【 Defender for Endpoint 】オンボーディング手順

2026年05月29日

改訂履歴

版数	発行日	改訂内容
第1版	2026年05月29日	初版発行

本資料の内容は 2026/05/29 時点のものです。製品のアップデートにより変更となる場合がございます旨ご了承ください。

Agenda

1. 前提情報
   1. 本書の目的
   2. 用語集

2. 背景
   1. 複数のオンボーディング方式が求められる背景

3. オンボーディング方式について
   1. 3種類のオンボーディング方式の概要
   2. 方式①：Microsoft Intune（MDM）
   3. 方式②：グループポリシー（GPO）
   4. 方式③：ローカルスクリプト（手動）
   5. 各オンボーディング方式の比較表

4. オンボーディング方式の組み合わせや変更
   1. オンボーディング方式の組み合わせ
   2. オンボーディング方式の変更

5. 各オンボーディング方式の実装手順
   1. 方式①：Microsoft Intune（MDM）
   2. 方式②：グループポリシー（GPO）
   3. 方式③：ローカルスクリプト（手動）

1. 前提情報

1.1. 本書の目的

目的

本資料は、Defender for Endpoint のオンボードについて、お客様自身が環境に適したオンボーディング方式を選択し、運用できるようにすることを目的としています。そのために必要な関連情報や知識を整理しています。

1.2. 用語集

本書で使用する用語及び略称を以下の通り定義します。

No.	用語	説明
1	オンプレミス	自社内のサーバーやネットワークなど、社内環境に設置・運用される IT 基盤。
2	クラウド	インターネット経由で提供されるサービスや基盤を利用し、社内に設備を持たずに IT 環境を構築する形態。
3	OS（Operating System）	PC やデバイスの基本動作を制御し、アプリケーションを動作させるための基盤となるソフトウェア。
4	ハイブリッドワーク	オフィス勤務とリモート勤務を組み合わせた働き方。
5	オンボード／オンボーディング	オンボード：デバイスをサービスに登録する行為。 オンボーディング：準備から完了までの一連の流れ。
6	Microsoft Intune	クラウドベースでデバイスやアプリを管理する Microsoft のエンドポイント（利用者側の端末）管理サービス。
7	MDM（Mobile Device Management）	デバイスを登録・管理し、セキュリティ設定やポリシーを配布するための仕組み。
8	グループポリシー（GPO）	Active Directory 環境で、ユーザーやデバイスに対する設定を一元的に配布・管理する仕組み。
9	ローカルスクリプト	管理者が端末上で直接実行するスクリプトによって設定や処理を行う方法。
10	Microsoft Defender for Endpoint	エンドポイント（利用者側の端末）の脅威検知・可視化・対応を行う Microsoft のセキュリティサービス。

1.2. 用語集

本書で使用する用語及び略称を以下の通り定義します。

No.	用語	説明
11	Active Directory（AD）	ユーザー、デバイス、権限、ポリシーを一元管理する Microsoft のディレクトリサービス。
12	VPN（Virtual Private Network）	社外から安全に社内ネットワークへ接続するための仮想的な専用通信経路。
13	ゼロタッチ展開	ユーザー操作を必要とせず、初期設定や構成を自動的に適用する展開方式。
14	スケーラビリティ	利用規模の増減に応じて柔軟に拡張・縮小できる特性。
15	BYOD（Bring Your Own Device）	社員が個人で所有しているパソコンやスマートフォンを、業務にも利用する運用形態。
16	クラウドファースト	システム導入や設計において、クラウド利用を優先的に検討する考え方。
17	PoC（概念実証）	本格導入前に、小規模で技術的・運用的な有効性を検証する取り組み。
18	GUI（Graphical User Interface）	画面操作を中心に設定や管理を行うための視覚的な操作インターフェース。
19	PowerShell	Windows 環境で管理や自動化を行うためのコマンドラインおよびスクリプト環境。
20	ポリシー	セキュリティや運用ルールを定義し、デバイスやユーザーに適用する設定の集合。

1.2. 用語集

本書で使用する用語及び略称を以下の通り定義します。

No.	用語	説明
21	ウイルス対策	マルウェアや不正プログラムの検出・防御を行うセキュリティ機能。
22	スクリーンセーバー	一定時間操作がない場合に画面を保護・制御するための機能。
23	自動是正	検知された問題に対して、人手を介さず自動的に修復や対応を行う仕組み。
24	チェックイン	各端末が Microsoft Intune に定期的に接続し、当該端末自身の状態を報告するとともに、割り当てられたポリシーを取得・適用する処理。
25	オンボード用パッケージ	デバイスを Defender for Endpoint に登録するために必要な設定情報をまとめたファイル。
26	グループポリシー管理コンソール（GPMC）	グループポリシーの作成・編集・適用を管理するための管理ツール。
27	OU（Organizational Unit）	Active Directory 内でユーザーやデバイスを論理的に分類・管理する単位。
28	セキュリティ管理者	セキュリティ関連の設定や運用を担当する管理者ロール。
29	グローバル管理者	テナント全体に対するすべての管理操作が可能な最上位の管理者ロール。
30	ドメイン管理者	Active Directory ドメインの管理を行う高権限の管理者。

1.2. 用語集

本書で使用する用語及び略称を以下の通り定義します。

No.	用語	説明
31	Intune 管理センター	Microsoft Intune の設定・管理を Web 画面から行うための管理ポータル。
32	Defender 管理センター	組織内のパソコンや端末のセキュリティ状態をまとめて確認・管理するための Web 画面。
33	Endpoint Security Manager	Intune においてエンドポイントセキュリティ関連のポリシー管理を行うための管理者ロール。

2. 背景

2.1. 複数のオンボーディング方式が求められる背景

企業の IT 環境や運用前提は一様ではなく、管理対象となる OS・デバイス構成や働き方、端末の利用形態は組織ごとに大きく異なります。また、既存環境や運用を考慮すると、全端末を同時に切り替えるのではなく、段階的な導入・移行を前提とした対応が求められる場面も多く見られます。そのため、Microsoft 社では複数のオンボーディング方式を提供しています。

企業ごとに IT 環境の成熟度・前提が異なる

企業によって、オンプレミス中心の環境を長年運用しているケースもあれば、クラウドを前提とした新しい IT 基盤を採用しているケースもあります。

管理対象の OS・デバイスが混在している

企業内では Windows 端末に加えて、macOS、モバイルデバイスなど、複数の OS やデバイスが併存しています。

働き方・端末の利用形態が多様化している

テレワークやハイブリッドワークの普及により、端末の利用場所は社内だけでなく、自宅や外部ネットワークに広がっています。また、会社支給端末だけでなく、利用形態や接続方式も多様化しています。

段階的な導入・移行が求められる

既存端末の稼働状況や更新サイクル、業務影響を考慮すると、全端末を同時に新しい管理方式へ切り替えることは難しく、一定期間、段階的な導入・移行を前提とした運用が求められます。

これらの様々な環境に応じたオンボーディングができるように、Microsoft では複数のオンボーディング方式を提供しています。

3. オンボーディング方式について

3.1. 3種類のオンボーディング方式の概要

オンボーディング方式が複数あることを前述しましたが、本資料では、Microsoft Intune（MDM）・グループポリシー（GPO）・ローカルスクリプト（手動）の3種類について紹介します。オンボーディング方式の違いを正しく理解することは、現在の管理環境に適した方式を選択し、安定したセキュリティ運用を設計するうえで非常に重要です。

Microsoft Intune（MDM）

Intune で管理されている端末を、ポリシー配布によって自動的に Defender for Endpoint に登録する方法

必要条件
- ✓ Microsoft Defender for Endpoint が含まれるライセンス
- ✓ Microsoft Intune が含まれるライセンス
- ✓ 対象デバイスが Intune（MDM）に登録済みであること
- ✓ 対象デバイスがインターネットに接続できること

グループポリシー（GPO）

Active Directory 環境で、グループポリシー（GPO）を使って Windows 端末を Defender for Endpoint に登録する方法

必要条件
- ✓ Microsoft Defender for Endpoint が含まれるライセンス
- ✓ 対象デバイスがサポート OS であること（Windows 10/Windows 11）
- ✓ Active Directory（AD）に参加している Windows デバイスであること
- ✓ 対象デバイスがインターネットに接続できること

ローカルスクリプト（手動）

Defender 管理センターから取得したオンボーディング用スクリプトを、 各端末で手動実行して Defender for Endpoint に登録する方法

必要条件
- ✓ Microsoft Defender for Endpoint が含まれるライセンス
- ✓ 対象デバイスがサポートOSであること（Windows 10/Windows 11）
- ✓ 対象デバイスに管理者権限でサインインできること
- ✓ 対象デバイスがインターネットに接続できること

次のページより、各オンボード方式について詳しく説明します。

3.2. 方式①：Microsoft Intune（MDM）

Microsoft Intune（MDM）経由のオンボーディングとは、Intune で管理しているデバイスを、管理者の設定だけで自動的に Defender for Endpoint に登録する方式です。各端末で直接操作する必要がなく、在宅や社外のデバイスでも同じポリシーを一括で適用できることや、macOS やモバイル端末にも対応していることから、現在の主流かつ Microsoft に推奨されるケースが多い方式です。

メリット

- **リモート端末も管理できる**
  ネットワークの通信要件が整っていれば、VPN がない環境でも対応できる
- **ゼロタッチ展開ができる**
  管理者は Intune 上で設定するだけで、端末側でオンボード作業は発生しない
- **多様な端末を一元管理できる**
  Windows に加え、macOS やモバイル端末にも対応しているため、マルチプラットフォーム環境でも一元的に管理可能
- **自動化・スケーラビリティが高い**
  デバイスやユーザー数が増加しても、管理や運用の負荷が大きく増えない

注意点

- **グループポリシー（GPO）と同一端末での二重管理は不可**
  Intune と GPO の併用は可能であるが、同じポリシー設定はできない
- **ポリシー反映は即時ではない**
  Intune の設定は、端末が再起動などをしたタイミングで反映されるため、管理者が設定を保存しても、すべての端末に同時・即座に反映されるわけではない

ユースケース

- ✓ 端末管理やセキュリティを新規に導入する組織や、従来の GPO 管理からクラウド管理へ段階的に移行している組織
- ✓ テレワークや BYOD といった、利用場所や端末が固定されない環境
- ✓ クラウドサービスの活用を前提とするクラウドファーストな企業

3.3. 方式②：グループポリシー（GPO）

グループポリシー（GPO）によるオンボーディングとは、Active Directory（AD）で管理されている Windows 端末に対して、グループポリシーを使って Microsoft Defender for Endpoint に登録する方式です。既存のオンプレミス環境や GPO 管理をそのまま活かせるため、Intune を導入していない組織や、従来型の Windows 管理を続けている環境に適しています。

メリット

- **既存 AD / GPO 資産をそのまま活用できる**
  既に構築・運用されている Active Directory やグループポリシーの仕組みを変更することなく活用できる
- **閉域網・制限ネットワークでも使いやすい**
  オンプレミスの AD 環境を前提とするため、インターネット通信が制限された閉域網やセキュリティ要件の厳しいネットワーク環境でも利用できる
- **オンプレミス前提の自動化された展開方式**
  ポリシーが適用されている場合、端末側でのオンボード作業は発生しない

注意点

- **クラウド管理には不向き**
  オンプレミスの Active Directory（AD）と社内ネットワークを前提とした管理方式であるため、クラウド管理には適していない
- **リモート端末では反映が遅れる場合がある**
  社外利用の端末は Active Directory に接続できるタイミングが限られるため、GPO の適用が遅れる

ユースケース

- ✓ オンプレミスの Active Directory（AD）を中心に端末管理を行っている環境
- ✓ 端末の利用が主に社内ネットワーク内に限定されている環境

3.4. 方式③：ローカルスクリプト（手動）

ローカルスクリプト（手動）によるオンボーディングとは、管理者が各端末でオンボーディング用スクリプトを直接実行し、Defender for Endpoint に登録する方式です。Intune や GPO といった一斉展開の管理基盤を使用しないため、少数端末の検証や一時的な利用に向いています。

メリット

- **端末だけでオンボードを行うことができる**
  対象端末上でオンボーディング用スクリプトを実行するだけで Defender for Endpoint に登録することができる
- **導入までが最短**
  オンボーディング用スクリプトを取得して実行するだけで完了するため、準備や設計に時間をかけず、最短で Defender for Endpoint を有効化できる
- **既存環境への影響が少ない**
  既存の GPO 設定や Intune 構成を変更する必要がなく、他の端末や管理ポリシーに影響を与えない

注意点

- ◆ **大量端末への展開は現実的ではない**
  管理者が各端末でオンボーディング用スクリプトを手動実行する必要があるため、作業工数がかかる

- ◆ **自動化/一元管理ができない**
  Intune や GPO のような「中央から設定を配布・是正する管理基盤」がないため、ポリシーを一斉に全デバイスへ適用・変更することはできない

ユースケース

- ✓ PoC（概念実証）の場合
- ✓ 一時的なトラブル調査や特定端末のみの確認をしたい場合

3.5. 各オンボーディング方式の比較表

Microsoft Intune（MDM）、グループポリシー（GPO）、ローカルスクリプト（手動）のそれぞれのオンボーディング方式の特徴を表で比較します。以下の比較表より、自身の環境にあったオンボーディング方式を選択するために、どのようなケースに適しているかを確認します。

項目	Microsoft Intune（MDM）	グループポリシー（GPO）	ローカルスクリプト（手動）
管理場所	Intune	Active Directory	各端末ローカル
対象OS	Windows / macOS など	Windows のみ	Windows のみ
規模	小～大規模	中規模	極めて小規模
ユーザー操作	ポリシーが反映 されていた場合不要	ポリシーが適用 されている場合不要	必要（管理者が実行）
設計・運用視点	・設計がシンプル ・自動化/標準化しやすい	・既存 AD の活用可能 ・リモート端末に弱い	・動作検証が可能 ・運用不可 ・属人化/統制不可
実装・作業視点	・GUI 中心 ・一度設定すれば放置 ・反映にタイムラグあり	・オンプレ環境だけで完結 ・反映タイミングがわかりにくい	・PowerShell 実行だけ ・1台ずつ手作業が必要
ユースケース	・新規導入 ・テレワーク中心 ・クラウドファースト	・既存 AD 環境 ・社内ネットワークが中心	・ PoC /評価目的 ・数台だけ今すぐ試したい

4. オンボーディング方式の組み合わせや変更

4.1. オンボーディング方式の組み合わせ

Microsoft Defender for Endpoint のオンボーディングは、Intune、GPO、ローカルスクリプトを組み合わせての利用や、運用途中で別の方式へ変更したりすることが可能です。これは、企業の管理環境や移行状況に合わせて段階的に導入・移行できるように設計されているためです。ただし、同一デバイスに対して同じポリシーを複数の方式で同時に管理しないよう、役割分担を明確にすることが重要です。

組み合わせ

オンボーディング方式の組み合わせは可能ですが、同一端末に対して同じポリシー設定を複数方式で同時に有効化することはできません。※設定自体は複数方式で行える場合がありますが、実際に適用・有効となるポリシーはどちらか一方のみとなります。

OKパターン

Intune

Defender 管理
ウイルス対策：有効

✓

GPO

Windows 固有の設定
スクリーンセーバー等

Intune と GPO の2つで管理しているが、
設定内容は**役割分担**をして管理している

NGパターン

Intune

Defender 管理
ウイルス対策：有効

✕

GPO

Defender 管理
ウイルス対策：有効

Intune と GPO の双方から
「Defender ウイルス対策を有効にする」という同一ポリシーが
配布されるため、**二重適用**されてしまっている

4.2. オンボーディング方式の変更

前述したように、オンボーディング方式の変更は可能です。
以下では、オンボーディング方式の変更パターン例を、変更する背景、変更内容、影響・効果という項目で説明します。

変更パターン①：GPO 方式から Intune 方式

背景

・テレワークが増え、社内ネットワークや VPN 前提の運用が難しくなった
・Windows 以外に macOS や iOS／Android も管理対象に含めたい

変更内容

・GPO で行っていた Defender for Endpoint やセキュリティ設定を Intune に移行
・既存の Windows 設定は GPO で維持しつつ、今後のデバイス管理やセキュリティ管理は Intune を中心に行う

影響・効果

✓社外・在宅端末でも自動オンボードと自動是正が可能
✓OS 混在環境でも同じ管理モデルで運用できるようになる

変更パターン②：ローカルスクリプト方式から GPO / Intune 方式

背景

・まずは 1 台だけで Defender for Endpoint の動作確認を行いたい
・管理基盤を構築する前に PoC（概念実証）を実施したい

変更内容

・初期検証はローカルスクリプトで手動オンボード
・本番展開時に GPO または Intune に切り替え、一斉展開を行う

影響・効果

✓ 手動運用から自動化された管理に移行できる
✓ 設定の一括反映や自動是正が可能になり、継続運用が安定する

5. 各オンボーディング方式の実装手順

5.1. 方式①：Microsoft Intune（MDM）

Microsoft Intune 経由でのオンボーディングは以下の流れで行います。
各詳細な手順につきましては、次のページより説明します。

0 **前提条件・事前準備**
Intune 経由でオンボードを始める準備をします

1 **Microsoft Defender 管理センターで Intune 接続を有効化**
Intune にてオンボードしたデバイスを、Defender 管理センターで管理するための設定を行います

2 **Intune でユーザーグループを作成**
オンボード対象となるユーザー（当該ユーザーがサインインしている Intune 登録済みデバイス）を1つのグループにまとめます

3 **Microsoft Defender for Endpoint の機能を設定するポリシーの作成＆割り当て**
対象のユーザーグループに割り当てるポリシーを作成し、割り当てます

4 **各端末による Intune への自動チェックイン後、Defender 管理センターにてオンボード完了を確認**
各端末にてチェックイン完了後、Defender 管理センターでオンボード状況を確認します

5.1. 方式①：Microsoft Intune（MDM）

0 前提条件・事前準備

Intune 経由でのオンボーディングを行うためには、以下の準備が必要となります。

前提条件

- ✓ **Microsoft Defender for Endpoint** が含まれるライセンスを所持していること
  - Microsoft 365 E5
  - Microsoft 365 E3
  - Microsoft 365 Business Premium
  - Defender for Endpoint 単体ライセンス
- ✓ **Microsoft Intune** が含まれるライセンスを所持していること
  - Microsoft 365 E5
  - Microsoft 365 E3
  - Microsoft 365 Business Premium
  - Intune 単体ライセンス
- ✓ 対象デバイスが Intune（MDM）に登録済みであること
- ✓ 対象デバイスがインターネットに接続できること

事前準備

- ☐ Intune 管理センターにアクセスできる権限付与
  - Intune 管理者
  - Endpoint Security Manager
- ☐ Defender 管理センターにアクセスできる権限付与
  - セキュリティ管理者
  - グローバル管理者

5.1. 方式①：Microsoft Intune（MDM）

1 Microsoft Defender 管理センターで Intune 接続を有効化

まず、Defender 管理センターにて Intune との接続を有効化します。有効化設定が完了後、Intune 管理センターにて接続状況を確認します。

有効化手順

1. Defender 管理センターにサインイン
2. [設定]> [エンドポイント]
3. [全般]> [高度な機能]より、[Microsoft Intune 接続]をオン
4. [ユーザー設定の保存]をクリック

有効化完了後

1. Intune 管理センターにサインイン
2. [エンドポイントセキュリティ]> [セットアップ]
3. [Microsoft Defender for Endpoint]
4. 接続の状態より、[有効]になっていることを確認

※更新には最大 15 分かかる場合があります。

[有効]になっていた場合、Defender for Endpoint と Intune の接続は完了となります。

5.1. 方式①：Microsoft Intune（MDM）

2 Intune でユーザーグループを作成

オンボード対象となるユーザーをまとめるために、Intune 管理センターでユーザーグループを作成します。このユーザーグループにオンボード用ポリシーを割り当てることで、当該ユーザーがサインインしている **Intune 登録済みデバイス**に対して、Defender for Endpoint のオンボードが実行されます。

グループ作成・追加手順

1. Intune 管理センターにサインイン
2. [グループ]> [新しいグループ]をクリック
3. 詳細を入力し、作成
4. [グループ]> [すべてのグループ]をクリック
5. 先ほど作成したグループを開く
6. [メンバー]より[メンバーの追加]をクリック
7. ユーザーを選択

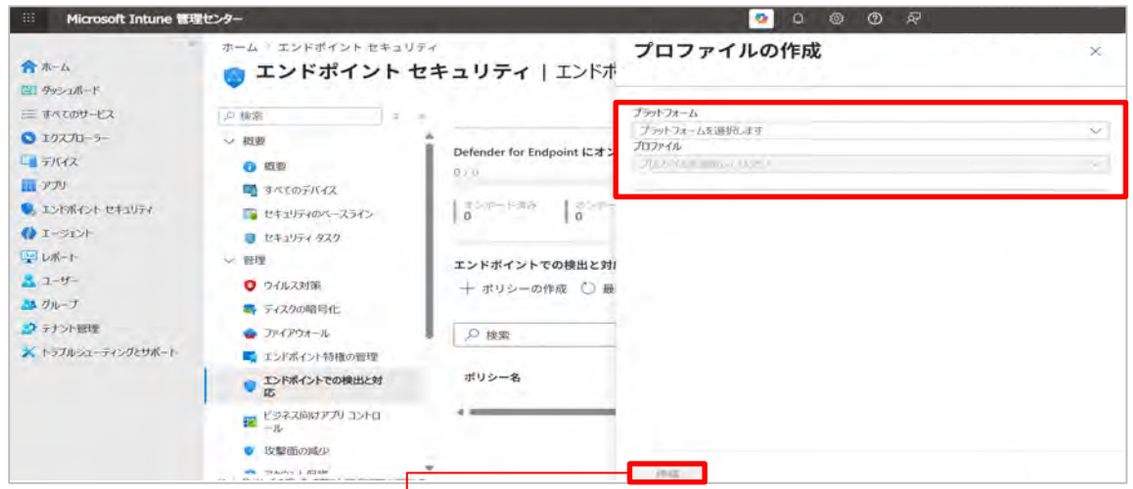
5.1. 方式①：Microsoft Intune（MDM）

3 Microsoft Defender for Endpoint の機能を設定するポリシーの作成＆割り当て

Defender for Endpoint にオンボードするために、対象のグループに適用するポリシーを Intune にて作成します。
具体的には、[エンドポイントセキュリティでの検出と対応]にて、Defender for Endpoint にオンボードされるグループを選択する構成ポリシーを作成します。

ポリシーの作成/割り当て手順

1. Intune 管理センターにサインイン
2. [エンドポイントセキュリティ]> [エンドポイントでの検出と対応]をクリック
3. [ポリシーの作成]を選択
4. [プラットフォーム]にて該当するものを選択
5. [プロファイル]にて[エンドポイントの検出と応答]を選択
6. [作成]をクリック
7. [Basic]にて、[名前]と[説明]を入力



5.1. 方式①：Microsoft Intune（MDM）

3 Microsoft Defender for Endpoint の機能を設定するポリシーの作成＆割り当て

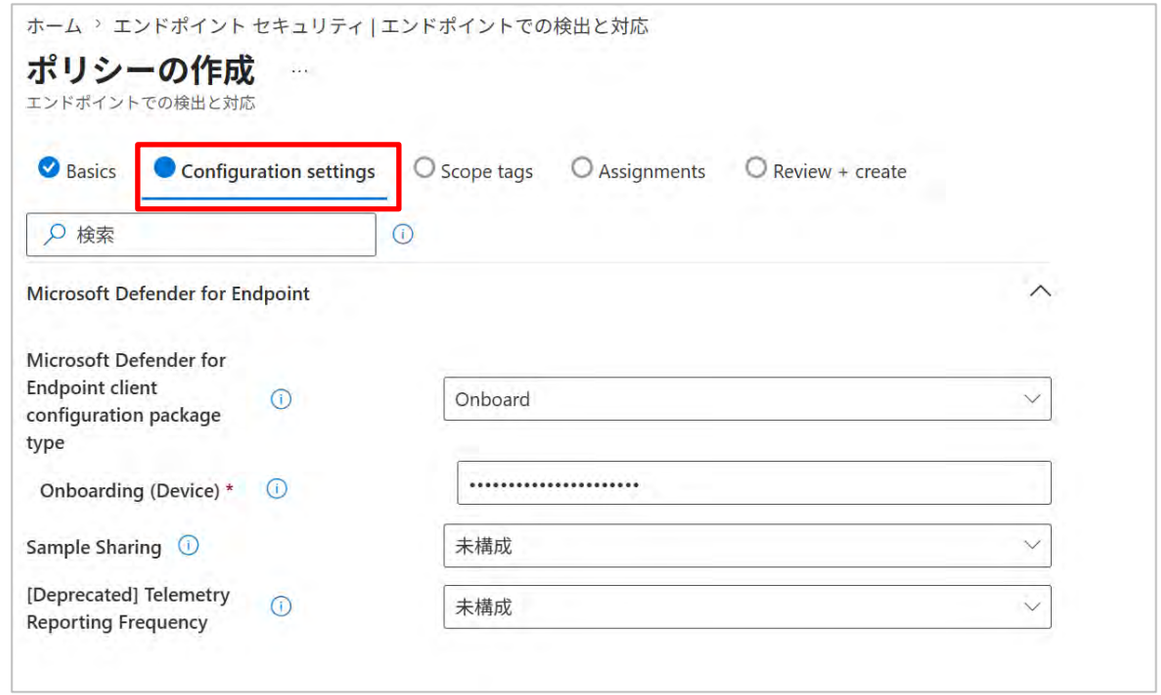
ポリシーの作成/割り当て手順

8. [Configuration settings]の[Microsoft Defender for Endpoint client configuration package type]にて[Onboard]を選択
   ※Onboarding(Device)は既定で入力されています。

9. [Sample Sharing] にてプルダウンより選択
   ※Defender が検出した疑わしいファイルなどのサンプルを、Microsoft に送信するかどうかを制御する設定。

10. [Deprecated]Telemetry Reporting Frequencyにてプルダウンより選択
    ※Defender が Microsoft に送信する動作情報（テレメトリ）の頻度を指定する設定。

9,10 の設定において、[未構成]にすることはオンボードには影響ございません。
※この設定は、ポリシー作成後にも編集が可能となっています。



5.1. 方式①：Microsoft Intune（MDM）

3 Microsoft Defender for Endpoint の機能を設定するポリシーの作成＆割り当て

ポリシーの作成/割り当て手順

11. [Scop tags]でスコープタグを選択

12. [Assignments]にて作成したグループを検索し、クリック

13. [次へ]進み、[Review + create]にてこれまでの設定を確認

14. 問題ない場合、作成

15. [エンドポイントでの検出と対応]にて、作成したポリシー、また、割り当て状況を確認することができます

ここまでで、構成ポリシーの作成と対象グループへの割り当てが完了です。

詳細な手順については、こちらもご確認ください。

5.1. 方式①：Microsoft Intune（MDM）

4 各端末による Intune への自動チェックイン後、Defender 管理センターにてオンボード完了を確認

Intune のポリシーを用いた Defender for Endpoint へのオンボード設定は完了していますが、各端末にて自動的に Intune にチェックインされることで、オンボードが完了します。各端末のオンボード状況は、Defender 管理センターにて確認します。

各端末による Intune へのチェックイン
以下のような場合にチェックインが行われます。

- 端末の起動後
- ユーザーのサインイン後
- 一定時間ごとの定期通信など

オンボード状況の確認手順
オンボードが完了したデバイスは、Defender 管理センターにて確認できます。なお、オンボードが完了していないデバイスは表示されません。

1. Defender 管理センターにサインイン
2. [アセット]> [デバイス]

※反映には時間がかかる場合があります。

5.2. 方式②：グループポリシー（GPO）

グループポリシー（GPO）でのオンボーディングは以下の流れで行います。
各詳細な手順につきましては、次のページより説明します。

0 **前提条件・事前準備**
グループポリシー（GPO）でオンボードを始める準備をします

1 **Defender 管理センターからグループポリシー用オンボードパッケージを取得**
Defender for Endpoint にデバイスを登録するための構成情報（オンボード用パッケージ）を取得します

2 **グループポリシー管理コンソール（GPMC）で GPO を作成**
オンボード設定を適用するための GPO を作成し、対象となるデバイスを指定します

3 **作成した GPO をオンボード対象 OU にリンクする**
作成した GPO をオンボード対象の OU に関連付け、デバイスがポリシーを受け取れる状態にします

4 **各端末による Active Directory への自動チェックイン後、Defender 管理センターにてオンボード完了を確認**
各端末が Active Directory に接続することで自動的にチェックインが行われ、オンボード処理が実行されます

5.2. 方式②：グループポリシー（GPO）

0 前提条件・事前準備

グループポリシー（GPO）でのオンボーディングを行うためには、以下の準備が必要となります。

前提条件

- ✓ **Microsoft Defender for Endpoint** が含まれるライセンスを所持していること
  - Microsoft 365 E5
  - Microsoft 365 E3
  - Microsoft 365 Business Premium
  - Defender for Endpoint 単体ライセンス
- ✓ 対象デバイスがサポート OS であること
  - Windows 10
  - Windows 11
- ✓ Active Directory（AD）に参加している Windows デバイスであること
- ✓ 対象デバイスがインターネットに接続できること

事前準備

- ☐ Defender 管理センターにアクセスできる権限の付与
  - セキュリティ管理者
  - グローバル管理者
- ☐ GPO を管理できる権限の付与
  - ドメイン管理者、または委任された権限
- ☐ オンボード対象デバイスがどの OU に所属しているかの確認/整理

5.2. 方式②：グループポリシー（GPO）

1 Defender 管理センターから GPO 用オンボードパッケージを取得

まず、Defender 管理センターにて、グループポリシー（GPO）用のオンボードパッケージを取得します。

<u>オンボードパッケージ取得手順</u>

1. Defender 管理センターにサインイン
2. [設定]> [エンドポイント]
3. [デバイス管理]> [オンボーディング]
4. デバイスの種類で[Windows 10と 11]を選択
5. [接続の方法]にてプルダウンより選択
   ※既定で[合理化]となっています

6. [展開方法]にて[グループポリシー]を選択
7. [オンボードパッケージのダウンロード]にて.zip ファイルを保存
8. デバイスからアクセスできる共有の読み取り専用の場所に、.zip ファイルの内容を抽出
   ※OptionalParamsPolicy という名前のフォルダーとファイル WindowsDefenderATPOnboardingScript.cmdが必要

5.2. 方式②：グループポリシー（GPO）

2 グループポリシー管理コンソール（GPMC）で GPO を作成

グループポリシー管理コンソール（GPMC）で GPO を作成します。
ここでは、Defender for Endpoint をオンボードするための設定を定義するために、グループポリシーオブジェクトを新規に作成します。

※こちらの手順より、PC での設定になるためキャプチャが提供できかねますこと、何卒ご理解いただきますようお願いします。

グループポリシーの作成手順

1. グループポリシー管理コンソール（GPMC）を起動
2. 構成するグループポリシーオブジェクトを右クリックし、[新規作成]を選択
3. 新しいグループポリシーの名前を入力し、[OK]をクリック
4. 作成したグループポリシーオブジェクト (GPO)を右クリックして [編集] をクリック
5. [グループ ポリシー管理エディター]にて[コンピューターの構成]へ移動
6. [ユーザーの設定]>[コントロール パネルの設定]>[タスク] をクリック
7. [スケジュールされたタスク] を右クリックし、[新規作成]より[即時タスク（Windows Server 7 以降）]をクリック

5.2. 方式②：グループポリシー（GPO）

2 グループポリシー管理コンソール（GPMC）で GPO を作成

グループポリシーの作成手順

8. [タスク]ウィンドウが開いたら、 [セキュリティ オプション] の [全般] タブに移動し、以下を設定
    - 名前：任意のタスク名
    - セキュリティ オプション
        - [タスクの実行時に使うユーザーアカウント]：[ユーザーまたはグループの変更] を選択し、「SYSTEM」と入力し、[名前の確認] を選択し、[OK] 。NT AUTHORITY¥SYSTEM は、タスクを実行するユーザーアカウントとして表示される。
        - [ユーザーがログオンしているかどうかにかかわらず実行する]：有効
        - [最高の特権を持つ実行] ：チェック
9. [アクション]タブに移動し、[新規]を選択
10. [プログラムの開始]が選択されていることを確認
11. 設定の[プログラム]にて[WindowsDefenderATPOnboardingScript.cmd]のファイルサーバーの完全修飾ドメイン名 (FQDN) を使用して、UNC パスを入力
12. [OK]を選択し、開いているグループポリシー管理コンソール（GPMC）を閉じる

詳細な手順については、こちらもご確認ください。

5.2. 方式②：グループポリシー（GPO）

3 作成した GPO をオンボード対象 OU にリンクする

「2.グループポリシー管理コンソール（GPMC）で GPO を作成」で作成したグループポリシーを対象の OU にリンクします。

対象 OU へのリンク手順

1. グループポリシー管理コンソール（GPMC）を開く
2. 作成した GPO の適用対象である OU を右クリック
3. 既存の GPO のリンクをクリック
4. 表示されるダイアログボックスで、該当のグループポリシーオブジェクトを選択し、[OK]をクリック

5.2. 方式②：グループポリシー（GPO）

4 各端末による Active Directory への自動チェックイン後、Defender 管理センターにてオンボード完了を確認

各端末が Active Directory に接続したタイミングでグループポリシー（GPO）が自動的に適用され、対象 OU 内のデバイスが Microsoft Defender for Endpoint にオンボードされます。各端末のオンボード状況は、Defender 管理センターにて確認します。

各端末による Active Directory へのチェックイン
以下のような場合にチェックインが行われます。

- 端末の起動後
- ユーザーのサインイン時
- 社内ネットワークや VPN に接続したとき
- 定期的なバックグラウンド更新など

オンボード状況の確認手順
オンボードが完了したデバイスは、Defender 管理センターにて確認できます。なお、オンボードが完了していないデバイスは表示されません。

1. Defender 管理センターにサインイン
2. [アセット]> [デバイス]

※反映には時間がかかる場合があります。

5.3. 方式③：ローカルスクリプト（手動）

ローカルスクリプト（手動）でのオンボーディングは以下の流れで行います。
各詳細な手順につきましては、次のページより説明します。

0 **前提条件・事前準備**
ローカルスクリプト（手動）でオンボードを始める準備をします

1 **Defender 管理センターからローカルスクリプト用のオンボードパッケージを取得**
Defender for Endpoint にデバイスを登録するための構成情報（オンボード用スクリプト）を取得

2 **zip ファイルの中身を確認し、端末でスクリプトを管理者として実行**
取得したオンボード用スクリプトを対象端末で手動実行し、オンボード処理を開始します

3 **Defender 管理センターにてオンボード完了を確認**
オンボード処理が正常に完了したことを管理センター上で確認します

5.3. 方式③：ローカルスクリプト（手動）

0 前提条件・事前準備

ローカルスクリプト（手動）でオンボードを行う際の前提条件と事前準備について説明します。

前提条件

- ✓ **Microsoft Defender for Endpoint** が含まれるライセンスを所持していること
  - Microsoft 365 E5
  - Microsoft 365 E3
  - Microsoft 365 Business Premium
  - Defender for Endpoint 単体ライセンス
- ✓ 対象デバイスがサポートOSであること
  - Windows 10
  - Windows 11
- ✓ 対象デバイスに管理者権限でサインインできること
- ✓ 対象デバイスがインターネットに接続できること

事前準備

- ☐ Defender 管理センターにアクセスできる権限付与
  - セキュリティ管理者
  - グローバル管理者
- ☐ オンボード対象のデバイスの決定

5.3. 方式③：ローカルスクリプト（手動）

1 Defender 管理センターから ローカルスクリプト用のオンボードパッケージを取得

まず、Defender 管理センターにて、ローカルスクリプト用のオンボードパッケージを取得します。

<u>オンボードパッケージ取得手順</u>

1. Defender 管理センターにサインイン
2. [設定]> [エンドポイント]
3. [デバイス管理]> [オンボーディング]
4. デバイスの種類で[Windows 10と 11]を選択
5. [接続の方法]にて選択
   ※既定で[合理化]となっています
6. [展開方法]にて[ローカルスクリプト（最大10台のデバイス用）]を選択
7. [オンボードパッケージのダウンロード]を選択し、WindowsDefenderATPOnboardingPackage.zip ファイルをダウンロード
8. デバイス上の .zip ファイルの内容を、見つけやすい場所 (デスクトップなど) に抽出　※.zip ファイルには、WindowsDefenderATPLocalOnboardingScript.cmdという名前の1つのファイルが含まれている

5.3. 方式③：ローカルスクリプト（手動）

2 zip ファイルの中身を確認し、端末でスクリプトを管理者として実行

コマンドの実施手順

1. デバイスで、[管理者として実行]で次のコマンドを実行
2. 抽出したWindowsDefenderATPLocalOnboardingScript.cmd ファイルを保存したフォルダーに移動
   a. Desktop フォルダーに移動するには、次のコマンドを実行
      if exist "%OneDrive%¥Desktop" (cd /d "%OneDrive%¥Desktop") else if exist "%USERPROFILE%¥Desktop" cd /d "%USERPROFILE%¥Desktop"
   b. WindowsDefenderATPLocalOnboardingScript.cmd スクリプトを実行
      WindowsDefenderATPLocalOnboardingScript.cmd
3. スクリプトが完了後、[任意のキーを押して続行します...] と表示される
4. 任意のキーを押し、デバイスの手順を完了

詳細な手順については、こちらもご確認ください。

5.3. 方式③：ローカルスクリプト（手動）

3 Defender 管理センターにてオンボード完了を確認

「2. zip ファイルの中身を確認し、端末でスクリプトを管理者として実行」にてオンボードは完了していますが、Defender 管理センターでの反映には時間がかかる場合があります。各端末のオンボード状況は、Defender 管理センターにて確認します。

<u>オンボード状況の確認手順</u>
オンボードが完了したデバイスは、Defender 管理センターにて確認できます。なお、オンボードが完了していないデバイスは表示されません。

1. Defender 管理センターにサインイン
2. [アセット]> [デバイス]