ベストプラクティス：

ZTNA

ゼロトラストネットワークアクセス

常に意識すべきZTNAのベストプラクティス：

→ 最小特権の原則に基づいてアクセスを許可する
→ 多要素認証（MFA）とクラウド IdPでIDを検証する
→ コンプライアンス要件を設定し、ユーザやデバイスの管理とセキュリティを確保する
→ 決して信用せず、常に検証し、初めてのアクセス後も継続的に検証する

最新のIDおよびアクセス管理についてまだ不慣れなら、この記事を読んでIDおよびアクセス戦略の方針の決め方について学びましょう。

jamf

銀行でお金を引き出す時、口座番号と身分証明書で本人確認が行われ、口座の名前と合致すれば、その口座にのみアクセスすることができます。もし、あなたのIDを渡すと、窓口係が銀行の金庫に案内して「全てどうぞ」と言うとしたらどうですか？それはありえない話ですよね。しかし、ネットワークアクセスではこれと同じようなことが起こっています。

VPN（仮想プライベートネットワーク）は、ユーザが全体アクセスを必要とするか否かにかかわらず、ネットワーク全体へのアクセスが可能であり、データをリスクに晒しています。**ゼロトラストネットワークアクセス（ZTNA）は、アプリケーションごとにユーザとデバイスのIDを厳密に検証しながら、従業員が必要とするリソースのみに最小限の権限でアクセスできるようにすることで、企業情報のストレージ（Vault）をロックダウン。**また、ネットワークへの帯域幅需要を削減し、スプリットトンネリングによってユーザのプライバシーを保護します。つまり、VPNとZTNAは切っても切れない関係にあります。

では、ZTNAはどのように機能しているのでしょうか？最も基本的なことではありますが、ZTNAでは以下の点を確認します：

1. **アイデンティティ：**あなたは誰ですか？あなたは名乗っている人物本人ですか？承認を受けていますか？
2. **セキュリティ：**あなたのデバイスは安全ですか？
3. **コンテキスト：**必要なリソースのみへのアクセシビリティを要求していますか？

ZTNAをうまく導入するには、これらの疑問をクリアにする必要があります。まずZTNAでは、ユーザとデバイスの両方が身元を証明する必要があり、デバイスは既知の正規デバイスでなければなりません。これは、特定のユーザに関連付けられたデバイスをデバイス管理ソリューションに登録することで対応可能です。次にユーザは、クラウドIDプロバイダの多要素認証に正しい認証情報とレスポンスを提供する必要があります。

IDが認証されたとしても、会社のリソースにアクセスしようとする際のさらなるリスクを軽減するために、デバイスのセキュリティを確保することが重要です。つまり、デバイスはセキュリティポリシーに準拠し、最新のOSと脆弱性パッチが適用されている必要があります。

IDとセキュリティが確認されると、ユーザは必要なアプリケーションへのアクセスが許可されます。ZTNAでは、ユーザは許可されたものしかアクセスできません。これを実現するために、事前承認済みアプリのみが各ユーザに提供されます。これにより、ユーザがこれらのアプリにアクセスしようとした時点で、既にアクセシビリティを持っているはずということになります。

Jamfは、デバイス管理、アプリのプロビジョニング、クラウドIDプロバイダとの統合、ソフトウェアアップデート、エンドポイントプロテクションなど、これらすべてを行います。ZTNAをシームレスに提供する方法については、初心者のためのゼロトラストネットワークアクセスeブックをご覧ください。

ZTNAでデータを守りませんか？JamfのTrusted Accessによって、ZTNAでデータをロックダウンする方法などを学びましょう。

jamf

www.jamf.com/ja/