Microsoft Defender for Endpoint

IP アドレス除外手順書

Version 1.0

April, 2026

Panasonic Corporation

目次

1 はじめに

1.1　本書の背景

Microsoft Defender for Endpoint（企業向け Microsoft Defender。以降 MDE と記載）が導入された PC 環境で Media Production Suite ソフトウェア（以降 MPS と記載）を使用した場合、MDE による通信遮断が発生して、MPS の動作が不正規になる問題が発生します。

具体的には、MPS 上で以下のような症状が発生します。

1. MPS の画面が更新されなくなる
2. MPS でカメラ操作が効かなくなる
3. オートトラッキング、オートフレーミングの動作が止まる
   タイミングによってカメラのパン・チルト・ズームが一方向に動き続ける

1〜2 分程度で再び使用できる　→　数分後に再び不正規になる、を繰り返す

上記問題が発生した場合、企業の情報システム管理者の MDE 管理コンソールでカメラの IP アドレスを除外登録する必要があります。

MDE が有効になっているか、Windows サービスの Sense が実行中であることによって判別できます。

Powershell コマンドでの確認例

```
PS> Get-Service Sense

Status     Name               DisplayName
------     ----               -----------
Running    Sense              Sense
```

1.2　本書の目的

本書は、企業の情報システム管理者向けに、MDE 管理コンソールでカメラの IP アドレスを除外登録するための手順を示すものです。

2　IP アドレスの除外登録手順

2.1　重要事項（デバイス管理形態の確認）

デバイスの管理形態（Microsoft Defender for Endpoint 管理端末、Intune 管理端末）により、IP アドレス除外の設定方法が異なります。

・Microsoft Defender for Endpoint 管理端末の場合

以下リンク先を参照して除外設定を行ってください。

2.2　グループ ポリシーでカメラの IP アドレス除外を行う方法

・Intune 管理端末の場合

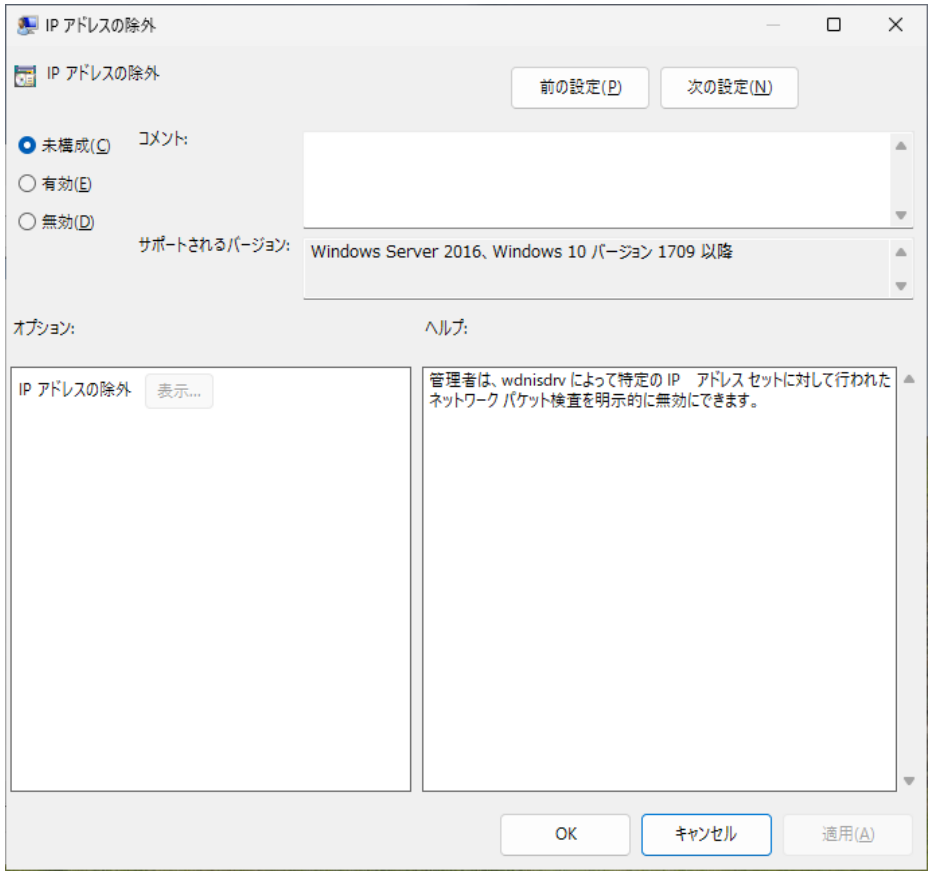
以下リンク先を参照して除外設定を行ってください。

2.3　Intune から IP アドレスの除外を行う方法

2.2　グループ ポリシーでカメラの IP アドレス除外を行う方法

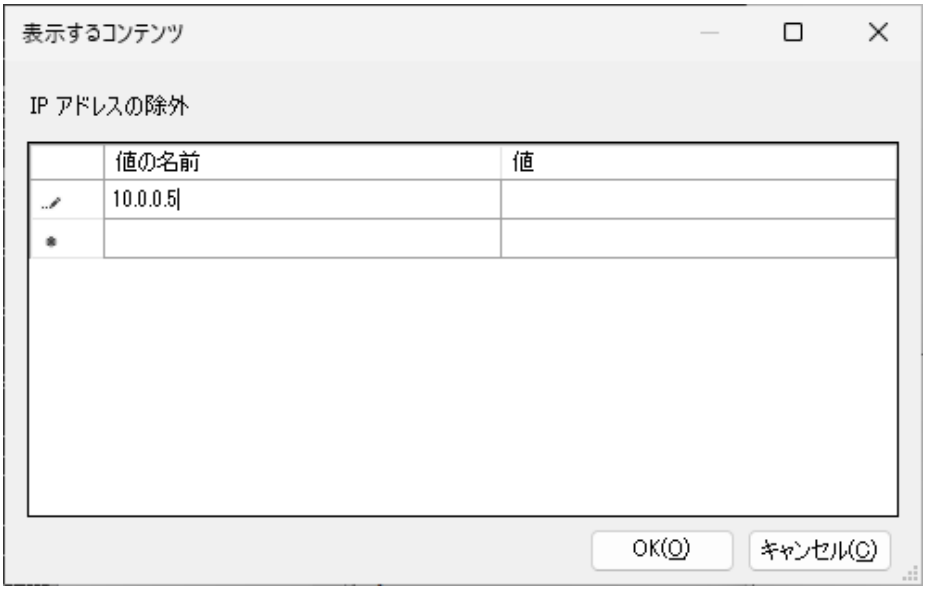
以下の ActiveDirectory グループポリシー管理から カメラの IP アドレスの除外指定を行うことで、そのカメラを MDE による通信遮断の対象外とすることができます。

Windows の[ファイル名を指定して実行]で gpedit.msc と入力してグループポリシーエディターを起動して、以下の項目を開きます。
パス：[管理用テンプレート] > [Windows コンポーネント] > [Microsoft Defender ウイルス対策] > [除外]
項目：IP アドレスの除外



“IP アドレスの除外” ポリシーで、除外対象にしたいカメラの IP アドレスを "値の名前" に指定することで、除外指定が行えます。

例） IP アドレス 10.0.0.5 を除外指定する場合の例



設定には IP アドレスのみが有効であり、CIDR 表記（例: 192.168.10.0/24）やワイルドカードは指定できません。除外対象にしたいカメラの IP アドレスを 1 つずつ指定してください。

設定を確認したい場合は、Media Production Suite を実行する PC において管理者権限で起動した PowerShell で Get-MpPreference コマンドを利用します。

確認コマンド：
Get-MpPreference | select -expand ExclusionIPAddress

グループポリシーで IP アドレスの除外を行う手順は以上となります。

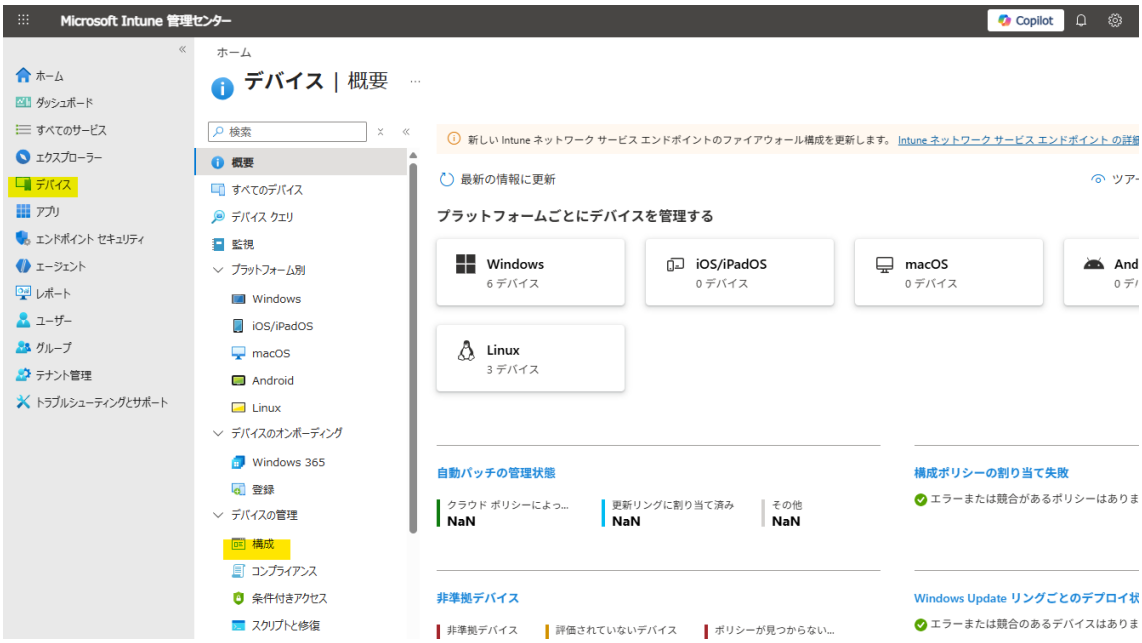
2.3　Intune から IP アドレスの除外を行う方法

※補足事項（Intune 管理端末の場合） Intune により管理されているデバイスでは、Microsoft Defender ウイルス対策の設定は Intune による構成が最優先されます。 この場合、グループ ポリシーやローカル PowerShell コマンドによる IP アドレス除外設定は反映されません。 Intune 管理端末に対して IP アドレス除外を行う場合は、本章に記載の Intune による設定方法を使用してください。

通常、Intune から Microsoft Defender ウイルス対策（MDAV）の設定を変更する場合には、[エンドポイント セキュリティ] - [ウイルス対策] から AV ポリシーが利用できます。
ただし、IP アドレスの除外は AV ポリシーに対応していないため、Intune を利用する場合には、デバイス構成ポリシーから設定カタログを利用することで設定が可能です。

以降は新規ポリシーを作成する場合の例として記載します。

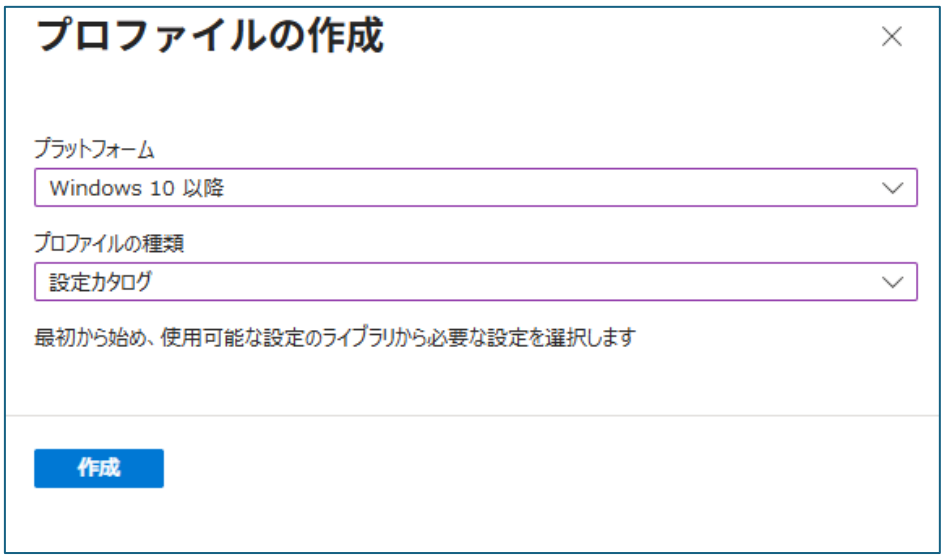
Microsoft Intune 管理センター（intune.microsoft.com）にサインイン後、[デバイス] – [デバイスの管理] – [構成] と遷移し、”作成” より新しいポリシーの作成を開始します。



“プロファイルの作成”で以下のように指定します。

プラットフォーム：Windows 10 以降

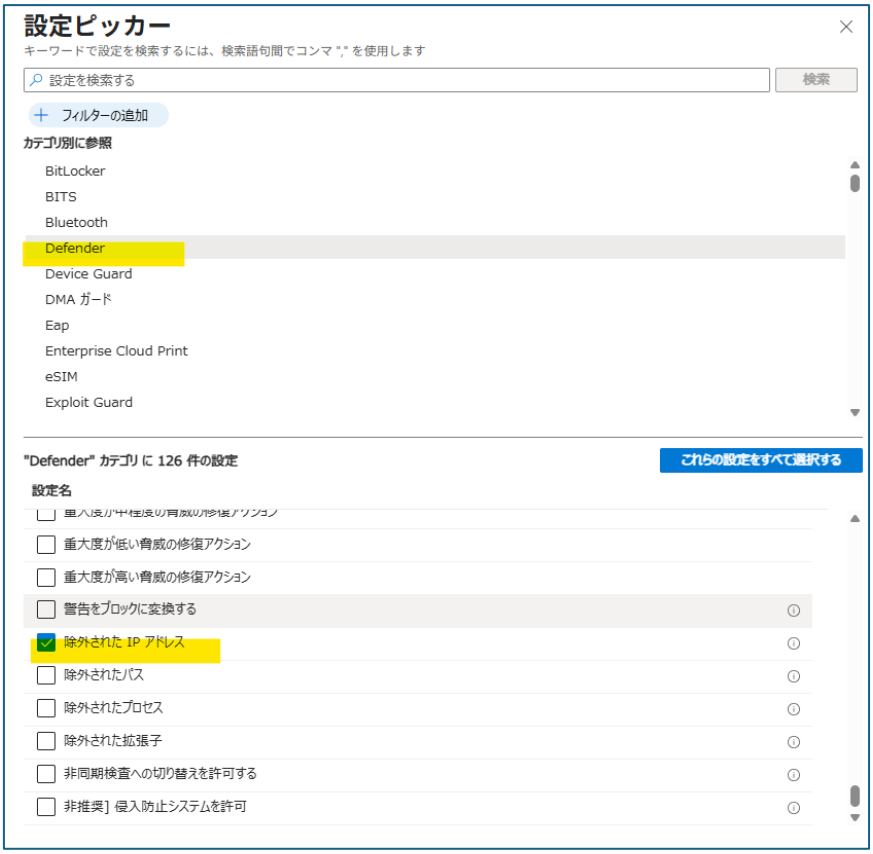
プロファイルの種類：設定カタログ



“基本情報”タブでは、任意のポリシーの名前を入力します。以下は例としてポリシー名に「IP アドレス除外」と指定していますが、ご利用環境に応じ、任意の名称を付与することができます。

“構成設定”タブでは“設定の追加”を選択し、設定ピッカーを起動します。

設定ピッカーで“カテゴリ別に参照”から Defender を選択し、設定名“除外された IP アドレス”にチェックし、設定ピッカーのウィンドウに表示された × で閉じます。



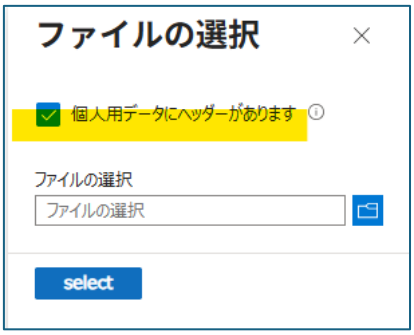
“構成設定” タブに戻り、除外対象にしたいカメラの IP アドレスを入力ボックスに入力します。
設定には IP アドレスのみが有効であり、CIDR 表記（例: 192.168.10.0/24）やワイルドカードは指定できません。除外対象にしたいカメラの IP アドレスを 1 つずつ指定してください。

また、Intune の設定ではインポートが利用できます。以下のように改行区切りにて複数 IP アドレスをリストしたテキストファイルを利用することで、インポートによる設定も可能です。

テキストファイルの内容例：

192.168.10.1
192.168.10.2
192.168.10.3

なお、Intune でファイルのインポートを行う場合には、"個人用データにヘッダーがあります" のチェックが付与されている場合には、最初にデータが入力された行をヘッダー行としてスキップします。



インポート対象のファイルにヘッダー行を付与しない場合には、本項目のチェックを外すことで、最初にデータが入力された行からインポートすることが可能です。

“スコープ タグ” のタブでは設定は既定値のみの指定でスキップ可能であり、必須ではありません。

“割り当て”タブではご利用環境に応じ、ポリシーを適用するグループや、適用対象から除外するグループを指定します。

“レビューと作成”タブで設定内容に誤りがないかを確認し、ポリシーの作成を完了します。

デバイスへのポリシー適用完了後、デバイス上で設定を確認する場合は、 Media Production Suite を実行する PC において管理者権限で起動した PowerShell で Get-MpPreference を利用します。

確認コマンド：
Get-MpPreference | select -expand ExclusionIPAddress

Intune から IP アドレスの除外を行う手順は以上となります。

更新履歴

本書の更新履歴を記載します。

文書バージョン	変化点
1.0	初版