第 10 章

Microsoft Intune による更新プログラムと Endpoint Protection の管理

目次

概要

大多数のエンタープライズ デスクトップおよびデバイスの管理者にとっての主要な責務として、管理対象のクライアントに対するソフトウェア更新プログラムと Endpoint Protection の保守が挙げられます。従来の LAN ネットワーク ソリューションでは、Windows Server Update Services や System Center Configuration Manager などの製品に依存して更新プロセスを管理していました。Microsoft Intune は、クラウドベースのソリューションを求めている組織にとって、最新のソフトウェア更新プログラムとマルウェア対策定義ファイルでコンピューターを最新の状態に維持するのに役立つ強力なソリューションとなります。この章では、Intune を使用して、ソフトウェア更新プログラムと Endpoint Protection を構成および管理するプロセス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 を使用して更新プログラムを管理することができます。
- Endpoint Protection を管理することができます。

レッスン 1
Intune による更新プログラムの管理

Intune は、Microsoft および Microsoft 以外のソフトウェア更新プログラムの展開をサポートして、管理対象コンピューターが、発見された脆弱性から安全に保護されるようにします。ソフトウェア更新プログラムの構成、承認、および展開プロセスを理解することが重要です。このレッスンでは、Intune を使用してソフトウェア更新プログラムを管理する方法と、レポートを使用してソフトウェア更新プロセスの有効性を判断する方法について説明します。

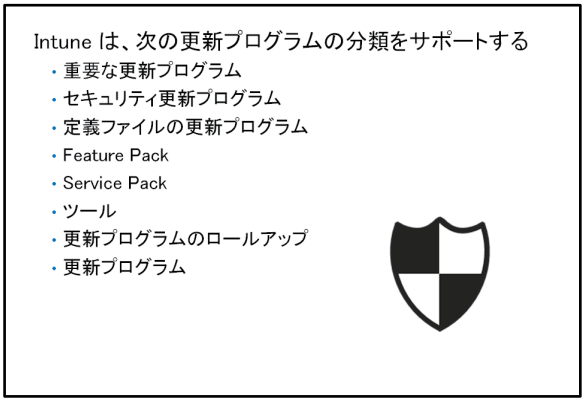
目的

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更新プログラムの種類を説明することができます。
- Intune で更新プログラムを構成および管理するプロセスを説明することができます。
- 構成できる更新ポリシー設定を説明することができます。
- 製品カテゴリ、更新プログラムの分類、および自動承認規則の構成方法について説明することができます。
- Microsoft 以外の更新プログラムの管理方法を説明することができます。
- 更新プログラムの承認および展開の方法を説明することができます。
- ソフトウェア更新プログラムを構成して展開することができます。

Intune により管理できる更新プログラムの種類

Intune を使用して、大多数の Microsoft 製品の更新プログラムを管理して展開できます。Intune 管理コンソールを使用して、管理する Microsoft 製品を選択できます。組織の要件を満たすためにサポートする必要がある更新プログラムの分類を選択して、各管理対象製品の更新プログラムをさらに詳細に制御できます。



Intune は、次の種類の更新プログラムの分類をサポートしています。

- **重要な更新プログラム :** セキュリティの問題に関連しない、特定の重要な問題を修正します。
- **セキュリティ更新プログラム :** 製品固有のセキュリティ関連の脆弱性を修正します。Microsoft は、各セキュリティ更新プログラムの重要度を、緊急、重要、警告、注意の 4 段階で評価しています。
- **定義ファイルの更新 :** 製品の定義データベースに対するソフトウェア更新プログラムです。定義データベースは、製品内の悪意のあるコード、ファイル、および参照を検出するために使用されます。例えば、Outlook の迷惑メール フィルターは、この種類の更新を使用して保守されます。
- **Feature Pack :** 新しい製品機能を提供するもので、通常は定期的な Service Pack のリリース サイクル以外でリリースされます。
- **Service Pack :** すべての重要な更新プログラム、セキュリティ更新プログラム、および通常の更新プログラムの累積的なセットです。特定の製品の新機能を含む場合もあります。
- **ツール :** ユーティリティや製品の特定の機能の修正プログラムを提供します。

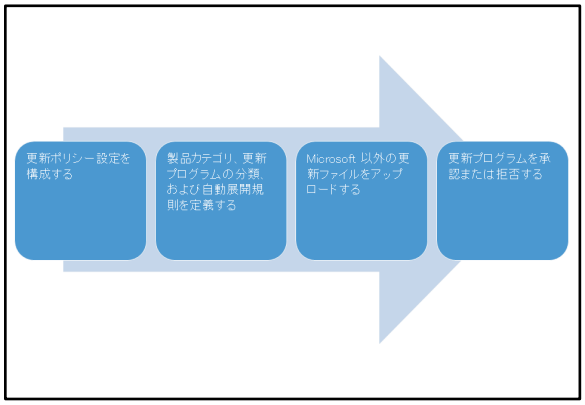
- **更新プログラムのロールアップ :** Service Pack と同様に、すべての重要な更新プログラム、セキュリティ更新プログラム、および更新プログラムの累積的なセットが含まれます。ただし、更新プログラムのロールアップは通常、製品の特定のコンポーネントまたは機能を対象にしています。
- **更新プログラム :** 特定の問題を修正し、セキュリティに関連せず、深刻ではない問題に対処します。

製品、および更新プログラムの分類の選択に基づいて、使用可能な更新プログラムをすべて表示できます。更新プログラムを表示するには、[更新プログラム] をクリックします。

注 : [更新プログラム] は、1 つ以上のクライアント コンピューターに Intune クライアント ソフトウェアをインストールした後でのみ、Intune 管理コンソールで表示できます。

更新プログラムの構成および管理プロセス

Intune クライアント ソフトウェアをクライアント コンピューターにインストールすると、[更新プログラム] が Intune 管理コンソールに表示されます。Windows ベースの製品と Office ベースの製品は、既定では、重要な更新プログラム、セキュリティ更新プログラム、および定義の更新を提供するように選択されています。Service Pack と更新プログラムのロールアップも既定で選択されています。このような既定の設定があっても、選択および展開オプションを変更したいこともよくあります。



次のプロセスで、管理対象コンピューターに更新プログラムを効果的に展開するのに役立つガイドラインを示します。

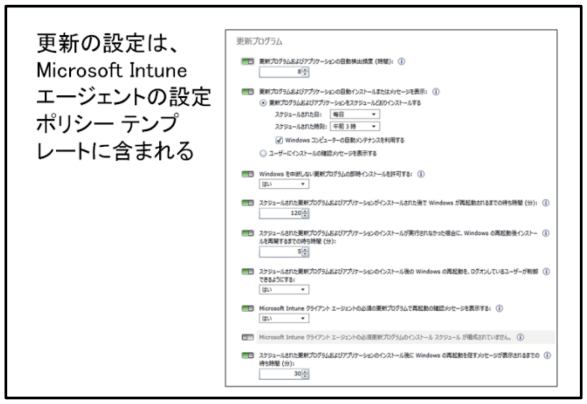
1. 更新ポリシー設定を構成する : 最初に構成する必要のあるコンポーネントは、管理対象のコンピューターに適用する更新ポリシー設定です。これらの設定は、Microsoft Intune エージェントの設定ポリシーの [更新プログラム] セクションにあります。
2. 製品カテゴリ、更新プログラムの分類、および自動展開規則を定義する : 前述したように、製品カテゴリと更新プログラムの分類のセットは既定で選択されています。この既定の選択を変更して、使用環境で管理する更新プログラムの種類のみを含めることができます。自動展開規則を作成して、一般的な更新プログラムの承認と展開のプロセスを自動化するように選択することもできます。
3. Microsoft 以外の更新ファイルをアップロードする : 更新プログラムのアップロード ウィザードを使用して、Microsoft 以外の更新ファイルを Intune にアップロードすることができます。ファイルをアップロードすると、他の Microsoft ベースの更新プログラムと同様に承認または拒否ができます。
4. 更新プログラムを承認または拒否する : 更新プログラムが管理対象コンピューターに適用可能になると、[更新プログラム] の [概要] ページでそのことが通知されます。この通知を開くと、承認待ちの更新プログラムの一覧が表示されます。フィルターを使用して、特定の種類の更新プログラムまたは更新状態を検索することもできます。新しい更新プログラムを承認すると、更新プログラムを展開するグループを選択して、展開の種類を指定できます。展開の種類には、利用可能なインストール、必須のインストール、またはアンインストールを含めることができます。更新プログラムのインストールが特定の時間までにおこなわれるように、期限を指定することもできます。

更新プログラムを拒否すると、現在のすべての承認が削除され、更新プログラムはすべての既定のビューで非表示になります。[更新プログラム] で [拒否済み] フィルターを選択すると、拒否された更新プログラムの一覧を表示できます。

更新ポリシー設定の概要

第 9 章で、Intune ポリシーの管理と展開の概要を説明しました。Intune では構成可能なさまざまな構成ポリシーを提供して、ユーザーや管理対象のクライアントに展開できることを思い出してください

Intune の更新機能は、Microsoft Intune エージェントの設定ポリシー テンプレートでの設定によって構成されます。次の表に、ポリシー テンプレートで使用できる更新プログラムの設定とその説明を示します。



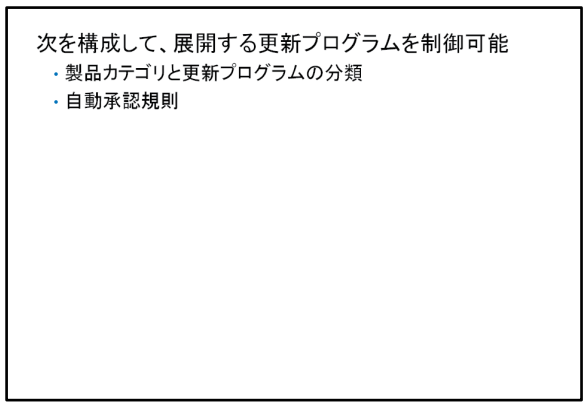
設定	説明
更新プログラムおよびアプリケーションの自動検出頻度 (時間)	Intune エージェントが新しい更新プログラムおよびアプリケーションをチェックする頻度を指定します。この設定は 8 ～ 22 時間の範囲で構成できます。 既定の設定は 8 時間です。
更新プログラムおよびアプリケーションの自動インストールまたはメッセージを表示	更新プログラムおよびアプリケーションを自動的にインストールするか、ユーザーにインストール確認メッセージを表示するかを指定します。更新プログラムおよびアプリケーションを自動的にインストールするように選択した場合は、展開する日時のスケジュールをさらに定義できます。 また、[Windows コンピューターの自動メンテナンスを利用する] オプションを選択することもできます。このオプションは、すべてのインストールおよび更新を自動メンテナンス機能の一部として実行します。 既定の設定では、更新プログラムおよびアプリケーションは毎日午前 3 時に自動的にインストールされます。Windows コンピューターの自動メンテナンスは既定で選択されています。
Windows を中断しない更新プログラムの即時インストールを許可する	この設定で [はい] を選択した場合、更新によって Windows オペレーティング システムを中断または再起動することがわかっている場合以外、更新プログラムをダウンロード後すぐにインストールします。すぐにインストールされない更新プログラムは、[更新プログラムおよびアプリケーションの自動インストールまたはメッセージを表示] 設定に従ってインストールされます。 この設定で [いいえ] を選択した場合、すべての更新プログラムは、[更新プログラムおよびアプリケーションの自動インストールまたはメッセージを表示] 設定に従ってインストールされます。 既定の設定は [はい] です。
スケジュールされた更新プログラムおよびアプリケーションがインストールされた後で Windows が再起動されるまでの待ち時間 (分)	スケジュールされた更新プログラムおよびアプリケーションがインストールされてから、Windows オペレーティング システムが再起動するまでの待ち時間を指定します。これは 1 ～ 240 分の範囲で構成できます。 既定の設定は 120 分です。

設定	説明
スケジュールされた更新プログラムおよびアプリケーションのインストールが実行されなかった場合、Windows の再起動後インストールを再開するまでの待ち時間 (分)	スケジュールされた更新プログラムおよびアプリケーションのインストールが実行されなかった場合、Windows オペレーティング システムの再起動後、インストールを開始するまでの待ち時間を指定します。これは、1 ～ 60 分の範囲で設定できます。 既定の設定は 5 分です。
スケジュールされた更新プログラムおよびアプリケーションのインストール後の Windows の再起動を、ログオンしているユーザーが制御できるようにする	このポリシー設定を [はい] に設定すると、Windows オペレーティング システムを再起動する必要がある場合、ユーザーは再起動の確認メッセージを受け取ります。この設定を [いいえ] に設定すると、更新プログラムのインストールを完了するために Windows オペレーティング システムの再起動が必要な場合、サインインしているユーザーに自動的に再起動されることが通知されます。 既定値は [はい] です。
Microsoft Intune クライアント エージェントの必須の更新プログラムで再起動の確認メッセージを表示する	このポリシー設定を [はい] に設定すると、Intune クライアント エージェントが更新されて再起動が必要な場合、サインインしているユーザーに再起動の確認メッセージが表示されます。この設定を [いいえ] に設定すると、サインインしているユーザーに、Windows オペレーティング システムの再起動の確認メッセージは表示されません。この場合、クライアントが再起動するまで Intune は正しく機能しない可能性があることに注意してください。 既定値は [はい] です。
Microsoft Intune クライアント エージェントの必須更新プログラムのインストール スケジュール	Intune クライアント エージェントの更新プログラムのスケジュールを構成します。既定では、この設定は無効です。
スケジュールされた更新プログラムおよびアプリケーションのインストール後に Windows の再起動を促すメッセージが表示されるまでの待ち時間 (分)	スケジュールされた更新プログラムまたはアプリケーションが Windows オペレーティング システムの再起動を必要とし、ユーザーがこれを延期した場合、ユーザーに再起動を促すメッセージを表示する頻度を指定します。これは 1 ～ 1,440 分 (24 時間) の範囲で構成できます。 既定値は 30 分ごとです。

ポリシー設定を構成して保存した後、ポリシーを展開するデバイス グループを指定します。

製品カテゴリ、更新プログラムの分類、および自動承認規則の構成

更新プログラムをクライアント デバイスに効果的に展開するには、サポートする製品および各製品の更新プログラムの分類を決定する必要があります。また、組織全体に展開する必要のある一般的な更新プログラムの承認と展開を自動化したい場合もあります。



製品カテゴリと更新プログラムの分類

Intune を使用した更新プログラムの展開を計画する場合の主な考慮事項の 1 つは、組織内で管理する必要がある製品と更新プログラムの種類を特定することです。Intune では、更新プログラムを管理する必要がある製品または製品のカテゴリを選択できます。また、選択した製品に対して管理する必要がある更新プログラムの分類も選択できます。これらの選択の結果は、[更新プログラム] に使用可能な更新プログラムの一覧として表示されます。

製品カテゴリと更新プログラムの分類の設定を構成するには、[管理者]、[更新プログラム] ノードの順にクリックします。コンソールの [サービスの設定 : 更新] ページで設定を構成します。

自動承認規則

[管理者] の [更新プログラム] ノードには、自動承認規則を作成および管理できるセクションもあります。自動承認規則により、承認プロセスを自動化して、常に展開する更新プログラムに対する管理負荷を最小限に抑えることができます。例えば、更新プログラムの一覧を参照して更新プログラムを 1 つずつ手動で選択して承認する代わりに、Office の重要な更新プログラムをすべて自動で承認して展開するように決定する場合があります。

自動承認規則を作成するには、次の手順を実行します。

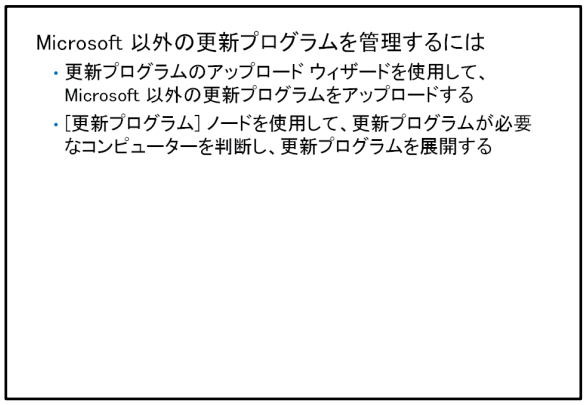
1. [管理者] で、[更新プログラム] ノードをクリックします。
2. [自動承認規則] で、[新規作成] をクリックします。
3. [全般] ページで、[名前] と [説明] を入力します。
4. [製品カテゴリ] ページで、この規則で使用する製品を選択します。
5. [更新の分類] ページで、自動で展開する更新プログラムの分類を選択します。
6. [展開] ページで、自動更新を受信するデバイス グループを選択します。また、更新プログラムが承認後の特定の日数以内にインストールされるようにインストールの期限を指定することもできます。

新しい規則を作成すると、その規則は今後更新プログラムが利用可能になったときに、それらすべてに適用されます。既存の更新プログラムを承認したい場合は、規則を選択して [選択項目の実行] をクリックすると、規則を実行できます。

Microsoft 以外の更新プログラムの管理

Intune を使用して、Microsoft 以外のアプリケーションの更新プログラムを承認し展開できます。Microsoft 以外の更新プログラムを管理するには、次の点を考慮してください。

- ベンダーから更新プログラムを入手し、更新プログラムのアップロード ウィザードを使用して、それを Intune にアップロードする必要があります。
- サポートされる更新プログラムのファイル形式は、.exe、.msi、.msp です。
- 更新ファイルは、ユーザーの介在を必要としない展開方法をサポートしている必要があります。



Microsoft 以外の更新プログラムを追加するには、次の手順を実行します。

1. [更新プログラム] をクリックし、[概要] ノードで [更新プログラムの追加] をクリックします。また、[更新プログラム] で更新プログラムの分類ノードのいずれかをクリックし、[アップロード] をクリックして更新プログラムのアップロード ウィザードを開始することもできます。
2. [更新ファイル] ページで、アップロードする更新ファイルを参照して選択します。そのファイルが追加のサポート ファイルを必要とする場合は、[追加のファイルおよび同じフォルダーのサブフォルダーを含める] チェック ボックスをオンにします。
3. [更新プログラムの説明] ページで、次の項目を指定します。
   - 発行元 : ファイルの発行元の名前を入力します。
   - 名前 : アップロードするファイルの名前を指定します。
   - 分類 : アップロードする更新プログラムの種類を指定します。選択肢には、更新プログラム、重要な更新プログラム、セキュリティ更新プログラム、更新プログラムのロールアップ、Service Pack があります。
   - 説明 : 更新プログラムの説明を入力します。
4. [要件] ページで、更新プログラムのアーキテクチャ (32 ビットまたは 64 ビット) とオペレーティング システムの要件を指定します。
5. [検出規則] ページで、既定の検出規則を使用するかを指定します。特定のファイル、MSI 製品コード、またはレジストリ キーが存在するかに基づいた、独自のカスタム規則を追加できます。

注 : .msi および .msp ファイルを展開する場合、これらのパッケージ内には独自の検出規則が含まれるため、[検出規則] ページは表示されません。

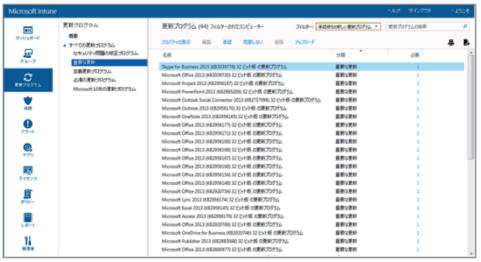
6. [前提条件] ページで、この更新プログラムをインストールする前にインストールしておく必要があるソフトウェアを指定できます。[なし] を指定するか、Intune で管理されるソフトウェア パッケージを指定するか、またはファイル、MSI 製品コード、特定のレジストリ キーが存在するかどうかに基づいて手動で規則を追加できます。このオプションは、.msi または .msp ファイルを展開する場合は無効です。
7. [コマンド ライン引数] ページで、更新プログラムのインストール中に適用する追加のコマンドライン スイッチを指定できます。例えば、更新プログラムがユーザーの介在なしにインストールされるようにするために、「/q」などのスイッチの指定が必要になる場合があります。
8. [リターン コード] ページで、インストールのリターン コードの解釈方法を指定できます。既知のリターン コードを追加して、成功や成功 (再起動が必要) など、各コードが何を表すかを指定できます。このオプションは、.msi または .msp ファイルを展開している場合は無効です。

更新ファイルをアップロードすると、[更新プログラム] で更新プログラムを表示できます。更新プログラムを確認するには、[Microsoft 以外の更新プログラム] ノードを使用して表示を簡単にフィルター処理することができます。また、更新プログラムをアップロードしたときに指定した、更新プログラムの分類に対応するノードから、更新プログラムを表示することもできます。これらのノードから、更新プログラムが必要なコンピューターの数、更新プログラムがインストールされたコンピューターの数、およびインストールに失敗したコンピューターを表示できます。

更新プログラムの承認と展開

[更新プログラム] の [概要] ノードで、クライアントの更新状態を確認できます。更新状態には、承認待ちの新しい更新プログラムの数と、追加の承認が必要な更新プログラムの数が示されます。[承認待ちの新しい更新プログラム] リンクをクリックすると、[すべての更新プログラム] ノードに移動し、[承認待ちの新しい更新プログラム] フィルターがリスト ビューに適用されます。

[更新プログラム] で、更新プログラムを承認し、展開する



更新プログラムを選択すると、次のオプションが表示されます。

- **プロパティの表示 :** 説明、分類、想定される動作、更新プログラムを適用する製品など、更新プログラムに関する詳細情報を表示します。更新が必要なコンピューターの数や、更新を要求しているコンピューターに関する詳細情報を表示することもできます。
- **編集 :** Microsoft 以外の更新プログラムのプロパティを編集できます。
- **承認 :** 更新プログラムの展開を承認します。また、更新プログラムのグループと展開スケジュールを構成することもできます。
- **拒否 :** 更新プログラムを拒否して現在の承認を削除します。このオプションにより、更新プログラムは既定のビューで非表示になります。さらに、更新プログラムのレポート データも削除されることに注意してください。
- **削除 :** Intune にアップロードされた Microsoft 以外の更新プログラムを削除できます。
- **アップロード :** 更新プログラムのアップロード ウィザードを開始して、Microsoft 以外の更新プログラムをアップロードします。

更新プログラムの承認

更新プログラムを承認するには、次の手順を実行します。

1. 更新プログラムを選択して、[承認] をクリックします。
2. [グループの選択] ページで、更新プログラムを展開するグループを選択し、[追加] をクリックします。
3. [展開アクション] ページで、適切な承認と期限を選択します。期限には、[なし]、[直ちに]、[1 週間]、[2 週間]、[1 か月]、または [カスタム] 設定を指定できます。承認には、次のオプションがあります。
    - 必須のインストール : グループ内のコンピューターに更新プログラムをインストールします。
    - 該当なし : 更新プログラムをインストールしません。これは、更新プログラムをインストールせずに適用性をレポートする場合に役立ちます。
    - 利用可能なインストール : ユーザーは、Intune ポータル サイトからオンデマンドでアプリケーションをインストールできます。
    - アンインストール : 更新プログラムを削除します。

注 : 子グループに [該当なし]、[必須のインストール]、または [アンインストール] が明示的に構成されている場合を除き、子グループは親グループに構成されているすべてのアクションを継承します。

デモンストレーション : 更新プログラムの構成と展開

講師は、次のデモンストレーションをおこないます。

- Intune を使用して、更新プログラムを構成し展開する

デモンストレーションの手順

1. LON-CL1 で、http://manage.microsoft.com から Intune 管理コンソールにサインインします。
2. [更新プログラム] で、既定の製品カテゴリと更新プログラムの分類設定に基づいて一覧される既定の更新プログラムを確認します。
3. [管理者] で、[更新プログラム] ノードをクリックし、[製品カテゴリ] と [更新プログラムの分類] の選択を必要に応じて修正します。
4. [更新プログラム] で、必要に応じて表示をフィルター処理します。
5. 展開する更新プログラムを選択します。
6. [承認] をクリックし、グループ選択と展開アクションを指定します。
7. [概要] ノードをクリックし、更新状態を確認します。

知識の確認

質問	
次の種類の更新プログラムのみを提供するには、Intune の更新プログラムの分類を構成する必要があります。 • **重要な、セキュリティ関連以外の問題** • **製品固有のセキュリティの問題** • **Outlook の迷惑メール フィルター** **どの更新プログラムの分類を選択する必要がありますか。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。	
	更新プログラム
	重要な更新プログラム
	ツール
	セキュリティ更新プログラム
	定義ファイルの更新プログラム

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**
子グループを含むグループに対して更新プログラムが承認され展開された場合、承認は子グループにも適用されます。	

レッスン 2
Endpoint Protection の管理

Intune Endpoint Protection により、組織でしばしば発生するマルウェアの脅威に対するリアルタイム保護を実現できます。Intune を使用して、マルウェア定義を最新の状態に保つことができます。また、マルウェアによる攻撃の管理と監視に役立つツールも提供しています。このレッスンでは、Intune で管理対象クライアントの Endpoint Protection を管理する方法について説明します。

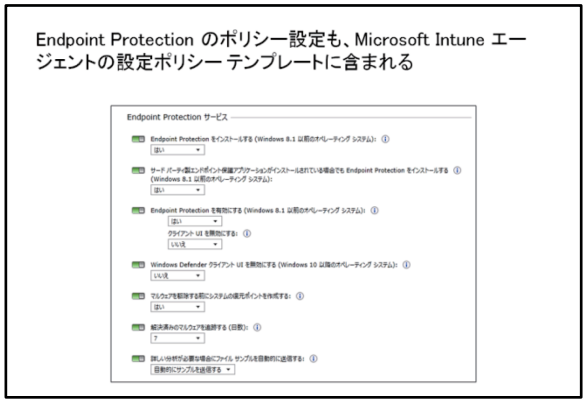
目的

このレッスンにより、次のことを習得できます。

- Endpoint Protection のポリシー設定を説明することができます。
- Endpoint Protection の監視方法を説明することができます。
- Endpoint Protection の管理タスクを説明することができます。

Endpoint Protection サービス設定の構成

Endpoint Protection の設定は、「Microsoft Intune エージェントの設定」ポリシー テンプレートに含まれています。次の表では、ポリシー テンプレートで使用可能な Endpoint Protection サービス設定とその説明を示します。



設定	説明
Endpoint Protection のインストール (Windows 8.1 以前のオペレーティング システム)	このポリシーで [はい] を選択した場合、Intune Endpoint Protection が、Windows 8.1 以降のオペレーティング システムを実行するクライアント コンピューターにインストールされます。 [いいえ] を選択した場合、Intune Endpoint Protection は管理対象コンピューターからアンインストールされます。 既定の設定は [はい] です。 Windows 10 クライアントには、Intune Endpoint Protection クライアントはインストールされません。Intune で、Windows 10 クライアントの組み込みの Windows Defender サービスを管理できます。
サード パーティ製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 (Windows 8.1 以前のオペレーティング システム)	Microsoft 以外の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 クライアントのインストールを強制します。 既定の設定は [はい] です。 Endpoint Protection クライアントをインストールして正常に機能するようになったら、Microsoft 以外のアプリケーションを削除することをお勧めします。

設定	説明
Endpoint Protection を有効にする (Windows 8.1 以前のオペレーティングシステム)	この設定で [はい] を選択すると、Endpoint Protection は、Endpoint Protection クライアントをインストールしているクライアントで有効になり、機能するようになります。 [いいえ] を選択すると、Endpoint Protection クライアントは無効になり、クライアント UI はユーザーに表示されなくなります。 既定の設定は [はい] です。
Windows Defender クライアント UI を無効にする (Windows 10 以降のオペレーティング システム)	この設定で [はい] を選択すると、Intune は Windows Defender クライアント設定をエンド ユーザーに対して非表示にします。 [いいえ] を選択すると、Windows Defender クライアントはエンド ユーザーに表示されます。 既定の設定は [いいえ] です。
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	[はい] を選択すると、クライアント コンピューター上で検出されたアイテムを消去する直前に、Windows でシステムの復元ポイントが作成されます。 既定の設定は [はい] です。
解決済みのマルウェアを追跡する (日数)	指定した日数の間、解決済みのマルウェアを追跡します。0 ～ 30 日の日数を指定できます。 既定値は 7 日です。
詳しい分析が必要な場合にファイル サンプルを自動的に送信する	詳しい分析のための Microsoft へのファイルの送信と通知に関する Endpoint Protection クライアントの対応方法を制御します。 [常に確認する] と [自動的にサンプルを送信する] のいずれかを選択できます。 既定値は [自動的にサンプルを送信する] です。

一般的なサービス設定のほかに、Endpoint Protection クライアントまたは Windows Defender (Windows 10 以降の場合) の動作に関連する設定を構成することもできます。これらの設定は、次の項目に関連します。

- [リアルタイム保護] で、リアルタイム保護、動作の監視、およびネットワーク検査システムのスキャンを制御するための設定をおこないます。
- [スキャンのスケジュール] で、クライアント コンピューター上で実行するスキャン スケジュールの頻度と種類を制御するための設定をおこないます。
- [スキャンのオプション] で、電子メール メッセージのスキャン、ネットワーク ドライブのスキャン、スキャン中の CPU 使用率の制限など、追加のオプションを制御するための設定をおこないます。
- [既定の処置] で、コンピューターでマルウェアが検出された際の既定の操作を指定します。重大、高、中、低など、さまざまなアラート レベルに対する既定の操作を指定できます。
- [除外するファイルとフォルダー] で、スキャンの実行時またはリアルタイム保護の使用時に、ファイルまたはフォルダーを除外する設定をおこないます。
- [除外するプロセス] で、スキャンの実行時またはリアルタイム保護の使用時に、特定のプロセスを除外するための設定をおこないます。
- [除外するファイルの種類] で、スキャンの実行時またはリアルタイム保護の使用時に、特定のファイル拡張子を除外するように指定できます。
- [Microsoft Active Protection Service] で、Microsoft Active Protection Service に参加するか、およびメンバーシップ レベルを指定するかを指定できます (Windows 8.1 以降のオペレーティング システム用)。

ポリシー設定を構成して保存した後、ポリシーを展開するデバイス グループを指定します。

注 : Intune は、Microsoft 以外のマルウェア対策アプリケーションを自動的にアンインストールしません。Microsoft 以外のアプリケーションをアンインストールしてから、Intune Endpoint Protection をインストールする必要があります。

Endpoint Protection の監視

次のワークスペースにアクセスして、クライアント デバイスで Endpoint Protection の状態を監視できます。

- 保護
- アラート

ワークスペース	アラートの種類
保護	• 概要 　• マルウェアの状態 　• 検出数の最も多いマルウェア 　• デバイスの状態 • すべてのマルウェア
アラート	• Endpoint Protection エラーの調査 • 解決済みのマルウェアの調査 • Endpoint Protection の警告の調査 • 新しいマルウェアの調査

保護ワークスペースによる監視

[保護] をクリックすると、次の 2 つのメイン ページにアクセスできます。

- [概要] ページに、Endpoint Protection に関連する状態情報のダッシュボードが表示されます。このページに表示される情報の種類として、フォローアップが必要なマルウェア インスタンス、注意が必要なマルウェアを含むコンピューター、保護されていないデバイスの一覧、および別のマルウェア対策アプリケーションを実行しているデバイスの一覧があります。
- [すべてのマルウェア] ページに、その環境でレポートされたすべてのマルウェアの一覧が表示されます。ここでマルウェアが最近解決されたか、フォローアップが必要か、および現在までの検出数を特定できます。また、リンクをクリックして、検出された特定の種類のマルウェアの詳細を確認することもできます。

注 : [保護] は、少なくとも 1 台のコンピューターに Intune クライアント ソフトウェアをインストールして管理するまで表示されません。

アラート ワークスペースによるアラートの確認

[アラート] には、最新のアラートの概要が表示されます。これには、最近解決されたマルウェアおよび検出された新しいマルウェアに関連するアラートが含まれます。アラート ウィンドウで、[Endpoint Protection] ノードをクリックして、Endpoint Protection に関連して生成されたすべてのアラートを表示することもできます。

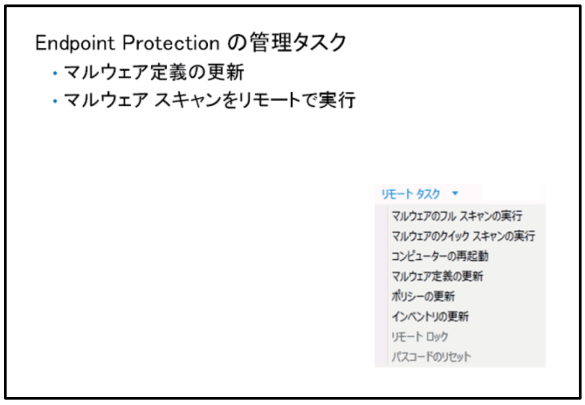
次の手順で、組み込みのアラートの種類を表示できます。

1. [管理者] をクリックします。
2. [アラートと通知] で、[アラートの種類] をクリックします。
3. アラートの種類を表示します。これには次が含まれます。
    - Endpoint Protection エラーの調査
    - 解決済みのマルウェアの調査
    - Endpoint Protection の警告の調査
    - 新しいマルウェアの調査

注 : 特定の種類のアラートが生成されると必ず通知するようにしたい場合は、[管理者] にアクセスして、必要に応じて管理者に電子メール通知を送信する通知規則を構成します。

Endpoint Protection の管理タスク

Intune には、Endpoint Protection を管理するために実行できる多数のリモート タスクが用意されています。リモート タスクには次のものが含まれます。



- **マルウェア定義の更新 :** このタスクは、マルウェア定義を更新して、コンピューター クライアントで確実に最新の保護が使用可能になるようにします。
- **マルウェア スキャンをリモートで実行 :** Intune 管理コンソールから選択したコンピューターでマルウェアのフル スキャンまたはマルウェアのクイック スキャンを実行できます。

リモート タスクを実行するには、次の手順を完了します。

1. [グループ] から、適切なデバイス グループを選択するか、[すべてのデバイス] を選択します。
2. 必要に応じて [デバイス] ページをクリックします。
3. リモート タスクを実行するコンピューターを選択します。
4. [リモート タスク] ドロップダウン リストをクリックし、適切なタスクを選択します。

コンソールの [リモート タスクの状態] をクリックすると、[リモート タスクの状態] ダイアログ ボックスが開き、リモート タスクに関する最新の状態情報が表示されます。

知識の確認

質問	
次の Intune ワークスペースのうち、マルウェアの状態、検出数の最も多いマルウェア、およびデバイスの状態を提供するのはどれですか。	
正しい解答を選択してください。	
	アプリ
	ポリシー
	レポート
	保護

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
Intune は、すべての Windows 10 ワークステーションに Endpoint Protection クライアントをインストールします。	

演習 : Microsoft Intune による更新プログラムと Endpoint Protection の管理

シナリオ

あなたは、Intune を使用して、A. Datum 社に更新プログラムの管理と Endpoint Protection を実装する必要があります。Intune クライアント ソフトウェアは、A. Datum 社のクライアント コンピューターに展開済みで、この機能の管理に必要なポリシーを構成する準備が整いました。

目的

この演習により、次のことを習得できます。

- Intune で更新プログラムを構成することができます。
- Intune で Endpoint Protection 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 : 30 分

仮想マシン	23697-2B-LON-DC1 23697-2B-LON-CL1 MSL-TMG1
ユーザー名	Adatum¥Administrator 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。

この演習を完了するためには、第 8 章と第 9 章のすべての前提条件を満たし、第 8 章と第 9 章の演習が完了している必要があります。

練習 1 : Intune での更新プログラムの構成

シナリオ

Intune 実装の次の段階は、ソフトウェア更新プログラムの管理機能の使用を開始することです。組織に代わって管理する製品と更新プログラムの分類を指定する必要があります。また、適切なポリシー設定を構成し、必要な更新プログラムのクライアント コンピューターへの展開を開始する必要があります。

主な作業は次のとおりです。

1. 製品および更新プログラムの分類を構成する
2. 更新ポリシー設定を構成する
3. 更新レポートを表示する
4. 更新プログラムを承認し展開する
5. 自動承認規則を構成する

▶ 作業 1 : 製品および更新プログラムの分類を構成する

1. LON-CL1 に切り替え、Internet Explorer を開きます。
2. http://manage.microsoft.com を参照します。
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、[更新プログラム] ページを参照します。
5. [製品カテゴリ] で、既定の選択のすべてをオフにします。
6. [製品カテゴリ] で、次を選択します。
   - Office 2013
   - Windows 10
   - Windows 10 LTSB
7. [更新プログラムの分類] で、次のプログラムのみ (他はすべてオフ) を選択します。
   - セキュリティ問題の修正プログラム
   - 重要な更新
   - 定義更新プログラム
8. すべての変更を保存します。
9. [更新プログラム] で、すべての新しい更新プログラムを表示し、承認します。更新プログラムが表示されるまで、時間がかかる場合があります。承認待ちの更新プログラムが少なくとも 1 つある必要があります。

注 : 更新プログラムを承認する前に、クライアント コンピューターの更新プログラム ポリシー設定を構成します。

▶ 作業 2 : 更新ポリシー設定を構成する

1. [ポリシー] で、既存の Microsoft Intune エージェントの設定ポリシーを編集します。このポリシーは前の演習で作成されました。
2. [更新プログラム] セクションで、次の設定を構成して、ポリシーを保存します。
   - 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
   - Windows を中断しない更新プログラムの即時インストールを許可する : いいえ
   - スケジュールされた更新プログラムおよびアプリケーションのインストールが実行されなかった場合に、Windows の再起動後インストールを再開するまでの待ち時間 (分) : 30
3. ポリシーが [すべてのコンピューター] デバイス グループに適用されるように、展開を変更します。

▶ 作業 3 : 更新レポートを表示する

1. [更新プログラム] で、[概要] ノードをクリックし、更新レポートを表示します。[更新レポート] ノードドが選択された状態で、[レポート] が表示されます。
2. [更新レポート] ページで次の値を選択し、[レポートの表示] をクリックします。
   - 更新プログラムの分類の選択 : 重要な更新プログラム
   - 更新状態の選択 : 必要

[更新レポート] が表示され、クライアント コンピューターに必要な更新プログラムがすべて表示されます。結果が表示されるまで、時間がかかる場合があります。

注 : このレポートは、他のファイル形式で印刷またはエクスポートできることを確認します。

▶ 作業 4 : 更新プログラムを承認し展開する

1. [更新プログラム] で、[重要な更新] をクリックします。
2. 一覧の先頭の更新プログラムを承認し、[すべてのコンピューター] デバイス グループに展開します。
3. [1 週間] の期限付きの [必須のインストール] として、更新プログラムを構成します。

▶ 作業 5 : 自動承認規則を構成する

1. [管理者] で [更新プログラム] をクリックし、[自動承認規則] まで下にスクロールします。
2. 自動承認規則を次のように構成します。
   - 名前 : Critical Office Updates
   - 製品カテゴリ : Office 2013
   - 更新プログラムの分類 : 重要な更新プログラム
   - 展開 : すべてのコンピューター
3. インストールの期限 : 承認後 7 日

結果 : この練習により、Intune 更新プログラムの機能を構成することができました。

練習 2 : Intune での Endpoint Protection の構成

シナリオ

更新プログラム機能と共に、Intune を使用して、Endpoint Protection を実装することに決めました。保護すべき Windows 7 と Windows 10 のクライアントがあります。また、次の要件を満たす必要があります。

- Endpoint Protection をすべての Windows 7 コンピューターにインストールする必要がある。
- Windows 8 コンピューターでは Windows Defender を使用する。
- 詳しい分析用にファイル サンプルを送信しない。
- 毎日午前 3:00 にフル スキャンを実行するようにスケジュールする必要がある。
- 毎日正午にクイック スキャンを実行するようにスケジュールする必要がある。

主な作業は次のとおりです。

1. Endpoint Protection ポリシー設定を構成する
2. マルウェアの検出をテストする
3. Endpoint Protection 管理タスクを実行する

▶ 作業 1 : Endpoint Protection ポリシー設定を構成する

1. [ポリシー] で、既存の Microsoft Intune エージェントの設定ポリシーを編集します。このポリシーは前の演習で作成されました。
2. [Endpoint Protection] セクションで、次の設定を構成し、ポリシーを保存します。
   - Endpoint Protection のインストール : はい
   - 詳しい分析が必要な場合にファイル サンプルを自動的に送信する : 送信しない
   - 毎日のクイック スキャンのスケジュール/スケジュールされた時刻 : 午後 12 時
   - フル スキャンのスケジュール : はい

▶ 作業 2 : マルウェアの検出をテストする

1. LON-CL1 で、エクスプローラーを開き、C:¥Files を参照します。
2. Sample.txt ファイルを編集し、<remove> のすべてのインスタンスを削除します (山かっこを含む)。
3. ファイルを保存して閉じます。

注 : Windows Defender は、直ちにマルウェア ファイルのサンプルを検出し、クリーンアップします。

4. Microsoft Intune Center を起動します。

注 : このページから Windows Defender を起動できることを確認します。アプリケーションを取得し、それらの更新プログラムを確認することもできます。

5. [更新プログラムの確認] をクリックします。

▶ 作業 3 : Endpoint Protection 管理タスクを実行する

1. [グループ] で [すべてのコンピューター] をクリックし、[LON-CL1.Adatum.com] をクリックします。
2. LON-CL1.Adatum.com で、[マルウェア定義の更新] リモート タスクを実行します。
3. [リモート タスクの状態] を開き、タスクの状態を確認します。
4. [保護] の [概要] と [すべてのマルウェア] ページを使用して、検出されたマルウェアの種類を判定します。クライアントから情報を表示するためにしばらく時間がかかる場合があります。

結果 : この練習により、Intune の Endpoint Protection を構成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。

質問 : この演習で、検出されたマルウェアの種類は何ですか。自動的に解決されましたか。

質問 : 演習で、あなたは自動承認規則を構成し、すべての既存の更新プログラムが自動的に承認されず、展開されないことに気づきました。この場合、何をする必要がありますか。

復習とまとめ

復習問題

質問 : Intune を使用して、Microsoft 以外の更新プログラムを展開する必要があります。Microsoft 以外の更新プログラムの展開を成功させるための 2 つの主要な考慮事項は何ですか。

質問 : 新しい種類のマルウェアが検出されるたびに、必ずあなたに通知されるようにする必要があります。この場合、何をする必要がありますか。