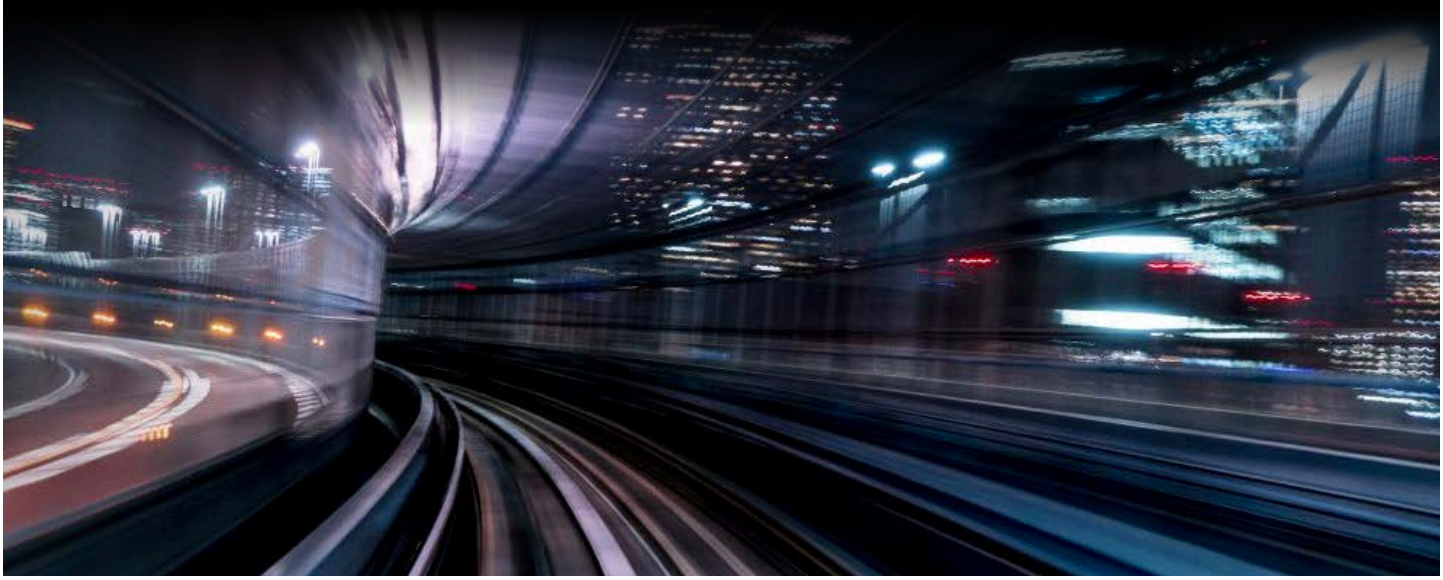
PassLogicとIceWall MFAの連携
IceWall MFA 認証プラグインによる各種認証方式との連携

IceWall技術レポート



1. はじめに

IceWall MFAでは、Webアプリケーションへのログインのセキュリティを強化するために、IDとパスワードに加え他の認証方式を追加する多要素認証を行うことができます。

多要素認証に使用される認証方式は、ICカード、生体認証、ワンタイムパスワード（OTP）などが主流ですが、それぞれ、ICカードとカードリーダー、生体情報読取り機、OTPトークンなどのデバイスの追加とその運用管理にコストが発生します。

OTPの場合、ハードウェアトークンではトークンの購入コスト、紛失リスク、電池切れや時刻ズレによる買い替えコストなどが課題となります。

一方、ソフトウェアトークンでは、ソフトウェアをインストールする端末の用意、ソフトウェアのインストールとseed値の登録操作など、ユーザーが利用し始めるときのサポートが必要です。

パスロジ株式会社が提供する認証システム製品「PassLogic」 は、ハードウェアトークンや特別なデバイスが不要で、かつユーザーが特別なソフトウェアをインストールする必要のないパスロジック方式のOTP認証を提供します。

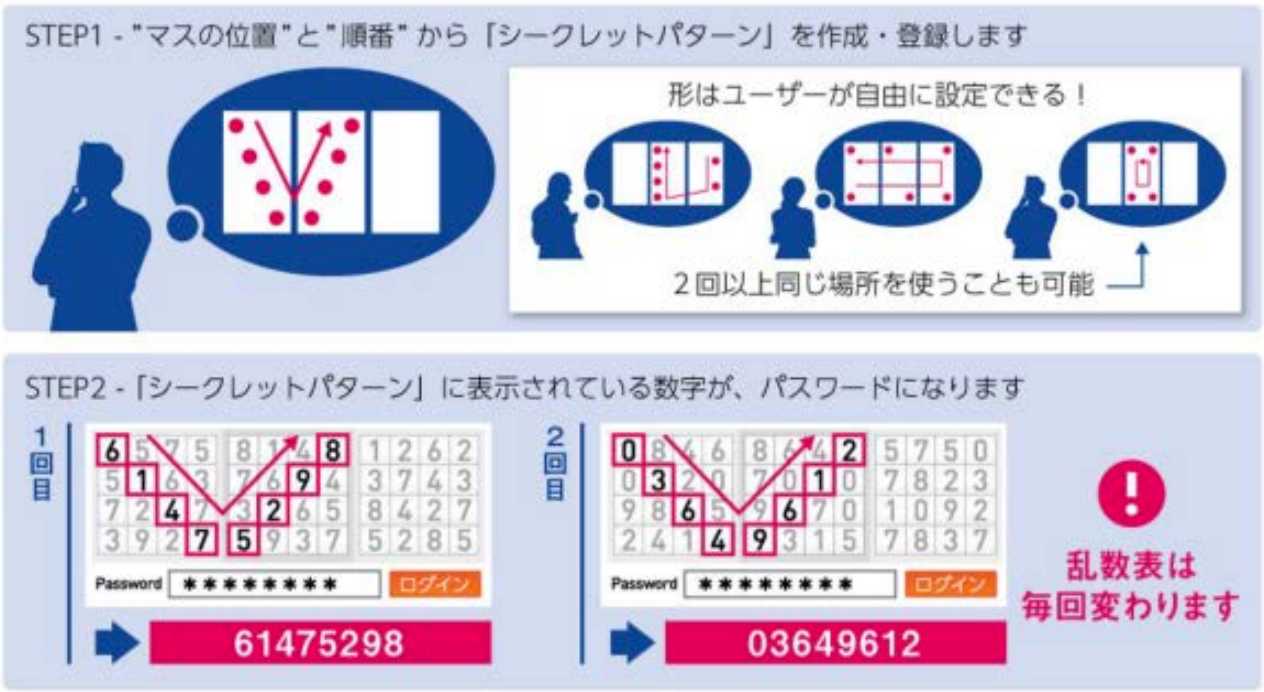
パスロジック方式はOTPの実現方式として「トークンレス方式」および「マトリクス方式」に分類され、実装方式は「チャレンジ・レスポンス方式」に分類されます。

本レポートでは、IceWall MFA 4.0 に、PassLogic製品によるパスロジック方式のOTP認証 を追加する方法をご紹介いたします。

---

2. パスロジック方式による認証

パスロジック方式は、乱数表からユーザーが記憶しているパターンに沿って抜き出した数字をパスワードとする認証方式です。



ユーザーは、数字が記されたマス目の表（乱数表）の「マス目の位置と順番」（シークレットパターン）を記憶します。

乱数表から記憶しているシークレットパターンに沿って、数字を抜き出してこれをパスワードとします。

認証のたびに乱数表に記される数字がすべて一新され、パスワードは一度限り有効です。

パスロジック方式は「チャレンジ・レスポンス方式」によるOTP認証であり、１回の乱数表の表示に対して１度しかログインの要求が受付けられません。つまりログインの操作を行う度に、新しい乱数表を使ってパスワードを作成します。一定時間内であれば同じパスワードが何度でも使用できる「時刻同期方式」のOTP認証と比べると、パスロジック方式はハッキングに強いと言えます。

パスロジ株式会社のPassLogic製品は、乱数表をWebブラウザー上に表示することで特別なデバイスを使用せずにOTP認証を実現できることが特徴です。

さらに端末へインストールするソフトウェアが不要なため、マルチデバイス環境でも利用することができます。

ユーザーが記憶するシークレットパターンには、複雑さのポリシーの設定ができます。

例えば、一筆書きでなぞれるシークレットパターンを禁止するなどが可能です。また、乱数表とシークレットパターンから生成するパスワードに加えて、固定文字列の付加を必須とさせるなどのポリシー設定もできます。

---

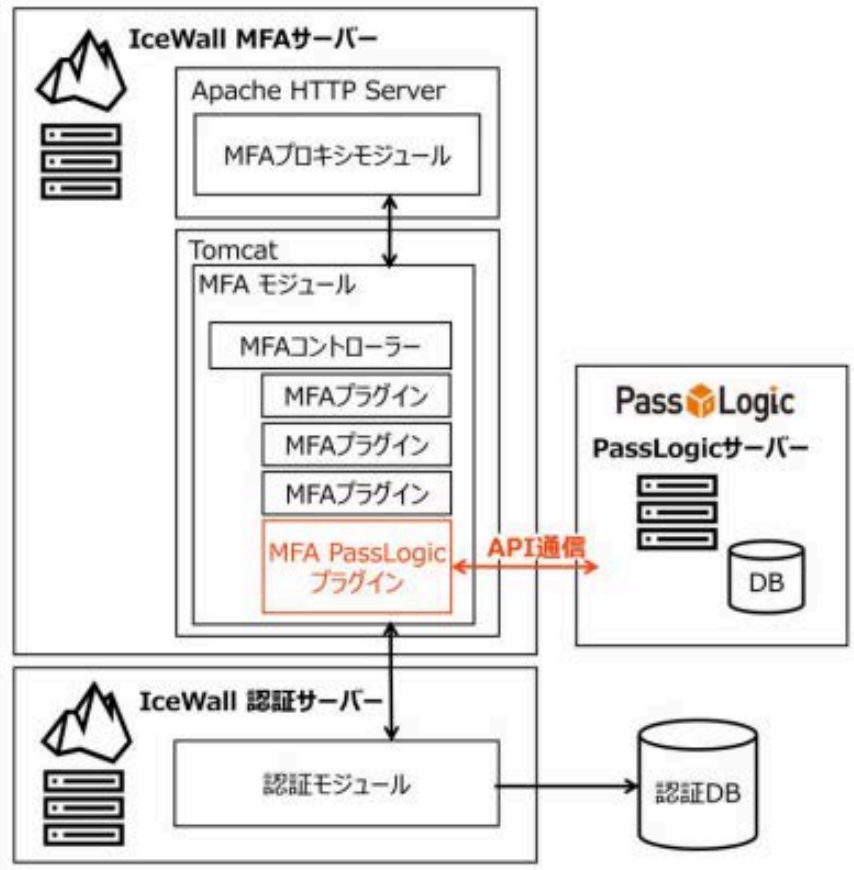
3. IceWall MFAとPassLogicの連携

3.1 IceWall MFA のプラグイン

IceWall MFA には、サードパーティが提供する認証方式と容易に連携するための、プラグインの仕組みが用意されています。

プラグインの仕様はテクノロジーパートナー各社へ公開され、仕様に基づいてプラグインモジュールを開発することで、様々な認証方式を取り込むことができます。

今回は、PassLogic用のプラグインを開発し、パスロジック方式の認証がIceWall MFA の追加認証として動作することを確認しました。



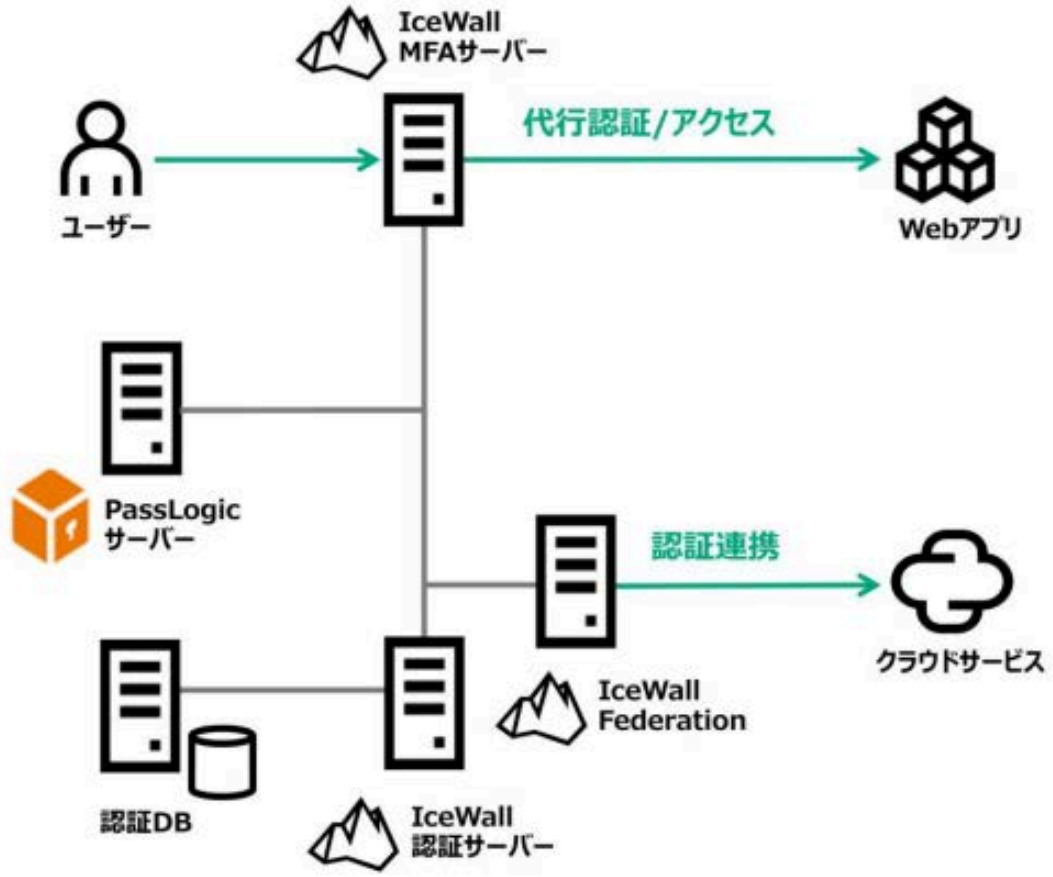
3.2 PassLogic連携プラグイン概要

開発したPassLogic連携プラグインは、PassLogicが提供するXMLベースのREST APIを利用して、マトリクス情報（乱数表情報）の取得と認証要求処理を行います。

乱数表の画面 および エラー画面はHTMLテンプレートファイルを修正することでカスタマイズが可能になっています。

3.3 システム構成

IceWall MFA とPassLogicとを連携するシステム構成の概略図です。

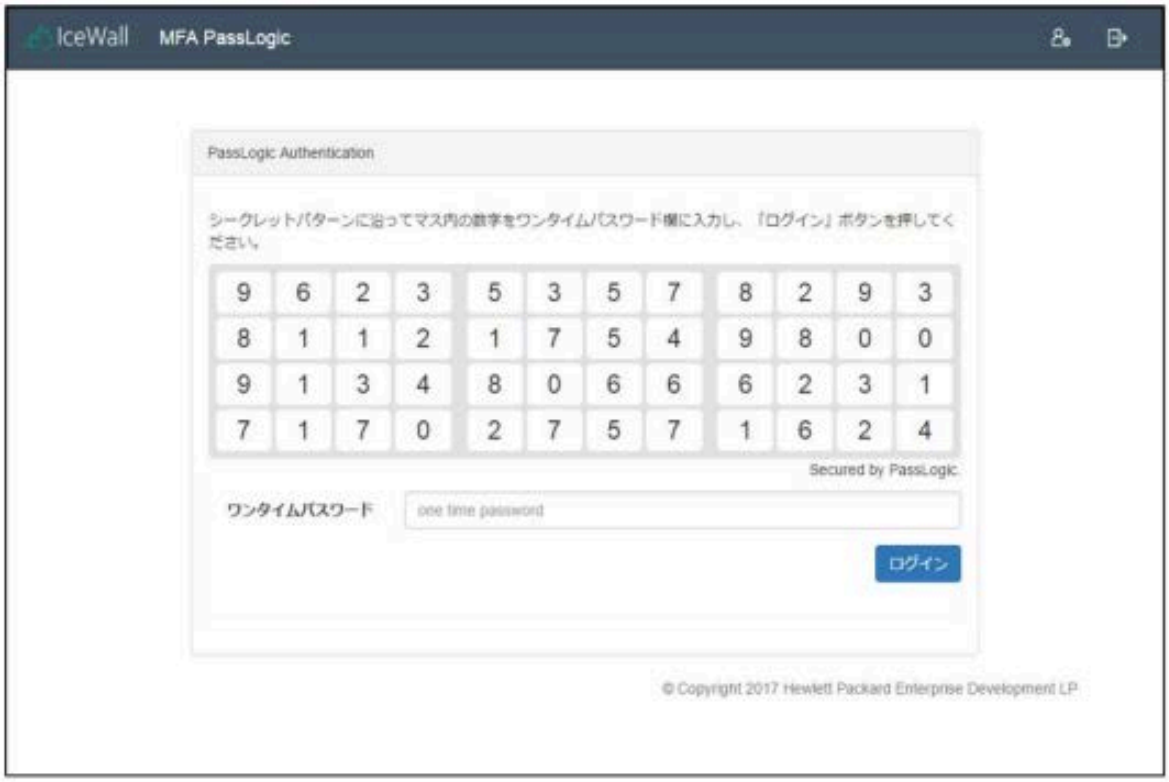


3.4 ユーザーシーケンス

以下は連携プラグインによってID・パスワード認証の後にパスロジック方式の認証を行った際の画面遷移です。

① ユーザーIDとパスワードを入力してログインします

② 乱数表が表示されるので、シークレットパターンに沿ってワンタイムパスワードを入力します。



③ ログインが完了し、アプリケーションの画面が表示されます

4. まとめ

PassLogic連携プラグインによってIceWall MFA の追加認証にPassLogicを使用できる事を確認できました。
連携プラグインの詳細について情報が必要な場合はお問い合わせください。
多要素認証の１つとしてワンタイムパスワードを採用される場合は、トークン不要でマルチデバイスで利用できるPassLogicをご検討ください。

参考URL：

パスロジ株式会社「PassLogic」 →

多要素認証基盤 IceWall MFA →

2017/8/24 新規掲載

執筆者　：パスロジ 株式会社

PassLogic事業部

日本ヒューレット・パッカード株式会社
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

大村 卓央

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

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)