GlobalSign by GMO

クラウド時代の不正アクセス対策

Microsoft Entra IDを クライアント証明書で セキュリティ強化

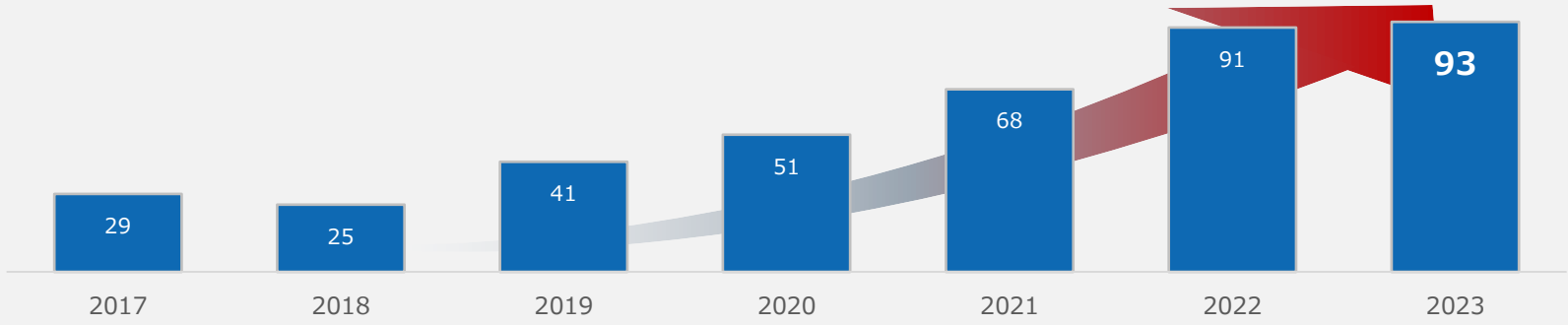
目次

はじめに

増加する不正アクセス要因の情報漏えい事故

不正アクセス要因の事故が年々増加している中、機密情報や個人情報を管理しており、利用者数の多いサービスは、今後も攻撃の対象になりやすいと想定できます。そこで、今回は、**ID管理サービスとして多く利用されている**Microsoft Entra ID**に迫る不正アクセスの危険性**と、その**不正アクセス対策となる認証強化として有効な**クライアント証明書**について、詳しく解説します。

上場企業とその子会社におけるウイルス感染・不正アクセス事故件数

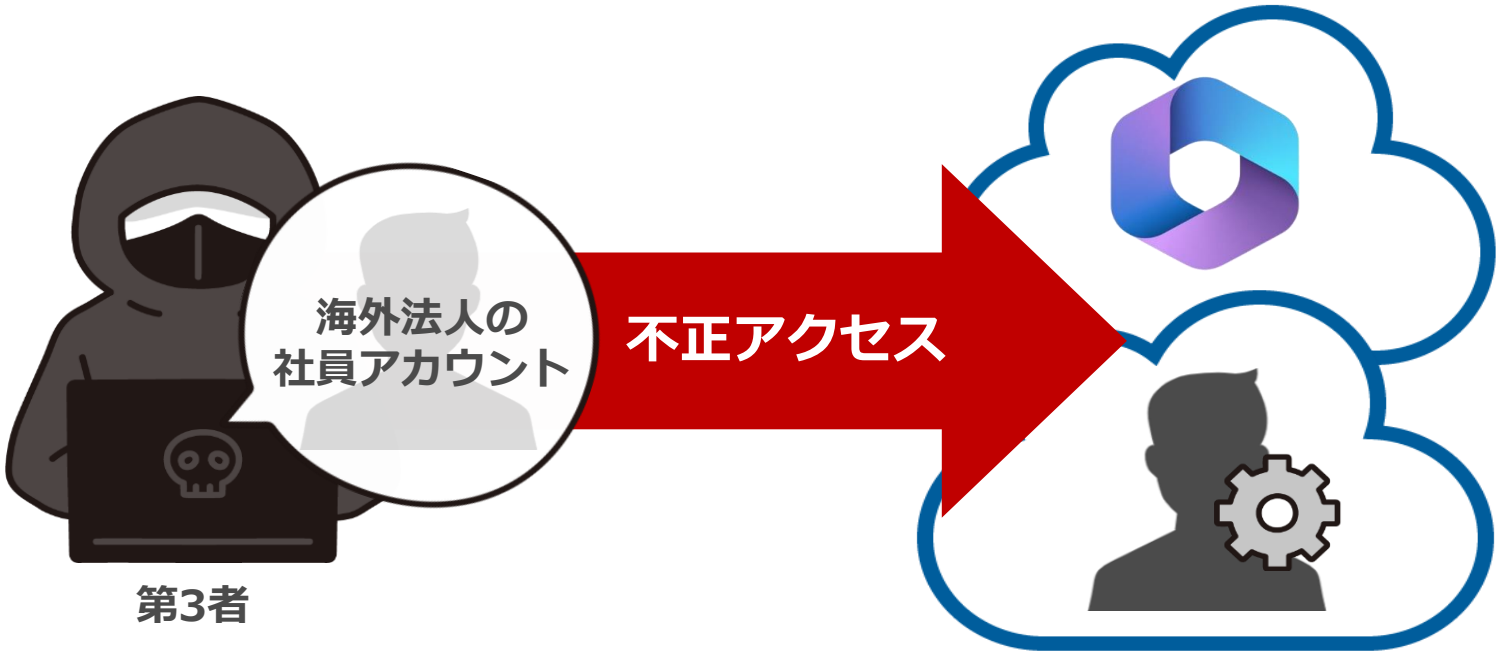


引用元：東京商工リサーチ 2023年「上場企業の個人情報漏えい・紛失事故」調査

増加するサイバー攻撃

Microsoft製品・ID管理システムへの不正アクセス

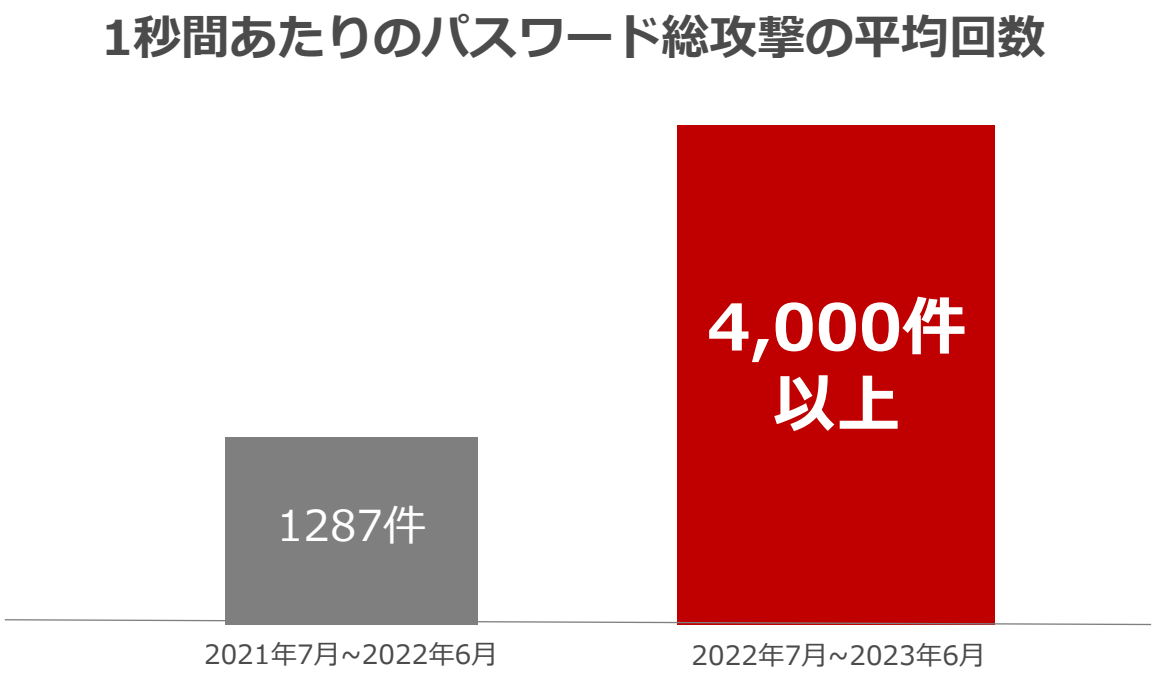
第3者が海外法人の社員アカウントを悪用した結果、グループ全体として**約11,000件の取引先関係者の情報漏えい**の可能性がある事故が報告されました。



引用元：不正アクセスによる個人情報流出の可能性に関するお詫びとご報告

増加するパスワード攻撃

2021年7月から2023年6月に行った調査で、Entra IDに対する**パスワード総攻撃の回数が1年で約3倍に増加**したという報告がありました。



引用元：Microsoft Japan Blog

Microsoft Entra IDへのパスワード攻撃の種類

攻撃名	長く複雑なPWは対策として有効か？	
クレデンシャルスタッフィング	✕	ユーザが別サイトでもPWを再利用している限り、攻撃者は正確なPWを保持できてしまうため、効果なし。
パスワードスプレー	△	攻撃者がよく試すような簡単なPW、また、推測されづらいPWを使用しない限りは、安全。
フィッシング（中間者攻撃）	✕	攻撃者はフィッシングサイトに入力されたPWを正確に知ることができるため、効果なし。
キーログ	✕	マルウェアが入力した情報を正確に窃取しているため、効果なし。
パスワード総攻撃	△	パスワードマネージャーでの管理や、ユニークなPWを使用している場合には、安全。

長く複雑なパスワードの設定をした場合でも、
不正アクセス対策として効果的でないケースが多く存在します。

引用元：Japan Azure Identity Support Blog パスワードで攻撃は防げない - Your Pa$$word doesn't matter

AiTM（Adversary-in-the-Middle）

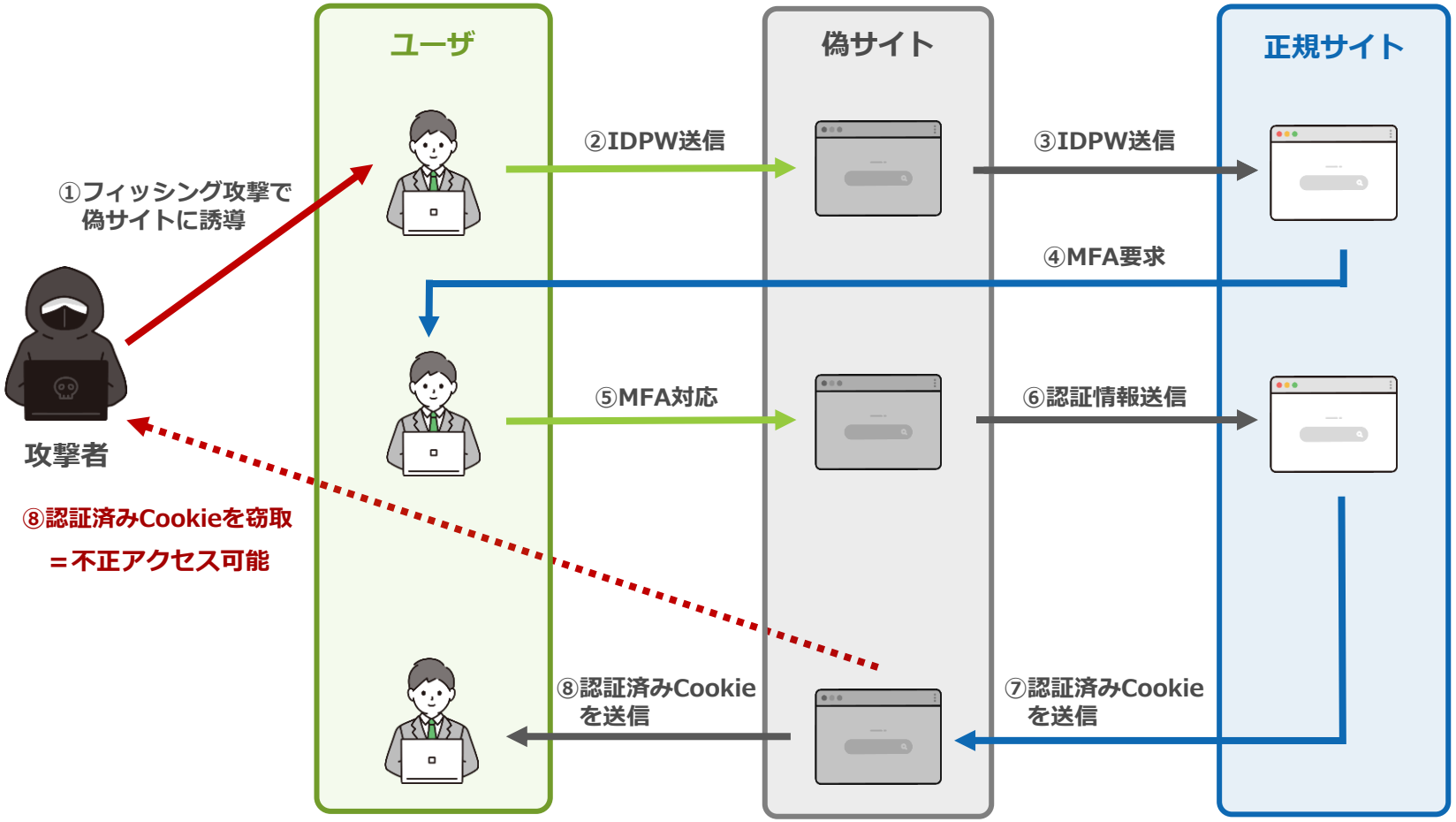
AiTM（Adversary-in-the-Middle）攻撃とは、**攻撃者がターゲットと、ターゲットがアクセスしようとしている正規のWebサイトの間にプロキシサーバを配置することで、ターゲットのパスワードや、Webサイトの認証済みセッションCookieを窃取することを目的としたフィッシング手法**です。この手法により、**プッシュ通知認証やSMSなどによるワンタイムパスワードを含む多要素認証（MFA）を突破することも可能**となります。

2022年7月時点の報告によると、2021年9月以降、この攻撃手法により1万を超える組織が標的とされています。また、2023年6月時点でも、AiTM攻撃は進化を続けており、さらなるリスクが指摘されています。

引用元：Detecting and mitigating a multi-stage AiTM phishing and BEC campaign

引用元：From cookie theft to BEC: Attackers use AiTM phishing sites as entry point to further financial fraud

AiTM の流れ



引用元：From cookie theft to BEC: Attackers use AiTM phishing sites as entry point to further financial fraud

フィッシング攻撃に有効とされる対策

AiTM フィッシングと BEC からの防御

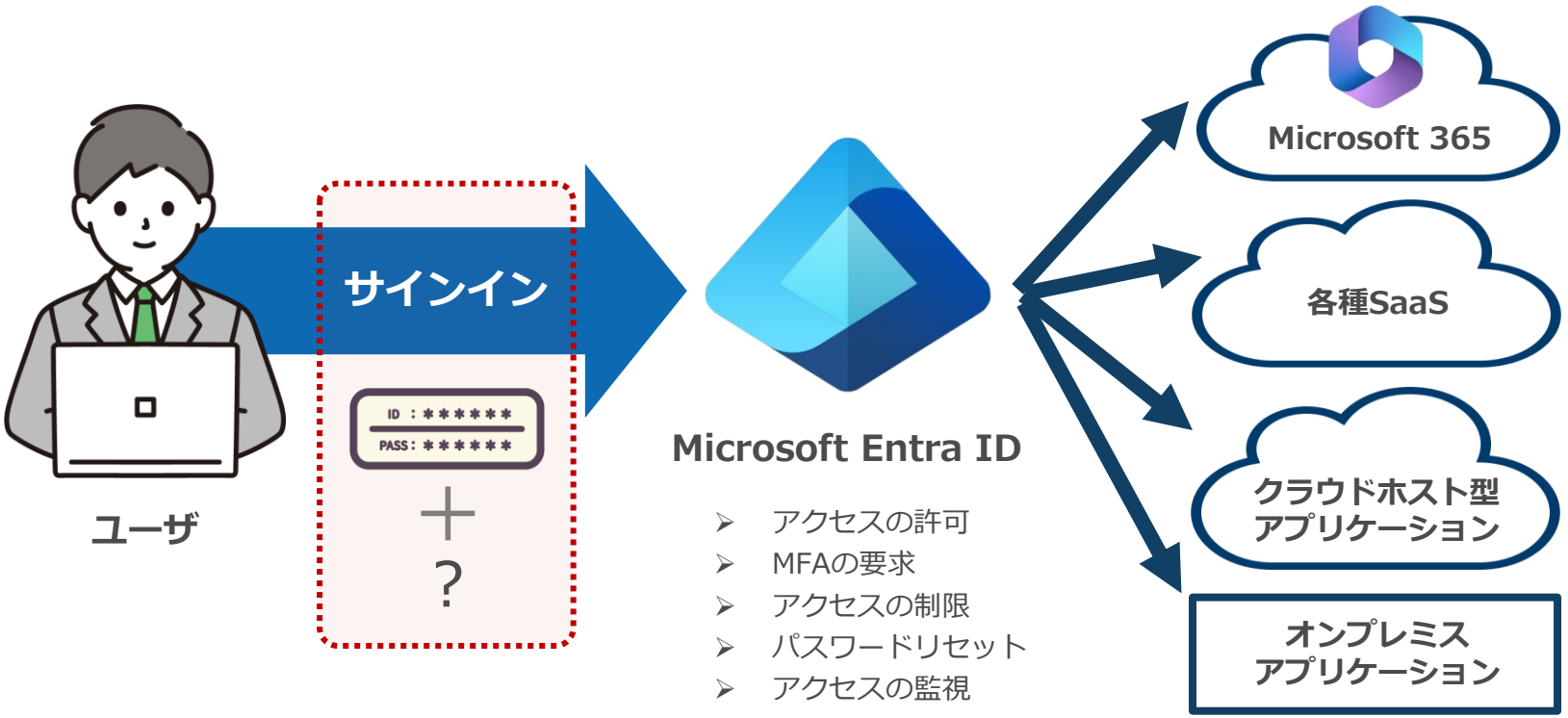
この AiTM フィッシング キャンペーンは、組織が潜在的な攻撃から身を守るために導入したセキュリティ対策やポリシーに応じて、脅威がどのように進化し続けるかを示すもう 1 つの例です。また、昨年はクレデンシャル フィッシングが最も被害を与える攻撃の多くに悪用されていたため、同様の試みが規模と巧妙さを増していくことが予想されます。

AiTM フィッシングは MFA を回避しようとしますが、MFA の実装が依然としてアイデンティティ セキュリティの重要な柱であることを強調することが重要です。MFA は、さまざまな脅威を阻止するのに依然として非常に効果的です。AiTM フィッシングが最初に出現したのは、その有効性が理由です。したがって、組織は、Fast ID Online (FIDO) v2.0と証明書ベースの認証をサポートするソリューションを使用することで、MFA 実装を「フィッシング耐性」のあるものにすることができます。

フィッシング耐性のある認証方法は、
「クライアント証明書認証」と「FIDO2認証（生体認証）」

引用元： Cookie の盗難から BEC まで

不正アクセスによる情報漏えいを防ぐには



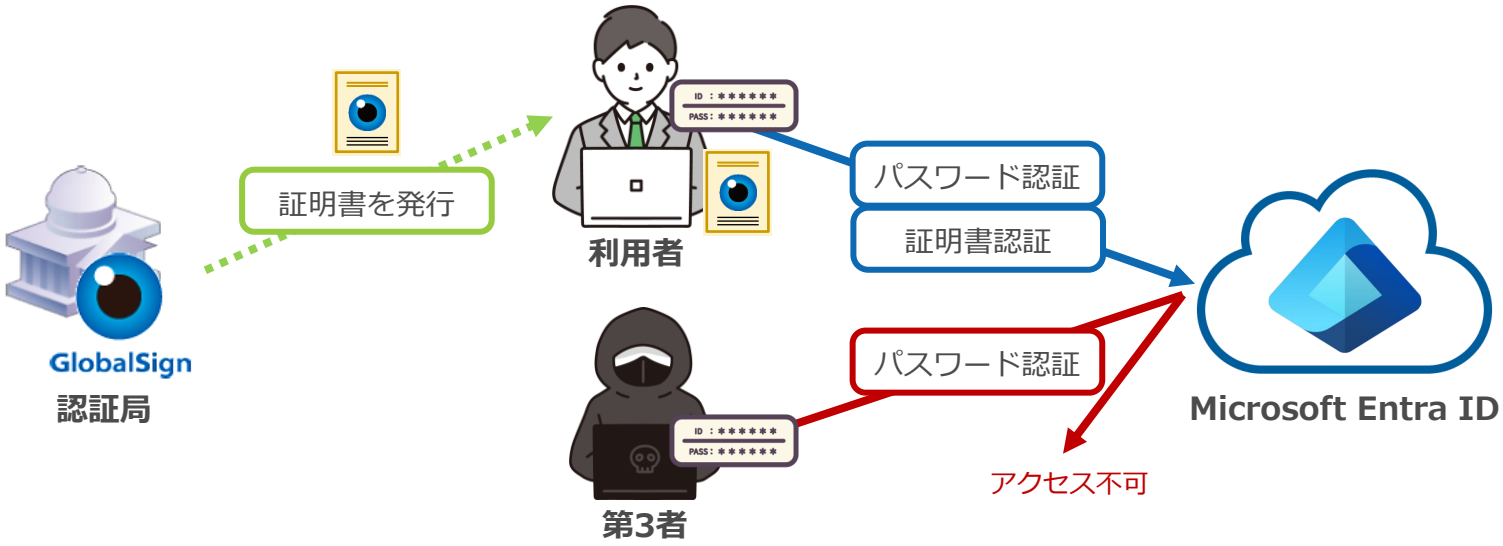
Entra IDへの不正アクセスを狙った攻撃やその被害が増加中
＝フィッシング耐性のある認証強化が必要。

クライアント証明書のメリット

クライアント証明書とは

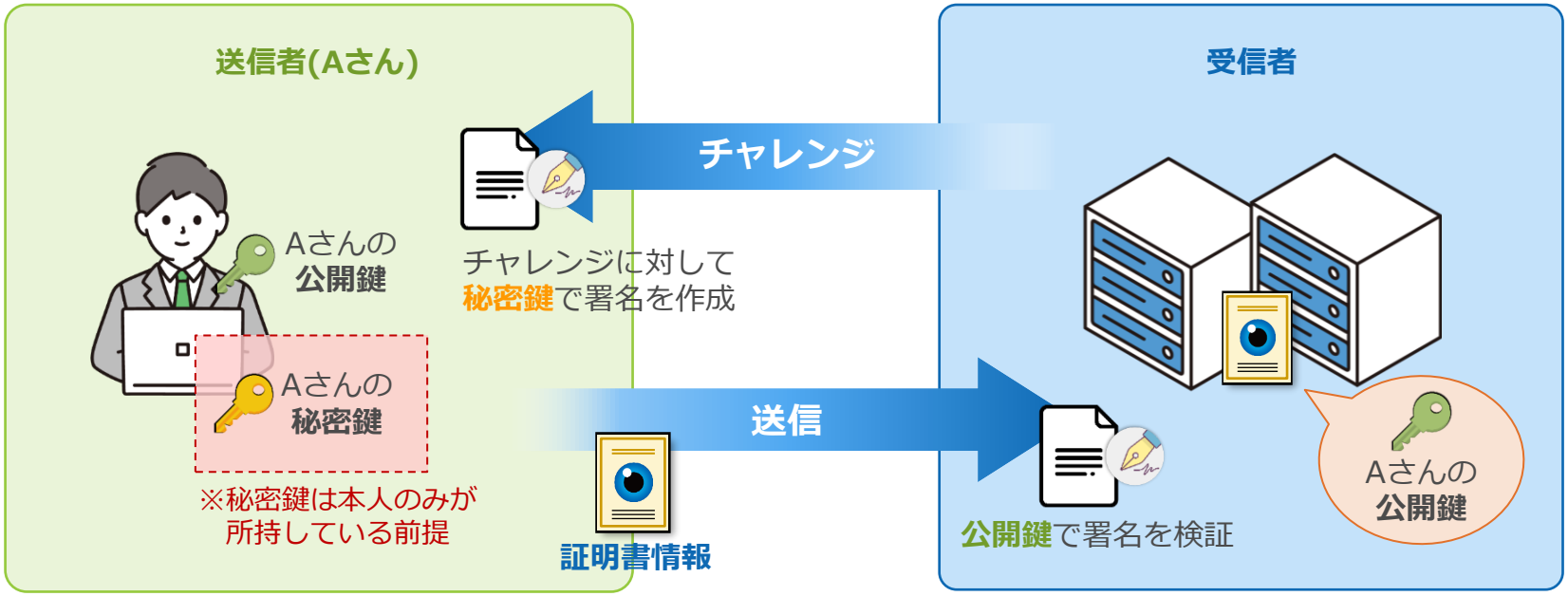
クライアント側（PC・モバイル端末）に
インストールする電子証明書の一般名称 ▶ **クライアント証明書**

1. フィッシング耐性のある **パスワードレス認証**
2. パスワード認証との組み合わせによる **多要素認証**
3. 証明書がある端末のみアクセス可能な **アクセスコントロール**



パスワードレス認証

公開鍵暗号方式を使用しているため、パスワードに依存しないことから、フィッシング耐性のあるセキュアな認証になります。また、認証時は証明書を選択するのみなので、ユーザの利便性も向上します。



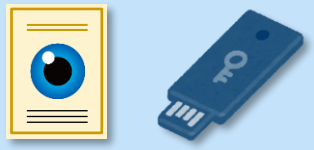
多要素認証に対応

クライアント証明書は所持情報にあたります。そのため、パスワード認証や生体認証などと組み合わせることで多要素認証に対応することができます。

知識情報

- ✓ パスワード
- ✓ PINコード
- ✓ 秘密の質問

所持情報



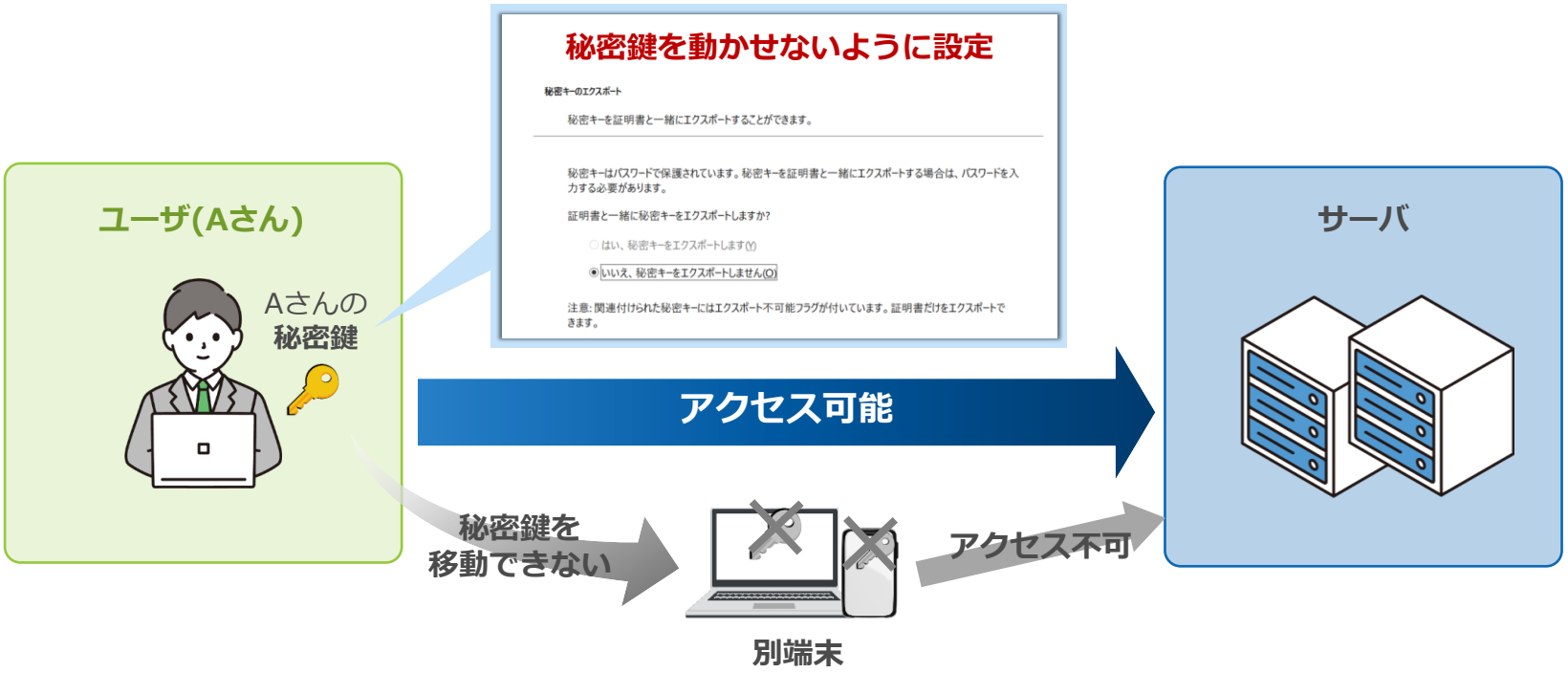
- ✓ クライアント証明書
- ✓ ハードウェアトークン
- ✓ 携帯

生体情報

- ✓ 指紋
- ✓ 静脈
- ✓ 虹彩

アクセス可能な端末を制限

証明書認証は、証明書の秘密鍵を持つ端末から出ないとアクセスできません。そのため、秘密鍵を持つ端末を制限することで、アクセス可能な端末を制限できます。



証明書ベースの認証（CBA）とは

証明書利用のハードルが大幅にダウン

Entra ID単体で証明書認証が可能。CBAの利用で、追加の費用は発生しません。

[Tips] CBA実装前にクライアント証明書を利用した場合

Entra IDのみではクライアント証明書認証は出来ず、通常のADとは別に、ADFS用のサーバ構築も推奨されており、コストがかかりました。

Microsoft Entra CBAの設定概要

01 **認証局証明書の登録**

Entra IDにグローバルサインのルート証明書・中間CA証明書を登録します。

02 **CBAの有効化**

証明書ベースの認証の有効化を行います。
対象のユーザの設定や、証明書とユーザを紐づける情報を設定します。

03 **条件付きアクセスの設定**

認証ポリシーを適用する対象の、デバイスやアプリケーション、
ネットワークの種類などを設定します。

※詳細なポリシー設定は出来ませんが、条件付きアクセスがないプランの場合もCBAの設定は可能です。

04 **証明書認証が可能**

多要素認証の場合は、IDPWの入力と合わせて証明書認証が求められ、
1要素のパスワードレス認証の場合、証明書認証のみでアクセスできます。

GMOグローバルサイン
カレッジ

パスワードレス認証
（クライアント証明書認証のみ）

多要素認証
（IDPW＋クライアント証明書）

※画像クリックで該当ブログ記事へ遷移します。

解説ウェビナーオンデマンド

2023年12月開催

- ✓ Microsoft Entra IDの概要
- ✓ クライアント証明書がセキュアな理由
- ✓ CBA（証明書ベースの認証）とは

2024年10月開催

- ✓ Microsoft Entra IDへの攻撃の最新情報
- ✓ 多要素認証の各認証方法の比較
- ✓ 具体的なCBAの設定方法

その他クライアント証明書関連のウェビナーも公開中！ 詳細はこちら

※サムネイル画像クリックで該当動画のYoutubeへ遷移します。

まとめ

まとめ

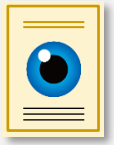
不正アクセスによる情報漏えい事故が増加している昨今、利用者数が多く、社内の様々なリソースにアクセスできる**Microsoft Entra IDは、非常に狙われており、突破されやすいID・パスワードのみの認証では危険な状態**といえます。

そこで、認証強化による不正アクセス対策を行う場合、**クライアント証明書は、フィッシング耐性のあるユーザビリティの高い認証方法**になっております。自社のセキュリティ強化として、クライアント証明書にご興味がございましたらお気軽にお問い合わせください。

サービスカタログや解説資料など無料公開中！

ダウンロードはこちら

Entra IDでも検証可能なテスト用証明書 無償提供中！



お申し込みはこちら

※ 証明書の配布までに1営業日前後いただきます。

クライアント証明書に関するお問い合わせ

03-4545-2300 （受付時間 平日10:00-18:00）

https://jp.globalsign.com/contact/mpki/

GMOグローバルサイン株式会社

〒150-0043
東京都渋谷区道玄坂1-2-3　渋谷フクラス
https://jp.globalsign.com/