仮想デスクトップサービス

「Amazon WorkSpaces」への認証に「PassLogic」のソフトウェアトークン型ワンタイムパスワードを導入

TOKAI グループとして情報通信事業を手掛け、「Amazon WorkSpaces」の導入支援に力を入れている TOKAI コミュニケーションズ社では、社員が社外に持ち出して使用する PC 端末で、Amazon WorkSpaces を利用する際の認証に PassLogic のソフトウェアトークン型 OTP（ワンタイムパスワード）認証機能を導入しています。
その利用シーンと、システム構成、認証システムとして PassLogic を採用した理由について、今回の導入製品選定に携わられた TOKAI コミュニケーションズ社 法人営業本部 クラウドソリューション推進室 インテグレーション課 課長 高谷様と、同課 武井様にお話を伺いました。

TOKAI GROUP
TOKAIコミュニケーションズ

株式会社 TOKAI コミュニケーションズ
TOKAI Communications Corporation

設立：1977年3月18日　従業員数：1,140人 ※2016年4月1日時点
URL：http://www.tokai-com.co.jp/

法人営業本部
クラウドソリューション推進室
インテグレーション課
課長 高谷様

法人営業本部
クラウドソリューション推進室
インテグレーション課
武井様

導入の背景・課題

- ☐ 社外からAmazon WorkSpaces利用時の認証強化
- ☐ PassLogicを取扱製品とするための研究

導入後の改善効果

- ✓ 「2要素認証」の実現による認証の強靭化
- ✓ インシデント発生時の状況把握が容易になった。

社外からの接続に「Amazon WorkSpaces」を利用

企業のIT化が進んだ現在において、PC 端末を社外に持ち出して、打ち合わせやプレゼン、デモンストレーションに使用することは当たり前になっていると思います。当社でも営業部をはじめとした社員たちが、PC 端末を持ち出して使用しています。そこでコンプライアンス上の課題となるのが、端末紛失時のデータ漏洩対策です。
当社では、持ち出し PC からの社内ネットワークへの接続には、仮想デスクトップサービス「Amazon WorkSpaces」を導入し、PC 端末上にはデータを残さない仕組みを構築しました。
しかし、Amazon WorkSpaces に、通常のアカウントとパスワードだけでログインできてしまう状況は、セキュリティとして十分ではありません。パスワード以外の認証要素による強化が必要だという判断があり、そこでワンタイムパスワード製品の導入を検討しました。

PassLogic 採用の理由

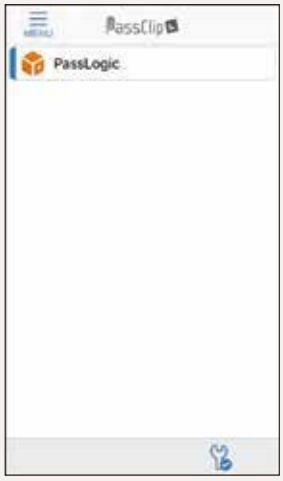
情報サービス事業を展開し、顧客に IT システムの導入支援を行っている当社としては、実際に運用して問題がなければ、取扱製品として販売することも視野に入れて、日本製、海外製を問わず、さまざまなワンタイムパスワード製品を検討しました。
ワンタイムパスワードというと、時間によって切り替わる TOTP（Time based One-Time Password）が一般的で、ハードウェアトークン型とソフトウェアトークン型があります。
当社では、対象の社員にはすでに業務用スマートフォンを配備しており、ソフトウェアトークン型であれば新たなデバイスを用意する必要がありません。顧客企業の間でも社員のスマートフォン利用は進んでいる状況です。ですので、ソフトウェアトークン型 OTP 製品からの選択となりました。
ワンタイムパスワードというと、ハードウェア型、ソフトウェア型に関わらず、大抵の場合はデバイス上に数字をそのまま表示するタイプになります。その点、PassLogic は独特なパスワード表示方法を採用しています。PassLogic は、パスロジ社が無償配信しているパスワード管理アプリ「パスクリップ」と連携する形で、ソフトウェアトークン型 OTP 機能を提供しているのですが、このパスクリップのパスワード表示形式は、第3者にパスワード表示画面を盗み見られたとしても、パスワードを知られることがありません。画面を肩越しに見られる「ショルダーハッキング」に強い仕組みです。この独自性を評価しました。
価格においてもPassLogic はリーズナブルで、サーバソフトウェアとライセンスといった導入時の費用において、他の製品の7割程度の価格が算出されました。また、日本製なので、国内からのメーカーサポートが受けられる点も大きな利点です。実際の導入過程においてもメーカから十分なサポートを受けることができました。インストールプログラムも用意されているため、サーバ準備の手間もかかりませんでした。

スマートフォン用アプリ「パスクリップ」の特徴

ひとつの「パターン」を覚えるだけで、複数のパスワードを管理できるパスワード管理アプリです。
パスワードは、ビンゴのような５×５のマス目の中に文字が表示され、ユーザがあらかじめ決めて置いた「パターン（マス目の位置と順番）」に沿って文字を抜き出して、パスワードを判別する仕組みとなっています。PassLogic サーバと連携し、その認証サーバ用の TOTP を表示することも可能です。

■認証手順：Amazon WorkSpaces 連携の場合

❶スマートフォン上の「パスクリップ」を起動し、対象のスロットをタップ



❷5×5のマス目からパターンに沿って数字を抜き出し、OTP を確認

❸Amazon WorkSpaces を起動。サインイン画面が表示される。

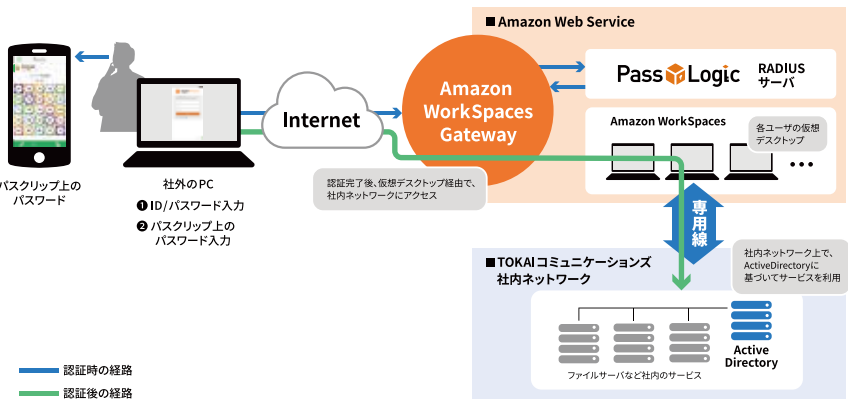
❹通常の「ユーザ名」と「パスワード」に加えて、パスクリップで確認したOTPを「MFACode」に入力

サインイン成功／失敗

各システムとの連携方法

PassLogic の認証サーバは、Amazon WorkSpaces の MFA（Multi Factor Authentication）機能で追加可能な RADIUS サーバとして働きます。Amazon WorkSpaces で標準設定されているアカウントとパスワードに加えて、RADIUS プロトコルに則った認証を Amazon WorkSpaces と PassLogic 間で行います。この設定は、Amazon WorkSpaces と PassLogic、それぞれの管理画面上で行えばよいので、特に難しいこともなく、手間なく行うことができました。
Amazon WorkSpaces と PassLogic への認証が完了すると、専用線を経由して当社の社内ネットワーク内にある「ActiveDirectory」にアクセスし、アカウント情報を参照します。そのアカウント情報に応じて、社内ネットワーク上のファイルサーバなどにアクセス可能となります。

■利用イメージ図



PassLogic 導入後の状況と、今後の予定

PassLogic の導入により、「アカウント&パスワード」＋「ソフトウェアトークン型 OTP」という組み合わせの2要素認証が実現し、コンプライアンス上の課題が解決しました。しかも、パスクリップのビンゴ型表示形式も採用しているため、通常の数字を表示するだけの OTP よりも強力です。
トラブル時にログを参照する際にも、PassLogic は当社でも理解が進んでいるオープンソースソフトウェアで構成されているため、分析が容易に行えることも利点です。
今回は PassLogic を Amazon WorkSpaces への認証として連携しましたが、他の仮想デスクトップサービスや VPN サービス、クラウドサービスなどにも連携可能です。当社では今後、さまざまなサービスとの連携方法を習得し、運用実績を重ねて、顧客の皆様にも安心して利用できる IT システム環境の構築を提案してまいりたいと思います。

PASSLOGY™
パスロジ株式会社
www.passlogy.com
パスロジック事業部
03-5283-2263
受付時間 10:00～17:00［土・日・祝休］
E-MAIL：sales@passlogy.com
セキュリティ情報サイト
せぐなべ 検索
www.segunabe.com
お問い合わせ先