# はじめに

100 XP

1 分

従来は、システムとデータへのアクセスの保護には、オンプレミスのネットワーク境界と物理的なアクセス制御が関係していました。

ユーザーがどこからでも作業できるようになり、また、BYOD (Bring Your Own Device) 戦略、モバイル アプリケーション、クラウド アプリケーションが増加しています。これらのアクセス ポイントの多くは、企業の物理的なネットワークの外部にあります。

そこで、*ID* が新しい基本的セキュリティ境界になりました。 ユーザーがシステムの有効なユーザーであり、適切なレベルのアクセス権を持っていることを正確に証明することは、データの制御を維持するために不可欠です。 この ID レイヤーは、ネットワークよりも攻撃の対象となることが多くなっています。

## Tailwind Traders 社の紹介

Tailwind Traders は、架空のホームセンターです。 この会社は、世界中およびオンラインでホームセンターを運営しています。


Tailwind Traders には、競争力のある価格設定、迅速な出荷、および幅広い商品という特徴があります。 クラウド テクノロジによって事業運営を改善し、新しい市場への成長をサポートできると考えています。 クラウドへの移行によって、ショッピング体験を強化し、自社と競合他社との差別化を促進しようとしています。

## Tailwind Traders はクラウド アプリケーションへのアクセスをどのようにセキュリティで保護するでしょうか?

Tailwind Traders がクラウドで実行しているアプリケーションの数と同様に、同社のモバイル ワーカーは増加しています。

世界各地で働く販売員にはタブレット デバイスが支給されていて、顧客のために注文を作成したり、配送スケジュールを追跡したり、作業スケジュールを計画したりできます。

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できます。 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。

Tailwind Traders は Active Directory を使用して、オンプレミス環境をセキュリティで保護しています。 従業員だけが会社のビジネス アプリケーションにサインインしてアクセスできるようにする必要があります。 また、短期契約のスタッフがこれらのアプリケーションに契約が有効である期間にのみアクセスできるようにする必要もあります。

Tailwind Traders がイントラネットとパブリック ネットワークからのアクセスをすべてのアプリケーションで一貫してセキュリティで保護することができるようにするには、Azure Active Directory (Azure AD) をどのように使用すればよいでしょうか?

# 学習の目的

このモジュールを終了すると、次のことができるようになります。

- 認証と承認の違いについて説明する。
- Azure AD で ID とアクセスの管理が提供される方法について説明する。
- ユーザー ID を管理するためのシングル サインオン (SSO)、多要素認証、および条件付きアクセスの役割について説明する。

# 前提条件

- コンピューティングの基本的な概念と用語について理解している必要があります。
- クラウド コンピューティングに関する知識は有用ですが、必須ではありません。