IceWall技術レポート:

HP SoftwareのIT運用管理製品とIceWall SSOとの連携効果および構成の注意点

1. はじめに

本技術レポートでは、IT運用管理のClosed Loop Incident Process（CLIP）で主に利用されるHP Software製品とIceWall SSOを連携させてシングルサインオンを行う場合の効果と構成例、技術的な注意点を記述します。

2. Closed Loop Incident Process（CLIP）とは

Closed Loop Incident Process（CLIP）とは、リアクティブな運用管理から予測型の運用管理への移行を促進し、サービスの計画外の中断を防ぎ、高いサービス品質を維持するためのプロセスで、複数のHP Software製品から構成されます。

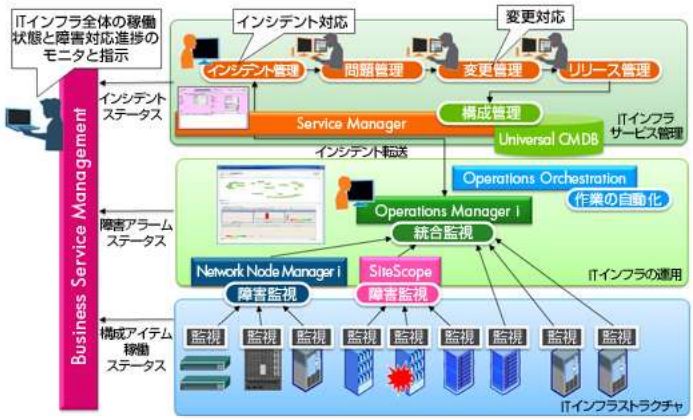

図1 CLIPを構成するHP Software製品とその役割

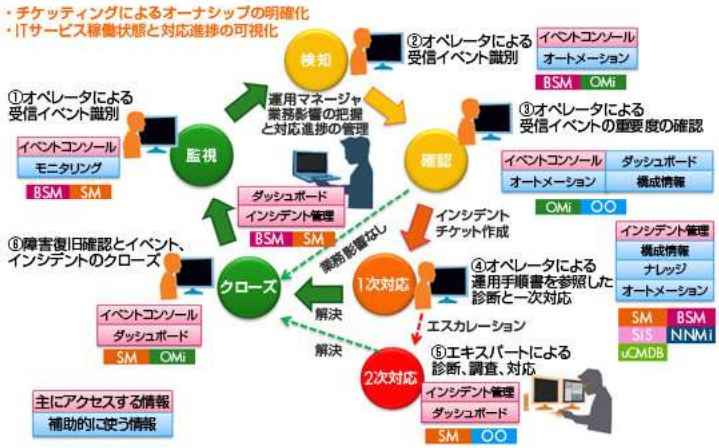

図2 インシデント対応プロセスと各製品の対応

3. 運用管理製品の導入における課題

CLIPを構成するHP Software製品やその他の運用管理製品の進化により高度な運用管理の実現が可能になりましたが、他の業務システム数の増加やクラウドサービス（プライベート、パブリック含む）の利用拡大により、ITリソースとアクセス方法が非常に多様化しています。
そのため、アクセスするアプリケーションごとにログインが必要になるアカウント情報（＝ID・パスワード）を使い分けなければならないといった利便性の低下が問題になるケースがあり、生産性の向上にあたっての課題となっています。また、各アプリケーションへのアクセス方法が別々に存在する状況では、利用ユーザーの管理は難しくなります。さらにインターネット等外部からアクセスを行う場合には、そのセキュリティをどう確保するかということも課題です。
これらの課題に対して、シングルサインオンソリューションであるIceWall SSOと各アプリケーションの連携はひとつの有効な回答となります。

4. 運用管理製品とIceWall SSOを連携させることによる効果

前記のような課題に対し、運用管理製品にIceWall SSOを連携させることによって、以下のような効果を得ることができます。

- シングルサインオンにより各製品にシームレスにアクセス可能になることによる利便性向上
- 利用者の役割（オペレータ、エキスパート、運用マネージャ等）に応じた各製品へのアクセス制御やアクセスログを一元化でき、シンプルかつセキュアな管理が可能
- 外部からの入口をIceWall SSOのリバースプロキシサーバーに統一することで、一ヶ所に重点的にセキュリティ対策（Webアプリケーション攻撃対策等）を行うことが可能
- 運用管理製品だけではなく、他のWebシステムとのシングルサインオンも可能となり、さらにクラウドサービス等との認証連携も可能となる。また、ユーザーの認証に統合Windows認証も利用できるようになる。

イントラネットシステムでの利用イメージを以下に示します。

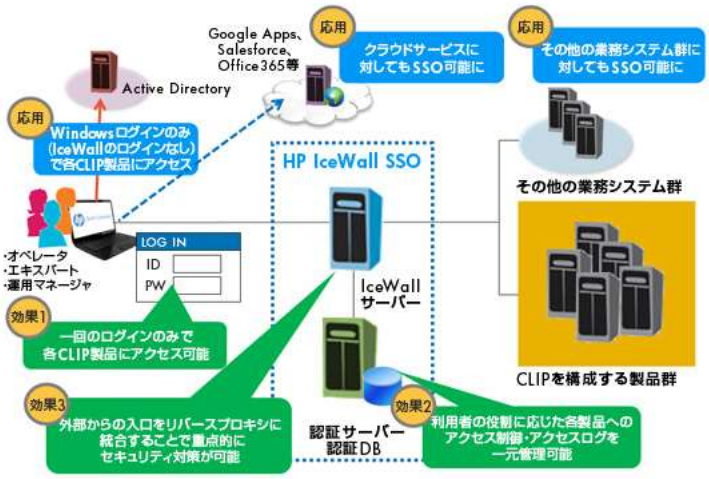

図3 利用イメージ1:イントラネットシステム構成

さらに、複数企業のシステムに対して運用管理を提供するクラウドサービスにおいて、各企業のシステム管理者にシングルサインオンでのアクセスを提供する利用イメージを以下に示します。

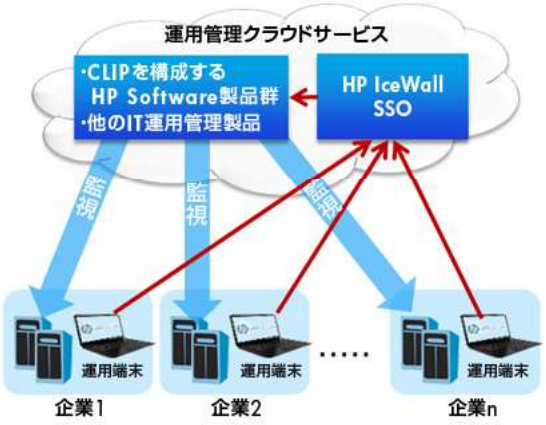

図4 利用イメージ2:クラウドサービス構成

5. 連携方法と注意点

- アクセスURL方式
  - HP Softwareの運用管理製品では、そのグラフィカルなGUI等によって各ページの内容が多岐に渡るため、IceWall SSOとの連携にはページに含まれるリンク先URLの変換を必要としない「オリジナルURL方式」を用いるのがスムーズです。
    「オリジナルURL方式」についての詳細は以下の技術レポートをご参照ください。
    ≫ オリジナルURL対応機能特集1: 基本編
- 認証機能を持つアプリケーションとの連携方式
  - IceWall SSOは、認証機能を持つアプリケーション(自身でログイン機能を持つアプリケーション)に対してもシングルサインオンを実現するための「自動フォーム認証」という機能を持っています。HP Softwareの運用管理製品との連携においても「自動フォーム認証機能」を利用します。
    「自動フォーム認証機能」についての詳細は以下の技術レポートをご参照ください。
    ≫ フォーム認証特集 – どうする既存の認証?
  - Universal CMDBとの連携には、自動フォーム認証の間接送信方式をご利用ください。
- その他注意点
  - ブラウザから “Accept-Encoding: gzip, deflate” ヘッダを含んだリクエストが送信されることで、バックエンドサーバーから圧縮したコンテンツが返却される場合があります。
    その場合、IceWall SSOの「自動フォーム認証」やコンテンツ内の指定されたURLやキーワードを置き換える機能(「URL変換機能」や「コンテンツ変換機能」)が動作しませんので、ブラウザから受信した“Accept-Encoding”ヘッダをシングルサインオン対象のアプリケーションに送信しないようにする追加設定(「ホスト設定ファイル」の「HEADER」項目設定)を行うようにしてください。
    本追加設定についての詳細は以下の技術レポートをご参照ください。
    ≫ オリジナルURL対応機能特集3:SAP EPとの連携

6. 連携確認済み製品

以下のHP Softwareの運用管理製品とIceWall SSOについて、実際の試験環境で連携の動作確認が済んでいます。
また、動作確認の際に実際に行った設定内容をサンプルとしてご用意しておりますので、お客様のシステムでも容易に実装していただけます。

- Business Service Management 9.22.111
- Service Manager 9.30.021
- Operations Manager i 9.22 (※Business Service Managementより起動)
- Operations Orchestration 10.10
- SiteScope 11.23
- Universal CMDB 10.10
- Network Node Manager i 9.22

(2014年7月現在)

7. まとめ

本技術レポートでは、IT運用管理のClosed Loop Incident Process（CLIP）で主に利用されるHP Software製品とIceWall SSOを連携させてシングルサインオンを行う場合の効果と構成例、技術的な注意点を説明しました。
本連携ソリューションにより、CLIPを構成する製品群に対するアクセス性が大幅に高まり、かつその他のシステムやクラウドサービス等とも認証の連携が可能となるため、運用効率の改善が期待できます。

8. アップデート情報

HPの提供するビッグデータ解析プラットフォームを採用したSaaS型ITサービス管理ソリューションであるService Anywhereへの認証連携を確認しました。
これにより、オンプレミスのシステムとクラウドベースのサービスを組み合わせながら、シームレスに利用可能なIT運用管理基盤の実現が可能となります。こちらも是非ご検討ください。

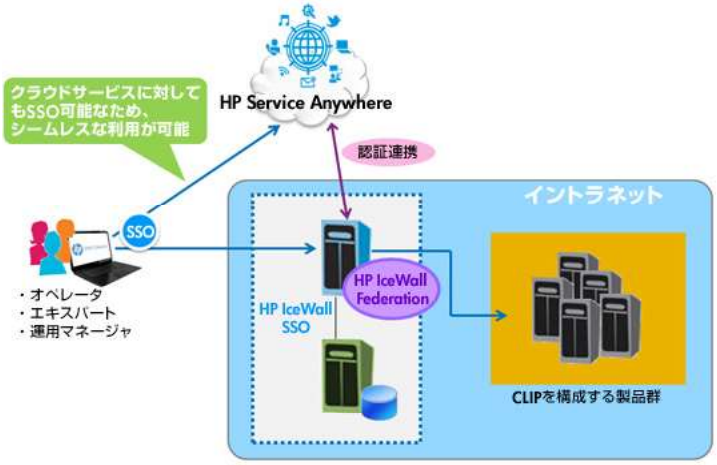

図5 Service Anywhereとの接続イメージ

≫ Service Anywhereの詳細はこちら
≫ IceWall Federationの詳細はこちら

2014.6.30	新規掲載
2014.7.31	見出し5、6を更新
2014.10.10	見出し8を追加掲載

執筆者　日本ヒューレット・パッカード テクノロジーコンサルティング事業統括
テクニカルコンサルタント
谷垣　敦