リスク評価
多要素認証（MFA）セキュリティ

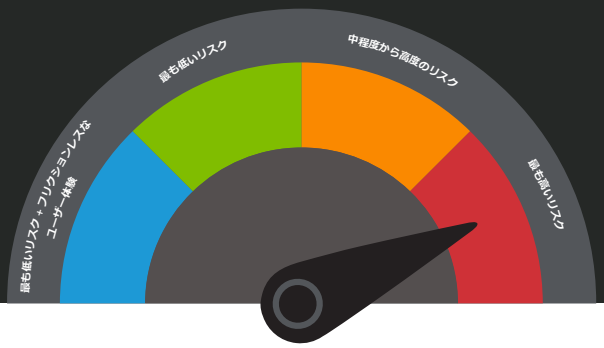
今日の認証ソリューションのリスクの規模を把握する

ハッキングに関連するあらゆるデータ漏えいのうち 80% は、ユーザーの認証情報の盗難や安全性の低いパスワードに起因し[1]、6 億 1,300 万個以上のパスワードがデータ漏えいによって流出しています。[2] ログインセキュリティ層として多要素認証（MFA）を追加することで、リスクを大幅に軽減できますが、従来の MFA ソリューションのほとんどはまだ比較的簡単に侵害される可能性が残っています。

貴社の認証セキュリティはどの程度成熟していますか？現在の認証モデルのリスクを把握することが重要です。

最も高いリスク

ユーザー名とパスワードでの認証



セキュリティ認証において認証情報の強度のみに依存する組織は、攻撃に対して非常に脆弱です。ユーザー名とパスワードは、以前にも増して安全性が低くなっています。ログイン情報は、モチベーションの高い攻撃者によって盗難、ハッキング、収集され、すぐに収益化（ダークウェブで使用または販売）されます。

攻撃者は、以下の手法によりユーザー名とパスワードを回避します。

- Credential Stuffing
- **フィッシング**
- **パスワードスプレー**
- **ブルートフォース**
- **事前データ漏えい／パスワードの再利用**
- **パスワードのリセット**
- **キーストロークロギング**
- **ローカル検出**

また、ユーザーは複数のサイトでパスワードを繰り返し使用する傾向があるため、エンタープライズのセキュリティはさらなる脅威にさらされています。つまり、ユーザーの個人アカウントのセキュリティが低ければ、その程度のセキュリティしか確保できないということです。アルゴリズムによって生成された最も複雑なパスワードであっても脆弱性が伴うため、MFA が必須であることは明らかです。つまり、単一のセキュリティレベル（この場合は単要素認証）を使用することはお勧めできません。クラス最高のセキュリティには、必ず複数の防御層が設定されています。

中程度から高度のリスク

標準の多要素認証（MFA）

認証セキュリティスタックに MFA 機能を追加することで、エンタープライズセキュリティは瞬く間に向上します。2 要素認証（2FA）を始めとする MFA では、ユーザー確認に個別の認証要素を 2 つ以上使用します。最初の要素は通常、パスワードです。2 番目（場合によっては 3 番目）の要素には、PIN やセキュリティの質問などのユーザーが知っている情報、デバイスや 1 回限りのコード／パスワード、ハードウェア／ソフトウェアトークンなどのユーザーが持っているもの、指紋や Face ID などの生体認証や場所などのコンテキスト信号を始めとするユーザー自身を表すものを使用できます。

従来の MFA では、単一要素のユーザー名／パスワード認証と比較してリスクが大幅に軽減されますが、次のような認証セキュリティを回避するさまざまな手法に対してはいまだに脆弱です。

- **フィッシング**
- **透過型プロキシ（中間者（MITM：man-in-the-middle）攻撃）の使用**
- **電子メールまたは SMS による認証コードの傍受**
- Credential Stuffing
- **リプレイ攻撃**
- **SIM スワップ**
- **ソーシャルエンジニアリング**
- **MFA 操作を処理するオンラインページの脆弱性**

多要素認証を回避する攻撃者の例が数多くの文書に記録されています。その 1 つが、2020 年に大きな注目を集めたセキュリティ侵害です。このセキュリティ侵害は、ソーシャルエンジニアリングとフィッシングを組み合わせて MFA ソリューションを回避することで実行されましたが、物理的なセキュリティキーを使用していれば避けることができたかもしれません。

最も低いリスク

物理的なセキュリティキーを使用した FIDO2 MFA

FIDO2 は、利用可能な標準ベースの認証方法の中で最も強力なものであり、従来の MFA のセキュリティ上の脆弱性を解決し、フィッシング、MITM、リプレイ攻撃のリスクを排除します。FIDO2 標準は、World Wide Web Consortium の Web Authentication 仕様と、FIDO Alliance の対応する Client to Authenticator Protocol で構成されています。この認証モデルは、未来の MFA、すなわちユーザーのデバイスから離れず、サーバーに保存されることもない暗号化ログイン識別情報を介して行われる認証を実現します。また、FIDO2 により、最終的には、まったくパスワードを使用しない認証へと進化できます。

FIDO2 MFA の欠点は、すべてのユーザーが認証要素として使用できる物理的なセキュリティキーを購入しなければならない点です。

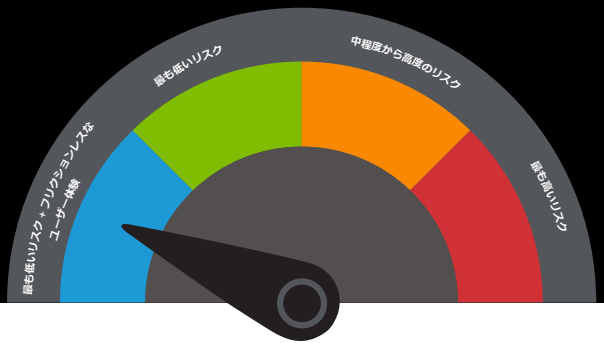
FIDO2 は最も安全な標準ですが、ハードウェアセキュリティキーを使用した実装では、次のような多くの課題が発生する可能性があります。

- **各ユーザーのキーの購入と保守にかかるコスト**
- **キーの配布と管理の複雑さ**
- **紛失したハードウェアキーの交換**
- **ハードウェアキーの更新またはパッチ適用ができない**
- **不均一な配布 - 一部の従業員のみがキーを入手**

従業員全員分の物理ハードウェアキーを購入、構成、発行、管理するためにはコストと時間がかかります。さらに、ログインごとに物理キーをデバイスに差し込む必要があるため、ユーザー体験が煩雑になり、生産性が低下します。

最も低いリスク + フリクションレスなユーザー体験

エッジの次世代 MFA



Akamai MFA は、暗号化によってセキュリティが確保され、フィッシングに対応した認証要素を備えた次世代の FIDO2 ソリューションです。このサービスでは、物理的なセキュリティキーの代わりにスマートフォンアプリケーションを活用するため、エンタープライズにとって FIDO2 MFA 実装の実現を妨げてきた課題が解決されます。また、既存のスマートフォンを使用して迅速かつ簡単に導入でき、フリクションレス（スムーズ）なユーザー体験で最高レベルの認証セキュリティを実現できます。Akamai MFA により、フィッシングのリスクを排除し、最終的には、まったくパスワードを使用しない未来の認証へと進化できます。

Akamai MFA の詳細をご覧の上、ぜひ 60 日間の無料トライアルをお試しください：**akamai.com/mfa**

出典：

1. https://www.infosecurity-magazine.com/blogs/pwned-passwords-business-risk/
2. https://haveibeenpwned.com/Passwords

Akamai は世界中の企業に安全で快適なデジタル体験を提供しています。Akamai のインテリジェントなエッジプラットフォームは、企業のデータセンターからクラウドプロバイダーのデータセンターまで広範に網羅し、企業とそのビジネスを高速、スマート、そしてセキュアなものにします。マルチクラウドアーキテクチャの力を拡大させる、俊敏性に優れたソリューションを活用して競争優位を確立するため、世界中のトップブランドが Akamai を利用しています。Akamai は、意思決定、アプリケーション、体験を、ユーザーの最も近くで提供すると同時に、攻撃や脅威は遠ざけます。また、エッジセキュリティ、Web ／モバイルパフォーマンス、エンタープライズアクセス、ビデオデリバリーによって構成される Akamai のソリューションポートフォリオは、比類のないカスタマーサービスと分析、365 日 /24 時間体制のモニタリングによって支えられています。世界中のトップブランドが Akamai を信頼する理由について、www.akamai.com、blogs.akamai.com および Twitter の @Akamai で紹介しています。全事業所の連絡先情報は、www.akamai.com/locations をご覧ください。公開日：2021 年 3 月。