yubico

金融サービス業界のサイバーセキュリティリスクを軽減する強固な認証

サイバー攻撃に常に晒される金融サービス業界

金融サービス業界はサイバー攻撃者の格好のターゲットとなっており、金融サービス全体でのデータ侵害のコストは平均597万ドルに上ります。金融サービス企業の従業員はIDフィッシングの脅威にさらされ、顧客はオンラインバンキングやモバイルバンキングに関連するアカウント乗っ取りの脅威に直面しています。

リモートワークとハイブリッドワークの長期的な増加により、セキュリティ境界が拡大し、企業全体のフィッシング攻撃の問題が悪化しました。安全対策が施されていないホームネットワーク、さらに企業のネットワークに接続した個人用デバイスは、攻撃者のターゲットをさらに広げています。

金融サービス業界は、SMS、OTP、プッシュ通知などのモバイルベースの認証を早くから採用していましたが、これらの認証形式はユーザー名とパスワードの認証に似ており、フィッシングやアカウントの乗っ取りを防ぐことはできません。パスワードは簡単に侵害され、セキュリティの質問、SMSコード、OTP、プッシュ通知を使った耐フィッシングMFAは、フィッシング攻撃、SIMスワップ、中間者（MitM）攻撃を受けやすい認証です。パスワードとモバイル認証も、ユーザーにとって負担となります。

強固な認証は、保護対象が企業の資産か顧客の資産かに関係なく、金融サービス企業にとって強力な防御の最前線となります。

強固な認証に必要な2つの特性

- どの段階でも、共有秘密鍵プロセスまたはプロトコル（対称鍵）だけに頼ることはありません。パスワード、OTP、SMSコード、パスワードをリセットするための質問などもそうです。
- 資格情報のフィッシング、MitM、なりすましを確実に撃退します。強固な認証では、一部の攻撃がエンドユーザーに到達することを前提としており、認証メカニズムによって攻撃を阻止します。

さまざまな認証プロトコルの中で、強固な認証はスマートカード、最新のFIDO U2F、FIDO2/WebAuthnプロトコルに限定されます。セキュリティに加えて、実用性、移植性、スケーラビリティを考慮することも重要です。

YubiKeyを導入し、セキュリティと実用性を向上

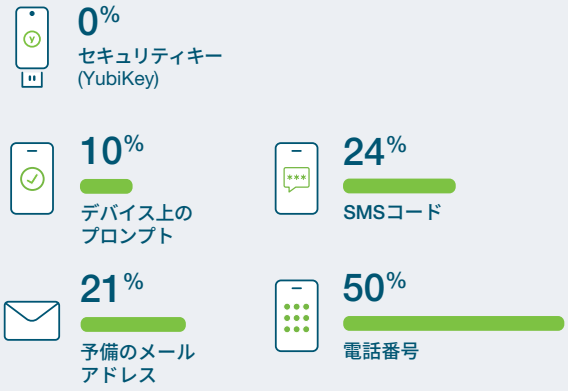
Yubicoでは、企業全体のIDフィッシングや顧客アカウント乗っ取りを減らすことを目的に、価格が手頃で使いやすい2要素認証、多要素認証、パスワードレス認証を実現するYubiKeyを提供しています。

YubiKeyにより、金融機関は次のことが可能になります。

- 優れたハードウェア暗号化セキュリティにより、アカウント乗っ取りを阻止し、中間者攻撃を防ぐ。
- 認証時間が4倍速くなり、簡単にプレゼンスと所有を証明できるため、これまでになく簡単にログインできる。
- SOX、PSD2、PCI、FIPS、GDPR、CFPB Circular 2022-04など、従来および新規の規制に準拠できる。
- パスワードのリセットに関連するITサポートコストを削減できる。
- 業界をリードする世界的な認証規格のパイオニアが提供する信頼性の高いソリューションは、ユーザーに信頼感と安心感を与える。

YubiKeyは、独立調査機関によって、アカウント乗っ取りに対して最高レベルのセキュリティを提供し、標的型攻撃を防止することが証明されています。

アカウント乗っ取りのリスク



実際にあった35万件の乗っ取りの試みを基にGoogle、NYU、UCSDが調査した結果。上記の結果は標的型攻撃の割合。

金融業界によくあるYubiKeyの使用例

1. リモートワーカーとハイブリッドワーカーの保護

強固な多要素認証（MFA）は、リモートワークとハイブリッドワークのポリシーに設定すべき重要な要件の1つです。YubiKeyは確実な多要素認証を実現し、Microsoft、Okta、Duo、Pingなど、IDやアクセス管理システムを含む、既存のシステムやインフラストラクチャに簡単に取り入れることができます。YubiKeyを使用すると、金融サービス企業のリモートワーカーやハイブリッドワーカーは、どこで働いていても、コンピュータ、VPN（仮想プライベートネットワーク）、パスワードマネージャーを安全に利用できます。YubiKeyは、1回限りのパスコードを安全に生成するために使用することもできます。

2. 高リスク、高価値の取引の保護

高リスクで価値の高い取引を日常的に行う従業員は、サイバー犯罪者のターゲットになることが少なくありません。高リスクシステムへのアクセスは、YubiKeyを使用した最新の強固なMFAを導入して強化できます。承認済みアカウントにアクセスを限定し、権限を与えられた高価値の取引のみ行えるようにします。

3. 特権ユーザーの保護

特権ユーザーは、企業や顧客の機密情報へのアクセスが増えるため、サイバー犯罪者の主要なターゲットとなります。金融サービス企業は、認証セキュリティのベストプラクティスに従い、YubiKeyなどの耐フィッシングハードウェアセキュリティキーを使用した認証を特権ユーザーに義務づけることで、特権アクセス管理を強化し、標的型攻撃を阻止できます。

4. コールセンタースタッフの保護

従業員の離職率が高く、季節的なピークが発生し、その他困難なビジネス情勢に左右されるコールセンター環境では、重要なシステムやデータへのアクセス権を付与する前に、エージェントの身元を検証する安全でシンプルなアプローチが求められます。YubiKeyは、PIIやその他の機密データへのアクセス権を付与する、クレジット限度額の引き上げなど顧客アカウントに変更を加えるなどの作業をする前に、コールセンターのエージェントの本人確認を確実に行う強固なセキュリティを実現します。顧客データや財務データの画像を撮影できる携帯電話とは異なり、はるかに安全な認証ソリューションです。

5. 共有ワークステーション/端末の保護

共有ワークステーションで行員や従業員が作業するのは、銀行やコールセンターでは一般的です。窓口係はステーション間を移動し、スーパーバイザは取引を承認するために移動します。多くの場合、このような環境のユーザーは離職率の高いパートタイムの従業員であり、会社に対する責任感が非常に弱いため、内部脅威が増します。YubiKeyは、共有アクセス端末と共有ワークステーションに強固な認証を実装し、価値の高いシステムやリソースへの不正アクセスを防止します。

6. 富裕層顧客の保護

YubiKeyは、ユーザー名とパスワード、SMS、OTPコードと比較して、富裕層顧客のオンラインバンキングやモバイルバンキング用アカウントをアカウント乗っ取りから保護する極めて強固なセキュリティを実現します。金融サービス企業は、使いやすい強固な認証を顧客に提供することで、新規顧客の獲得件数を増やし、顧客の定着を促すことができます。YubiKeyのサポートは、オンラインバンキングやモバイルバンキングに簡単に取り入れることができます。VanguardやMorgan Stanleyなどの金融サービス企業は、ハードウェアセキュリティキーをサポートする優れた認証ソリューションを提供しています。

調達や広範囲への配布が容易なYubiKeyの認証ソリューション

Yubicoでは、500人以上のユーザーを抱える組織や、従来型の突破されやすいMFAをやめ、短期間で耐フィッシング認証を大規模導入したい組織に役立つ、柔軟で費用対効果の高い企業向けプランをご用意しています。

YubiEnterpriseサブスクリプションを選択すると、予測可能なOPEXモデルを活用できることはもちろん、ユーザーの好みに合わせて柔軟にYubiKeyを選べるだけでなく、最新のYubiKeyにアップグレードでき、すぐに展開することができます。また、導入サービスや優先サポートも利用でき、専任のカスタマーサクセスマネージャーにも相談できます。

また、サブスクリプション契約を結んでいるお客様は、YubiEnterprise Delivery（49ヵ国の家庭やオフィスで利用されているグローバルなターンキーハードウェアキー配布サービス）など、さまざまな追加サービスや製品を購入することもできます。

信頼できる認証リーダー

Yubicoは、FIDOアライアンスに採用されているWebAuthn/FIDO2およびU2F認証規格の主要な発明者であり、U2Fセキュリティキーとマルチプロトコル FIDO2認証器を製造した最初の企業です。

YubiKeyは、米国とスウェーデンで製造されており、製造プロセス全体のセキュリティと品質管理が維持されています。

YubiKey 5シリーズ

左から右：YubiKey 5 NFC、YubiKey 5C NFC、YubiKey 5Ci、YubiKey 5C、YubiKey 5 Nano、YubiKey 5C Nano

お問合せ
yubi.co/contact-ja

詳細情報
yubi.co/yk5

[1] IBM Cost of a Data Breach Report 2022