# HP ArcSightとHP IceWall SSOの連携

## はじめに

HP ArcSightはネットワーク上に存在するネットワーク機器、サーバー、アプリケーション等からリアルタイムでログを収集、分析し、保管・レポート機能を提供するログ管理・監視ソリューションです。

HP ArcSightでHP IceWall SSOのアクセスログや他システムの様々なログを相関づけて分析することにより、

- 経営層のみが閲覧可能な（機密性の高い）情報に対象者ではないユーザーがアクセスしている…
- 既に退職した従業員のユーザーIDでログインしている…
- ソースIPが異なる場所（数箇所）から同時に同じユーザーIDでアクセスしている…

など、挙動の疑わしいユーザーやアクセスを自動的にリアルタイムで検出することが可能になります。

本稿では、その連携に必要なHP IceWall SSO用 HP ArcSight FlexConnectorとそのインストール方法についてご紹介します。

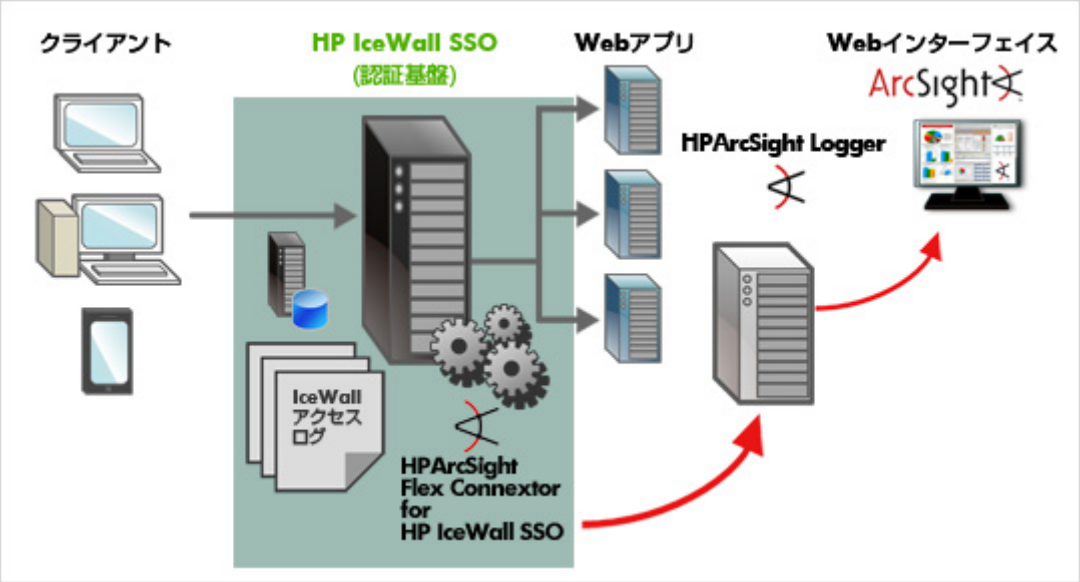
※HP ArcSightについての詳細はこちら をご参照ください。

## ArcSight FlexConnector for IceWall

HP ArcSight FlexConnectorとは、簡単な設定ファイルを記述することにより、様々な製品のログをHP ArcSightのログ形式（CEF形式）に変換し、HP ArcSightのコアエンジンサーバーへ送る役割を担うコンポーネントです。

CEFとはCommon Event Format の略称で、HP ArcSightが提唱している標準ログフォーマット形式です。この形式に従うことで、HP ArcSight上でより緻密なログ解析が可能になります。

HP IceWall SSO用のFlexConnectorは、下図のように、HP IceWall SSOのアクセスログ（dfw.log,cert.logなど）をリアルタイムにCEF形式に変換し、HP ArcSight LoggerなどのHP ArcSightサーバーへ送ります。




今回、HP IceWall SSOのログファイルから得られる最も基本的な情報をHP ArcSigntに取り込む事ができるFlexConnectorをサンプルとして作成しました。 ≫サンプルのダウンロードはこちら

- リバースプロキシ アクセスログ
  dfw.log用設定ファイル：dfw.log.sdkrfilereader.properties
- 認証モジュール アクセスログ
  cert.log用設定ファイル：cert.log.sdkrfilereader.properties
- MCRPモジュール アクセスログ
  iwp.log用設定ファイル：iwp.log.sdkrfilereader.properties

- フェデレーションモジュール アクセスログ
  iwgapps.log用設定ファイル：iwgapps.log.sdkrfilereader.properties
  iwsalesf.log用設定ファイル：iwsalesf.log.sdkrfilereader.properties
  iwsts.log用設定ファイル：iwsts.log.sdkrfilereader.properties

実際のシステム上では個別の要件に合わせてよりカスタマイズが必要ですが、基本的な動作はこのサンプルで実現可能です。

dfw.log

| HP IceWall SSOのログ要素 | CEF形式のログ要素 |
|---|---|
| 日時 | deviceReceiptTime |
| 時間1 | deviceCustomFloatingPoint1 |
| 時間2 | deviceCustomFloatingPoint2 |
| 時間3 | deviceCustomFloatingPoint3 |
| ユーザーID | destinationUserName |
| リクエストメソッド | requestMethod |
| リクエストURL | requestUrl |
| コンテンツサイズ | bytesOut |
| IPアドレス | sourceAddress |
| バックエンドWebサーバーステータス | deviceEventClassId |
| トランザクションID | externalId |

cert.log

| HP IceWall SSOのログ要素 | CEF形式のログ要素 |
|---|---|
| 日時 | deviceReceiptTime |
| ログメッセージ ※ | name |
| ユーザーID | destinationUserName |
| リクエストURL | requestUrl |
| IPアドレス | sourceAddress |
| ログイン時間 | deviceCustomString1 |
| トランザクションID | externalId |

※以下のいずれか。
Request URL Denied.
Request Group Denied.
Unknown UserID.
Password Error.
Access Control Request. (Client Certificate)
Access Control Request. (Uid/Password)
Access.
User Login Request.
User Login.
User Logout.
Login Timeout.

iwp.log

| HP IceWall SSOのログ要素 | CEF形式のログ要素 |
|---|---|
| 日時 | deviceReceiptTime |
| 時間1 | deviceCustomFloatingPoint1 |
| 時間2 | deviceCustomFloatingPoint2 |
| 時間3 | deviceCustomFloatingPoint3 |
| ユーザーID | destinationUserName |
| リクエストメソッド | requestMethod |
| リクエストURL | requestUrl |

| | |
|---|---|
| コンテンツサイズ | bytesOut |
| IPアドレス | sourceAddress |
| バックエンドWebサーバーステータス | deviceEventClassId |
| トランザクションID | externalId |

iwgapps.log

| HP IceWall SSOのログ要素 | CEF形式のログ要素 |
|---|---|
| 日時 | deviceReceiptTime |
| リクエスト受信からレスポンス返信までの時間 | deviceCustomNumber1 |
| IceWallで認証したユーザーID | destinationUserName |
| Google AppsのID | sourceUserName |
| トランザクションID | externalId |

iwsalesf.log

| HP IceWall SSOのログ要素 | CEF形式のログ要素 |
|---|---|
| 日時 | deviceReceiptTime |
| リクエスト受信からレスポンス返信までの時間 | deviceCustomNumber1 |
| IceWallで認証したユーザーID | destinationUserName |
| SalesforceのID | sourceUserName |
| トランザクションID | externalId |

iwsts.log

| HP IceWall SSOのログ要素 | CEF形式のログ要素 |
|---|---|
| 日時 | deviceReceiptTime |
| リクエスト受信からレスポンス返信までの時間 | deviceCustomNumber1 |
| IceWallで認証したユーザーID | destinationUserName |
| トランザクションID | externalId |

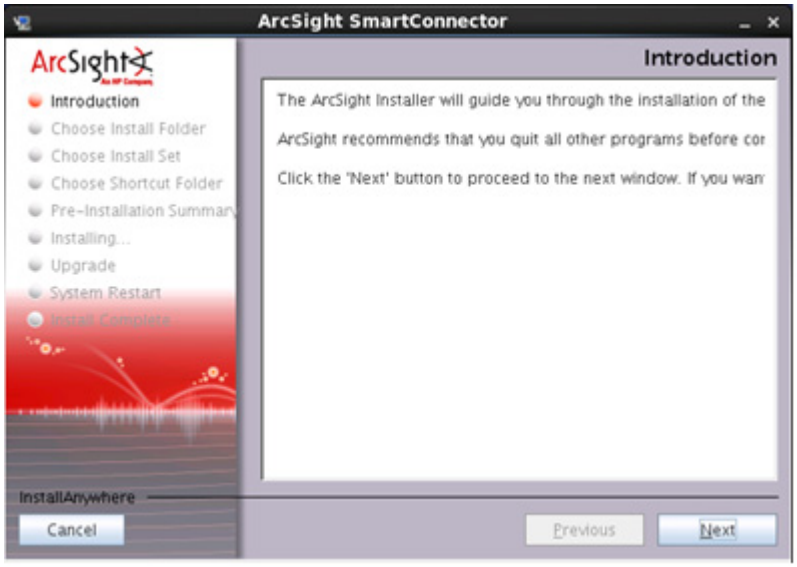
## FlexConnectorのインストールと設定手順

ここでは、HP IceWall SSOの認証サーバーを例に、FlexConnectorのインストール手順を記します。

1. FlexConnectorのインストールキットを入手し、認証サーバーで実行します。

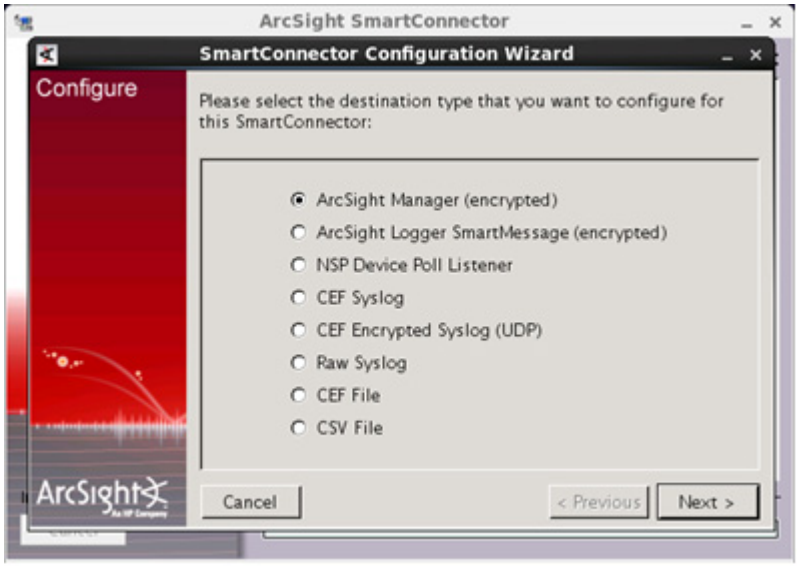
```
# ./ArcSight-x.x.x.xxxx.x-Connector-Linux.bin
```

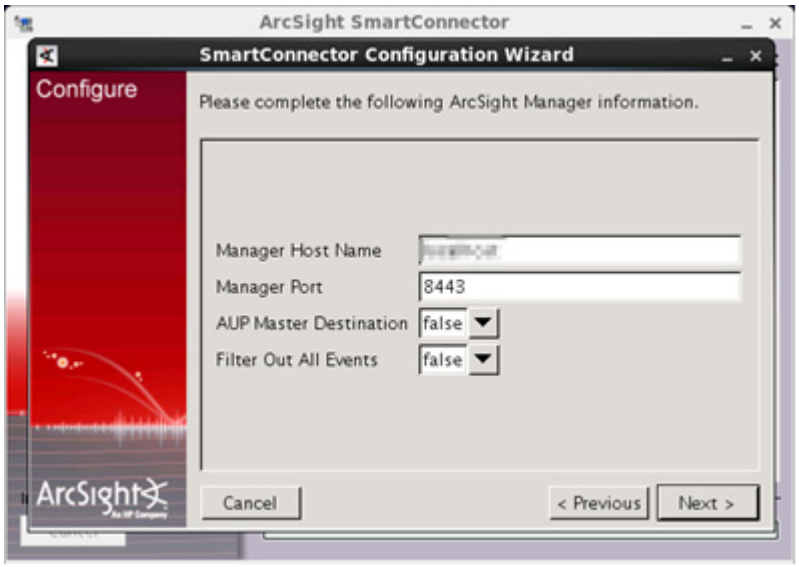
インストール用のGUIが起動します。



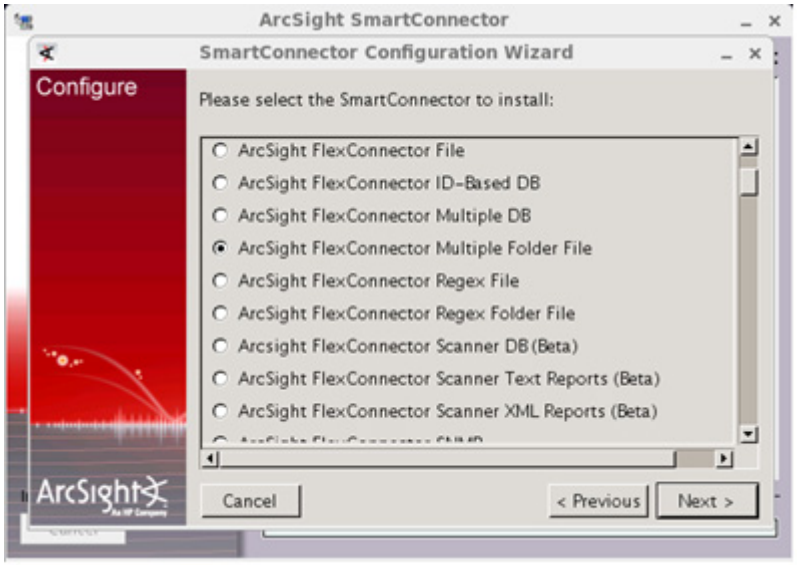
2. 以降、以下の「Pre-Instration Summary」が表示されるまでは、デフォルトの設定でインストールを進めます。


3. ログの送信先を指定します。（ここではデモ用に用意されたHP ArcSight Managerを指定しています）

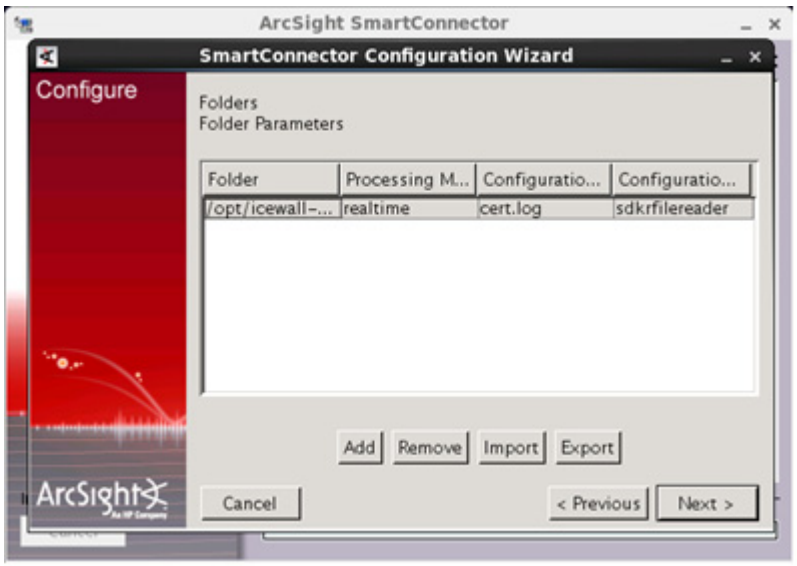



4. FlexConnectorのタイプとして「Multiple Folder File」を指定します。

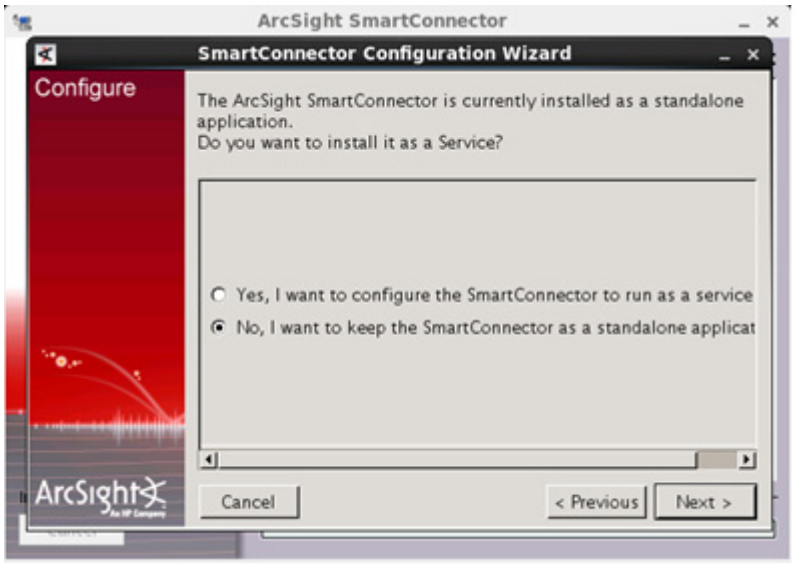



5. パラメータとして、以下の値を入力します。
Folder: /opt/icewall-sso/logs/（certdのログの出力先）
Procesing Message: realtime
Configuration File: cert.log（ログファイル名）
Configuration Type: sdkrfilereader




6. Connector名などを指定します。


7. FlexConnectorをサービスとして動かすか、スタンドアロンアプリケーションとして動かすかを指定します。
（ここではスタンドアロンアプリケーションとして動かすよう指定）




以上でインストールは完了です。

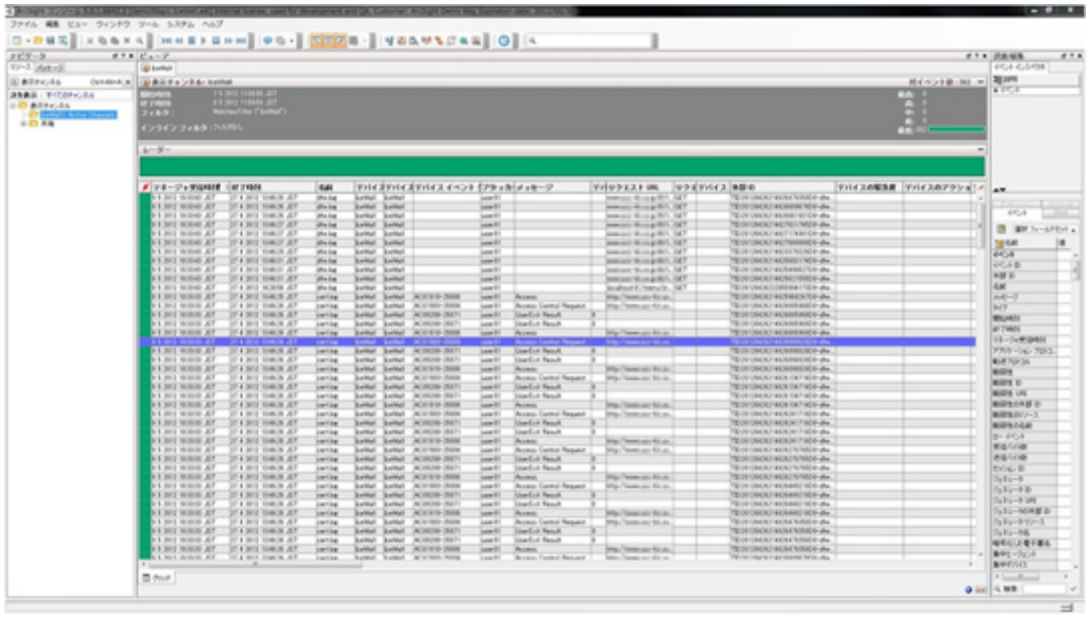

8. 設定ファイル（cert.log.sdkrfilereader.properties）を以下のフォルダに配置します。

```
/root/ArcSightSmartConnectors/current/user/agent/flexagent
```

9. 以下のコマンドでFlexConnectorを起動します。

```
# /root/ArcSightSmartConnectors/current/bin/arcsight
```

10. HP ArcSight ESM Managerの管理画面等でログが転送されていることを確認します。

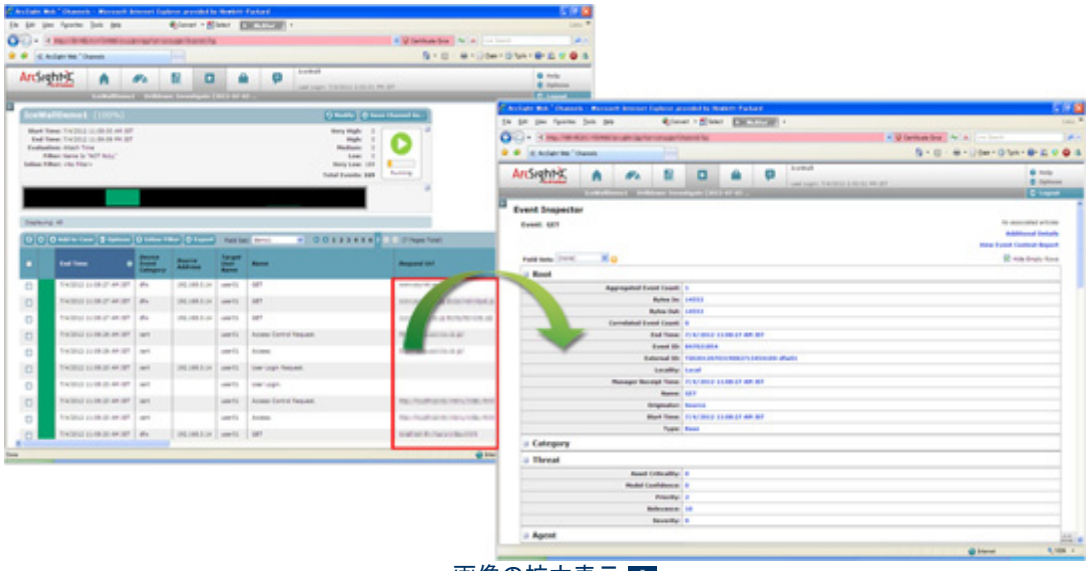


画像の拡大表示

## HP ArcSight ESM Manager上での表示例

HP ArcSight ESM Managerへ送信したHP IceWall SSOのログを用いた簡単な分析の画面例をご紹介します。

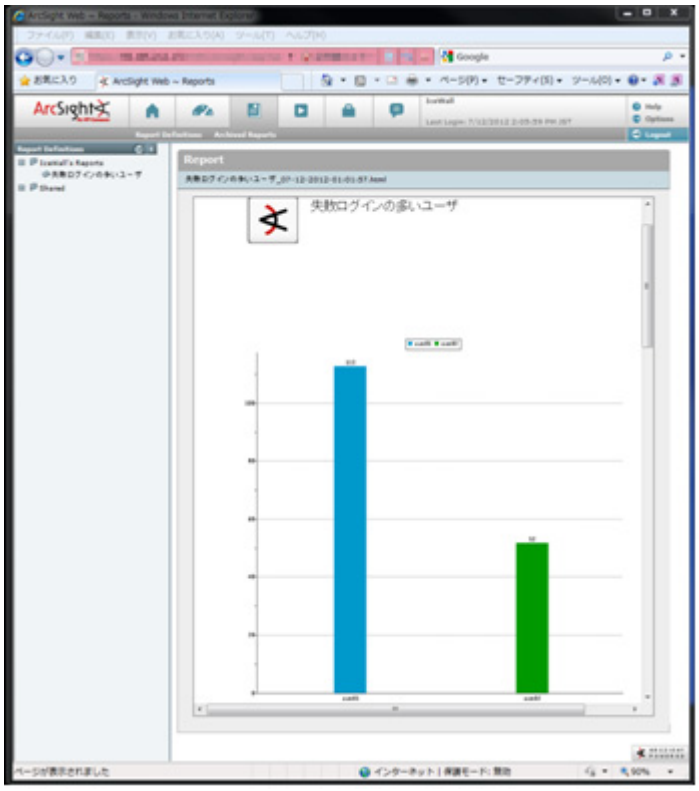
画面例1
左側の画面では、リバースプロキシ（dfw）および認証モジュール（certd）のログをトランザクションIDでソートして表示しています。
この中の特定の行を選択すると、右側の画面のようにより詳細な内容が確認可能です。



画像の拡大表示

画面例2
任意のログをベースにわかりやすくビジュアル表示が可能です。
下の画面では、ある一定期間のUserのログイン状況のログを収集・分析し、User01とUser02のみ1時間に1回

以上の頻度でログインに失敗していることが判明した例です。

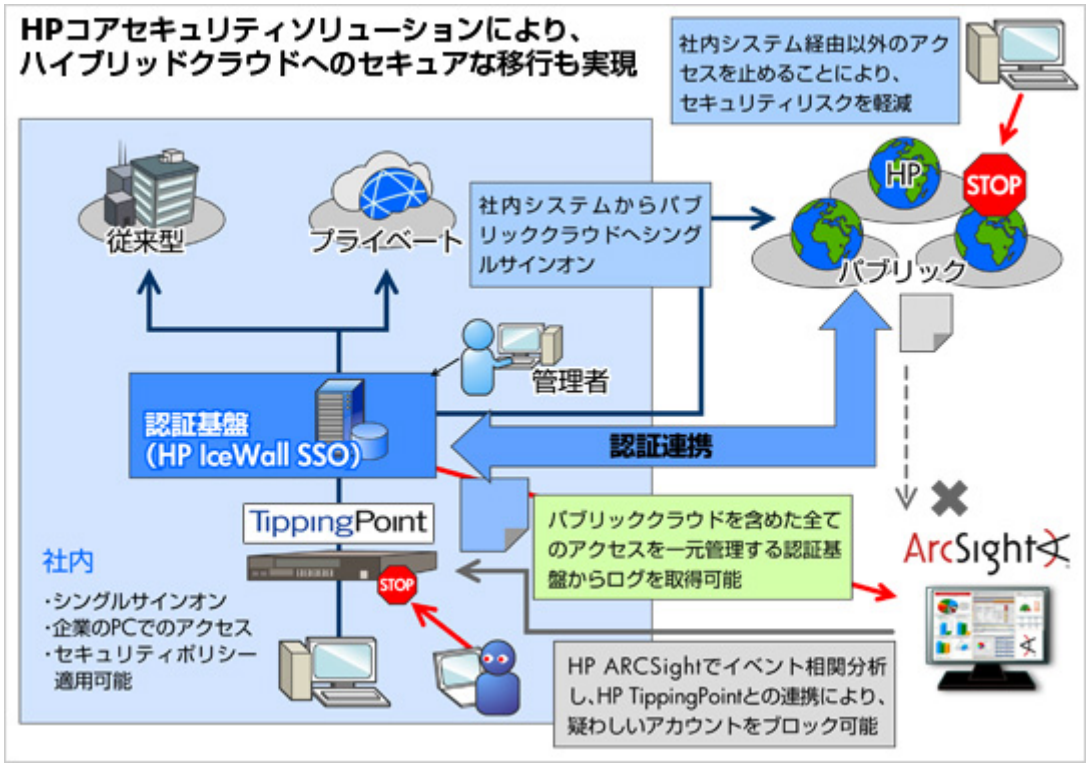



画像の拡大表示

## おわりに

以上、HP IceWall SSO と HP ArcSightの連携に必要なFlexConnectorについて、サンプルConnectorを例として基本的な内容と動作をご紹介しました。

さらに、HP TippingPoint と連携させれば、挙動の疑わしいユーザーのアクセスを即座に遮断するといった事も可能になります。HP IceWall SSO と HP ArcSightとHP TippingPoint を連携させ、ハイブリッドクラウド環境へセキュアに移行するためのソリューション例のイメージを以下に示します。




ここで述べた内容な技術的観点に基づいて検証した結果を示したもので特定の環境での動作や性能を保証するものではありません。実際の構築に関しては、HPまたはIceWall販売パートナーへご相談ください。

2012.11.15 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統括本部　テクニカルコンサルタント　小山重宣