Akamai

ホワイトペーパー

MFAの現状 – セキュリティの幻想か

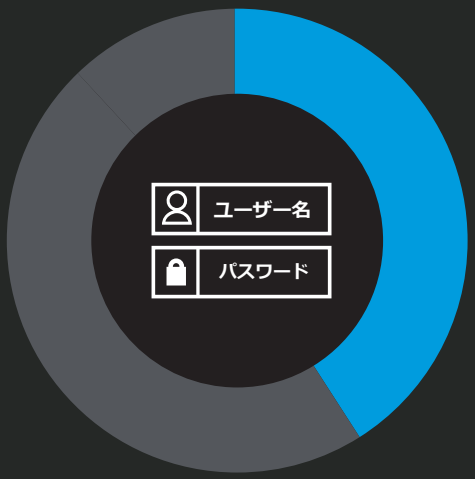
ユーザー名とパスワードでは不十分

セキュリティ侵害の 80% は、認証情報の不正取得が関係しています。[1]安全性の低いパスワードが原因になっている場合もありますが、アルゴリズムで作成された複雑で解読不能なパスワードでさえ問題になることがあります。[2]最近実施された、あるダークウェブ監査では、10 万件の侵害から 150 億件のログイン情報が盗まれていたことが判明しました。[3]

デジタル接続の必要性、クラウドサービスへの依存、ハイブリッド環境の現実は、パスワードへの依存と相まって、ユーザーを以下のような無数の認証攻撃ベクトルに対して脆弱な状態に曝しています。

- Credential Stuffing
- **パスワードスプレー攻撃などの総当たり攻撃のメカニズム**
- Local Discovery **とインサイダーの取り組み**
- **フィッシングとソーシャルエンジニアリング**
- **キーストロークロギング**
- **悪性プロキシおよび返信キャンペーン**

状況は世界的なパンデミックにより悪化しており、デバイスや場所に依存しない安全なアクセスの必要性が浮き彫りになっています。認証情報関連の侵害がすべて、ユーザー認証後に発生していることを考えると、パスワードが正確な認証タスクとして適合していないことは明らかです。



このような脆弱性が知られているにも関わらず、組織の 41% は、いまだにユーザー名とパスワードが最も効果的なアクセス管理ツールの 1 つだと考えています。[4]

500%

Akamai は、フィッシング、ソーシャルエンジニアリング、Credential Stuffing、総当たり攻撃が増加していることを発見しました。2020 年 3 月から 5 月の期間、マルウェアが約 500% 増加しています。

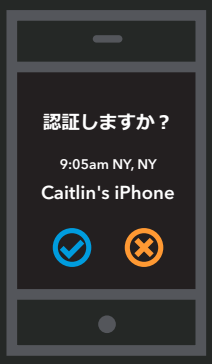
多要素認証の利点

多要素認証（MFA）技術の人気が着実に高まっているのは当然の流れです。簡単に言えば、MFA は、アクセスを許可する前に、複数の検証ソースを使ってアイデンティティを確認して、エンタープライズを保護します。

MFA では、以下の 3 つの認証情報のうち 2 つ以上を正しく組み合わせる必要があります。

ユーザーが持っている情報

知識ベースの認証です。パスワードや PIN、セキュリティ質問への回答のほか、ピクトグラフも含まれます。



ユーザーが持っているモノ

トークンベースの認証であり、ハードとソフトが含まれます。これには、スマートカードやキーフォブ、ワンタイムパスワード、プッシュ通知、携帯機器に送信される SMS コードなどがあります。

ユーザー自身

コンテキスト認証または生体認証ベースの認証です。これには、ふるまい、位置信号または時間、指紋、顔認識、音声または音声パターン、署名などがあります。

MFA ソリューションを実装すると、不正アクセスやシステム侵入のリスクが大幅に減少します。事実、MFA を採用している組織は、そうでない組織よりも侵害の確率が 99.9% 低減されています。[5]MFA は、クラウド、オンプレミス、Web ベース、SaaS、IaaS アプリケーションなど、すべての環境で安全なアクセスを実現し、効率化する効果があるのです。MFA ソリューションは、エンタープライズセキュリティをゼロトラストや SASE などのフレームワークに移行する際の重要なコンポーネントでもあります。

ユーザー名とパスワード以外を要求し、サインオン体験に組み合わせ、他のクラウドネイティブなセキュリティツールと統合することで、MFA テクノロジーはユーザーの生産性とユーザビリティの向上に役立つ可能性があります。さらに、一元管理された認証は、コンプライアンスに関する多くの懸念や要件にも対応します。

思うほど安全ではない従来の MFA

標準的なプッシュ上に構築されている MFA サービスは、ハッカーが簡単に操作して、アカウントを乗っ取ることができます。追加のセキュリティで強化されていない限り、現時点の MFA テクノロジーには危険が残ります。

MFA は境界セキュリティの一形態ですが、クラウドと現在の働き方に境界はありません。MFA は、ログインに関係のない攻撃を阻止するように設計されていません。ユーザーがシステムにアクセスしようとしている際に、境界でのサインオンのセキュリティが確保されるにすぎません。サイバー犯罪者は、この現実を回避するために、比較的単純ながら非常に効果的なソーシャルエンジニアリングおよびフィッシングメカニズムを開発してきました。

このようなシナリオを考えてみてください。

1. **何らかの形でソーシャルエンジニアリングが実施された後、従業員は攻撃者が設定した偽の（フィッシング）サイトに正しいユーザー名とパスワードを入力します。**
2. **認証情報を取得すると、攻撃者は実際のログインポータルにその情報を入力します。**
3. **すると、従業員の電話にプッシュ通知が送信されます。**
4. **従業員は、通常のログイン過程でプッシュ通知を受け入れます。**
5. **これで、攻撃者は 2 つの形式の検証を完了し、アクセスを許可されました。**

これは、標準的なプッシュ通知のセキュリティ上の重大な弱点です。盗んだ認証情報を手に入れた攻撃者は、プッシュ通知を従業員の電話に送信することができます。セキュリティ侵害と通常のビジネスを分ける唯一のものは、合法的なプッシュと詐欺を見分ける従業員の能力です。攻撃者は、従業員数千人のうち一度侵入に成功すれば十分です。

フィッシング対応の MFA

真に安全な MFA ソリューションには、FIDO2 標準が採用されています。最も基本的なレベルで、ユーザーの決定に依存するのではなく、テクノロジーによってセキュリティが確保されます。

これはどのようにして実現できるのでしょうか？FIDO2 標準には、フィッシングを防止するいくつかの技術が採用されています。

まず、認証要求（MFA チャレンジ）は、常にアクセス要求が発生したワークステーションに送信されます。そのワークステーションのブラウザーは、ローカルに接続されている任意のセキュリティキーに認証要求を送信します。上記のシナリオに以下が適用されます。攻撃者が MFA サービスを取得して、従業員の電話にプッシュ通知を送信する代わりに、MFA チャレンジが攻撃者のワークステーションに戻ります。攻撃者は従業員のセキュリティキーを持っていないため、応答できません。これでアカウントの乗っ取りは防止されます。

定義：認証標準と仕様

Fast IDentity Online（FIDO）Alliance

認証標準の開発、使用、遵守を使命とする団体です。

FIDO2

FIDO Alliance の最新の認証仕様全体を表す用語。これには CTAP1、CTAP2、WebAuthn などが含まれています。FIDO2 を使用すると、一般的なデバイスを活用して、モバイル環境とデスクトップ環境の両方でオンラインサービスに簡単に認証を実施できます。

WebAuthn

World Wide Web Consortium（W3C）が発表した Web 標準の 1 つであり、FIDO2 の中核コンポーネントです。プロジェクトの目的は、公開鍵暗号を使用して Web ベースのアプリケーションやサービスへのユーザー認証インターフェースを標準化することです。

Client to Authenticator Protocol（CTAP）

ローミング認証システム（スマートフォンなど）と内部認証システム（クライアントまたはプラットフォーム）間のセキュアな通信を可能にする、FIDO Alliance によって開発された仕様。

次に、ブラウザーから認証要求とともにセキュリティキーにデータが送られます。ブラウザーに表示されるように、このデータには認証要求を送信した送信元のドメイン名が含まれます。攻撃者が、受け取った認証要求を単に従業員のワークステーションに転送した場合、このデータにはフィッシングサイトのドメイン名が含まれます。セキュリティキーは、最初に登録されたサイトのドメイン名と認証を要求するドメイン名との不一致を認識し、応答を拒否します。ここでも、攻撃が阻止されます。

より安全性が高く、フィッシング対応の MFA が可能ならば、それが広く普及していないのはなぜでしょうか？それは、物理的なセキュリティキーが必要であり、コストと手間がかかるからです。少なくとも従来はそうでした。

エッジの次世代 MFA

これまで、IT が MFA テクノロジーを評価、実装する際には、トレードオフを覚悟しなければなりませんでした。最高のセキュリティを確保するためには、ハードウェアの展開、全従業員分の物理的なセキュリティキーの購入、キーすべての配布と運用の管理など、現在よりも多くのコストをかける必要があります。また IT は、キーがもたらす理想的とは言えない体験、つまり追加ハードウェアの使用と継続追跡の必要性、にユーザーが適応できるように図る必要があります。

あるいは、セキュリティ面で劣るものの、従業員のスマートフォンにプッシュ通知を送信するという追加コストが不要で便利な方法もあります。比較的簡便なので、プッシュ MFA は現在広く利用されています。また、多くの企業がデータ漏えいのリスクを抱えているのもその理由です。

しかし、コストや導入の容易さのために、セキュリティを犠牲にする必要はありません。

Akamai MFA サービスには、新しい認証要素が導入されています。FIDO2 のセキュリティをスマートフォンと Web ブラウザーだけでデジタル化し、プッシュ通知の簡単で使い慣れた体験と組み合わせると、あらゆるプラットフォームでローミング認証システムとして使用できます。物理的なセキュリティキーは不要です。このソリューションは、FIDO2 標準の最も安全な機能を低コストで提供するとともに、インストールと消費が容易で、一般的なアイデンティティプロバイダーとの相互運用性も備えています。

Akamai MFA は、フィッシング、Credential Stuffing、アカウントの乗っ取りから組織を保護します。Akamai の一番最初の MFA テクノロジーを、真に安全でパスワードレスな未来への備えに、お役立てください。

詳細は akamai.com/mfa をご覧ください。

出典：

1. https://enterprise.verizon.com/resources/reports/dbir/
2. https://www.infosecurity-magazine.com/opinions/problem-password-everything-1/
3. https://www.forbes.com/sites/daveywinder/2020/07/08/new-dark-web-audit-reveals-15-billion-stolen-logins-from-100000-breaches-passwords-hackers-cybercrime/?sh=27fa6368180f
4. https://www.businesswire.com/news/home/20200616005047/en/Weakest-Link-Prevails-Overreliance-Passwords-Continues-Compromise
5. https://www.hipaajournal.com/multi-factor-authentication-blocks-99-9-of-automated-cyberattacks/