

自治体情報システム強靱化 インターネット分離環境におけるIceWall SSOの利用 IceWall技術レポート



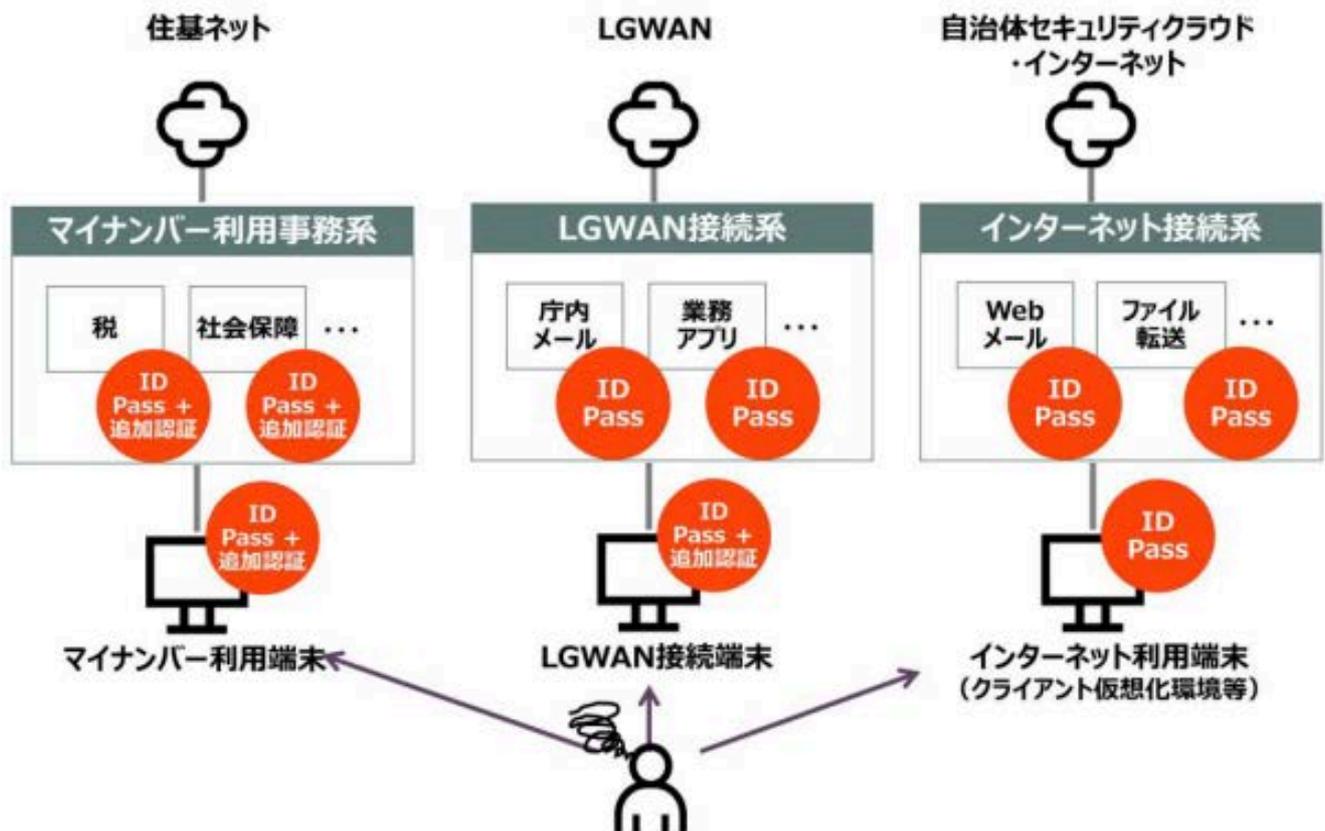
1. はじめに

総務省の自治体情報セキュリティ対策検討チームによる提言を受けて、各自治体においては庁内ネットワークのマイナンバー利用事務系・LGWAN接続系・インターネット接続系への通信経路の分離が行われていますが、それに伴うシステム利用の際の認証環境の複雑化により、ユーザーの生産性低下やセキュリティリスクの上昇が課題となりつつあります。

本技術レポートでは、インターネット分離環境における認証統合の例として、VMware® Horizon™によるクライアント仮想化環境へのIceWall SSOの適用例をご紹介します。

2. ネットワーク環境の分離に伴う課題

自治体情報システム強靱化のために分離された各ネットワーク環境においては、それぞれに使用する端末や業務システムが分かれることにより、その利用に必要なID/パスワードの種類が増え、目的のシステムまでに何度もログイン操作が必要になる等、ユーザーの利便性や生産性が低下しているケースがあります。

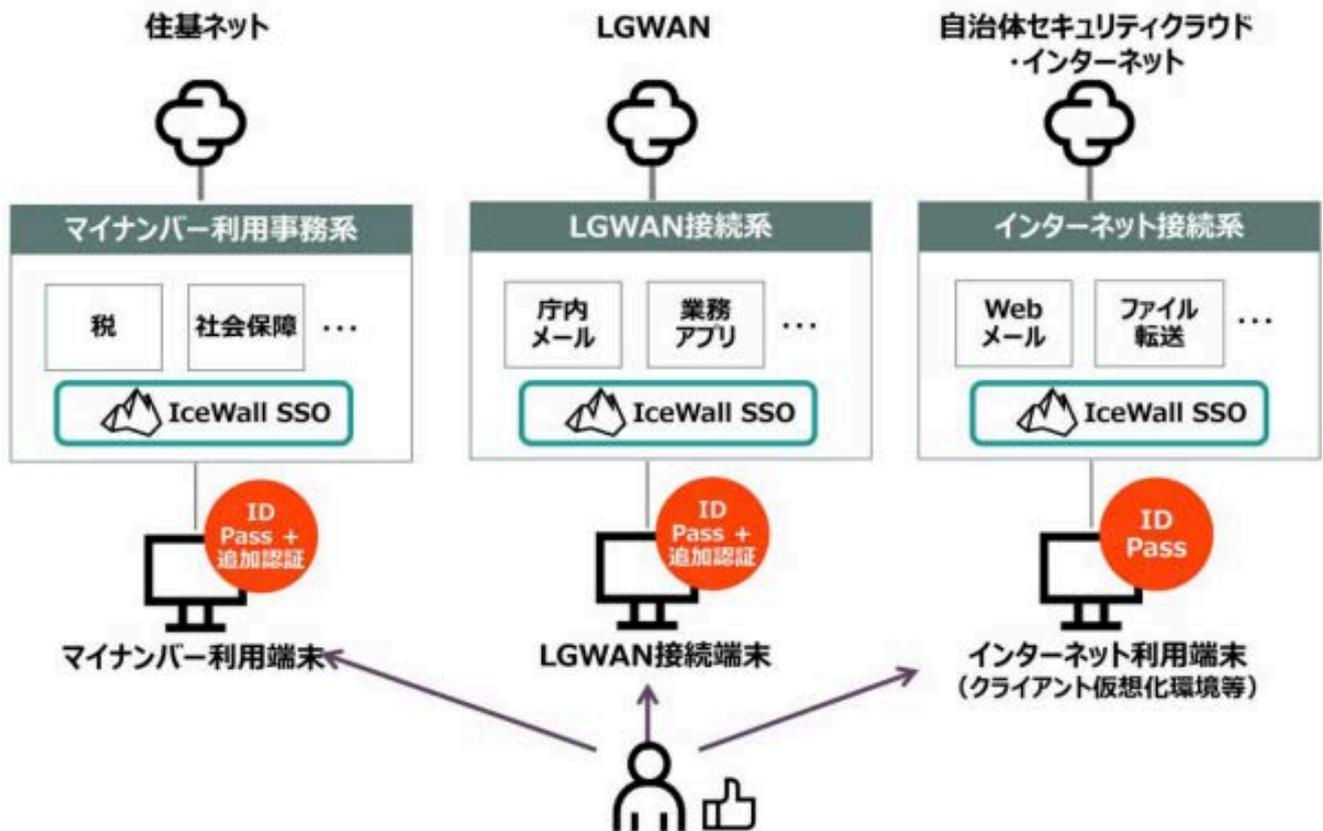


ID、パスワードの管理については、総務省より発行されている「地方公共団体における情報セキュリティポリシーに関するガイドライン」※の順守が重要であり、全業務システムのパスワードの定期的な変更、同じパスワードを連続して使用ができない、などが求められます。

したがって、パスワードが多数存在すると職員の記憶に限界が生じ、禁じられてはいるものの、結果的にパスワードの使い回しなどが増加し、情報漏えいリスクが上昇します。

これらの課題への対策としては、SSOが有効なソリューションであり、システム利用までのログイン回数を削減することにより、ユーザーの利便性とセキュリティの両立を実現します。

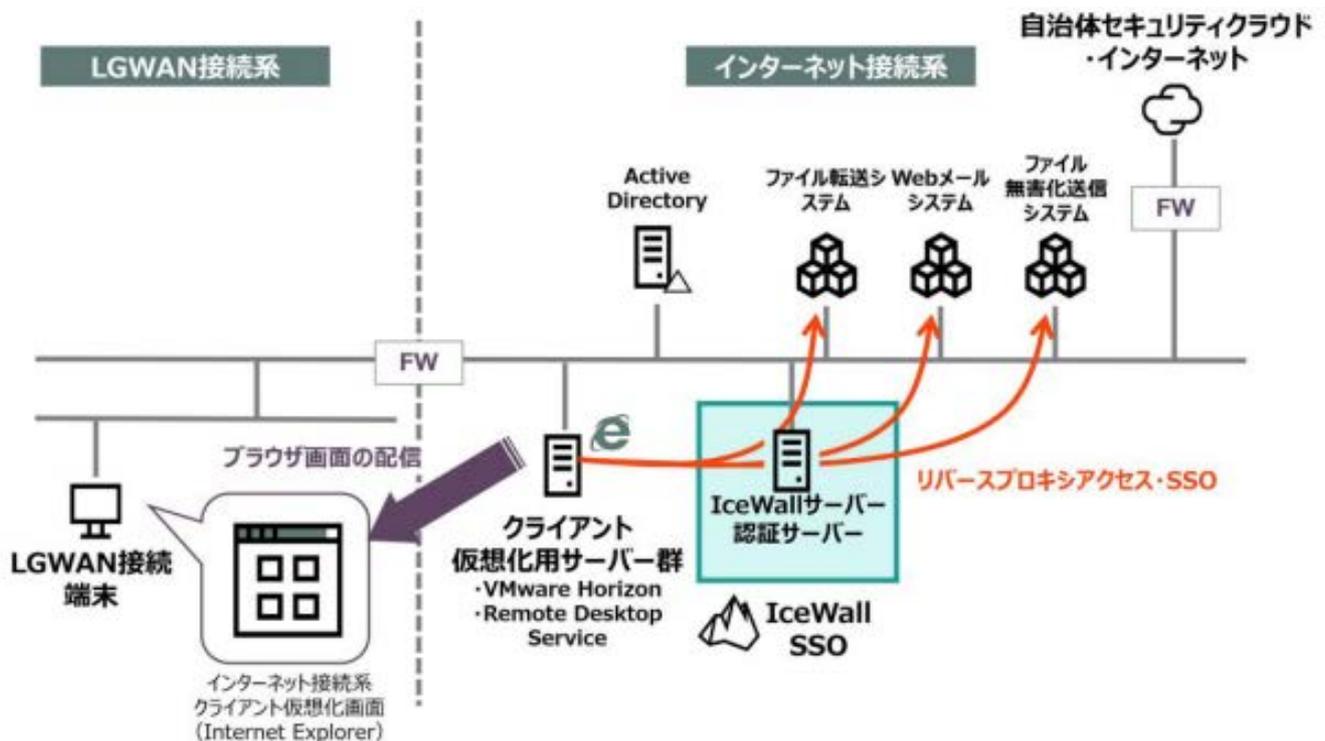
※「地方公共団体における情報セキュリティポリシーに関するガイドライン」 →



3. VMware® Horizon™によるクライアント仮想化環境へのIceWall SSOの適用例

今回は、自治体向けインフラ構築を多く手掛けている伊藤忠テクノソリューションズ株式会社(以下、「CTC社」と共同で、VMware® Horizon™によるクライアント仮想化環境の「Remote Desktop Service (RDS) を用いたアプリケーション配信 (公開アプリケーション)」から利用するインターネット接続系のWebシステム群に対し、Webシステム群の前段にIceWall SSOのサーバーを配置して、リバースプロキシ方式によるSSOの動作を検証しました。

システム構成は以下のイメージとなります。



今回、SSO対象としたWebシステムは次の通りです。

- ファイル転送システム FileZen V4.0.8 (株式会社ソリトンシステムズ)
- Webメールシステム DEEPMail 4.0.0 (QUALITIA社)
- ファイル無害化送信システム SWC (CTC社開発アプリケーション)

※ファイルサニタイズ(無害化)ソリューション VOTIRO Secure Data Sanitization (VOTIRO社)のフロントエンドアプリケーション

本検証では、以下の動作を確認しました。

- VMware Horizon Clientより起動した公開アプリケーション (Internet Explorer) から各Webシステムへのアクセス時のIceWallによる認証
- 各Webシステムへの認証をIceWall SSOが代行
- IceWallのリバースプロキシを経由した各Webシステムへのアクセス

設定上の注意事項は以下の通りです。

■ アクセスURL方式

■ 各Webシステムの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」を用いることで、リバースプロキシアクセスに容易に対応することが可能となります。「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 →

なお、次項に記載する「自動フォーム認証機能」を利用するため、ホスト設定ファイルにおいて、CTYPE項目の設定行は有効行(コメントアウトしない)にします。

■ 各Webシステムアプリケーションとの連携方式

■ 各Webシステムは、個別に認証機能を持つアプリケーションになるため、「自動フォーム認証機能」を利用して、アプリケーションへのシングルサインオンを実現します。「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？ →](#)

■ その他の連携設定

■ 各Webシステムのサーバーから圧縮したコンテンツがクライアントに返却される場合、「自動フォーム認証機能」が利用できないため、各Webシステムのサーバーへのリクエスト時に“Accept-Encoding”ヘッダを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）を行います。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 →](#)

■ IceWallによる認証機能のユーザー情報参照先DBとして、その環境内のユーザー情報を管理している既存のAD/LDAP等を設定することができます。それにより、既存のユーザー情報の登録管理やユーザーのパスワード変更等の運用の変更なしにSSO機能の追加が可能となります。

4. まとめ

IceWallでは、クライアント仮想化等を含むインターネット分離環境においても、各Webシステムに対するSSOが可能です。

オリジナルURL対応機能や自動フォーム認証機能等により、ご利用中のWebシステムのアプリケーションの改修やアクセスURL等の変更なく容易にSSO化することができます。

IceWallを既存のAD/LDAP等のユーザー情報で認証する設定にすることで、IceWallサーバーの導入だけで既存のユーザー情報によるSSOを実装することも可能です。

地方自治体向けにIceWall SSOを特別価格でご提供するキャンペーンを行っておりますので、この機会にぜひご検討ください。

[IceWall SSO 地方自治体向けキャンペーンはこちら →](#)

また、二要素認証が求められるマイナンバー利用事務系・LWAN接続系のWebシステム群に対しては、多要素認証ソリューションのIceWall MFAにより、ワンタイムパスワード認証やFIDOデバイス認証、その他現在ご利用中の認証デバイス/認証方式を使用し、お客様のポリシーに従った多要素認証の実装も可能になりますので、そちらも合わせてご検討ください。

[IceWall MFAについてはこちら →](#)

2017/10/5 新規掲載

執筆者 : 伊藤忠テクノソリューションズ株式会社
西日本支社 西日本システム技術第1部

日本ヒューレット・パカード株式会社
テクノロジーコンサルティング事業統括 IceWallソフトウェア本部 認証コンサルティング
部
谷垣 敦

[技術レポート一覧へ →](#)

お探しの情報は見つかりましたか？



ご購入方法



製品サポート



営業へのお問い合わせ



お問い合わせ先一覧



企業情報



会社情報

アクセス

お問い合わせ

採用情報

HPEについて

インクルージョン & ダイバーシティ

サステナビリティと企業責任

経営幹部

お知らせ



ニュースルーム

イベント・セミナー

新着情報

重要なお知らせ

パートナー



パートナープログラム

認定資格制度

OEMソリューション

サポート



製品サポート

ソフトウェア & ドライバー

標準保証確認

オペレーショナルサポート

教育とトレーニング

製品リサイクル

機器部品の妥当性確認

コミュニティ



HPE Japan ブログ

リソース



お客様事例

ご購入方法

オンラインストア

HPE Customer Center

Eメール登録

ドキュメントライブラリ

Resource Library

ビデオギャラリー

金融サービス

 日本 (ja)

© Copyright 2024 Hewlett Packard Enterprise Development LP

[個人情報保護方針](#) | [ご利用条件](#)・[免責事項](#) | [AdChoices & クッキー](#) | [サイトマップ](#)



