されると、引数に指定された内容でBWのプロセスチェーンのログを取得し、結果を標準出力に出力します。
BWプロセスチェーンログ取得コマンドを起動する際に指定する引数には、以下に示す内容を指定して下さい。

警告

引数を指定する場合、アルファベットの大文字と小文字を絶対に間違えないようにして下さい。

```
sjPEX_bwChain_logget
        -cl クライアント -u R/3ユーザー名 -p パスワード -d デスティネーション
        -chain プロセスチェーン名 -clogid ログID
        [-l 言語]
```

オプション	省略	デフォルト	長さ	説明
-cl	不可		3	クライアント
-u	不可		12	R/3ユーザー名
-p	不可		8	パスワード
-d	不可		32	デスティネーション
-chain	不可		25	プロセスチェーン名
-clogid	不可		25	ログID
-l	可	E	1	言語[J/E/D](J:日本語、E:英語、D:独語)

- クライアント、R/3ユーザー名、パスワード、言語には、「R/3ログオン画面」で入力する内容と同じものを指定して下さい(言語は省略すると'E'になります)。
- デスティネーションには、saprfc.iniのデスティネーションを指定して下さい(saprfc.iniについては、「saprfc.iniの設定」を参照して下さい)。
- ログIDには、BWプロセスチェーン起動コマンド(sjPEX_bwChain_start)で出力されたものを指定して下さい。

【実行例】

- 設定

クライアント	500
R/3ユーザー名	ABC
パスワード	pass
デスティネーション	R3SRV1
プロセスチェーン名	MASTER_DATA
ログID	CPBHTQ3NFGSHGO2152HM2FLJA

- コマンドライン:

```
 sjPEX_bwChain_logget -cl 500 -u ABC -p pass -d R3SRV1 -chain MASTER_DATA
-clogid CPBHTQ3NFGSHGO2152HM2FLJA
```

- 実行結果:

```
ChainID[MASTER_DATA] LogID[CPBHTQ3NFGSHGO2152HM2FLJA] log
Line :  1 ====================
MSGID   : RSPC
MSGNO   : 009
MSGTY   : S
MSGV1   : Start Process
MSGV2   : Process Chain START Variant
MSGV3   : DPG6YOAYPEFVLOWQFWGIZBQBG
MSGV4   : Completed

Line :  2 ====================
MSGID   : RSPC
MSGNO   : 009
MSGTY   : S
MSGV1   : ABAP Program
MSGV2   : 1st Run of BTC
MSGV3   : AQLZOBJTB2NRZANKJJ6Q5NHIA
MSGV4   : Completed

Line :  3 ====================
MSGID   : RSPC
MSGNO   : 009
MSGTY   : S
MSGV1   : ABAP Program
MSGV2   : 2nd Run of BTC
MSGV3   : 7C727E743ASTSDWC061VNL5JM
MSGV4   : Completed

Line :  4 ====================
MSGID   : RSPC
MSGNO   : 009
MSGTY   : S
MSGV1   : AND (Last)
MSGV2   : wait 1 AND 2
MSGV3   : ANDP_C7BD2RULW7JOUW13G429YCPRZ
MSGV4   : Completed

Line :  5 ====================
MSGID   : RSPC
MSGNO   : 009
MSGTY   : S
MSGV1   : AND (Last)
MSGV2   : wait 1 AND 2
MSGV3   : ANDP_2XFVXTXUHNRLPD6H9FWSNHAXD
MSGV4   : Completed

Line :  6 ====================
MSGID   : RSPC
MSGNO   : 009
MSGTY   : S
MSGV1   : ABAP Program
MSGV2   : 3rd and Final program
MSGV3   : B1FO2TH9HF4AHCG579ATD0LXM
MSGV4   : Completed
```

7.3.4.22. BWプロセスチェーンプロセス一覧コマンド(sjPEX_bwChain_processList) の利用方法

BWプロセスチェーンプロセス一覧コマンド(sjPEX_bwChain_processList)は、BWのプロセスチェーンのプロセスを取得するコマンドです。
BWプロセスチェーンプロセス一覧コマンドが起動されると、引数に指定された内容でBWのプロセスチェーンのプロセスを取得し、結果を標準出力に出力します。
BWプロセスチェーンプロセス一覧コマンドを起動する際に指定する引数には、以下に示す内容を指定して下さい。

警告

引数を指定する場合、アルファベットの大文字と小文字を絶対に間違えないようにして下さい。

```
sjPEX_bwChain_processList
        -cl クライアント -u R/3ユーザー名 -p パスワード -d デスティネーション
        -chain プロセスチェーン名 -clogid ログID
        [-detail] [-l 言語]
```

オプション	省略	デフォルト	長さ	説明
-cl	不可		3	クライアント
-u	不可		12	R/3ユーザー名
-p	不可		8	パスワード
-d	不可		32	デスティネーション
-chain	不可		25	プロセスチェーン名
-clogid	不可		25	ログID
-detail	可	簡易表示	0	詳細表示を行う
-l	可	E	1	言語[J/E/D](J:日本語、E:英語、D:独語)

- クライアント、R/3ユーザー名、パスワード、言語には、「R/3ログオン画面」で入力する内容と同じものを指定して下さい(言語は省略すると'E'になります)。
- デスティネーションには、saprfc.iniのデスティネーションを指定して下さい(saprfc.iniについては、「saprfc.iniの設定」を参照して下さい)。
- ログIDには、BWプロセスチェーン起動コマンド(sjPEX_bwChain_start)で出力されたものを指定して下さい。

【実行例】

- 設定

クライアント	500
R/3ユーザー名	ABC
パスワード	pass
デスティネーション	R3SRV1
プロセスチェーン名	MASTER_DATA
ログID	CPBHTQ3NFGSHGO2152HM2FLJA

1. 簡易表示形式
    - コマンドライン:

```
 sjPEX_bwChain_processList -cl 500 -u ABC -p pass -d R3SRV1 -chain MASTER_DATA
-clogid CPBHTQ3NFGSHGO2152HM2FLJA
```

    - 実行結果:

```
ChainID[MASTER_DATA] LogID[CPBHTQ3NFGSHGO2152HM2FLJA] process
 1 ====================
TYPE            : TRIGGER
VARIANTE        : NRIDS_VAR
INSTANCE        : 64VHIL1MGQ93C0T3USHASR5T2
STATE           : F

 2 ====================
TYPE            : ABAP
VARIANTE        : BTCTEST1
INSTANCE        : BWI10T79H804LHKET1ILASDT9
STATE           : F

 3 ====================
TYPE            : ABAP
VARIANTE        : BTCTEST2
INSTANCE        : 8RB4FVNS4KL9AFYV88UXI3DLO
STATE           : F

 4 ====================
TYPE            : AND
VARIANTE        : EVEN_9S4R94DCKHYQ3DQND5OK31GK2
INSTANCE        : ANDP_8LKIEBP9I3GL559458EZTMYYZ
STATE           : F

 5 ====================
TYPE            : AND
VARIANTE        : EVEN_9S4R94DCKHYQ3DQND5OK31GK2
INSTANCE        : ANDP_4GGCJN8C4R7YMV1JMDSWT6VYV
STATE           : F

 6 ====================
TYPE            : ABAP
VARIANTE        : BTCTEST3
INSTANCE        : 714WE91RF0HTOWHZUUT7BYZFX
STATE           : F
```

2. 詳細表示形式

- コマンドライン:

```
 sjPEX_bwChain_processList -cl 500 -u ABC -p pass -d R3SRV1 -chain MASTER_DATA
-clogid CPBHTQ3NFGSHGO2152HM2FLJA -detail
```

- 実行結果:

```
ChainID[MASTER_DATA] LogID[CPBHTQ3NFGSHGO2152HM2FLJA] process
 1 ====================
EVENT_START    :
EVENTP_START   :
EVENTNO_START  : 00
BACKLINK_START :
TYPE           : TRIGGER
VARIANTE       : NRIDS_VAR
PREDECESSOR    : X
INSTANCE       : 64VHIL1MGQ93C0T3USHASR5T2
STATE          : F
EVENT_END      : RSPROCESS
EVENTP_END     : 777LLXHZFJ7MQNTTD4X5KX01H
BACKLINK_END   :
ACTUAL_STATE   : F
EVENT_GREEN    :
EVENTP_GREEN   :
BACKLINK_GREEN :
EVENT_RED      :
EVENTP_RED     :
BACKLINK_RED   :
GREEN_EQ_RED   :
WAIT           : 0
STARTTIMESTAMP :
ENDTIMESTAMP   :
JOB_COUNT      :

 2 ====================
EVENT_START    : RSPROCESS
EVENTP_START   : 777LLXHZFJ7MQNTTD4X5KX01H
EVENTNO_START  : 00
BACKLINK_START :
TYPE           : ABAP
VARIANTE       : BTCTEST1
PREDECESSOR    : X
INSTANCE       : BWI10T79H804LHKET1ILASDT9
STATE          : F
EVENT_END      : RSPROCESS
EVENTP_END     : 6PX4BPV6MQQB20HBJXTVYE4M4
   :
（以下略）
```

7.3.4.23. BWプロセスチェーンプロセスログ取得コマンド(sjPEX_bwChain_processLog) の利用方法

BWプロセスチェーンプロセスログ取得コマンド(sjPEX_bwChain_processLog)は、BWのプロセスチェーンのプロセスのログを取得するコマンドです。
BWプロセスチェーンプロセスログ取得コマンドが起動されると、引数に指定された内容でBWのプロセスチェーンのプロセスのログを取得し、結果を標準出力に出力します。
BWプロセスチェーンプロセスログ取得コマンドを起動する際に指定する引数には、以下に示す内容を指定して下さい。

警告

引数を指定する場合、アルファベットの大文字と小文字を絶対に間違えないようにして下さい。

```
sjPEX_bwChain_processLog
        -cl クライアント -u R/3ユーザー名 -p パスワード -d デスティネーション
        -chain プロセスチェーン名 -clogid ログID
        [-l 言語]
```

オプション	省略	デフォルト	長さ	説明
-cl	不可		3	クライアント
-u	不可		12	R/3ユーザー名
-p	不可		8	パスワード
-d	不可		32	デスティネーション
-chain	不可		25	プロセスチェーン名
-clogid	不可		25	ログID
-l	可	E	1	言語[J/E/D](J:日本語、E:英語、D:独語)

- クライアント、R/3ユーザー名、パスワード、言語には、「R/3ログオン画面」で入力する内容と同じものを指定して下さい(言語は省略すると'E'になります)。
- デスティネーションには、saprfc.iniのデスティネーションを指定して下さい(saprfc.iniについては、「saprfc.iniの設定」を参照して下さい)。
- ログIDには、BWプロセスチェーン起動コマンド(sjPEX_bwChain_start)で出力されたものを指定して下さい。

【実行例】

- 設定

クライアント	500
R/3ユーザー名	ABC
パスワード	pass
デスティネーション	R3SRV1
プロセスチェーン名	MASTER_DATA
ログID	CPBHTQ3NFGSHGO2152HM2FLJA

- コマンドライン:

```
 sjPEX_bwChain_processLog -cl 500 -u ABC -p pass -d R3SRV1 -chain MASTER_DATA
-clogid CPBHTQ3NFGSHGO2152HM2FLJA
```

- 実行結果:

```
ChainID[MASTER_DATA] LogID[CPBHTQ3NFGSHGO2152HM2FLJA] log

Process :  1 ====================
MSGID      : RSPC
MSGNO      : 009
MSGTY      : S
MSGV1      : Start Process
MSGV2      : Process Chain START Variant
MSGV3      : DPG6YOAYPEFVLOWQFWGIZBQBG
MSGV4      : Completed

JOBNAME    : BI_PROCESS_TRIGGER
JOBCOUNT   : 11082802
STATUS     : F (Completed : success)

JOB_LOG :
DATE     TIME   MSGID               CODE TY TEXT
--------|------|--------------------|----|--|----------------------
20060426 145754 00                  516  S Job started
20060426 145754 00                  550  S Step 001 started (program RSPROCESS, variant
&0000000067006, user ID BWALEREMOTE)
20060426 145758 RSMPC               090  S Event RSPROCESS with parameter
777LLXHZFJ7MQNTTD4X5KX01H successfully triggered
20060426 145804 00                  517  S Job finished

Process :  2 ====================
MSGID      : RSPC
MSGNO      : 009
MSGTY      : S
MSGV1      : ABAP Program
MSGV2      : 1st Run of BTC
MSGV3      : AQLZOBJTB2NRZANKJJ6Q5NHIA
MSGV4      : Completed

JOBNAME    : BI_PROCESS_ABAP
JOBCOUNT   : 11082801
STATUS     : F (Completed : success)

JOB_LOG :
DATE     TIME   MSGID               CODE TY TEXT
--------|------|--------------------|----|--|----------------------
20060426 145758 00                  516  S Job started
20060426 145758 00                  550  S Step 001 started (program RSPROCESS, variant
&0000000067001, user ID BWALEREMOTE)
20060426 145759 00                  544  S Test: SY-BATCH indicates background processing
20060426 145811 RSMPC               090  S Event RSPROCESS with parameter
6PX4BPV6MQQB20HBJXTVYE4M4 successfully triggered
20060426 145817 00                  517  S Job finished

   :
（以下略）
```

7.3.5. 付録

7.3.5.1. メッセージ一覧

ID	レベル	表示	警報	メッセージ内容	原因・内容
!PEX500	E	1	ON	R/3ジョブスケジュールコマンドの起動に失敗しました。	R/3ジョブスケジュールコ
!PEX501	E	1	ON	R/3サーバーにログオンできませんでした。	R/3サーバーにログオンて
!PEX502	E	1	ON	R/3ジョブの登録に失敗しました。	R/3ジョブの登録に失敗
!PEX503	E	1	ON	R/3ジョブの起動に失敗しました。	R/3ジョブの起動に失敗
!PEX504	I	1	OFF	R/3ジョブを登録しました。	R/3ジョブを登録しました
!PEX505	E	1	ON	R/3ジョブの状態の取得に失敗しました。	R/3ジョブの状態の取得
!PEX506	I	1	OFF	R/3ジョブが起動しました。	R/3ジョブが起動しました
!PEX507	I	1	OFF	R/3ジョブを強制停止します。	R/3ジョブを強制停止し
!PEX509	E	1	ON	R/3ジョブの強制停止に失敗しました。	R/3ジョブの強制停止に
!PEX510	E	1	ON	R/3ジョブスケジュールコマンドが異常な終了をしました。	R/3ジョブスケジュールコ
!PEX511	E	1	ON	R/3ジョブスケジュールコマンドの起動に失敗しました。	R/3ジョブスケジュールコ
!PEX512	E	1	ON	R/3ジョブスケジュールコマンドの終了まで待てませんでした。	R/3ジョブスケジュールコ
!PEX513	E	1	ON	R/3ジョブが異常終了しました。	R/3ジョブが異常終了し
!PEX514	I	1	OFF	R/3ジョブが正常終了しました。	R/3ジョブが正常終了し
!PEX516	E	1	ON	指定されたABAP/4プログラムはバリアントが必要ですが、まだ1つも定義されていません。	指定されたABAP/4プロ
!PEX517	E	1	ON	指定されたABAP/4プログラムはバリアントの指定が必要です。	指定されたABAP/4プロ
!PEX518	E	1	ON	指定されたABAP/4プログラムには、指定されたバリアントは存在しません。	指定されたABAP/4プロ
!PEX519	E	1	ON	指定されたABAP/4プログラムは存在しません。	指定されたABAP/4プロ
!PEX520	E	1	ON	指定されたABAP/4プログラムはバリアントは必要ありません。	指定されたABAP/4プロ
!PEX521	E	1	ON	ABAP/4プログラムとバリアントの確認に失敗しました。	ABAP/4プログラムとバリ
!PEX522	I	1	OFF	R/3ジョブを削除しました。	R/3ジョブを削除しました
!PEX523	E	1	ON	R/3ジョブの削除に失敗しました。	R/3ジョブの削除に失敗
!PEX524	I	1	OFF	R/3ジョブを変更しました。	R/3ジョブを変更しました
!PEX525	E	1	ON	R/3ジョブの変更に失敗しました。	R/3ジョブの変更に失敗
!PEX526	I	1	OFF	R/3ジョブを強制停止しました。	R/3ジョブを強制停止し
!PEX527	I	1	OFF	R/3ジョブをコピーしました。	R/3ジョブをコピーしまし
!PEX528	E	1	ON	R/3ジョブのコピーに失敗しました。	R/3ジョブのコピーに失敗
!PEX529	I	1	OFF	R/3ジョブのイベントを送信しました。	R/3ジョブのイベントを送
!PEX530	E	1	ON	R/3ジョブのイベント送信に失敗しました。	R/3ジョブのイベント送信
!PEX531	I	1	OFF	BWプロセスチェーンを起動しました。	BWプロセスチェーンを起
!PEX532	E	1	ON	BWプロセスチェーンの起動に失敗しました。	BWプロセスチェーンの起
!PEX533	I	1	OFF	R/3ジョブが指定された稼働猶予時間内で起動しませんでした。	R/3ジョブが指定された
!PEX534	I	1	OFF	R/3ジョブが打ち切り時間内に起動しなかったため、R/3ジョブを削除します。	R/3ジョブが打ち切り時

7.3.5.2. エラーメッセージとその対処方法

R/3ジョブスケジュールコマンド(sjPEX_r3job)およびR/3ジョブ起動コマンド(sjPEX_r3job_start)の実行中にエラーが起きた場合、エラーメッセージがメッセージモニタに表示されますが、それ以外の各コマンドの実行中にエラーが起きた場合、エラーメッセージが標準出力に出力されます。

以下に、R/3ジョブスケジュールコマンド(sjPEX_r3job)およびR/3ジョブ起動コマンド(sjPEX_r3job_start)以外の各コマンド共通で出力されるエラーメッセージを示します。

エラー内容	終了値	対処方法
getenv(SENJUHOME) fail	26	Senju DevOperation Conductorのインストールが正しく行われて
SENJUHOME(*****) is too long	26	Senju DevOperation Conductorのインストールが正しく行われて
getenv(*****) fail	26	Senju DevOperation Conductorのジョブスケジュールサブシステム
getenv(*****) fail (*****(***) too long)	26	Senju DevOperation Conductorのジョブスケジュールサブシステム
chdir(*****) fail	25	Senju DevOperation Conductorのインストールが正しく行われて
*****need num("******" is not num)	17	数字が必要なオプションに、文字を指定していないか確認して下さい
length **("***" is long)	17	オプションに指定した文字列の長さが長すぎます。
*****has no param	17	オプションにパラメータが指定されていません。
duplicate *****option	17	オプションが2重に指定されています。
-I can take only J or E or D("***" is error)	17	オプションはJかEかDしか指定できません
-jn cannot take 0("***" is error)	17	-jnオプションに0を指定することは出来ません。
*****is invalid option	17	不明なオプションが指定されています。
*****option not found	17	必須オプションのうち、足りないオプションがあります。
memory allocate error	27	コマンドが稼働するエージェントでメモリ不足が起きています。
data_file open("***") fail(***)	24	引数に指定された運用日付、フレーム名より特定されるデータファイ 引数の運用日付、フレーム名、ネット名、ジョブ名は正しくあってい データファイル(運用日付.フレーム名)がUNIXの場合は、R/3ジョブ データファイルの読み取り権限はありますか？ ()内のエラー番号より、原因を調べて下さい。
read_jobcount search fail	31	引数に指定された運用日付、フレーム名より特定されるデータファイ 引数の運用日付、フレーム名、ネット名、ジョブ名は正しくあってい データファイルが壊れていませんか？ -jnジョブ番号 を指定した場合、指定したネット名、ジョブ名のレコー
Job[***] cannot find Count	39	引数に指定されたR/3ジョブ名よりジョブカウントを検索することがで 引数のR/3ジョブ名は正しくあっていますか？
RfcOpen failure R/3 exception raised(*****)(func:cll_bapi_xmi_logon,line:***), system exception raised(*****)(func:cll_bapi_xmi_logon,line:***), rfc failure(func:cll_bapi_xmi_logon,line:***), other rfc failure(***)(func:cll_bapi_xmi_logon,line:***)	16	SAP R/3サーバーへのログオンに失敗しました。以下のような原因が 引数のアルファベットの大文字と小文字は正しくあっていますか？ saprfc.iniファイルの内容は正しく、抜けがありませんか？ SAP R/3のサーバーは稼働していますか？ ネットワークケーブルはきちんと接続されていますか？

7.3.5.2.1. R/3ジョブスケジュールコマンド(sjPEX_r3job)

コマンドの実行中にエラーが起きると、エラーメッセージがメッセージモニタに表示されます。

メッセージID	エラー内容	終了値	対処方法
!PEX500	getenv(SENJUHOME) fail	26	Senju DevOperation Conductorのインストールが正しく行われているか確認
	SENJUHOME(*****) is too long	26	Senju DevOperation Conductorのインストールが正しく行われているか確認
	getenv(*****) fail	26	Senju DevOperation Conductorのジョブスケジュールサブシステムのジョブと
	getenv(*****) fail (*****(***) too long)	26	Senju DevOperation Conductorのジョブスケジュールサブシステムのジョブと
	chdir(*****) fail	25	Senju DevOperation Conductorのインストールが正しく行われているか、ディ
	*****need num("******" is not num)	17	数字が必要なオプションに、文字を指定していないか確認して下さい。
	length **("***" is long)	17	オプションに指定した文字列の長さが長すぎます。
	*****has no param	17	オプションにパラメータが指定されていません。
	duplicate *****option	17	オプションが2重に指定されています。
	-i can take 10-300("***" is error)	17	-i オプションは10から300までの数しか指定できません。
	-I can take only J or E or D("***" is error)	17	-I オプションはJかEかDしか指定できません
	-a option is found before -h option	17	-c オプションの後に必要な-h オプションがなく、-a オプションが来ています。
	-v option is found before -a option	17	-v オプションの前に -a オプションが必要です。
	-c option is found before -h option	17	-c オプションの後に必要な-h オプションがなく、-c オプションが来ています。
	-h option is found before -c option	17	-h オプションの前に -c オプションが必要です。
	*****is invalid option	17	不明なオプションが指定されています。
	*****option not found	17	必須オプションのうち、足りないオプションがあります。
	memory allocate error	27	コマンドが稼働するエージェントでメモリ不足が起きています。
!PEX501	R/3 exception raised(*****) system exception raised(*****) rfc failure other rfc failure(***)	16	SAP R/3サーバーへのログオンに失敗しました。以下のような原因が考えられま 引数のアルファベットの大文字と小文字は正しくあっていますか？ saprfc.iniファイルの内容は正しく、抜けがありませんか？ SAP R/3のサーバーは稼働していますか？ネットワークケーブルはきちんと接続
!PEX502	R/3 exception raised(*****) system exception raised(*****) rfc failure other rfc failure(***)	15	R/3ジョブの登録に失敗しました。以下のような原因が考えられます。 引数のアルファベットの大文字と小文字は正しくあっていますか？ 指定したABAP/4プログラム、ABAP/4バリアントは存在しますか？ ABAP/4バリアントを指定しなければならないABAP/4プログラムでABAP/4バ SAP R/3のサーバーは稼働していますか？ネットワークケーブルはきちんと接続
	printer: ****not found	67	指定されたプリンタは存在しません。 正しいプリンタを指定して再実行して下さい。
!PEX503	R/3 exception raised(*****) system exception raised(*****) rfc failure	14	R/3ジョブの起動に失敗しました。以下のような原因が考えられます。 引数のアルファベットの大文字と小文字は正しくあっていますか？ 指定したABAP/4プログラム、ABAP/4バリアントは存在しますか？

メッセージID	エラー内容	終了値	対処方法
!PEX505	R/3 exception raised(*****) system exception raised(*****) rfc failure other rfc failure(***)	13	R/3ジョブの状態の取得に失敗しました。以下のような原因が考えられます。 SAP R/3のサーバーは稼働していますか？ ネットワークケーブルはきちんと接続されていますか？
!PEX509	R/3 job Finish(cannot Abort)	11	R/3ジョブを強制停止しようとしましたが、R/3ジョブは正常終了しました (エラー
	r3job_abort:R/3 job not abort	11	R/3ジョブを強制停止しようとしましたが、最大監視回数内にR/3ジョブが終了 R/3ジョブ状態確認コマンド(sjPEX_r3job_check)を実行するか、R/3のGUI
	R/3 exception raised(*****) system exception raised(*****) rfc failure other rfc failure(***)	11	R/3ジョブの強制停止に失敗しました。以下のような原因が考えられます。 SAP R/3のサーバーは稼働していますか？ ネットワークケーブルはきちんと接続されていますか？
!PEX510	child killed by SIGNAL(***)	19	(UNIX) R/3ジョブスケジュールコマンドの子プロセスがシグナルを受けて終了しま (Windows) Windowsエージェントではこのメッセージは出力されません。
!PEX511	child process start failed(***)	20	R/3ジョブスケジュールコマンドが子プロセスの起動に失敗しました。 ()内のエラー番号より、原因を調べて下さい。
!PEX512	wait error:***	21	R/3ジョブスケジュールコマンドが子プロセスの終了待機に失敗しました。 末尾のエラー番号より、原因を調べて下さい。
	GetExitCodeProcess error:***	22	R/3ジョブスケジュールコマンドが子プロセスの終了値取得に失敗しました。 末尾のエラー番号より、原因を調べて下さい。
!PEX513	R/3 job Abort	12	R/3ジョブが異常終了しました。
!PEX516	ABAP/4:***	41	指定されたABAP/4プログラムはバリアントが必要ですが、まだ1つも定義されて バリアントを定義して再実行して下さい。
!PEX517	ABAP/4:***	42	指定されたABAP/4プログラムはバリアントの指定が必要です。 バリアントを指定して再実行して下さい。
!PEX518	ABAP/4:***	43	指定されたABAP/4プログラムには、指定されたバリアントは存在しません。 バリアント名称を確認して再実行して下さい。
!PEX519	ABAP/4:***	44	指定されたABAP/4プログラムは存在しません。 ABAP/4プログラム名称を確認して再実行して下さい。
!PEX520	ABAP/4:***	45	指定されたABAP/4プログラムはバリアントは必要ありません。 バリアントの指定を削除して再実行して下さい。
!PEX521	R/3 variant info get failed	46	ABAP/4プログラムとバリアントの確認に失敗しました。以下のような原因が考 SAP R/3のサーバーは稼働していますか？ネットワークケーブルはきちんと接続
!PEX534	(エラー文言なし)	69	-kオプションで指定された打ち切り時間までにR/3サーバーで稼働しなかったと R/3サーバーの状態を確認し、再実行して下さい。

7.3.5.2.2. R/3ジョブ起動コマンド(sjPEX_r3job_start)

コマンドの実行中にエラーが起きると、エラーメッセージがメッセージモニタに表示されます。

メッセージID	エラー内容	終了値	対処方法
!PEX500	getenv(SENJUHOME) fail	26	Senju DevOperation Conductorのインストールが正しく行われているか確認
	SENJUHOME(*****) is too long	26	Senju DevOperation Conductorのインストールが正しく行われているか確認
	getenv(*****) fail	26	Senju DevOperation Conductorのジョブスケジュールサブシステムのジョブと
	getenv(*****) fail (*****(***) too long)	26	Senju DevOperation Conductorのジョブスケジュールサブシステムのジョブと
	chdir(*****) fail	25	Senju DevOperation Conductorのインストールが正しく行われているか、ディ
	*****need num("*****" is not num)	17	数字が必要なオプションに、文字を指定していないか確認して下さい。
	length **("**" is long)	17	オプションに指定した文字列の長さが長すぎます。
	*****has no param	17	オプションにパラメータが指定されていません。
	duplicate *****option	17	オプションが2重に指定されています。
	-i can take 10-300("***" is error)	17	-i オプションは10から300までの数しか指定できません。
	-I can take only J or E or D("***" is error)	17	-Iオプションは JかEかDしか指定できません
	*****is invalid option	17	不明なオプションが指定されています。
	*****option not found	17	必須オプションのうち、足りないオプションがあります。
	memory allocate error	27	コマンドが稼働するエージェントでメモリ不足が起きています。
!PEX501	R/3 exception raised(*****) system exception raised(*****) rfc failure other rfc failure(***)	16	SAP R/3サーバーへのログオンに失敗しました。以下のような原因が考えられま 引数のアルファベットの大文字と小文字は正しくあっていますか？ saprfc.iniファイルの内容は正しく、抜けがありませんか？ SAP R/3のサーバーは稼働していますか？ネットワークケーブルはきちんと接続
!PEX502	R/3 exception raised(*****) system exception raised(*****) rfc failure other rfc failure(***)	15	R/3ジョブの登録に失敗しました。以下のような原因が考えられます。 引数のアルファベットの大文字と小文字は正しくあっていますか？ 指定したABAP/4プログラム、ABAP/4バリアントは存在しますか？ ABAP/4バリアントを指定しなければならないABAP/4プログラムでABAP/4バ SAP R/3のサーバーは稼働していますか？ネットワークケーブルはきちんと接続
!PEX503	R/3 exception raised(*****) system exception raised(*****) rfc failure other rfc failure(***)	14	R/3ジョブの起動に失敗しました。以下のような原因が考えられます。 引数のアルファベットの大文字と小文字は正しくあっていますか？ 指定したABAP/4プログラム、ABAP/4バリアントは存在しますか？ ABAP/4バリアントを指定しなければならないABAP/4プログラムでABAP/4バ SAP R/3のサーバーは稼働していますか？ネットワークケーブルはきちんと接続
!PEX505	R/3 exception raised(*****) system exception raised(*****) rfc failure other rfc failure(***)	13	R/3ジョブの状態の取得に失敗しました。以下のような原因が考えられます SAP R/3のサーバーは稼働していますか？ネットワークケーブルはきちんと接続
!PEX509	R/3 job Finish(cannot Abort)	11	R/3ジョブを強制停止しようとしましたが、R/3ジョブは正常終了しました (エラー
	r3job_abort:R/3 job not abort	11	R/3ジョブを強制停止しようとしましたが、最大監視回数内にR/3ジョブが終了

メッセージID	エラー内容	終了値	対処方法
	R/3 exception raised(*****) system exception raised(*****) rfc failure other rfc failure(***)	11	R/3ジョブの強制停止に失敗しました。以下のような原因が考えられます。 SAP R/3のサーバーは稼働していますか？ネットワークケーブルはきちんと接続
!PEX510	child killed by SIGNAL(***)	19	(UNIX) R/3ジョブ起動コマンドの子プロセスがシグナルを受けて終了しました。 (Windows) Windowsエージェントではこのメッセージは出力されません。
!PEX511	child process start failed(***)	20	R/3ジョブ起動コマンドが子プロセスの起動に失敗しました。 ()内のエラー番号より、原因を調べて下さい。
!PEX512	wait error:***	21	R/3ジョブ起動コマンドが子プロセスの終了待機に失敗しました。 末尾のエラー番号より、原因を調べて下さい。
	GetExitCodeProcess error:***	22	R/3ジョブ起動コマンドが子プロセスの終了値取得に失敗しました。 末尾のエラー番号より、原因を調べて下さい。
!PEX513	R/3 job Abort	12	R/3ジョブが異常終了しました。

7.3.5.2.3. R/3ジョブ定義取得コマンド(sjPEX_r3job_defget)

コマンドの実行中にエラーが起きると、エラーメッセージが出力されます。「エラーメッセージとその対処方法」の各コマンド共通のエラーメッセージもあわせて参照して下さい。

エラー内容	終了値	対処方法
R/3 exception raised(*****)(func:cll_bapi_xbp_job_definition_get,line:***), system exception raised(*****)(func:cll_bapi_xbp_job_definition_get,line:***), rfc failure(func:cll_bapi_xbp_job_definition_get,line:***), other rfc failure(***)(func:cll_bapi_xbp_job_definition_get,line:***)	32	R/3ジョブの定義内容の取得に失敗しました。以下の 引数のアルファベットの大文字と小文字は正しくあって saprfc.iniファイルの内容は正しく、抜けがありませんた SAP R/3のサーバーは稼働していますか？ネットワー
R/3 job definition get failed	32	R/3ジョブの定義内容の取得に失敗しました。以下の R/3ジョブ名及びジョブカウントは正しいですか？

7.3.5.2.4. R/3ジョブログ取得コマンド(sjPEX_r3job_logget)

コマンドの実行中にエラーが起きると、エラーメッセージが出力されます。「エラーメッセージとその対処方法」の各コマンド共通のエラーメッセージもあわせて参照して下さい。

エラー内容	終了値	対処方法
R/3 exception raised(*****)(func:cll_bapi_xbp_job_joblog_read,line:***), system exception raised(*****)(func:cll_bapi_xbp_job_joblog_read,line:***), rfc failure(func:cll_bapi_xbp_job_joblog_read,line:***), other rfc failure(***)(func:cll_bapi_xbp_job_joblog_read,line:***)	33	R/3ジョブのジョブログの取得に失敗しました。以下のよ 引数のアルファベットの大文字と小文字は正しくあってい saprfc.iniファイルの内容は正しく、抜けがありませんか SAP R/3のサーバーは稼働していますか？ネットワーク
R/3 joblog read failed	33	R/3ジョブのジョブログの取得に失敗しました。以下のよ R/3ジョブ名及びジョブカウントは正しいですか？

7.3.5.2.5. R/3ジョブ状態確認コマンド(sjPEX_r3job_check)

コマンドの実行中にエラーが起きると、エラーメッセージが出力されます。「エラーメッセージとその対処方法」の各コマンド共通のエラーメッセージもあわせて参照して下さい。

エラー内容	終了値	対処方法
R/3 exception raised(*****)(func:cll_bapi_xbp_job_status_check,line:***), system exception raised(*****)(func:cll_bapi_xbp_job_status_check,line:***), rfc failure(func:cll_bapi_xbp_job_status_check,line:***), other rfc failure(***)(func:cll_bapi_xbp_job_status_check,line:***)	34	R/3ジョブの状態の取得に失敗しました。以下のよう 引数のアルファベットの大文字と小文字は正しくあって saprfc.iniファイルの内容は正しく、抜けがありません SAP R/3のサーバーは稼働していますか？ネットワー
R/3 job status check failed	34	R/3ジョブの状態の取得に失敗しました。以下のよう R/3ジョブ名及びジョブカウントは正しいですか？

7.3.5.2.6. R/3ジョブバリアント取得コマンド(sjPEX_r3job_variant)

コマンドの実行中にエラーが起きると、エラーメッセージが出力されます。「エラーメッセージとその対処方法」の各コマンド共通のエラーメッセージもあわせて参照して下さい。

エラー内容	終了値	対処方法
R/3 exception raised(*****)(func:cll_bapi_xbp_variant_info_get,line:***), System exception raised(*****)(func:cll_bapi_xbp_variant_info_get,line:***), Rfc failure(func:cll_bapi_xbp_variant_info_get,line:***), Other rfc failure(***)(func:cll_bapi_xbp_variant_info_get,line:***)	35	ABAP/4プログラムのバリアントの取得に失敗しました。 引数のアルファベットの大文字と小文字は正しくあって saprfc.iniファイルの内容は正しく、抜けがありませんか SAP R/3のサーバーは稼働していますか？ネットワーク
R/3 variant info get failed	35	ABAP/4プログラムのバリアントの取得に失敗しました。 ABAP/4プログラム名は正しいですか？

7.3.5.2.7. R/3ジョブログレベル設定コマンド(sjPEX_r3job_logset)

コマンドの実行中にエラーが起きると、エラーメッセージが出力されます。「エラーメッセージとその対処方法」の各コマンド共通のエラーメッセージもあわせて参照して下さい。

エラー内容	終了値	対処方法
R/3 exception raised(*****)(func:cll_bapi_xmi_set_auditlevel,line:***), System exception raised(*****)(func:cll_bapi_xmi_set_auditlevel:***), Rfc failure(func:cll_bapi_xmi_set_auditlevel,line:***), Other rfc failure(***)(func:cll_bapi_xmi_set_auditlevel,line:***)	36	R/3ジョブログレベルの設定に失敗しました。以下のような原因 引数のアルファベットの大文字と小文字は正しくあっていますか Saprfc.iniファイルの内容は正しく、抜けがありませんか？ SAP R/3のサーバーは稼働していますか？ネットワークケーブ
R/3 set auditlevel failed	36	R/3ジョブログレベルの設定に失敗しました。

7.3.5.2.8. R/3ジョブ削除コマンド(sjPEX_r3job_delete)

コマンドの実行中にエラーが起きると、エラーメッセージが出力されます。「エラーメッセージとその対処方法」の各コマンド共通のエラーメッセージもあわせて参照して下さい。

エラー内容	終了値	対処方法
R/3 exception raised(*****)(func:cll_bapi_xbp_job_delete,line:***), system exception raised(*****)(func:cll_bapi_xbp_job_delete,line:***), rfc failure(func:cll_bapi_xbp_job_delete,line:***), other rfc failure(***)(func:cll_bapi_xbp_job_delete,line:***)	37	R/3ジョブの削除に失敗しました。以下のような原因が考えら 引数のアルファベットの大文字と小文字は正しくあっていますか saprfc.iniファイルの内容は正しく、抜けがありませんか？ SAP R/3のサーバーは稼働していますか？ネットワークケーブ R/3ジョブ名及びジョブカウントは正しいですか？ R/3ジョブは稼働中ではありませんか？
R/3 job delete failed	37	R/3ジョブの削除に失敗しました。以下のような原因が考えら R/3ジョブ名及びジョブカウントは正しいですか？

7.3.5.2.9. R/3ジョブ検索コマンド(sjPEX_r3job_select)

コマンドの実行中にエラーが起きると、エラーメッセージが出力されます。「エラーメッセージとその対処方法」の各コマンド共通のエラーメッセージもあわせて参照して下さい。

エラー内容	終了値	対処方法
R/3 exception raised(*****)(func:cll_bapi_xbp_job_select,line:***), system exception raised(*****)(func:cll_bapi_xbp_job_select,line:***), rfc failure(func:cll_bapi_xbp_job_select,line:***), other rfc failure(***)(func:cll_bapi_xbp_job_select,line:***)	39	R/3ジョブの検索に失敗しました。以下のような原因が考えら 引数のアルファベットの大文字と小文字は正しくあっていますか saprfc.iniファイルの内容は正しく、抜けがありませんか？ SAP R/3のサーバーは稼働していますか？ネットワークケーブ
R/3 job select failed	39	R/3ジョブの検索に失敗しました。

7.3.5.2.10. R/3ジョブ管理情報照会コマンド(sjPEX_r3job_confprint)

コマンドの実行中にエラーが起きると、エラーメッセージが出力されます。「エラーメッセージとその対処方法」の各コマンド共通のエラーメッセージを参照して下さい。

7.3.5.2.11. R/3ジョブコピーコマンド(sjPEX_r3job_copy)

コマンドの実行中にエラーが起きると、エラーメッセージが出力されます。「エラーメッセージとその対処方法」の各コマンド共通のエラーメッセージもあわせて参照して下さい。

エラー内容	終了値	対処方法
R/3 exception raised(*****)(func:cll_bapi_xbp_job_copy,line:***), system exception raised(*****)(func:cll_bapi_xbp_job_copy,line:***), rfc failure(func:cll_bapi_xbp_job_copy,line:***), other rfc failure(***)(func:cll_bapi_xbp_job_copy,line:***)	47	R/3ジョブのコピーに失敗しました。以下のような原因が考えら 引数のアルファベットの大文字と小文字は正しくあっていますか saprfc.iniファイルの内容は正しく、抜けがありませんか？ SAP R/3のサーバーは稼働していますか？ネットワークケーブル R/3ジョブ名及びジョブカウントは正しいですか？ R/3ジョブは稼働中ではありませんか？
R/3 job copy failed	47	R/3ジョブのコピーに失敗しました。以下のような原因が考えら R/3ジョブ名及びジョブカウントは正しいですか？

7.3.5.2.12. R/3ジョブ強制停止コマンド(sjPEX_r3job_stop)

コマンドの実行中にエラーが起きると、エラーメッセージが出力されます。「エラーメッセージとその対処方法」の各コマンド共通のエラーメッセージもあわせて参照して下さい。

エラー内容	終了値	対処方法
R/3 exception raised(*****)(func:cll_bapi_xbp_job_abort,line:***), system exception raised(*****)(func:cll_bapi_xbp_job_abort,line:***), rfc failure(func:cll_bapi_xbp_job_abort,line:***), other rfc failure(***)(func:cll_bapi_xbp_job_abort,line:***)	11	R/3ジョブの強制停止に失敗しました。以下のような原因が考 引数のアルファベットの大文字と小文字は正しくあっていますか saprfc.iniファイルの内容は正しく、抜けがありませんか？ SAP R/3のサーバーは稼働していますか？ネットワークケーブル R/3ジョブ名及びジョブカウントは正しいですか？ R/3ジョブは稼働中ではありませんか？
R/3 job abort failed	11	R/3ジョブの強制停止に失敗しました。以下のような原因が考 R/3ジョブ名及びジョブカウントは正しいですか？

7.3.5.2.13. R/3ジョブ子ジョブ取得コマンド(sjPEX_r3job_listChildJobs)

コマンドの実行中にエラーが起きると、エラーメッセージが出力されます。「エラーメッセージとその対処方法」の各コマンド共通のエラーメッセージもあわせて参照して下さい。

エラー内容	終了値	対処方法
R/3 exception raised(*****)(func:cll_bapi_xbp_job_children_get,line:***), system exception raised(*****)(func:cll_bapi_xbp_job_children_get,line:***), rfc failure(func:cll_bapi_xbp_job_children_get,line:***), other rfc failure(***)(func:cll_bapi_xbp_job_children_get,line:***)	51	R/3ジョブの子ジョブの取得に失敗しました。以下のよう 引数のアルファベットの大文字と小文字は正しくあって saprfc.iniファイルの内容は正しく、抜けがありませんか SAP R/3のサーバーは稼働していますか？ネットワーク R/3ジョブ名及びジョブカウントは正しいですか？ R/3ジョブは稼働中ではありませんか？
R/3 job children get failed	51	R/3ジョブの子ジョブの取得に失敗しました。以下のよう R/3ジョブ名及びジョブカウントは正しいですか？

7.3.5.2.14. R/3ジョブスプール取得コマンド(sjPEX_r3job_listSpool)

コマンドの実行中にエラーが起きると、エラーメッセージが出力されます。「エラーメッセージとその対処方法」の各コマンド共通のエラーメッセージもあわせて参照して下さい。

エラー内容	終了値	対処方法
R/3 exception raised(*****)(func:cll_bapi_xbp_job_spoollist_read_20,line:***), system exception raised(*****)(func:cll_bapi_xbp_job_spoollist_read_20,line:***), rfc failure(func:cll_bapi_xbp_job_spoollist_read_20,line:***), other rfc failure(***)(func:cll_bapi_xbp_job_spoollist_read_20,line:***)	55	R/3ジョブのスプールの取得に失敗しました。以下 引数のアルファベットの大文字と小文字は正しく saprfc.iniファイルの内容は正しく、抜けがあり SAP R/3のサーバーは稼働していますか？ネッ R/3ジョブ名及びジョブカウントは正しいですか？ R/3ジョブは稼働中ではありませんか？
R/3 job spool get failed	55	R/3ジョブのスプールの取得に失敗しました。以下 R/3ジョブ名及びジョブカウントは正しいですか？

7.3.5.2.15. R/3イベント送信コマンド(sjPEX_r3job_sendEvent)

コマンドの実行中にエラーが起きると、エラーメッセージが出力されます。「エラーメッセージとその対処方法」の各コマンド共通のエラーメッセージもあわせて参照して下さい。

エラー内容	終了値	対処方法
R/3 exception raised(*****)(func:cll_bapi_xbp_event_raise,line:***), system exception raised(*****)(func:cll_bapi_xbp_event_raise,line:***), rfc failure(func:cll_bapi_xbp_event_raise,line:***), other rfc failure(***)(func:cll_bapi_xbp_event_raise,line:***)	48	R/3イベントの送信に失敗しました。以下のような原因が考え 引数のアルファベットの大文字と小文字は正しくあっていますか saprfc.iniファイルの内容は正しく、抜けがありませんか？ SAP R/3のサーバーは稼働していますか？ネットワークケーブ R/3イベントID及びイベントパラメータは正しいですか？
R/3 event raise failed	48	R/3イベントの送信に失敗しました。以下のような原因が考え R/3イベントID及びイベントパラメータは正しいですか？

7.3.5.2.16. R/3プリンター覧コマンド(sjPEX_r3job_listOutputDevice)

コマンドの実行中にエラーが起きると、エラーメッセージが出力されます。「エラーメッセージとその対処方法」の各コマンド共通のエラーメッセージもあわせて参照して下さい。

エラー内容	終了値	対処方法
R/3 exception raised(*****)(func:cll_bapi_xbp_output_device_search,line:***), system exception raised(*****)(func:cll_bapi_xbp_output_device_search,line:***), rfc failure(func:cll_bapi_xbp_output_device_search,line:***), other rfc failure(***)(func:cll_bapi_xbp_output_device_search,line:***)	52	R/3プリンタの取得に失敗しました。以下のような 引数のアルファベットの大文字と小文字は正しく saprfc.iniファイルの内容は正しく、抜けがありま SAP R/3のサーバーは稼働していますか？ネッ
R/3 output device get failed	52	R/3プリンタの取得に失敗しました。

7.3.5.2.17. R/3ABAPレポート一覧コマンド(sjPEX_r3job_listABAPReport)

コマンドの実行中にエラーが起きると、エラーメッセージが出力されます。「エラーメッセージとその対処方法」の各コマンド共通のエラーメッセージもあわせて参照して下さい。

エラー内容	終了値	対処方法
R/3 exception raised(*****)(func:cll_bapi_xbp_report_search,line:***), system exception raised(*****)(func:cll_bapi_xbp_report_search,line:***), rfc failure(func:cll_bapi_xbp_report_search,line:***), other rfc failure(***)(func:cll_bapi_xbp_report_search,line:***)	53	ABAPレポートの取得に失敗しました。以下のような原因 引数のアルファベットの大文字と小文字は正しくあってい saprfc.iniファイルの内容は正しく、抜けがありませんか？ SAP R/3のサーバーは稼働していますか？ネットワークケ ABAPレポート名は正しいですか？
R/3 ABAP report get failed	53	ABAPレポートの取得に失敗しました。以下のような原因 ABAPレポート名及びは正しいですか？

7.3.5.2.18. R/3ジョブバリアント変更コマンド(sjPEX_r3job_variantChange)

コマンドの実行中にエラーが起きると、エラーメッセージが出力されます。「エラーメッセージとその対処方法」の各コマンド共通のエラーメッセージもあわせて参照して下さい。

エラー内容	終了値	対処方法
R/3 exception raised(*****)(func:cll_rs_change_created_variant_rfc,line:***), System exception raised(*****)(func:cll_rs_change_created_variant_rfc,line:***), Rfc failure(func:cll_rs_change_created_variant_rfc,line:***), Other rfc failure(***)(func:cll_rs_change_created_variant_rfc,line:***)	66	ABAP/4プログラムのバリアントの変更に失敗しま 引数のアルファベットの大文字と小文字は正しくあ saprfc.iniファイルの内容は正しく、抜けがありませ SAP R/3のサーバーは稼働していますか？ネット
R/3 variant change fail	66	ABAP/4プログラムのバリアントの変更に失敗しま ABAP/4プログラム名及びABAP/4バリアント名は

7.3.5.2.19. BWプロセスチェーン検索コマンド(sjPEX_bwChain_select)

コマンドの実行中にエラーが起きると、エラーメッセージが出力されます。「エラーメッセージとその対処方法」の各コマンド共通のエラーメッセージもあわせて参照して下さい。

エラー内容	終了値	対処方法
BWexception raised(*****)(func:cll_rspc_api_get_chains,line:***), system exception raised(*****)(func:cll_rspc_api_get_chains,line:***), rfc failure(func:cll_rspc_api_get_chains,line:***), other rfc failure(***)(func:cll_rspc_api_get_chains,line:***)	56	プロセスチェーンの検索に失敗しました。以下のような原因が 引数のアルファベットの大文字と小文字は正しくあっていますか saprfc.iniファイルの内容は正しく、抜けがありませんか？ AP BWのサーバーは稼働していますか？ネットワークケーブル プロセスチェーン名は正しいですか？

7.3.5.2.20. BWプロセスチェーン起動コマンド(sjPEX_bwChain_start)

コマンドの実行中にエラーが起きると、エラーメッセージが出力されます。「エラーメッセージとその対処方法」の各コマンド共通のエラーメッセージもあわせて参照して下さい。

エラー内容	終了値	対処方法
BW exception raised(*****)(func:cll_rspc_api_chain_get_processes,line:***), system exception raised(*****)(func:cll_rspc_api_chain_get_processes,line:***), rfc failure(func:cll_rspc_api_chain_get_processes,line:***), other rfc failure(***)(func:cll_rspc_api_chain_get_processes,line:***)	57	プロセスチェーンのプロセスの取得に失敗しました。 引数のアルファベットの大文字と小文字は正しくあ saprfc.iniファイルの内容は正しく、抜けがありませ SAP BWのサーバーは稼働していますか？ネット プロセスチェーン名及びログIDは正しいですか？

7.3.5.2.21. BWプロセスチェーン状態確認コマンド(sjPEX_bwChain_check)

コマンドの実行中にエラーが起きると、エラーメッセージが出力されます。「エラーメッセージとその対処方法」の各コマンド共通のエラーメッセージもあわせて参照して下さい。

エラー内容	終了値	対処方法
BW exception raised(*****)(func:cll_rspc_api_chain_get_status,line:***), system exception raised(*****)(func:cll_rspc_api_chain_get_status,line:***), rfc failure(func:cll_rspc_api_chain_get_status,line:***), other rfc failure(***)(func:cll_rspc_api_chain_get_status,line:***)	58	プロセスチェーンの状態の取得に失敗しました。以下の 引数のアルファベットの大文字と小文字は正しくあって saprfc.iniファイルの内容は正しく、抜けがありませんか SAP BWのサーバーは稼働していますか？ネットワー プロセスチェーン名及びログIDは正しいですか？

警告

- このコマンドでは、引数に存在しないプロセスチェーン名やログIDを指定した場合、「status：」のように空で表示されます。

- 正しいプロセスチェーン名及びログIDを指定して下さい。

7.3.5.2.22. BWプロセスチェーンログ取得コマンド(sjPEX_bwChain_logget)

コマンドの実行中にエラーが起きると、エラーメッセージが出力されます。「エラーメッセージとその対処方法」の各コマンド共通のエラーメッセージもあわせて参照して下さい。

エラー内容	終了値	対処方法
BW exception raised(*****)(func:cll_rspc_api_process_get_log,line:***), system exception raised(*****)(func:cll_rspc_api_process_get_log,line:***), rfc failure(func:cll_rspc_api_process_get_log,line:***), other rfc failure(***)(func:cll_rspc_api_process_get_log,line:***)	59	プロセスチェーンのプロセスのログの取得に失敗しました。 引数のアルファベットの大文字と小文字は正しくあってい saprfc.iniファイルの内容は正しく、抜けがありませんか SAP BWのサーバーは稼働していますか？ネットワーク プロセスチェーン名及びログIDは正しいですか？

7.3.5.2.23. BWプロセスチェーンプロセス一覧コマンド(sjPEX_bwChain_processList)

コマンドの実行中にエラーが起きると、エラーメッセージが出力されます。「エラーメッセージとその対処方法」の各コマンド共通のエラーメッセージもあわせて参照して下さい。

エラー内容	終了値	対処方法
BW exception raised(*****)(func:cll_rspc_api_chain_get_processes,line:***), system exception raised(*****)(func:cll_rspc_api_chain_get_processes,line:***), rfc failure(func:cll_rspc_api_chain_get_processes,line:***), other rfc failure(***)(func:cll_rspc_api_chain_get_processes,line:***)	60	プロセスチェーンのプロセスの取得に失敗しました。 引数のアルファベットの大文字と小文字は正しくあ saprfc.iniファイルの内容は正しく、抜けがありませ SAP BWのサーバーは稼働していますか？ネット プロセスチェーン名及びログIDは正しいですか？

7.3.5.2.24. BWプロセスチェーンプロセスログ取得コマンド(sjPEX_bwChain_processLog)

コマンドの実行中にエラーが起きると、エラーメッセージが出力されます。「エラーメッセージとその対処方法」の各コマンド共通のエラーメッセージもあわせて参照して下さい。

エラー内容	終了値	対処方法
BW exception raised(*****)(func:cll_rspc_api_process_get_log,line:***), system exception raised(*****)(func:cll_rspc_api_process_get_log,line:***), rfc failure(func:cll_rspc_api_process_get_log,line:***), other rfc failure(***)(func:cll_rspc_api_process_get_log,line:***)	61	プロセスチェーンのプロセスのログの取得に失敗しました。 引数のアルファベットの大文字と小文字は正しくあってい saprfc.iniファイルの内容は正しく、抜けがありませんか SAP BWのサーバーは稼働していますか？ネットワーク プロセスチェーン名及びログIDは正しいですか？

7.3.5.3. パスワード指定の省略方法

SAP ERP(RFC SDK 7.20)用のR/3ジョブスケジュールコマンド(sjPEX_r3job)および一部のJob Scheduler for R/3コマンドは、設定を行うことによりパスワードの指定を省略することができます。

注釈

パスワードの指定の省略はwindowsのみ有効です。

7.3.5.3.1. 省略可能なコマンド

Job Scheduler for R/3コマンドの中で、パスワードの指定を省略することができるコマンドは以下です。

- sjPEX_r3job_logget
- sjPEX_bwChain_start
- sjPEX_bwChain_check

7.3.5.3.2. 設定手順

以下に設定手順を記述します。

ログイン：Windowsの千手エージェントに千手稼働アカウントでログイン後、コマンドプロンプトを起動して下さい。

パスワード指定を省略するSAPサーバーの情報設定

(追加)パスワード指定を省略するSAPサーバーを追加する場合は、mオプションにaddを指定します。

```
%sj_setup_r3job.exe -m add -c クライアント -u R/3ユーザー名 -d デスティネーション
Password:パスワード
success
```

(変更)指定したパスワードを変更する場合は、mオプションにchgを指定します。

```
%sj_setup_r3job.exe -m chg -c クライアント -u R/3ユーザー名 -d デスティネーション
Password:パスワード
success
```

(削除)パスワード指定を省略するSAPサーバーを削除する場合は、mオプションにdelを指定します。

```
%sj_setup_r3job.exe -m del -c クライアント -u R/3ユーザー名 -d デスティネーション
success
```

(一覧参照)設定されているSAPサーバーを確認する場合は、mオプションにlstを指定します。

```
%sj_setup_r3job.exe -m lst
クライアント  ユーザー     デスティネーション
```

警告

この設定コマンドは同時に実行しないようにして下さい。正しく設定できない可能性があります。

7.3.5.3.3. sj_setup_r3jobコマンド

R/3ジョブスケジュールコマンド(sjPEX_r3job)および一部のJob Scheduler for R/3コマンドのパスワード指定を省略可能にする設定を行います。

```
sj_setup_r3job
        -m {{add|chg|del} -c クライアント -u R/3ユーザー名 -d デスティネーション | lst}
```

オプション	省略	長さ	説明
-m	不可	3	モード add：省略可能とする環境のパスワードを追加する。 chg：設定されている環境のパスワードを変更する。 del：設定されている環境のパスワードを削除する。 lst：省略可能となっている環境の一覧を表示する。
-c	不可	3	クライアント
-u	不可	12	R/3ユーザー名
-d	不可	32	デスティネーション