PassLogic 導入事例 キリン株式会社

「働き方改革」実現に向けた「BYOD」対応を推進！仮想デスクトップサービスの認証強化に「PassLogic」を導入

“あたらしい飲料文化をお客様と共に創り、人と社会に、もっと元気と潤いをひろげていく。”という理念のもと、総合飲料事業を手掛けるキリン社およびキリングループでは、社員がより働きやすくなるよう業務環境改善に取り組んでいます。その一環として、社外での業務が多い社員や、在宅勤務を実施する社員などが、社外から業務システムを利用できる「テレワーク環境」を運用しています。
以前はこのテレワーク環境の利用を会社支給端末からの接続に限定していましたが、このたび個人所有端末でも接続できるように利用範囲を広げる計画を実施。その接続の際の認証強化ソリューションとして「PassLogic」をご導入いただきました。
このテレワーク環境の概要と、PassLogic 採用理由とその効果について、キリン社の情報戦略部担当者様にお話を伺いました。

KIRIN

キリン株式会社 および国内キリングループ
Kirin Company, Limited

設立：2013年1月1日
従業員数：約15,000人 ※2017年5月時点
URL：http://www.kirin.co.jp/

導入の背景・課題

- ☐ 自分が使い慣れたパソコンを利用して業務をすること「BYOD」を可能とし、テレワーク環境利用者の拡大、及び、業務効率の向上を実現したい。

➔ そのためには、仮想デスクトップサービス利用時の認証強化が必須

導入後の改善効果

- ✔ 本人認証において「2要素認証」を実現し、セキュリティを強化
- ✔ 副次的に、事業継続計画「BCP」にも効果を発揮

「働き方改革」のために「BYOD」を導入

昨今、話題となっている「働き方改革」の実現はキリングループでも課題となっており、社外での業務が多い社員が外出先からでも業務が実施できたり、急に出社できなくなった社員が自宅で最低限の業務を実施できたりする等、多様な働き方を許容できる業務環境作りに積極的に取り組んでいます。
当グループでは仮想デスクトップサービス（VDI）とシンクライアント端末の導入を2014年に完了し、社外から業務システムに接続できる「テレワーク環境」を運用してまいりました。しかし、接続できるのは、あくまでも会社が支給したシンクライアント端末に限られておりました。
そこで、「働き方改革」により積極的に取り組むために、より多くの社員がテレワーク環境を利用できるよう、社員が所有する端末でも接続可能とする方針「BYOD」を導入することを決定いたしました。

VDIへの接続を認証強化

当グループでは、Citrix社のVDI「XenDesktop」を導入し、テレワーク環境を運用しています。社内ネットワーク上にある業務情報はVDI上でのみ運用され、持ち出し端末上には残らず、万が一、端末が紛失や盗難された場合でも、情報流出は発生しないようになっています。
今回の取り組みは、この既存のVDIへの接続をBYODに対応することです。より多くの社員を対象とし、各自の端末で利用するわけですから、「誰が」、「どの端末から」接続しているのかを、よりきちんと制御する必要があります。そこで、接続可能な端末を制限する「端末認証」と、利用できる人物を制限する「本人認証」の2つの面における認証強化の検討が行われました。
端末認証は、例えばネットカフェにある端末など、セキュリティ対策が行われておらず、ウイルス感染している恐れがある端末からの接続を防止するための対策です。この端末認証に対しては、クライアント証明書の発行・認証サービスを導入することで対応しました。
加えて、「なりすまし」による社員以外の接続を防止する本人認証については、通常のパスワード認証に加えて、ワンタイムパスワード（OTP）認証を追加することで認証強化を図りました。

本人認証に「PassLogic」を採用

OTP製品の選定にあたっては、国内での導入実績のある製品から候補を出し、比較を行いました。機能適合性、利用者負荷、運用性、サポート体制、コストの5つの観点から評価を行った結果、PassLogicが最も優れていると判断し導入を決めました。
今回の導入ではPassLogicのソフトウェアトークン型OTP認証機能を利用した導入になります。ユーザは、自分のスマートフォンにインストールしたスマートフォンアプリ「パスクリップL」でOTPを確認して、パスワードを入力するのですが、その時点のパスワードがアプリ上にそのまま表示されるので、ユーザがパスワードを忘れるという恐れはありません。実際、ユーザからの問合せ数は少なく、管理コストは抑えられています。
ユーザがスマートフォンを紛失した際も、そのスマートフォン上のパスクリップLのOTPを、管理者側で簡単に無効にすることができるのも決定要素となりました。
また、利用中のCitrix製品との連携検証が完了していたことや、国内製品であること、冗長化構成が持てることでBCP対応が可能であることも、安心して導入を進められる要因となりました。

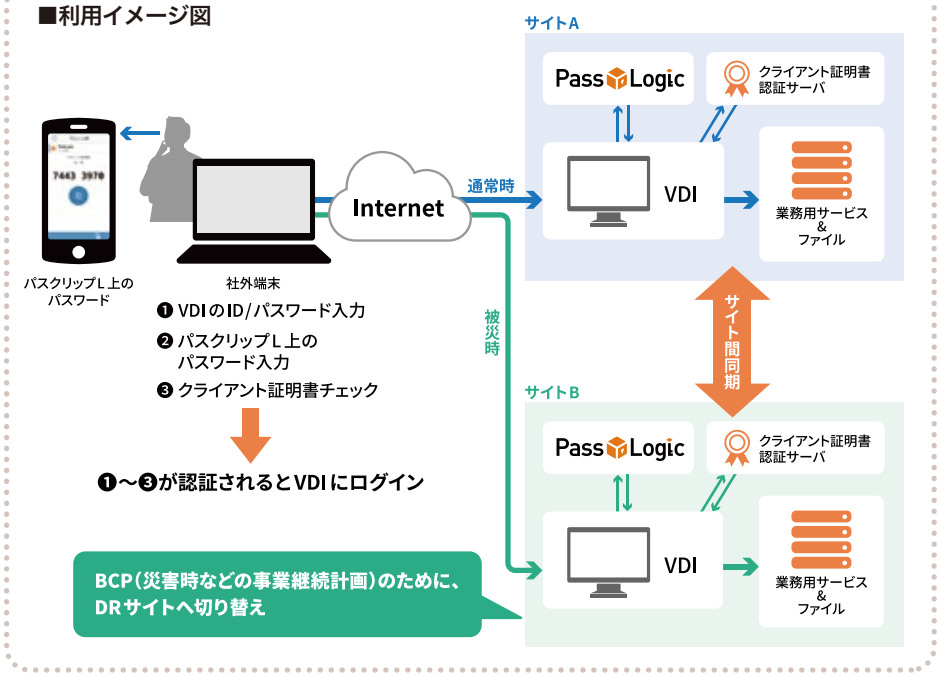
PassLogic 導入後の状況

本人認証に「パスワード+ソフトウェアトークン型OTP」による2要素認証を導入したことで、セキュリティ上の要件を満たし、テレワーク環境を利用できる社員の拡大を進めることができました。2016年12月に、本仕組みの利用を開始しています。

以前より会社支給端末ユーザが社外から接続する際には2要素認証が必要だったため、2要素認証によるセキュリティ強化の必要性と認証手順は、社内で認識されていたように感じます。ですので、今回本仕組みを利用する社員に抵抗感なく、スムーズに導入できました。今後も対象社員を増やし、働きやすい職場作りを支援し、働き方改革を実現していきます。

また、BYOD導入は、事業継続計画「BCP」にも寄与できたと考えています。災害時に「被災地に不足している飲料を届けること」と「被災地以外の地域へ通常通りに飲料を届けること」は当グループの課題です。パスロジサーバにおいても、BCPの一環として、拠点を複数設置する冗長化を行い、被災時でも継続稼働できる環境を整えました。そして今回の取り組みにより、災害時でも、できるだけ多くの社員が業務を遂行するための準備ができたのではないかと考えています。

■利用イメージ図



PassLogic のソフトウェアトークン型 OTP 認証機能について

PassLogic と連携するスマートフォン用アプリ「パスクリップ L（iOS/Android・無償）」に表示された OTP を入力して認証します。

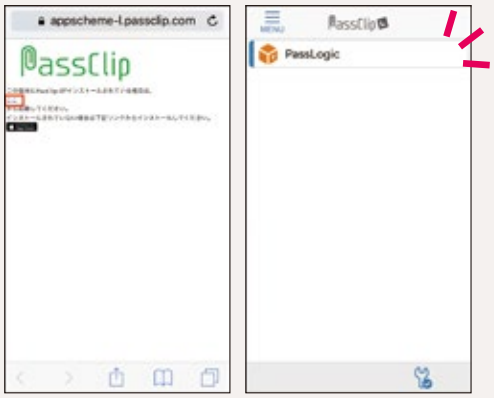
■利用開始手順

❶ App Store/Google Playから「パスクリップL」をダウンロード&インストール

❷管理者から送信される利用開始メール内のリンクをタップ

❸ブラウザ上に表示される連携画面でリンクをタップ

❹ パスクリップ L上に「PassLogic」スロットが出現し、連携完了



■認証手順

❶スマートフォン上の「パスクリップL」を起動し、「PassLogic」スロットをタップ

❷表示されるOTPを確認
※管理者側で設定した時間で変更

❸ 認証するシステム / サービスの認証画面に、ID&パスワードと、確認した OTP を入力

接続成功／失敗

■ビンゴ型表示

パスワードとなる文字列を５×５のマスの中に表示することで、抜き出し位置を知らない他人にはパスワードを読み取れなくする表示方法です。より強固な認証を求める場合に管理者側で設定し、採用することができます。

※キリン様は、通常の表示方法「ベーシック型表示」にて運用されています。

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