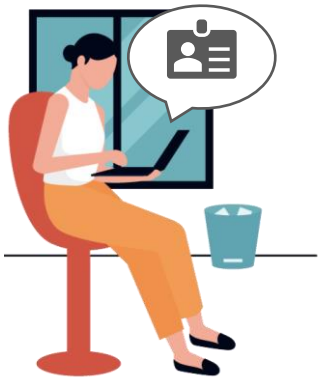
UserLock

セキュアなSSO（シングルサインオン）を実現する UserLockの新機能「UserLock SSO」③つのポイント

UserLockの新機能「UserLock SSO」

UserLock SSOを使用すると、ユーザーが既存のオンプレミスのActive Directoryに多要素認証も含めて一度ログインすれば、Microsoft 365やその他のクラウドアプリケーション、プラットフォームなどに、セキュアかつシームレスにアクセスすることができます。

▶ SSO（シングルサインオン）とは？



シングルサインオン（SSO）は、生産性を向上させる強力なツールです。SSOを使用すると、ユーザーは一度の認証で、オンプレミスだけでなく、クラウド上のアプリケーションにもアクセスすることが可能になるため、ユーザーエクスペリエンスは劇的に向上します。
ユーザーはWindowsにログインするだけで、設定されたすべてのアプリケーションを開くことができるようになりますが、SSOの利便性が高いほど、セキュリティのリスクも上がります。

▶ SSO（シングルサインオン）におけるセキュリティの注意点

一般的なSSOの機能はアクセスを制限することよりも、アクセスを提供することに長けているため、さまざまなメリットがある反面、多くのセキュリティリスクも生まれやすくなります。

⚠ エンドポイント以外もアクセス可能なってしまう

ログインの認証情報が流出するとSSOが導入されたアプリケーション、システム、データセットなど、すべてに自動的にアクセスすることができます。SSOがユーザーにとって素晴らしいものであることは、同時に危険なものでもあるのです。

⚠ 一度認証されたアクセスには制御が甘くなってしまう

もし攻撃者がエンドポイントへのアクセス権を入手した場合、導入されているSSOソリューションとリンク先のアプリケーションのセキュリティモデルによっては、アカウントを無効にしても攻撃者が特定のアプリケーションにアクセスできる状態でログインし続ける可能性があるのです。

⚠ 最少特権の原則の遵守ができなくなってしまう

最小特権の原則は、ユーザーが業務を遂行するために必要な最低限のデータ、アプリケーション、システムのみにアクセスできるようにすることですが、SSOは1回の認証でさまざまなアプリケーションやシステムにアクセスできるようにするものなので、この基本原則と相反します。

UserLock SSOを活用してリスクを軽減する３つのポイント

ユーザーアカウント管理のために、オンプレミスのActive Directoryを保持する

UserLockにより、既存のオンプレミスActive DirectoryをID管理ソリューションとして、クラウドの連携を拡張することが可能になります。

- ユーザーIDを新しいディレクトリに統合する必要がない
- 既存のActive Directoryを活用することができる
- アカウントやサービス、グループポリシーを新しくする必要がない
- オンプレミス認証を維持することでセキュリティリスクが低減できる
- 主要なクラウドアプリケーションやカスタムアプリケーションのSSOに対応。
- 障害時でもリカバリー機能を搭載

SSOと多要素認証（MFA）を組み合わせて、パスワードの脆弱性を保護する

UserLockでは、MFAをSSOと簡単に組み合わせることができるため、ユーザーにとっても大きな手間をかけずに、強力なセキュリティを実装することができます。

- Googleなどが提供する無料の認証アプリケーションに対応
- 「YubiKey」「Token2」といったハードウェアトークンに対応
- 企業や組織のセキュリティポリシーに従って、カスタマイズ可能

SSOをさらにセキュアにするコンテキストアウェアセキュリティ

コンテキストアウェアセキュリティとは、あるユーザーがアクセスしようした場合、状況を分析してユーザー本人であるかどうかを判断するテクノロジーです。
UserLockではログインプロセスの一部として、コンテキストアウェアセキュリティが実行されるため、SSOによる利便性を損なうことなく高機能なログインセキュリティを実行することが可能です。

- 端末、IP、部門、会社、場所などによる制限
- 時間帯や最大セッション時間やアイドル時間などによる制限
- Wi-Fi、VPN、IISセッションなどによる制限
- 同一のアカウントからの同時ログインによる制限
- エンドユーザーに対して追加の認証手順の必要がない

OCEANBRIDGE

株式会社オーシャンブリッジ

〒107-0051 東京都港区元赤坂1-5-12 住友不動産元赤坂ビル7F
https://www.isdecisions.jp/
userlock@oceanbridge.jp