多要素認証と条件付きアクセスとは

100 XP

4 分

Tailwind Traders では、配送ドライバーは、自分のモバイル デバイスを使用して、スケジュールや物流のアプリケーションにアクセスすることが許可されています。 一部の配送ドライバーは、Tailwind Traders の永続的な従業員です。 その他のドライバーは短期的な契約で働いています。 アクセス試行が本当に有効な Tailwind Traders ワーカーからのものであることを IT 部門はどのように確認できるでしょうか?

ここでは、セキュリティで保護された認証を有効にする 2 つのプロセス (Azure AD Multi-Factor Authentication と条件付きアクセス) について説明します。 まず、多要素認証の概要について簡単に見てみましょう。

多要素認証とは

"多要素認証" は、ユーザーがサインイン プロセス中に追加の識別形式を求められるプロセスです。 例として、携帯電話のコードや指紋スキャンなどがあります。

Web サイト、電子メール、またはオンライン ゲーム サービスにサインインする方法について考えてみてください。 ユーザー名とパスワードに加えて、電話に送信されたコードを入力する必要があったことがありますか? その場合は、多要素認証を使用してサインインしています。

多要素認証では、完全な認証のために 2 つ以上の要素を必須とすることで、ID のセキュリティが強化されます。

これらの要素は、次の 3 つのカテゴリに分類されます。

- **ユーザーが知っていること**

  これには電子メール アドレスとパスワードが該当します。

- **ユーザーが持っているもの**

  これにはユーザーの携帯電話に送信されるコードが該当します。

- **ユーザー自身の特徴**

  通常、これは多くのモバイル デバイスで使用されている指紋や顔スキャンなどのある種の生体認証です。

多要素認証を使用することで、資格証明露出 (たとえば、ユーザー名やパスワードの漏洩など) の影響が限られ、ID のセキュリティが強化されます。 多要素認証を有効にすると、攻撃者があるユーザーのパスワードを持っていたとしても、そのユーザーの電話や指紋がなければ完全には認証されません。

多要素認証と単一要素認証を比較してみましょう。 単一要素認証では、ユーザー名とパスワードのみで攻撃者が認証されてしまいます。 多要素認証はセキュリティに大きなメリットを与えるため、可能な限り有効にしてください。

Azure AD Multi-Factor Authentication とは

Azure AD Multi-Factor Authentication は、多要素認証機能を提供する Microsoft のサービスです。 Azure AD Multi-Factor Authentication を使用すると、ユーザーはサインイン時に追加の形式の認証 (電話やモバイル アプリの通知など) を選択できます。

Azure AD Multi-Factor Authentication の機能は次のサービスで提供されています。

- **Azure Active Directory**

  Azure Active Directory Free エディションでは、管理者は Microsoft Authenticator アプリ、通話、または SMS コードを介して、"グローバル管理者" レベルのアクセス権で Azure AD Multi-Factor Authentication を使用できます。 Azure AD Multi-Factor Authentication では、Azure AD テナントで "セキュリティの既定値" を有効にすることによって、Microsoft Authenticator アプリ経由の場合にのみすべてのユーザーに適用することもできます。

  Azure Active Directory Premium (P1 または P2 ライセンス) を使用すると、条件付きアクセス ポリシー (以下で説明します) を使用して Azure AD Multi-Factor Authentication の包括的かつ詳細な構成を行うことができます。

- **Office 365 の多要素認証**

  Azure AD Multi-Factor Authentication 機能のサブセットは、Office 365 サブスクリプションの一部です。

ライセンスと Azure AD Multi-Factor Authentication の機能の詳細については、Azure AD Multi-Factor Authentication の使用可能なバージョンに関する記事をご覧ください。

条件付きアクセスとは

条件付きアクセスは、ID の "シグナル" に基づいてリソースへのアクセスを許可 (または拒否) するために Azure Active Directory によって使用されるツールです。 これらのシグナルには、ユーザーが誰であるか、ユーザーの所在地、ユーザーがアクセスを要求しているデバイスなどが含まれます。

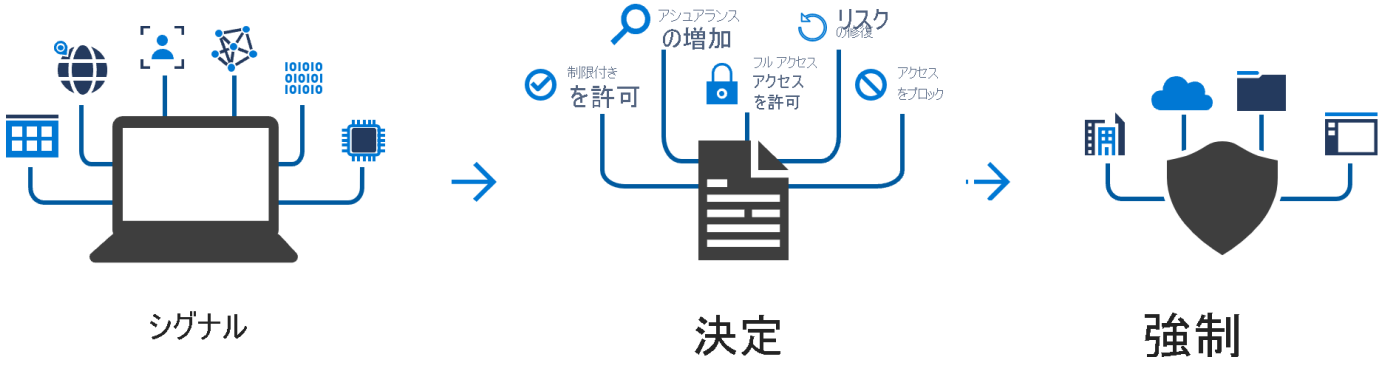
条件付きアクセスを使用すると、IT 管理者は次のことを行うことができます。

- ユーザーがいつでも、どこでも生産性を上げられるようにする。
- 組織の資産を保護する。

また、条件付きアクセスにより、ユーザーに対してより細やかな多要素認証エクスペリエンスが提供されます。 たとえば、ユーザーが既知の場所にいる場合は、2 番目の認証要素が求められない可能性があります。 ただし、サインイン シグナルが異常な場合やユーザーが予期しない場所にいる場合は、2 番目の認証要素が求められることがあります。

サインイン時には、条件付きアクセスによってユーザーからシグナルが収集され、それらのシグナルに基づいて判断されます。その後、アクセス要求を許可または拒否するか、多要素認証応答を求めることによって、その判断が適用されます。

このフローを示す図を次に示します。



ここで、シグナルはユーザーの場所、ユーザーのデバイス、またはユーザーがアクセスしようとしているアプリケーションである可能性があります。

これらのシグナルに基づくと、ユーザーが通常の場所からサインインしている場合、フル アクセスを許可するように判断されることがあります。 ユーザーが通常とは異なる場所からサインインする場合、または危険としてマークされている場所からサインインする場合は、アクセスが完全にブロックされるか、ユーザーが 2 番目の形式の認証を行った後に許可される可能性があります。

強制は判断を適用するアクションです。 たとえば、アクションにより、アクセスを許可したり、2 番目の形式の認証をユーザーが行うことを求めたりすることができます。

条件付きアクセスはいつ使用できますか?

条件付きアクセスは、次のことを行う必要がある場合に役に立ちます。

- アプリケーションへのアクセスに多要素認証を求める。

  すべてのユーザーに多要素認証を求めるか、管理者などの特定のユーザーのみに求めるかを構成できます。

  また、すべてのネットワークからのアクセスに多要素認証を適用するか、信頼されていないネットワークのみに適用するかを構成することもできます。

- 承認されたクライアント アプリケーションからのみサービスにアクセスするように求める。

  たとえば、ユーザーが Outlook モバイル アプリなどの承認されたクライアント アプリを使用している場合にのみ、モバイル デバイスから Office 365 サービスにアクセスできるようにすることができます。

- マネージド デバイスからのみアプリケーションにアクセスするようにユーザーに求める。

  マネージド デバイス とは、セキュリティとコンプライアンスの標準を満たしているデバイスです。

- 不明な場所または予期しない場所からのアクセスなど、信頼されていないソースからのアクセスをブロックする。

条件付きアクセスには、*What If* ツールが付属しています。これは、条件付きアクセス ポリシーの計画とトラブルシューティングに役立ちます。 このツールを使用すると、ユーザーからの最近のサインイン試行から提案された条件付きアクセス ポリシーをモデル化して、それらのポリシーを有効にした場合の影響を確認できます。 What If ツールを使用すると、提案された条件付きアクセス ポリシーを実装する前にテストすることができます。

条件付きアクセスはどこで入手できますか?

条件付きアクセスを使用するには、Azure AD Premium P1 または P2 ライセンスが必要です。 Microsoft 365 Business Premium ライセンスをお持ちの場合も、条件付きアクセス機能にアクセスすることができます。