監視の技 13　システム障害時の切り分けとして、構成情報の変更有無を迅速に調査できるようにしたい

現状の課題

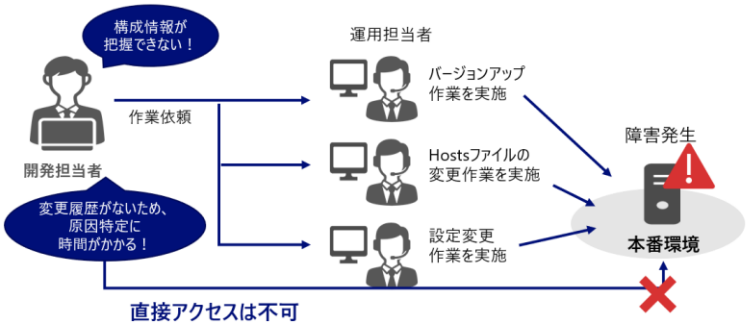
サーバーの構成変更は頻繁に実施されており、証明書更新等を手作業で実施した場合、正しく設定されずシステム稼働時に障害が発生して初めて気付くこともある。これは、いつどのような変更が実施されたのか把握できていないことが原因である。

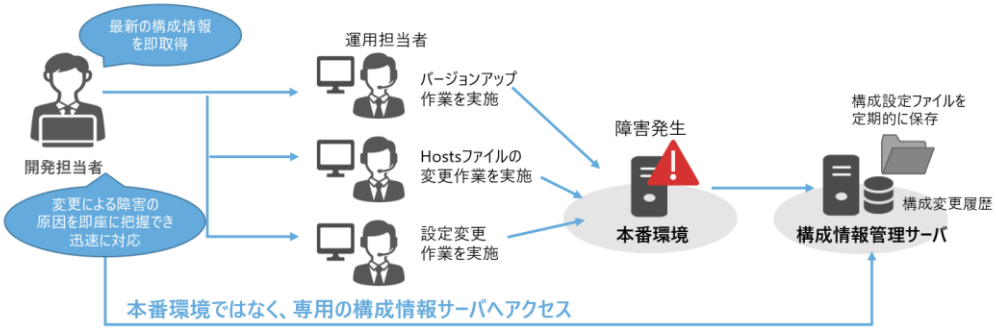
また、度重なるシステムのバージョンアップ、設定変更によって**現在のシステム構成情報を把握することは非常に困難**である。昨今開発と運用の職責分離が進められており、開発担当者は直接本番環境にアクセスできない。変更箇所の履歴がなければ、障害発生時にすぐに変更前に戻すという作業にも時間が掛かる。

解決策

構成変更の作業においては、実施前後で変更箇所の履歴を必ず取り、障害発生時には作業前後の設定情報を即座に確認できるようにしておくべきである。いつどのような変更が実施されたのかを把握できていれば、障害発生時の原因特定は迅速になる。

最新の構成情報は、本番環境にログインしなくても参照可能なサーバーを構築することが望ましい。アプリケーションやシステムが稼働するための設定ファイルを、1 日に 1 回など定期的に保存しておく。変更による障害が発生した際には、変更前後の設定情報を即座に把握でき、変更前の構成にすぐに戻せるようにしておくことが重要なポイントだ。





Senju Family での実践方法

Senju DevOperation Conductor(Senju/DC)では「コンフィグレーション」機能を提供している。構成情報をスケジュールに従って取得することで、システムが稼働するための設定ファイルを定期的に自動で保存する。監視とあわせて各管理対象の情報(システム、IT 情報)を取得し管理したい場合に有効である。もし連絡先情報やラック情報、外部の脆弱性情報などシステム的に収集できない情報もあわせて管理したい場合には、「Senju Configration Manager(Senju/CM)」の利用が有効である。

Senju/DC では構成情報は、今すぐ取得、前回保存分からの差分取得、変更履歴の表示、変更作業前後の構成情報をまとめて取得、といったさまざまな取得方法が可能だ。予定した変更が実施されたかどうか一覧で確認することもできる。これらの機能により、いつ、どのような変更が行われたのか視覚的に把握することが可能となる。

また集められた構成情報は、本番環境とは異なるファイルサーバーに蓄積される。開発担当者は本番業務サーバーへアクセスせず、必要な時に必要なファイルを参照することが可能になる。

また、**構成情報を自動収集し、サービス障害や脆弱性情報受信の際に自システム環境への影響を迅速に特定**するための構成管理ツールとして、Senju/CM が有効である。本製品では、IT 資産管理の要件をベースに「エージェントレスで情報収集」、「対象セグメント内のノード一覧自動取得」の機能を提供している。Senju DevOperation Conductor とは完全に分離した形で提供しているため、既存のジョブ運用や監視を止めることなく簡単に機能拡張も可能となる。