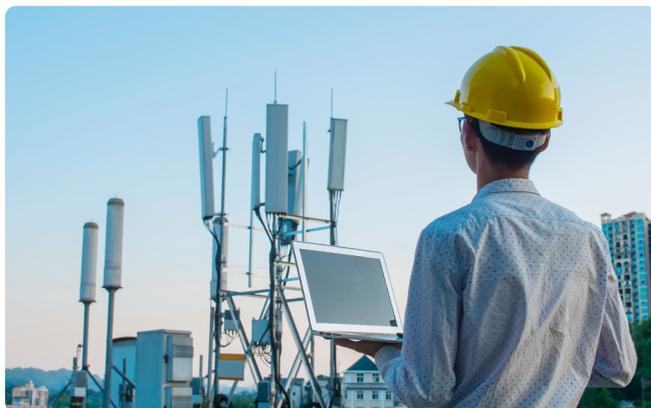


# 通信会社向け耐フィッシング二要素認証

YubiKeyの最新セキュリティにより、既存のセキュリティアプローチを強化



## 最新セキュリティを導入する必要性が差し迫っている

デジタルドリブンデジタルドリブン駆動型で常時接続された今日の世界において、電気通信事業者は、消費者や企業が大きく依存する重要なインフラストラクチャです。SpyCloudが2021年に発表した『Telecommunications Industry Credential Exposure』レポートにより、企業1社あたりで見た無防備な状態の資産に関して、通信事業者は、リスクの高い業界（金融、テクノロジー、医療、防衛）を含む他のどの業界よりも上回っていることがわかりました。この業界の脆弱性の大きな原因は、複数のアカウント間でのパスワード再利用率が高いことにあり、アカウント乗っ取りやデータ侵害の主な原因は、資格情報の盗難です。侵害はコストがかかるだけでなく、ブランドの評判や顧客ロイヤリティを大きく損なうおそれがあります。

高度化し続けるサイバー攻撃から保護するには、強固な多要素認証（MFA）を総合的なセキュリティ戦略の基礎とする必要があります。そうすることで、認証されていない人物やデバイスがネットワークに侵入することができなくなります。とはいえ、すべての多要素認証が同じように作られているわけではありません。ユーザー名やパスワードなど従来の認証方法は、容易にハッキングされるおそれがあります。セキュリティの質に加えて、認証ソリューションの実用性、移植性、スケーラビリティを考慮することも重要です。それを怠ると、多要素認証に弱点が生まれ、ユーザーへの定着率が低下し、侵害リスクも高まります。

## 人、テクノロジー、データをYubiKeyで保護

Yubicoは、最新のサイバー脅威を防ぐ手段として、耐フィッシングMFA（2FA）、多要素認証、パスワードレス認証の大規模導入を実現するハードウェアセキュリティキー、YubiKeyを提供しています。YubiKeyは、アカウント乗っ取りを完全に阻止することが独立調査機関によって証明されている唯一のソリューションです。通信会社がサイバー脅威から従業員と顧客を保護するとともに、規制コンプライアンスを推進します。

この最新セキュリティソリューションは、既存のセキュリティアプローチを強化します。モバイルベースのMFAを使用している場合は、YubiKeyを導入することでフィッシング耐性の高い保護層を追加できます。YubiKeyは、幅広い事業シナリオに対応し、最高水準のセキュリティとユーザーエクスペリエンスを実現します。セルフサービスのパスワードリセットも可能で、ITサポートコストを大幅に削減できます。YubiKeyは導入と使用が簡単で、1本のYubiKeyを新旧両方のアプリケーション、サービス、デバイスで使用できます。1つのキーでスマートカード/PIV、OTP、OpenPGP、FIDO U2F、FIDO2/WebAuthnの複数プロトコルをサポートします。ここからは、YubiKeyが最新のサイバー脅威から通信会社を保護する5つの方法を紹介いたします。

### 1. 重要なシステムとデータへの安全なアクセスを幅広いユーザーベースに提供

重要なシステムとデータへの安全なアクセスを幅広いユーザーベースに提供社内やリモートのナレッジワーカーや経営幹部、または店内の従業員とそのアカウントのセキュリティを強化することは、強固な最新認証プロセスを確立するうえ重要な第一歩です。生産性を低下させることなく、従業員が重要なシステム、アプリケーション、従業員と顧客の個人情報（PII）にアクセスできるようにすることは、最新のサイバー脅威から身を守るために欠かせません。YubiKeyは、許可されたユーザーのみPIIデータや重要システムにアクセスできるようにします。Microsoft、Okta、Duo、Pingなどの既存のIAMソリューションとシームレスに統合し、数百ものアプリケーションやサービスに対して安全な認証を提供し、既存のソリューションのリッピングや置き換えを阻止します。ユーザーは複雑な設定をせずにすぐに保護されます。

## 通信業界で従来使用されている認証の影響

\*\*\*\*\* 76%

通信会社の従業員のパスワード再利用率<sup>1</sup>

\*\*\*\*\* 82%

人為的要素による社会的攻撃、ミス、不正使用、資格情報の盗難に関連する侵害の割合<sup>2</sup>

💰 491万ドル以上

最初の攻撃としてフィッシングによるデータ侵害が発生した場合の平均コスト<sup>3</sup>

<sup>1</sup> Spycload, 2021 Special Report Telecommunications Industry Credential Exposure

<sup>2</sup> Verizon, 2022 Data Breach Investigations Report

<sup>3</sup> IBM, Cost of a Data Breach Report 2022

<sup>4</sup> Google, How effective is basic account hygiene at preventing account takeovers

## 2. 顧客サービスの品質を向上

サードパーティ、加盟店、小売店の従業員は、顧客と接する際に企業のブランドを直接反映する存在です。YubiKeyを使用すると、従業員は認証のために電話を見る必要がないため、顧客サービスを効率化できます。ユーザー認証に必要な操作は、YubiKeyをタップするだけ、または差し込んでタッチするだけです。YubiKeyは、USB-A、USB-C、NFC、Lightningポートの対応を含めさまざまなフォームファクタがあるため、メーカーやオペレーティングシステムに関係なくどの最新デバイスでも簡単に認証を行うことができます。さらに、NFC機能を備えたYubiKeyは、リストバンドやストラップなどのウェアラブルと組み合わせると、迅速かつ簡単な認証を実現するうえで明らかに効果があります。

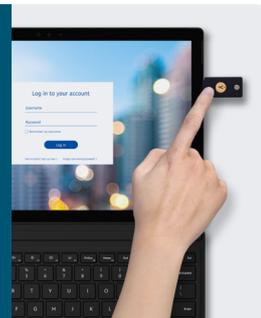
## 3. 共有ワークステーションを保護

実店舗の従業員は、コンピュータ、キオスク端末、POSシステムを共有することが少なくありません。そのため、スピード、使いやすさ、信頼性を考慮し、各従業員を明確に区別する、合理化された認証方法が必要です。YubiKeyは独自に関連付けることができ、移植性が非常に高いため、特定のシステム、アプリケーション、機能へのアクセス権限を持つ人物だけがアクセスできるようになります。慎重なアクセスポリシーを実装すれば、外部のサイバー脅威だけでなく内部の脅威からも組織を守ることができます。

## 4. モバイルが制限された環境に最新MFAを導入

携帯電話に適していない環境では、弱い形式の認証をデフォルトで使用しないでください。モバイルが制限された環境のコールセンターやデバイスには、安全性が高く、コンプライアンス基準に沿った、使いやすい認証が必要です。YubiKeyは、携帯電話を使用できない、または使用しない場合にお勧めの安全な認証です。

YubiKeyは、常に利用可能な耐フィッシング認証を実現します。バッテリーやインターネット接続を必要とせず、耐久性、耐衝撃性、耐水性に優れています。遠隔地にサービスを提供する技術者も、安全なMFAをいつでもすぐに利用できます。



## 5. 業界規制や認証規格へのコンプライアンスを推進

2022年1月、米国連邦通信委員会 (FCC) は、通信業界に新しい規則を提案しました。その内容は、顧客に侵害を通知する際に義務づけられていた7営業日の待機期間をなくし、消費者保護を拡大し、通信事業者に対し主要組織への通知を義務づけるというものです。この目的は、進化する侵害とその影響に対応することです。さらに、行政管理予算局 (OMB) の覚書 (M-22-09) が発表され、州、地域、企業の各レベルでサイバーセキュリティを強化することを目指す大統領令を受けて、実行可能なさまざまな戦略を示しました。

## 調達や広範囲への配布が容易なYubiKey

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、短期間でフィッシング耐性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  
Subscription



YubiEnterprise  
Delivery

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カ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。

Yubicoのプロフェッショナルサービスチームは、YubiKeyの実装と展開を合理化し、お客様のニーズに応じたサービスを提供します。

## YubiKeyは耐フィッシングMFAの最高水準

YubiKeyは、MFAへの取り組みがどのような段階であっても、パスワードのない未来への架け橋となります。既存のOTP認証を活用しつつ、FIDO2またはスマートカードを使用した最新の耐フィッシング認証を1つのキーで導入できます。YubiKeyは、将来を見据えたセキュリティ対策であり、従業員は卓越したサービス品質を提供することに集中できます。安心してYubiKeyを導入してください。アカウント乗っ取りを防ぐ優れたソリューションです。

YubiKeyを使用して通信業界におけるサイバーセキュリティのリーダーになるために、今すぐYubicoの営業担当者にお問い合わせください



## YubiKeyファミリ

YubiKeyは、デスクトップ、ノートパソコン、モバイルデバイス向けに複数のフォームファクタで提供されています。



お問い合わせ  
yubi.co/contact-ja



詳細情報  
yubi.co/yk5

※北米以外のお客様は、地域のYubico担当者に詳細をお問い合わせください