ホワイトペーパー

MFA（多要素認証）導入ガイド

2023 年 1 月

目次

はじめに：サイバー攻撃が激化する中で守りを固める

高度なサイバー攻撃が増加の一途をたどり、その大部分を占めているのが認証情報を利用する攻撃です。最近の報告によると、組織に対するメール攻撃は 2022 年上半期に 48% 増加しました。直前の半年と比較して、攻撃の 3 分の 2 以上がクレデンシャルフィッシング（悪意のあるリンクを含むメールを使用した機密アカウント情報の窃取）の試みでした。こうした攻撃で、なりすましが実行されたブランドの数は 265 に上ります。

攻撃者は、リモートワークへの移行が進んでいる状況に付け入り、フィッシングなどのソーシャルエンジニアリングの手口を強化したり、データ侵害を利用してアカウント乗っ取りを実行したりしています。その結果、確実な本人確認のための主たる手法として、多要素認証（MFA）の採用が急速に拡大しました。リモートワークやハイブリッドワークの拡大に対応しなければならない現代の組織は、MFA を利用することで、コンシューマー / 企業向けの Web アプリやモバイルアプリを含むすべてのリソースへのアクセスを保護できます。最新のセキュリティ態勢は、「決して信用せず、常に検証する」というゼロトラストの原則に基づきます。政府や規制機関、そして企業は、こうしたセキュリティ態勢の確立において MFA が重要な役割を果たしていることを理解するようになっています。

今日、アイデンティティ第一のアプローチをとる強固なセキュリティ戦略で、MFA は不可欠な要素となっています。一例として、2022 年 1 月に米大統領府行政管理予算局が公布した大統領令では、連邦政府機関全体でサイバーセキュリティを近代化するための基本

要件の 1 つとして、フィッシング耐性のある MFA が定められました。政府、企業、サイバー犯罪者の活動が進化する中、パスワードレス認証の台頭や、セキュリティ態勢の評価における管理 / 非管理デバイスの重要性の高まりなど、MFA の性質も変化しています。

本書は、パスワードレス認証へのアップグレードを含め、MFA の有用性を十分に活用するためのベストプラクティスを提供することを目的としています。Okta が IDG との提携により実施した調査の結果には、現代の認証とセキュリティにおいてアイデンティティおよびアクセス管理（IAM）が果たす強力な役割が実証され、IT / セキュリティ部門のリーダー全般に見られる最新の優先事項と採用のトレンドが明確に示されています。また、MFA ソリューションを設計する際に考慮すべき以下のような重要な要素についても、わかりやすく解説します。

- フィッシング耐性の実装
- ポリシーと規制の理解
- アクセスのニーズの変化に関する考慮事項

最後に、Okta のエンジニアリングチームや製品チームと共同での観察に基づいて、アプリケーションに MFA を構築するための実践的なアドバイスを提供します。

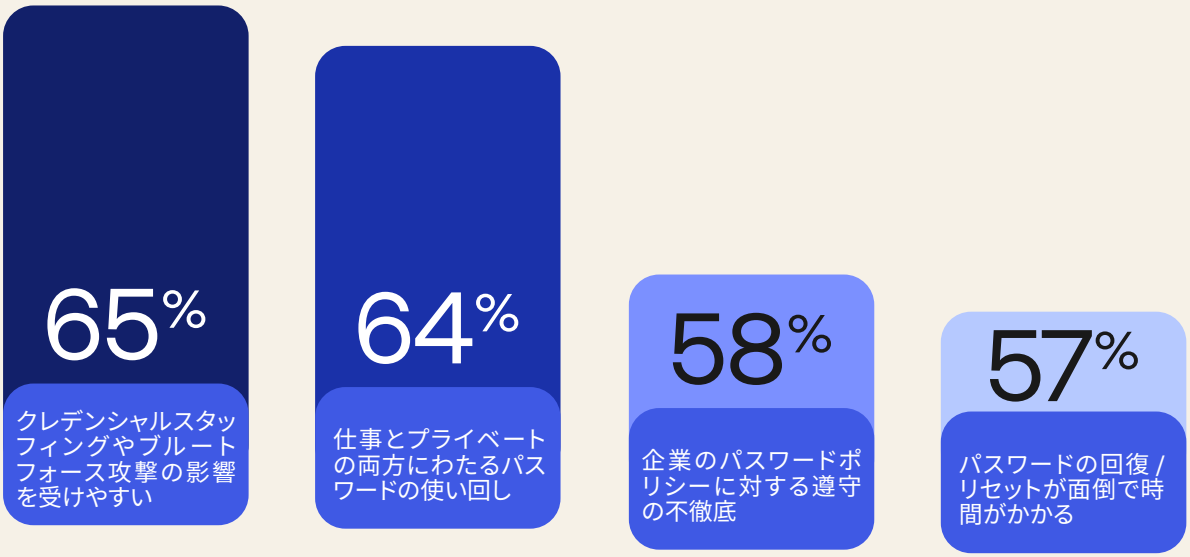
強力な IAM 戦略の一環として、フィッシング耐性のある MFA を導入する

今日のアイデンティティベースの脅威は、マルウェア、ハッキング、フィッシングなど、さまざまな形態をとっています。これらの攻撃は結果的に、認証情報の窃取、アカウントの侵害、データの流出といった影響をもたらしています。こうした一般的な脅威を防ぐためには、セキュリティ態勢を強化して対応しなければならず、その最前線で防御を担うのがアイデンティティです。オンプレミスのアプリやファイアウォールなど、従来のアプローチでアイデンティティに対処している企業は、高度な攻撃に対して驚くほど脆弱です。つまり、機敏さに欠け、複雑で断片的な枠組みに依拠したまま、組織と従業員を保護しようとしているのです。

ここで、問題を切り分けて見ていきましょう。Okta と IDG の共同調査では、IT / セキュリティ部門のリーダーが抱える、安全な認証に関する具体的ないくつかの懸念点と統計データが明らかになりました。

パスワードに関する主な懸念

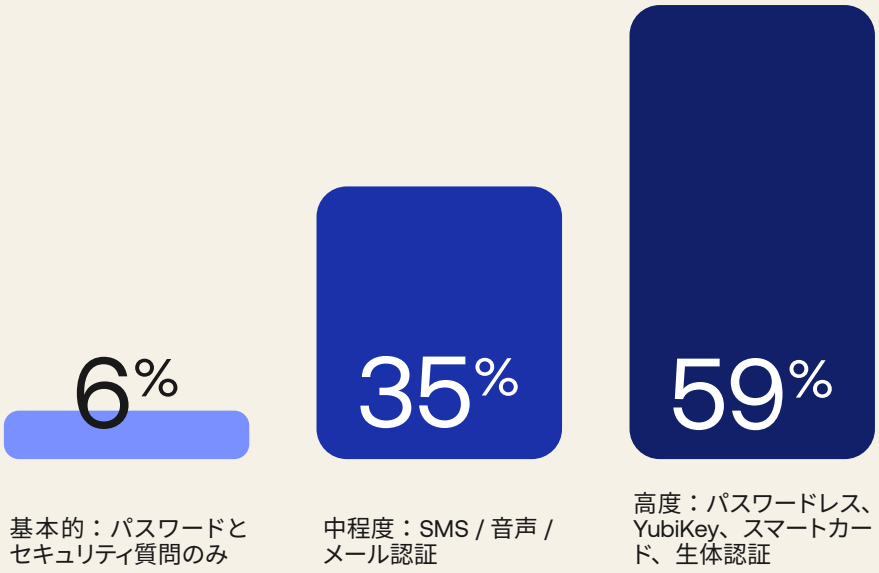
従業員数 1,000 人以上　70%
従業員数 500 ～ 999 人　52%



洞察：回答者は、認証情報の窃取、仕事とプライベートの両方のアカウントにわたるパスワードの使い回しなど、パスワードに関する懸念を複数挙げている。

ビジネスにとって最も理にかなった MFA のレベル

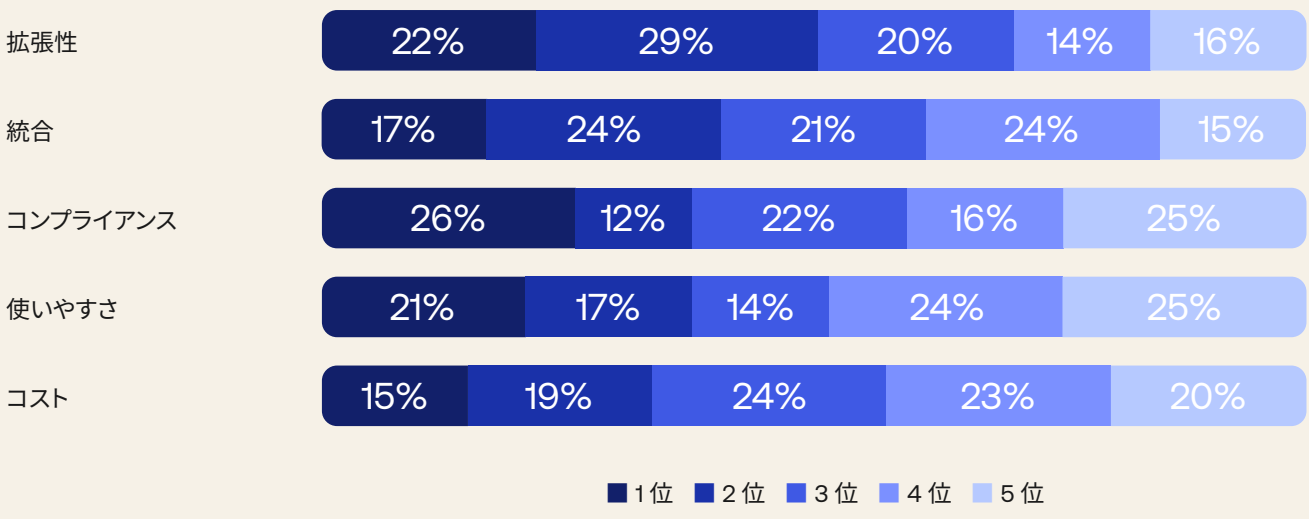
IT 部門の VP 以上	73%
IT 部門のディレクター / マネージャー	53%



洞察：回答者の過半数（59%）が、利用可能な最も強力な MFA ソリューションが自社のビジネスに最も適していると回答している。

MFA ソリューションを選択する際の基準の重要性

各組織は、5 つの基準すべてについて、重要性の高い順からランク付けを行いました。



洞察：回答者の 51% が、MFA ソリューションを選択する際の上位 2 つの検討事項の中に拡張性を挙げている。

さまざまな認証要素の保証レベルを検討する

認証では一般的に、以下に示す 3 タイプの要素のいずれか 1 つを使用してアイデンティティを検証します。

- 知識要素（パスワードなど）
- 所有要素（本人確認用スマートカードなど）
- 生体要素

MFA は、セキュリティをさらに高めるため、2 種類以上の要素を採用します。最も一般的となっているのは、依然としてパスワードを使用し、これに一定期間有効なトークン、モバイルアプリへのプッシュ通知、または生体認証要素を組み合わせるというものです。しかし、MFA にはさまざまなアプローチがあり、それぞれ長所と短所が異なります。

認証器（アイデンティティ確認に使用される手段やツール）は多様であり、それぞれに強度が異なっています。Okta では、認証器を保証レベル別に以下のように分類しています。

低：パスワード、セキュリティ質問、SMS / 音声 / メールによるワンタイムパスワード（OTP）、Authy や Google Authenticator などの OTP アプリ

中：モバイルプッシュ通知と物理トークンによる OTP

高：PIV（Personal Identity Verification）/ CAC（Common Access Card）スマートカード、FIDO 2.0 / WebAuthn と CTAP2 の組み合わせ

もちろん、MFA を強化しようとする組織が考慮するのは保証レベルだけではありません。従業員や顧客が認証器を簡単に導入し、使用できることも重要です。また、中間者攻撃（MiTM）あるいは認証プロセスに特化した中間者攻撃（AiTM）のような特定の脅威に対しても耐性が求められます。しかし、セキュリティを強化する上で最も効果があるのは、保証レベルが最も高い認証要素を使用することです。

たとえば、SMS を認証要素として提供することは、ユーザーに MFA を導入してもらうためには手っ取り早い方法かもしれませんが、高いレベルの保証を提供するものではありません。SIM ハイジャック、大規模なスミッシング / ビッシング攻撃などのセキュリティ問題が一般的になっているため、SMS 認証が提供できる保証レベルが損なわれています。そのため、Okta Verify Push、生体認証（WebAuthn 経由）、PIV / CAC スマートカード（米国政府機関の場合）のように、さらに強力な MFA 要素を利用することが強く推奨されます。

強力な MFA を設計するためのベストプラクティス

1. MFA ポリシーを検討（および再考）する

MFA ソリューションを導入する前に、自社が直面しているセキュリティリスクと具体的な脅威を評価する必要があります。最も懸念されるリソースや攻撃ベクトルはどれでしょうか。リスクベースのポリシーを十分に検討し、リスクが特に高い場合には「ステップアップ」認証のチャレンジを要求するように構成する必要があります。

たとえば、既知のネットワークからログインするときは 8 時間ごとに 2 つ目の要素を要求するようにする、または新しいデバイスや地理的位置からログインするときにのみ 2 つ目の要素を要求するといったポリシーを構成できます。あるいは、機密データに広範にアクセスできるユーザーアカウントグループに対しては、より厳格なポリシーを適用する必要があるでしょう（ソースコードにアクセスできる社内の開発者や、機密データにアクセスできる経営幹部など）。たとえば、より強力な認証要素タイプを要求したり、追加の MFA プロンプトに応答するよう求めたりすることができます。機密性の高いアクション向けの MFA を、アプリケーション内に実装することを検討してもよいでしょう。機密性が高いと判断される業務（発注の承認、送金など）をより細かく制御できるようにすることで、リスクを軽減できるだけでなく、コンプライアンス要件に継続的に対応するセキュリティをシームレスに実装できます。

最終的には、どのような検証を追加する場合でも、可能な限り透明性が高く、摩擦を排除するものでなければなりません。セキュリティを犠牲にすることなく、優れたユーザーエクスペリエンスを促進する必要があります。

2. アクセスの多様なニーズを想定して対応する

たとえば、インターネットにアクセスできても、携帯電話会社からのサービスをほとんど / まったく利用できないユーザー（Wi-Fi を利用できる飛行機、田舎の住宅、コンクリートの建物の地下など）にとっては、音声通話や SMS の利用は現実的ではありません。このような場合は、Okta Verify のプッシュやワンタイムパスワード（OTP）の方が、電話のインターネット接続を介して通信が暗号化されるために、より優れた選択肢となります。また、イベントベースまたは時間ベースのワンタイムパスワード（TOTP）を生成するハードウェアデバイスは、通信チャネルを必要とせず、改ざんやコピーが困難です。しかし、物理デバイスは導入コストが高く、従業員が自宅に忘れたり紛失したりしやすいというデメリットがあります。こうした理由から、短期の契約社員や離職率の高い職務向けの認証要素タイプとしては、必ずしも適していない可能性があります。

すべての状況に対応できる万能のソリューションは稀であることから、多種多様なシナリオを解決できるように MFA 要素を選択する必要があります。一般的に、以下のヒントを参考にすることで、セキュリティの強化とエンドユーザーエクスペリエンスの向上を両立できます。

- ユーザーに複数の要素オプションを提供し、常にバックアップを利用できるようにします。認証要素の1つがパスワードである場合は、漏洩したパスワードを検知するよう計画し、ユーザーに警告を発し、漏洩したパスワードの使用をブロックできるように対策を講じます。
- 強力でフィッシング耐性のある要素のみを有効にし、できればパスワードレスの MFA や PIV / CAC スマートカード（米国政府機関用）に移行します。
- 認証前に Web URL の出所をチェックします。認証情報は、アクセス要求の発信元ドメインにリンク / バインドされている必要があります。
- ハードウェアが対応している場合は、Windows Hello、Touch ID などの生体認証をユーザーが 2 つ目の要素として使用できるようにします。これにより、エンドユーザーエクスペリエンスが簡素化され、本人確認の保証レベルが高まります。

3. 機密性の高いアプリについては、MFA ポリシーの一環として、高保証でフィッシング耐性のある認証器を適用します。

前述したように、すべての認証器にフィッシング耐性があるわけではありません。どの認証器も、ソーシャルエンジニアリングに対する耐性をさまざまな程度で提供し、アカウントの乗っ取りを企てる攻撃者にコストとリスクを発生させています。たとえば、SMS を利用するワンタイムパスワードは、かなり簡単に傍受される可能性があります。プッシュ機能を使用する認証器は、静的なクレデンシャルフィッシングキャンペーンに対して、OTP に依存する認証器よりも高い耐性を提供します。

プッシュとナンバーチャレンジを組み合わせることによって、プッシュ要求を検証するため、示された番号をサインインページに入力するようユーザーに求めることができるようになり、「MFA 疲労」攻撃を含む広範な攻撃手法に対して耐性を提供できます。ハードウェアベースの認証器は、最高レベルの保証を提供します。

フィッシング耐性に関しては、米国国立標準技術研究所（NIST）が最も信頼できる定義を提供しています。NIST によると、認証されるチャネルが認証器の出力に対して暗号的に紐付けられていることが、フィッシング耐性に必要とされます。つまり、ユーザーがサインインする Web サイトのドメイン（アドレス）が、ユーザーの認証器に結び付けられていなければなりません。これによって、フィッシング Web ページに認証情報を発行することが防止されます。

Okta のプラットフォームでは、この定義を満たしている複数の認証器を利用できます。Okta は、ローミング FIDO2 WebAuthn 認証器（セキュリティキー）とデバイスバインド FIDO2 WebAuthn 認証器（Face ID、Touch ID、Windows Hello など）をサポートしています。また、特定のアプリにアクセスするために、アプリのサインオンポリシー内で PIV スマートカード認証を使用することもサポートしています。導入モデルによっては、FastPass（Okta のデバイスバウンドのパスワードレス認証器）もこの定義を満たします。少なくとも 1 つのフィッシング耐性のある認証器の使用を義務付けることで、ソーシャルエンジニアリングや AiTM 攻撃による高度なフィッシング攻撃のリスクを排除できます。

4. コンプライアンス要件を慎重にチェックする

PCI DSS（ペイメントカード業界データセキュリティ基準）、SOX（Sarbanes Oxley 法）、HIPAA（医療保険の相互運用性と説明責任に関する法律）など、IT コンプライアンス標準のほとんどは、ユーザー認証の強力なコントロールを義務付けています。こうした標準を満たすことを目標にする場合は、要件を詳細に理解し、構成やポリシーが要件に沿うように調整する必要があります。たとえば、PCI や HIPAA のコンプライアンスでは、3 つの強力な認証手法のうち少なくとも 2 つを含む強力な認証が必要です。SOX では、テクノロジー以上に監査への対応が重視されていますが、依然として財務会計データが安全であることを証明する必要があります。IT コンプライアンスでは、関連する標準を導入し、対応していることを証明しなければなりません。構成 / 実装プロセスの一環として慎重な文書化を行い、監査ですみやかに証拠を作成できるように備えることが、IT / セキュリティリーダーと組織の双方にとって後々大きく役立ちます。

5. ハイブリッドワークの拡大に対応する MFA 導入モデルを採用する

リモートやハイブリッドで働く従業員や契約社員がクラウドのリソースを利用していることから、セキュリティの強化が不可欠になっています。理想的には、既存の従業員が IT に直接アクセスできるオフィスで新入社員のオンボーディングを行うべきですが、リモートワークが MFA の導入とトラブルシューティングに新たな課題をもたらしています。

MFA の導入をスピードアップするためには、ハードトークンの受け取りのため

にユーザーを待たせるのではなく、すぐに業務を開始できるような認証要素（デバイス組み込みの生体認証や Okta Verify のようなモバイルアプリの認証器など）をユーザーが利用できるようにすることが推奨されます。これにより、セットアップに必要なリソースに素早くアクセスできるようになります。新入社員のオンボーディングにリモートで対応するため、バーチャルオンボーディングセッションを開催し、新入社員が会社のメールを使用できるようになる前でも情報を伝達できるよう、従業員の私的なメールアドレスにセットアップ手順を送信する組織もあります。

6. デバイスを紛失した場合の対応策を準備する

BYOD（個人所有デバイスの業務利用）を認めている職場では、個人所有のデバイスから企業資産にアクセスする従業員が急増しています。しかし、こうした非管理デバイスには、セキュリティ上の大きな課題があります。BYOD ポリシーを導入している多くの企業では、従業員のデバイスを介したデータ侵害が発生しており、このオープンな脅威ベクトルを保護することが不可欠となっています。

デバイス保証ポリシーでは、認証ポリシーの一部として、OS バージョン、ディスク暗号化、ジェイルブレイク / root 検知など、セキュリティに関する一連のデバイス属性をチェックできます。このようにして、デバイス保証ポリシーは、認証ポリシールールの上に追加のセキュリティレイヤを作成し、使用中のデバイスのセキュリティ態勢を検証します。

さらに、従業員が日常的に企業データをデスクトップ / ノート PC にダウンロードしているという事実も考慮する必要があります。そのため、ユーザーがマシンのロックを解除するためにパスワードを入力した後、MFA チャレンジを完了するよう要求できることが重要です。ほとんどのコンプライアンスガイドラインには、MFA が要件として含まれており、マシンレベルでこれを実行できることで、デスクトップ関連の攻撃のリスクを回避し、ノート PC の紛失や盗難の際にデータを保護できます。

しかし、ユーザーが持っているものは、どれも紛失する可能性があります。そのため、IT ヘルプデスクの包括的なプレイブックの一部として、紛失したデバイスを処理する手順を定めておく必要があります。MFA に使用されるデバイスについて、紛失したデバイスが報告された場合に以下の対応が実行されるように確保します。

- 現在のセッションをすべて閉じて、ユーザーに再認証を要求する
- ユーザーのアカウントとアクセス権からデバイスの関連付けを解除する
- モバイルデバイスの企業情報をリモートから消去する（通常は企業所有デバイスに対して実行）

また、デバイスを紛失する前のユーザーアカウントのアクティビティを監査して、

異常なアクティビティがないかを確認することも重要です。不審な点に気づいたら、侵害の可能性を検討し、それに応じてエスカレーションを行います。当面のセキュリティ上の懸念に対処したら、代替のデバイスやログイン方法により従業員が業務を再開できるよう注力します。たとえば、IT ヘルプデスクに電話してアイデンティティ要件を確認するといった代替プロセスによって、代替の認証要素を置き換えるまでの間も従業員が生産性を低下させずに作業できるよう確保できます。

7. アダプティブ MFA の導入を検討する

ステップアップ MFA は、MFA を適用する方法とタイミングをきめ細かく制御できる反面、構成には慎重な検討が必要です。明確に定義されたポリシーや基準であっても、ユーザーやデバイスのコンテキストの変化に基づいて、動的なアクセス判定を実行できるようにしたい場合もあるでしょう。

アダプティブ MFA は、アクセスパターンに注目し、各ユーザー / グループにポリシーを適応させます。たとえば、頻繁に出張し、海外でメールをチェックすることの多い従業員には、2 つ目の要素を定期的に要求するだけでよいでしょう。一方、出張のない従業員が海外からアクセスする場合は、即座に MFA チャレンジを受けることになります。未認可のプロキシを経由してリソースにアクセスしようとすると、ステップアップ認証のチャレンジを求めたり、既知の悪意のある IP からのアクセスを自動的にブロックしたりするようなリスクベースのポリシーも、不審なイベントがトリガーとなって適用されることがあります。アダプティブ MFA は、自動的に動的なポリシーを継続的に導く強力なツールであり、組織が必要とするセキュリティを提供するのに十分な厳格さと、ユーザーを個人として扱うのに十分な柔軟性を両立させます。

8. 段階的に導入する

複雑な導入やポリシーが、最初から完璧に機能することはほとんどありません。プロセスの変更が全従業員に影響する場合は、導入の効果を継続して追跡し、観察に基づいてポリシーを調整するよう備える必要があります。導入を段階的に進め、IT 部門やセキュリティ部門が最初に MFA を使い始め、続いてユーザーグループを拡大させていくようにします。プロセスの早い段階で監査機能に慣れるように取り組むことで、将来、トラブルシューティングやポリシーの構成を調整する際に非常に役立ちます。

たとえば、特定のユーザーグループに MFA を導入したら、監査ツールを使っ

て導入と利用をチェックできます。また、ユーザーからのフィードバックの仕組みを導入するとよいでしょう。ユーザーが時間を割いてフィードバックを書くとは限りませんが、監査証跡があれば、ユーザーが経験したことをある程度把握できます。ワンタイムパスワードの入力を 3 回試行したのか、あきらめたのかといった問題は、構成ミス、ユーザー教育の足りない部分、あるいは単に当初のロールアウト計画で考慮されなかったシナリオを示唆している可能性があります。監査ツールを使用し、従業員からのフィードバックを促すことで、すべてのステークホルダーが、システムが意図したとおりに機能し、新しいセキュリティポリシーが問題なく採用されていることを確認できます。

9. ユーザー教育を提供する

パスワードだけに依存したアクセスによるセキュリティリスクを軽減するために MFA を導入することは、高度にデジタル化した世界では不可欠なセキュリティプラクティスです。しかし、このプロセス変更によって、忙しい一日の貴重な時間が奪われるのではないかと懸念し、不便だと考えるユーザーも出てくるでしょう。マネジメントから IT チーム、セキュリティチーム、エンドユーザーに至るまで、全員が MFA に移行する理由を認識して足並みを揃えることが不可欠です。組織全体から賛同を得ることで、全員が自社のセキュリティを確保する役割を受け入れ、理解できるようになります。教育を通じて、この追加ステップを踏むことのセキュリティ上の利点をユーザーが理解できます。

一般的なアプローチとしては、IT 部門が今後の変更を通知するメールを送ることが有効です。また、社内でフィッシングの模擬訓練を実施することで、どれほど熟練した従業員でも騙されて認証情報を漏洩させる可能性があることを示すことができます。従業員が簡単に連絡できるように、スクリーンショット、FAQ、連絡先を明記します。

アカウント回復フローの脆弱性を理解し、管理する

多要素認証の安全性は、アカウント回復のためにどのようなフローを使用するかに左右されます。最近では、攻撃者がアカウント回復プロセスの脆弱性を悪用し、アカウントのコントロールを取得した事件が大きく報道されました。

ここで、Acme という会社の例で考えてみましょう。この会社の Web アプリケーションは、ユーザーのスマートフォンにインストールされたソフトトークンアプリに基づく MFA を提供しています。さらに、ユーザーがソフトトークンにアクセスできない場合のアカウント回復のため、バックアップの 2 つ目の要素を受け取るための電話番号を登録できます。そのため、Acme の 2 つ目の要素の強度は、通信プロバイダーが顧客を認証し、通話や SMS を転送するプロセスの強度に依存します。攻撃者はユーザーになりすまして、通話や SMS を自分が管理する番号に転送するよう、カスタマーサービス担当者を説得したり圧力をかけたりできるでしょうか。

すべての 2 つ目の要素には信頼できる代替手法が必要となるため、組織は安全な回復フローを設計しなければなりません。状況によって適したアプローチは異なりますが、留意すべきベストプラクティスを以下に紹介します。

第 1 要素と 2 つ目の要素の回復を独立させる：
2 つ目の要素の回復を、第 1 要素の回復と切り離すことが重要です。これを怠ると、攻撃者が第 1 要素にアクセスできるようになった場合、侵害されたパスワードを使用して 2 つ目の要素をリセットできてしまうと、2 つ目の要素が信頼できないものになります。2 つ目の要素の回復は、パスワードの回復とは完全に異なるフローにすべきです。たとえば、メールメッセージを回復手段として使用する場合、2 つ目の要素は別のチャネルを使用して回復するようにします。

管理者を関与させる：
管理者は、さまざまなシナリオで、高度な高保証の認証手法を実装できます。企業のシナリオにおいては、企業は、従業員の仕事やプロファイルの内容、会社、人間関係から導き出される共有シークレットを通じて、組織のメンバーを認証する最良の立場にあります。注目すべきアプローチの 1 つは、従業員の上司にユーザーを認証してもらい、IT 部門に MFA リセットの実行を認可してもらうことです。

コンシューマー向けのシナリオでは、管理者は、共有シークレットの大規模なセットにわたってユーザーに質問できます。たとえば、コンシューマー向けのバンキングアプリケーションは、オンボーディングで、個人に関してあまり知られていない細かい情報を、アカウント回復のための共有シークレットとして大規模に収集することがあります。アプリケーションや企業が保持するユーザーの履歴に含まれる最近のイベントも、共有シークレットとして役立つ可能性があります。一連の共有シークレットの評価は、Web や音声を介して自動化でき、ソーシャルエンジニアリングに対して脆弱でないため、多くの場合に人間よりも優れた保証を提供できます。

バックアップの 2 つ目の要素を提供する：
多くのシナリオでは、2 つ目の要素を回復するための自動化された手法を必要とします（たとえば、1対1のサポートが非常に高額になるサービスを多数のユーザーに提供する製品や、運用コストの削減が必要な場合など）。オンボーディング時に登録する 2 つ目の要素を複数にすることで、ユーザーはバックアップの2つ目の要素を使用して認証を完了することで2つ目の要素を回復できます。シンプルかつ低コストな方法で、特筆すべき例としては、一度しか使用できないコードのセットを含むカード（物理的なカードまたは印刷可能なカード）をユーザーに提供し、それをバックアップの2つ目の要素として使用することです。

ブルートフォース攻撃やクレデンシャルスタッフィング攻撃からログインフローを保護する

安価なコンピューティングリソースが利用可能になるにつれて、推測を利用するブルートフォース攻撃に対する認証システムの脆弱性も増しています。しかし、いくつかの簡単な手法を使用することで、パスワードが漏洩した際の MFA のセキュリティを大幅に向上させることができます。

ログとアラートを分析する：
2 つ目の要素の試みの失敗を収集して分析します。2 つ目の要素のチャレンジに何度も失敗した場合は、この不審な行動についてユーザーまたは管理者に警告し、新しいトークンを登録するようユーザーに求めます。

帯域外のトークンを使用する：
2 つ目の要素の検証に第 1 要素とは異なるチャネルを使用することで、ブルートフォース攻撃やフィッシング攻撃に対する保護をさらに強化できます。たとえば、新たに広く使用されている要素として、認証要求の詳細と、要求を受け入れるか拒否するかのプロンプトを含むプッシュ通知を携帯電話に送るという方法があります。このチャネルは、従来のブルートフォースによる推測のアプローチではアクセスできません。

リスク、ユーザビリティ、コストのバランスを念頭に設計する

MFA 機能の設計は、どのような状況においても、セキュリティ、ユーザビリティ、コストに大きな影響を与えます。保証レベルがより高い 2 つ目の要素を使用することで、かえって製品の MFA の採用率が低下しセキュリティを損なう可能性もあるため、エンドユーザーや管理者にとって不必要な余分な負担のように感じられる場合があるかもしれません。そこで、リスク、ユーザビリティ、コストのバランスをとることが重要となります。そのためのベストプラクティスを以下にいくつか紹介します。

多様なユーザー層に対応するため、さまざまなオプションを提供する：
ユーザー層によってリスクレベルが異なるため、必要とされる保証レベルも異なります。たとえば、管理者は個人ユーザーよりもアクセス範囲が広範になることがあります。そのような場合、一般の従業員にはより便利なオプションを提供する一方で、管理者にはより強力な 2 つ目の要素を提供する必要があります。コンシューマー向けのシナリオでは、ユーザーによって、自分のアカウントに求めるセキュリティとユーザビリティのバランスに対する好みが異なります。SMS のような保証レベルが低く、より馴染みのあるオプションが使われるのであれば、保証レベルが高くても広く採用されないオプションよりも安全性が高まるかもしれません。

フェデレーション方式のアイデンティティと認証をサポートする：
アイデンティティのフェデレーション（認証連携）は、フェデレーション方式のシングルサインオン（SSO）とも呼ばれます。複数のアイデンティティ管理システム間でユーザーのアイデンティティをリンクする手法であり、ユーザーはセキュリティを維持しながらシステム間を迅速に移動できます。企業向けのシナリオでは、多くの企業が自社が管理するアイデンティティの認証と MFA をローカルに実装し、リソースに連携させています。製品開発チームはこのアプローチにより、ポリシーやセキュリティプロセスの管理を顧客やパートナーに任せることができます。このような場合、ユーザーは独自に MFA を実装でき、それぞれの状況や制約に応じて、前述のような事項を総合的に考慮した上での最適化が可能になります。たとえば、パートナーは、特定の IT 機能に合わせてアカウント回復の管理を設計できます。こうしたアウトソーシングのアプローチには、ユーザーが 1 つのトークンを使ってすべてのリソースにアクセスできるという利点もあります。

ゲーム チェンジャー としての Okta

アイデンティティ管理に対して最新のアプローチをとっている Okta は、企業の MFA を含むアイデンティティ管理のコントロールを支援し、データ侵害などの悪影響を軽減する上で独自の地位を確立しています。以下に、Okta のメリットを紹介します。

従業員 / 顧客向けの MFA を迅速に有効にする：

- すぐに利用可能な 7,000 以上の接続（Okta のアプリケーションネットワークで提供）により、MFA を迅速かつ容易に導入
- RADIUS、RDP、ADFS、LDAP、さらに Okta Access Gateway を介したヘッダーベース認証と Kerberos のサポートにより、オンプレミスアプリケーションへ適用範囲を拡大
- デバイスと接続の属性に基づく、インテリジェントでコンテキストに応じたアクセス判定を促進
- シングルサインオンとパスワードレス認証により、パスワードへの依存を低減

確信を持ってアイデンティティを一元化する：

- アカウント管理の複雑さを軽減
- ユーザーのアクセスを統一し、パスワードを排除すると同時に、優れたエクスペリエンスを提供
- インテリジェントな SAML 接続を介してサービスへのアクセスを制限することで、リスクを軽減し、アイデンティティの増大を抑制

攻撃対象領域を縮小し、認証情報の侵害に迅速に対応する：

- プロビジョニング / プロビジョニング解除を自動化し、一貫性のあるオンボーディングを加速させるとともに、孤立アカウントを排除
- SCIM、SDK、Okta の充実した API を通じて、セキュリティポリシーをカスタムアプリケーションに拡張
- アクセス要求ワークフローと包括的なアイデンティティライフサイクル管理により、適切なタイミングで適切なアプリケーションに適切なレベルのアクセスを確実に付与

このデモでは、Okta の Adaptive MFA（Multi-Factor Authentication）ソリューションの管理や認証プロセスの試験運用がいかに簡単かをご確認いただけます。

Okta の Adaptive MFA ソリューションの詳細については、https://www.okta.com/jp/products/adaptive-multi-factor-authentication/ をご覧ください。

まとめ：MFA を成功させるためのロードマップ

多要素認証は、アプリケーション開発者がアプリケーションへのアクセスを保護するための世界的なベストプラクティスとなっています。しかし、その裏では、従業員を混乱させることなく MFA によるセキュリティの効果を十分に生かすために、多くのステップを踏まなければなりません。ベストプラクティスには、2 つ目の要素の回復フローを分析すること、ブルートフォース攻撃に耐性のあるシステムを設計すること、セキュリティ、ユーザビリティ、コストの適切なバランスを見つけることなどが含まれます。

MFA に対する最新の自動化されたアプローチは、組織がアクセスを制御し、回復を安全に自動化し、データ侵害のリスクを劇的に軽減するのに役立ちます。

ホワイトペーパー

MFA（多要素認証）導入ガイド

okta

Okta Japan 株式会社
〒 150-8510 東京都渋谷区渋谷 2-21-1
渋谷ヒカリエ 30 階
お問い合わせ先：
okta.com/jp/contact-sales/