PassLogic 導入事例 クオリカ株式会社

BCP対応から全社的テレワーク対応へ
VPNの認証強化に「トークンレス・ワンタイムパスワード」を採用

製造業・流通サービス業を中心に、企業の情報システムに関して、課題やより効率の良い活用に向けたコンサルティングから、企画～設計～運用・保守まで一貫したサービスを提供するクオリカ社は、全社的にテレワークを導入しています。
このテレワークで利用する仮想デスクトップ（VDI）サービスを利用する際の SSL-VPN 接続に、「PassLogic」のトークンレス・ワンタイムパスワードによる認証をご採用いただきました。
PassLogic 導入の経緯や導入プロセス、導入後の効果について、クオリカ株式会社 イノベーションテクノロジー本部 生産革新部 菊井様にお話を伺いました。

QUALICA TIS INTEC Group

クオリカ株式会社
QUALICA Inc.

設立：1982 年 11 月 1 日
従業員数：969 名　※2020 年 4 月時点
URL：https://www.qualica.co.jp/

クオリカ株式会社 イノベーションテクノロジー本部
生産革新部 菊井様

導入の背景・課題

- ☐ SSL-VPN 接続環境を全社的に導入。その本人認証を強化は必須
- ☐ 以前に利用していた端末証明書は、証明書発行に手間がかかる
- ☐ 共同利用端末内の異なるアカウントでも認証を容易に
- ☐ 海外のビジネスパートナーのオフィスにも同等の環境を構築

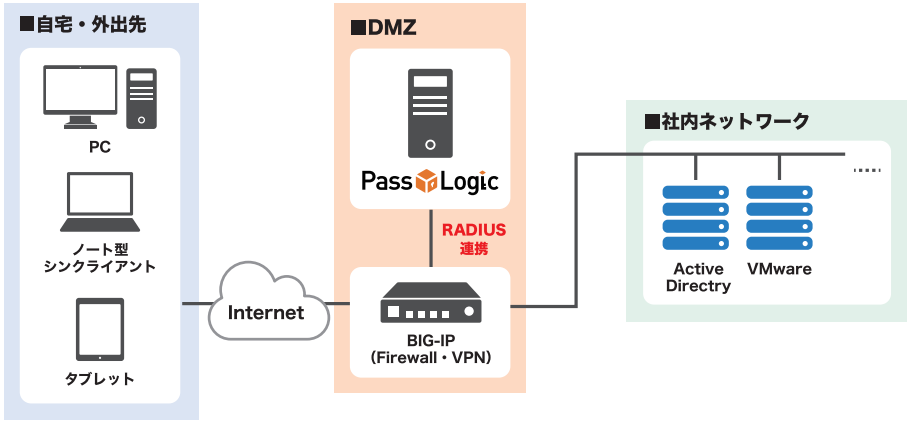
導入後の改善効果

- ☑ 安全性と、利用者の利便性を両立したテレワーク環境を実現
- ☑ 業務端末更新が手間なく、迅速になった
- ☑ アカウントごとの認証設定が不要に
- ☑ 国内・海外を問わず、遠隔地でも迅速に導入が完了

東日本大震災による BCP 対策から、新型コロナによるテレワーク導入へ

当社においてリモート業務環境の構築を開始するきっかけは、2011 年の東日本大震災でした。局地的な停電が発生した状況でも業務を継続する環境（BCP）の構築が必須だと認識し、VDI システム「VMware Horizon」と、VDI への接続に「BIG-IP APM」による SSL-VPN を導入。東京地区を皮切りに全国の拠点に展開しました。
この時すでに、リモート業務環境へのログインにはパスワード認証だけでは不十分だと認識していましたので、端末証明書による認証製品を導入しました。しかしこの製品は、端末内でアカウントを切り換えるたびに、証明書を新たに発行し、インストールをし直す必要があり、利用者および管理者の手間がかかることが判明しました。
さらに、2018 年には大阪北部震災の際には、現地の従業員が出勤不可能となるの恐れが生じ、在宅勤務への移行に急遽対応することとなりました。この際には、対象となった従業員への証明書の発行と送付、そしてインストール方法を指示する作業に手間と時間がかかり、勤務開始時刻に間に合わず、業務に支障が出てしまう可能性が発生。結果としては在宅勤務には至らず、事なきを得ましたが、ここでも運用の課題が残りました。
その後、端末証明書製品のサポートが終了したことを受け、全社的なリモート業務の導入と運用コストの削減を念頭においた次期認証製品の選定を開始。PassLogic が候補として挙がりました。

■ 利用イメージ図



PassLogic 採用の理由

まず、既存の SSL-VPN である BIG-IP APM と連携可能なことは必須条件です。PassLogic には連携実績があり、BIG-IP APM のメーカーである F5 ネットワークスジャパン社との連絡も取り合っていることから問題ないと判断しました。

また、大阪北部震災時の経験から運用の利便性を重視しました。PassLogic のトークンレス・ワンタイムパスワードは、認証用にデバイスや証明書を用意し、従業員に送付する必要がなく、管理画面からメールを送信するだけで利用開始できることが今回の課題に合致していました。

ライセンスの契約単位が端末数ではなく、ユーザー数であることも判断材料になりました。テレワーク利用が前提ですので、従業員は拠点と自宅で、または複数の拠点で業務し、複数の端末を使用するケースが多くなるため、端末数で契約するとなるとライセンス数が増え、コスト増となります。従業員が利用する端末数を増減させる際にも契約管理が必要となり、運用コストがかさんでしまいます。その点、PassLogic はユーザーアカウント単位の契約ですので、対象者の増減にのみ対応すれば問題ありません。

新型コロナ対応で、テレワーク対象拡大と迅速な導入を実施

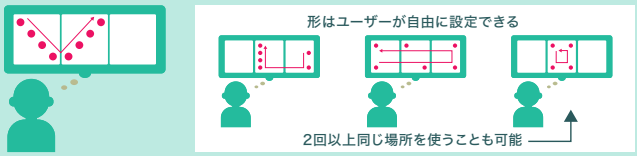
製品選定の途中で、新型コロナウイルス感染症が流行し始めました。この対策として、テレワークの対象を海外のビジネスパートナーにも広げることに決定。PassLogicの適用範囲も拡大することとしました。その際にも、現地訪問や機材送付等のコストがかからない利点が生かされています。

また、英語にも対応しているため、日本語を母語としない海外スタッフでも問題なく利用を開始しています。

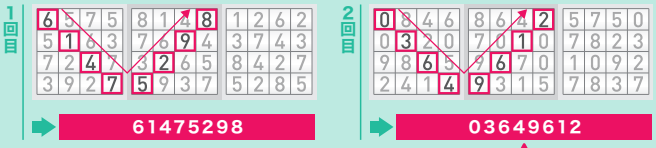
ただし、「乱数表からパターンに沿って数字を抜き出す」というログイン方法は、従業員にとって初めて接する方法なため、オンライン説明会を行いながら、段階的な導入を進めています。説明の際には「Androidスマートフォンのロック解除の方法に近い」と言うと理解してもらいやすいようです。

トークンレス・ワンタイムパスワードの仕組み

STEP 1 “マスの位置”と“順番”から「パターン」を作成・登録します



STEP 2 「パターン」に表示されている数字が、パスワードになります



認証用デバイスや証明書は不要（※）
※証明書を利用した二要素認証も実現可能

- ブラウザさえあればログイン可能
- 導入・運用コストが削減
- 利用開始はメール送付のみ

乱数表は毎回変わります → パスワードも毎回変わります！

ID 入力を自動化し、管理コストを削減

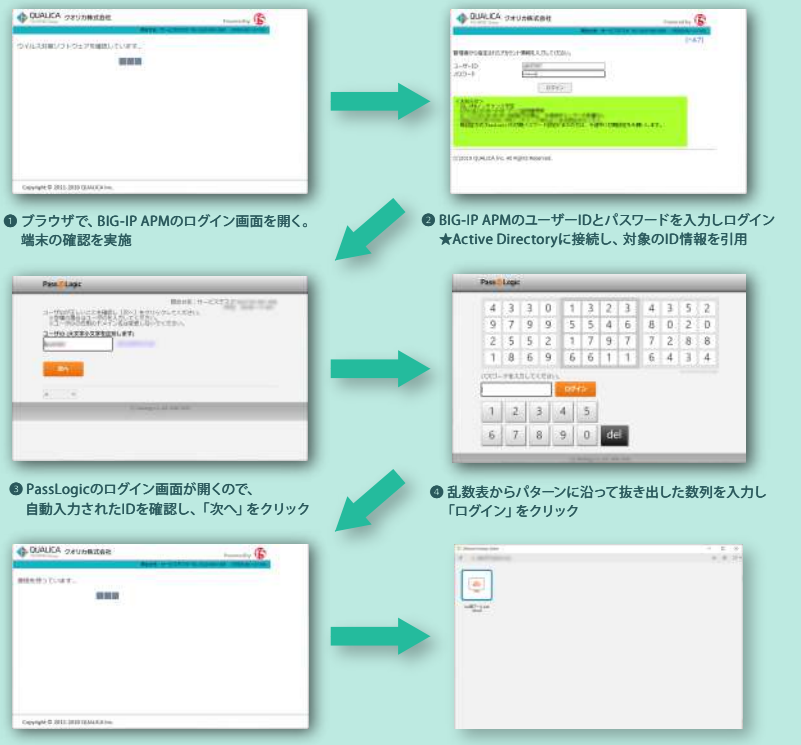
ログインの手順は、まず BIG-IP APM のクライアントを起動します。そして、ユーザー ID とパスワードを入力しログインします。ここではまだ VPN 接続は確立していません。連携している Active Directory に接続しつつ、PassLogicのログイン画面にリダイレクトします。この時に Active Directory から対象のユーザー ID 情報を引き出し、PassLogic ログイン画面に自動入力するようにしました。これにより入力の手間を削減し、誤入力によるお問合せを予防しています。

運用方針の変更にも対応できる豊富な機能

PassLogic は機能が豊富で、認証機能だけでも各ワンタイムパスワード認証機能やクライアント証明書認証機能などを、どのように適用するかを検討する必要がありました。そのために実際にテスト環境を構築し、機能を検証し、検討・選択する骨の折れる作業でした。

しかし、この作業を経て、機能を理解した現在では、会社のテレワーク運用やセキュリティ方針が変更になった場合でも、PassLogic なら対応できると考えています。

PassLogicを用いた BIG-IP APMへのログイン手順



❶ ブラウザで、BIG-IP APMのログイン画面を開く。端末の確認を実施

❷ BIG-IP APMのユーザーIDとパスワードを入力しログイン ★Active Directoryに接続し、対象のID情報を引用

❸ PassLogicのログイン画面が開くので、自動入力されたIDを確認し、「次へ」をクリック

❹ 乱数表からパターンに沿って抜き出した数列を入力し「ログイン」をクリック

❺ BIG-IP APMのログイン画面に自動的に遷移

❻ ログイン成功すると、VMware Horizonのクライアントがログイン状態で起動。利用するデスクトップを選択して利用開始

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

PassLogic 製品サイト
パスロジック 検索
passlogic.jp

お問い合わせ先