# 第 9 章

# Microsoft Intune によるデスクトップとモバイル クライアントの管理

## 目次



# 概要

デスクトップ コンピューターの管理は、これまで、Microsoft System Center Configuration Manager などのオンプレミス エンタープライズ管理システムを使用しておこなわれてきました。Microsoft Intune は、エンタープライズ デスクトップ管理の範囲をクラウドに拡張し、さまざまな展開シナリオでデスクトップとモバイル デバイスの両方を管理できるようにします。この章では、Intune クライアント ソフトウェアを管理対象のコンピューターにインストールして、Intune によって提供される機能を使用する方法について説明します。また、ポリシーを構成し、管理対象のコンピューターおよびデバイスでコンプライアンスと機能固有の設定を適用する方法についても説明します。最後に、モバイル デバイスをサポートするように Intune を構成する方法について説明します。

### 目的

この章により、次のことを習得できます。

- Intune クライアント ソフトウェアを展開することができます。
- Intune ポリシーを説明することができます。
- Intune を使用してモバイル デバイスを管理することができます。

# レッスン 1
# Intune クライアント ソフトウェアの展開

Intune をスタンドアロン サービスとして実行する場合、Intune クライアントを使用してコンピューターを管理することを選択できます。Intune クライアントは、ほとんどの Intune 機能を管理するのに役立つクライアント側のコンポーネントを提供します。このような Intune 機能には、インベントリ、アプリケーション管理、ソフトウェア更新プログラム、Endpoint Protection、リモート アシスタンスなどがあります。このレッスンでは、Intune クライアントをコンピューターに展開する際の考慮事項と処理について説明します。

### 目的

このレッスンにより、次のことを習得できます。

- Intune クライアントの機能を説明することができます。
- Intune クライアントのソフトウェア要件を説明することができます。
- Intune クライアント ソフトウェアを展開する方法を説明することができます。
- クライアントのインストールを検証する方法を説明することができます。
- ユーザーとデバイスの関連付けおよびグループによって、オブジェクトを管理する方法を説明することができます。
- Intune でグループを作成することができます。
- Intune で利用可能なレポートについて説明することができます。

## Intune クライアントとは

コンピューターを Intune クライアントで管理するには、まず、管理対象のコンピューターに Intune クライアント ソフトウェアをダウンロードしてインストールする必要があります。クライアント ソフトウェアは、次の機能を管理するのに役立つコンポーネントをインストールします。

Intune クライアントは、次の機能のサポートを可能にする

- インベントリとレポート処理
- アプリケーション管理
- ソフトウェア更新プログラム
- Endpoint Protection
- Windows ファイアウォール
- リモート アシスタンス


- **インベントリとレポート処理 :** Intune クライアントは、管理対象のコンピューターに存在するハードウェアとソフトウェアについての情報を収集します。これらの情報は、レポートを生成するため、およびコンピューターを共通グループにまとめて、アプリケーションまたはソフトウェア更新プログラムをより効果的に対象を絞って展開するための基盤として使用されます。
- **アプリケーション管理 :** Intune が管理するコンピューターにソフトウェア アプリケーションをインストールできます。Windows インストーラー (.msi) や Windows アプリケーション パッケージ (.appx) などのさまざまな形式を使用して、ソフトウェアをリモートから展開するように選択できます。Windows ストアで提供されているアプリケーションへのリンクを展開することもできます。
- **ソフトウェア更新プログラム :** コンピューターを Intune に登録すると、Microsoft ソフトウェア更新プログラムや他の企業のソフトウェア更新プログラムの検出と展開を管理できるようになります。

- **Endpoint Protection :** ポリシーを構成して、管理対象のコンピューターで定義ファイルを更新したり、マルウェアを検出したりできます。また、マルウェア検出時のアクションを指定することもできます。
- **Windows ファイアウォール :** 管理対象コンピューターでファイアウォール設定を構成するために、Windows ファイアウォール ポリシーを適用できます。
- **リモート アシスタンス :** Microsoft Easy Assist を利用すると、ユーザーはリモート アシスタンスを要求できるようになります。この機能は、Windows 8 以降のオペレーティング システムが動作するコンピューターではサポートされません。

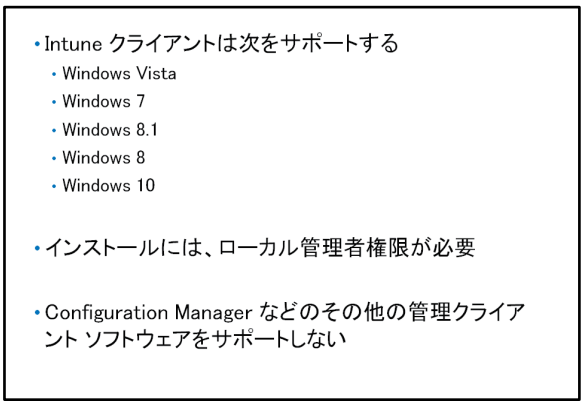
Intune クライアント ソフトウェアをインストールすると、Microsoft Intune Center アプリケーションが、管理対象コンピューターで利用できるようになります。このアプリケーションは、次の機能を提供します。

- Microsoft Intune ポータル サイト アプリから発行済みのアプリケーションを取得するためのリンクを提供します。
- ソフトウェア更新プログラムをチェックします。
- Windows Defender を起動します。
- リモート アシスタンス セッションを起動します (サポートされている場合)。

## Intune クライアントの要件

Intune クライアントは、次の x86 ベースおよび x64 ベースのオペレーティング システムが動作しているコンピューターでサポートされます。

- Windows Vista Business、Windows Vista Enterprise、および Windows Vista Ultimate
- Windows 7 Professional、Windows 7 Enterprise、および Windows 7 Ultimate (Service Pack なしまたは Service Pack 1)
- Windows 8.1 Pro、Windows 8.1 Enterprise、Windows 8 Pro、および Windows 8 Enterprise
- Windows 10 Pro および Windows 10 Enterprise




Intune クライアントをインストールするには、そのコンピューターに対するローカル管理者権限が必要です。また、コンピューターには、Windows Installer 3.1 以降がインストールされている必要があります。ポート 80 およびポート 443 のインターネット アクセスで必要です。

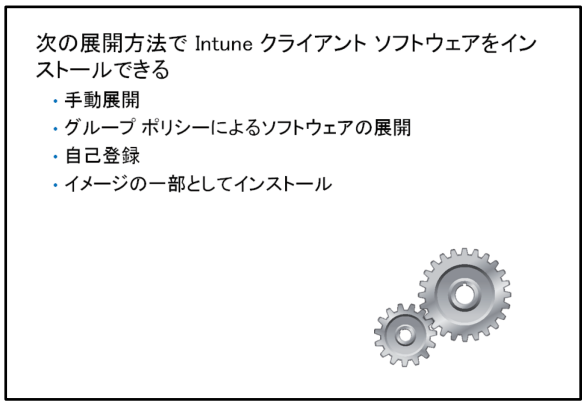
次の Web ブラウザーで、Microsoft Intune アカウント ポータル、Microsoft Intune 管理コンソール、および Microsoft Intune ポータル サイトへのアクセスがサポートされています。

- Microsoft Internet Explorer 9 以降
- Google Chrome (バージョン 42 よりも前のバージョン)
- Mozilla Firefox

**注 :** Intune クライアント ソフトウェアをインストールする前に、Microsoft Systems Management Server、System Center Configuration Manager 2007、System Center 2012 Configuration Manager、および System Center 2012 R2 Configuration Manager のあらゆるバージョンからクライアント ソフトウェアを削除する必要があります。

## Intune クライアント ソフトウェアを展開する方法

Intune を使用してクライアント コンピューターを管理するには、まず、クライアント ソフトウェアをダウンロードしてインストールする必要があります。Intune クライアント ソフトウェアは、Microsoft Intune 管理コンソールから入手できます。




クライアント ソフトウェアをダウンロードするには、コンソールで、[管理者]、[クライアント ソフトウェアのダウンロード] の順にクリックします。[クライアント ソフトウェアのダウンロード] ページに、Intune セットアップ パッケージをダウンロードするためのリンクが提供されています。ダウンロード パッケージには、Microsoft_Intune_Setup.exe と MicrosoftIntune.accountcert の 2 つのファイルが含まれています。パッケージを展開し、展開方法からアクセス可能で安全なネットワーク共有にファイルを移動します。

**注 :** クライアント ソフトウェア パッケージには、コンピューターを Microsoft Intune テナントに登録するための情報が含まれています。これらのファイルを安全な場所に保管して、未承認のユーザーによってコンピューターが登録されないようにしてください。また、Accountcert ファイルの名前を変更したり、それを削除したりしないでください。そのようなことをおこなうと、クライアント インストールが失敗します。

クライアント パッケージは、さまざまな方法を使用してコンピューターに展開できます。次に、その方法を示します。

- **手動展開 :** 管理対象となるコンピューターから、クライアント インストール パッケージが格納されているネットワーク共有にアクセスします。Microsoft_Intune_Setup.exe を実行すると、クライアント コンピューターのタスク バーのアイコンから、インストールの進捗状況を表示できます。このソフトウェアをインストールするには、ローカルの Administrators グループのメンバーである必要があることに注意してください。
- **グループ ポリシーによるソフトウェアの展開 :** グループ ポリシーを使用して、Intune クライアント ソフトウェアを展開できます。グループ ポリシーの主なメリットは、管理者権限を使用して、展開を一括して実行できることです。グループ ポリシーを使用するには、まず、次のコマンドを使用して .exe パッケージを展開します。

  ```
  Microsoft_Intune_Setup.exe /Extract <展開先フォルダー>
  ```

  パッケージを展開すると、次の 2 つのファイルが提供されます。

  - Microsoft_Intune_x86.msi
  - Microsoft_Intune_x64.msi

  これらのファイルは、グループ ポリシー ソフトウェア展開を使用して適用できます。これらのファイルは MicrosoftIntune.accountcert ファイルと一緒に、すべての潜在的なクライアント コンピューターがアクセスできる安全なネットワーク共有に配置する必要があります。

- **自己登録 :** Microsoft Intune ポータル サイトを展開済みの場合、またはユーザーにインストールさせようとしている場合、ユーザーはポータルを通して各自のコンピューターを自己登録できます。ポータルを使用することのメリットは、登録されたコンピューターにユーザー アカウントが自動的に関連付けられることです。ただし、自己登録方法を使用する場合は、いくつかの点について考慮する必要があります。
  - ユーザーは、登録対象のコンピューターでローカル Administrators グループのメンバーである必要があります。
  - ユーザーは、職場または学校アカウントを使用する必要があります。Microsoft アカウントを使用して自己登録することはできません。

Microsoft Intune ポータル サイトから自己登録するには、次の手順を実行します。

1. Microsoft Intune ポータル サイトにサインインします。
2. [デバイスの追加] をクリックします。
3. ソフトウェアをダウンロードして、インストールを実行します。

**参考資料 :** Microsoft Intune クライアント ソフトウェアは、イメージの一部としてインストールすることもできます。詳細については、次のサイトを参照してください。
Microsoft Intune を使用して Windows PC クライアントをインストールする
https://technet.microsoft.com/ja-jp/library/dn646969.aspx

## クライアント インストールの検証

Intune クライアント ソフトウェアをインストールしたら、クライアントへの展開が正常におこなわれたことを検証し、状態を監視する必要があります。Intune は、クライアントの状態を、リアルタイムおよびレポートベースで検証する方法を提供します。これらの方法を次に示します。

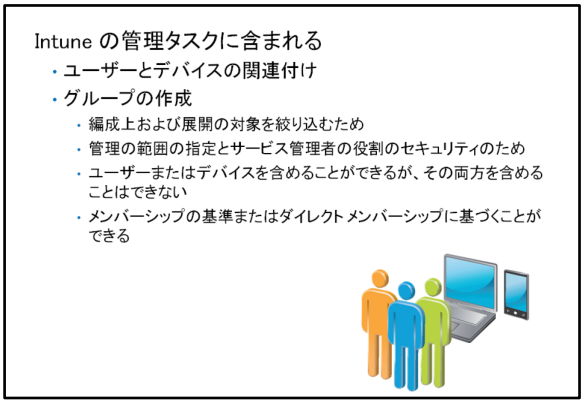

- **Microsoft Intune ダッシュボード :** Microsoft Intune 管理コンソールには、Intune 環境のヘルスの全体的な概要を示すダッシュボードが用意されています。Intune クライアントをインストールして展開したら、次の情報を表示して、インストール後の検証に役立てることができます。
  - **デバイスのヘルス :** ダッシュボードの [デバイスのヘルス] セクションには、デバイスと Intune サービスとの間の通信で発生した問題の概要が表示されます。[デバイスのヘルス] タイルをクリックすると、管理対象の各コンピューターの詳細な状態を示す [すべてのデバイス] グループが表示されます。
  - **アラート :** [アラート] タイルは、Intune 環境に関連するすべての警告または重大な問題の全体的な詳細を表示します。Intune クライアントをコンピューターにインストールすると、ソフトウェア更新プログラム、Endpoint Protection、またはアプリケーションの各問題に基づくすべてのアラートが表示されます。[アラート] タイルをクリックすると、Microsoft Intune 管理コンソールの [アラート] が表示されます。

- **ポリシー :** [ポリシー] タイルは、適用されているポリシー設定のヘルスの全体的な概要を表示します。この情報を使用することによって、新たにインストールされたクライアント環境が、Intune サービスからポリシーを正常に受信しているかどうかを判断できます。[ポリシー] タイルをクリックすると、Microsoft Intune 管理コンソールの [ポリシー] が表示されます。

- **コンピューター インベントリ レポート :** Intune クライアント ソフトウェアを展開した後に、登録されているすべてのコンピューターのリストを示すレポートを生成することができます。Microsoft Intune 管理コンソールの [レポート] から、[コンピューター インベントリ レポート] レポートを生成できます。このレポートは、オペレーティング システム、製造元、モデル、シャーシの種類、メモリなどのさまざまな種類の条件を指定することによって、カスタマイズできます。

## ユーザーとデバイスの関連付けおよびグループによるオブジェクトの管理

ユーザーとデバイスの関連付けおよびグループにより、オブジェクトを管理できます。




### ユーザーとデバイスの関連付け

ユーザーへのソフトウェアの展開など、一部の Intune 機能は、そのユーザーがコンピューターに関連付けられていることを必要とします。コンピューターをユーザーに関連付けると、ソフトウェアをユーザー オブジェクトにすばやく展開でき、その後、そのユーザーに関連付けられているすべてのコンピューターにソフトウェアをインストールできます。複数のコンピューターを特定のユーザーに関連付けることができますが、特定のコンピューターに関連付けられるユーザーは 1 人のみです。

**注 :** ユーザーが自分の所有しているコンピューターを Microsoft Intune ポータル サイトを使用して登録すると、ユーザーはそのコンピューターに自動的に関連付けられ、関連付けに関するそれ以上のアクションは必要ありません。

コンピューターをユーザーに関連付けるには、次の手順を実行します。

1. Microsoft Intune 管理コンソールで、[グループ] を参照します。
2. 関連付けるコンピューターを含むグループをクリックし、[ユーザーの関連付け] をクリックします。コンピューターに関連付けられている現在のユーザーを示すダイアログ ボックスが表示されます。現在のユーザーが存在しない場合、[ユーザーなし] と表示されます。
3. ユーザーの一覧からユーザーを選択して、[OK] をクリックします。別のユーザーがコンピューターに関連付けられている場合、新しいユーザーが以前のユーザー オブジェクトを置き換えます。

### グループによるユーザーとデバイスの管理

Microsoft Intune のグループは、編成上の機能とセキュリティを管理する機能の両方を提供します。グループを使用することにより、ポリシー設定、ソフトウェア更新プログラム、およびアプリケーション展開の対象を絞り込むことができます。また、特定の IT 管理者が Microsoft Intune 管理コンソール内で表示および管理できるグループを、フィルターを使用して制限することもできます。

グループを作成し管理するには、Microsoft Intune 管理コンソールの [グループ] を参照する必要があります。既定では、Intune には、削除することも編集することもできない組み込みグループが 9 つ用意されています。これらのグループは、管理目的でカスタム グループを作成する際の基盤となります。

グループ メンバーシップに関して、次の点を考慮する必要があります。

- グループは、ユーザーまたはデバイスのみを含むことができます。デバイス グループには、登録されている、または検出されているコンピューターおよびモバイル デバイスの両方が含まれます。ユーザー グループには、同期された Active Directory ドメイン サービス (AD DS) インスタンスからのユーザー、または Microsoft Intune アカウント ポータル内で作成されたユーザーが含まれます。
- ユーザーまたはデバイスは、複数のグループに属することができます。
- グループは、次の名前で呼ばれるメンバーシップの規則に基づいて、メンバーシップを追加または削除します。
    - **メンバーシップの基準 :** この規則は、AD DS から同期されるセキュリティ グループと属性情報を使用します。この種類のグループは動的であり、セキュリティ グループまたは属性データが変更されると、グループ メンバーシップも変化します。
    - **ダイレクト メンバーシップ :** この規則は、メンバーの静的リストを含みます。
- 作成するすべてのグループには親グループがあります。親グループは作成する子グループの利用可能なメンバーシップを定義します。さらに、ユーザーまたはデバイスを子グループに追加すると、それらは自動的に親グループのメンバーになります。

フィルターされたグループ ビューを構成することもできます。このビューは、特定の IT 管理者に関連するグループを表示するのに役立ちます。フィルターされたグループ ビューを構成するには、サービス管理者にとって表示可能となる必要のあるグループを選択して、既存のサービス管理者ユーザー オブジェクトを変更します。フィルター設定が構成されると、管理者は、フィルターされたグループのみを選択および表示できます。

## デモンストレーション : Microsoft Intune でのグループの作成

講師は、次のデモンストレーションをおこないます。

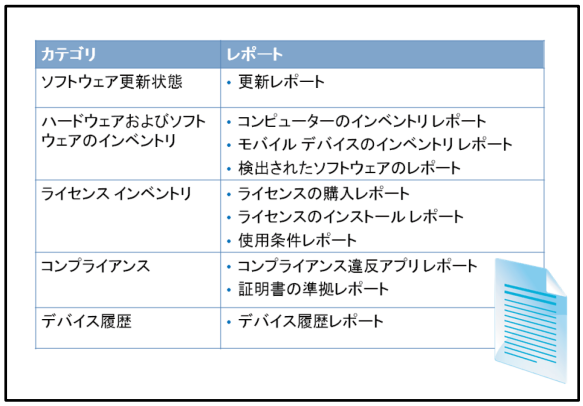
- Intune でグループを作成する

### デモンストレーションの手順

1. LON-CL1 で、Internet Explorer を使用して、Microsoft Intune 管理コンソール (http://manage.microsoft.com) にサインインします。
2. [グループ] で「Marketing Users」という名前の新しいグループを作成します。このグループは、すべてのユーザー既定グループをベースにします。
3. [グループ] で「Marketing Computers」という名前の新しいグループを作成します。このグループは、すべてのデバイス既定グループをベースにします。
4. [管理者] で、[管理者の管理] に新しいサービス管理者を作成します。
5. [グループの管理] をクリックし、既定グループを削除します。
6. Marketing Computers グループを追加します。

# Intune レポートの概要

Intune には、必要に応じてカスタマイズおよび保存できるさまざまな種類のレポートが用意されています。次に、それらのレポートの詳細を示します。



| カテゴリ | レポート |
|---|---|
| ソフトウェア更新状態 | • 更新レポート |
| ハードウェアおよびソフトウェアのインベントリ | • コンピューターのインベントリ レポート<br>• モバイル デバイスのインベントリ レポート<br>• 検出されたソフトウェアのレポート |
| ライセンス インベントリ | • ライセンスの購入レポート<br>• ライセンスのインストール レポート<br>• 使用条件レポート |
| コンプライアンス | • コンプライアンス違反アプリ レポート<br>• 証明書の準拠レポート |
| デバイス履歴 | • デバイス履歴レポート |

- **ソフトウェア更新状態**：「更新レポート」レポートでは、分類、更新状態、Microsoft セキュリティ レスポンス センター (MSRC) の重大度、および更新プログラムの有効な承認を指定できます。必要に応じて、特定のデバイス グループについてもレポートできます。
- **ハードウェアおよびソフトウェア インベントリ**：ハードウェアおよびソフトウェア インベントリに関して、さまざまなレポートが利用できます。次に、それらのレポートを示します。
  - **コンピューター インベントリ レポート**：デバイス グループ、オペレーティング システム、製造元、モデル、シャーシの種類、ディスク領域、メモリ、および CPU 速度に基づいて、独自のハードウェア インベントリ レポートを作成できます。
  - **モバイル デバイスのインベントリ レポート**：デバイス グループ、脱獄またはルート化されたデバイスの状態、およびオペレーティング システムに基づいて、モバイル デバイス インベントリ レポートを作成できます。
  - **検出されたソフトウェアのレポート**：デバイス グループ、発行者、およびソフトウェアのカテゴリに基づいて、独自のレポートを作成できます。
- **ライセンス インベントリ**：ライセンス インベントリには、次のレポートを含むさまざまなレポートが用意されています。
  - **ライセンスの購入レポート**：ライセンスの種類およびライセンス グループに基づいて、独自のレポートを作成できます。
  - **ライセンスのインストール レポート**：デバイス グループ、ライセンスの種類、およびライセンス グループに基づいて、独自のレポートを作成できます。
  - **使用条件レポート**：使用条件を受け入れたユーザーのリストを提供するレポートを作成できます。
- **コンプライアンス**：コンプライアンスには、次のレポートを含むさまざまなレポートが用意されています。
  - **コンプライアンス違反アプリ レポート**：このレポートは、デバイス グループのオペレーティング システム、およびコンプライアンス違反またはコンプライアンス準拠の状態を指定することによって、カスタマイズできます。
  - **証明書の準拠レポート**：このレポートは、ユーザー グループまたはデバイス グループ、証明書の有効期限、および証明書の発行状態を指定することによって、カスタマイズできます。
- **デバイス履歴**：このレポートは、インベントリからの使用中止、ワイプ、および削除の各操作の履歴ログを提供します。過去 90 日までの日付範囲を指定することによって、レポートをカスタマイズできます。

## 知識の確認

| 質問 | |
|---|---|
| **Microsoft Intune クライアント ソフトウェアを、x64 コンピューターのグループにインストールする必要があります。グループ ポリシーを使用して、Microsoft_Intune_Setup.exe を展開しようとしていましたが、.msi ファイルを使用して展開を実行する必要があることが判明しました。最初に何をおこなう必要がありますか。** | |
| 正しい解答を選択してください。 | |
| | Microsoft_Intune_Setup.exe ファイルの名前を Microsoft_Intune_x64.msi に変更する必要があります。 |
| | MicrosoftIntune.accountcert ファイルの名前を Microsoft_Intune_x64.msi に変更する必要があります。 |
| | Microsoft_Intune_Setup.exe ファイルを抽出する必要があります。 |
| | MicrosoftIntune.accountcert ファイルを削除する必要があります。 |

記述が正しい場合は、右側の列にチェック マークを入れます。

| 記述 | 解答 |
|---|---|
| ユーザーとデバイスの関連付けを実行するには、Microsoft Intune 管理者の権限が常に必要です。 | |

# レッスン 2
# Microsoft Intune ポリシーの概要

ほとんどの Windows ベースの IT 管理者は、グループ ポリシーを使用してコンピューター設定を構成したり適用したりすることを経験しています。Active Directory 環境では、グループ ポリシーは、コンピューターのグループに同様のセキュリティと機能ベースの設定が確実に適用されるようにするための重要なコンポーネントです。Microsoft Intune はこれと同種の概念に従っており、ポリシーを作成して、モバイル デバイスやコンピューターにおける Intune の機能およびサービスに関連する設定を制御することができます。

### 目的

このレッスンにより、次のことを習得できます。

- Intune ポリシーを定義することができます。
- 構成ポリシーの種類を説明することができます。
- コンプライアンス ポリシーと条件付きアクセス ポリシーについて説明することができます。
- Intune ポリシーを構成することができます。

## Intune ポリシーとは

Intune ポリシーは、モバイル デバイスおよび Intune クライアント コンピューターにおける機能を制御するために構成できる設定のグループです。ポリシーは、テンプレートを使用することによって、デバイス グループまたはユーザー グループに対して、構成および適用できます。テンプレートには、推奨される設定を含めることができます。また、特定の要件を満たす独自の設定を定義することもできます。


Microsoft Intune 管理コンソールでは、いくつかのカテゴリでポリシー設定が編成されます。[ポリシー] をクリックすると、次のノードが表示されます。

- **概要 :** ダッシュボード タイルがあり、現在のポリシー状態が表示されます。また、レポート ポリシーと競合するポリシー テンプレート設定およびデバイスへの直接的なリンクも表示されます。さらに、新しい構成ポリシーを追加するためのリンクと、コンプライアンス違反アプリ レポートを生成および表示するためのリンクもあります。
- **ポリシーの競合 :** ポリシーの競合と、競合が検出されたおおよその時間を表示できます。
- **構成ポリシー :** さまざまなモバイル デバイスおよびコンピューターに設定を適用するためのポリシー テンプレートを追加、編集、削除、または展開できます。
- **コンプライアンス ポリシー :** デバイスの特定のコンプライアンス レベルおよびそれらの要件を満たさないデバイスについてのレポートを定義するために使用できるポリシー設定を追加、編集、削除、または展開できます。コンプライアンス ポリシーは、条件付きアクセス ポリシーと組み合わせて使用して、デバイスが特定のサービスにアクセスできるかどうかを評価するのに役立てることができます。

- **条件付きアクセス :** Exchange Online および SharePoint Online へのアクセスを制御および管理できます。Intune によって管理されていないデバイスまたは構成されているコンプライアンス ポリシーに準拠していないデバイスが、特定の要件を満たさない限り、接続するのを禁止できます。
- **Exchange ActiveSync :** Exchange ActiveSync を使用して Exchange に接続されたモバイル デバイス用の接続ルールを指定するための設定をおこないます。
- **業務用デバイスの登録 :** 業務用デバイスの登録プロファイルを作成するために必要な設定をおこないます。このプロファイルは Apple デバイス登録プログラムと連携して、企業所有の iOS デバイスの無線通信経由による登録を可能にします。
- **使用条件 :** ユーザーが、ポータル サイトを使用する前に特定の企業の条件を受け入れるために必要とする使用条件を作成するために必要な設定をおこないます。

**注 :** 多くの Microsoft Intune ポリシーは、AD DS のグループ ポリシー設定に似ています。設定の競合が発生した場合、ドメインレベルのグループ ポリシーが Intune ポリシーよりも優先されます。コンピューターがドメインにサインインできない場合、Intune ポリシーがコンピューターに適用されます。

## コンピューター用の構成ポリシーの種類

Intune には、モバイル デバイスとコンピューターの両方の設定を構成するのに役立つ多くのテンプレートが用意されています。これらのテンプレートは、オペレーティング システムプラットフォームとデバイスの種類に基づいて分類されています。

このトピックでは、コンピューターに適用できるテンプレートの概要について説明します。この章の最後のレッスンで、モバイル デバイスに関連する構成ポリシーについて説明します。

| カテゴリ | テンプレート |
|---|---|
| コンピューターの管理 | • Microsoft Intune エージェントの設定<br>• Microsoft Intune Center の設定<br>• Windows ファイアウォール設定 |
| Windows | • カスタム構成<br>• エンタープライズ データ保護<br>• 全般構成<br>• SCEP 証明書プロファイル<br>• 信頼済み証明書プロファイル<br>• VPN プロファイル<br>• Wi-Fi インポート |

### コンピューターの管理テンプレート

次のテンプレートを使用して、コンピューター設定と Microsoft Intune Center 設定を管理できます。

- **Microsoft Intune エージェントの設定 :** Endpoint Protection サービスを制御するための設定を提供します。これらの設定には、Endpoint Protection のインストールと有効化、リアルタイム保護の構成、スキャン スケジュールの設定などがあります。また、このテンプレートは、更新プログラムとアプリケーションの自動検出頻度、インストールと再起動の動作など、ソフトウェア更新の設定を制御するためにも使用できます。更新頻度設定を使用して、新しいアプリケーション、新しいポリシー、および更新されたポリシーを検出することができます。この設定は、既定では 8 時間ごとに実行するように構成されます。最後に、このテンプレートを使用して、ユーザーが自身をコンピューターに関連付けられるかどうかを指定したり、バックグラウンド インテリジェント転送サービス (BITS) のネットワーク帯域幅設定を指定したりできます。このテンプレートは、コンピューターを含むデバイス グループに対してのみ適用できます。

**注 :** ポリシーは、[更新プログラムおよびアプリケーションの自動検出頻度] 設定に従って更新されます。この頻度の既定の設定は、8 時間ごとです。ポリシーを強制的に更新することもできます。これをおこなうには、更新対象のデバイスを選択し、[リモート タスク]、[ポリシーの更新] の順にクリックします。

- **Microsoft Intune Center の設定 :** サポート連絡先情報、Web サイトの URL、サポート ノートなど、Microsoft Intune Center で表示される情報を提供します。このテンプレートを使用して作成されるポリシーは、Intune クライアント ソフトウェアがインストールされているコンピューターを含むデバイス グループに対してのみ適用されます。
- **Windows ファイアウォール設定 :** ネットワーク プロファイルの各種類 (ドメイン、プライベート、およびパブリック) に対して Windows ファイアウォール設定を構成できます。設定には、ファイアウォールの有効化、受信接続のブロック、およびファイアウォールが新しいプログラムをブロックした際のユーザーへの通知などがあります。また、特定のサービスへのアクセスを許可または禁止する定義済みの例外を数多く構成することもできます。このテンプレートを使用して作成されるポリシーは、Intune クライアント ソフトウェアがインストールされているコンピューターを含むデバイス グループに対してのみ適用されます。

### Windows テンプレート

テンプレートを Windows ベースのコンピューターに適用して、企業リソースへの安全なアクセスを提供するのに役立てることができます。次に、これらのテンプレートを示します。

- **カスタム構成 :** Windows デバイスの制御に使用できる Open Mobile Alliance Uniform Resource Identifier (OMA-URI) 設定を含むポリシーを作成できます。このテンプレートは、ユーザー グループに対してのみ展開でき、Windows 10 デスクトップとモバイル デバイスでサポートされます。
- **エンタープライズ データ保護 :** Windows 10 デバイス上にエンタープライズ データ保護ポリシーを構成できます。また、特定の種類のアプリケーションがデータにアクセスし、それを使用する方法を制御することもできます。
- **全般構成 :** 管理対象の Windows 10 コンピューター、Windows 8.1 コンピューター、およびモバイル デバイス上でさまざまな設定を管理するためのポリシーを作成できます。
- **SCEP 証明書プロファイル :** Simple Certificate Enrollment Protocol (SCEP) 設定を構成できます。このプロファイルは、証明書の登録タスクおよび更新タスクを実行する際に使用します。このプロファイルを構成するには、まず、信頼済み証明書プロファイル テンプレートを作成する必要があります。この種類のプロファイルは、ユーザー グループに対してのみ適用でき、Windows 8.1 以降のコンピューターでサポートされます。
- **信頼済み証明書プロファイル :** 信頼されたルート証明機関 (CA) 証明書または中間 CA 証明書をコンピューターに展開できます。これは、作成済みの各 SCEP 証明書プロファイルと一緒に使用されます。この種類のプロファイルは、ユーザー グループに対してのみ適用でき、Windows 8.1 以降のコンピューターでサポートされます。

**注 :** 証明書プロファイルを管理するには、Active Directory 証明書サービス (AD CS) とネットワーク デバイス登録サービス (NDES) が必要です。詳細については、次のサイトを参照してください。
Microsoft Intune で証明書ポリシーを使用して会社のリソースへのアクセスを有効にする
https://technet.microsoft.com/ja-jp/library/dn818904.aspx

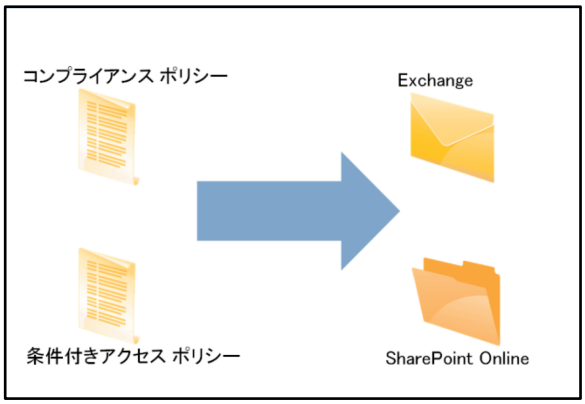
- **VPN プロファイル :** Juniper Pulse、F5 Edge Client、Dell SonicWALL、および Check Point Mobile VPN に基づいて、仮想プライベート ネットワーク (VPN) 接続の VPN 接続設定を構成できます。この種類のプロファイルは、ユーザー グループに対してのみ適用でき、Windows 10、Windows 8.1 以降のコンピューターでサポートされます。

**注 :** VPN プロファイルを使用するには、事前に、そのプロファイルの適用可能な VPN アプリケーションを展開する必要があります。

- **Wi-Fi インポート :** Microsoft Wi-Fi 構成をインポートして展開できます。このポリシーを使用するには、まず、Wi-Fi 構成を .xml ファイルにエクスポートする必要があります。Windows 8.1 以降のコンピューターの場合、netsh wlan ユーティリティを使用して、既存の Wi-Fi プロファイルを .xml ファイルにエクスポートできます。この種類のプロファイルは、ユーザー グループまたはデバイス グループに展開できます。

## コンプライアンス設定ポリシーと条件付きアクセス ポリシー

コンプライアンス ポリシーと条件付きアクセス ポリシーは連携して機能し、特定のサービスに対するアクセスが許可される前に、デバイスが要件を必ず満たすようにします。現在、サポートされるサービスには、Exchange Online、オンプレミスの Exchange、および SharePoint Online があります。




### コンプライアンス ポリシー

コンプライアンス ポリシーはオプションで、次に示すさまざまな設定を評価するために、ユーザーおよびデバイスに展開できます。

- パスワード要件
- 暗号化設定
- 脱獄またはルート化されたデバイスの許可/不許可の指定
- 電子メール プロファイル設定

### 条件付きアクセス ポリシーの構成

条件付きアクセス ポリシーは、Exchange 電子メールまたは SharePoint Online への実際のアクセスを管理します。条件付きアクセス ポリシーが構成されている場合、ユーザーは自身の電子メールにアクセスする際に、次の要件を満たす必要があります。

- デバイスは、Microsoft Intune に登録されている必要があります。
- デバイスは、職場に接続されている必要があります (以前は社内参加と呼ばれていました)。これは、デバイスの登録時に自動的におこなわれます。
- デバイスは、すべての Intune コンプライアンス ポリシーに準拠している必要があります。

**注 :** 現在、組み込みの Exchange ActiveSync クライアントを使用するデバイスから Exchange 経由で受信される電子メールへのアクセスをブロックできます。次のプラットフォームが対象になります。

- Android 4.2 以降
- iOS 6.0 以降
- Windows Phone 8.1 以降
- Windows 8.1 以降に搭載されているメール アプリケーション

また、Android および iOS 用の Outlook アプリを使用することによって、Exchange Online へのアクセスを制御することもできます。

次のアプリから SharePoint Online へのアクセスを制御できます。

- Office Mobile (Android)

- Word、Excel、PowerPoint、および OneNote (iOS)
- Microsoft OneDrive (Android および iOS)

**参考資料 :** Microsoft Intune で Exchange ActiveSync を使用してモバイル デバイス管理をセットアップする方法については、次のサイトを参照してください。
Microsoft Intune で Exchange ActiveSync を使用してモバイル デバイス管理をセットアップする
https://technet.microsoft.com/ja-jp/library/dn646988.aspx

## デモンストレーション : Intune ポリシーの構成

講師は、次のデモンストレーションをおこないます。

- Intune ポリシーを構成する

### デモンストレーションの手順

1. LON-CL1 で、Internet Explorer を使用して、Microsoft Intune 管理コンソール (http://manage.microsoft.com) にサインインします。
2. [ポリシー] で、各ポリシー ノードを表示します。
3. [ポリシー] で、Microsoft Intune エージェントの設定テンプレートに基づいて、新しい構成ポリシーを作成します。
4. ポリシーを編集して、Marketing Computers グループに適用します。

### 知識の確認

| 質問 | |
|---|---|
| **新しいポリシーを作成して、クライアント コンピューター用の更新プログラムおよびアプリケーションの自動検出頻度を構成する必要があります。このポリシーはどのテンプレートに基づく必要がありますか。** | |
| 正しい解答を選択してください。 | |
| | Microsoft Intune Center の設定 |
| | Microsoft Intune エージェントの設定 |
| | 構成ポリシー |
| | Windows カスタム ポリシー |

記述が正しい場合は、右側の列にチェック マークを入れます。

| 記述 | 解答 |
|---|---|
| 条件付きアクセス ポリシーを使用して VPN クライアントを検疫し、それらが最新のソフトウェア更新プログラムとマルウェア定義を確実に受信するようにすることができます。 | |

# 演習 A : Intune クライアント ソフトウェアのインストールとポリシーの構成

## シナリオ

Microsoft Intune 試用版サブスクリプションにサインアップすることができました。Intune で管理されるコンピューターにクライアント ソフトウェアをインストールする必要があります。また、クライアント コンピューター上に管理の設定を適用するために、ポリシー テンプレートを構成する必要もあります。

## 目的

この演習により、次のことを習得できます。

- Microsoft Intune クライアント ソフトウェアをインストールすることができます。
- Intune のポリシー設定を構成することができます。

## 演習のセットアップ

予定所要時間 : 25 分

| | |
|---|---|
| 仮想マシン | 23697-2B-LON-DC1<br>23697-2B-LON-CL1<br>MSL-TMG1 |
| ユーザー名 | Adatum¥Administrator<br>Adatum¥Don |
| パスワード | Pa$$w0rd |

この演習では、用意された仮想マシン環境を使用します。演習を開始する前に、次の手順を実行する必要があります。

1. ホスト コンピューターで、Hyper-V マネージャーを起動します。
2. Hyper-V マネージャーで [23697-2B-LON-DC1] をクリックし、操作ウィンドウで [起動] をクリックします。
3. 操作ウィンドウで [接続] をクリックします。仮想マシンが起動するまで待ちます。
4. 次の資格情報を使用してサインインします。
    - ユーザー名 : Adatum¥Administrator
    - パスワード : Pa$$w0rd
5. 23697-2B-LON-CL1 に対して、手順 2 ～ 3 を繰り返します。ユーザー名「Adatum¥Don」、パスワード「Pa$$w0rd」を使用してサインインします。
6. インターネットへのアクセスのために、MSL-TMG1 を起動します。

この演習を正常に完了するために、アクティブな Intune 試用版サブスクリプションを持っている必要があります。第 5 章の演習 B および第 8 章のすべての演習が完了している必要があります。

# 練習 1 : Intune クライアント ソフトウェアのインストール

## シナリオ

Intune で管理されるコンピューターに Intune クライアントをインストールする準備をしています。管理者用ワークステーションで Microsoft Intune 管理コンソールにサインインし、Intune クライアント ソフトウェアをダウンロードします。ワークステーションにインストールすることによって、ソフトウェアをテストします。テストが完了したら、管理対象の他のコンピューターにソフトウェアを配布します。

また、Research 部門からのコンピューターを含むカスタム グループを作成する必要があります。このカスタム グループを使用することにより、Research チームの特定のポリシー設定、およびアプリケーションの対象を絞り込むことができます。

主な作業は次のとおりです。

1. Intune クライアント ソフトウェアをダウンロードしてインストールする
2. カスタム グループを作成する

## ▶ 作業 1 : Intune クライアント ソフトウェアをダウンロードしてインストールする

1. LON-CL1 で、[検索] ボックスに「iexplore」と入力します。[Internet Explorer] を右クリックし、[タスク バーにピン留めする] をクリックします。
2. Internet Explorer を開き、[http://manage.microsoft.com] に移動します。
3. Microsoft Intune 管理コンソールにアクセスするための資格情報を入力します。第 5 章で構成した資格情報を使用します。
4. [管理者] で、[クライアント ソフトウェアのダウンロード] ページを参照し、LON-CL1 で、クライアント ソフトウェアをダウンロード フォルダーにダウンロードします。
5. クライアント ソフトウェアをダウンロードしたら、Microsoft_Intune_Setup.zip をダウンロード フォルダーに展開します。
6. Microsoft_Intune_Setup.exe を実行し、LON-CL1 にクライアント ソフトウェアをインストールします。
7. 承認のメッセージ ダイアログが表示されたら、ユーザー名「Adatum¥Administrator」、パスワード「Pa$$w0rd」を入力します。
8. 通知領域で、矢印をクリックし、Microsoft Intune インストール アイコンをポイントします。Microsoft Intune クライアント ソフトウェアがインストール中であると表示されることを確認します。インストールが完了するまで、5 ～ 10 分以上かかります。

## ▶ 作業 2 : カスタム グループを作成する

1. 必要に応じて、LON-CL1 で、http://manage.microsoft.com を参照し、資格情報を入力して、Microsoft Intune 管理コンソールにアクセスします。
2. [グループ] で、次の情報を使用して新しいカスタム グループを作成します。
   - 親グループ : すべてのデバイス
   - グループ名 : Research Computers
   - メンバーシップの基準
     - デバイスの種類 : コンピューター
     - グループのメンバーシップ : 空のグループ
   - ダイレクト メンバーシップ : LON-CL1.Adatum.com
3. 新しいグループを選択し、[全般] タブと [デバイス] タブの情報を表示します。

**結果 :** この練習により、Intune クライアント ソフトウェアをダウンロードし、Research 部門のカスタム グループを作成することができました。

## 練習 2 : Intune のポリシー設定の構成

### シナリオ

あなたは、最近実施された経営会議の中で、Intune クライアントに適用する必要がある特定のポリシー設定について知らされました。まず、すべてのクライアント コンピューターの Microsoft Intune Center に連絡先情報が提供されていることを確認します。また、次のように、Research デバイス グループの Microsoft Intune エージェントを設定するために特別な設定をおこなう必要もあります。

- マルウェアを駆除する前にシステムの復元ポイントを作成する。
- [更新プログラムおよびアプリケーションの自動検出頻度 (時間)] を「12」時間にする。

主な作業は次のとおりです。

1. Microsoft Intune Center の設定ポリシーを作成する
2. Microsoft Intune エージェントの設定ポリシーを作成する
3. Microsoft Intune Center を使用して設定を検証する

### ▶ 作業 1 : Microsoft Intune Center の設定ポリシーを作成する

1. Microsoft Intune 管理コンソールで、Microsoft Intune Center の設定用テンプレートに基づいて新しいポリシーを作成します。
2. [Microsoft Intune Center] ページで次を構成し、[ポリシーの保存] をクリックします。
    - ポリシーの名前 : Intune Center Settings
    - 名前 : Adatum Admins
    - 電話番号 : 204-555-0100
    - 電子メールアドレス : Admin@Adatum.com
    - Web サイトの名前 : Adatum Support
    - Web サイトの URL : http://www.adatum.com/support
3. メッセージ ダイアログが表示されたら、ポリシーを [すべてのコンピューター] グループに展開します。

### ▶ 作業 2 : Microsoft Intune エージェントの設定ポリシーを作成する

1. Microsoft Intune 管理コンソールで、Microsoft Intune エージェントの設定テンプレートに基づいて、新しいポリシーを作成します。
2. [推奨設定を使用してポリシーを作成および展開する] を選択し、次の設定を変更します。
    - 展開の管理 : Research Computers
    - マルウェアを駆除する前にシステムの復元ポイントを作成する : いいえ
    - 更新プログラムおよびアプリケーションの自動検出頻度 (時間) : 12
3. ポリシー設定を保存します。
4. [グループ] で、[すべてのデバイス] ノードをクリックします。
5. リモート タスクを実行して LON-CL1.Adatum.com のポリシーを更新します。

### ▶ 作業 3 : Microsoft Intune Center を使用して設定を検証する

1. LON-CL1 で、スタート メニューから [Microsoft Intune Center] を起動します。
2. Microsoft Intune Center の下部にあるサポート情報を確認します。
3. Microsoft Intune Center を閉じます。

**結果 :** この練習により、Intune のポリシー設定を構成することができました。

### ▶ 次の演習の準備をする

次の演習のために、仮想マシンを起動したままにします。

レッスン 3
# Intune によるモバイル デバイス管理

モバイル デバイス管理 (MDM) を使用すると、企業情報を引き続き確実に保護しながら、組織でさまざまな種類のデバイスを使用できるようになります。企業のユーザー ベースは、作業しやすいデバイスを柔軟に選択して作業効率を高めることができます。このレッスンでは、MDM の機能、要件、および Intune での操作手順について説明します。

### 目的

このレッスンにより、次のことを習得できます。

- Intune を使用して管理できるデバイスの種類について説明することができます。
- Intune がサポートする MDM 機能について説明することができます。
- MDM 機関を構成する方法を説明することができます。
- Intune を使用してモバイル デバイスを管理するための特定のモバイル デバイス要件について説明することができます。
- モバイル デバイスに適用できる MDM ポリシーについて説明することができます。
- モバイル デバイスをサポートするための管理タスクについて説明することができます。

## Intune による MDM 用モバイル デバイス サポート

Intune は、多様なモバイル デバイスおよびコンピューターをサポートしており、それらはモバイル デバイス管理ポリシー設定を使用して管理できます。ユーザーは、Microsoft Intune ポータル サイト アプリをインストールして、デバイスの登録と削除、発行されたアプリのインストール、および IT サポートへの問い合わせに役立てることができます。MDM 機能用に Intune に組み込む主な方法として、次の 2 つが用意されています。

| MDM ソリューション | デバイス サポート |
|---|---|
| 直接管理 | • Apple iOS 6.0 以降<br>• Android 4.0 以降<br>• Samsung KNOX<br>• Windows Phone 8 以降<br>• Windows 8.1 RT および Windows RT<br>• Windows 8.1 以降のコンピューター |
| Exchange ActiveSync | • Exchange ActiveSync が有効なあらゆるモバイル デバイス<br>• Windows Phone<br>• Nokia の携帯電話<br>• Android の携帯電話とタブレット<br>• iOS ベースの携帯電話とタブレット |

- **直接管理 :** Intune では、次の種類のデバイスに対してダイレクト管理をサポートしています。
  - **Apple iOS 6.0 以降 :** 新しく登録されるデバイスでは、iOS 7.1 以降が動作している必要がありますが、以前に登録された iOS 6.0 デバイスは、登録されたままとなり、管理対象として残ることに注意してください。
  - Android 4.0 以降 (Samsung KNOX を含む)
  - Windows Phone 8 以降
  - Windows 8.1 RT および Windows RT
  - **Windows 8.1 以降のコンピューター :** Windows 8.1 以降のコンピューターをモバイル デバイスとして管理できます。これをおこなうには、Open Mobile Alliance Device Management (OMA DM) プロトコルと OMA-URI (Windows 10 の場合) プロトコルをサポートする設定を構成します。

- **Exchange ActiveSync :** Exchange ActiveSync を使用してモバイル デバイスを登録している場合、On-Premises Connector をインストールして、Intune 内からお使いの Exchange Server に接続できます。Exchange Online を使用している場合、Service to Service Connector を構成して、Intune を Exchange のオンライン インスタンスに接続できます。この方法を使用すると、Exchange ActiveSync をサポートするあらゆる携帯電話やタブレットを管理できます。

**注 :** Microsoft Office 365 も、iOS、Android、および Windows Phone の各デバイスに対する最小限の MDM 機能を提供します。Office 365 管理センターを使用して、デバイスを管理できます。別の選択肢として、System Center 2012 R2 Configuration Manager と Intune を統合することもできます。このハイブリッド ソリューションを使用すると、Configuration Manager コンソールから完全な MDM 機能を活用できます。Intune を使用してデバイスを管理するためのさまざまな方法については、次のサイトを参照してください。
エンタープライズ モビリティを実現する方法
https://technet.microsoft.com/library/dn957912.aspx

## Intune によりサポートされる MDM 機能

Intune によりサポートされる MDM 機能は、管理対象のモバイル デバイス プラットフォームに基づいて異なりますが、すべてのデバイスで、次の高レベルの機能がサポートされます。

| カテゴリ | 機能 |
|---|---|
| デバイスのセキュリティと構成 | • 構成ポリシー<br>• パスワード管理<br>• リモート ワイプとリモート ロック<br>• カスタム ポリシー |
| アプリの管理 | • アプリの展開<br>• アプリの制限<br>• モバイル デバイスのアプリケーションの管理 |
| 企業リソースのアクセス | • VPN プロファイル<br>• Wi-Fi プロファイル<br>• 電子メール プロファイル<br>• 証明書プロファイル<br>• 条件付きアクセス ポリシーの構成 |
| インベントリとレポート処理 | • ハードウェア インベントリ<br>• アプリケーション インベントリ<br>• レポート機能 |

- **デバイスのセキュリティと構成 :** ほとんどのデバイスで、デバイスの機能、パスワード管理、リモート ワイプ、およびリモート ロックを管理するための構成ポリシーや、場合によってはカスタム ポリシーなどの MDM 機能がサポートされます。
- **アプリの管理 :** モバイル アプリを管理できます。これには、インストール ファイルやプラットフォームベースのアプリ ストアからの展開も含まれます。また、どのアプリをインストールするかを制御することもできます。最近の多くのモバイル プラットフォームでは、モバイル アプリケーション管理 (MAM) がサポートされます。MAM を使用すると、コピーや貼り付け、データの外部バックアップ、アプリ間のデータ転送などのアプリケーションの動作を制限できます。
- **企業リソースのアクセス :** ユーザーは、ドキュメント リポジトリや内部サービスなどの企業リソースにアクセスすることが必要な場合があります。このようなアクセスを可能にするために、VPN プロファイル、Wi-Fi プロファイル、電子メール プロファイル、証明書プロファイル、および条件付きアクセス プロファイルを構成できます。
- **インベントリとレポート処理 :** 登録されているすべてのデバイスは、ハードウェアとアプリケーションの両方のインベントリを提供するので、Intune に組み込まれているレポート機能を使用してコンプライアンスを監視できます。

## MDM 機関の構成


Intune で MDM を構成する場合、まず、MDM 機関を決定します。Microsoft Intune をスタンドアロン モードで使用する場合、Intune がデバイスを管理するので、MDM 機関は容易に決定できます。ただし、System Center 2012 R2 Configuration Manager を使用する場合、または Office 365 MDM ソリューションを使用する場合、注意を払って MDM 機関を決定する必要があります。現在、MDM 機関をいったん設定すると、この設定を変更するには Microsoft サポートの支援が必要になります。

Intune 用に MDM 機関を設定するには、次の手順を実行します。

1. Microsoft Intune 管理コンソールで、[管理者]、[モバイル デバイス管理] の順にクリックします。
2. 詳細ウィンドウで、[モバイル デバイス管理機関の設定] をクリックします。

## モバイル デバイスを管理するための前提条件

考慮が必要な Intune デバイスの前提条件
- Microsoft Intune ポータル サイト アプリ
- iOS 用 APNs 証明書
- Windows Phone 用のアプリ署名をサポートするための証明書
- Windows 用のサイドローディング キー
- Windows 用の DNS CNAME
  - enterpriseenrollment.<組織ドメイン名>(manage.microsoft.com へのポイント用)
  - enterpriseregistration.<組織ドメイン名>(enterpriseregistration.windows.net へのポイント用)

管理対象のデバイス プラットフォームによっては、特定のプラットフォーム前提条件を考慮することが必要な場合があります。次に、それらの前提条件を示します。

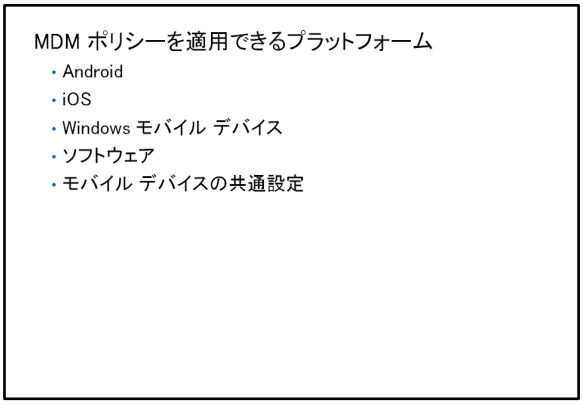
- **Microsoft Intune ポータル サイト アプリ :** Android、iOS、および Windows などのオペレーティング システムでは、各プラットフォームのアプリ ストアからダウンロードできるポータル サイト アプリがサポートされます。
- **iOS 用 APNs 証明書 :** iOS モバイル デバイスを管理するには、Apple Push Notification Service (APNs) 証明書が必要です。この証明書は、Intune で要求、更新、およびアップロードをおこなうことができます。これをおこなうには、[管理者] にアクセスし、[iOS および MacOS X] ノードの下で、[APNs 証明書のアップロード] をクリックします。このノードは、MDM 機関を構成した後でのみ表示されます。
- **Windows Phone 用のアプリ署名をサポートするための証明書 :** Windows Phone 8、または Windows ストアにアクセスしないか、サイドローディングされた基幹業務 (LOB) アプリを必要とする Windows Phone 8.1 をサポートする場合、Windows Phone デベロッパー センター アカウントを要求し、Symantec のコード署名証明書を購入する必要があります。また、この証明書を使用して、Microsoft Intune ポータル サイト アプリを署名します。これは、Windows Phone 8 の要件です。
- **Windows 用のサイドローディング キー :** Windows ストア アプリを Windows デバイスにインストールする場合、サイドローディング キーを取得して、Intune に追加する必要があります。
- **Windows 用の DNS CNAME :** ドメイン ネーム システム (DNS) の正規名 (CNAME) レコードを作成することにより、Windows Phone およびコンピューターが容易に Intune を見つけたり、登録を実行したりできるようすることができます。次の CNAME レコードを作成する必要があります。
  - enterpriseenrollment.<組織のドメイン名> (manage.microsoft.com へのポイント用)

- enterpriseregistration.<組織のドメイン名> (enterpriseregistration.windows.net へのポイント用)

**参考資料 :** Intune でデバイス登録をセットアップする方法または特定のデバイス要件については、次のサイトを参照してください。
Microsoft Intune にデバイスを登録する準備
https://technet.microsoft.com/ja-jp/library/dn646962.aspx

## MDM ポリシーの概要

Intune には、管理対象コンピューターと同様に、管理対象モバイル デバイス用のポリシー テンプレートも用意されています。各モバイル プラットフォームには、セキュリティと機能ベースの設定を構成するための特定のテンプレート設定があります。具体的には、次のものがあります。




- Android
- iOS
- Windows
- ソフトウェア
- モバイル デバイスの共通設定

### Android

Android デバイス用の設定を管理するために、次のテンプレートを使用できます。

- **全般構成ポリシー :** パスワード長、暗号化設定、および許可またはブロックされるアプリなどの設定が含まれます。このテンプレートは、ユーザー グループまたはデバイス グループに展開できます。
- **カスタム構成ポリシー :** OMA-URI 設定を含むポリシーを作成して展開できます。このテンプレートは、ユーザー グループに対してのみ適用できます。
- **Samsung KNOX 用電子メール プロファイル :** Exchange ActiveSync などの電子メール プロファイル用の設定が含まれます。このテンプレートは、ユーザー グループに対してのみ適用できます。
- **PKCS #12 (.PFX) 証明書プロファイル :** PFX モバイル デバイス証明書プロファイルが含まれます。このテンプレートは、ユーザー グループに対してのみ適用できます。
- **SCEP 証明書プロファイル :** Simple Certificate Enrollment Protocol (SCEP) 証明書プロファイル用の設定が含まれます。これには、証明書の種類と有効期間が含まれます。このテンプレートは、ユーザー グループに対してのみ適用できます。
- **信頼済み証明書プロファイル :** 信頼済みのモバイル デバイス証明書に関連する設定が含まれます。このテンプレートは、ユーザー グループに対してのみ適用できます。
- **VPN プロファイルと Wi-Fi プロファイル :** VPN または Wi-Fi に接続するための設定が含まれます。このテンプレートは、ユーザー グループに対してのみ適用できます。

### iOS

次のテンプレートを使用して作成されたポリシーを iOS デバイスに適用できます。

- **電子メール プロファイル :** Exchange ActiveSync などの電子メール プロファイル用の設定が含まれます。このテンプレートは、ユーザー グループに対してのみ適用できます。

- **全般構成ポリシー :** パスワード長、暗号化設定、および許可またはブロックされるアプリなどの設定が含まれます。このテンプレートは、ユーザー グループおよびデバイス グループの両方に展開できます。
- **カスタム構成ポリシー :** Apple Configurator を使用して作成した iOS デバイス用のプロファイルをアップロードできます。このテンプレートは、ユーザー グループおよびデバイス グループの両方に展開できます。
- **SCEP 証明書プロファイル :** SCEP 証明書プロファイル用の設定が含まれます。これには、証明書の種類と有効期間が含まれます。このテンプレートは、ユーザー グループに対してのみ適用できます。
- **信頼済み証明書プロファイル :** 信頼済みのモバイル デバイス証明書に関連する設定が含まれます。このテンプレートは、ユーザー グループに対してのみ適用できます。
- **VPN プロファイルと Wi-Fi プロファイル :** VPN または Wi-Fi に接続するための設定が含まれます。このテンプレートは、ユーザー グループに対してのみ適用できます。

### Windows モバイル デバイス

次のテンプレートを使用して作成されたポリシーを Windows モバイル デバイスに適用できます。

- **電子メール プロファイル :** Exchange ActiveSync などの電子メール プロファイル用の設定が含まれます。このテンプレートは、ユーザー グループに対してのみ適用できます。
- **SCEP 証明書プロファイル :** SCEP 証明書プロファイル用の設定が含まれます。これには、証明書の種類と有効期間が含まれます。このテンプレートは、ユーザー グループに対してのみ適用できます。
- **信頼済み証明書プロファイル :** 信頼済みのモバイル デバイス証明書に関連する設定が含まれます。このテンプレートは、ユーザー グループに対してのみ適用できます。
- **VPN プロファイル :** VPN または Wi-Fi に接続するための設定が含まれます。このテンプレートは、ユーザー グループに対してのみ適用できます。
- **Windows 10 用全般構成ポリシー :** Windows 10 に関連する機能設定やパスワード設定などの設定が含まれます。カスタム ポリシーを使用すると、OMA-URI 設定を含むポリシーを構成することもできます。
- **Windows Phone とカスタム構成ポリシー :** Windows Phone に関連する機能設定やパスワード設定などの設定が含まれます。カスタム ポリシーを使用すると、OMA-URI 設定を含むポリシーを構成することもできます。
- **Windows Wi-Fi インポート ポリシー :** Wi-Fi プロファイルをインポートできます。

### ソフトウェア

次のテンプレートをモバイル デバイスに適用できます。

- **Android 用 Managed Browser ポリシー :** このテンプレートには、インターネット ブラウザー アプリを管理および制御するための設定が含まれます。
- **iOS 用 Managed Browser ポリシー :** このテンプレートには、インターネット ブラウザー アプリを管理および制御するための設定が含まれます。
- **Android 用モバイル アプリケーション管理ポリシー :** このテンプレートには、Android デバイス用の管理対象アプリケーションに関連する設定が含まれます。
- **iOS 用モバイル アプリケーション管理ポリシー :** このテンプレートには、iOS デバイス用の管理対象アプリケーションに関連する設定が含まれます。

### モバイル デバイスの共通設定

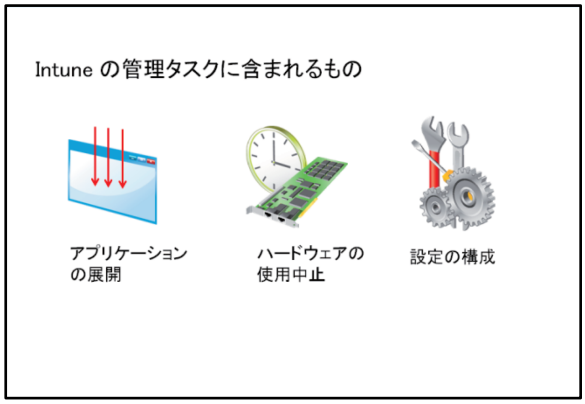
次のテンプレートをモバイル デバイスに適用できます。

- **Exchange ActiveSync ポリシー :** このテンプレートには、すべてのプラットフォームを対象にする、Exchange ActiveSync を管理するための設定が含まれます。
- **モバイル デバイスのセキュリティ ポリシー :** サポートされているすべてのデバイスに対して、このテンプレートを使用してパスワード長と暗号化を定義します。

## モバイル デバイスの管理

モバイル デバイスでは、次の管理タスクを実行することが必要になることがあります。

- **アプリケーションの展開 :** アプリケーションを対応するアプリ ストアから展開する、またはプラットフォームによっては、アプリケーションを直接インストールする、のいずれかを選択できます。
- **ハードウェアの使用中止 :** デバイスがその使用期間を経過したら、[インベントリからの削除/ワイプ] コマンドを発行できます。デバイスを工場出荷時の設定に戻す完全なワイプまたは企業データのみをデバイスから削除する選択的なワイプのいずれかを実行できます。




**参考資料 :** Intune によるリモート ワイプ、リモート ロック、またはパスコード リセットの機能を使用したデータの保護する方法については、次のサイトを参照してください。
Microsoft Intune によるリモート ワイプ、リモート ロック、パスコードのリセットを使用したデータの保護
https://technet.microsoft.com/library/jj676679.aspx

### 知識の確認

| **質問** | |
|---|---|
| **次のうち、MDM のためのプラット フォーム前提条件はどれですか (適合するものをすべて選択します)。** | |
| 正しい解答を選択してください。 | |
| | Windows 用 APNs 証明書 |
| | iOS 用 APNs 証明書 |
| | Windows 用の DNS CNAME |
| | AD DS でのグループ ポリシー設定 |

記述が正しい場合は、右側の列にチェック マークを入れます。

| **記述** | **解答** |
|---|---|
| Microsoft Intune は Windows RT デバイスをサポートします。 | |

# 演習 B : Microsoft Intune によるモバイル デバイスの管理

## シナリオ

A. Datum 社は、Microsoft Intune MDM による管理が必要な数多くのモバイル デバイスをサポートしています。あなたは、Windows 10 クライアントを使用して MDM の機能をテストすることになりました。

## 目的

この演習により、次のことを習得できます。

- モバイル デバイスを構成し、Microsoft Intune に登録することができます。

## 演習のセットアップ

予定所要時間 : 30 分

| | |
|---|---|
| 仮想マシン | 23697-2B-LON-DC1<br>23697-2B-LON-CL1<br>23697-2B-LON-CL2<br>MSL-TMG1 |
| ユーザー名 | Adatum¥Administrator<br>Adatum¥Don |
| パスワード | Pa$$w0rd |

この演習では、用意された仮想マシン環境を使用します。演習を開始する前に、次の手順を実行する必要があります。

1. ホスト コンピューターで、Hyper-V マネージャーを起動します。
2. Hyper-V マネージャーで [23697-2B-LON-DC1] をクリックし、操作ウィンドウで [起動] をクリックします。
3. 操作ウィンドウで [接続] をクリックします。仮想マシンが起動するまで待ちます。
4. 次の資格情報を使用してサインインします。
    - ユーザー名 : Adatum¥Administrator
    - パスワード : Pa$$w0rd
5. 23697-2B-LON-CL1 に対して、手順 2 ～ 3 を繰り返します。ユーザー名「Adatum¥Don」、パスワード「Pa$$w0rd」を使用してサインインします。
6. 23697-2B-LON-CL2 に対して、手順 2 ～ 3 を繰り返します。指示されるまで、サインインしないでください。
7. インターネットへのアクセスのために、MSL-TMG1 を起動します。

この演習を正常に完了するために、「演習 A : Intune クライアント ソフトウェアのインストールとポリシーの構成」を完了させる必要がります。また、演習 A で必要な以前の前提条件をすべて完了する必要もあります。

# 練習 : モバイル デバイスの構成と Microsoft Intune への登録

## シナリオ

組織の MDM 機能をサポートするために Intune を準備しているところです。MDM 機関を構成し、ポリシー設定を作成して適用し、Microsoft Intune ポータル サイト アプリをインストールして、モバイル デバイスを Intune に登録する必要があります。

主な作業は次のとおりです。

1. MDM 機関を構成する
2. MDM ポリシーを作成する
3. Microsoft Intune に登録する

### ▶ 作業 1 : MDM 機関を構成する

1. LON-CL1 に切り替え、Internet Explorer を開きます。
2. Internet Explorer で、http://manage.microsoft.com にアクセスします。
3. Microsoft Intune 管理コンソールにアクセスするための資格情報を入力します。
4. [管理者] で、[モバイル デバイス管理] を参照します。
5. [モバイル デバイス管理機関] を設定して Microsoft Intune を使用します。

### ▶ 作業 2 : MDM ポリシーを作成する

1. 必要に応じて、LON-CL1 で、http://manage.microsoft.com を参照し、資格情報を入力して、Microsoft Intune 管理コンソールにアクセスします。
2. [ポリシー] で、[全般構成 (Windows 10 Desktop および Mobile 以降)] に基づいて新しいポリシーを作成し、次を指定します。
   - 名前 : Windows 10 Mobile Device Policy
   - デバイスのロック解除にパスワードを必要とする : はい
   - 必要なパスワードの種類 : 英数字
   - 最小文字セット数 : 1
   - パスワードの最小文字数 : 6
3. ポリシーをすべてのモバイル デバイス グループに展開します。

### ▶ 作業 3 : Microsoft Intune に登録する

1. LON-CL2 で、ユーザー名「Adatum¥Don」、パスワード「Pa$$w0rd」を使用してサインインします。
2. スタート メニューで、[設定]、[アカウント]、および [職場のアクセス] の順に開きます。
3. [職場のアクセス] ページで「DonFunk@<ドメイン>.onmicrosoft.com」と入力し、Microsoft Intune に接続します。このアカウントは、第 8 章で作成しました。
4. メッセージ ダイアログが表示されたら、パスワードを「Pa$$w0rd」に変更します。
5. [Adatum Corporation] オブジェクトをクリックし、接続を同期します。
6. 開いているウィンドウをすべて閉じます。

**結果 :** この練習により、モバイル デバイスを構成し、Microsoft Intune に登録することができました。

### ▶ 次の章の準備をする

次の章の演習のために、仮想マシンを起動したままにします。

# 復習とまとめ

## 復習問題

**質問 :** Intune クライアント ソフトウェアと、OMA-URI によるデバイスの管理との違いは何ですか。

**質問 :** Microsoft Intune を使用して、どのような種類のモバイル デバイスを管理できますか。