Press Release

2023 年 6 月 15 日
Okta Japan 株式会社

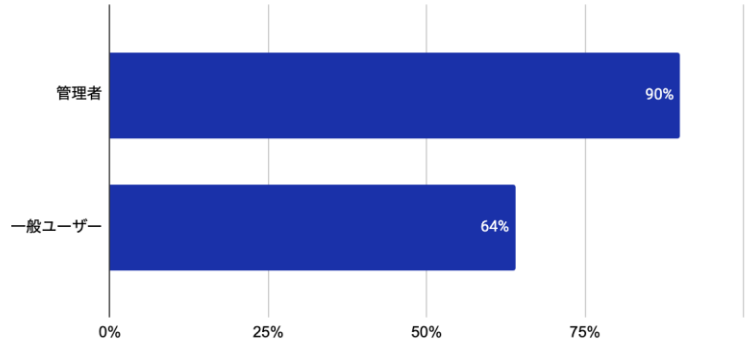
報道関係者各位

Okta ユーザーの MFA 導入状況を調査したトレンドレポート「The Secure Sign-in Trends Report」の調査結果を発表

Okta Japan 株式会社（本社：東京都渋谷区、代表取締役社長：渡邉 崇）は、Okta が提供する従業員向けアイデンティティ管理ソリューション「Okta Workforce Identity Cloud」の月間数 10 億件以上におよぶ認証データを匿名化し、Okta ユーザーの MFA（多要素認証）導入状況を調査したトレンドレポート「The Secure Sign-in Trends Report」の調査結果を発表します。本レポートでは、Okta のお客様をユーザー別、業種別、企業規模別に見た場合の MFA 導入率（*[1]）や、MFA で利用する認証要素のトレンドを調査しています。調査は 2023 年 1 月に実施しました。

ユーザー別の MFA 導入率

2023 年 1 月の 1 ヶ月間に、Okta 管理者の約 90%、Okta の一般ユーザー約 64%が MFA を使用してサインインしています。

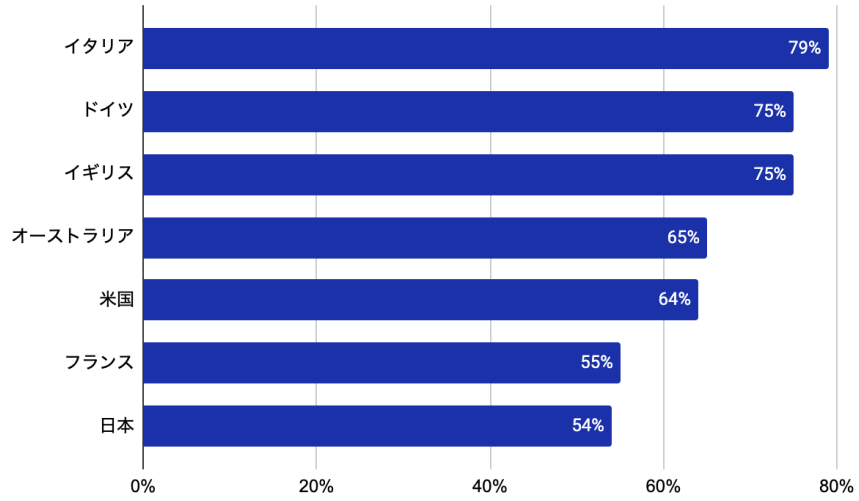


Okta 管理者の MFA 導入率が高い理由は、Okta の管理サイト「Okta Admin Console」にアクセスする際にデフォルトで MFA が必要であるためです。

地域別と国別の MFA 導入率

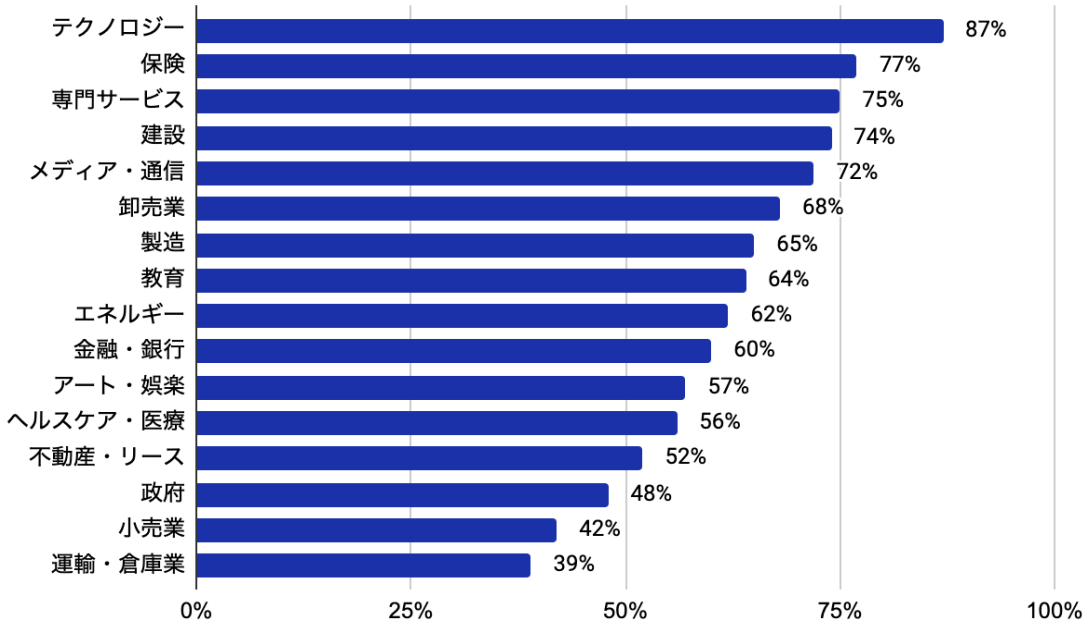
[1] 本レポートでの MFA 導入率は、Okta Workforce Identity Cloud での直接の MFA 認証イベントのみをカウントしています。他のアイデンティティプロバイダが提供する MFA のみを使用して認証し、エンタープライズフェデレーションやソーシャルログインを使用して Okta に接続する場合、それらは MFA 導入率データの対象外となります。

地域別の MFA 導入率は、北米、APAC、EMEA で平均して 64%の導入率ですが、国別に見た場合、日本での MFA 導入率が 54%で遅れている傾向が見られます。



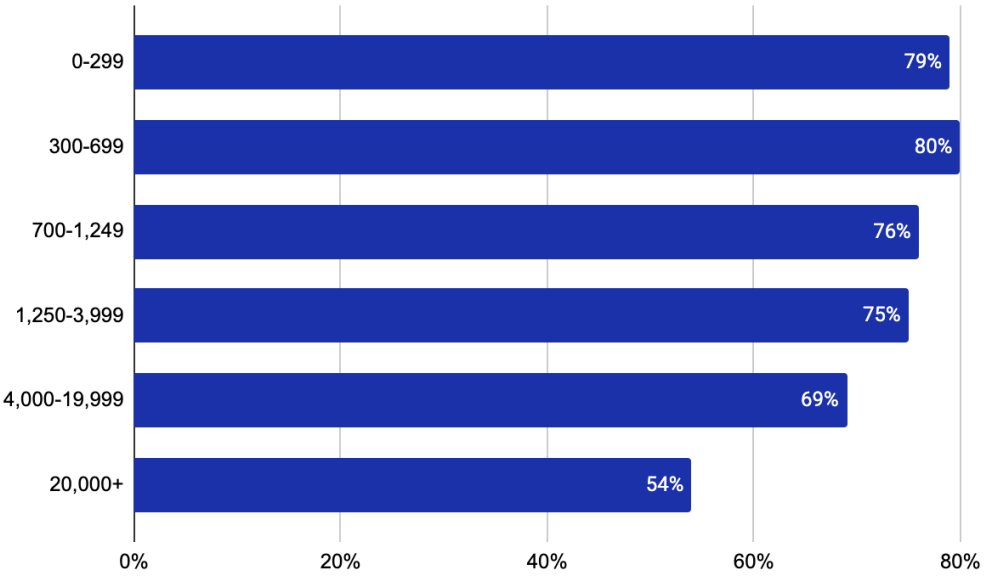
業界別の MFA 導入率

テクノロジー業界では、アカウントログインの 87%がすでに MFA を導入しています。続いて、保険業界（77%）、専門サービス業界（75%）、建設業界（74%）、メディア・通信業界（72%）が、上位 5 を占めています。政府（48%）、小売（42%）、ヘルスケア・医療業界（56%）など、規制の厳しい業界での MFA 導入率が遅れている傾向が見られます。



企業規模別の MFA 導入率

従業員数 699 人未満の組織では MFA の導入率が高く（79%～80%）、従業員数 2 万人以上の組織では導入率が低い（54%）傾向にあります。



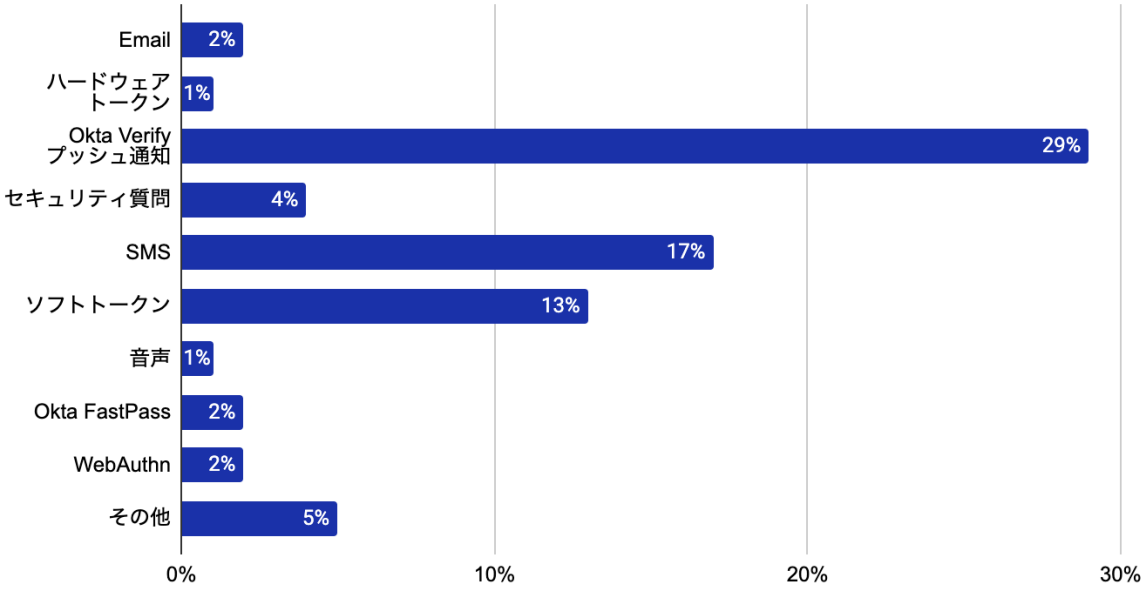
大企業と中小企業の導入率に差がある要因として考えられるのは、大企業では、レガシーインフラの置き換えが複雑なため、MFA の導入が遅れている可能性があります。また、大企業は複

数のアイデンティティ管理製品を使用している可能性が高く、Okta 以外の MFA ソリューションを使用している可能性もあります。

MFA で利用する認証要素のトレンド

MFA は、アプリケーションやオンラインアカウントへのアクセスを許可する前に、ユーザーが本人であることをより確実に証明するものです。MFA は、アカウントやアプリケーションにアクセスするために、ユーザーにさまざまな種類の認証要素の提供を求めることでアイデンティティを検証します。しかし、MFA をバイパスする巧妙な攻撃の増加により、組織はフィッシングに強い認証フローの必要性を理解するようになってきています。

パスワードを除く MFA 認証要素に限ると、Okta Verify プッシュ通知（29%）が最も多く利用されており、次いで SMS（17%）、ソフトトークン（13%）となっています。



パスワードレス認証を可能にする Okta FastPass と WebAuthn は、強固なフィッシング耐性を提供するサインイン方法で、ユーザーは体験の質を低下させることなく、アカウントのセキュリティを向上させることができます。現在、これらの認証要素の導入率が低い傾向にあるのは、管理者の認識不足や不慣れさに原因がある可能性があります。Okta FastPass は新しいカテゴリーの認証要素であり、その独自のフィッシング耐性はまだ新しいものです。WebAuthn の標準規格も比較的新しく、ブラウザや OS のカバー率は近年まであまり向上していません。

組織が取るべき今後のステップ

より強固な認証への移行は困難と思われるかもしれませんが、組織は比較的簡単なステップで開始することができます。

- サインオンポリシーに MFA を義務付け、機密性の高いアプリケーションやデータへの管理アクセスにはフィッシング耐性を強化する。パスワードレス認証の Okta FastPass が提供するフィッシング耐性とデバイス保証機能を活用する。
- MFA の導入を経営者および取締役会レベルの優先事項とする。組織の最も貴重なリソースと情報を保護するための MFA の有効性を考えると、MFA の導入率は組織の最上位レベルで確認する必要がある。
- アクセスに対するゼロトラストアプローチを採用する。このアプローチでは、アクセスはセッションごとに最小特権ベースでアイデンティティのプロパティに従って付与され、要求されたアプリケーションまたはデータの保証要件に従って決定される。
- ユーザー属性、デバイスのコンテキスト、ネットワークの属性、および要求が以前のユーザー行動と一致しているかどうかを評価する動的アクセスポリシーを作成する。
- パスワードの使用を最小化または廃止するための長期的な計画を策定する。

Okta について

Okta は、独立系アイデンティティ管理のリーディングカンパニーとして、あらゆる人があらゆる場所で、あらゆるデバイスやアプリで、あらゆるテクノロジーを安全に利用できるようにします。最も信頼されているブランド企業は、Okta を信頼して安全なアクセス、認証、自動化を実現しています。Okta の Workforce Identity Cloud と Customer Identity Cloud の中核には柔軟性と中立性があり、ビジネスリーダーや開発者はカスタマイズ可能なソリューションと 7,500 以上のアプリケーションとの事前統合により、イノベーションに集中し、デジタル変革を加速させることができます。私たちは、アイデンティティがお客様のものである世界を構築しています。詳しくは以下をご覧ください。
https://www.okta.com/jp/

【本件に関するお問い合わせ先】
■ Okta Japan 株式会社
広報担当：中田清光
Email: kiyomitsu.nakata@okta.com
■Okta PR 事務局（株式会社プラップジャパン内） 担当：山本・中根・冨安・藤沢
TEL: 080-9821-6995（**山本携帯**）、080-6859-3639（**中根携帯**）
Email: okta@prap.co.jp