

# Windows Intune

Windows Intune トライアル版 活用ガイド  
(2013 年 10 月 機能更新対応)

---

# 目次

---

|  |    |
|--|----|
| 1. 概要  | 4  |
| 2. Windows Intune の構成                                | 5  |
| 3. Windows Intune のサインアップ                            | 8  |
| 4. Windows のポータル                                     | 9  |
| 5. Windows Intune の導入準備                              | 12 |
| 5.1 管理者の追加   | 12 |
| 5.1.1 Windows Intune アカウントポータルの管理者                   | 12 |
| 5.1.2 Windows Intune 管理コンソールの管理者                     | 12 |
| 5.2 既定のポリシーの設定                                       | 16 |
| 5.3 Endpoint Protection の有効化                         | 17 |
| 5.4 管理対象のコンピューターの使用率帯域の計画                            | 18 |
| 6. Windows Intune へのユーザーとグループ、コンピューター、およびモバイルデバイスの追加 | 19 |
| 6.1 ユーザーおよびセキュリティグループの追加                             | 19 |
| 6.1.1 ユーザーおよびセキュリティグループの手動の追加                        | 19 |
| 6.1.2 Active Directory によるユーザーとセキュリティグループの自動の追加      | 21 |
| 6.2 ユーザーグループとデバイスグループの管理                             | 22 |
| 6.3 コンピューターの登録                                       | 24 |
| 6.3.1 管理者による登録                                       | 25 |
| 6.3.2 ユーザーによる登録                                      | 27 |
| 6.3.3 展開イメージへの組み込み                                   | 28 |
| 6.4 モバイルデバイスの登録                                      | 29 |
| 6.4.1 モバイルデバイス管理機能の有効化                               | 29 |
| 6.4.2 Windows RT デバイスの登録                             | 30 |
| 6.4.3 Windows Phone 8 デバイスの登録の準備                     | 34 |
| 6.4.4 Windows Phone 8 デバイスの登録                        | 35 |
| 6.4.5 iOS デバイスの登録の準備                                 | 37 |
| 6.4.6 iOS デバイスの登録                                    | 37 |
| 6.4.7 Android デバイスの登録                                |    |

|  |    |
|--|----|
| 7. アプリケーションの展開                             | 39 |
| 7.1 モバイルデバイス用アプリケーションの展開                   | 39 |
| 7.2 Windows RT (Windows 8) アプリケーションのセットアップ | 40 |
| 7.3 Windows Phone 8 アプリケーションのセットアップ        | 42 |
| 7.4 iOS アプリケーションのセットアップ                    | 42 |
| 7.5 Android アプリケーションのセットアップ                | 43 |
| 8. Windows Intune の環境の最適化                  | 44 |
| 8.1 更新プログラムと自動承認の管理                        | 44 |
| 8.2 アラート通知のセットアップ                          | 45 |
| 8.3 レポートの作成                                | 47 |
| 8.4 デバイスの削除                                | 49 |
| 9. まとめ                                     | 52 |
| 10. リソース                                   | 54 |

# 1. 概要

---

このドキュメントは、はじめて Windows Intune を使用される方を対象に、Windows Intune 環境のセットアップと、Windows Intune の主要機能について紹介します。ドキュメントでは、実際の Windows Intune の画面ショットとともに構成手順を示します。読者は記載された手順を実行して、自社のビジネス ニーズに適した環境を作成し、カスタマイズすることができます。

## ●改訂履歴

| バージョン | 年月日             | 内容 |
|-------|-----------------|----|
| 1.0   | 2014 年 3 月 27 日 | 初版 |
|       |                 |    |
|       |                 |    |
|       |                 |    |

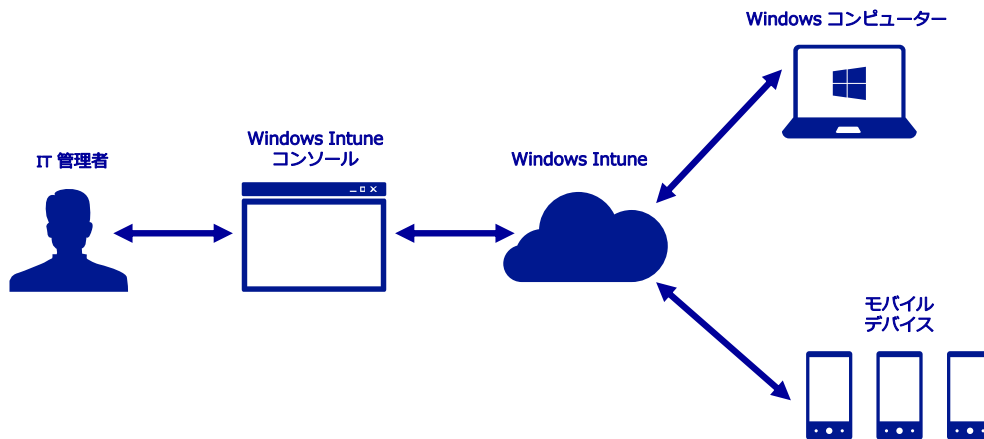
## 2. Windows Intune の構成

---

Windows Intune の構成には、「クラウド単体構成」と「ハイブリッド構成」があります。

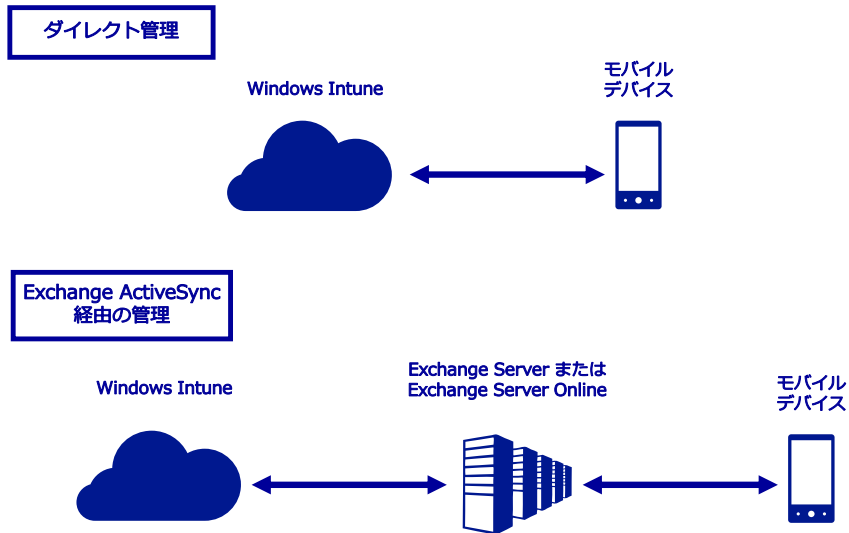
### ●クラウド単体構成

社内設置型のインフラストラクチャを必要としない場合は、Windows Intune をクラウド単体構成で運用できます。その場合、構成は図 1 のようになります。



●図 1 ●クラウド単体構成における Windows Intune

Windows Intune は、Windows コンピューター以外に、Windows RT、Windows Phone 8、iOS、Android の各モバイルデバイスを直接管理することができます。これを「ダイレクト管理」と呼びます。また、組織が Exchange Server または Exchange Online Server でモバイルデバイスを管理している場合、Exchange Server 経由でモバイルデバイスを管理することもできます。これを「Exchange ActiveSync 経由での管理」と呼びます。

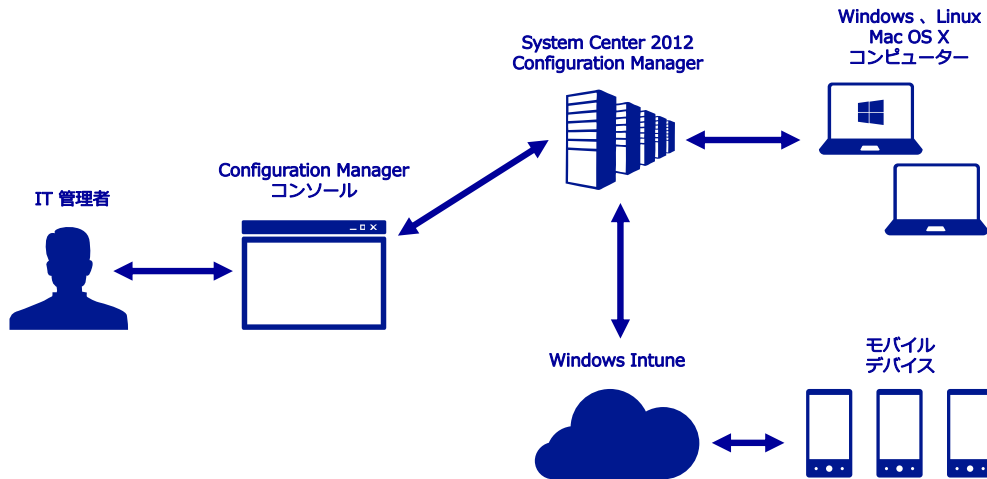


●図 2 ●ダイレクト管理と Exchange ActiveSync 経由の管理

## ●ハイブリッド構成

Windows Intune には、オプションとしてハイブリッド構成も選択できます。このオプションでは、クラウドベースの環境を Microsoft System Center 2012 Configuration Manager SP1 または Microsoft System Center 2012 R2 Configuration Manager（以後、まとめて Microsoft System Center 2012 Configuration Manager と称す）と統合、連携させることが可能になります。この構成では、Configuration Manager コンソールを使用して、PC、サーバー、モバイルデバイス、さらには Mac OS コンピューターまで管理できます。

ハイブリッド構成の場合、System Center 2012 Configuration Manager によってコンピューターが管理され、モバイルデバイスを管理する Windows Intune サービスを Configuration Manager 管理コンソールにコネクタを使って追加します。次の図は、ハイブリッド構成ですべてのサポート対象プラットフォームが管理されるしくみの例を示しています。



●図 3●ハイブリッド構成における Windows Intune

ハイブリッド構成を使用する場合、System Center 2012 Configuration Manager のセットアップ方法に関する技術ガイダンスの詳細については、「[System Center 2012 Configuration Manager の概要](#)」を参照してください。

このドキュメントではクラウド単体構成の Windows Intune サービスを最大限に活用するための情報を提供します。

### 3. Windows Intune のサインアップ

---

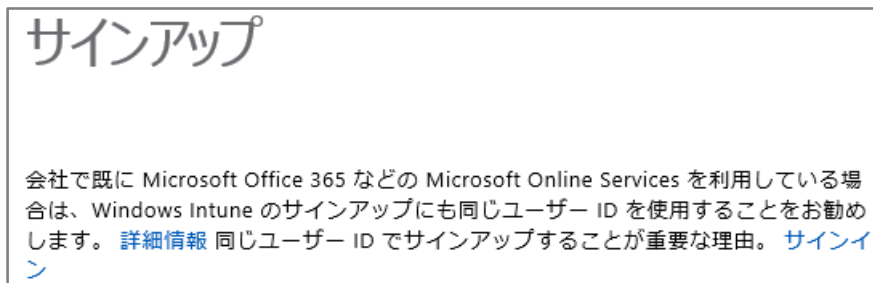
Enterprise Agreement または同等のボリュームライセンス契約をマイクロソフトと締結していない企業のお客様は、次の Web サイトから Windows Intune の 30 日間無料トライアルにサインアップできます。

[http://www.microsoft.com/ja-jp/windows/Windows Intune/try.aspx](http://www.microsoft.com/ja-jp/windows/Windows%20Intune/try.aspx)

#### ■重要■

お客様の組織が Enterprise Agreement (EA) を締結している場合は、マイクロソフト担当者にお問い合わせください。担当者がエンタープライズ向けのトライアル版をセットアップするお手伝いをいたします。

「30 日間無料トライアルの入手」をクリックすると、「サインアップ」ページが表示されます。このページの左上には次のようなメッセージが表示されています。



●図 4●サインイン

会社で既に Microsoft Online Services の組織 ID (OrgID) をお持ちの場合は、このテキストの「サインイン」オプションをクリックし、そのアカウントの全体管理者アカウントを使用して認証を行ってください。これにより、Windows Intune のトライアル版が既存の Microsoft Online Services アカウントに確実に関連付けられます。

#### ■重要■

既存の Microsoft Online Services アカウントをお持ちでない場合、この「サインアップ」フォームに詳細情報を入力して、組織の新しいドメイン名を作成します。



## 4. Windows Intune のポータル

Windows Intune サービスのさまざまな機能にアクセスするために使用できる、2 種類の管理者向けのポータルと 1 種類のユーザー向けのポータルがあります。図 5 の Windows Intune アカウントポータルと、図 6 の Windows Intune 管理コンソール、そして図 7 の Windows Intune 会社のポータルです。

### ● Windows Intune アカウントポータル (<https://account.manage.microsoft.com>)

Windows Intune アカウントポータルは、Windows Intune や Office365 などのすべての Microsoft Online Services のユーザー、グループ、およびドメインを管理者が管理するための共通の構成用インタフェースです。このページでは、サブスクリプションの状態の確認、新しいサブスクリプションの追加、および新しいユーザーアカウントのアクティブ化を行うことができます。社内設置型の Active Directory ドメインサービス (AD DS) インスタンスへのリンクをセットアップして構成することもできます。またこのポータルは、エンドユーザー向けに、各自のパスワードを変更する機能を備えています。



● 図 5 ● Windows Intune アカウントポータル

### ● Windows Intune 管理コンソール (<https://admin.manage.microsoft.com>)

Windows Intune 管理コンソールは、3 つの主要な情報パネルで構成されます。左側はナビゲーションパネルで、各 Windows Intune ワークスペースへのリンクが含まれています。Windows Intune の各機能にはワークスペースが存在します。画面中央はメインの情報パネルで、ワークスペース（この例では、[システムの概要] ワークスペース）の詳細ビューが表示されます。右側は [タスク] パネルで、そのワークスペースで使用可能なタスクが状況に応じて一覧表示されます。

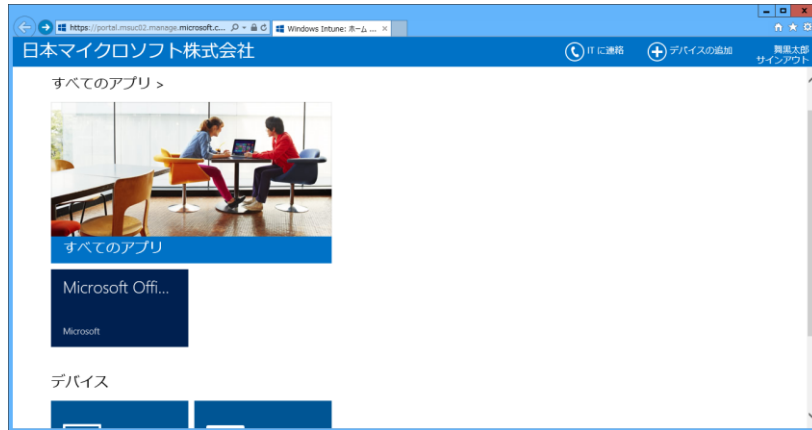


●図 6●Windows Intune 管理コンソール

この時点では、まだシステムにコンピューターを登録していないため、表示される情報は多くありませんが、各領域で使用可能なワークスペースとタスクに今から慣れておくことができます。

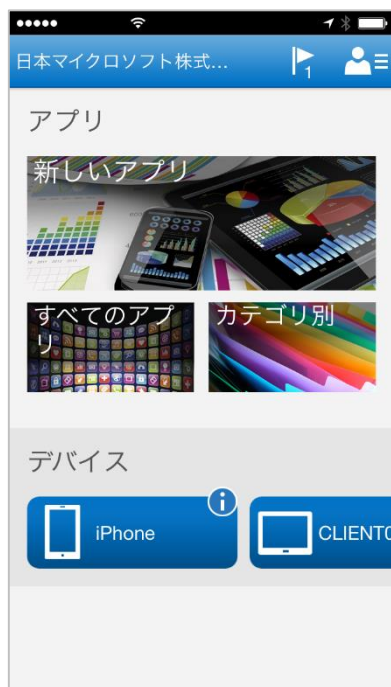
## ●Windows Intune 会社のポータル (<https://portal.manage.microsoft.com>)

Windows Intune 会社のポータルは、ユーザーがカタログ一覧からアプリケーションやソフトウェアを選択してインストールするための Web インタフェースです。カタログ一覧は、ユーザーの部署や職位、適正に合わせてカスタマイズすることができます。



●図 7● Windows Intune 会社のポータル (Web インタフェース)

また、Windows ストア、iOS および Android のモバイルデバイス向けの会社のポータルアプリも用意されています。



●図 8● モバイルデバイス向けの開始のポータルアプリ (iOS)

## 5. Windows Intune の導入準備

---

Windows Intune に管理対象となるコンピューターまたはモバイルデバイスを追加する前に、管理者と既定のポリシーを設定しておく必要があります。

### 5.1 管理者の追加

Windows Intune では、Windows Intune アカウントポータルと Windows Intune 管理コンソールで役割の異なる管理者を個別に設定することができます。

#### 5.1.1 Windows Intune アカウントポータルの管理者

Windows Intune アカウントポータルでは、サブスクリプション、サービスリクエスト、パスワードのそれぞれの管理する次の管理者を設定することができます。

|   |  |
|---|--|
| 課金管理者<br>(Billing Administrator)        | 購入、サブスクリプションの管理、サポートチケットの管理、サービスの正常性の監視をおこないます。                  |
| サービス管理者 (Service Support Administrator) | サービスリクエストの管理とサービスの正常性の監視をおこないます。                                 |
| パスワード管理者                                | パスワードの再設定、サービスリクエストの管理、およびサービスの正常性の監視をおこないます。                    |
| ユーザー管理の管理者                              | パスワードの再設定とサービスの正常性の監視、およびユーザーアカウント、ユーザーグループ、サービスリクエストの管理をおこないます。 |
| 全体管理者                                   | すべての管理機能にアクセスできます。   |

#### 5.1.2 Windows Intune 管理コンソールの管理者

組織内で管理を委任できるよう、Windows Intune 管理コンソールへのアクセスを提供する、2 つのレベルの管理者の役割があります。

## ●Windows Intune テナント管理者

Windows Intune テナント管理者には、Windows Intune 管理コンソールに対する完全な管理者権限が付与されます。そのため、Windows Intune サービス管理者の追加と削除など、あらゆる操作をコンソールで行うことができます。さらに、テナント管理者は、Windows Intune アカウントポータルを使用して、他のテナント管理者を割り当てることもできます。テナント管理者は、Windows Intune アカウントポータルで割り当てる必要があることに注意してください。テナント管理者の割り当てに Windows Intune 管理コンソールを使用することはできません。

## ●Windows Intune サービス管理者

Windows Intune サービス管理者には、フルアクセスと読み取り専用の 2 つのレベルのコンソールアクセスが付与されます。

|            |   |
|------------|---|
| フルアクセス     | Windows Intune 管理コンソールのすべての管理権限が付与されるため、他のサービス管理者の追加と削除など、あらゆる操作をコンソールで行うことができます。           |
| 読み取り専用アクセス | 読み取り専用権限が付与されるため、Windows Intune 管理コンソールでデータを変更することはできません。コンソールでのデータの表示とレポートの作成のみを行うことができます。 |

サービス管理者を作成するには、Windows Intune 管理コンソールを使用します。サービス管理者はユーザーID とパスワードを持ち、Windows Intune ユーザーグループのメンバーである必要があります。ユーザーID を所有していない個人の場合、まず、テナント管理者が、Windows Intune アカウントポータルを使用してその個人のユーザーID を作成し、Windows Intune ユーザーグループのメンバーとして含める必要があります。

## ■注意■

Windows Intune サービス管理者は、Windows Intune アカウントポータルに表示されるサービス管理者とは異なります。Windows Intune アカウントポータルに表示される Microsoft Online Services のサービス管理者は、ユーザーのアカウントとグループおよびサービスリクエストを管理し、サービスの状態を監視しますが、必ずしも Windows Intune で管理されているユーザーやデバイスの状態とは限りません。

既定では、サブスクリプションの所有者が Windows Intune サービスのテナント管理者となります。テナント管理者とは、購入時に Microsoft Online サブスクリプション契約（MOSA）に同意した個人のことであり、Windows Intune 管理コンソールのすべてのタスクを実行する権利があります。

タスクの委任を支援するため、およびその単一アカウントのパスワードを忘れた場合にロックアウトされることを防ぐために、追加の管理者を作成してください。

## ▼Windows Intune テナント管理者を追加するには

次の手順に従って、少なくとも 1 つのテナント管理者アカウントを追加で作成することをお勧めします。なお、Windows Intune アカウントポータルでは、テナント管理者は全体管理者と表示されます。

(1) Windows Intune アカウントポータルにサインインして、[管理] の下の [ユーザー] メニュー項目をクリックします。

(2) テナント管理者に昇格させるユーザーの横にあるチェックボックスをオンにして [編集] をクリックするか、[新規] をクリックして新しいユーザーを追加します。

(3) [設定] を選択し、の [役割の割り当て] の [はい] ラジオボタンをオンにして、[全体管理者] を選択します。



●図 9●テナント管理者の追加

(4) ユーザーの連絡用電子メールアドレスを入力し、[保存] をクリックします。

## ▼サービス管理者を作成するには

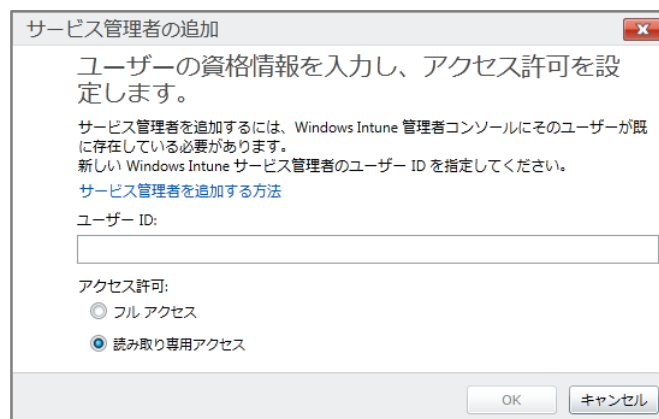
テナント管理者アカウントは日常的な IT サポートタスクに使用されないようにする必要があります。そのために、サービス管理者をセットアップしてください。Windows Intune で日常的な管理タスクを行うサービス管理者を追加するには、次の手順を実行します。

(1) Windows Intune アカウントポータルで、サービス管理者として登録するユーザーのユーザーアカウントを作成します。

(2) Windows Intune 管理コンソールにサインインし、それらのユーザーが [すべてのユーザー] グループ内に表示されていることを確認します。

(3) [管理] の [サービス管理者] をクリックします。

(4) [追加] をクリックすると、次のようなウィンドウが表示されます。



●図 10●サービス管理者の追加

(5) ユーザーID を入力し、そのユーザーに対するアクセス許可を選択したら、[OK] をクリックします。

(6) この Windows Intune アカウントのサービス管理者にするすべてのユーザーID に対して、上記の手順を繰り返します。

サービスの管理者をセットアップしたら、デバイスを展開する環境をセットアップできます。次の数ページでは、アカウントへのコンピューターまたはモバイルデバイスの展開を開始する前に実行することが推奨される、いくつかの追加手順について確認します。

## 5.2 既定のポリシーの設定

Windows Intune のポリシーの主な目的は、モバイルデバイスのセキュリティ設定の制御、コンピューターの更新プログラムの提供、確実なエンドポイント保護、ファイアウォール設定の保守を行い、エンドユーザーエクスペリエンスの向上を実現するための、迅速かつわかりやすい設定を提供することです。これらの設定は、コンピューターが参加しているドメインに関係なく適用でき、ドメインに参加していないコンピューターにも適用できます。

### ■注意■

ポリシー管理システムの競合によってポリシーの競合が発生するのを防ぐため、Windows Intune クライアントソフトウェアを展開する際に、Windows Intune ポリシーで管理されているコンピューターが Active Directory グループポリシーからも同じ構成設定を受け取ることのないようにする必要があります。詳細については、Windows Intune オンラインヘルプの「[Windows Intune を使用する際のグループ ポリシーに関連する計画](#)」を参照してください。

次の手順では、コンピューターの Windows Intune エージェントの設定ポリシーをセットアップする方法について説明します。

### ▼既定の Windows Intune ポリシーをセットアップするには

- (1) Windows Intune 管理コンソールを開きます。
- (2) ワークスペースのショートカットウィンドウの [ポリシー] アイコンをクリックします。
- (3) [タスク] の下にある [ポリシーの追加] をクリックします。
- (4) [新しいポリシーの作成] ダイアログボックスの左側のウィンドウにあるテンプレートの一覧の中に、次のポリシーテンプレートが表示されます。



- ・ Windows Intune Center の設定
- ・ Windows Intune エージェントの設定
- ・ Windows ファイアウォールの設定
- ・ モバイルデバイスのセキュリティポリシー

## ■ 注意 ■

特定のポリシーの設定については、Windows Intune オンラインヘルプの「[Windows Intune エージェント ポリシーのリファレンス](#)」を参照してください。

(5) 推奨設定で展開するには、セットアップするポリシーテンプレートを選択し、[推奨設定を使用してポリシーを作成および展開する] をクリックします。このポリシーを作成する前に設定を表示するには、[このポリシーテンプレートの推奨設定を表示] をクリックします。(手順 8 に飛びます)

(6) 推奨設定にカスタマイズをするには、[カスタムポリシーの作成および展開] をクリックし、既定のポリシーに変更を構成した後、ポリシーの名前と説明（省略可）を入力して、[ポリシーの保存] をクリックします。

(7) ポリシーを今すぐ展開するかどうかの指定を要求するメッセージが表示されたら、[はい] をクリックします。

(8) [このポリシーを展開するグループを選択します。] ダイアログボックスで、(選択したポリシーに応じて) [すべてのデバイス] グループまたは [すべてのユーザー] グループを選択し、[OK] をクリックします。

(9) 他の既定のポリシーの設定に対して、これらの手順を必要に応じて繰り返します。

これらのポリシーが展開されると、すべてのユーザーまたはデバイスがこれらの設定を基本ポリシーとして継承します。また、[ポリシー] ワークスペースからこれらのポリシーの詳細をレビューし、必要に応じて編集できます。

## 5.3 Endpoint Protection の有効化

Endpoint Protection は、マルウェア対策を含むコンピューターのエンドポイント保護を実現します。Windows Intune の管理対象となるコンピューターに Endpoint Protection がインストールされるか、また有効化されるかは、Windows Intune ポリシーの [Windows Intune エージェントの設定] により決定されます。[Windows Intune エージェントの設定] には、[Endpoint Protection のインストール] と [Endpoint Protection を有効にする] のポリシー設定があります。また、[サードパーティ制エンドポイント保護アプリケーションがインストールされている場合でも Endpoint Protection をインストールする] のポリシー設定もあります。このポリシー設定は、Symantec や McAfee、Trend Micro の既存のマルウェア対策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に対する挙動を決定します。なお、既定では、これらのポリシー設定はすべてのデバイスで有効となっています。

コンピューターを Windows Intune サービスに追加する前に、エンドポイントの保護の要件を考慮します。既存のエンドポイント保護アプリケーションの代わりに Windows Intune Endpoint Protection を使用するか、または既存のアプリケーションを引き続き使用するかを決定します。管理対象のコンピューターがセキュリティで保護されていない状態にならないよう、いずれかの手法を実装する方法については、Windows Intune オンラインヘルプの「[Windows Intune Endpoint Protection または既存のエンドポイント保護アプリケーションの使用](#)」を参照してください。

## 5.4 管理対象のコンピューターの使用帯域幅の計画

Windows Intune で管理されているコンピューターは、Windows Intune 関連の操作のために追加のネットワーク帯域幅を使用することを覚えておいてください。管理対象のコンピューターに Windows Intune クライアントソフトウェアをインストールする前に、既存のネットワークトラフィックおよび Windows Intune の実装による増加を考慮する必要があります。Windows Intune の帯域幅の計画に影響を与える要因に関する情報、および包括的な展開計画のガイダンスについては、Windows Intune オンラインヘルプの「[Windows Intune クライアントの展開と登録のための計画](#)」を参照してください。

## 6. Windows Intune へのユーザーとグループ、コンピューター、およびモバイルデバイスの追加

---

次に Windows Intune を使用するユーザーとグループを追加します。また、管理対象となるコンピューターとモバイルデバイスも追加します。

### 6.1 ユーザーおよびセキュリティグループの追加

Windows Intune では、「ユーザーグループ」と「デバイスグループ」の 2 種類のグループを使用します。ユーザーグループに対しては、ソフトウェアを公開してポータルサイトからのインストールを可能にしたり、ユーザーに紐づくモバイルデバイス向けのセキュリティポリシーを適用したりできます。一方、デバイスグループを使用すると、ソフトウェアおよび更新プログラムをコンピューターにプッシュで展開したり、デバイス単位で Endpoint Protection の状況を監視したり、Windows Intune エージェントの設定ポリシーと Windows ファイアウォールの設定ポリシーを適用することができます。

また、ユーザーに Windows Intune ポータルサイトへのアクセス権を付与して、ユーザーが IT ヘルプデスクの支援なしに一般的なタスクを実行できるようにすることも可能です。ユーザーが Windows Intune 会社のポータルを使用して、Windows Intune 管理環境に対して各自のデバイスの追加または削除を行うこともできます。また、任意の利用可能なライセンスされたソフトウェアアプリケーションをインストールすることも可能です。

なお、Windows Intune 管理コンソールにユーザーとセキュリティグループが表示されるようにするには、事前に Windows Intune ポータルサイトにユーザーおよびセキュリティグループを手動で追加するか、Active Directory 同期を使用して、自動で追加しておく必要があります。

#### 6.1.1 ユーザーとセキュリティグループの手動の追加

Windows Intune アカウントポータルにユーザーまたはセキュリティグループ、またはその両方を手動で追加する手順は次のとおりです。

#### ▼手動でユーザーを追加するには

- (1) Windows Intune アカウントポータルを開きます。
- (2) ヘッダーで、[管理者] をクリックします。
- (3) 左側のウィンドウの [管理] の下にある [ユーザー] をクリックします。
- (4) [ユーザー] ページの [新規] をクリックし、[ユーザー] をクリックします。
- (5) [詳細] ページでユーザーの情報を入力します。[追加の詳細] の横にある矢印をクリックして、役職名や部門名などの任意のユーザー情報を追加して、[次へ] をクリックします。
- (6) [設定] ページで、ユーザーに管理者の役割を割り当てる場合は [はい] をクリックし、リストから管理者の役割を選択します。
- (7) [ユーザーの所在地の設定] の下でユーザーまたはユーザーの勤務地を選択して、[次へ] をクリックします。
- (8) [グループ] ページの [Windows Intune ユーザーグループ] の画面で、チェックボックスが選択されていることを確認します。
- (9) [結果を電子メールで送信] ページで、[電子メールを送信する] をチェックして、自分自身および選択した受信者宛てに、新しく作成したユーザーのユーザー名と一時的なパスワード（Windows Intune はパスワードを自動的に作成します）を電子メールで送信します。電子メールアドレスは、セミコロン (;) で区切って入力し、[作成] をクリックすることで、最大で 5 つの電子メールアドレスを入力できます。
- (10) [結果] ページに新しいユーザー名と一時的なパスワードが表示されます。結果を確認して、[完了] をクリックします。

## ■ 注意 ■

1 つのファイルソースから複数のユーザーアカウントを Windows Intune にインポートすることができます。ファイルはコンマ区切り値 (CSV) ファイルで、指定された形式に従う必要があります。

詳細については、Windows Intune オンラインヘルプの「[Windows Intune での一括インポートで複数のユーザーを追加](#)」を参照してください。

手動でセキュリティグループを Windows Intune アカウントポータルに追加する手順は次のとおりです。

## ▼手動でセキュリティグループを追加するには

- (1) Windows Intune アカウントポータルを開きます。
- (2) ヘッダーで、[管理者] をクリックします。
- (3) 左側のウィンドウの [管理] の下にある [セキュリティグループ] をクリックします。
- (4) [セキュリティグループ] ページで [新規] をクリックします。
- (5) [詳細] ページで、グループの表示名と説明を入力して、[保存] をクリックします。

### ■注意■

表示名には英数字またはスペースのみが利用可能です。

(6) [メンバーの選択] ページで、[リストの種類] リストから、新しいセキュリティグループに追加するメンバーの種類として [ユーザー] または [グループ] (他のセキュリティグループ) を選択します。選択されたリストの種類で利用できるメンバーが [利用できるメンバー] の下に表示されます。

(7) 追加する各メンバーの横にあるチェックボックスをオンにし、[追加] をクリックします。追加されたメンバーが [選択したメンバー] リストに表示されます。

(8) [選択したメンバー] リストからメンバーを削除するには、削除するメンバーの横にあるチェックボックスをオンにし、[削除] をクリックします。

(9) メンバーリストの作業が完了したら、[保存して閉じる] をクリックします。

## 6.1.2 Active Directory によるユーザーとセキュリティグループの自動の追加

Active Directory 同期を使用して、ローカルの Active Directory のユーザーとセキュリティグループをアカウントポータルに自動で追加することができます。これにより、管理者にとっては、アカウントの二重管理による負荷が軽減され、ユーザーにとっては、組織の資格情報を使用して、Windows Intune ヘシングルサインオンすることができるため、利便性が向上します。

Active Directory 同期では、別途、インストールが必要なディレクトリ同期ツールを使用して、ローカルの Active Directory のアカウントと Windows Azure Active Directory（以後、Windows Azure AD）を定期的に同期します。ローカルの Active Directory でアカウントの追加や削除をおこなうと、次の同期のタイミングで Windows Azure AD に反映されます。同期は 3 時間以内におこなわれ、強制的に同期させることもできます。なお、Windows Azure AD でアカウントの追加や削除をおこなうこともできますが、これはローカルの Active Directory には反映されません。

ディレクトリ同期プロセスの詳細については、Windows Intune アカウントポータルの「[Active Directory 同期のセットアップと管理](#)」を参照してください。

ユーザーアカウントをセットアップしてアクティブ化したら、Windows Intune 管理コンソールに戻り、ユーザーグループとデバイスグループの整理を計画する必要があります。

## 6.2 ユーザーグループとデバイスグループの管理

サービスに追加したユーザーとデバイスを整理するために役立つグループを構成するプロセスを確認します。次の手順は、最初のコンピューターグループのセットアップの進め方の一例です。組織のニーズに合わせてこの手順をカスタマイズできます。

以下の例では、デバイスグループの作成を扱います。ユーザーグループの作成も手順は同じです。

### ▼デバイスグループを作成するには

- (1) Windows Intune 管理コンソールで [グループ] タブをクリックします。
- (2) [すべてのデバイス] グループには、常にシステムによって管理されるすべてのデバイスが含まれ

ます。[グループに属していないデバイス] グループには、システム管理者によってまだグループに割り当てられていないデバイスが含まれます。

(3) 右側の [タスク] パネルで [グループの作成] リンクをクリックします。

(4) [グループ名] ボックスに、「東京」と入力します。

(5) 説明に「東京拠点の PC」と入力します。

(6) デバイスグループを作る場合は、[親グループ] という見出しの下で、今回作成するグループの親グループを選択し、[次へ] をクリックします。

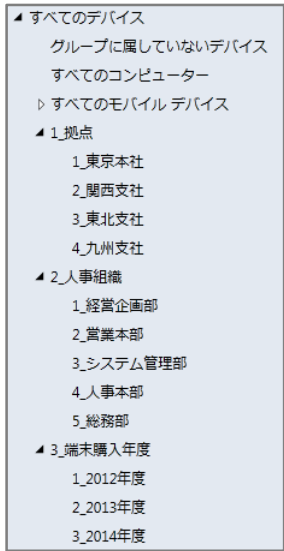
(7) [メンバーシップの基準の定義] ページにおいて、グループに含めるデバイスの種類、親グループを継承するか、どの組織単位 (OU) をグループに含めるかといった設定を行い、[次へ] をクリックします。

(8) [ダイレクトメンバーシップの定義] ページにおいて、前ページで定義した基準の例外として直接デバイスを追加したり、外したりすることができます。

(9) [次へ] をクリックし、概要を確認します。

(10) [完了] をクリックすると新たに [東京] のデバイスグループが [すべてのデバイス] 配下に作成されていることが確認できます。

作成するすべてのグループに対して、この手順を繰り返し実行することで、組織の運用に適したグループを作成します。次の図は、コンピューターを整理するために 3 つのグループに分けた場合の例を示しています。管理対象のユーザーおよびデバイスはどちらも、複数のグループのメンバーにすることができます。このように整理することで、グループを非常に柔軟に利用することができます。



● 図 11 ● グループ化の例

## ■ 注意 ■

図の部門別の例のグループ名に振られている数字は、単にリスト内でグループの順番を整理するために使用されています。グループは既定で、英数字順に表示されます。

これらのグループは、ドメインで使用する Active Directory ドメインサービス (ADDS) のグループに基づくことができますが、Windows Intune のグループが ADDS に再度レプリケートされることはありません。これらのグループは Windows Intune エージェントにのみ適用されるため、ADDS グループとの競合を気にすることなく、組織のニーズに合わせて自由に変更できます。

## 6.3 コンピューターの登録

Windows Intune にコンピューターを登録するには、次の 3 つの方法があります。

|              |   |
|--------------|---|
| 管理者による登録     | Windows Intune 管理者がコンピューターを使用するユーザーに代わってコンピューターの登録とユーザーとデバイスの関連付けをおこないます。                     |
| ユーザーによる登録    | コンピューターを使用するユーザーが Windows Intune ポータルサイトを使用して自分自身でコンピューターを登録します (ユーザーとデバイスの関連付けは自動的におこなわれます)。 |
| 展開イメージへの組み込み | Windows Intune 管理者がオペレーティングシステム展開イメージに Windows Intune サービスを組み込みます。管理者がコンピューター                 |



|  |                                      |
|--|--------------------------------------|
|  | を使用するユーザーに代わってユーザーとデバイスの関連付けをおこないます。 |
|--|--------------------------------------|

### 6.3.1 管理者による登録

Windows Intune を使用してコンピューターを管理する前に、コンピューターに Windows 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。このコンピューターは、物理コンピューターでも仮想マシンでもかまいません。

#### ■ 注意 ■

Windows Intune クライアントソフトウェアには、一意のアカウント識別子が含まれています。未承認または悪意のあるユーザーがクライアントソフトウェアにアクセスした場合、それらのユーザーが、埋め込みの証明書によって表されるアカウントにコンピューターを追加することが可能です。未承認のアクセスを防ぐために、次のベストプラクティスを採用することをお勧めします。

- ・ パッケージをダウンロードした後、それをセキュリティで保護された場所に保管します。
- ・ クライアントソフトウェアを展開するときに、必要なユーザーにのみ読み取り専用のアクセス権を提供する、セキュリティで保護された共有の場所にパッケージを配置します。Everyone グループのあらゆるアクセス許可を削除します。
- ・ IPsec または同様のセキュリティテクノロジーを使用して、共有の場所とターゲットとなるクライアントの両方を含むネットワークを保護します。

### ▼ クライアントソフトウェアをダウンロードするには

- (1) Windows Intune 管理コンソールを開きます。
- (2) ワークスペースのショートカットウィンドウの [管理] アイコンをクリックします。
- (3) ナビゲーションウィンドウで、[クライアントソフトウェアのダウンロード] をクリックします。
- (4) 画面中央の [クライアントソフトウェアのダウンロード] をクリックします。クライアントソフトウェアは、zip 形式の圧縮フォルダー (Windows\_Intune\_Setup.zip) に収められています。圧縮フォ

ルダの操作の選択を要求するメッセージが表示されたら、[保存] をクリックして、そのフォルダーをセキュリティで保護された場所に保存します。

## ■注意■

ダウンロードした圧縮フォルダーに含まれる Windows Intune.accountcert (ACCOUNTCERT) ファイルの名前を変更したり、移動したりしないでください。これらの操作を実行すると、クライアントソフトウェアのインストールが失敗します。

(6) ダウンロードが完了したら [フォルダーを開く] をクリックして、次の手順に従います。

Windows Intune サービスに追加するコンピューターごとに、次の手順を繰り返します。

## ■注意■

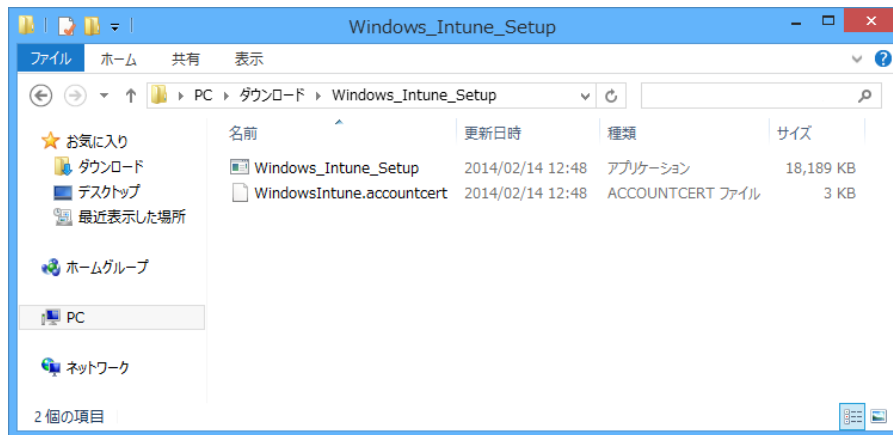
Windows Intune クライアントソフトウェアは、1、2 カ月ほどの間隔でバージョンアップがおこなわれます。そのため、クライアントソフトウェアをインストールする際は、インストールパッケージのファイルのバージョンが最新であることを確認した上で、各デバイスへ展開してください。

## ▼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には

(1) インストールパッケージを保存したフォルダーを開きます。

(2) Windows\_Intune\_Setup.zip 圧縮フォルダーを右クリックし、[すべて展開] をクリックします。

(3) [展開先の選択とファイルの展開] ダイアログボックスで、Windows Intune セットアップファイルの展開先となるセキュリティで保護された場所を選択し、[展開] をクリックします。展開が完了すると、次の図に示すように、指定した展開先のフォルダー内のファイルを表示する新しいウィンドウが開きます。



●図 12●Windows Intune セットアップファイル

## ■注意■

クライアントソフトウェアの EXE ファイルをネットワーク共有やリムーバブルディスクにコピーしたり、電子ソフトウェア展開（ESD）システムを使用して展開したりすることもできます。ただし、EXE ファイルの実行時に ACCOUNTCERT ファイルも要求されるため、これらのファイルを同じ場所に保存することが重要です。

(4) 標準的なインストールを行う場合は、ローカルの Administrators グループのメンバーアカウントを使用してインストール先のコンピューターにログオンし、Windows\_Intune\_Setup.exe ファイルをダブルクリックして、セットアップウィザードの手順に従ってインストールを完了します。

(5) インストールが完了したら、コンピューターを再起動します。EndpointProtection エージェントと更新エージェントのインストールを完了し、必要な EndpointProtection の定義や他のエージェントの更新プログラムをダウンロードするには、コンピューターを再起動する必要があります。

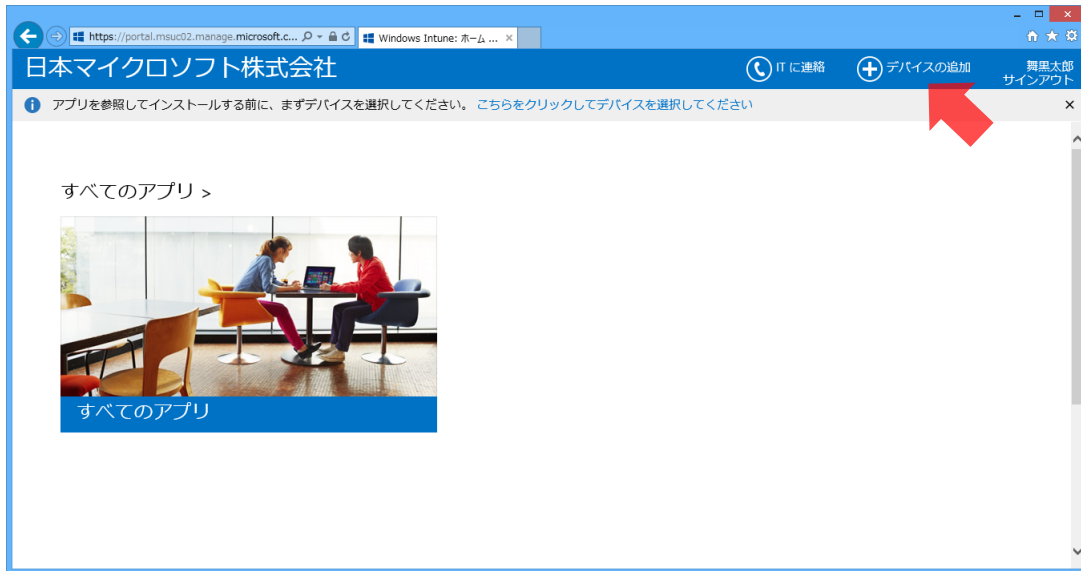
数分後、管理対象のコンピューターが Windows Intune 管理コンソールに表示されますが、エージェントのインストールが完了し、すべてのインベントリおよび状態の更新が報告されるまでに、最大で 30 分程度かかる場合もあります。

### 6.3.2 ユーザーによる登録

ユーザーがコンピューターを自分自身で登録するには、まず次のアドレスから Windows Intune 会社のポータルへアクセスして、各自の Windows Intune ユーザーID でサインインする必要があります。

<https://portal.manage.microsoft.com>

ユーザーは、Windows Intune 会社のポータル画面の画面上の「デバイスの追加」ボタンをクリックして、クライアントソフトウェアをダウンロードし、実行します。



●図 13●デバイスの追加

## ■注意■

Windows Intune（2013 年 10 月機能更新）では、会社のポータルサイトに、[デバイスの追加] が表示されない場合があります。その場合は、6.3.1「管理者による登録」に従い、クライアントソフトウェアをダウンロードし、ユーザーからアクセス可能な場所にクライアントソフトウェアを配置してください。

### 6.3.3 展開イメージへの組み込み

標準のエージェントのインストールプロセスを完了すると、インターネット接続を使用して、Windows Intune にコンピューターが登録されます。そのため、展開イメージにエージェントをインストールすると、複数のコンピューターを展開した際、Windows Intune でコンピューターアカウントの重複が生じてしまいます。この問題を解決するには Windows\_Intune\_Setup.exe の Prepare Enroll コマンドライン引数を使用して、後でコンピューターの登録するタスクをスケジュールする必要があります。このようなインストールを完了する方法については、Windows Intune オンラインヘルプの「[システム イメージを使用した Windows Intune クライアント ソフトウェアのインストール](#)」を参照してく

ださい。

## 6.4 モバイルデバイスの登録

Windows Intune では、Windows RT、Windows Phone 8、iOS、Android のデバイスをモバイルデバイスとして登録し、管理します。なお、モバイルデバイスを登録する前に、モバイルデバイス管理機能の有効化と管理対象のモバイルデバイスを準備する必要があります。

### 6.4.1 モバイルデバイス管理機能の有効化

Windows Intune を使用し、Windows Intune 単体での管理、Exchange ActiveSync 経由での管理、または、SCCM と連携した管理ができます。Windows Intune でモバイル デバイスを管理を開始するにはモバイル デバイス管理機能（Mobile Device Management 以下より MDM）を有効にする必要があります。

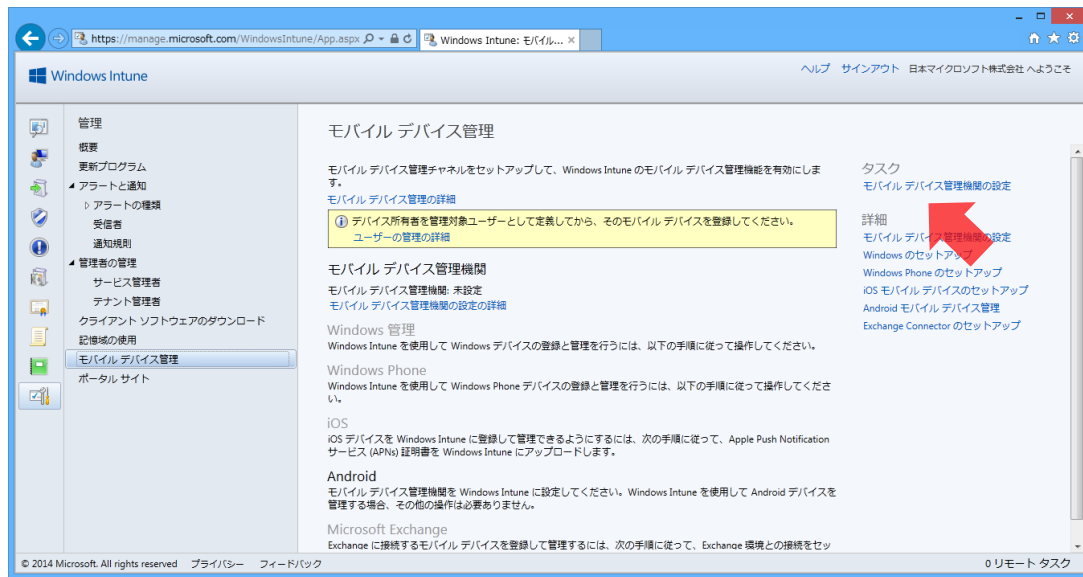
#### ■重要■

System Center 2012 Configuration Manager を使用してモバイルデバイスを管理する場合は、この手順を中断し、代わりに Configuration Manager 管理コンソールから MDM の準備を完了する必要があります。このプロセスの詳細については、「[System Center 2012 Configuration Manager の概要](#)」を参照してください。

Windows Intune のモバイルデバイス管理機能を有効にするには、次の手順を実行します。

#### ▼MDM を有効化するには

- (1) Windows Intune 管理コンソールにフルアクセスを持つサービス管理者としてサインインします。
- (2) [管理] ワークスペースをクリックします。
- (3) [モバイルデバイス管理] メニューオプションをクリックし、[モバイルデバイス管理機能の設定] を選択します。



●図 14●モバイルデバイス管理機能の設定

(4) [MDM 機能の設定] ウィンドウで、[はい] を選択します。

## ■ 注意 ■

モバイル デバイスの管理に Windows Intune のみを使用するか、System Center 2012 Configuration Manager と Windows Intune の統合を使用するかについて、慎重に検討します。モバイル デバイス管理機能をこれらのいずれかのオプションに設定した後は、弊社にお問い合わせいただいても変更はできません。変更においては Windows Intune テナントの再契約が必要になります。

Windows Intune 管理コンソールでモバイルデバイス管理機能を有効化したら、管理対象の Windows RT および Windows Phone 8 デバイス、iOS デバイス、Android デバイスの登録を開始できます。

## 6.4.2 Windows RT デバイスの登録

Windows RT デバイスはコンピューターではなく、モバイルデバイスとして登録します。なお、使用するアカウントがマイクロソフトアカウントか独自のドメインアカウントによって、登録の手順が異なります。

### ●マイクロソフトアカウントの場合

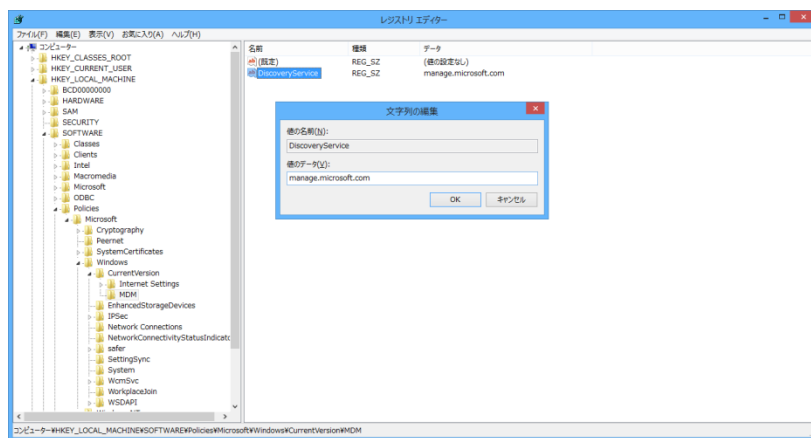
「XXX@XXX.onmicrosoft.com」などのマイクロソフトアカウントを使用して、Windows RT デバイスを Windows Intune へ登録する場合、ユーザーが各自のデバイスで次の手順を実行する必要があります。

## ▼マイクロソフトアカウントで Windows RT デバイスを登録するには

- (1) スタート画面で「regedit」と入力し、[レジストリエディター] を起動します。
- (2) [レジストリエディター] を展開し、次のパスまで移動します。なお、[MDM] キーが存在しない場合、キーを新規に作成します。

HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\MDM

- (3) [MDM] キー配下に、値として [文字列値 (REG\_SZ)] の「DiscoveryService」を新規作成し、値のデータとして「manage.microsoft.com」を設定します。



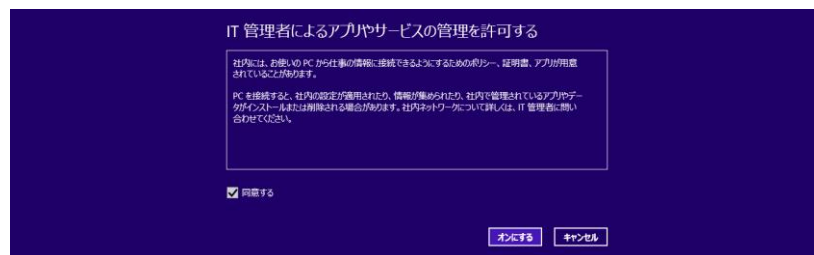
●図 15●DiscoveryService の追加

- (4) 設定チャームを表示して、[PC 設定の変更] をクリックし、[ネットワーク] の [社内ネットワーク] を選択します。[ユーザーID を入力して社内ネットワークのアクセスを取得するか、デバイス管理を有効にしてください] に<Windows Intune のユーザー名>を入力したら、[デバイスの管理をオンにすると、IT 管理者がアプリやサービスをセットアップできるようになります] の [オン] をクリックします。



●図 16●デバイス管理の有効化

(5) [IT 管理者によるアプリやサービスの管理を許可する] で [同意する] にチェックし、[オンにする] ボタンをクリックします。



●図 17●IT 管理者によるアプリやサービスの管理の許可の同意

## ●独自のドメインアカウントの場合

「XXX@contoso.com」などの独自のドメインアカウントを使用して、Windows RT デバイスを Windows Intune へ登録する場合、管理者が登録サーバーのアドレスのセットアップと Windows Intune 管理コンソールでの手順の実行が必要です。

## ▼登録サーバーのアドレスのセットアップするには

独自のドメインアカウントでデバイスを登録する際、Windows RT と Windows Phone 8 の各デバイスは、ドメインネームサービス (DNS) サーバーにより自動検出された登録サーバーへアクセスします。そのため、「contoso.com」などの独自のドメイン名アカウントを Windows Intune で使用している場合、DNS サーバーに次の登録サーバーの CNAME レコードを作成しておく必要があります (「xxxx.onmicrosoft.com」などのマイクロソフトアカウントを使用している場合は不要です)。



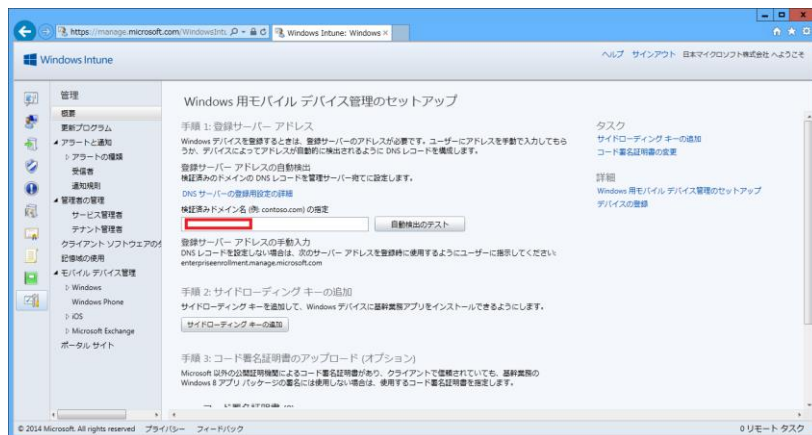
- ・エイリアス名: enterpriseenrollment.<独自のドメイン名>
- ・FQDN: enterpriseenrollment.manage.microsoft.com

## ■重要■

CNAME レコードの登録方法は、パブリック DNS サービスにより異なるため、サービス提供者へお問い合わせください。

## ▼独自のドメインアカウントで Windows RT デバイスを登録するには

- (1) Windows Intune 管理コンソールで [管理]、[モバイルデバイスの管理] の [Windows] の順にクリックします。
- (2) [検証済みドメイン名 (例: contoso.com) の設定] に<独自のドメイン名>を入力して、[自動検出のテスト] ボタンをクリックします。



●図 18● 検証済みドメイン名の設定

- (3) [テスト成功] のメッセージが表示されることを確認します。



●図 19●テスト成功

## ■重要■

DNS の設定変更が反映されるまで、最大 72 時間が掛かることがあります。

〔検証済みドメインの設定〕のテストの完了後、ユーザーは自身のデバイスで〔マイクロソフトアカウントで Windows RT デバイスを登録するには〕の手順(4)以降と同じ操作をおこない、Windows RT デバイスを登録します。

これで、Windows Intune で Windows RT デバイスが管理されます。認証されたユーザーは、Windows ストア版の会社のポータルを使用し、会社のアプリケーションにアクセスしたり、各自のデバイスを管理したりできるようになります。

### 6.4.3 Windows Phone 8 デバイスの登録の準備

Windows Phone 8 デバイスを管理するには、まず組織のアプリケーションに必要な「コード署名証明書」を用意する必要があります。次に、その証明書を使用して、Windows Phone 8 ポータルサイトアプリケーションに署名し、それを Windows Intune サービスにアップロードして、デバイスの登録時に展開できるようにします。次の表は、このプロセスを完了するために必要な手順を示しています。

|   |  |
|---|--|
| 手順 1 :<br>Windows Phone デベロッパーセンターアカウントとエンタープライズモバイルコード署名証明書の取得 | Windows Phone Dev Center に移動し、会社の「発行者 ID」を取得します。発行者 ID を使用して、エンタープライズモバイル用コード署名証明書を購入します。通常、これらの手順は、組織に対して一度だけ実行する必要があり、組織が開発しているアプリケーションの開発者が使用します。   |
| 手順 2 :<br>LOB アプリケーションの署名                                       | Windows Phone 8 SDK ( <a href="https://dev.windowsphone.com/ja-JP">https://dev.windowsphone.com/ja-JP</a> ) から署名ツールをダウンロードします。アプリケーションをエンドユーザーに展開するには、ターゲットの Windows Phone 8 デバイスが信頼している証明機関によって署名される必要があります。署名ツールアプリケーションを使用して、組織のエンタープライズモバイル用コード署名証明書でアプリケーションに署名します。 |
| 手順 3 :<br>Windows Phone 8 ポータルサイトアプリケーションの署名                    | Windows Phone 8 ポータルサイトアプリケーションをダウンロードし、署名ツールを使用して、エンタープライズモバイル用コード署名証明書でポータルサイトアプリケーションに署名します。  |

|   |   |
|---|---|
| <p>手順 4 :</p> <p>署名済みの Windows Phone 8 ポータルサイトアプリケーションをアップロードして展開</p> | <p>Windows Intune 管理コンソールから、署名済みのポータルサイトアプリケーションのファイルをアップロードし、すべてのユーザーに展開します。</p> |
|---|---|

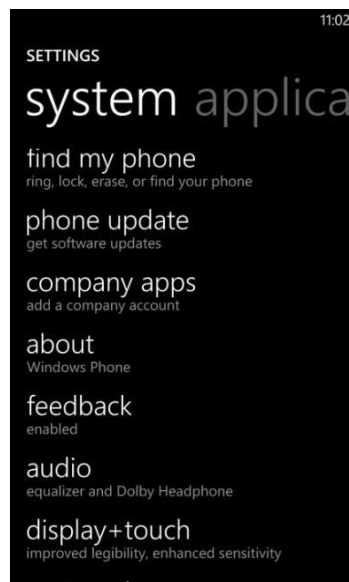
署名済みのポータルサイトアプリケーションをアップロードすると、ユーザーがデバイスを登録する際に、ポータルサイトアプリケーションが自動的にデバイスにダウンロードされるようになります。

#### 6.4.4 Windows Phone 8 デバイスの登録

Windows Phone 8 デバイスを登録するには、ユーザーが次の手順を実行する必要があります。

##### ▼Windows Phone 8 デバイスを登録するには

(1) Windows Phone 8 デバイスから登録を開始するには、次の図に示すように、システム設定に移動して、[業務用アプリ (company apps)] を選択します。

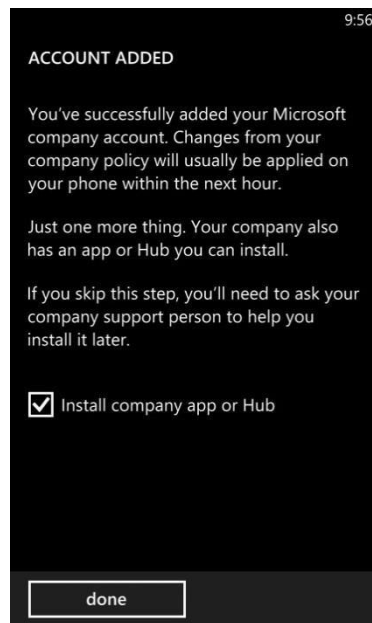


●図 20● [業務用アプリ] の設定

(2) ユーザーは、登録プロセスで会社の資格情報の入力を求められます。管理コンソールで自動登録 DNS エントリが指定されていなかった場合、ユーザーは登録を完了するために登録サーバーのアドレス

を入力する必要があります。認証に成功すると、ユーザー、Windows Phone 8 デバイス、および Windows Intune サービス間の関係が確立されます。次に、Windows Intune サービスによる認証用に証明書がデバイスにインストールされます。

(3) ユーザーは、[業務用アプリまたはハブをインストールする (Install company app or Hub)] チェックボックスをオンにして、各自のデバイスの管理を有効にする必要があります。このチェックボックスをオンにしないと、ユーザーはポータルサイトアプリケーションをダウンロードできません。



●図 21●ポータルサイトのインストールの有効化

(4) ポータルサイトアプリケーションがデバイスにインストールされ、Windows Intune でインベントリを収集し、管理設定を適用することが可能になります。これで、ユーザーは、Windows Phone 8 ポータルサイトアプリケーションを使用して、LOB アプリケーションにアクセスできるようになりました。

### 6.4.5 iOS デバイスの登録の準備

iOS デバイスのモバイルデバイス管理機能を有効にするには、「Apple Push Notification Service (APNs) 証明書」を取得して、その証明書を Windows Intune で使用可能にする必要があります。次の表は、このセットアッププロセスを完了するために必要な手順の詳細を示しています。

|        |   |
|--------|---|
| 手順 1 : | Windows Intune 管理コンソールから、APNs 証明書要求ファイル |
|--------|---|

|                           |  |
|---------------------------|--|
| APNs 証明書の要求のダウンロード        | (CSR ファイル) をダウンロードし、ローカルコンピュータに保存します。  |
| 手順 2 :<br>APNs 証明書の取得     | Windows Intune 管理コンソールから [Apple Push Certificates Portal] へアクセスし、APNs 証明書要求ファイルを使用して APNs 証明書ファイル (MDM_Microsoft Corporation_Certificate.pem ファイル) を作成します。引き続き、個人ではなく会社の電子メールアカウントに関連付けられた会社の AppleID を使用します。APNs 証明書ファイルをローカルに保存します |
| 手順 3 :<br>APNs 証明書のアップロード | Windows Intune 管理コンソールから、Windows Intune アカウントに APNs 証明書ファイルをアップロードします。   |

## ■重要■

会社の AppleID は、outlook.jp など自由なメールアドレスで作成することができます。また、AppleID は APNs 証明書の取得のために、管理者が使用します。そのため、ユーザーやデバイスの AppleID とは関係はありません。

## 6.4.6 iOS デバイスの登録

iOS デバイスを登録するには、ユーザーが次の手順を実行する必要があります。

### ▼iOS デバイスを登録するには

- (1) iOS デバイスの Web ブラウザーから Windows Intune ポータルサイトの Web サイト (<https://m.manage.microsoft.com>) を直接参照することも、ユーザーにポータルサイトへのリンクと各自のユーザーID の詳細を含む招待状を電子メールで送信することもできます。
- (2) Windows Intune ユーザー資格情報を入力すると、登録プロセスが開始されます。
- (3) 会社の管理プロファイルのインストールを求めるプロンプトに同意します。
- (4) 認証に成功すると、ユーザー、iOS デバイス、および Windows Intune サービス間の関係が確立されます。

(5) Windows Intune でインベントリが収集され、管理設定が適用されます。

(6) App Store より、[Windows Intune ポータルサイト] をインストールします。インストールが成功すると、ホーム画面に [ポータル] が追加されます。これでユーザーは [ポータル] から LOB アプリケーションにアクセスできるようになりました。

## 6.4.7 Android デバイスの登録

Android デバイスには事前の準備は必要ありません。すぐに Android デバイスを登録することができます。Android デバイスを登録するには、ユーザーが次の手順を実行する必要があります。

### ▼Android デバイスを登録するには

(1) Android デバイスにて、[Google Play Store] を開き、「Windws Intune ポータルサイト」を検索します。

(2) [Windws Intune ポータルサイト] アプリケーションをダウンロード、インストールします。

(3) [Windws Intune ポータルサイト] アプリケーションを開き、[このデバイスの追加] ボタンをクリックし、Microsoft Online Services ID を入力します。その後、デバイスが追加されます。

(4) デバイスの追加が完了すると、ユーザーは [Windws Intune ポータルサイト] アプリケーション上にて、使用可能なアプリケーションを参照することができます。また、管理者は、登録されたデバイスを Windows Intune 管理コンソールの [すべてのデバイス]、[すべてのモバイル デバイス] にて確認することができます。

## 7. アプリケーションの展開

Windows Intune では、.exe および.msi アプリケーションを、Windows Intune で管理している Windows PC に直接展開できます。具体的には管理コンソールを使用して、これらのアプリケーションをデバイスグループに展開します。

さらに、Windows (.appx)、Windows Phone (.xap)、Android (.apk)、iOS (.ipa) の各アプリケーションパッケージ、Web アプリケーション、およびパブリックストアアプリケーションを（ディープリンクを通じて）ユーザーに提供し、ユーザーが Windows Intune ポータルサイトからインストールできるようにすることが可能です。これらのアプリケーションは、ユーザーグループに展開されるため、ユーザーはポータルサイトアプリケーション（Company portal アプリケーション）または Web サイトから必要なアプリケーションを選択できます。次の表は、各プラットフォームがポータルサイトにアクセスする方法を示しています。

|                 | Windows 8 | Windows RT | Windows 7,Vista,XP | Windows Phone 8 | iOS | Android |
|-----------------|-----------|------------|--------------------|-----------------|-----|---------|
| ポータルサイトアプリケーション | ○         | ○          | ×                  | ○               | ×   | ×       |
| Web ページ         | ○ ※       | ○ ※        | ○                  | ○               | ○   | ○       |

※ ポータルサイトアプリケーションを通じてアプリケーションインストールが提供されています。

### 7.1 モバイルデバイス用アプリケーションの展開

Windows Intune を使用してモバイルデバイスにアプリケーションを展開するには、次の 2 つの方法があります。

|       |  |
|-------|--|
| 外部リンク | いずれかのストアにあるアプリケーションへのリンクアドレスをすべてのデバイスに提供できます。Windows Store、Windows Phone Store、アプリケーションストア、および Google Play へのリンクをセットアップするには、管理コンソールを使用します。また、このリ |
|-------|--|

|               |  |
|---------------|--|
|               | リンクは、デバイス自体の Web ブラウザーを通じてデバイス上で実行される Web ベースのアプリケーションへのリンクとすることも可能です。   |
| ソフトウェアインストーラー | 署名済みのアプリケーションパッケージを提供することができます。管理者は、そのパッケージを Windows Intune サービスに直接アップロードしてから、管理対象デバイスに「サイドローディング」します。アプリケーションのサイドローディングを行うことで、パブリックアプリケーションストアを通さずに、アプリケーションをデバイスに直接配布できます。 |

次の表は、Windows Intune のサイドローディング先とすることが可能なモバイルデバイスのプラットフォームと、そのプラットフォームに必要なソフトウェアファイルの種類を示しています

|                 |                            |
|-----------------|----------------------------|
| Windows RT      | .appx および .appxbundle ファイル |
| Windows Phone 8 | .xap ファイル                  |
| iOS             | .ipa および .plist マニフェストファイル |
| Android         | .apk ファイル                  |

これらのデバイスにアプリケーションを公開するには、署名済みアプリケーションをインストールするために必要な証明書とキーが用意できていることを確認する必要があります。次のセクションでは、サポート対象のデバイスプラットフォームごとにアプリケーションの公開機能を有効化するための手順について説明します。

## 7.2 Windows RT (Windows 8) アプリケーションのセットアップ

Windows ストアアプリは、Windows ストアからのみ入手ができます。ただし、社内専用の Windows ストアアプリを開発し、「サイドローディング」と呼ばれる方法で、コンピューターへ追加することもできます。

ドメインに参加しているコンピューターでは、グループポリシーを構成して、サイドローディングを有効化することができます。ドメインに参加していない PC では、サイドローディングキーが必要となります。Windows RT デバイスもサイドローディングキーが必要です。



マイクロソフトからこのサイドローディングキーを取得するには、ボリュームライセンスサービスセンター（VLSC）にサインインする必要があります。次の表は、その手順の概要とそれぞれの手順の詳細を示しています。

|                                  |   |
|----------------------------------|---|
| 手順 1 :<br>サイドローディングキーの取得とアップロード  | サイドローディングを行う LOB アプリケーションを Windows 8 デバイスにインストールする前に、ライセンスを購入し、 <a href="#">VLSC</a> からサイドローディングキーを取得してアクティブ化する必要があります。サイドローディング製品アクティベーションキーの詳細については、「 <a href="#">マイクロソフトボリュームライセンス</a> 」を参照してください。次に、Windows Intune 管理コンソールからサイドローディングキーをアップロードします。              |
| 手順 2 :<br>コード署名証明書のアップロード        | 会社の証明機関からの証明書がある場合、Windows Intune 管理コンソールで「コード署名証明書の変更」オプションを使用して、対象の LOB アプリケーションに使用する「コード署名証明書」を指定できます。すべての LOB アプリケーションがコード署名されている必要がありますが、信頼された証明書チェーンの一部である公開キーがある場合は、ここでさらにコード署名証明書を追加する必要はありません。この構成変更が必要になるのは、公共の証明機関ではない、検証できない証明書によってアプリケーションに署名する場合のみです。 |
| 手順 3 :<br>LOB アプリケーションのアップロードと公開 | Windows Intune 管理コンソールから署名済みの LOB アプリケーションをアップロードして、ターゲットユーザーに展開します。  |

## ■重要■

マイクロソフト ボリューム ライセンス（サイドローディングキー）に関しては、マイクロソフト ボリューム ライセンス コールセンターまでお問い合わせください。

マイクロソフト ボリューム ライセンス コールセンター(VLCC)

<https://www.microsoft.com/ja-jp/licensing/contact-us.aspx>

電話番号：0120-737-565（選択番号 1）

営業時間：9:00 - 17:30（土日祝日、弊社指定休業日を除く）

これで、管理対象の Windows RT デバイスのユーザーは、公開された LOB アプリケーションを各自

のデバイスにインストールすることができます。Windows 8 PC でこれらの LOB アプリケーションのサイドローディングを行えるようにするには、TechNet ページの「[Windows 8 のサイドローディングの要件](#)」を参照してください。

## 7.3 Windows Phone 8 アプリケーションのセットアップ

モバイルデバイスへの Windows Phone 8 アプリケーションのサイドローディングを有効にするには、前述の Windows Phone 8 デバイスの登録の準備で取得したエンタープライズモバイル用コード署名証明書を使用して開発者がアプリケーションに署名することを確認するだけで済みます。次の表は、このプロセスを完了するために必要な手順を示しています。

|                                  |  |
|----------------------------------|--|
| 手順 1 :<br>LOB アプリケーションの署名        | Windows Phone 8 SDK の署名ツールアプリケーションを使用して、組織のエンタープライズモバイル用コード署名証明書でアプリケーションに署名します。 |
| 手順 2 :<br>LOB アプリケーションのアップロードと公開 | Windows Intune 管理コンソールから署名済みの LOB アプリケーションをアップロードして、ターゲットユーザーに展開します。             |

## 7.4 iOS アプリケーションのセットアップ

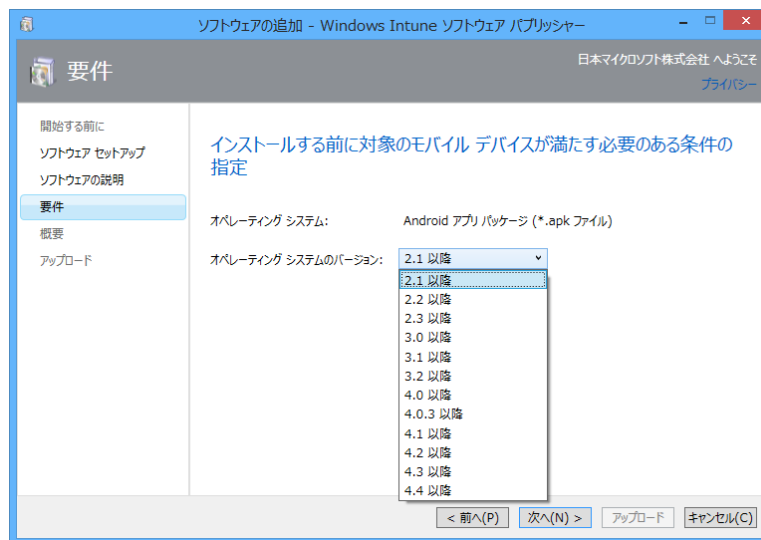
iOS デバイスのモバイルデバイス管理機能を有効にするには、Apple Push Notification Service (APNs) 証明書を取得して、その証明書を Windows Intune で使用可能にする必要があります。加えて、すべての LOB アプリケーションが、有効な iOS Developer Enterprise Program の証明書によって署名されることによって、iOS デバイスでそのアプリケーションが受け入れられるようにする必要があります。次の表は、このセットアッププロセスを完了するために必要な手順の詳細を示しています。

|   |  |
|---|--|
| 手順 1 :<br>iOS Developer Enterprise Program への参加 | Windows Intune を使用してインストールする独自の社内 iOS アプリケーションを開発する場合、iOS Developer Enterprise Program のメンバーシップを購入する必要があります。なお、登録には Dun&Bradstreet (D-U-N-S) 番号が必要です。LOB アプリケーションの作成を外部開発者に委託している場合は、外部開発者が有効な iOS Developer Enterprise Program の証明書を使用してアプリケーションに署名できることを確認する必要があります。 |
|---|--|

|  |  |
|--|--|
| 手順 2 :<br>iOS デバイスに展開するすべてのアプリケーションの署名 | 管理者または iOS 開発者は、同じ証明書を使用して iOS デバイスに展開するすべてのアプリケーションに署名する必要があります。  |
| 手順 3 :<br>LOB アプリケーションのアップロードと公開       | これで、Windows Intune 管理コンソールを使用してアプリケーションをアップロードできます。次に、ManageDeployment ウィザードを使用して、アプリケーションを必要なユーザーに展開できます。 |

## 7.5 Android アプリケーションのセットアップ

Android アプリケーションのセットアップには証明書などの特別な準備はありません。Android アプリケーション（.apk）ファイルを用意した上で、[ソフトウェア] ワークスペースから [ソフトウェアの追加] をクリックして、Android アプリケーションファイルをアップロードします。なお、要件として Android のバージョンを指定することも可能です。



●図 22● Android ソフトウェアの追加

Android アプリケーションファイルをアップロードした後、[ソフトウェア] ワークスペースの [展開の管理] より任意のデバイスに Android ソフトウェアを展開することができます。

## 8. Windows Intune の環境の最適化

---

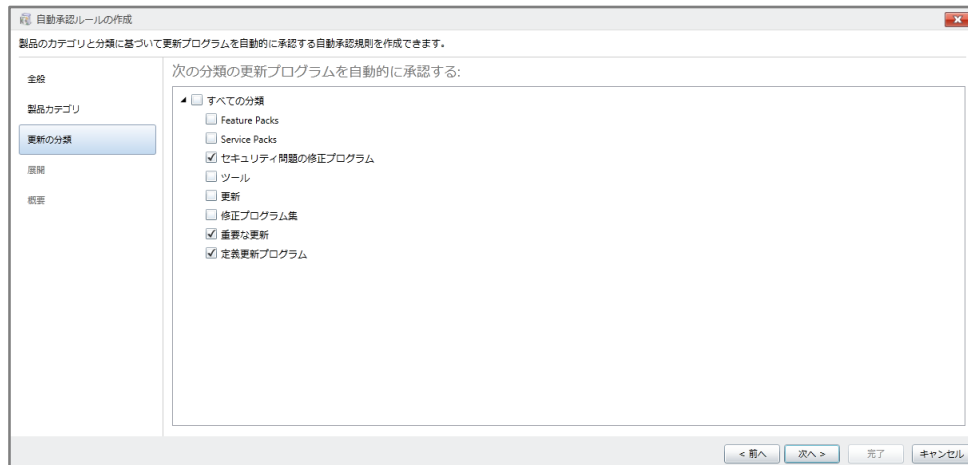
次のトピックでは、ユーザーおよび管理者双方のサービスエクスペリエンスを最適化するために、Windows Intune 環境を構成する方法について確認します。

### 8.1 更新プログラムと自動承認の管理

前述の手順で作成したグループを使用して、Windows Intune ポリシーとマイクロソフトの更新プログラムの両方を展開することができます。Windows Intune で管理されるすべての更新プログラムを自分で詳細に管理したい場合には、[更新プログラム] ワークスペースの [承諾] または [拒否] オプションを使用することができます。ただし、重要な更新プログラムやセキュリティ更新プログラムをできるだけ迅速に管理対象のコンピューターにインストールしたい場合には、Windows Intune の自動承認規則を使用することができます。自動承認規則を設定し、選択した分類に従って更新プログラムの承認プロセスを自動化するには、次の手順を実行します。

#### ▼更新プログラムの承認プロセスを自動化するには

- (1) Windows Intune 管理コンソールで、[管理]、[更新プログラム] の順にクリックします。
- (2) 必要に応じてページの下部までスクロールして [自動承認規則] の [新規作成] をクリックします。
- (3) 「既定の承認規則」など、適切な規則名を入力して、[次へ] をクリックします。
- (4) [すべてのカテゴリ] など適切な適用対象のオプションをオンにして、[次へ] をクリックします。
- (5) 自動承認の対象とする更新プログラムの分類を選択します。次の図に示したカテゴリを自動承認の対象として選択することをお勧めします。これらのカテゴリを使用すると、管理対象のコンピューターが新たな脅威や脆弱性から、より強力に保護されます。



●図 23●承認規則の分類

(6) 自動化する分類をすべて選択したら、[次へ] をクリックします。

(7) この規則を展開するグループを選択します。たとえば、管理対象のコンピューターすべてにこの規則を展開する場合、[すべてのコンピューター] グループを選択します。

(8) [完了] をクリックします。

(9) [選択項目の実行] をクリックすると、この規則によって選択したカテゴリと分類の既存の更新プログラムがすべて評価され、管理対象のコンピューターが次回チェックインした際（既定では 8 時間ごと）に利用できるようになります。また、ここで [保存] をクリックすると、規則は今後リリースされる更新プログラムにのみ適用されます。

管理対象のコンピューターでサービスに再度チェックインすると、すべての重要な更新プログラムやセキュリティ更新プログラムが利用可能になった時点で、直ちに適用するよう求められます。なお、[更新プログラム] ワークスペースでは、承認済みとなった特定の更新プログラムで [拒否] オプションを使用し、そのすべての承認を削除して、更新プログラムのインストールを中止することもできます。

## ■注意■

自動承認規則を使用してもステータスが承認済みにならない更新プログラムが一部あります。これらの更新プログラムについては、管理者が手動で使用許諾書の同意をおこなう必要があります。

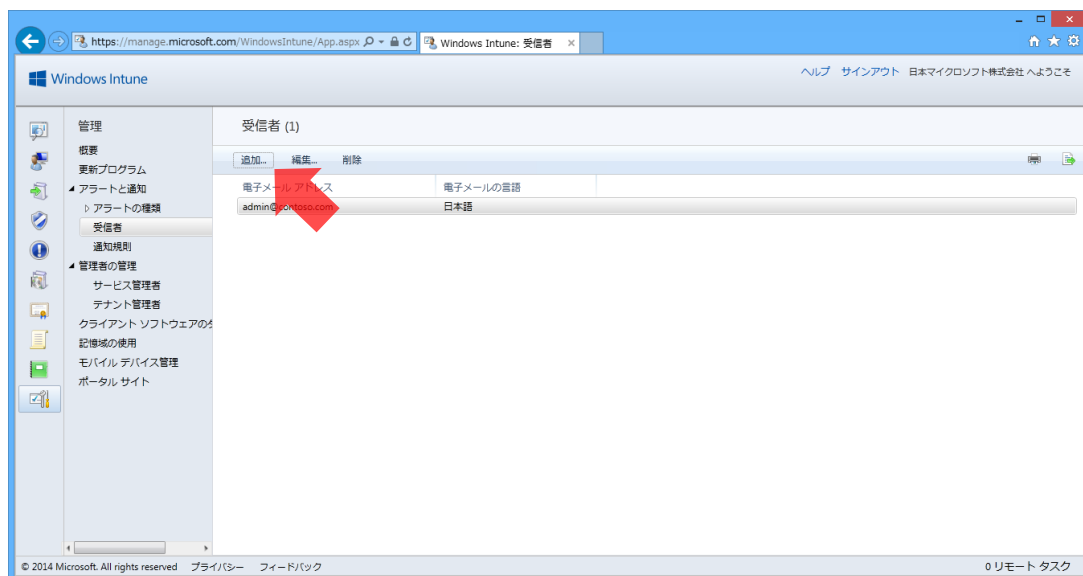
## 8.2 アラート通知のセットアップ

Windows Intune では、管理対象コンピューターに対するアラートを追跡するため、[アラート] ワークスペースのアラートを監視したり、アラートを指定した電子メールアドレスへ直接送信したりすることができます。

アラート通知を構成するには、Windows Intune 管理コンソールで [管理] ワークスペースタブをクリックします。

## ▼アラート通知を構成するには

- (1) [アラートと通知] をクリックします。
- (2) 次に [受信者] をクリックし、[追加] オプションをクリックします。



● 図 24 ● 受信者の追加

- (3) 電子メールのエイリアスを必要な数だけ追加します。

## ■ 重要 ■

アラートの受信者に設定されても、Windows Intune 管理コンソールへのアクセスが許可されるわけではありません。これらの受信者がコンソールにサインインできるようにするには、その受信者を管理者として追加する必要があります。

(4) 次に「通知規則」を選択し、電子メールを送信するアラートの規則を選択します。

## ■ 注意 ■

Windows Intune（2013 年 10 月機能更新）では、通知規則の名前が文字化けします。暫定の対処方法については、「[通知規則名の文字化けへの暫定対処策](#)」を参照してください。

(5) 「受信者」オプションをクリックします。

(6) これらのアラートを電子メールで受信する、電子メール受信者を選択します。



● 図 25 ● 通知規則の選択

「リモートアシスタンス要求」の通知をセットアップすることをお勧めします。通常、これらの要求には即座の応答が必要なためです。

## ■ 重要 ■

通知機能を使用し、Windows Intune の大きな機能変更に関するお知らせをメールで受信することができます。詳細については、「[【重要】 Windows Intune からの通知をメールで受信する方法](#)」を参照してください。

## 8.3 レポートの作成

レポートを作成すると、特定のアプリケーションや更新プログラムがインストールされたコンピューター

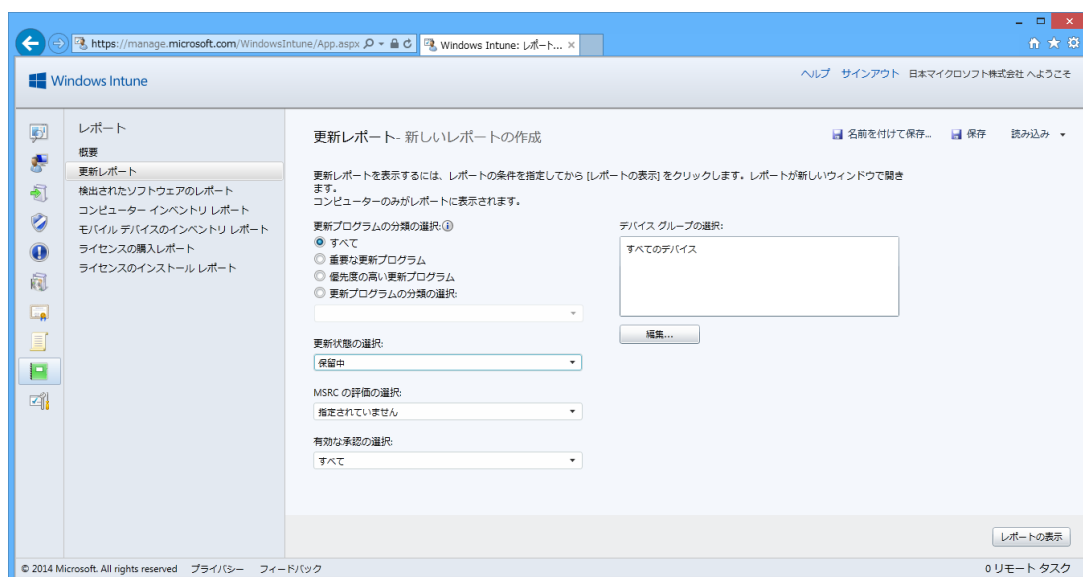
ターの数、ブロックされたマルウェアの種類、先月にリモートアシスタンスが必要だったユーザーの数など、さまざまな情報を確認することができます。Windows Intune には、すぐに使用できるレポートテンプレートのセットが用意されています。また、レポートテンプレートをカスタマイズしてレポートを作成することもできます。

これらのレポートは印刷することも、HTML 形式またはコンマ区切り値（CSV）ファイルとしてエクスポートすることもできます。エクスポート機能によって Windows Intune からデータをエクスポートし、そのデータを分析に使用するプログラムにインポートすることが可能です。たとえば、データを Microsoft Excel にインポートし、経営陣によるプレゼンテーションで使用する表やグラフを作成できます。

## ▼レポートを作成するには

ここでは、更新プログラムのインストールを保留しているすべてのコンピューターを特定するための Windows Update の更新レポートを作成する手順について説明します。

- (1) [レポート] ワークスペースタブをクリックします。
- (2) [更新レポート] をクリックします。
- (3) 次の図のようにレポートの設定をカスタマイズします。



●図 26●更新レポートの作成



(4) [レポートの表示] をクリックします。

これにより、次の図のようなレポートが生成されます。この情報を使用して、まだ更新プログラムを適用していないコンピューターを特定したり、更新プログラムのトラブルシューティングのプロセスを開始したりすることができます。

| 更新プログラムのタイトル                                      | 分類          | 承認済み | 必要 | インストール済 | 失敗 | 保留中 | 評価済み % |
|---|-------------|------|----|---------|----|-----|--------|
| Microsoft .NET Framework 4.5.1 用セキュリティ            | セキュリティ問題の修正 | はい   | 0  | 0       | 0  | 2   | 100%   |
| Microsoft .NET Framework 4.5.1 用セキュリティ            | セキュリティ問題の修正 | はい   | 0  | 0       | 0  | 2   | 100%   |
| Microsoft Online Management Policy Agent (x64)    | 重要な更新       | はい   | 0  | 1       | 0  | 1   | 100%   |
| Microsoft Online Management コンポーネント               | 重要な更新       | はい   | 0  | 1       | 0  | 1   | 100%   |
| Microsoft Online Management の更新プログラム              | 重要な更新       | はい   | 0  | 1       | 0  | 1   | 100%   |
| Windows 8 および 8.1、Windows Server 2012 および 2012 R2 | セキュリティ問題の修正 | はい   | 0  | 0       | 0  | 2   | 100%   |
| Windows 8.1 for x64-based Systems の ActiveX       | セキュリティ問題の修正 | はい   | 0  | 0       | 0  | 2   | 100%   |
| Windows 8.1 for x64-based Systems 用 Internet      | セキュリティ問題の修正 | はい   | 0  | 0       | 0  | 2   | 100%   |
| Windows 8.1 for x64-based Systems 用 Internet      | セキュリティ問題の修正 | はい   | 0  | 0       | 0  | 2   | 100%   |
| Windows 8.1 for x64-Based Systems 用セキュリ           | セキュリティ問題の修正 | はい   | 0  | 0       | 0  | 2   | 100%   |
| Windows 8.1 for x64-Based Systems 用セキュリ           | セキュリティ問題の修正 | はい   | 0  | 0       | 0  | 2   | 100%   |
| Windows 8.1 for x64-Based Systems 用セキュリ           | セキュリティ問題の修正 | はい   | 0  | 0       | 0  | 2   | 100%   |
| Windows 8.1 for x64-Based Systems 用セキュリ           | セキュリティ問題の修正 | はい   | 0  | 0       | 0  | 2   | 100%   |
| Windows 8.1 for x64-Based Systems 用セキュリ           | セキュリティ問題の修正 | はい   | 0  | 0       | 0  | 2   | 100%   |
| Windows 8.1 for x64-Based Systems 用セキュリ           | セキュリティ問題の修正 | はい   | 0  | 0       | 0  | 2   | 100%   |
| Windows 8.1 for x64-Based Systems 用セキュリ           | セキュリティ問題の修正 | はい   | 0  | 0       | 0  | 2   | 100%   |
| Windows 8.1 for x64-Based Systems 用セキュリ           | セキュリティ問題の修正 | はい   | 0  | 0       | 0  | 2   | 100%   |
| Windows 8.1 for x64-Based Systems 用セキュリ           | セキュリティ問題の修正 | はい   | 0  | 0       | 0  | 2   | 100%   |
| Windows 8.1 for x64-Based Systems 用セキュリ           | セキュリティ問題の修正 | はい   | 0  | 0       | 0  | 2   | 100%   |
| Windows 8.1 for x64-Based Systems 用セキュリ           | セキュリティ問題の修正 | はい   | 0  | 0       | 0  | 2   | 100%   |
| Windows 8.1 for x64-Based Systems 用更新プロ           | 重要な更新       | はい   | 0  | 0       | 0  | 2   | 100%   |
| Windows 8.1 for x64-Based Systems 用更新プロ           | 重要な更新       | はい   | 0  | 0       | 0  | 2   | 100%   |

●図 27●更新レポートの表示

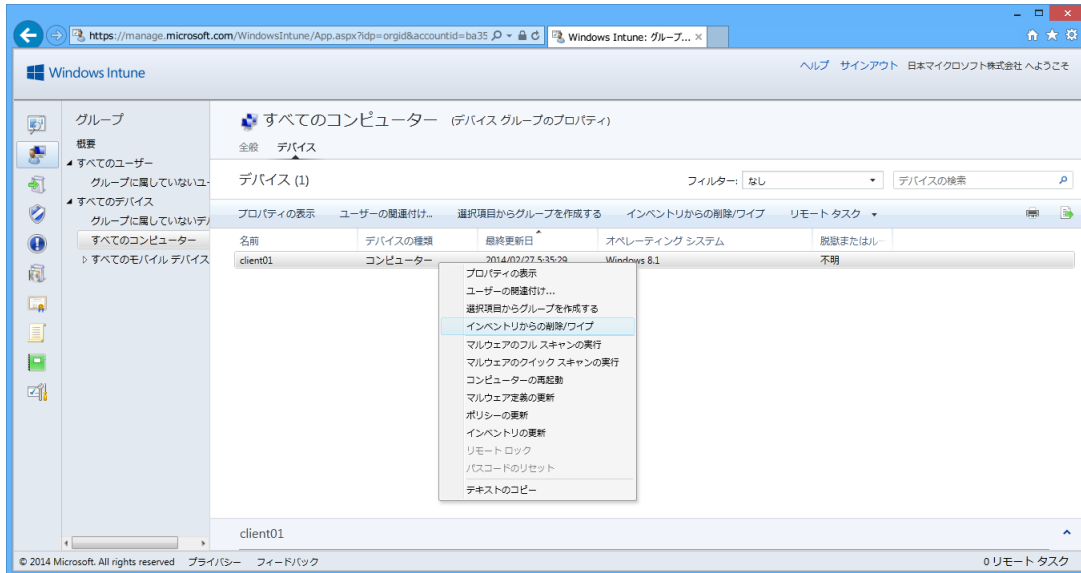
## 8.4 デバイスの削除

Windows Intune に登録したコンピューターとモバイルデバイスを管理対象から除外するには、Windows Intune 管理コンソールの [グループ] から、それらのデバイスを削除する必要があります。

### ▼デバイスを削除するには

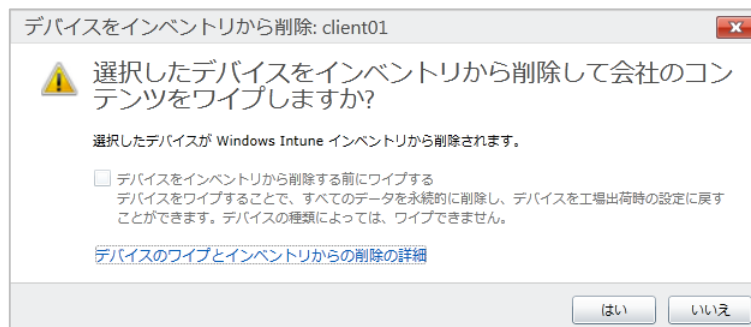
- (1) Windows Intune 管理コンソールを開きます。
- (2) ワークスペースのショートカットウィンドウの [グループ]、[すべてのデバイス] の [すべてのコンピューター] の順にクリックします。
- (3) ヘッダーで、[デバイス] をクリックします。

(4) 右側ウィンドウの削除したいデバイスで右クリックし、[インベントリからの削除/ワイプ] をクリックします。



●図 28●インベントリからの削除/ワイプ

(5) [選択したデバイスをインベントリから削除して会社のコンテンツをワイプしますか?] が表示されたら、[はい] をクリックします。



●図 29●デバイスをインベントリから削除

コンピューターを削除した場合、自動的に Windows Intune エージェントがアンインストールされます。1 時間経っても、Windows Intune エージェントがアンインストールされない場合、コマンドラインプログラムやスクリプトからアンインストールをおこないます。コマンドラインプログラムとスクリプトからアンインストールする方法については「[Windows Intune アンインストール方法について](#)」を参照してください。

## ■重要■

モバイルデバイスの場合、モバイルデバイスの会社のポータルアプリから削除をおこなうこともできます。ただし、削除登録には、最大 1 ヶ月掛かることがあります。

## 9. まとめ

---

Windows Intune は、あらゆる規模の企業が世界各地でパーソナルコンピューターやモバイルデバイスの管理およびセキュリティ保護を行うのに役立つ、クラウドベースの統合管理サービスを提供します。この最新のソリューションにより、Windows 8、Windows RT、Windows クラウドサービスを使用する Windows Phone 8、および Apple、iOS の各デバイスに、クライアントサポートが拡張されます。Windows Intune を使用すると、「個人所有デバイスの業務利用 (Bring Your Own Device)」をサポートすることができます。これにより、社員が場所に関係なく自分のコンピューターやモバイルデバイスを管理しながら、各自の業務に集中できるようになります。

このガイドでは、Windows Intune クラウドサービスのトライアル期間においてコンピューターのセットアップと管理を行うための主な作業のいくつかについて説明しました。ぜひこのトライアル版をご活用ください。

Windows Intune の 30 日間の無料トライアルを始めるには、次の URL へアクセスしてください。

Windows Intune 30 日間無料トライアルの入手

<http://www.microsoft.com/ja-jp/windows/Windowsintune/try.aspx>

また、ご契約や請求書関連手続きについては、次の Microsoft Online Service カスタマー サポート窓口へご相談ください。

Microsoft Online Service カスタマー サポート窓口

<https://support.microsoftonline.com/default.aspx?productkey=intunesupp>

営業時間 : 月 - 金 9:00 - 18:00 (Web / 電話とも)

電話番号 : 0120-996-680 (フリーダイヤル)

※ [選択なしで日本語での対応が開始されます] - [2 ご契約関連]

Windows Intune 機能に関する技術的支援をご要望の場合、次の Windows Intune クラウド サービス 窓口へご相談ください。

Windows Intune クラウド サービス

受付窓口営業時間：月 - 金 9:00 - 18:00 (Web / 電話とも)

サポート サービス営業時間：月 - 金 9:00 - 17:30 (Web / 電話とも)

(無料通話用窓口) 電話番号：0120-996-680

(有料通話用窓口) 電話番号：03-5767-9793

Web :[電子メール サポート]

<https://support.microsoftonline.com/default.aspx?productkey=intunesupp>

Windows Intune SA (Software Assurance) 権でご使用いただける製品についてご不明点がある場合には、次のカスタマー インフォメーション センターにてご相談を承っております。

Microsoft カスタマー インフォメーション センター

営業時間：月 - 金 9:00 - 17:30

電話番号：0120-41-6755 (フリーダイヤル)

※ 自動音声ガイダンスに従って、「1」 - 「1」の順に番号をご選択頂くと、担当者へ繋がります。

Windows Intune SA (Software Assurance) 権でご使用いただける OS ライセンスに関するご質問がある場合には、次のライセンス認証専用窓口にてご相談を承っております。

マイクロソフト ライセンス認証専用窓口の電話番号

<http://www.microsoft.com/ja-jp/licensing/existing-customers/activation-centers.aspx>

(無料通話用窓口) 電話番号：0120-801-734

(有料通話用窓口) 電話番号：03-6831-3460

## 10. リソース

---

- Windows Intune の Web サイト

<http://www.microsoft.com/ja-jp/windows/windowsintune/>

- Windows Intune のオンラインヘルプ

<http://onlinehelp.microsoft.com/ja-jp/windowsintune.latest>

- Windows IntuneTechNet

<http://technet.microsoft.com/ja-jp/library/hh456367.aspx>

- 日本マイクロソフト Windows Intune チームのブログ

<http://blogs.technet.com/b/jpintune/>

- Windows Intune チームのブログ（英語）

<http://blogs.technet.com/b/windowsintune>

一部の情報はプレリリース版の製品およびサービスに関連しており、製品版としてリリースされる前に大幅に変更される可能性があります。マイクロソフトはこのドキュメントで提供する情報について、明示または黙示を問わずいかなる保証もしません。製品およびサービスによっては、すべての言語、あるいはすべての国または地域で提供されていないものもあり、プレリリース版ソフトウェアの英語バージョンが使用される場合があります。一部の機能では、Windows Intune サービスと System Center 2012 Configuration Manager SP1 または System Center 2012 R2 Configuration Manager を使用する必要があることがあります。

©2014 Microsoft Corporation

