



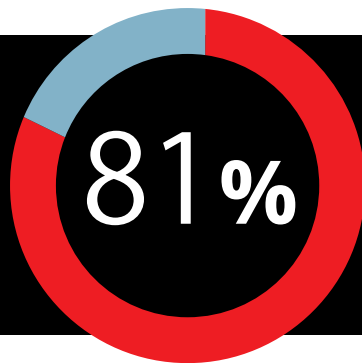
パスワード管理の問題と 多要素認証による解決

はじめに

パスワードセキュリティは、今日の情報セキュリティが直面している最も重要な問題の1つです。2017 Verizon Data Breach Reportによると、情報漏えいの81%はパスワードの脆弱さや盗難がきっかけで発生しています。これらの問題を解決するため、多くの組織が多要素認証(MFA)テクノロジーを採用して多層型アプローチを導入し、情報へのアクセスにあたってパスワードが果たす役割を軽減しようとしています。

多要素認証とは、本人確認のために2つ以上の認証要素の提示をユーザに要求する認証方法のことであり、ユーザが把握している情報(パスワードや暗証番号など)、所持しているもの(ハードウェアトークンやスマートフォンなど)、あるいはユーザの生体認証(指紋スキャンなど)が認証要素として使用されます。簡単な例として、たとえばATMの場合であれば、ログオン時にキャッシュカード(所持するもの)を挿入し、暗証番号(把握している情報)を入力するようユーザに要求します。

しかしながら、従来からあるMFAソリューションの多くに、特にITリソースが不足している企業にとっては導入・運用管理が困難であるという問題があります。パスワードセキュリティとMFAの利用状況を理解するため、米国、英国、オーストラリアの、従業員数が1,000名未満の企業のビジネスオーナーとIT責任者を対象に独自調査を実施しました。この調査の主な結果を以下にご紹介します。



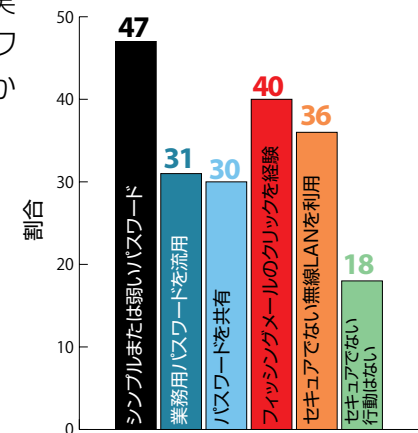
攻撃者による情報漏えいの81%は、
脆弱、または搾取されたパスワードによって発生

パスワードセキュリティの現状

脆弱なパスワードは深刻な問題であり、今回の調査でも、企業のビジネスオーナーとIT責任者の83%が、強固なパスワードと管理の重要性を従業員が認識していると回答しました。多くのビジネスオーナーが、パスワードセキュリティの必要性を従業員が認識していると回答しているにもかかわらず、企業、従業員、顧客情報の保護をパスワードだけに頼っていることについて、大きな不安を抱いています。84%の回答者が、サイバー攻撃の60%は脆弱なパスワードがきっかけで発生していると考えていますが、実際にはこの割合も前述のベライゾンの報告書のデータと比べると低い数字です。

以上のことから、パスワードのベストプラクティスとセキュリティに対する認識は広まっているにもかかわらず、その認識が実際の行動に移されていないことがわかります。回答者の半数近く(46%)が、強力なパスワードを常に使用するよう従業員に強制することはできないと考えています。調査対象の企業のほとんどが、何らかの形でパスワードセキュリティに関するトレーニングを実施したりポリシーを設けたりすることで、ベストプラクティスを奨励しています。これには、長い複雑なパスワードを使用することや、パスワードを定期的に変更するよう従業員に義務付けることなどが含まれます。しかしながら、以下の結果から判るように、実際には正しくないパスワードの使い方をしている従業員も多いのが現状です。

- 47%の回答者が、自社の従業員はシンプルまたは弱いパスワードを使っていると考えている
- 31%が、従業員は業務用パスワードを個人用アプリケーションにも使っていると考えている
- 30%が、従業員は同じパスワードをあちこちで使い回していると考えている
- 40%が、従業員はフィッシングメールをクリックすると疑っている
- 36%が、従業員はセキュアではない無線LANを使用していると考えている
- 18%が、従業員によるセキュリティを脅かすリスクの高い振舞いはないと考えている



従業員のパスワードプラクティス管理統計

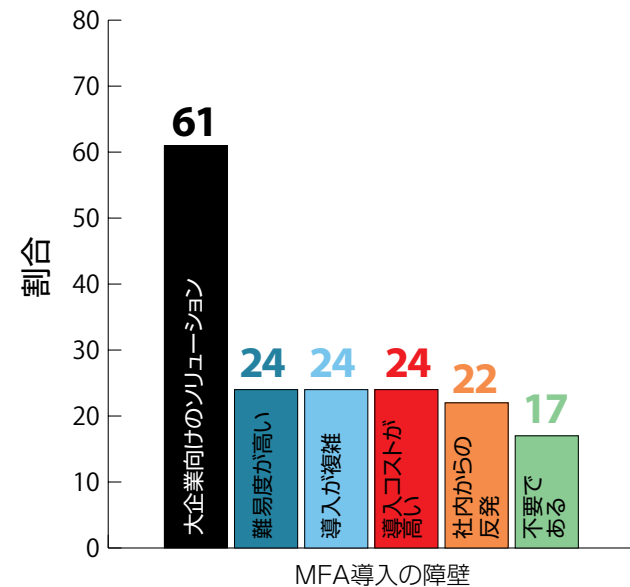
これらの問題を解決する手段として、従業員数が1,000名未満の企業のIT責任者の84%が、パスワードに関するポリシーの実行よりも、強力なパスワードを強制するテクノロジーの導入に前向きであることがわかった。

MFA導入の課題

IT責任者がMFAソリューションの導入に肯定的であり、パスワードのベストプラクティスに従わない従業員も多いと考えているのであれば、何がMFAソリューションの導入の障壁になっているのでしょうか。

調査から判明した、IT責任者のMFAについての考え:

- 61% : MFAソリューションは**大企業のみを対象**とした製品
- 24% : MFAは**保守と運用サポートが困難**
- 24% : MFAは**実装が複雑**すぎる
- 24% : MFAソリューションの**導入コストは高価**
- 22% : MFAに対する抵抗が**社内から**ある
- 17% : MFAソリューションは**不要**



これらはいずれも妥当な意見であると言えます(最後の回答については妥当とは言えません。我々の調査研究によって企業の規模に関係なくMFAが必要であることがわかっています)。ITリソースが限られている企業は、予算の範囲内で購入でき、導入とサポートが容易なMFAソリューションを必要としています。

MFAはどの程度普及しているのか？

MFAを未導入の企業の中で、83%は関心があると回答し、65%は今後導入する予定があると回答したことから、従業員数1,000名未満の企業においても、MFAソリューションの導入が大きな関心事であることがわかりました。調査対象企業の67%で、少なくとも一部のユーザが何らかの形のMFAを現在使用していますが、29%は、MFAを使用していないと回答しました。たった1人の従業員の行動が企業のデータ漏えいにつながることを考えれば、29%という割合は、かなり大きな数字です。また、67%という数字にも実態を掴みきれないところがあるため、さらに詳しいデータを見てみることにしましょう。

MFAを導入済みの企業に関して、以下の事実が明らかに：

- 56%：デスクトップでの認証を使用している
- 47%：SMSを使用している
- 44%：モバイルトークンを使用している
- 40%：使用している種類が不明
- 61%：クラウドベースの認証サーバを使用している



MFAが多くの企業で使用されているのは良い傾向ですが、MFAであればどれも同じというわけではありません。企業が高度なセキュリティ技術を持たないMFAソリューションを採用した場合、さらなるリスクに直面する恐れがあります。たとえば、SMSメッセージが使用されている場合、攻撃者に偽造されたり傍受されたりする可能性があるため、安全であるとは言えません。ハードウェアトークンの場合は、トークンの紛失や盗難によってセキュリティリスクの問題があります。

まとめ

MFAが大企業だけのソリューションである時代は終わりました。調査結果から、従業員数が1,000名未満の企業のIT責任者の半数以上がパスワードに関する何らかのポリシーを設けたり、トレーニングを実施したりいること、また、4分の3が従業員のセキュリティに対する認識が不十分であると考えていることがわかりました。そして、ほぼすべての回答者が、ポリシーやトレーニングに加え、強力なパスワードが要求される技術がより有効な手段であると考えています。

低コストで、導入・管理が容易であり、ビジネスオーナーやIT責任者にとって、従来の導入の障壁と考えられてきた課題が解消されるMFAが鍵となっています。最新のMFAは、単なるオプションの1つではなく、すべての企業のビジネスに不可欠な要素となりました。



調査の詳細:

本調査は、ウォッチガードの依頼によりCITE Researchにより実施されたもので、その回答者は、米国、英国、オーストラリアの、従業員数が1,000名未満の中小企業650社のビジネスオーナーとIT責任者です。本調査は2018年4月と5月に実施されました。



ウォッチガードのセキュリティポートフォリオ



ネットワークセキュリティ

ウォッチガードのセキュリティプラットフォームは、強固なエンタープライズグレードのセキュリティと、導入、運用・管理、保守の容易さを両立させ、中堅・中小企業、分散拠点を持つ大企業などすべての企業に最適なソリューションです。



セキュアWi-Fi

セキュアWi-Fiは、安全に保護された無線LAN環境を提供し、管理者の運用負荷の軽減やコスト削減を同時に可能にする変革的な無線LANソリューションです。豊富なエンゲージメントツールとビジュアル化された可視性の高いビジネス分析により、ユーザのビジネス成功に貢献します。



多要素認証

AuthPoint™は、情報漏えいリスクに繋がるパスワードだけのセキュリティの課題を解決するソリューションです。クラウドベースの使いやすいプラットフォームで強固な認証を実現します。ウォッチガード独自の「モバイルデバイスDNA」を認証要素として追加することで、正規のユーザのみに重要なネットワークやクラウドアプリケーションへのアクセスを許可する事が可能となります。

本書の内容は、明示的または暗黙的ないかなる保証をするものではありません。本書に記載されているすべての仕様は、変更される可能性があり、また、本書に記載されている将来的に提供される製品、特性、または機能の実現性と時期は、いずれも見込みに基づくものです。©2018 WatchGuard Technologies, Inc. All rights reserved. WatchGuard, WatchGuard のロゴ、および AuthPoint は、米国またはその他の国、あるいはその両方における WatchGuard Technologies, Inc. の商標または登録商標です。その他のすべての商標は、その所有者の資産です。文書番号: WGCE67114_072518_JP