Microsoft

中小企業に最適なエンドポイント セキュリティ ソリューション

Microsoft Defender for Business

かんたんセットアップ ガイド

- 導入手順をわかりやすく解説 –

Microsoft Defender for Business を使いませんか

中小企業のためのエンドポイント セキュリティ ソリューション、Microsoft Defender for Business のセットアップは非常にシンプル。
本紙では Microsoft Defender for Business を Windows 11 に展開するための導入方法を解説します。

目 次

準備 1 Microsoft Defender for Business のオンボーディング方法 3 選！

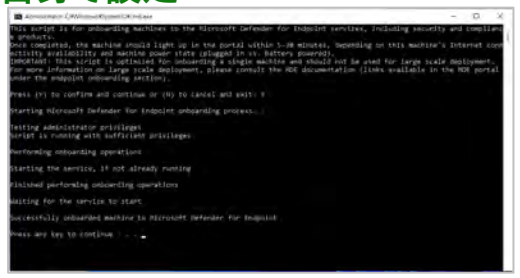
Microsoft 365 ファミリーに新たに加わった Microsoft Defender for Business は、従業員数 300 人以下の企業のためのエンドポイント セキュリティ ソリューションです。シンプルなセットアップで、エンタープライズ グレードのエンドポイント保護を行えます。
ソフトウェアの脆弱性特定、推奨されるセキュリティ ポリシーの有効化、ネットワークのセキュリティ境界強化、攻撃の検知と対応をこのプロダクトのみで実現します。
本紙では Microsoft Defender for Business を Windows 11 に展開するためのオンボーディング方法を解説していきます。
オンボーディングとは、一般的なセットアップと異なり、習熟を必要とする対応を指し示す言葉です。
簡単なオンボーディング プロセスで、快適に Microsoft Defender for Business をお使いいただけます。
まずは基本的な設定で利用を開始していきましょう。

自分に合う
方法を選ぼう！

準備

PC の所有者が自身で設定

クライアント から

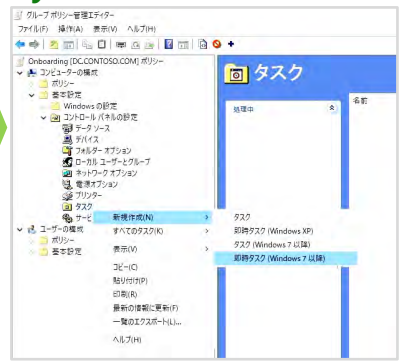


Intune を使用している場合

Intune から

Active Directory を使用している場合

グループ ポリシー から



本手順は動画でも配信しています。手順を参照したい場合は以下の URL にアクセスしてください。
https://aka.ms/JPMDB

準備 2 Microsoft Defender for Business を始めてみよう！

Microsoft Defender for Business は Microsoft 365 Defender の一部です。そのため、設定は Microsoft 365 の管理機能から行います。
管理機能は以下 URL からアクセスできます。

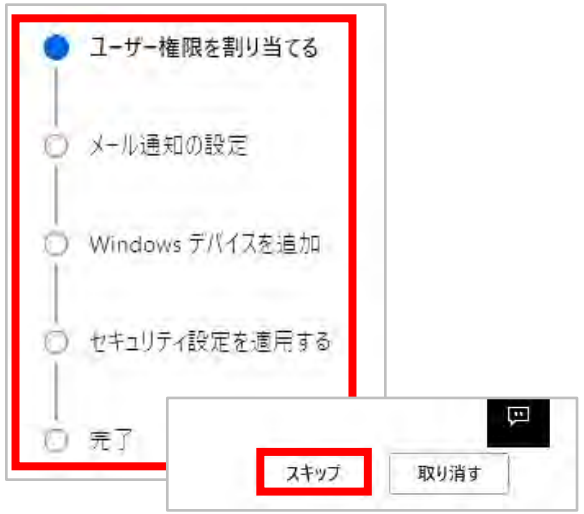
▶ https://security.microsoft.com

以下の手順に沿って Microsoft Defender for Business を利用する事前準備を行いましょう。
この手順で Microsoft Defender for Business の事前準備は完了です。

1.「デバイスのインベントリ」を選びます。

2. 初期化が始まり、しばらくすると表示される画面で「開始する」をクリックします。

3. ウィザードでの設定は行わずすべてスキップします。



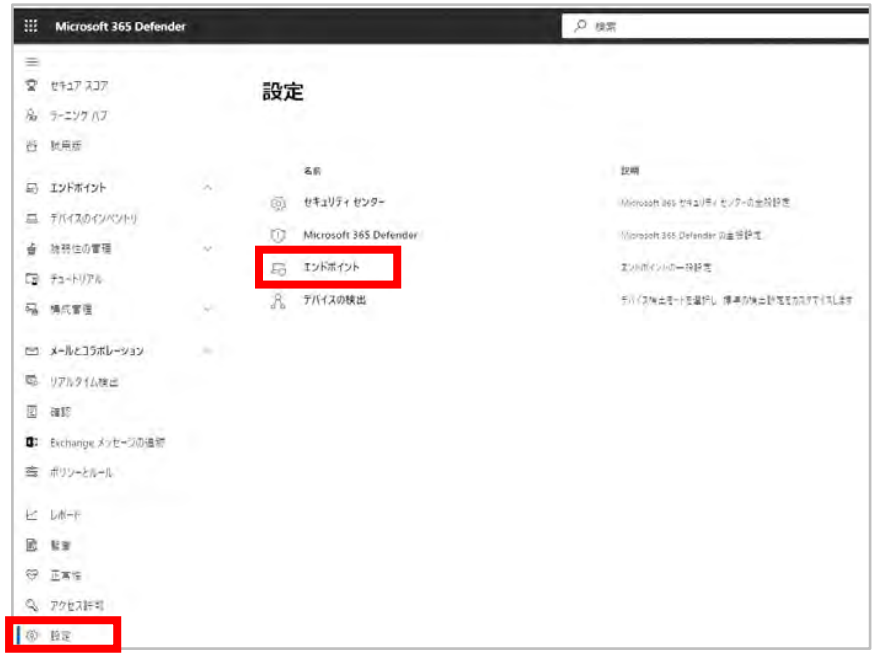
※ ウィザードからご自身で設定できそうであれば、ウィザードから設定いただけます。
本紙はウィザードをスキップしてしまった場合を想定して作成しておりますので、
以降は実際の管理画面からオンボーディングする方法をご説明します。

ローカル オンボーディング

STEP 1 ローカル オンボーディング (管理者での準備) 1/2

ローカル オンボーディングとは PC の保有者に Microsoft Defender for Business の設定を行ってもらう方法です。
事前に管理者側で PC の保有者が利用するためのスクリプトを準備します。

1. 設定>
エンドポイントを選びます。



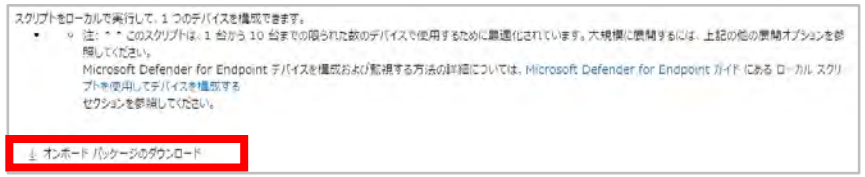
2. エンドポイント>
オンボーディングを選びます。

3. OS、展開方法の選択で
「Windows 10 と Windows 11」
「ローカル スクリプト (最大 10 台のデバイス用) 」を選びます。

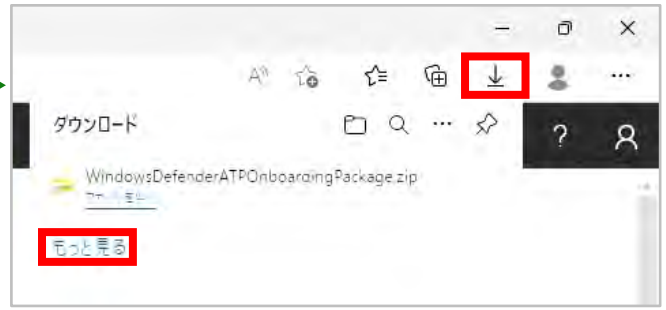
STEP 1 ローカル オンボーディング (管理者での準備) 2/2

スクリプトは zip 形式でダウンロードされます。
Windows Defender ATP Onboarding Package.zip を開くと、Windows Defender ATP Local Onboarding Script.cmd コマンド スクリプトが入っています。
Microsoft Defender for Business を展開したい PC の保有者がアクセスできる場所に、このファイルを配置してください。

4. オンボード パッケージ ダウンロード リンクをクリックします。



5. ダウンロードしたファイルを開きます。

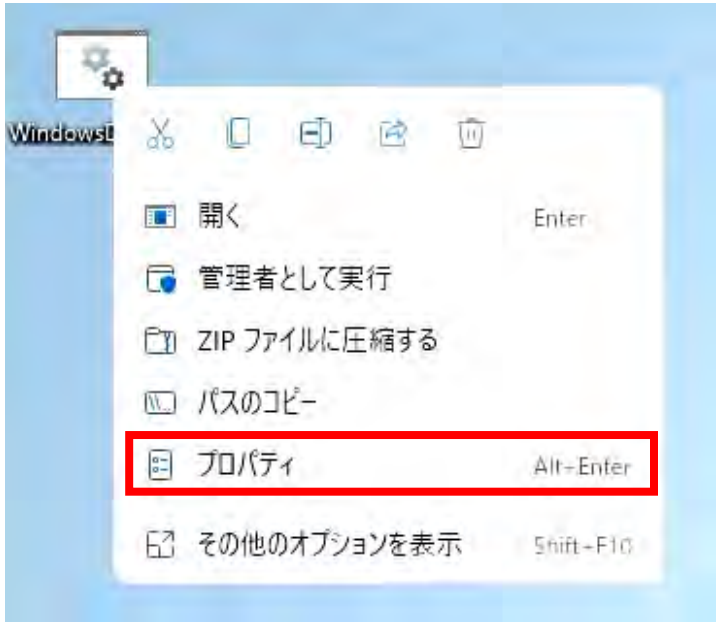


6. Zip を展開し、ユーザーに配布しましょう。

STEP 2 ローカル オンボーディング (クライアントでの実行)

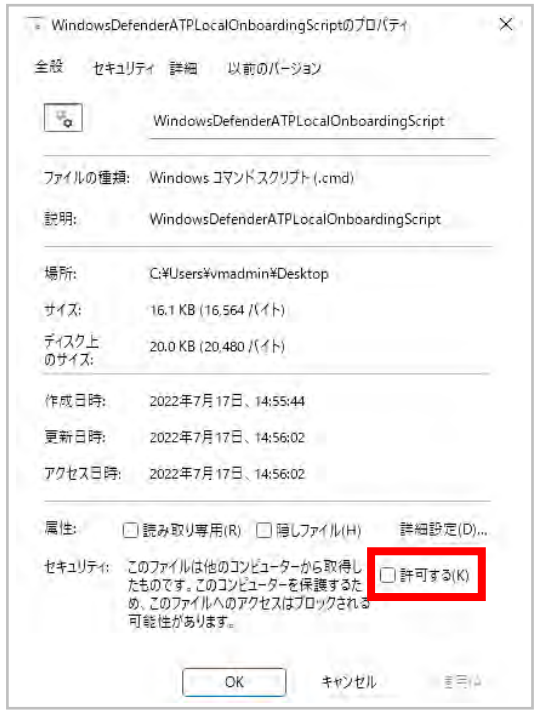
スクリプト ファイルは PC 保有者が実行します。
このスクリプトはインターネットからダウンロードした扱いとなるため、このままでは実行できません。
実行するために実行許可を与えます。この許可は信頼できるファイルにのみ実施するようにしてください。
管理者として実行すると黒いコマンド プロンプトが表示されます。途中、Y キーを押し、先に進める必要があります。最後に何かキーを押すとインストール完了です。

1. 自分の PC にコピーし 右クリックでプロパティを開きます。

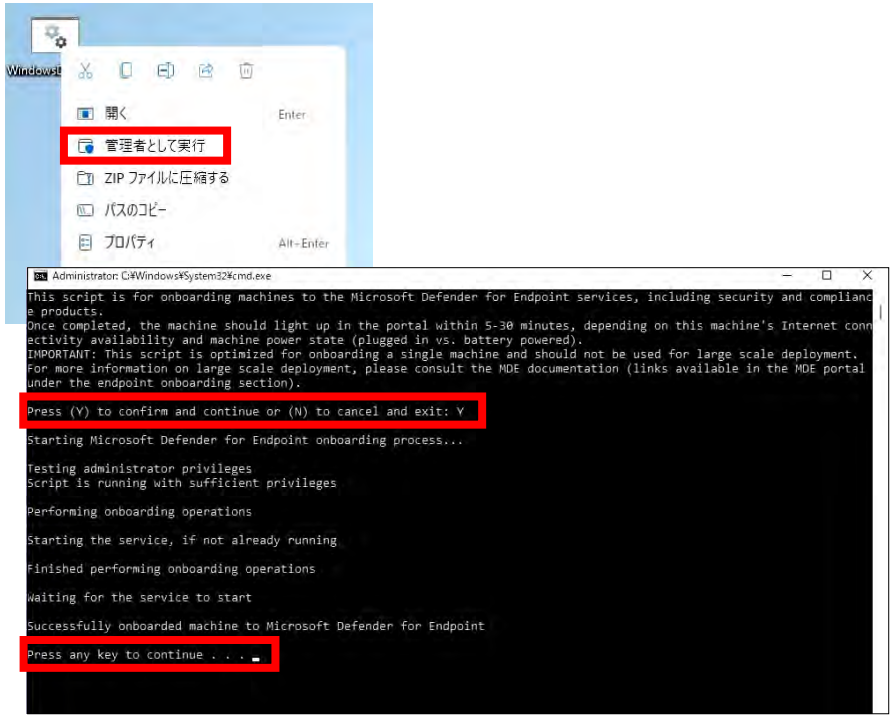


2. 実行を「許可する」にチェックを入れます。

注意 危険なので信頼する時のみ実行



3. 「管理者として実行」の後、Y キーを押し、何かキーを押します。



STEP 3 ローカル オンボーディング (クライアントでの検出確認)

ここまでの手順で実行は完了ですが、設定が問題なく行われたか気になる場合はアラート検出の試験を行いましょう。
以下の手順でコマンドを PC 保有者に伝えます。このコマンドをコマンド プロンプトから起動すると何も起こりませんが、 Microsoft Defender for Business の設定が完了した場合、数分後にアラートが Microsoft Defender for Business 上に表示されます。

コマンドは以下をコピーして利用することも可能です。

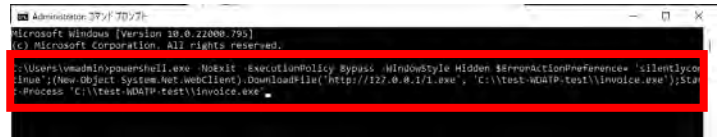
```
Powershell.exe –NoExit –ExecutionPolicy Bypass –WindowStyle Hidden $ErrorActionPreference= ‘silentlycontinue’;(New-Object System.Net.WebClient).DownloadFile(‘http://127.0.0.1/1exe’, ‘C:¥¥test-WDATP-test¥¥invoice.exe’);Start-Process ‘C:¥¥test-WDATP-test¥¥invoice.exe’
```

コマンドの内容は、PC からファイルをダウンロードして実行するものですが、ファイルがないためダウンロードに失敗し、続いてダウンロードしたファイルの実行にも失敗します。その失敗を検知してくれます。

1.【管理者側作業】
管理者がスクリプトをダウンロードした画面の下部にある検出テストの実行コマンドをコピーします。

2.【PC 保有者作業】
Win キーで検索画面を表示し「cmd」と入力します。表示されたコマンド プロンプトを管理者で起動します。

3.【PC 保有者作業】
コマンドを Ctrl + V キーで張り付け実行します。画面が閉じたら完了です。



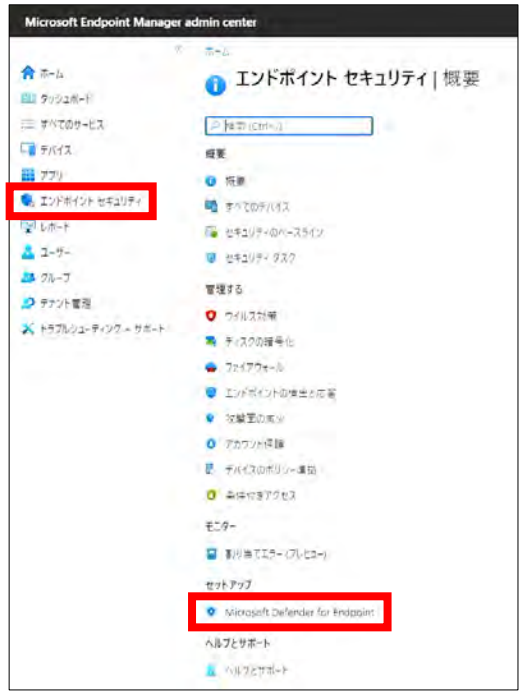
Microsoft Intune オンボーディング

STEP 1 Microsoft Intune オンボーディング 1/4

Intune オンボーディングとは、管理者が Intune を通じて Microsoft Defender for Business を設定する方法です。
Microsoft 365 の導入時に Intune を利用してデバイス管理を行っている場合はこの方法が簡単です。
Intune の設定画面は以下 URL からアクセスできます。

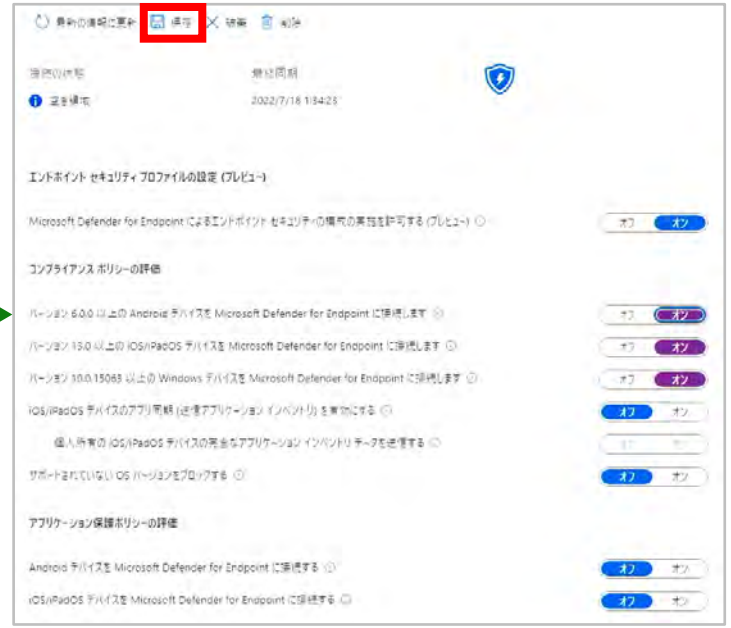
https://endpoint.microsoft.com

1. 「エンドポイント セキュリティ」を選択し
セットアップ セグメントにある
「Microsoft Defender for Endpoint」を選びます。



2. 「～に接続します」をオンにします。
Windows がターゲットの場合、
一番下のみでも構いません。

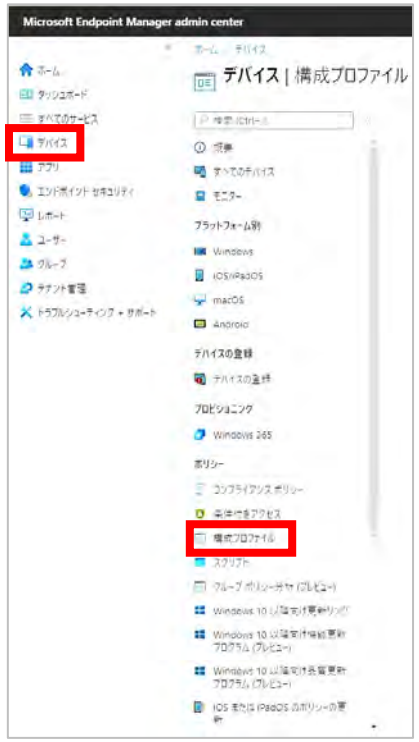
3. これだけでは適用されません。保存
ボタンを押し忘れないようにしましょう。



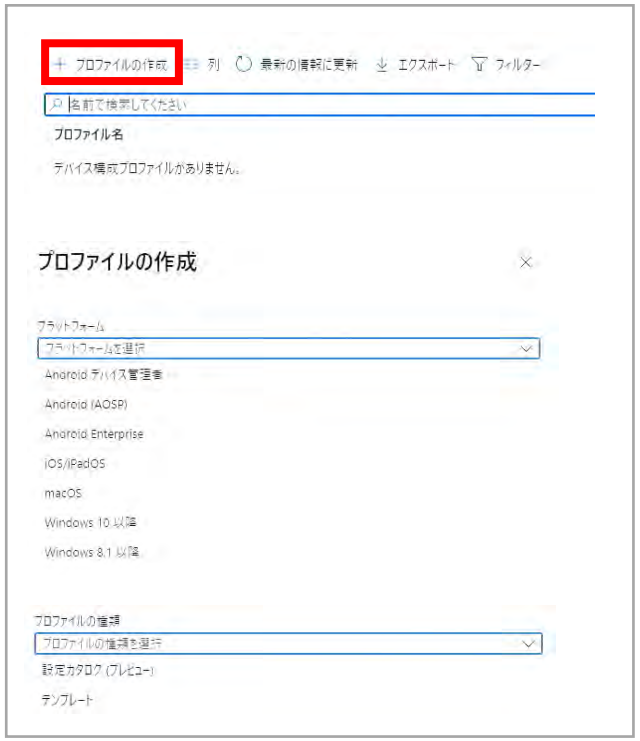
STEP 1 Microsoft Intune オンボーディング 2/4

以下の手順に沿ってボタンを押下することで Intune での展開設定を行っていきます。
PC 保有者の介在がないため、台数の多い場合に効果を発揮します。

4. 「デバイス」を選択しポリシー セグメントにある「構成プロファイル」を選びます。



5. 「プロファイルの作成」ボタンを押します。

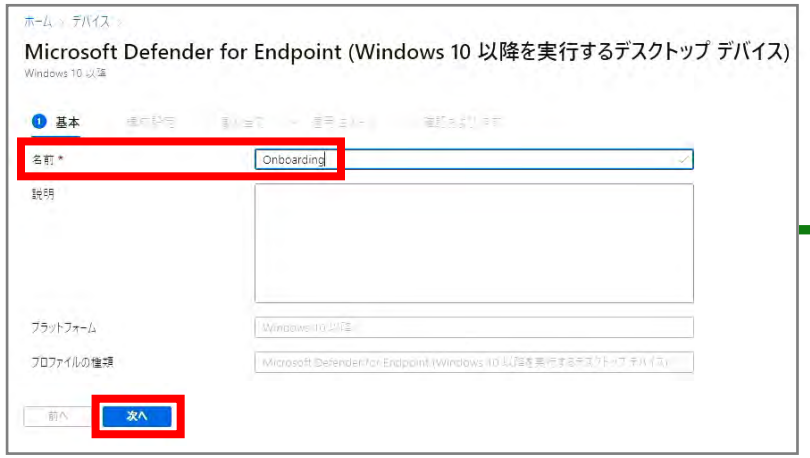


6. プロファイルの種類として「テンプレート」を選択し「Microsoft Defender for Endpoint (Windows 10 以降を実行するデスクトップ デバイス)」を押します。

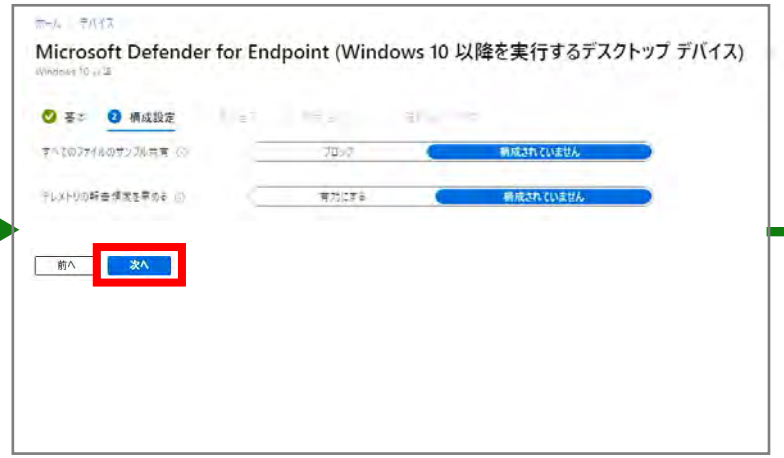
STEP 1 Microsoft Intune オンボーディング 3/4

プロファイル名称の決定を行ったら Microsoft Defender for Business を利用するユーザーを決定します。

7. プロファイルに名前を付け、「次へ」を押します。



8. 構成設定は変更せずに「次へ」を押します。



9. Microsoft Defender for Business を利用させたいユーザーを指定します。グループでの指定もしくはすべてのユーザー、すべてのデバイスを対象にできます。

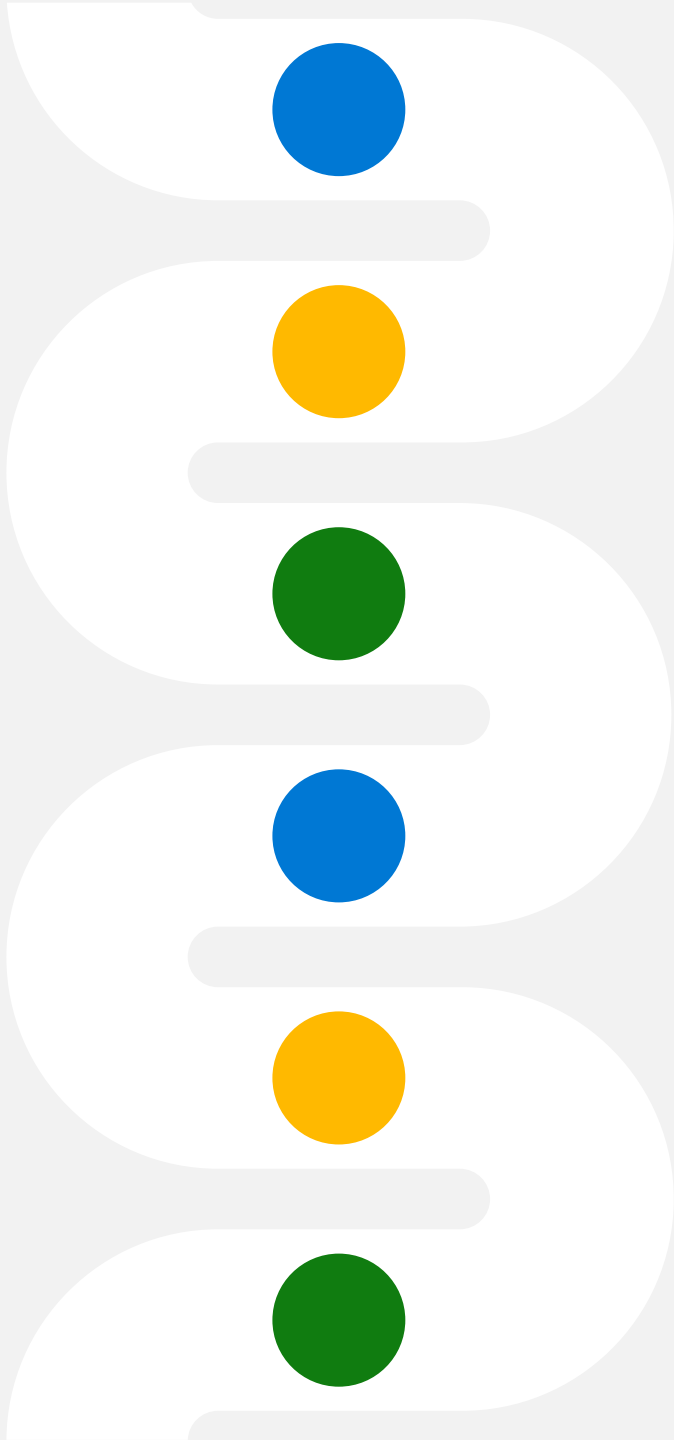
STEP 1 Microsoft Intune オンボーディング 4/4

プロファイルが作成されたのちに、自動的に Microsoft Defender for Business が各 PC に配布されていきます。

10. ルールの設定は不要です。「次へ」を押します。

11. 設定内容を確認し、「作成」を押します。

グループ ポリシー オンボーディング

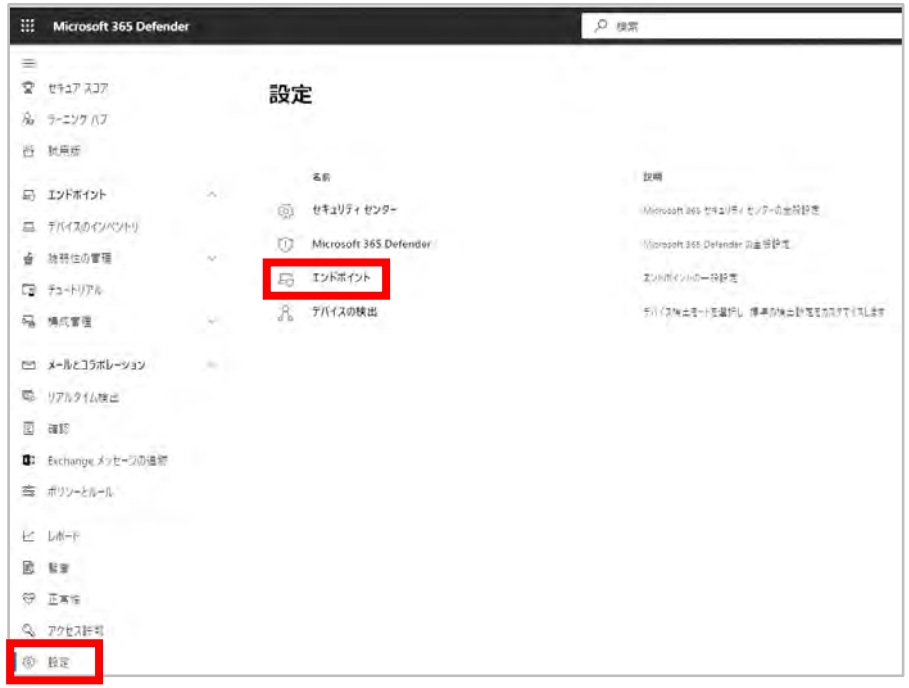


STEP 1 グループ ポリシー オンボーディング (準備) 1/2

グループ ポリシー オンボーディングは管理者が Active Directory を通じて Microsoft Defender for Business の設定を行う方法です。
Active Directory に PC が参加している場合はこの方法を利用します。
まず Microsoft 365 Defender サイトよりスクリプトをダウンロードします。

https://security.microsoft.com

1. 設定>
エンドポイントを選びます。



2. エンドポイント>
オンボーディングを選びます。

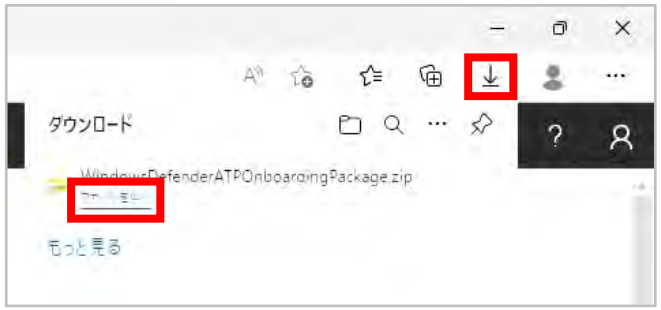
3. OSおよび展開方法の選択で
「Windows 10 と Windows 11」
「グループ ポリシー」を選びます。

STEP 1 グループ ポリシー オンボーディング (準備) 2/2

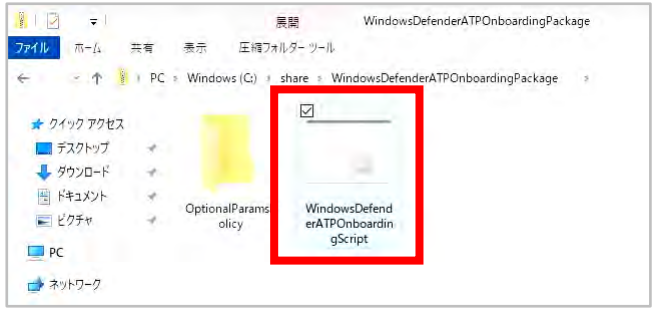
スクリプトは zip 形式でダウンロードされます。
Windows Defender ATP Onboarding Package.zip を開くと Windows Defender ATP Local Onboarding Script.cmd コマンド スクリプト が入っています。
このスクリプトを Active Directory Server 上の特定フォルダーに展開します。
この特定フォルダーは共有を有効化します。各 PC はこのフォルダーにあるファイルにアクセスを行います。

4. オンボード パッケージ ダウンロード リンクをクリックします。

5. ダウンロードしたファイルを開きます。



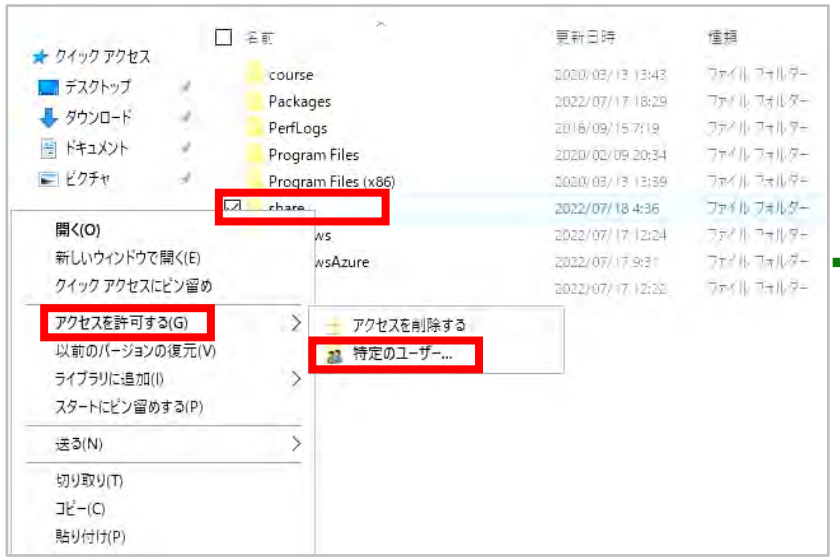
6. Active Directory Server にフォルダーを作成し、ダウンロードした Zip の中身を展開しましょう。
ここでは C:¥Share を作成しています。



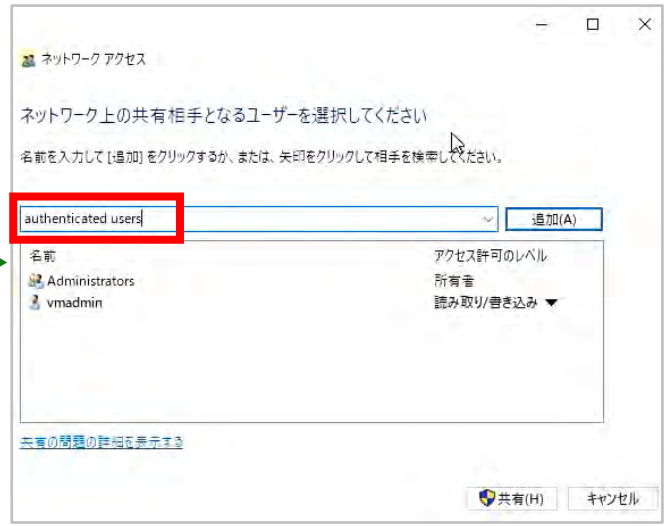
STEP 2 グループ ポリシー オンボーディング (Active Directory 準備) 1/5

Active Directory 上に用意したフォルダーにアクセス権を設定します。

1. 作成したフォルダーを選択、右クリックを行い、「アクセスを許可する」内の「特定のユーザー」をクリックします。



2. 「Authenticated users」を入力し「追加」ボタンを押します。



3. アクセス権一覧に「Authenticated Users」が表示されアクセス許可のレベルが「読み取り」となっていることを確認します。

STEP 2 グループ ポリシー オンボーディング (Active Directory 準備) 2/5

共有フォルダーの状態を確認します。
これによりすべてのドメイン内のユーザーはこのフォルダーにあるスクリプトにアクセスできるようになります。

4. フォルダーが共有されたことを確認し「終了」ボタンを押します。

5. 本例では、こちらのアドレスがスクリプトのネットワーク共有用パスとなっています。後程アドレスを利用するため、お手元にご自身のアドレスを控えておきましょう。

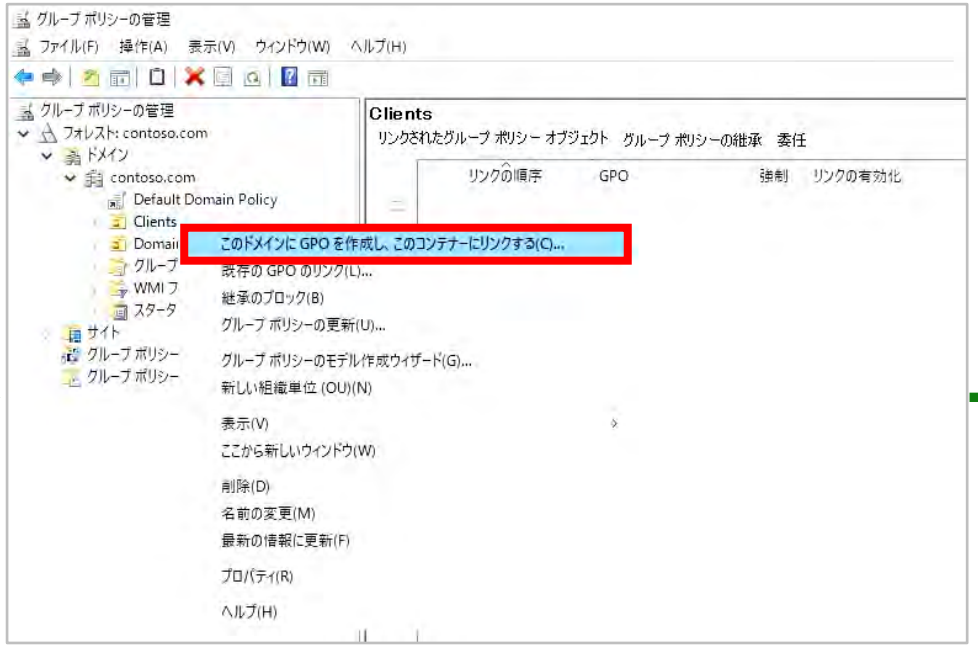
¥¥dc¥share¥WindowsDefenderATPOnboardingScript.cmd

STEP 2 グループ ポリシー オンボーディング (Active Directory 準備) 3/5

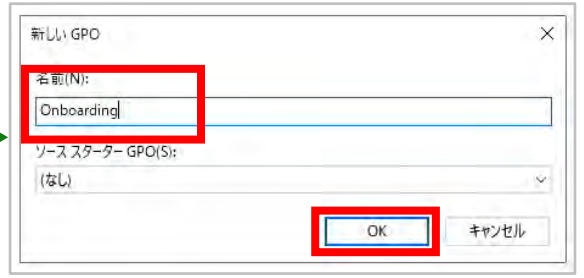
グループ ポリシーを作成し、ダウンロードしたスクリプトを実行するように設定します。
これによりドメイン ポリシーが PC に適用されると Microsoft Defender for Business がインストールされるようになります。

6. サーバー マネージャーを開き、ツールから「グループ ポリシーの管理」を選択します。

7. 適用したい OU を右クリックし「このドメインに GPO を作成し、このコンテナーにリンクする」をクリックします。



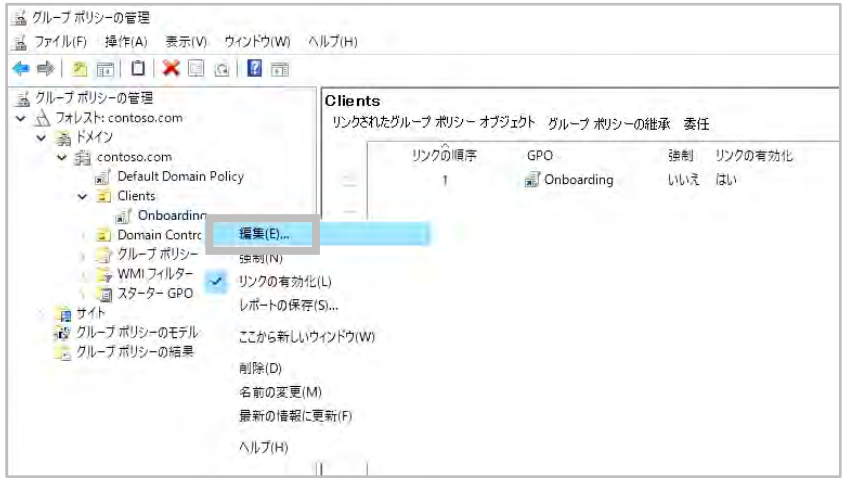
8. 新しい GPO の名称を設定し「OK」ボタンをクリックします。



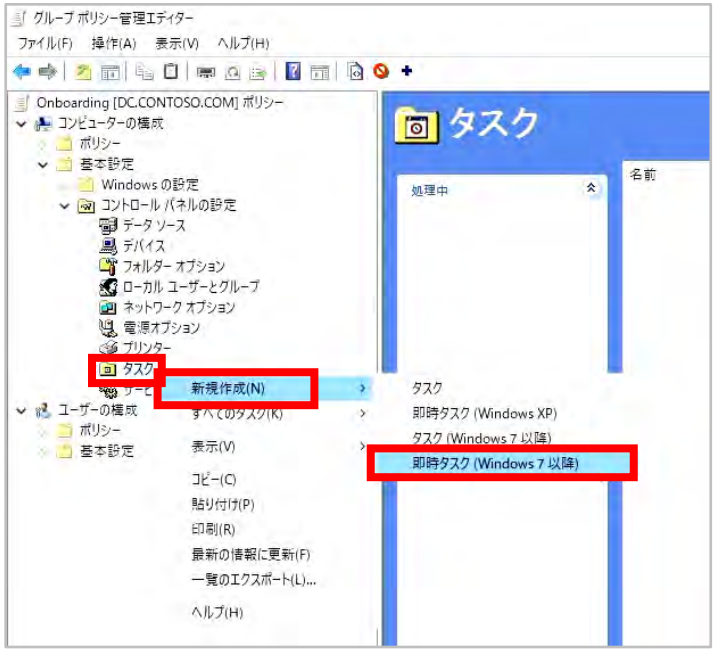
STEP 2 グループ ポリシー オンボーディング (Active Directory 準備) 4/5

タスク実行時は、システム権限やログインなしでも動作するように設定しましょう。
ポリシーがダウンロードされた時にログインせずとも実行されるようになります。

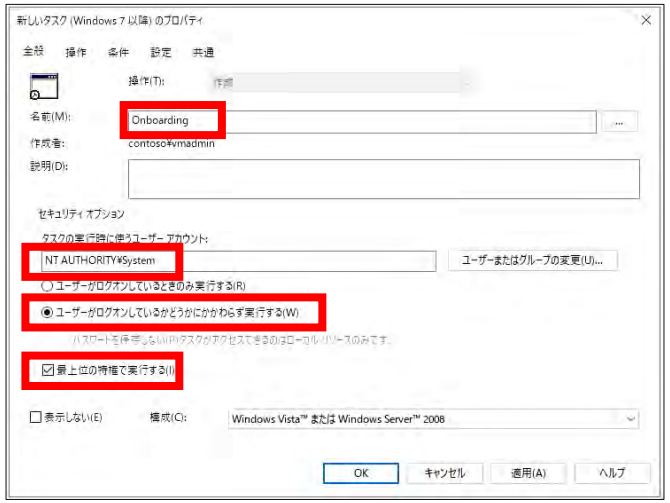
9. 作成された GPO を右クリックし、「編集」ボタンをクリックします。



10. グループ ポリシー管理エディターが開くので、コンピューターの構成>基本設定>コントロール パネルの設定>タスクを右クリックします。新規作成内の「即時タスク (Windows 7 以降)」をクリックします。



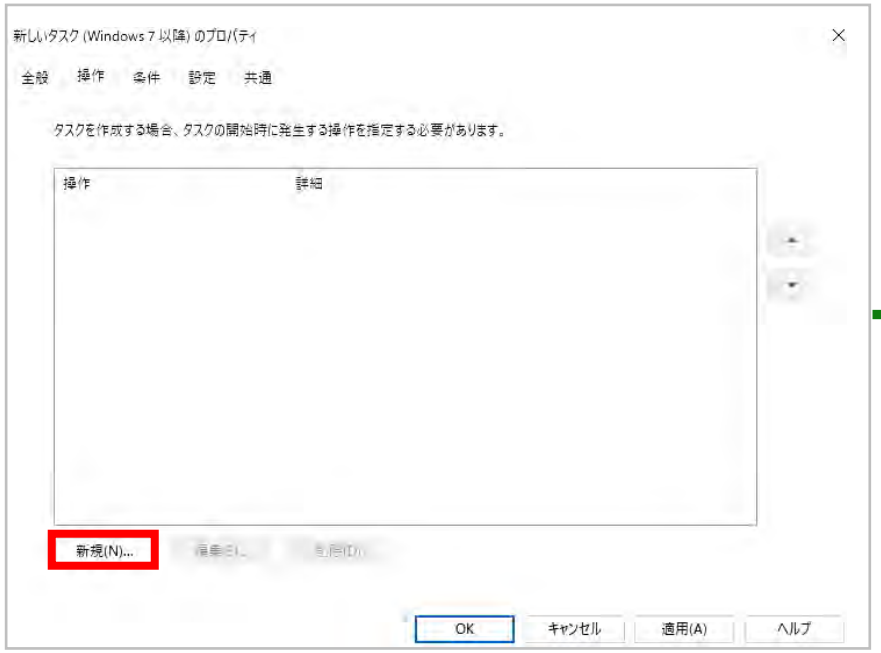
11. 名前とユーザー アカウント (NT AUTHORITY￥System) を入力し、「ユーザーがログオンしているかどうかにかかわらず実行する」と「最上位の特権で実行する」にチェックを入れ、「OK」ボタンを押下します。



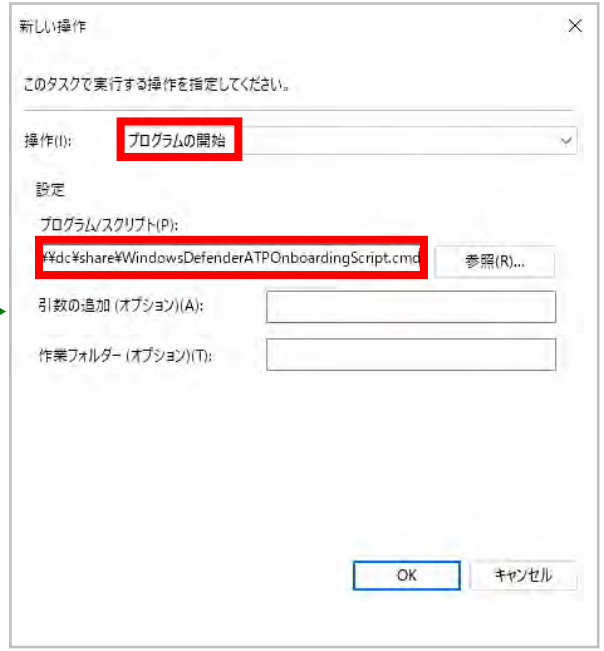
STEP 2 グループ ポリシー オンボーディング (Active Directory 準備) 5/5

タスクで実行するスクリプトは各 PC からアクセスできる必要があります。
先に共有設定したファイルをスケジュールに設定しましょう。

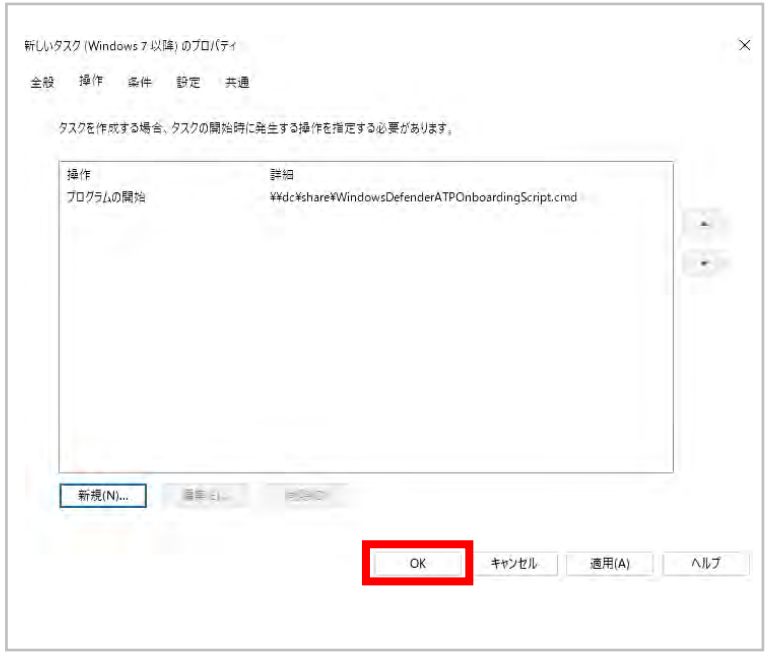
12.「新規」をクリックします。



13.「プログラムの開始」を選択し、
先に控えたスクリプトの
ネットワーク共有用パスを入力します。



14. 内容を確認し「OK」をクリックします。



Microsoft Defender for Business を使いたい場合は

セキュリティ強化の度合いや現在利用中のクラウド環境における対策状況に応じて 2 つのプランから選択できます。

Microsoft 365 Business Premium で ゼロ トラスト型セキュリティ対策が実現可能

Microsoft 365 の機能と Microsoft Azure AD P1/Microsoft Intune が提供されます。
Office アプリとパワフルなクラウド サービスに包括的なセキュリティを組み合わせたプランです。ビジネスを高度なサイバー脅威から守るのに役立ちます。

Microsoft Defender for Business で 端末セキュリティのみ切り出して対応可能

Microsoft Defender for Business 単独での購入もおすすめです。Windows OS 標準のセキュリティ対策ソフトを強化して、さらに EDR 機能を追加したい場合にはこちらを選択しましょう。

Microsoft 365 Business Premium のメリット　どこからでも安心して仕事ができる

包括的で使いやすい

- 1 つのソリューションで生産性とセキュリティを両立
- クラウド プラットフォームであるため、導入が簡単
- すぐに利用できる

コスト削減

- 複数のポイント ソリューションにかかるコストを廃止
- ヘルプ デスクのコストを削減
- ライセンスの複雑さを解消

エンタープライズ レベルのテクノロジー

- 多くのエンタープライズが信頼する高度なセキュリティ
- AI を活用した脅威インテリジェンス
- 評価の高いセキュリティ

Microsoft

ご相談は、IT よろず相談センターへ

0120-167-400

(営業時間 : 9:00 ～ 17:30 土日祝日、弊社指定休業日を除く)

Microsoft Security に関する最新情報はこちらをご覧ください。

https://aka.ms/JPMDB

日本マイクロソフト株式会社
〒108-0075 東京都港区港南 2-16-3 品川グランドセントラルタワー