CLOUDFLARE

ソリューション概説

強力な認証がフィッシング攻撃阻止にどのように役立つか

セキュリティキーとZero Trustのアプローチでフィッシング詐欺師の阻止が可能

フィッシングがもたらす脅威

データの紛失、安全性が損なわれたネットワーク、盗まれたアカウント

標的型フィッシング攻撃は、今日組織が直面する最も危険な脅威ベクトルのひとつです。フィッシング攻撃やソーシャルエンジニアリング攻撃は、機密情報を引き出したり、アクセスするためにユーザーを操作することに狙いを定めています。標的になりやすいのは、ログイン認証情報です。

そうした攻撃が成功すると、次のようなことをもたらす可能性があります。

- アカウントの乗っ取り
- より大きなサプライチェーン攻撃へのつながり
- PIIやIPなどのデータ流出
- ランサムウェアなどのマルウェア攻撃

幸いにも、フィッシングのリスクを軽減するための非常に効果的なソリューションがあります。重要なもののひとつが、多要素認証（MFA）です。

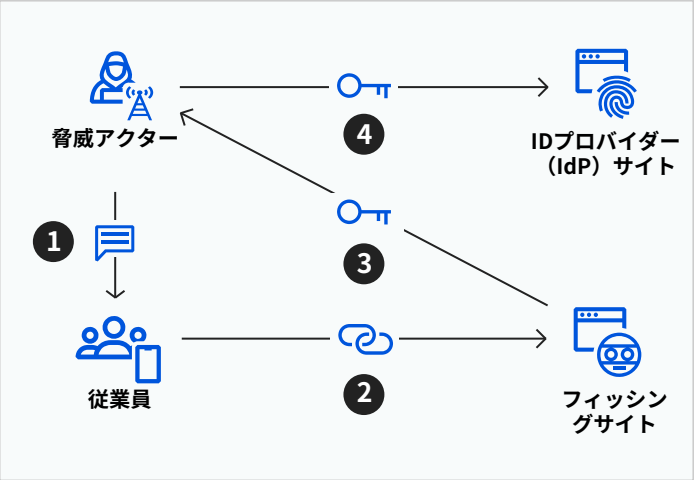


図1：SMSフィッシング攻撃の構造。1. 正当に見せかけたテキストメッセージを送信する。2. 正当に見せかけたサイトへリンクする。3. 被害者の資格情報と時間ベースのワンタイムパスコードがリアルタイムで転送される。4. 実在の企業IdPサイトにログインする。

多要素認証（MFA）がフィッシング阻止にどのように役立つか

パスワード盗難を無効にするMFA

MFAでは、ユーザーはログイン時にユーザー名とパスワードの他にキーを提示する必要があります。このキーなしでは、ユーザーは自分のアカウントにアクセスできず、攻撃者もアクセスできません。

ソフトキーを使用したMFA

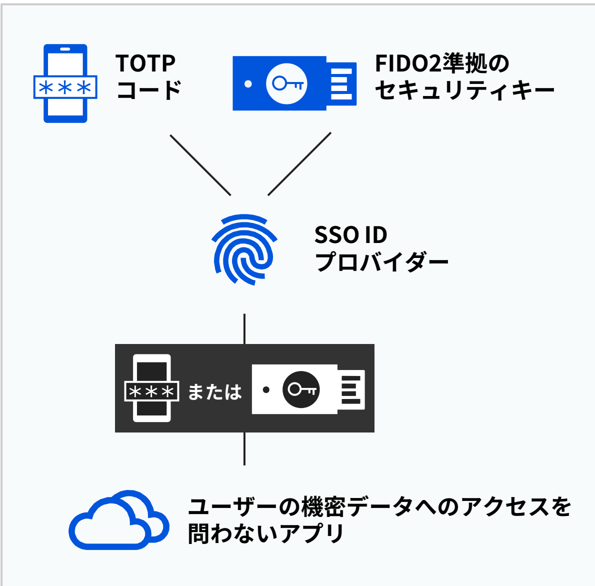
一般的なMFAの実装は、時間ベースのワンタイムパスコード（TOTP）のようなソフトキーを使用することです。多くの場合、TOTPはSMSメッセージ、メールまたはアプリ経由で発行されます。単一要素認証よりは安全ですが、ソフトキーは攻撃者に傍受される場合があります。

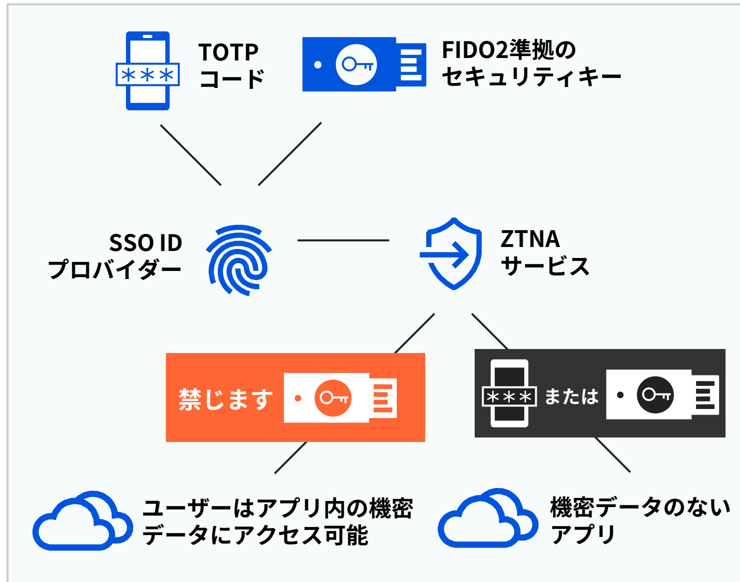
セキュリティキーを使用したMFA

FIDO2準拠のセキュリティキーが一度発行されると、攻撃者は傍受することができず、物理的なアクセスなしで盗むことはほぼ不可能です。Googleによる調査では、FIDO2/U2F準拠のセキュリティキーの使用で、アカウントの乗っ取り行為を100%ブロックすることが分かっています。[1]

強力な認証を選択的に実施

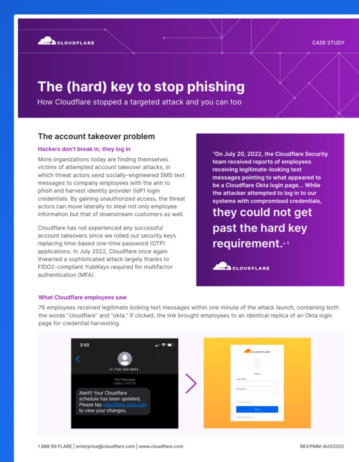
一部のIAMソリューションは強力な認証をサポートしているかもしれませんが、管理者が本当にそれを必要としても許可しない可能性があります。ZTNAを使用することで、特に機密データを格納するアプリでFIDO2認証の必要性を確保できます。Cloudflareでは、すべての認証にセキュリティキーMFAを必要としており、これにより当社のセキュリティ体制は大幅に強化されました。





「2022年7月20日、Cloudflareセキュリティチームに、Cloudflare Oktaのログインページらしきページに誘導する正当そうなテキストメッセージを従業員が受け取ったという通報がありました...しかし一方で攻撃者は漏洩した認証情報で当社のシステムにログインしようとしましたが、彼らは物理キーの要件をクリアすることができませんでした。」[2]

CLOUDFLARE


CLOUDFLARE CASE STUDY

The (hard) key to stop phishing

How Cloudflare stopped a targeted attack and you can too

The account takeover problem

Hackers don't break in, they log in

More organizations today are finding themselves victims of attempted account takeover attacks, in which threat actors send socially-engineered SMS text messages to company employees with the aim to phish and harvest identity provider (IdP) login credentials. By gaining unauthorized access, the threat actors can move laterally to steal not only employee information but that of downstream customers as well.

Cloudflare has not experienced any successful account takeovers since we rolled out security keys replacing time-based one-time password (OTP) applications. In July 2022, Cloudflare once again thwarted a sophisticated attack largely thanks to FIDO2-compliant YubiKeys required for multifactor authentication (MFA).

"On July 20, 2022, the Cloudflare Security team received reports of employees receiving legitimate-looking text messages pointing to what appeared to be a Cloudflare Okta login page... While the attacker attempted to log in to our systems with compromised credentials, they could not get past the hard key requirement."[1]

CLOUDFLARE

What Cloudflare employees saw

76 employees received legitimate looking text messages within one minute of the attack launch, containing both the words "cloudflare" and "okta." If clicked, the link brought employees to an identical replica of an Okta login page for credential harvesting.

1 888 99 FLARE | enterprise@cloudflare.com | www.cloudflare.com REV:PMM-AUG2022

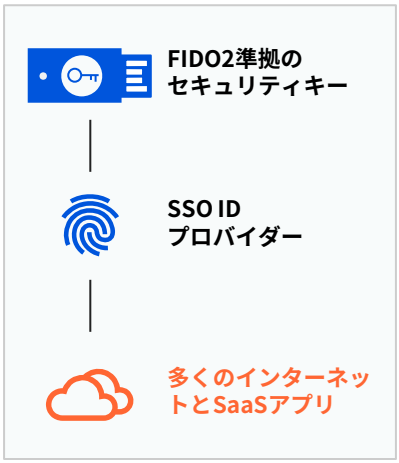
強力な認証をあらゆる場所に展開

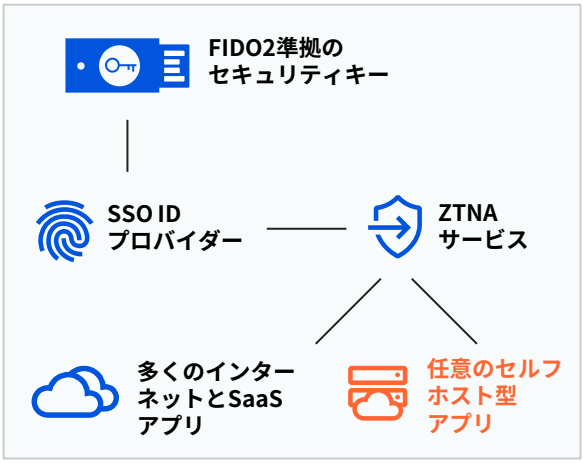
全アプリでFIDO2準拠のMFA

特にシングルサインオン（SSO）サービスが使用されている時に、従来のあらゆる方法でクラウドサービスへのMFAの実施が可能です。しかし、従来のアプリや非Webアプリではこのような認証をネイティブにサポートしていないことが多く、難しい場合があります。

ZTNAでロールアウトを簡素化

Zero Trustネットワークアクセス（ZTNA）は、すべてのリソースのアグリゲーション層として機能し、各リソースに対して厳格な認証ポリシーを有効にします。SaaS、セルフホスト型および非Webアプリケーションも同様にZTNAの背後に位置することが可能で、これによりすべてのアプリケーションで強力な認証が容易に実施できるようになります。





強力な認証を実装する組織への重要ポイント

1

IAMを一元化

すべてのアプリでMFAをより簡単に実装するために、IDとアクセス管理（IAM）を一元化します。

2

MFAを選択的に実施

IDとコンテキストに基づき、MFAオプション（TOTPとFIDO2、またはFIDO2のみ）の選択的な実施を確立します。

3

モバイル端末をサポート

ノートパソコン、デスクトップコンピューター、サーバーおよびモバイル端末向けにFIDO2ソリューションを発行します。

Zero Trustのロードマップを加速させる

アーキテクチャワークショップを依頼する

評価にまだ躊躇していますか？

無料お試しを申し込む。

1. krebsonsecurity.com/2018/07/google-security-keys-neutralized-employee-phishing/
2. 2022年8月9日のCloudflareのブログ投稿、「巧妙なフィッシング詐欺の仕組みとそれを阻止した方法」、blog.cloudflare.com/2022-07-sms-phishing-attacks/