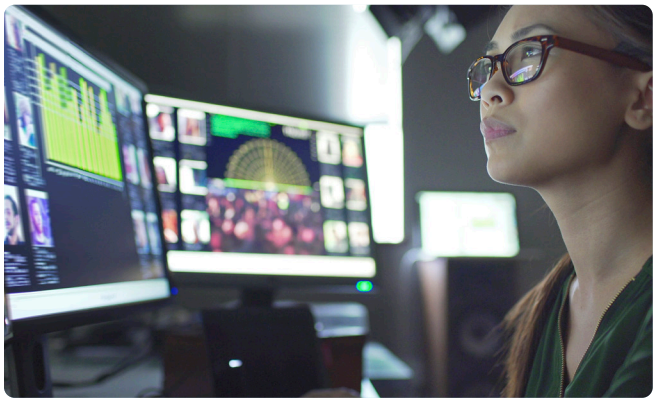
yubico



モバイル制限環境を最大限に保護する方法

モバイル制限環境とは何ですか？モバイル制限環境には何か固有の要件がありますか？

「モバイル制限」とは、セキュリティ上の理由で、モバイルデバイスが許可されない、信頼されない、または制限を受ける、機密性の高い環境を指します。ほとんどすべての組織には、モバイルデバイスの使用が許可されない、または不可能なケースがあります。また、最近ニュースで取り上げられているようにサイバー犯罪が頻発しているため、セキュリティチームは、機密性の高いワークスペースを保護する方法について、より戦略的に考えることを迫られています。

モバイル制限環境は、このような環境をホスティングしているさまざまな分野や産業、そして携帯電話がセキュリティ上の懸念として制限されている場所で見られます。このような環境は、金融サービス、製造、小売、接客などのさまざまな産業に加え、コールセンターなど、あらゆる産業に存在する特定の作業環境にも存在します。「モバイル制限」という概念は、接続の問題がコラボレーションや生産性の阻害要因になり得る環境にも適用される場合があります。たとえば、エネルギー資源や天然資源など、携帯の電波が届かない遠隔地で作業が行われるような場合です。このようなシナリオではいずれの場合も、モバイル認証などの従来の多要素認証（MFA）を使用したユーザーの認証は使用できません。そのため、組織では、機密性の高いリソースへのアクセスを許可する前に、ユーザーを安全に認証するための最新かつ効果的な方法を探す必要があります。

理想的な MFA ソリューションを選択する際に考慮すべき重要事項

モバイル制限環境で使われる認証ソリューションは、必ずセキュリティと使いやすさという 2 つの間でバランスを取る必要があります。このバランスがどこで安定するかは、ユーザーアクセスのニーズ、特定の産業の要件や標準など、現場の条件次第で変わります。しかし、一般的な指針としては、ユーザーが手順を無視したり、近道を探し始めたりせずにどのくらい「面倒な要因」に耐えられるかを吟味することが重要です。

以下をチェックリストとして、採用を検討している認証ソリューションがモバイル制限シナリオの重要な要件を満たしているかどうかを確認してください。

共有ワークステーションに適合

モバイル制限環境には、共有ワークステーションが含まれることが多く、これらのワークステーションにはログインとログアウトに特別な要件がある場合があります。これまで、このような環境では、企業は物理的なセキュリティ手順に依存してきましたが、セキュリティをより強固にするため、フィッシング耐性のある認証でワークステーション上でも物理プロトコルを補完する必要があります。

携帯回線を必要としない高耐久デバイスの提供

屋外や遠隔地の作業現場のセキュリティデバイスは、物理的な衝撃や気象条件に耐える必要があります。一般的なオフィスでも、デバイスを落としたり、不注意で飲み物をかけてしまったりと、デバイスへの負担は大きいものです。高耐久デバイスは、携帯回線を使用せずにあらゆる状況で動作し、オフラインまたはネットワーク上で動作している各種のコンピュータやその他の端末を保護できるものでなければなりません

使いやすいユーザーエクスペリエンス

ソリューションを探す際に、ユーザーが見過ごされることがよくあります。ユーザー調査のフィードバックに目を通し、社内展開チームに優秀なライターやコミュニケーターを見つけ、ユーザーに十分な事前準備をさせるようにしましょう。システムを使用可能にすることは、システムを安全にすることと同じくらい重要です。なぜなら、どちらか一方だけではシステムが成立しないからです。

複雑な環境のサポート

ほとんどのサイトに適合する汎用ソリューションはありません。ソリューションを既存の環境に簡単に適合させる必要がある場合は、さまざまなプロトコルを考慮する必要があります。組織が、主にオンプレミスのインフラストラクチャを使用しているモバイル制限環境のセキュリティをモダナイゼーションしようとしている場

YubiKeyの導入実績：

大手テクノロジー企業	米国の銀行	国際的な小売店
10社中9社	**10社中4社**	**10社中5社**

合、スマートカードベースのセキュリティアプローチを選択するかもしれません。一方、主にクラウドベースの環境を使用している場合は、FIDOベースのアプローチを検討するかもしれません。パスワードレス認証に移行しようとしている場合は、将来に対応するためのセキュリティ戦略として、スマートカードによるパスワードレスシナリオとFIDOによるパスワードレスシナリオの両方に対応できるソリューションを選択する必要があります。

強力なセキュリティの提供

ソリューションには、その認証メカニズム自体に対する高い信頼性が必要です。高い信頼性は、ベンダーが安全なサプライチェーンと製造プロセスを持っていることを確認することによって得られます。ベンダーのセキュリティチームがサプライチェーン全体で強力なセキュリティを実現し、適切なコード署名プロトコルに従っていれば、少しは安心できます。さらに、攻撃者はますます大胆になり、ヒューマンエラーを悪用するシステムを工夫しているため、洗練された高度な攻撃に対するセーフティーネットを作ることが重要です。フィッシング対策や、ランサムウェアやマルウェアの攻撃から身を守るための認証など、悪意のあるイノベーションを先取りするソリューションが必要です。

将来のコンプライアンスと規制に対応可能

リーダーは常に将来のコンプライアンス要件に目を光らせていなければなりません。今後はコンプライアンス規制の強化により、組織はモバイル制限環境を含むすべての環境で、フィッシング耐性のあるMFAアプローチへの移行が求められることになるでしょう。フィッシングに対して脆弱なOTPベースのアプローチから離脱し、フィッシング耐性が非常に優れているPIV（スマートカード）やFIDO2/WebAuthnベースのMFAアプローチが好まれるようになるでしょう。

2010年以来、YubiKeyは Googleの従業員を保護してきました

0	92%	4x	0
アカウント乗っ取り	サポートインシデントの減少	ログインのスピード	アカウントのロックアウト[1]

YubiKeyがモバイル制限環境に理想的なソリューションである理由

YubiKeyは、クライアントソフトウェアをインストールする必要がなく、バッテリーも必要ありません。モバイル制限環境で作業しているユーザーは、YubiKeyをUSBポートに接続してボタンをタップするか、NFCを使用してタップするだけでセキュア認証を行えます。YubiKeyには壊れるような画面はなく、携帯回線への接続が不要で、防水性と耐衝撃性があります（IP68等級）。このような特性はすべて、物理的な危険（工場の作業現場や屋外など）の可能性があるモバイル制限環境で役立ちます。

YubiKeyは、キー1つでOTP、OpenPGPなど複数の認証プロトコルをサポートします。また、スマートカード、FIDO U2F、FIDO2/WebAuthnなどの強力な認証プロトコルもサポートしています。レガシーのインフラストラクチャと最新のインフラストラクチャの両方に強力な認証を導入し、キー1つで利用できる柔軟性を備え、組織がパスワードレスに移行する過程のどの段階にあってもサポートします。

モバイル認証が選択肢にさえ入らない場合でも、汎用性に優れたYubiKeyは、常時認証が必須な、各種の機密環境やリモート作業環境でシームレスに動作します。

YubiKeyは、現代の新しい対面、ハイブリッド、リモートで働く従業員をサポートするために必要な利便性を提供します。モバイル制限エリアと未制限エリアの両方で使用できる便利さを備え、すべての環境で常に強力なフィッシング耐性のあるMFAアプローチを提供します。

まとめ

Yubicoは、モバイル制限環境で正しくバランスを取るため、最初にそのスペース固有のニーズを理解し、幅広い人材を結集して社内チームを設置し、要件（およびユーザーエクスペリエンスとフィードバック）をレビューしてから、信頼できるベンダーと協力して、生産性とセキュリティの両面で最適化されたソリューションを導入することをお勧めします。

OTPやデジタルトークンなどの従来のMFA手法には、攻撃を開始できる場面が多くあることがよく知られています。モバイル認証は、モバイル制限環境かどうかにかかわらず、どのような環境においても優れたソリューションとは言えません。ハードウェアベースのセキュリティキーは、モバイル制限環境で最高のソリューションを提供します。

お問合せ yubi.co/contact-ja

[1]「Google defends against account takeovers and reduces IT costs」Yubico