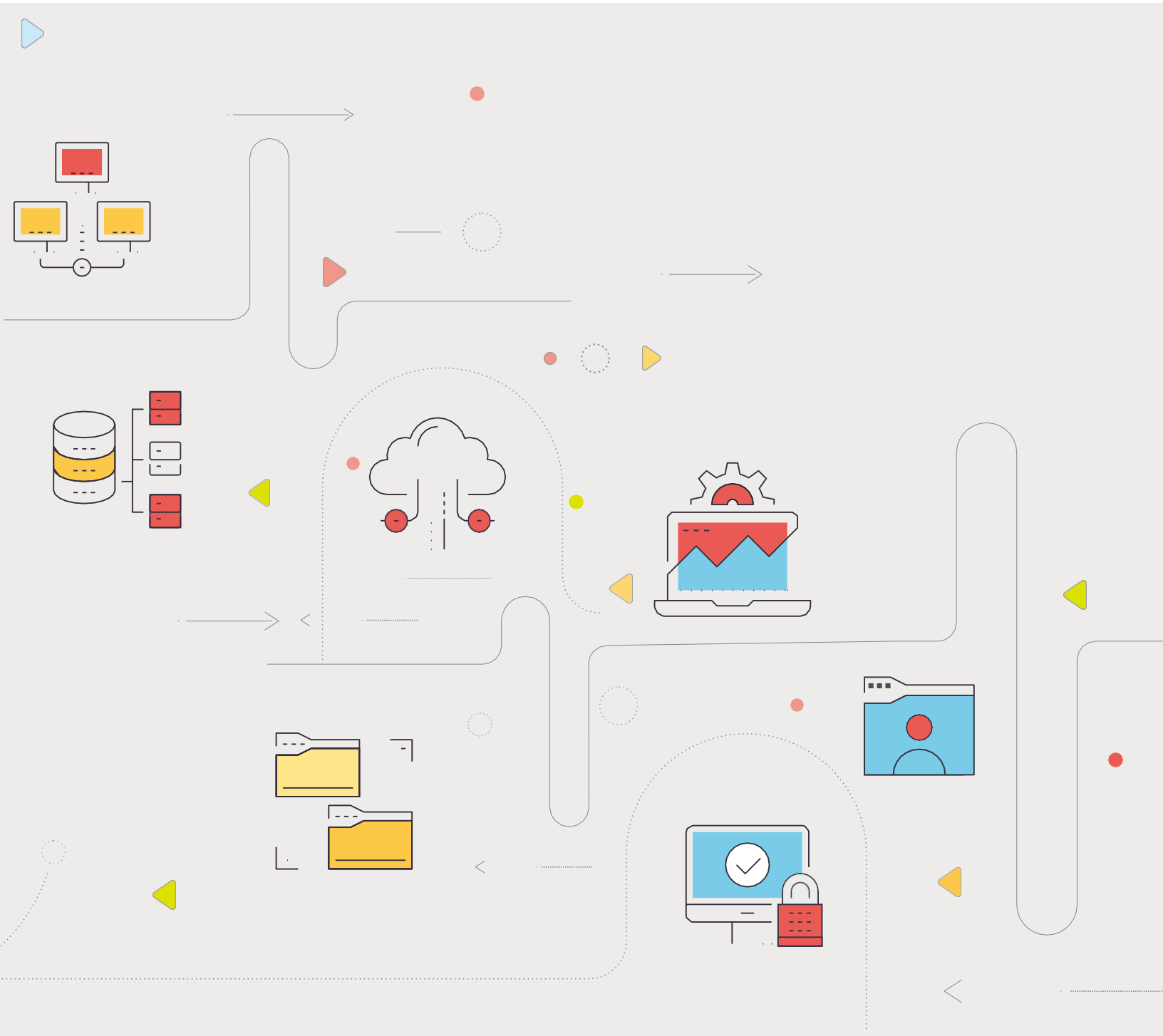
ZJTP20248192271

ManageEngine

スタートアップガイド

Endpoint Central Cloud



目　次

1. システム要件

Endpoint Central Cloud を利用するために必要なシステム要件は以下の通りです。

▶ システム要件:
https://www.manageengine.jp/products/Endpoint_Central/system-requirements.html
（オンプレミス版・クラウド版共通のページです。「クラウド版」を選択してご覧ください。）

Endpoint Central Cloud エージェントの最小ハードウェア要件

Endpoint Central Cloud の管理対象に追加するコンピューターは、以下の要件を満たす必要があります。

プロセッサー	メモリー	ハードディスク容量*1
Intel Pentium 1.0 GHz 以上	512.0 MB 以上	3.0 GB 以上 *1

*1 この容量はパッチやソフトウェアなどの配布ファイルを含みません。実際に必要な容量は配布ファイルのサイズや頻度によって異なります。
なお Endpoint Central Cloud では、インターネット接続のないコンピューターを管理することはできません（インターネット接続のない環境での管理には、オンプレミス版の Endpoint Central をご検討ください）。

Endpoint Central Cloud で管理可能なOS*2

Endpoint Central Cloud を使用して管理できるOSは以下の通りです。

- Windows 11
- Windows Server
- macOS
- Red Hat Enterprise Linux
- CentOS Stream
- Ubuntu
- Debian
- SUSE Linux Enterprise
- Oracle Linux
- Rocky Linux
- Amazon Linux
- Fedora *3
- OpenSUSE *3
- Linux Mint *3
- iOS *4
- iPadOS *4
- tvOS *4
- Android *4
- ChromeOS *4

*2 各OSの対応バージョンは上記 URL よりシステム要件のページをご覧ください。なお、Linux OS については、カーネルバージョンが 2.6.33 以上のOSをサポートしています（一部のディストリビューションには機能制限があります）。
*3 パッチ管理には対応しておりません。
*4 モバイルデバイス管理機能においてサポートしています。

Endpoint Central Cloud の配信サーバー

Endpoint Central Cloud では、必要に応じて配信サーバーを設置できます。
コンピューター台数の多い拠点がある場合など、パッチ/ソフトウェア配布時の帯域消費を特に抑えたいような場合に配信サーバーを設置します。また、Active Directory との同期を有効化する場合や Java SE など一部のサードパーティ製品のパッチを配布する場合、OS配布機能を使用する場合にも、配信サーバーが必要です（リモート制御機能やMDM機能においては、配信サーバーを使用しません）。

▶ システム構成に関するナレッジ:
https://www.manageengine.jp/support/kb/Endpoint_Central_Cloud/?p=2397

▶ 配信サーバーのインストール方法:
https://www.manageengine.jp/support/kb/Endpoint_Central_Cloud/?p=81

コンソール対応 Webブラウザー

Endpoint Central Cloud コンソールにアクセスする際、以下の Web ブラウザー[*5] を使用できます。

- Microsoft Edge （Chromium版、最新版の利用を推奨します）
- Mozilla Firefox （44 以降、最新版の利用を推奨します）
- Google Chrome （47 以降、最新版の利用を推奨します）
- Zoho Ulaa （2.0.0 以降、最新版の利用を推奨します）

*5 画面解像度は1280×1024ピクセル以上が必要です。

（参考）パッチ管理機能でサポートするアプリケーション

Endpoint Central Cloud のパッチ管理機能がサポートするアプリケーションは、以下をご覧ください。
なお、Endpoint Central Cloud のパッチ管理機能は Patch Manager Plus Cloud の機能と同一です。

▶ サポートするアプリケーション一覧:
https://www.manageengine.jp/products/Endpoint_Central/patch_management_supported_application.html

▶ サポートするアプリケーション一覧（ナレッジ）:
https://www.manageengine.jp/support/kb/Endpoint_Central_Cloud/?p=887

2． アカウントの作成

Endpoint Central Cloud を利用するには、Zoho アカウントが必要です。

● Zohoアカウントを既にお持ちの場合

Zoho のクラウドサービスを既にご利用いただいている場合、Endpoint Central Cloud 評価版のページから先へ進むと、既存のアカウントで自動的にログインできます。

● Zohoアカウントをお持ちでない場合

Zoho のクラウド製品に初めてアクセスする場合、Endpoint Central Cloud 評価版のページから先に進み、以下の情報を入力して Zoho アカウントを作成します。なお、アカウント作成時に利用するデータセンター（日本、米国、中国、EU、英国 など）を選択します。

▶名前	▶会社名
▶メールアドレス	▶電話番号

ここで入力された組織の詳細は機密事項です。ここで作成したアカウントが「スーパー管理者」となります。

▶ 評価版（オンプレミス版・クラウド版共通のページです。「クラウド版」を選択してください。）：
https://www.manageengine.jp/products/Endpoint_Central/download.html

▶ サインアップ～ログインまでの詳しい手順:
https://www.manageengine.jp/support/kb/Endpoint_Central_Cloud/?p=312

▶ 製品ユーザーの追加:
https://www.manageengine.jp/support/kb/Endpoint_Central_Cloud/?p=118

1 ご入力いただいたアドレスに確認メールが送信されます。
確認が完了すると、アカウントが作成されます。

2 コンソールにリダイレクトされます。
今後、Zohoアカウントから製品コンソール画面にアクセスできます。

3 製品ユーザーを追加する場合、[管理]タブ ＞ [グローバル設定] ＞ [ユーザー管理] よりメールアドレス等を追加すると、入力したメールアドレスに招待が送信されます。

3. 管理対象の定義（コンピューター）

Endpoint Central Cloud では、コンピューターとモバイルデバイスで管理方法が分かれています。コンピューターを管理する場合、エージェントをインストールする前にリモートオフィスを追加し、エージェントに関する設定を完了させて管理対象を定義します。その後、エージェントをインストールします。

A. リモートオフィスの追加

エージェントは必ずいずれかのリモートオフィスに所属し、デフォルトでは「Default Remote Office」に所属します。利用環境に応じてリモートオフィスの設定を編集し、必要な場合に新規リモートオフィスを追加します。

- 配信サーバーを設置する場合は、リモートオフィスの作成時に選択します。
- プロキシ経由でインターネットに接続する環境では、プロキシの詳細情報をリモートオフィスの設定に登録します（エージェントや配信サーバーのインストール前に設定する必要があります）。

1 [エージェント]タブへ移動し、左側のメニューから[リモートオフィス]を開きます。

2 新規にリモートオフィスを作成する場合、[リモートオフィスの追加]をクリックします。
既存のリモートオフィスを編集する場合、スクロールバーを右に移動させ、編集するリモートオフィスの「アクション」列の三点リーダアイコン ＞ [編集]をクリックします。

3 必要に応じてリモートオフィス名を編集します。

4 通信タイプを選択します。

- 配信サーバーを設置しないリモートオフィスの場合は「直接通信」を選択します。
- 配信サーバーを設置するリモートオフィスの場合は「配信サーバー（DS）による」を選択し、配信サーバーとなるコンピューターの詳細情報を入力します。詳細は B.配信サーバーのインストールとADとの同期 をご覧ください。

5 複製ポリシー*1（デフォルトでは「Default Replication Policy」）を選択します。

- 複製ポリシーは、各リモートオフィスで使用する帯域や通信間隔を指定します。必要に応じて [ポリシーの作成] をクリックし、新しい複製ポリシーを作成します（複製ポリシーにおいて帯域制御が可能です）。

6 プロキシ経由で接続する場合、「プロキシ設定」にチェックを入れて詳細を入力します。

- プロキシ設定は、配信サーバーやエージェントのインストール前に設定する必要があります。プロキシ設定を編集した場合、配信サーバーやエージェントを再インストールする必要があります。

7 [追加]をクリックします。

以上の手順でリモートオフィスが作成されます。評価版・製品版ではリモートオフィス数に上限はありません。

▶ リモートオフィスの追加:
https://www.manageengine.jp/support/kb/Endpoint_Central_Cloud/?p=81

B.配信サーバーのインストールとADとの同期

配信サーバーを設置する場合、配信サーバーをインストールします。（配信サーバーを設置しない場合は、この節をとばして 4章 エージェントのインストール/デバイスの登録 へ進みます。）

1 [エージェント]タブへ移動し、左側のメニューから[リモートオフィス]を開きます。

2 A.リモートオフィスの設定で追加したリモートオフィスの「エージェントのダウンロード」列のサーバーアイコンをクリックし、配信サーバーのインストーラーをダウンロードします。

3 ダウンロードしたインストーラーを実行します。インストールするコンピューターと、A.リモートオフィスの設定で入力した内容に差異があるとインストールが中断されます。

4 配信サーバーのフォルダーをアンチウイルスソフトの例外として登録します。

続いて、ADと同期する場合は以下の手順を実行します（同期なしでもEndpoint Centralは利用可能です）。

◇ ADドメイン環境では、配信サーバーを設置することでADサーバー（ドメインコントローラー）との同期が可能です。ADサーバーと同期することにより、以下の機能を使用できるメリットがあります。

- パッチの配布対象としてOUを指定
- ADドメインやOUを基にカスタムグループを作成
- ドメインに参加した新規コンピューターにエージェントを自動インストール
- ドメインから離脱したコンピューターでエージェントを自動アンインストール

5 [エージェント]タブへ移動し、左側のメニューから[ドメイン]を開きます。

6 [+ドメインの追加]をクリックし、「Active Directory」を選択し、詳細情報を入力します。*4

パラメーター	値の説明
ドメイン名	コンソール画面上での表示名を入力します。（例）mydomain
ドメインユーザ名	ドメインの管理者権限を持つユーザー名を入力します。
パスワード*2	ドメインの管理者権限を持つユーザーのパスワードを入力します。
ADドメイン名	ADドメインのFQDNを入力します。（例）mydomain.lan
ドメインコントローラー名	配信サーバーからホップ数の小さいドメインコントローラーを指定します。
AD Connector*3	指定したドメインコントローラーと通信可能な配信サーバーを指定します。

7 続いて同期情報時刻を入力したら、ドメイン情報を保存します。

*1「複製ポリシー」で指定した帯域は、クラウドと配信サーバー間の通信およびクラウドとエージェント間の通信に適用されます。配信サーバー・エージェント間の通信には適用されません。

▶ 複製ポリシー
https://www.manageengine.jp/support/kb/Endpoint_Central_Cloud/?p=464
▶ 帯域消費の抑制
https://www.manageengine.jp/support/kb/Endpoint_Central_Cloud/?p=1842

*2 ドメインの資格情報は、ドメイン全体に対して管理者権限を持つ必要があります。資格情報はクラウド上に暗号化して保持され、エージェントのインストールにのみ使用されます。ADと同期する場合、この資格情報の登録が必須です（AD環境でご利用いただく場合、必ずしもADと同期する必要はありません）。
資格情報の入力を避けたい場合、ADと同期しない運用をご検討ください（ADと同期しない場合、Endpoint Central Cloud上ではドメインを同名のワークグループとして扱うことが可能です）。

*3 ADコネクターに設定された配信サーバーは、ADサーバーと定期的に同期します。LDAP SSLを使用して同期する場合は「LDAP SSLを使用する」にチェックを入れます。

*4 ワークグループやEntra IDを登録する場合は、以下のナレッジをご覧ください。また、ドメインに参加/離脱したコンピューターへエージェントを自動インストール/自動アンインストールする場合は、[エージェント]タブ > [配布] > [AD同期設定] または [非アクティブコンピューターポリシー] を設定します。

▶ 通信ポート
https://www.manageengine.jp/support/kb/Endpoint_Central_Cloud/?p=66
▶ AD同期設定
https://www.manageengine.jp/support/kb/Endpoint_Central_Cloud/?p=507
▶非アクティブコンピューターポリシー
https://www.manageengine.jp/support/kb/Endpoint_Central_Cloud/?p=5481
▶ ドメイン/ワークグループの登録
https://www.manageengine.jp/support/kb/Endpoint_Central_Cloud/?p=509

4. エージェントのインストール/デバイスの登録

リモートオフィス（および配信サーバーの設定）が完了したら、Endpoint Central Cloud エージェントを管理対象となるすべてのコンピューターにインストールします。モバイルデバイスについては、デバイスを登録します。

- エージェントのインストールには複数の方法があり、エージェントの一括インストールには**ADグループポリシー（GPO）を利用する方法**のほか、他の資産管理ツール等でエージェントの配布が可能です。特定のインストール方法に問題がある場合は、他の方法をお試しください。
- Linuxエージェントを有効化するには [エージェント] タブ > [エージェント設定] > [Linuxエージェントの設定] を開き、Linuxが所属する既定グループ（デフォルト: linuxosgroup）を選択する必要があります。
- エージェントのインストールの完了には Endpoint Central Cloud との通信が必要です。
- Macエージェントの場合、エージェントのインストール完了後にプロファイルの配布が必要です。
- エージェントのインストールが完了すると [エージェント]タブ > [PC] 上に**「承認待ち」として追加され、承認すると管理対象として登録されます。**この承認ステップをスキップする場合、[エージェント]タブ > [SoM設定] > [Approval Settings] > 「Approval Settings Status」において『Approve all computers by-default』を選択します。（※英語表示は順次日本語化してまいります）
- エージェントのインストール後、エージェントフォルダーを必ずアンチウイルスソフトの例外に設定します。また、エージェントに必要な通信を許可します。
- Windows/Macエージェントに表示される通知を無効化するには、[エージェント]タブ > [エージェント設定] > [エージェントトレイアイコン] を開き、「設定中とパッチスキャン中に、情報バルーンを表示します」のチェックを外して [保存] をクリックします。

▶ サインアップ～セットアップの詳細な手順:
https://www.manageengine.jp/support/kb/Endpoint_Central_Cloud/?p=631

▶ エージェントのインストール方法:
https://www.manageengine.jp/support/kb/Endpoint_Central_Cloud/?p=80

▶ エージェント設定
https://www.manageengine.jp/support/kb/Endpoint_Central_Cloud/?p=138

▶ アンチウイルスソフトの除外登録:
https://www.manageengine.jp/support/kb/Endpoint_Central_Cloud/?p=143

▶ 通信ポート
https://www.manageengine.jp/support/kb/Endpoint_Central_Cloud/?p=66

▶ 通信の許可が必要なドメイン
https://www.manageengine.jp/support/kb/Endpoint_Central_Cloud/?p=21

A.インストーラーの実行（コンピューター）

1 [エージェント]タブへ移動し、左側のメニューから「管理対象」>[PC]を開きます。

2 右上の[エージェントのダウンロード]をクリックし、リモートオフィスおよびプラットフォームを選択して[エージェントのダウンロード]からダウンロードします。

3 インストーラーを実行します。ファイル名は OS およびリモートオフィスによって異なります。

- Windowsの場合: 次のファイルを管理者として実行し、表示される4桁の番号を入力して続行します。

  （例）DefaultRemoteOffice_Agent.exe

  または 、［エージェント］ タブ >「配布」>「エージェントのインストール」>「他の方法」>「コマンドライン」>［エージェントのダウンロード］ より、リモートオフィスを選択してzipファイルをダウンロードします。入手した zip ファイルを展開し、コマンドプロンプト等から次のコマンドを管理者として実行します（サイレントインストール）。

  （例）msiexec /i "UEMSAgent.msi" /qn TRANSFORMS="UEMSAgent.mst" ENABLESILENT=yes REBOOT=ReallySuppress INSTALLSOURCE=Manual DS_ROOT_CRT="%cd%\DMRootCA.crt" /lv "Agentinstalllog.txt

- Macの場合: zipファイルを展開し、管理者として実行します。（例）UEMS_MacAgent.pkg
- Linuxの場合: zipファイルを展開し、実行します。（例）sudo ./UEMS_LinuxAgent.bin

4 エージェントフォルダーをアンチウイルスソフトの例外として登録します。

5 [エージェント]タブ >「管理対象」>「PC」>「承認待ちです」を開き、承認します。

B.グループポリシー(GPO)を利用した配布（コンピューター）

1 [エージェント]タブ > [エージェントインストール]を開き、[GPO] >「エージェントのダウンロード」から、エージェントを所属させるリモートオフィスを選択します。

2 ナレッジの手順に沿ってグループポリシーを構成します。

▶ ドメインのGPOを利用したWindowsエージェントの自動インストール
https://www.manageengine.jp/support/kb/Endpoint_Central_Cloud/?p=80#GPO

3 コンピューターを再起動させます（スタートアップスクリプトにより、エージェントがインストールされます）。(次のページに続きます)

4 エージェントフォルダーをアンチウイルスソフトの例外として登録します。

5 [エージェント]タブ ＞「管理対象」＞「PC」＞「承認待ちです」を開き、承認します。

C.他の資産管理ツール等を使用した配布（コンピューター）

1 [エージェント]タブへ移動し、左側のメニューから[PC]を開きます。

2 右上の[エージェントのダウンロード]をクリックし、リモートオフィスおよびプラットフォームを選択して[エージェントのダウンロード]からダウンロードします。

3 インストールコマンドを入力し、資産管理ツールから配布します。

4 エージェントフォルダーをアンチウイルスソフトの例外として登録します。

5 [エージェント]タブ ＞「管理対象」＞「PC」＞「承認待ちです」を開き、承認します。

▶ 参考：（英語）Installing agents using Microsoft Intune
https://www.manageengine.com/patch-management/help/managing-computers-in-lan.html#install-using-msintune

---

- リモートオフィス間を管理対象コンピューターが移動する場合、「IPスコープ」機能を利用して自動的に通信先が変更されるように設定します。
- リモートオフィスよりも細かくグループ化するには、「カスタムグループ」を作成して対応します。また、一部機能の配布対象には、カスタムグループのみを指定可能です。
- パッチ管理機能をご利用いただく場合で、パッチを本番環境へ配布する前にテスト用端末に配布する「パイロット運用」を実施する場合は、作成したカスタムグループにテスト用端末を所属させ、「テストグループ」として選択します。詳細は「パッチテストと承認設定」ナレッジをご覧ください。
- エージェントはHTTPS通信を使用するため、OSのHTTPS通信に必要な要件（OSの時刻設定が正しいことや、証明書ストアの信頼されたルート証明書が最新であること）を満たす必要があります。

▶ IPスコープ
https://www.manageengine.jp/support/kb/Endpoint_Central_Cloud/?p=462
▶ カスタムグループ
https://www.manageengine.jp/support/kb/Endpoint_Central_Cloud/?p=151
▶ パッチテストと承認設定
https://www.manageengine.jp/support/kb/Endpoint_Central_Cloud/?p=255

D.エージェントのアンインストール（コンピューター）

- エージェントをアンインストールする方法は「エージェントのアンインストール」ナレッジをご覧ください。
- エージェントのアンインストール時に「OTP」（ワンタイムパスワード）の入力を求められた場合は、[エージェント]タブ > [エージェント設定] > [エージェント保護設定] において「ユーザーによるエージェント/配信サーバーのアンインストールを制限する」が有効になっています。[エージェント]タブ > [PC]を開き「ワンタイムパスワードの表示」をクリックして表示される数字を入力するか、または設定を変更して保護設定を無効化します。

▶ エージェントのアンインストール
https://www.manageengine.jp/support/kb/Endpoint_Central_Cloud/?p=446
▶ エージェント設定
https://www.manageengine.jp/support/kb/Endpoint_Central_Cloud/?p=138

E． モバイルデバイスの登録（モバイルデバイス/コンピューター）

- モバイルデバイスの登録方法については、MDMスタートアップガイドをご覧ください。

▶ MDMスタートアップガイド
https://manageengine.jp/sites/default/files/download/DC/dccmdm_startupguide.pdf

- Windows/Macコンピューターに対してリモートワイプ（データの遠隔消去）や位置情報の取得、アプリの配布などの操作を実行するには、ManageEngine Endpoint Central Cloud UEM Edition または Security Edition が必要です。詳細は 11章 トラブルシューティング・お問い合わせ をご覧ください。
- Endpoint Central Cloud UEM Edition または Security Edition においてWindowsコンピューターにエージェントを配布すると、MDMプロファイルが自動的に配布されます（コンソール画面の表示が反映されるには、しばらく時間を要する場合があります）。
- Endpoint Central Enterprise Edition、UEM Edition または Security Edition において Mac コンピューターにエージェントを配布すると、続いて APNs 証明書のアップロードが必要になります。APNs 証明書のアップロードが完了すると MDM プロファイルが配布されるため、各管理対象コンピューターにおいて表示される通知で許可する必要があります。
- Enterprise Editionの場合、MDM プロファイルは一部の構成機能を配布するためにのみ使用され、MDMの機能（リモートワイプや位置情報の取得など）をMacコンピューターで利用することはできません。

▶ APNs証明書の登録
https://www.manageengine.jp/support/kb/Endpoint_Central_Cloud/?p=1462
▶ Mac向け構成配布時の前提条件
https://www.manageengine.jp/support/kb/Endpoint_Central_Cloud/?p=1461

5. パッチ管理機能

パッチ管理機能を使用する場合、管理対象の定義を完了後、続いてパッチ管理機能のセットアップを実行します。

1 [管理]タブを開き、「パッチ設定」>「パッチDBの設定」を開きます。

▶ パッチDBの設定:
https://www.manageengine.jp/support/kb/Endpoint_Central_Cloud/?p=288

2 Endpoint Central Cloud で管理するパッチの種類を Windows, Mac, Linux について選択します。

▶ パッチの種類:
https://www.manageengine.jp/support/kb/Endpoint_Central_Cloud/?p=269

3 運用上、特に必要な場合のみ「更新済みパッチの管理」を有効化します（後から変更も可能）。

▶ 更新済みパッチの管理（パッチ管理機能の仕様変更・機能強化）:
https://www.manageengine.jp/support/kb/Endpoint_Central_Cloud/?p=1862

4 [保存]をクリックします。

5 Macコンピューターが含まれる場合、所定の手順を実行します。

▶ Appleシリコンを搭載するMacへのセキュリティパッチ配布に必要な手順:
https://www.manageengine.jp/support/kb/Endpoint_Central_Cloud/?p=1384

6 [パッチ管理]*1タブ>「システム」> 「システムスキャン」 へ移動します。

7 パッチスキャンを実行するコンピューターにチェックを入れ、［システムスキャン］をクリックし、しばらく待ちます（この操作が「手動スキャン」です）。

8 スキャン完了後、結果が更新されます。（以降、スキャンは定期的に自動実行されます）

セットアップ完了後、管理対象コンピューターでパッチスキャンが実行され、その結果がコンソール画面に反映されます。パッチ管理タブ配下の「ホーム」には全体の情報が表示されるほか、グラフや数字をクリックすることで詳細が表示されます。また、パッチ単位で確認する場合は「パッチ」を、コンピューター単位で確認する場合は「システム」をクリックして開きます。

*1 Security Editionや評価版の利用中は「脅威/パッチ」タブと表示されます。

▶ パッチ管理タブ配下の各ビューについて
https://www.manageengine.jp/support/kb/Endpoint_Central_Cloud/?p=2400

IT管理者は状況を確認し、検出された**「欠落パッチ」**を適用します。どのパッチを配布するかは企業や組織の方針によって異なりますが、基本的には「欠落パッチ」として検出されるパッチを減らすように運用します。

欠落パッチを配布する方法は**「手動配布」**と**「自動配布」**の2通りあり、Windows 11 や Mac などクライアントOSのパッチ管理の自動化を積極的に進めたい場合は「自動配布」を中心に、Windowsの機能更新プログラムやサーバーのパッチなど、パッチを慎重に適用する場合は「手動配布」を中心に構成します。管理対象やパッチの種類に合わせて自動配布と手動配布を組み合わせ、運用方針に合った構成を作成します。

なお、手動配布と自動配布のどちらにおいても、指定した曜日/時間帯に配布を実行できます。時間帯や通知/再起動の実行などを**「配布ポリシー」**で定義し、手動配布や自動配布の構成時に配布ポリシーを一つ選択します。

▶ 手動配布の構成
https://www.manageengine.jp/support/kb/Endpoint_Central_Cloud/?p=281
▶ 自動配布（パッチ配布の自動化）の構成
https://www.manageengine.jp/support/kb/Endpoint_Central_Cloud/?p=266
▶ 配布ポリシーの作成
https://www.manageengine.jp/support/kb/Endpoint_Central_Cloud/?p=115

◇ 特定のアプリケーションを Endpoint Central Cloud の管理対象から除外する場合は、そのアプリケーションをパッチDBの設定において管理対象から除外するか、または「パッチの拒否」を設定します。
◇ 本番環境に適用する前にテスト環境へ適用し、業務への影響を確認するパイロット運用がある場合は、テスト環境となるコンピューターをテストグループに登録し、「パッチテストと承認設定」を構成します。
◇ 機能更新プログラム（Feature Update）の配布を実施する場合は、ナレッジベースにて手順をご確認ください。また、Windowsの月例パッチを配布する場合はWindows Updateを停止し、自動配布などの方法で配布します。
◇ 配布したパッチをアンインストールする場合は、手動配布において「パッチのアンインストール」を選択します。なおベンダーがアンインストールをサポートしているWindowsパッチのみアンインストール可能です。

A．特定のパッチの配布（パッチの手動配布）

手動配布を構成して、特定のパッチを配布します。

1 [パッチ管理]タブ ＞「パッチ」＞「欠落パッチ」（または「適用可能なパッチ」）を開きます。

2 配布するパッチにチェックを入れ、「パッチをインストール/公開する」をクリックします。

3 構成の名前として任意の名前を指定します（デフォルトのままでも構いません）。

4 配布設定にて「配布」を選択し、配布ポリシーを選択します。

5 実行設定にて再試行回数、通知、スケジュールを必要に応じて選択します。

6 「配布」または「今すぐ配布」をクリックします。

B．特定のコンピューターへの欠落パッチの配布（パッチの手動配布）

手動配布を構成して、特定のシステムに対してパッチを配布します。

1. [パッチ管理]タブ ＞ 「システム」 のいずれかのビューを開きます。
2. 欠落パッチをインストールするシステムにチェックを入れ、「欠落パッチのインストール」または「承認済みパッチのインストール」をクリックします。
3. 構成の名前として任意の名前を指定します（デフォルトのままでも構いません）。
4. 配布設定にて「配布」を選択し、配布ポリシーを選択します。
5. 実行設定にて再試行回数、通知、スケジュールを必要に応じて選択します。
6. 「配布」または「今すぐ配布」をクリックします。

C．指定した種類のパッチの自動配布（パッチの自動配布）

自動配布を構成して、指定した種類の欠落パッチを自動的に欠落しているコンピューターに配布します。

1. [パッチ管理]タブ ＞ [配布] ＞ 「パッチ配布の自動化」 を開きます。
2. 「タスクの作成」をクリックし、OSを選択します。
3. 配布するパッチの種類にチェックを入れ、必要に応じてアプリケーションの条件を設定します。
4. 配布設定にて「配布」を選択し、配布ポリシーを選択します。
5. 配布対象のコンピューターを指定します。
6. 必要に応じて通知設定を有効化します。
7. 「保存」をクリックします。
8. 配布するタイミングを指定し、「次へ」をクリックします。
9. 「パッチをインストール/公開する」をクリックします。

その他、セルフサービスポータル経由でのパッチ配布方法があります。詳細は 7章ソフトウェア配布機能 ＞ B. カタログにソフトウェアを公開する（セルフサービスポータル）をご覧ください。パッチの配布後、[ホーム]タブやレポート等で結果を確認します。

▶ パッチ管理機能に関するナレッジ
https://www.manageengine.jp/support/kb/Endpoint_Central_Cloud/?p=1493

6. 資産管理機能

資産管理機能を使用する場合、エージェントのインストール完了後、続いてインベントリスキャンを実行します。
なおモバイルデバイスに関する情報は [モバイルデバイス管理] タブより確認します。

1. [インベントリ]タブ ＞「アクション設定」＞「システムスキャン」を開きます。
2. スキャンを実行するコンピューターにチェックを入れ、［システムスキャン］（または［すべてスキャン］）をクリックします。
3. スケジュールスキャンを実行する場合は、[インベントリ]タブ ＞ 「アクション設定」 ＞ 「スキャンのスケジューラー設定」 を開きます。
4. 「インベントリスキャン」が表示されていることを確認し、[スケジューラーの設定]をクリックします。
5. 実行間隔、開始時刻を指定します。必要に応じて通知メールアドレスを入力します。
6. 「保存」をクリックします。
7. 数分～ 30分程度待つと結果が更新されます。[インベントリ]タブ ＞ ビュー を確認します。
   各コンピューターごとに確認するには「PC」、ハードウェアごとの表示は「ハードウェア」、
   ソフトウェアごとの表示は「ソフトウェア」をクリックします。

インベントリ管理機能には、指定したWindowsソフトウェアの使用時間を計測する「ソフトウェア利用状況測定」や、ライセンスの過不足や期限切れ通知を確認する「ライセンス管理」、条件に応じてアラートメールを管理者に送信する「アラート」などの各機能があります。

▶ インベントリ管理機能に関するナレッジ
https://www.manageengine.jp/support/kb/Endpoint_Central_Cloud/?p=1498
▶ インベントリスキャン
https://www.manageengine.jp/support/kb/Endpoint_Central_Cloud/?p=101
▶ ソフトウェア使用時間の計測
https://www.manageengine.jp/support/kb/Endpoint_Central_Cloud/?p=394
▶ ソフトウェアライセンスの管理
https://www.manageengine.jp/support/kb/Endpoint_Central_Cloud/?p=392
▶ アラート（インベントリアラート）
https://www.manageengine.jp/support/kb/Endpoint_Central_Cloud/?p=397

A.インベントリレポート（定型）

Endpoint Central Cloud がインベントリスキャンを実行して管理対象のコンピューターから取得したデータは、［レポート］タブ >「他のレポート」>「インベントリレポート」から、以下の例のような様々な定型のレポートとして確認できます。

- ディスク使用率の確認
- 搭載メモリーの確認
- Windows 11への互換性のないコンピューターの確認
- BitLocker/FileVaultのステータスの確認

BitLockerの回復キーも確認可能です。［インベントリ］タブ >「ビュー」>「PC」を開き、各コンピューター名 >「セキュリティ」>「リカバリキーのステータス」>「Available」をクリックすると表示されます。なおBitLockerを操作する場合は Endpoint Central Cloud **Security Edition**で利用可能なBitLocker管理機能が必要です。

- アンチウイルスソフトの種類、ステータスの確認
- 期限切れが近い証明書の確認
- 各コンピューターに設定されている共有フォルダーの確認
- 特定の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
- 最近インストールされたソフトウェア
- 指定したWindowsソフトウェアの使用時間（［インベントリ］タブ >「アクション設定」>「ソフトウェア利用状況測定」において設定が必要です）
- ソフトウェアライセンスの過不足状況（［インベントリ］タブ >「アクション設定」>「ライセンス管理」>「ライセンス」において、購入数を手動で登録する必要があります）
- 更新が必要なソフトウェアライセンス（［インベントリ］タブ >「アクション設定」>「ライセンス管理」>「ライセンス」において、ライセンス期限を手動で登録する必要があります）

B.カスタムレポート

定型レポート以外にも、カスタムレポートを作成できます。

1. [レポート]タブ >「ユーザー定義のレポート」>「カスタムレポート」>「新規カスタムレポート」をクリックして開きます。
2. レポートの名前として任意の名前を指定します（デフォルトでも問題ありません）。
3. サブモジュールを選択します。
4. 条件および表示する列を指定して、［実行&保存］または［実行］をクリックします。

7. ソフトウェア配布機能

Endpoint Central Cloud のソフトウェア配布機能を使用して、Windows/Mac/Ubuntu/Debian コンピューターに対して様々な形式のソフトウェアを遠隔インストールできます（Ubuntu/Debian の場合、規定のソフトウェアのみ操作可能です）。サイレントインストールに対応しているWindowsアプリケーションの場合、サイレントインストールを実行しますが、対応していない場合は対話モードでのインストールとなります。
なお、モバイルデバイスに対してアプリをインストールする場合はモバイルデバイス管理（MDM）機能を使用します。

A. パッケージの作成

手動配布を構成して、特定のパッチを配布します。

1. ソフトウェアインストーラーの保管場所である「ソフトウェアリポジトリ」に共有フォルダーを設定する場合、[ソフトウェア配布]タブ ＞「設定」＞「ソフトウェアリポジトリ」 においてパスを指定します（特に設定しない場合はそのまま次の手順へ進みます）。
2. [ソフトウェア配布]タブ ＞ 「パッケージ作成」 ＞ 「パッケージ」 を開きます。
3. 配布するソフトウェアをパッケージ化します。既定のテンプレートから作成可能な場合は「テンプレート」から選択して[パッケージの作成]をクリックします。それ以外の場合は[パッケージの作成]をクリックして手動で作成します。

▶ ソフトウェアパッケージの作成
https://www.manageengine.jp/support/kb/Endpoint_Central_Cloud/?p=80#GPO

B. ソフトウェアの一括配布

手動配布を構成して、特定のパッチを配布します。

1. [ソフトウェア配布]タブ ＞「配布」＞ [ソフトウェアのインストール/アンインストール] をクリックし、Windowsコンピューター / Windowsユーザー / Macコンピューター / Linuxコンピューター から種類を選択します（パッケージによって選択できる形式が異なります）。
2. 構成の名前として任意の名前を指定します（デフォルトでも問題ありません）。
3. 操作の種類としてインストールを指定し、パッケージを選択します。
4. 配布設定にて配布ポリシーを選択します。
5. 配布対象を選択します。
6. 実行設定にて再試行回数、通知、スケジュールを必要に応じて選択します。
7. 「配布」をクリックします。

C．カタログにソフトウェアを公開する（セルフサービスポータル）

セルフサービスポータルにソフトウェアを公開することで、各ユーザーは管理者権限がなくても公開されたソフトウェアをインストールできます。グループごとに異なるソフトウェアを公開可能です。

1. [ソフトウェア配布]タブ ＞「配布」＞「セルフサービスポータル」を開きます。
2. 「パッケージの公開」をクリックし、コンピューターまたはユーザーを選択します。
3. カスタムグループ名を選択します。
4. 作成済みのパッケージ一覧から、そのカスタムグループに公開するソフトウェアをドラッグ&ドロップし、［公開］をクリックします。

▶ ソフトウェア配布機能
https://www.manageengine.jp/support/kb/Endpoint_Central_Cloud/?p=372
▶ セルフサービスポータル
https://www.manageengine.jp/support/kb/Endpoint_Central_Cloud/?p=2092

- セルフサービスポータル経由で配布できるのは、Windowsの場合: ソフトウェア および コンピューターへのパッチの公開、Macの場合: コンピューターへのソフトウェアの公開のみ、Linuxの場合: パッチの公開のみです。
- セルフサービスポータル経由でユーザーがソフトウェアをインストールした場合、その履歴はレポートとして確認できます。レポートタブ ＞ その他のレポート ＞ Self Service Portal Report をご確認ください。
- 管理対象コンピューターにおいてセルフサービスポータルを開くには、Windowsの場合: 通知領域に表示されるエージェントトレイアイコンを右クリック ＞ セルフサービスポータルを選択、 Macの場合: メニューバーのステータスメニューに表示されるエージェントアイコンをクリック ＞ セルフサービスポータルを選択、Linuxの場合: X Window システムにおいて、root権限で StartSelfServicePortal.sh を実行します。なお Windows / Mac においてはスタートメニューやデスクトップ上のショートカットアイコンなどからもアクセス可能です。

8. リモート制御機能

管理対象のWindows / Mac / Linux コンピューターに対して、画面共有による遠隔操作が可能です。また、画面共有をせずにコマンドプロンプトやターミナルを呼び出し、コンソール画面上で直接コマンドを入力することも可能です。また、シャットダウンツール（スケジュール実行も可能）、Wake on LAN ツールに加えて、Windows向けのポップアップメッセージを表示可能なアナウンスツールもリモート制御機能から利用できます。

▶ リモート制御機能
https://www.manageengine.jp/support/kb/Endpoint_Central_Cloud/?p=1490

A. リモートコントロール

1. エージェント側で必要なドメインとの通信が許可されていることを確認します。また、特定のフォルダーがアンチウイルスソフトのスキャン対象から除外されていることを確認します。
2. [ツール]タブ >「リモート制御」を開きます。
3. 接続するコンピューターのアイコンが緑色表示になっていることを確認し、「アクション」列 >[接続] をクリックします。
4. 新規タブでウィンドウが表示され、リモートコントロールが開始されます。
   - ファイルの送受信など各種メニューは左側に表示されます。複数ユーザーで同一コンピューターを制御する場合、操作可能なのは1ユーザーのみです。
5. 切断するときはタブを閉じます。

B. システムマネージャー

1. エージェント側でドメインとの通信が許可されており、また、特定のフォルダーがアンチウイルスソフトのスキャン対象から除外されていることを確認します。
2. [ツール]タブ >「システムマネージャー」を開きます。
3. 接続するコンピューターのアイコンが緑色表示になっていることを確認し、「アクション」列 >[管理] をクリックし、使用するツールを選択します。
4. 新規タブでウィンドウが表示され、システムマネージャーが開始されます。
   - 実行ユーザーを指定する場合、プルダウンから選択します。
5. 切断するときはタブを閉じます。

9. USB 制御機能

管理対象のWindows ユーザー / Windowsコンピューターに対して、USBデバイスの種類ごとに接続を許可または禁止します。また、USBデバイスの「デバイスインスタンスパス」を基準に特定のデバイスのみに使用許可を与えることも可能です。 Mac / Linuxコンピューターに対しては、USBストレージデバイスへの接続を許可/禁止します。

▶ USB制御機能
https://www.manageengine.jp/support/kb/Endpoint_Central_Cloud/?p=1129

1. [構成]タブ >「構成の追加」>「構成」を開きます。
2. 「USB制御」にカーソルを合わせ、ユーザーまたはコンピューターアイコンをクリックします。
3. 構成の名前および説明を入力します。
4. USBデバイスの種類ごとに「変更なし」「ブロック」「ブロック解除」のいずれかを選択します。特定デバイスのみ許可する場合は「ブロック」を選択し、続いて「デバイスを除外する」をクリックして除外デバイスの情報を入力します。
5. 配布対象を選択します。
6. 実行設定にて再試行回数、通知を必要に応じて選択します。
7. 「配布」（または「今すぐ配布」）をクリックします。
8. リフレッシュサイクルのタイミングで構成が適用されます（今すぐ配布の場合は即時）。
9. ブロックを解除する場合は、構成タブ>「ビュー」>「すべての設定」を開き、配布したUSB制御の構成をゴミ箱に移動します。

- USBデバイスのデバイスインスタンスパスは、デバイスのプロパティから確認可能です。なお、一部の種類のデバイスは一意のデバイスインスタンスパスを持たないため、個別の制御ができません。
- USB制御機能は、Endpoint Central Cloudの「構成」機能の一部です。通常の構成では、一度作成した構成を解除する場合、以前の設定内容を打ち消すような構成を配布する必要がありますが、USB制御機能に関しては、以前配布した構成をゴミ箱に移動するだけで解除可能です。

Endpoint Central Cloud **Security Edition** にアップグレードすると、Windows / Macコンピューターに対して、より柔軟なUSBデバイスの使用制限を設定できます。

▶ エディションごとの機能差異
https://www.manageengine.jp/support/kb/Endpoint_Central_Cloud/?p=1586

10. その他の機能

Endpoint Central Cloud では、ほかにも様々な機能をご利用いただけます。

- **構成機能**: Windows/Mac/Linuxコンピューターの設定を一括配布します（OSにより利用可能な機能が異なります）。スクリプトの実行やファイルの配布、レジストリ編集などにも対応しています。

- **OS配布機能**: Windowsコンピューターのマスターイメージを作成し、クローニングを実行します。（現在、OS配布機能は日本語によるサポートの対象外とさせていただいております。サポート開始までお待ちください。）

- **モバイルデバイス管理（MDM）機能:** iOS/iPadOS/Android/Chrome OS といったモバイルデバイスやWindows/Macコンピューターを対象に、アプリの配布や機能制限の適用、リモート制御、位置情報の取得、遠隔からのデータの削除（リモートワイプ）などの機能を利用できます。
なお、Windows/Mac コンピューターに対してモバイルデバイス管理機能を使用する場合、Endpoint Central Cloud UEM Editionが必要です（Enterprise Editionではご利用いただけません）。

- **レポート機能:** Endpoint Central Cloud の持つ情報をPDF/CSV/XLS形式で出力します。定期的なメール送信やカスタマイズも可能です。情報の保持期間は 30～750 日まで指定可能です。

- **アクションログビューア機能:** Endpoint Central Cloudコンソールの操作履歴やエージェントのインストール/アンインストール情報を表示します。情報の保持期間は 30～750 日まで指定可能です。

▶ 構成管理機能/USBデバイス制御機能に関するナレッジ
https://www.manageengine.jp/support/kb/Endpoint_Central_Cloud/?p=379
▶ OS配布機能に関するナレッジ
https://www.manageengine.jp/support/kb/Endpoint_Central_Cloud/?p=1140
▶ MDM機能に関するナレッジ
https://www.manageengine.jp/support/kb/Endpoint_Central_Cloud/?p=1774

また、以下の機能は Endpoint Central Cloud **Security Edition** にてご利用可能です。
（Enterprise Edition / UEM Edition ではご利用いただけません）。

- **脆弱性管理機能、デバイス制御機能、Webブラウザー制御機能、アプリケーション制御機能、BitLocker管理機能**（DLP機能は今後実装予定です）

以下の機能をご利用いただくには、オプションライセンスが必要です。

- **ランサムウェア対策機能、マルウェア対策機能**（DEX機能は今後実装予定です）

▶ エディションごとの機能差異
https://www.manageengine.jp/support/kb/Endpoint_Central_Cloud/?p=1586

11. トラブルシューティング・お問い合わせ

ご不明な点はドキュメントをご参照いただくか、またはお問い合わせください。

▶ Endpoint Central Cloud ナレッジベース （「トラブルシューティング」カテゴリーをご覧ください）
https://www.manageengine.jp/support/kb/Endpoint_Central_Cloud/

お問い合わせ

サポートをご利用の場合、以下をご確認ください（評価期間中とご購入後で窓口が異なります）。

▶ 評価版のサポート	https://www.manageengine.jp/support/trial.html
▶ 製品ご購入後のサポート	https://www.manageengine.jp/support/purchased.html
▶ お問い合わせ前のご確認事項	https://www.manageengine.jp/support/for-smooth-inquiry.html

［評価版について］

・ご導入にあたっては、ご利用環境に依存する問題の確認のため、ご購入前に評価版による検証をお願いいたします。

・評価版は Endpoint Central Cloud の全機能が有効化されており、最上位の Security Edition と同じ機能を利用可能です。他のEdition（Enterprise Edition / UEM Edition）を製品版としてご購入予定の場合、機能差異がある場合がございます。実際に購入予定のEditionと同じ機能でのご評価を希望される場合は、営業担当までお問い合わせください。

▶ エディションごとの機能差異
https://www.manageengine.jp/support/kb/Endpoint_Central_Cloud/?p=1586

・製品のご購入（ライセンスのご契約）をしていただきますと、当社にてライセンス有効化の処理を実施いたします。これにより、評価版として利用していた環境をそのまま引き続き製品版としてご利用いただけます。

・評価版のご利用期間は初回サインアップから30日間です。ライセンスを契約しない場合、評価期間終了後は保守サポートがご利用いただけない無料版に移行します。製品ご利用を終了する場合、エージェントのアンインストールをお願いいたします。

・ライセンスのご購入/ご変更については以下営業担当へお問い合わせください。

・製品機能や操作方法など、ご不明な点がございましたら、上記サポートへお問い合わせください。

［製品版について］

・Endpoint Central Cloud は、Enterprise Edition/UEM Edition/Security Editionの3種類について日本語でのサポートに対応しております。

・日本語でのサポートをご希望の場合、原則として日本法人からのご購入が必要です（代理店経由 または クレジットカード決済）。また日本円での決済をご希望の場合も、日本法人へお問い合わせください。

［オンプレミス版製品について］

・Endpoint Central は、インターネット接続のない環境でもご利用いただけるオンプレミス版製品もご用意しております。要件に応じてオンプレミス版・クラウド版をお選びください。

製品提供元

ゾーホージャパン株式会社

神奈川県横浜市西区みなとみらい 3-6-1 みなとみらいセンタービル13階

TEL：045-319-4612（ManageEngine 営業担当）

Webサイト：https://www.manageengine.jp/products/Endpoint_Central/

E-mail：jp-mesales@zohocorp.com