IceWall技術レポート:

# VDIをワンタイムパスワードで認証強化
# – VMware Horizon

## 1. はじめに　～働き方改革とテレワーク～

安全なリモートアクセスを実現する手段として、VDI（Virtual Desktop Infrastructure：仮想デスクトップ）」が使われるケースが多くあります。

本技術レポートでは、VDIの代表的な製品である「VMware Horizon」と、ワンタイムパスワード製品「OneTime認証連携ツール for IceWall VDIオプション」の連携検証によって、「VDI」の認証セキュリティを効果的に強化する方法を紹介します。

## 2. 安全なテレワークを実現するテクノロジー　～VDI（仮想デスクトップ）～

社外からのリモートアクセスにつきまとうセキュリティの問題を、一気に解決できるテクノロジーとして注目を集めているのがVDIです。
仮想デスクトップは、画面転送技術を使って、社外の端末から社内のデスクトップ環境を遠隔操作する仕組みです。重要情報などの情報資産そのものを端末にダウンロードする必要がない（ダウンロードできない）ので、端末の紛失・盗難時にも情報資産そのものが紛失・盗難されることはありません。この利点によって、社員の全面的なテレワークの手段として、VDIは加速度的に導入が進んでいます。

一方で、外部インターネット経由のVDIの認証においては 、広く一般に使われるパスワードによる認証だけでは十分に強固だとは言えず、実際様々な多要素認証（MFA: Multi Factor Authentication）の仕組みが使われています。

## 3. VDI（仮想デスクトップ）での多要素認証

VDIの多要素認証には、ICカードや生体認証など、様々な種類がありますが、VDIの利点である「Any Device：あらゆるデバイスで利用できること」と強固な認証を両立し、かつコスト的にも低く抑えられる理想的な方法と言えるのが、今回紹介する「ソフトウェアベースのワンタイムパスワード」です。

多種多様な多要素認証の中で、IceWall SSOで提供されるワンタイムパスワードの優位性は、下記の技術レポートに詳しく書かれています。
≫ IceWall SSO ワンタイムパスワード(OTP)ソリューション

上記技術レポートの内容を要約しますと、次の通りになります。
「なりすましに対する認証強度が極めて高く、十分なユーザーの利便性を持つ」と言う旧来型のワンタイムパスワードの利点をそのまま維持しながら、旧来型ワンタイムパスワードの唯一の欠点であった「導入コスト」を低くなるように抑えたのが、「OneTime認証連携ツール for IceWall」です。

「OneTime認証連携ツール for IceWall」はユーザー数に依存しないライセンス体系のため、特にユーザー数の多い大規模な利用においてコストを低く抑えられます。まさに、VDIを使ったテレワークを広い範囲の社員に使わせるにあたって、理想的な認証強化方法と言えるでしょう。

## 4. OneTime認証連携ツール for IceWall VDIオプションについて

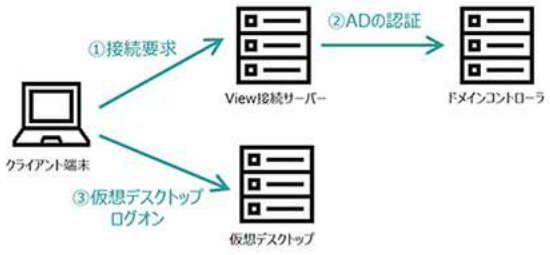
「OneTime認証連携ツール for IceWall 」は、本来 IceWall SSOへの認証を強化するためのワンタイムパスワード製品です。
その名の通り以前は、IceWall SSOと組合せでのみ利用可能でしたが、「VDIオプション」によって、IceWall SSOを構成すること無しに、VMware Horizon などのVDI製品と組み合わせて、VDI製品の認証強化を行うことができるようになりました。「VDIオプション」は、RADIUSプロトコルを使って、VDI製品との通信を行います。
OneTime認証連携ツール for IceWallに関する詳細は、開発元である株式会社エスシーシーの下記Webサイトをご覧ください。
≫ エスシーシー：OneTime認証連携ツール for IceWall（PDF）

## 5. VMware Horizon とは

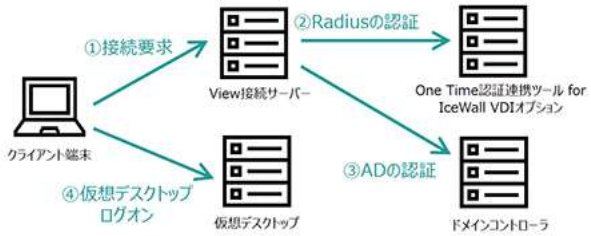
VMware Horizon は、VMware社が提供するVDI（仮想デスクトップ）製品です。 Windowsデスクトップやアプリケーションを、集中かつ効率的に管理しながら、エンドユーザーがセキュアかつ柔軟に利用できるように 、ネットワーク経由で配信します。VMware Horizon に関する詳しい情報は、下記のVMware 社のサイトをご覧ください。
≫ VMware Horizon 7

## 6. VMware Horizon ＋ OneTime認証連携ツール for IceWall VDIオプションの認証連携概略

通常の（多要素認証無しの）VMware Horizon では、クライアント端末からの接続要求を一旦セッションブローカーの役目を果たす「View 接続サーバー」が受け、利用者が入力したユーザー名とパスワードをドメインコントローラに照会した上で、その認証が通れば適切な仮想デスクトップセッションに接続させるような処理を行います。




VMware Horizon の機能として3rd Partyの多要素認証を付加することが可能ですが、その場合View 接続サーバーがドメインコントローラへの認証を行う前に、RADIUSプロトコルを使った認証が行われます。OneTime認証連携ツール for IceWall VDIオプションは、RADIUSサーバーとして動作し、View 接続サーバーからの認証要求を受ける形となります。





## 7. 連携設定と接続検証

下記の1) ～ 3) の流れで、設定と動作確認を行います。
1) 前提条件の確認
2) View 接続サーバーの設定
3) Horizon Clientでの動作確認

以下、設定の詳細について説明します。

### 1) 前提条件

まず、VMware Horizon の各コンポーネントについては、利用者がユーザー名とドメインのパスワードを使ってHorizon Clientにログオンし仮想デスクトップにアクセスできるように、正しく構成されていることを前提とします。


また、OneTime認証連携ツール for IceWall およびそのVDIオプションについても正しく構成され、アクティベートされたトークンが検証されていることを前提とします。


### 2) View 接続サーバー設定

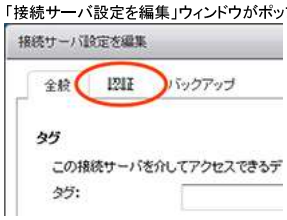
「Horizon Administrator」に、管理者アカウントでログオンします。


「Horizon Administrator」で、左側ナビゲーションペインの「サーバ」をクリックします。


右側ペインにて、「接続サーバ」タブをクリックします。


適切なView 接続サーバーを選択し、「編集…」ボタンをクリックします。


「接続サーバ設定を編集」ウィンドウがポップアップしますので、「認証」タブをクリックします。



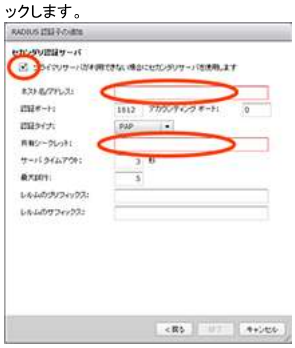

「高度な認証」の下の「多要素認証」プルダウンメニューで、「RADIUS」を選択します。


さらにその下にある「認証子」プルダウンメニューで「新しい認証子の作成」を選択します。


「RADIUS認証子の追加」ウィンドウがポップアップします。
まず「ラベル」欄に、新たに命名した認証子の名称を入力します。
この名称は、全角を含む任意の文字列で構いませんが、ユーザーのログオン時に「＜認証子の名称＞のユーザー名とパスコードを入力してください」と表示されますので、ユーザーにとって分かりやすい名称をつけてください。

続けて「ホスト名/アドレス」欄に、「OneTime認証連携ツール for IceWall VDIオプション」のIPアドレスを入力し、さらに「共有シークレット」欄に、OneTime認証連携ツール for IceWall で設定した秘密鍵を入力し、（その他の欄は、デフォルトのままで結構です）「次へ」をクリックします。

冗長化のため、2台目の「OneTime認証連携ツール for IceWall VDIオプション」を構成する場合は、「プライマリサーバが利用できない場合にセカンダリーサーバを使用します」にチェックを入れ、2台目の「OneTime認証連携ツール for IceWall VDIオプション」のIPアドレス、および共有シークレットを入力し、「終了」をクリックします。
2台目の「OneTime認証連携ツール for IceWall VDIオプション」を構成しない場合は、そのまま「終了」をクリックします。



すると「認証子」として、上でラベルとして入力した文字列が表示されていることが確認できます。
これでHorizon Administratorでの設定は終了です。

3）VMware Horizon Clientでの動作確認

Horizon Clientがインストールされたクライアント端末で、VMware Horizon Clientを起動します。


接続先のサーバーエントリをダブルクリックします。


最初にワンタイムパスワードが求められますので、ドメインのユーザー名と、トークンに表示されたワンタイムパスワードを入力します。

ワンタイムパスワードの認証が成功すると、次はドメインパスワードの認証が求められますので、続けてドメインのユーザー名とパスワードを入力します。

ワンタイムパスワードと、ドメインのパスワード、2つの認証を行うことで、仮想デスクトップにアクセスすることができるようになりました。つまり、仮想デスクトップの利用に、多要素認証が必要になったと言うことになります。


## 8. まとめ

上記の「連携設定と接続検証」で示した通り、View 接続サーバーの簡単な設定のみで、VMware HorizonとOneTime認証連携ツール for IceWall VDIオプションを連携できることが確認できました。

この連携によって、仮想デスクトップ利用時の認証にワンタイムパスワードを付加した多要素認証を義務付け、認証をより強固にすることが可能です。
OneTime認証連携ツール for IceWall VDIオプション を使った仮想デスクトップの多要素認証化は、「Any Device（どんな端末からでも同じように使える）」と言う仮想デスクトップの利点を活かしながら、認証の強化を比較的低い導入コストで実現できます。

## 本ソリューションに関するお問い合わせ

2017/2/21　新規掲載

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 IceWallソフトウェア本部
シニアプロダクトマネージャー　山田 晃嗣