SRGateクライアントエージェントとHP IceWall SSOを利用したクライアントサーバーアプリケーションへのシングルサインオンの実現

1.はじめに

ここ数年来、急速にアプリケーションのWeb化が進んでいる一方で、従来からのクライアントサーバーアプリケーションも、依然、相当数が使用され続けています。
HP IceWall SSOをはじめ、多くのシングルサインオン製品はWebアプリケーションを対象としているため、クライアントサーバーアプリケーションも稼働している混在環境においては、包括的なシングルサインオンソリューションの導入が困難な場合もあり、認証の一本化が進まず、結果的にユーザー自身が複数のID/パスワードを管理し、セキュリティリスクを解消できないという問題は少なくありません。

本ページでは、クライアントサーバー型（以下、C/S型）業務システムとのシングルサインオンを可能にする株式会社日立ソリューションズ製品「SRGateクライアントエージェント」とHP IceWall SSOの組み合わせにより、ユーザーは1つのIDとパスワードを管理するだけで、C/S型業務システムとWeb型業務システムの両者に対応可能なシングルサインオン環境の構築を実現するソリューションをご紹介します。

尚、2つのシングルサインオン製品を導入するにあたり、両製品が利用するユーザー情報を格納する認証DBを供用する構成とすることで、管理者の負担減を実現します。また、本ソリューション導入後にC/S型業務システムをWeb型業務システムへ移行した場合も、ユーザーから見たシングルサインオン環境が変化することはありません。

2.SRGateクライアントエージェントとは

SRGateクライアントエージェント（以下、SRGateCA）は、株式会社日立ソリューションズのエンタープライズシングルサインオンソフトウェアです。お客様は、SRGateCAを導入することで、Webアプリケーションからクライアントサーバーアプリケーションまでの幅広い範囲でシングルサインオンを実現します。

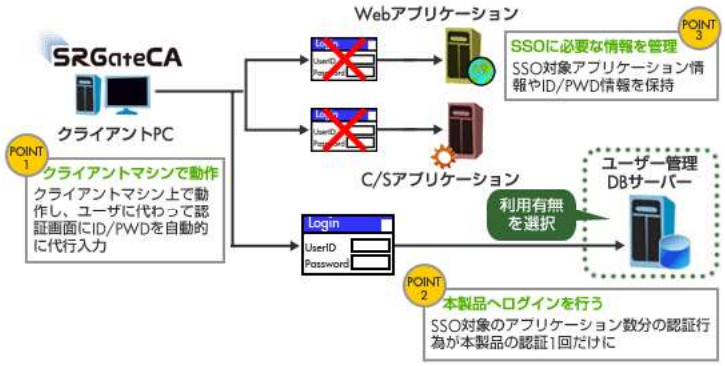

図2-1 SRGateCA機能概要図

SRGateCAの詳細は、以下URLからご確認ください。
≫ 株式会社日立ソリューションズ SRGate紹介サイト

3.ソリューション構成

3.1 システム構成

以下に本ソリューションを実現するシステム構成図と各構成要素についての役割を記述します。

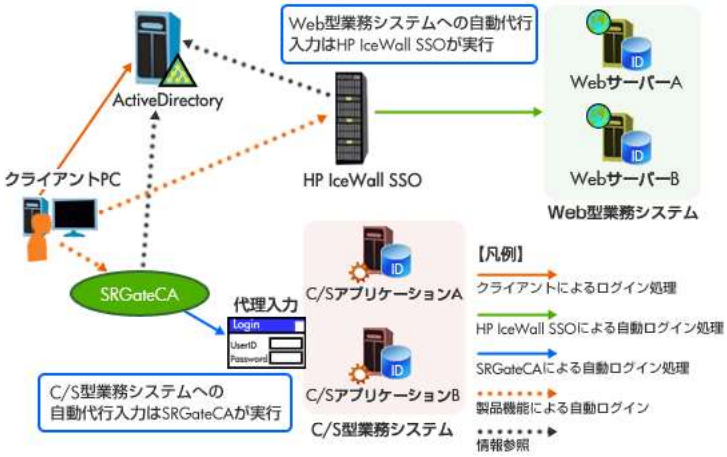

図3-1 基本システム構成図

項番	要素名	役割
1	クライアントPC	C/S型業務システム、Web型システム両方へアクセスする端末。
2	SRGateCA	C/S型業務システムとWeb型業務システムへのシングルサインオンを実現する製品。クライアントPCにインストールして利用する。
3	HP IceWall SSO（IceWallサーバーおよび認証サーバー）	Web型業務システムへのシングルサインオンを実現するHP IceWall SSOが導入されたシステム。HP IceWall SSOへの自動ログインを実現するためHP IceWall SSOのオプション製品であるDomain Gateway Optionを利用する。
4	認証DBサーバー	シングルサインオンを行うユーザー情報が格納されたDB。今回の検証ではSRGateCAとHP IceWall SSO両方の製品が対応しているActive Directoryを利用する。
5	C/S型業務システム	-
6	Web型業務システム	-

表3-1 システム構成要素

システム構成において、クライアントは通常以下3つの要素に対して認証行為が必要となります。

- クライアントPC
- SRGateCA
- HP IceWall SSO(IceWallサーバーおよび認証サーバー)

ただし、HP IceWall SSO、SRGateCAの各製品のオプション機能を利用することで、認証行為を不要とすることもできます。以下に認証行為を不要とする実現方法を記載します。

(a) SRGateCA
SRGateCAは製品標準機能でActive Direcoty連携(統合Windows認証)が可能です。
(b) HP IceWall SSO
HP IceWall SSOへアクセスすると、自動的にログインするDomain Gateway Option製品を利用します。

本ソリューションにおいては、クライアントの利便性を向上させることを目的として、クライアントが認証行為を不要とする構成としています。

3.2 本ソリューションの提供機能一覧

本ソリューションにより提供可能な機能一覧を記載します。

項番	機能名
1	業務システムへのログイン時にログインユーザーを選択してログインする機能。
2	ユーザーの属性情報を利用したWeb型業務システムへのアクセス制御機能。
3	Web型業務システムへのHTTPヘッダによる情報継承機能。
4	Web型業務システムへの認証・認可ログの一元化機能。

表3-2 提供機能一覧

3.3 ログインフロー

番号	内容
1	ユーザーは、クライアントPCへログインする。
2	統合Windows認証機能によりSRGateCAへ自動的にログインする。
3	C/S型業務システムへのアクセス。
3-1	ユーザーは、C/S型業務システムのログイン画面へアクセスする。
3-2	SRGateCAの代行入力により、C/S型業務システムへ自動ログインし、ユーザーはC/S型業務システムへアクセスできる。
4	Web型業務システムへのアクセス。
4-1	ユーザーは、Web型業務システムのログイン画面へアクセスする。
4-2	HP IceWall SSOの認証が必要であるが、Domain Gateway Option機能によりHP IceWall SSOへ自動ログインする。
4-3	HP IceWall SSOの代行入力により、Web型業務システムへ自動ログインし、ユーザーはWeb型業務システムへアクセスできる。

表3-3 ログインフロー

※認証DBがOpenLDAPの場合、以下の点が異なります。

- 番号2:ユーザーは手動でSRGateCAへログインする。
- 番号4-2:SRGateCAの代行入力により、HP IceWall SSOへ自動ログインする。

4.検証

4.1 検証環境の構成

検証環境で利用した製品のバージョンを記載します。

項番	要素名	導入製品とバージョン
1	クライアントPC	Windows7 64bit(日本語版)
2	SRGateCA	SRGateクライアントエージェント 02-00
3	HP IceWall SSO (IceWallサーバーおよび 認証サーバー)	HP IceWall SSO 10.0(Standard Edition) HP IceWall SSO 10.0 Domain Gateway Option
4	認証DBサーバー	Microsoft Active Directory(Microsoft Windows Server 2008 R2)

表4-1 検証環境製品バージョン

4.2 検証結果

以下の項目について動作することを確認しました。

- クライアントPCへログインすると、SRGateCAへ自動的にログインすること
- C/S型業務システムのログイン画面へアクセスすると、SRGateCAが自動的に代行入力を実行し、クライアントの認証行為は不要でC/S型業務システムへログインできること
- Web型業務システムのログイン画面へアクセスすると、Domain Gateway Option機能によりHP IceWall SSOへ自動ログインし、さらにWeb型業務システムへのログインはHP IceWall SSOが実行し、クライアントの認証行為は不要でWeb型業務システムへログインできること

※認証DBがOpenLDAPの場合も問題なく動作することを確認しました。

5.本ソリューションの前提条件

5.1 SRGateCAのクライアント展開について

5.1.1 システム構築の初回展開時

- 利用するすべてのクライアント端末にSRGateCAをインストールする必要があります。
- SRGateCAはサイレントインストール機能を有しており、例えば、お客様が既に構築済みの配布ツールと連携した自動配布等も検討が可能です。

5.1.2 SSO対象アプリケーションの更新時

- SSO対象アプリケーションの変更(新規追加、既存削除等)が発生した場合、利用するすべてのクライアント端末に更新データを再展開する必要があります。(C/S業務システム側の更新時のみ)

- 更新データは、SRGateCAが参照するLDAPから自動配布することも検討が可能です。

5.2 システム構築・運用時

- SRGateCAとHP IceWall SSO用にActive Directoryのスキーマ拡張の必要があります。
- パスワードは、Windowsのパスワード変更機能を利用して変更する必要があります。(※)

※認証DBがOpenLDAPの場合、下記の条件となります。

- HP IceWall SSOからパスワード変更を行った場合、SRGateCAへ再ログインする必要があるため、パスワード変更はSRGateCAから実行することを推奨します。

お問い合わせ
株式会社日立ソリューションズ
・お電話でのお問合せ
0120-571-488 (受付時間　月～金(祝祭日除く) 10:00～17:30)
・Webからのお問合せ
http://www.hitachi-solutions.co.jp/icewall/

2012.5.30　株式会社日立ソリューションズ　システムプロダクト事業部　システム基盤本部　新村 健太氏