ゼロサインオン:
パスワードレス認証のソリューション

ZSOの主なメリット

データ漏洩のリスクを軽減

ZSOは、パスワードをなくすことによりデータ漏洩 のリスクを軽減します。

スムーズなアクセスの提供

ZSOを使用すれば、複雑なパスワードを記憶、入 力、またはリセットする必要がなくなり、ユーザーは素早く簡単にクラウドベースのアプリにアクセスできます。

ヘルプデスクのコストを削減

ZSOのパスワードレスのアプローチで、パスワードのリセットやアカウントロックにヘルプデスクのリソースを使わなくて済みます。

スケーラブルなモバイルクラウドセキュリティの 導入

業界標準に基づいて構築されたZSOは、世界中のあらゆる管理対象デバイスまたは管理対象外デバイス上のエンタープライズクラウド、またはハイブリッドサービスに使用できます。

パスワードに別れを告げる時です

パスワードを好む人はいません。記憶するのが難しく、入力 に時間がかかり、リセットが面倒なだけでなく、エンタープ ライズクラウドで起こるデータ侵害の最大の原因でもありま す。[1] セキュリティ部門のリーダーの86%が、できればパスワ ードの使用をやめ、モバイルデバイスをエンタープライズID として使用したいと考えているのも当然と言えるでしょう。[2]

そこで、Ivantiはゼロサインオン(ZSO)を導入しまし た。ZSOは、ユーザーアイデンティティとしての安全なモバイルデバ イスにパスワードを置き換えるシンプルな認証機能で す。ゼロトラスト・セキュリティフレームワークを活用す ることで、ZSOにより組織はEverywhere Workplaceで次のことを実現できます。

- パスワードを多要素認証(MFA)に置き換えることでゼロトラスト・アーキテクチャへ移行できます。
- Microsoft Office 365などのビジネスアプリケーションやクラ ウドサービスへのパスワードレス・アクセスを提供しま す。
- 一般的な生体認証を使用して、消費者と同様の認証体験を企業に提供します。
- パスワードにかかわる手間とセキュリティリ スクを排除します。
- 確実に、検証済みのユーザー、デバイス、アプリ、およ びネットワークのみがビジネスリソースにアクセスでき るようにします。

当社独自のアプローチ

Ivanti Accessプラットフォームに備わるIvanti ZSOは、パスワードの代わりにモバイルデバイスをユーザーのアイデンティティおよび認証の第一要素として使用します。強力なFIDO2認証プロトコルを使用するZSOにより、パスワードは不要になります。

Ivanti AccessはEverywhere Workplaceのために構築されています。Ivanti UEMやSCCM、Jamfなどのサードパーティ製UEMシステムを含め、統合エンドポイント管理(UEM)を基盤として活用し、クラウドリソースへの安全なアクセスを許可する前に、すべてのユーザー、デバイス、アプリケーション、ネットワークを検証するゼロトラストセキュリティアプローチを提供します。

また、Ivanti AccessはIvanti Mobile Threat Defense（MTD）とシームレスに統合することで、ユーザーデバイスのセキュリティを強化するとともに、クラウドへのコンテキストを考慮した条件付きアクセスを提供します。MTDは、デバイス、アプリ、ネットワークへの脅威によりビジネスデータが漏洩する前に検知し、修復することができます。

さらにIvanti AccessとZSOは、UEMやMTDと連携してデバイスの健全性やモバイルの脅威がないかどうかを判断します。脅威が検出された場合、Ivanti Accessはエンドユーザーのセッショントークンを失効させ、デバイスがモバイルの脅威から解放され、コンプライアンスに準拠した状態に戻るまで、企業リソースへのアクセスをブロックします。

ZSOの機能

ユーザーアイデンティティとしてのモバイルデバイス

パスワードを安全なモバイルデバイスに置き換え、ユーザー認証の主要要素として生体認証を使用し ます。

適応型認証

IvantiのMFA機能を使用して、高リス ク環境のためのユーザー検証の追加レイヤーを提供し ます。

管理内外のデバイスすべてを安全に

ZSOは、すべてのAndroid、iOS、macOSとWindows 10および11デバイスで動作します。ユーザーは、Ivanti UEMまたはSCCMやJamfなどサードパーティのUEMソリューションにより管理されているデバイスでは、公開鍵認証（証明書）を使用して認証され、管理されていないデバイスでは、FIDOセキュリティキーまたは生体認証とペアリングされたQRコードを使用して認証されます。

標準ベースのセキュリティ

Ivanti ZSOはFIDO2プロトコルをサポートしており、WindowsやMacのデスクトップログインにおけるシンプルで強力な認証とSaaSベースやWebベースのアプリケーションに対する認証によるシームレスなSSOを実現します。

一般的なビジネスアプリやIDPをサポート

Ivanti Accessは、Microsoft 365、Google Workspace、Salesforceなど、あらゆるクラウドや連携サービスを保護します。また、Okta、Ping、Microsoftを含む多くのアイデンティティソリューションとの統合も可能です。

オフラインログイン

BluetoothでZSOを使用し、オフラインの時にモバイルデバイスでデスクトップやノートPCにログインすることができます。

ゼロトラスト・ポリシー・エンジン

すべてのクラウドアプリについて、安全でないネットワ ークを介した無許可のユーザー、デバイス、およびアプ リへのアクセスのブロックまたは制限、あるいは脅威が 検出されたときのポリシーを単一のコンソールで定義 できます。直感的な修復ワークフローにより、ユーザー は自己修復を行うことができます。

詳細なレポート

Ivantiのグローバル認証ダッシュボードでは、ビジネスサービス に接続するユーザー、アプリ、デバイスの詳細を表示したり、ポリ シー違反などを管理者に通知したりすることができます。

ivanti

ivanti.co.jp
+81 (0)3 52265960
contact@ivanti.co.jp

1. Verizon, “2019 Data Breach Investigations Report.” www.verizon.com/business/resources/reports/dbir/2019
2. IDG Research, “Say Goodbye to Passwords,” April 2019. www.mobileiron.com/sites/default/files/Whitepapers/Say-Goodbye-to-Passwords/Say-Goodbye-to-Passwords.pdf