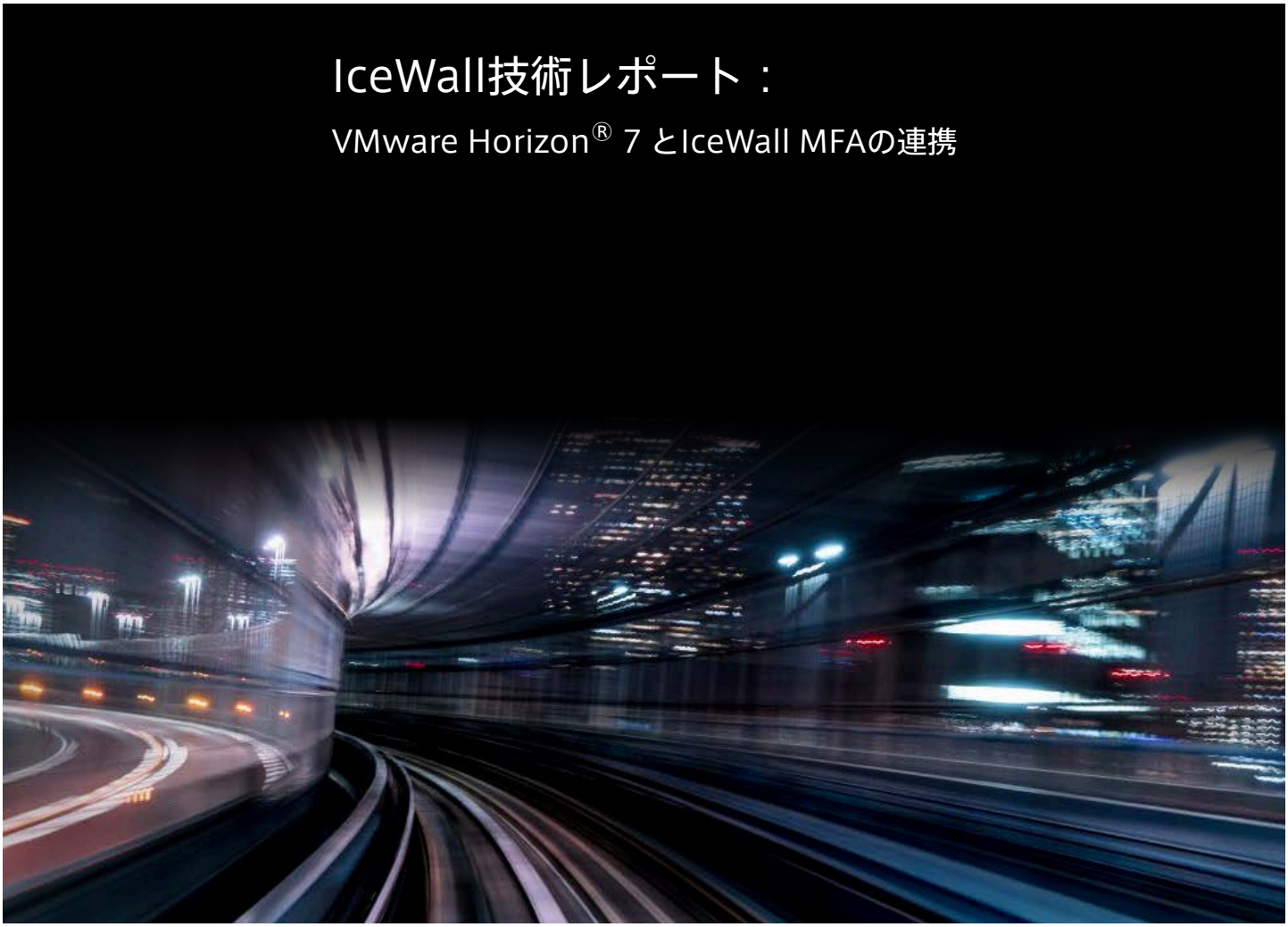
IceWall技術レポート：

VMware Horizon® 7 とIceWall MFAの連携



1. はじめに

仮想デスクトップ基盤（VDI）の利用が一般的となっている現在、社内だけでなく社外からの利用にも配慮したセキュアな認証要件が求められています。IceWall MFAは、各種生体認証やFIDO2準拠の認証、テクノロジーパートナーが提供する認証方式を取り入れ、様々な方式の認証の組み合わせによる多要素認証やパスワードレス認証を実現することが可能です。
本レポートでは、VMware Horizon 7 の認証連携としてIceWall MFAを利用する場合のユースケースおよび動作検証結果について説明します。

2. VMware Horizon 7 とは

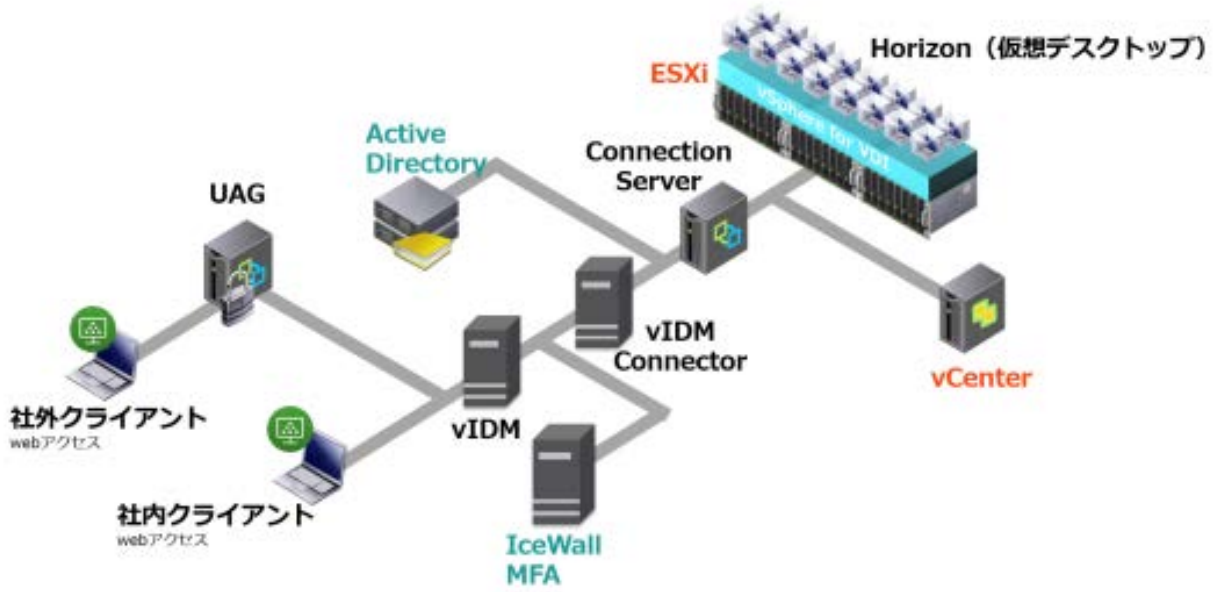
VMware Horizon 7 は業界をリードする仮想デスクトップとアプリケーションのプラットフォームを提供するVDIソリューションです。単一のデジタルワークスペースからの仮想デスクトップ、アプリケーションをエンドユーザーに提供します。

3. IceWall MFAとVMware Horizon 7 の連携

3.1ソリューション概要

IceWall MFAをVMware Horizon 7 の認証インターフェースとさせることで、IceWall MFAが提供する各種認証方式にてセキュリティ強化および利便性向上を実現することができます。
IceWall MFAとVMware Horizon 7 のシステム間は、VMware Identity Manager™（vIDM）*1 を使用してSAML2.0（IdP：IceWall / SP：vIDM）にて連携します。
これにより社内PCはもちろんのこと、BYODや社外の様々なデバイスからのアクセスに対して、柔軟な認証方式を適用できます。またVDIを利用するユーザーは、IceWallで認証連携しているその他のアプリケーションに対してシングルサインオンができるようになります。

*1 VMware Identity Managerは2019年8月からVMware Workspace ONE Accessに名称変更されましたが、本レポートでは検証時の旧名称を使用します。



3.2 システム構成

検証時のシステム構成を以下に示します。各コンポーネントについては次項以降で説明します。

本来であれば、社外アクセスのリバースプロキシを提供するUnified Access Gateway (UAG) はDMZ内に配置するのが一般的ですが、IceWall MFAとVMware Horizon 7 の連携がメインの検証目的のため、本環境ではインターネットアクセスは使用せずに簡易的な構成としています。

3.3 VMware コンポーネント

システム構成に記載の各種VMwareコンポーネントの説明は下記となります。

コンポーネント	機能
ESXi (vSphere) 6.7 EP 07	x86上でサーバー仮想化環境を提供するハイパーバイザー
vCenter Server Appliance (vCSA) 6.7 Update 1b	ESXi環境の一元管理
Horizon Connection Server 7.8.0	vCenterと連携してHorizon(VDI)環境を一元管理 クライアントとVDIとの接続を提供
VMware Identity Manager (vIDM) 19.03.0.0 *2	SAML SP として動作し、IceWall Federation(IdP)とSAML連携 クライアントの接続ゲートウェイとなりHorizonを含むアプリケーションカタログを提供

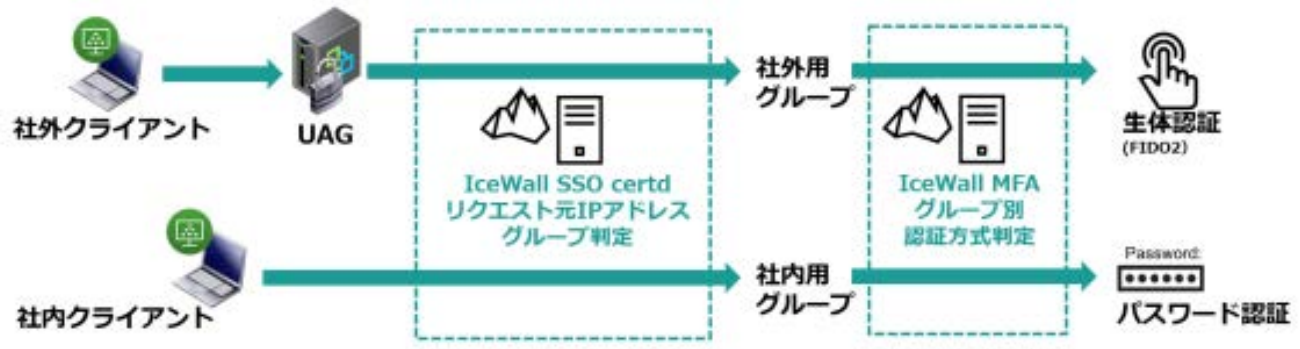
VMware Identity Manager Connector 19.03.0.0	vIDMとConnection ServerやADとの接続を中継
Unified Access Gateway (UAG) 3.4	社外からのアクセスの際にリバースプロキシとして動作
Active Directory ※Windows Server 2016	Microsoft社が提供するサービスコンポーネント DS/DNSを提供

*2 VMware Identity ManagerはHorizon 7 Advanced、またはHorizon 7 Enterpriseエディションにバンドルされています。

3.4 IceWall MFAコンポーネント

システム構成に記載の IceWall MFA サーバーには下記のIceWallコンポーネントが搭載されています。

コンポーネント	機能
IceWall MFA 4.0	多要素・多段階認証をコントロールする認証機能を提供する
IceWall Federation 4.0	SAML IdPとして動作し、VMware vIDM(SP)とSAML連携
IceWall SSO certd 11.0	IceWall MFAモジュールから認証リクエストを受付ける認証モジュール
OpenLDAP 2.4	IceWall 認証データベース



3.5 IceWall 設定

社外と社内別に認証方式を切り替えるため、IceWall SSO certdのグループ設定ファイルにリクエスト元のIPアドレス別のグループを定義します。IceWall MFAには認証方式に対応したpluginモジュールを設定します。これらの設定により、クライアント端末は 社外/社内 いずれかのグループに振り分けられ、グループに指定された認証方式を要求されます。

3.6 クライアントからのアクセス

社外クライアントのHorizon利用：

社外クライアントはUAGを経由してvIDMへアクセス（UAGは認証なしのリバースプロキシとして動作)。vIDM はSAML RequestをIceWall MFAにリダイレクトし、IceWall MFAにて認証が完了するとSAML ResponseをvIDMに送信します。vIDMにてセッションが払い出されHorizonが利用できるようになります。

社内クライアントのHorizon利用：

社内クライアントはvIDMにアクセスすると、vIDMがSAML RequestをIceWall MFAにリダイレクトし、IceWall MFAにて認証が完了するSAML ResponseをvIDMに送信します。vIDMにてセッションが払い出されHorizonが利用できるようになります。

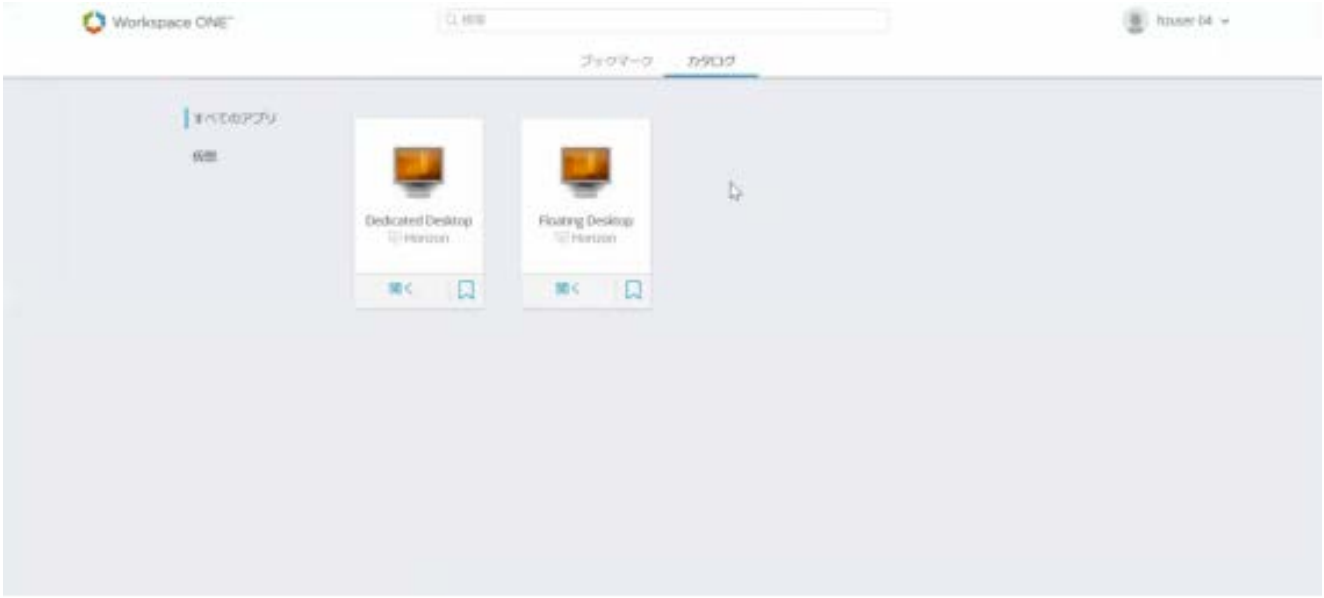
社外クライアントの場合には生体認証、社内クライアントの場合にはID/PWD認証といったように、アクセス元に応じてIceWall MFA の認証要素を切り替えることができます。

3.7 動作イメージ

① クライアント端末から（社外端末の場合はUAG経由で）vIDMにアクセスするとIceWall認証画面にリダイレクトされます。

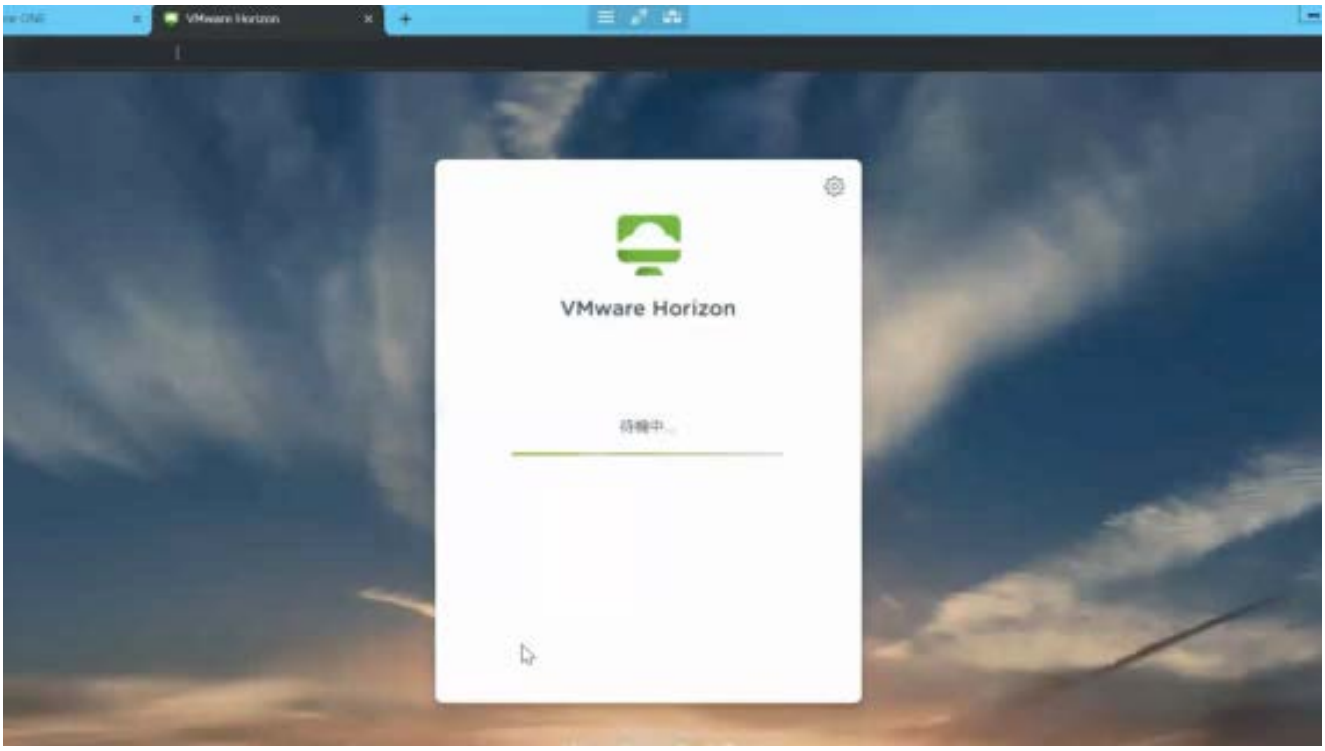
社外クライアントの場合：

社内クライアントの場合：



② 認証成功後 vIDMのメニュー画面（アプリケーションカタログ）に遷移します。

③ メニュー画面に表示されたVDIリンクをクリックすると ブラウザ または クライアントアプリ が起動してHorizonを利用することができます。



ブラウザ起動の場合：

認証されたユーザーで仮想デスクトップにシングルサインオン

Horizon Client起動の場合：

認証されたユーザーで仮想デスクトップにシングルサインオン

4. まとめ

VMware Horizon 7 とIceWall MFAをSAML2.0にて認証連携できることを確認しました。

IceWall MFA を VMware Horizon 7 の認証インターフェースにすることで、利用場所やユーザーアカウント別に認証方式を分け、セキュアで利便性に優れた認証ソリューションを実現することが可能となります。また、VMware Horizon 7 内で稼働する複数のWebアプリケーションに対して、IceWallのシングルサインオン機能を利用することで、IceWallを認証基盤として活用いただくことができます。

尚、具体的な設定方法につきましてはお問い合わせ下さい。

参考ＵＲＬ

VMware Horizon 7

2019/9/17

執筆者

- ヴイエムウェア株式会社

日本ヒューレット・パッカード株式会社

Pointnext事業統括 IceWallソフトウェア本部 認証コンサルティング部

技術レポート一覧へ →

お探しの情報は見つかりましたか？

検索のサポート

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

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)