ビジネス向け管理対象Apple IDの概要

組織内でAppleの製品を使用する際には、社員が必要とするサービスを、管理対象Apple IDがどのようにサポートするかについて理解しておくことが重要です。管理対象Apple IDは、Appleから提供される主要なサービスを企業で利用するための専用アカウントです。

Apple Business Managerを使用すると、組織は社員用の管理対象Apple IDを自動的に作成することができます。これにより、社員がAppleのアプリケーションやサービスを使って共同作業したり、iCloud Driveを使用する管理対象アプリケーションで企業のデータにアクセスしたりできるようになります。また、Federated Authenticationを設定すると、これらのアカウントで、組織が所有および管理する既存のインフラと同じ資格情報を使うことができます。

管理対象Apple IDとは

管理対象Apple IDは、通常のApple IDと同じようにデバイスのパーソナライズに使用します。Appleのアプリケーションやサービスへのアクセスのほか、IT部門がApple Business Managerにアクセスする場合にも使用します。通常のApple IDとは異なり、管理対象Apple IDは各組織が所有および管理します。パスワードのリセットや役割ベースの管理も組織が行います。

Apple Business Managerを使えば、組織の各社員に一意の管理対象Apple IDを簡単に作成できます。Microsoft Azure Active Directoryとの統合が可能なため、組織は既存の資格情報を使って社員に管理対象Apple IDを提供できます。

iOS、iPadOS、macOS Catalinaのユーザー登録機能を利用すれば、社員が所有するデバイスで、管理対象と個人用の両方のApple IDを使用することができます。また、どのデバイスでも、管理対象Apple IDを唯一のApple IDとして使うこともできます。Appleデバイスにはじめてサインインした後は、管理対象Apple IDでウェブ上のiCloudにアクセスすることもできます。

Apple IDは導入の技術的な必須事項ではありません。Apple IDがなくても、Appleデバイスを管理したりアプリケーションをデバイスに配布したりすることは可能です。組織で使用する予定のサービスを確認し、管理対象Apple IDへの最適な移行方法を検討してください。管理対象Apple IDはビジネス用途のみを想定しているため、組織を保護するために特定の機能を無効にしています。

組織が利用できる機能

- **Appleのサービスへのアクセス。**社員はiCloudなどのAppleのサービスを使ったり、iWorkやメモを使って共同制作したりできます。Eメールは無効になり、FaceTimeやiMessageは、管理対象Apple IDがデバイス上の唯一のApple IDである場合のみ使用可能になります。
- **ユーザーアカウントの検索。**社員はApple Business Managerの組織内にいるほかのユーザーの連絡先情報を検索できるので、様々なアプリケーションで簡単に共同作業できるようになります。
- **アカウント作成を効率化。**Apple Business Managerでは、社員がはじめてAppleデバイスにサインインした時にアカウントが自動的に作成されます。
- **Federated Authentication。**Apple Business ManagerはMicrosoft Azure Active Directoryに接続できるので、管理者は既存の資格情報を使って社員のアカウントを自動的に設定することができます。
- **役割と権限。**管理者は、IT部門がApple Business Managerの様々な機能を使用できるように、役割と権限を作成して割り当てることができます。
- **組み込まれているプライバシーとセキュリティ機能。**管理対象Apple IDでは、通常のApple IDと同様に暗号化によるデータ保護機能が使用され、Appleの広告プラットフォームでのターゲット広告もブロックされます。購入機能が無効になり、Apple PayやWalletなどのサービスも利用できません。MDMを使った紛失モードを利用できるため、「探す」も無効になります。

Federated Authentication

Federated AuthenticationをつかってApple Business ManagerをMicrosoft Azure Active Directory（Azure AD）に接続することで、社員が既存のユーザー名とパスワードを管理対象Apple IDとして使えるようになります。

Microsoft Azure ADはIDプロバイダ（IdP）です。ここには、Apple Business Managerで使用できるアカウントのユーザー名とパスワードが含まれています。

Microsoft Azure ADとの統合によって既存の資格情報が連携されるため、管理対象Apple IDでも同じパスワードポリシーが適用されます。

管理対象Apple IDは、ユーザーがAppleデバイスにサインインした時に自動的に作成されるので、IT管理者が時間をかけて準備する必要はありません。

社員は既存のAzure ADの資格情報を使って、iCloud Driveやメモ、リマインダー、共同作業などのAppleサービスを利用できます。

IDはすでに組織によって管理されているので、パスワードポリシーやリセット操作などはすべて組織、つまりMicrosoft Azure ADのユーザーによって処理されます。

Federated Authenticationの条件

- **Microsoft Azure Active Directory。**すでに設定済みの場合は、Federated Authenticationを使い始めることができます。
- **オンプレミスのActive Directory。**Azure ADと同期するための追加の設定手順があります。資料や同期用ツールは、以下のリソースの一番下にあるMicrosoftのリンク先から入手可能です。

Federated Authenticationの設定方法

1. **Appleでドメインを検証する。**管理者またはユーザマネージャのアカウントでApple Business Managerにサインインし、Federated Authenticationに使用するドメインを追加します。
2. **Microsoft Azure Active Directoryに接続し、Apple Business Managerのアクセスを許可する。**グローバル管理者またはアプリケーション管理者のアカウントを使ってAzure ADにサインインし、Apple Business Managerがユーザーのプロファイルを読み込むことを許可します。
3. **Microsoft Azure Active Directoryでドメインの所有権を検証する。**信頼関係を確立した上で、プロセスを進めてドメインを検証します。連携するドメイン名が使われているアカウントで、Apple Business ManagerからMicrosoft Azure ADにサインインします。この操作により、ドメインの設定と所有権の検証が行われます。
4. **ドメインの競合をチェックする。**Apple Business Managerは、このドメインに既存のApple IDとの競合がないかチェックします。個人用のApple IDやほかの組織が設定した管理対象Apple IDで、同じドメインが使用されている可能性があるためです。
5. **ドメインの競合を解消する。**連携するドメインが個人用のApple IDとして使用されていることがApple Business Managerによって検出されると、このユーザー宛に、Apple IDのEメールアドレスを変更する必要があることを知らせる通知が送られます。これまで購入したものやデータは、ユーザーの個人用Apple IDに関連付けられたままになります。
6. **既存のアカウントを移行する。**既存の管理対象Apple IDがある場合は、Apple IDの情報を変更し、連携するドメインとユーザー名に一致させることで、Federated Authentication用のIDとして移行することができます。

リソース

- Apple Business Managerスタートアップガイド
- Apple Business Managerユーザガイド
- Apple Business Managerでの管理対象Apple IDの作成
- Apple Business ManagerのFederated Authenticationについて
- Apple IDのメールアドレスの変更が必要になった場合
- オンプレミスのActive DirectoryドメインとAzure Active Directoryを統合する