多要素認証のROI

100人中4人から6人が、脆弱なパスワードを使用したりパスワードを共有したりしています。
該当する従業員が、あなたの職場にもいませんか?

たった1つのパスワードが盗まれるだけでネットワーク全体に危険が及びます。そこで、パスワードの管理に問題がある従業員が社内に1人以上いる可能性について検討する必要があります。さらに注意すべき事は、不正アクセスに関連するコストは、直接的な罰金、調査および修復のための費用だけでなく、顧客の喪失や従業員の生産性低下による間接的なコストによって、数百万ドルに及ぶ可能性があるという点です。以下の統計は、リスクを定量化し、予想されるMFA(多要素認証)ソリューションのコストと比較するのに役立ちます。

データへの不正アクセスのリスク/コスト

9,350
不正アクセスされたレコードの平均数

不正アクセスによって**盗まれたデータ**の数は平均で**9,350レコード**
2017 Ponemon State of SMB Cybersecurity Report

1億4千万円
不正アクセスされたレコードの平均コスト

データへの不正アクセスの平均コスト=
機密情報を含む1レコードあたり**約1万5千円**
2017 Ponemon Institute Cost of Data Breach Study

81%
脆弱な盗まれたパスワードによって実行された不正アクセスの割合

ハッカーが使用する**最も一般的な戦略**です
Verizon Data Breach Investigations Report 2017

3%
123456というパスワードを使用したユーザ数(100人中)

10%の人が今年のワースト25パスワードリスト内にあるパスワードを1つ以上使用し、
約3%の人が最悪のパスワードである**123456**を使用しています
Http://fortune.com/2017/12/19/the-25-most-used-hackable-passwords-2017-star-wars-freedom/

6%
すべてのオンラインログインで同じパスワードを使用するユーザ数(100人中)

2017年、すべてのアカウントで**同じパスワード**を使い回しした
米国のインターネットユーザは100人中6%
(https://www.statista.com/statistics/763091/us-use-of-same-online-passwords/)

1
MFAなしでネットワークに侵入するために必要な紛失/盗難パスワードの数

ダークウェブ上で確認した、ハッキングまたは漏えいしたパスワードファイルは**14億**
"ハッカーがいつでも「Credential Stuffing」アプリを使用して侵入できる状態になっている"
(Forbes誌、2017年12月11日)

クラウドベースMFAソリューションへの投資

0円
認証管理をホストする追加の基盤環境

追加費用なしでクラウド環境を利用し、すべての管理が可能
一部の機能を利用するには、ゲートウェイ上のソフトウェアとエージェントが必要

0円
ハードウェアトークンの導入コスト

無料のモバイルアプリで**スマートフォン**を認証します。追加のハードウェアは不要

約29万円
従業員100人あたりのMFAサービスの年間推定コスト

190円/ユーザ/月を前提としています(参考価格)。
AuthPointの価格については、WatchGuard販売店にお問い合わせください

最小
ITスタッフの費用

トークンの導入は**自動化されるため**、IT管理者の業務は主にメンテナンスと監視です

クラウドベースMFAの導入メリットはコストをはるかに上回ります

1ユーザあたり1か月わずか約190円(参考価格)を投資するだけで、盗難パスワードによる不正アクセスの可能性を減らすことができます。クラウドベースのMFAは、追加のインフラストラクチャ、ハードウェアトークン、ソフトウェアサポート、およびメンテナンスのための費用は必要ありません。

WatchGuard AuthPoint

AuthPointは、使いやすいクラウドプラットフォーム上での多要素認証(MFA)を提供します。AuthPointモバイルアプリは試行されるすべてのログインを可視化します。クラウドサービスなので、デプロイするハードウェアはありません。どこからでも管理でき、一般的なクラウドアプリケーション、ウェブサービス、VPN、ネットワークなどのサードパーティアプリケーションとの統合が可能です。
詳細はwww.watchguard.co.jp/authpointをご確認ください。

WatchGuard®