Trend Micro Apex Central™

Patch 8

インストールガイド

エンドポイント向けセキュリティの一元管理

※注意事項

複数年契約について

・お客さまが複数年契約（複数年分のサポート費用前払い）された場合でも、各製品のサポート期間については、当該契約期間によらず、製品ごとに設定されたサポート提供期間が適用されます。

・複数年契約は、当該契約期間中の製品のサポート提供を保証するものではなく、また製品のサポート提供期間が終了した場合のバージョンアップを保証するものではありませんのでご注意ください。

・各製品のサポート提供期間は以下の Web サイトからご確認いただけます。

https://success.trendmicro.com/dcx/s/solution/000207383?language=ja

法人向け製品のサポートについて

・法人向け製品のサポートの一部または全部の内容、範囲または条件は、トレンドマイクロの裁量により随時変更される場合があります。

・法人向け製品のサポートの提供におけるトレンドマイクロの義務は、法人向け製品サポートに関する合理的な努力を行うことに限られるものとします。

著作権について

本ドキュメントに関する著作権は、トレンドマイクロ株式会社へ独占的に帰属します。トレンドマイクロ株式会社が事前に承諾している場合を除き、形態および手段を問わず、本ドキュメントまたはその一部を複製することは禁じられています。本ドキュメントの作成にあたっては細心の注意を払っていますが、本ドキュメントの記述に誤りや欠落があってもトレンドマイクロ株式会社はいかなる責任も負わないものとします。本ドキュメントおよびその記述内容は予告なしに変更される場合があります。

商標について

TRENDMICRO、TREND MICRO、ウイルスバスター、InterScan、INTERSCAN VIRUSWALL、InterScanWebManager、InterScan Web Security Suite、PortalProtect、Trend Micro Control Manager、Trend Micro MobileSecurity、VSAPI、Trend Park、Trend Labs、Network VirusWall Enforcer、Trend Micro USB Security、InterScan Web Security Virtual Appliance、InterScan Messaging Security Virtual Appliance、Trend Micro Reliable Security License、TRSL、Trend Micro Smart Protection Network、SPN、SMARTSCAN、Trend Micro Kids Safety、Trend Micro Web Security、Trend Micro Portable Security、Trend Micro Standard Web Security、Trend Micro Hosted Email Security、Trend Micro Deep Security、ウイルスバスタークラウド、スマートスキャン、Trend Micro Enterprise Security for Gateways、Enterprise Security for Gateways、Smart Protection Server、Deep Security、ウイルスバスター ビジネスセキュリティサービス、SafeSync、Trend Micro NAS Security、Trend Micro Data Loss Prevention、Trend Micro オンラインスキャン、Trend Micro Deep Security Anti Virus for VDI、Trend Micro Deep Security Virtual Patch、SECURE CLOUD、Trend Micro VDI オプション、おまかせ不正請求クリーンナップサービス、Deep Discovery、TCSE、おまかせインストール・バージョンアップ、Trend Micro Safe Lock、Deep Discovery Inspector、Trend Micro Mobile App Reputation、Jewelry Box、InterScan Messaging Security Suite Plus、おもいでバックアップサービス、おまかせ！スマホお探しサポート、保険&デジタルライフサポート、おまかせ！迷惑ソフトクリーンナップサービス、InterScan Web Security as a Service、Client/Server Suite Premium、Cloud Edge、Trend Micro Remote Manager、Threat Defense Expert、Next Generation Threat Defense、Trend Micro Smart Home Network、Retro Scan、is702、デジタルライフサポート プレミアム、Air サポート、Connected Threat Defense、ライトクリーナー、Trend Micro Policy Manager、フォルダシールド、トレンドマイクロ認定プロフェッショナルトレーニング、Trend Micro Certified Professional、TMCP、XGen、InterScan Messaging Security、InterScan Web Security、Trend Micro Policy-based Security Orchestration、Writing Style DNA、Securing Your Connected World、Apex One、Apex Central、MSPL、TMOL、TSSL、ZERO DAY INITIATIVE、Edge Fire、Smart Check、Trend Micro XDR、Trend Micro Managed XDR、OT Defense Console、Edge IPS、スマスキャ、Cloud One、Cloud One - Workload Security、Cloud One - Conformity、ウイルスバスター チェック！、Trend Micro Security Master、Worry-Free XDR、Worry-Free Managed XDR、Network One、Trend Micro Network One、らくらくサポート、Service One、超早得、

先得、Trend Micro One、Workforce One、Security Go、Dock 365、TrendConnect、TREND MICRO FORUM、トレンドマイクロ知恵袋、Trend Cloud One、Trend Service One、および Accelerating You は、トレンドマイクロ株式会社の登録商標です。

本ドキュメントに記載されている各社の社名、製品名およびサービス名は、各社の商標または登録商標です。

Copyright © 2023 Trend Micro Incorporated. All rights reserved.

P/N: APEM89862/231117_JP (2023/12)

目次

はじめに

はじめに 1
ドキュメント 2
対象読者 3
ドキュメントの表記規則 3
用語 4

第 1 章：Apex Central の概要

Apex Central について 2
主な機能と利点 2
Apex Central アーキテクチャ 4

第 2 章：インストールの計画

インストール形態の決定 8
集中管理について 8
管理下の製品およびエンドポイントの数を決定する 9
サーバと管理下の製品の最適な比率を計画する 9
Apex Central サーバを指定する 9
分散管理について 10
管理下の製品をグループ化する 11
拠点数の決定 11
管理下の製品およびエンドポイントの数を決定する .. 12
サーバと管理下の製品の最適な比率を計画する 12
Apex Central サーバを指定する 12
Apex Central サーバのインストール場所を決定する .. 13
ネットワークトラフィックの計画 13
Apex Central のセットアップの流れ 14
テストインストール 15
テストインストールの準備 15
テストサイトの選定 16

テストインストールの開始 16
テストインストールの評価 16
サーバの配置計画 16
管理計画について 16
Apex Central サーバの配置について 17
単一サーバによる運用 18
複数サーバによる運用 18
ネットワークトラフィックの計画 18
Apex Central のネットワークトラフィックについて 18
ネットワークトラフィックの発生元 19
トラフィックの発生間隔 19
ログ 19
管理下の製品エージェントの接続ステータス 19
ネットワークプロトコル 20
ネットワークトラフィックの発生元 20
ログのトラフィック 20
Trend Micro Management Communication Protocol ポリシー 21
製品登録によるトラフィック 22
ポリシーの配信 23
アップデートの配信 23
データベースの計画 24
データベースの推奨設定 24
ODBC ドライバ 26
認証 26
Web サーバの設定 26

第 3 章：インストール

システム要件 30
Apex Central サーバをインストールする 35
Apex Central のインストールの流れ 36
すべての必須コンポーネントのインストール 36
インストール先の指定 40

製品とサービスのアクティベーション 41
Apex Central の Web サーバ設定を指定する 42
バックアップ設定の指定 44
root アカウントをセットアップする 46
データベース情報の設定 47

第 4 章：インストール後のタスク

インストール後の自動タスク 52
サーバのインストールまたはアップグレードを確認する 52
製品のアクティベーション 53
Apex Central のアクティベーションを実行する 54
製品版へのアップグレード 54
Active Directory 接続を設定する 55
ユーザアカウントの設定 58
最新コンポーネントのダウンロード 58
イベント通知を設定する 59

第 5 章：アップグレードと移行

Apex Central にアップグレードする 62
アップグレードがサポートされているバージョン 62
移行前にバックアップするサーバファイル 63
移行前のチェックリスト 63
アップグレードと移行のシナリオ 64
アップグレードの流れ 65
シナリオ 1: Control Manager サーバを Apex Central へアップグレードする 65
既存の Control Manager サーバとデータベースをバックアップしてアップグレードする 66
サーバの OS 全体と Apex Central データベースをバックアップしてアップグレードする 66
シナリオ 2: エージェント移行ツールを使用して Apex Central の新規インストールへ移行する 67
Control Manager サーバを Apex Central の新規インストールに移行する 67

Apex Central エージェントの移行を計画する 68
一括アップグレード 68
段階的アップグレード 68
Apex Central データベースを移行する 69
Apex Central SQL データベースを他の SQL Server に移行する 69
データベース設定ツールを使用する (DBConfig.exe) .. 69

第 6 章：移行後のタスク

成功したアップグレードまたは移行を確認する 72
Apex Central に Apex One サーバ設定を移行する 72
アプリケーションコントロールを有効にする 74
仮想パッチを有効にする 75
Endpoint Sensor を有効にする 77
Endpoint Sensor 向けに Apex One サーバを設定する 79

第 7 章：アンインストール

Apex Central のアンインストール 84
Apex Central を手動でアンインストールする 85
Apex Central アプリケーションをアンインストールする . 86
Apex Central サービスを停止する 86
Windows のサービス画面から Apex Central サービスを停止する 86
コマンドプロンプトから Apex Central および IIS サービスを停止する 87
Apex Central の IIS 設定を削除する 87
Apex Central のファイル/ディレクトリおよびレジストリキーを削除する 88
データベースコンポーネントの削除 89
Apex Central の ODBC 設定を削除する 89
SQL Server 2017 Express データベースを削除する 90
Apex Central サービスを削除する 90

第 8 章：Apex Central のシステムチェックリスト

サーバアドレスのチェックリスト 92
ポートのチェックリスト 93
Apex Central 入力規則 93
コアプロセスおよび設定ファイル 94
通信ポートおよびサービスポート 96

索引

索引 97

はじめに

はじめに

『Trend Micro Apex Central™インストールおよびアップグレードガイド』にようこそ。このドキュメントでは、Apex Central サーバをインストールしたり、以前のインストールからアップグレードしたりするための要件と手順について説明しています。

このセクションの内容:

ドキュメント

Apex Central のドキュメントには、次の情報が含まれます。

ドキュメント	説明
Readme ファイル	既知の問題の一覧が含まれます。また、オンラインヘルプや印刷ドキュメントにまだ収録されていない最新の製品情報が含まれる場合があります。
インストールおよびアップグレードガイド	Apex Central をインストールするための要件や手順を説明する PDF ドキュメント 注意 マイナーリリースバージョン、Service Pack、またはパッチでは、インストールおよびアップグレードガイドを利用できない場合があります。
管理者ガイド	Apex Central と管理下の製品の設定および管理方法に加えて、Apex Central の概要と機能の説明が記載された PDF ドキュメント
オンラインヘルプ	操作手順、使用のアドバイス、および目的別の作業手順を提供する、WebHelp 形式でコンパイルされた HTML ファイル。このヘルプは、Apex Central 管理コンソールからもアクセスできます。
ウィジェットおよびポリシー管理ガイド	Apex Central でのダッシュボードウィジェットおよびポリシー管理の設定方法の説明 このガイドを参照するには、https://docs.trendmicro.com/ja-jp/documentation/article/trend-micro-apex-central-2019-widget-and-policy-management-guide-preface-(wpg)_001 にアクセスしてください。
Automation Center	Apex Central のオートメーション API の使用方法を説明したオンラインユーザガイドとレファレンス: https://automation.trendmicro.com/apex-central/home
製品 Q&A	問題解決およびトラブルシューティング情報のオンラインデータベース。既知の製品の問題についての最新情報を提供します。製品 Q&A にアクセスするには、https://success.trendmicro.com/dcx/s/?language=ja を参照してください。

PDF ドキュメントおよび Readme の最新バージョンをダウンロードするには、次の Web サイトにアクセスしてください。

http://docs.trendmicro.com/ja-jp/enterprise/apex-central.aspx

対象読者

このドキュメントは、次のユーザを対象としています。

- Apex Central の管理者: Apex Central のインストール、設定、および管理を担当し、高度なネットワークおよびサーバ管理の知識を持っていることが求められます。
- 管理下の製品の管理者: Apex Central と統合されているトレンドマイクロ製品の管理を担当し、高度なネットワークおよびサーバ管理の知識を持っていることが求められます。

ドキュメントの表記規則

このドキュメントでは、次の表記規則を使用しています。

表 1. ドキュメントの表記規則

表記	説明
注意	設定上の注意
ヒント	推奨事項
重要	必須の設定や初期設定、および製品の制限事項に関する情報
警告!	避けるべき操作や設定についての注意

用語

次の表は、Apex Central 付属のドキュメントで使用されている用語を示しています。

用語	説明
管理者 (または Apex Central 管理者)	Apex Central サーバを管理しているユーザ
セキュリティエージェント	エンドポイントにインストールされている管理下の製品プログラム
コンポーネント	セキュリティリスクの検索、検出、および処理を実行するもの
Apex Central 管理コンソールまたは Web コンソール	Apex Central のアクセス、設定、および管理を実行するための Web ベースのユーザインタフェース 注意 統合された管理下の製品のコンソールは、管理下の製品名で示されます。たとえば、Apex One Web コンソールなどです。
管理下のエンドポイント	管理下の製品であるセキュリティエージェントがインストールされているエンドポイント
管理下の製品	Apex Central と統合されるトレンドマイクロ製品
管理下のサーバ	管理下の製品がインストールされているエンドポイント
サーバ	Apex Central サーバがインストールされているエンドポイント
セキュリティリスク	ウイルス、不正プログラム、スパイウェア、グレーウェア、および Web からの脅威の総称
製品サービス	Microsoft 管理コンソール (MMC) を使用してホストされる Apex Central サービス
デュアルスタック	IPv4 アドレスと IPv6 アドレスの両方のアドレスを持つエンティティ

用語	説明
IPv4 シングルスタック	IPv4 アドレスのみを持つエンティティ
IPv6 シングルスタック	IPv6 アドレスのみを持つエンティティ

第 1 章

Apex Central の概要

本章では、Trend Micro Apex Central™について説明し、その機能の概要を示します。

次のトピックがあります。

- 2 ページの「Apex Central について」
- 2 ページの「主な機能と利点」
- 4 ページの「Apex Central アーキテクチャ」

Apex Central について

Trend Micro Apex Central™は、トレンドマイクロの製品およびサービスを、ゲートウェイ、メールサーバ、ファイルサーバ、およびデスクトップの各レベルで集中管理するための Web ベースのコンソールです。管理者は、ポリシー管理機能を使用して製品設定を行い、管理下の製品やエンドポイントに配信できます。Apex Central の Web ベースの管理コンソールにより、ネットワーク全体のウイルス対策およびコンテンツセキュリティ製品やサービスを 1 か所で監視できます。

Apex Central により、システム管理者は感染、セキュリティ違反、ウイルス/不正プログラムの検出ポイントなどの活動を監視し、報告できるようになります。システム管理者は、パターンファイル、検索エンジン、スパムメール判定ルールなどのコンポーネントをダウンロードし、ネットワーク全体に配信することにより、最新の保護を確実に行うことができます。Apex Central では、手動アップデートと予約アップデートの両方が可能です。また、さらに柔軟性を高めるため、グループまたは個人として製品の設定や管理ができるようになっています。

主な機能と利点

Apex Central には、次の機能と利点があります。

機能	利点
Active Directory の統合	Apex Central では複数の Active Directory フォレストとの統合がサポートされ、ユーザだけでなく Active Directory グループもインポートできます。さらに、Active Directory Federation Services (ADFS) 認証を有効にすることで、Extranet 全体で提携ビジネスパートナーのユーザまたはグループが Apex Central ネットワークに安全にログオンできるようにすることができます。
ダッシュボード	[ダッシュボード] タブとウィジェットを使用すると、脅威の検出、コンポーネントのステータス、ポリシー違反などに関する、管理下の製品と Apex Central の情報を幅広く確認できます。
セキュリティ状態	[セキュリティ状態] タブを使用すると、パターンファイルと情報漏えい対策のコンプライアンスのステータス、重大な脅威の検出、およびネットワーク上で解決済みのイベントと未解決のイベントに関する情報をすぐに確認できます。

機能	利点
ユーザ/エンドポイントディレクトリ	Apex Central ネットワーク内のすべてのユーザとエンドポイント、およびセキュリティの脅威の検出に関する詳細情報が表示されます。
製品ディレクトリ	システム管理者は、管理下の製品に対して設定の変更を即座に配信したり、ウイルス/不正プログラムの大規模感染発生時であっても Apex Central 管理コンソールから手動検索を実行したりできます。
ポリシー管理	システム管理者は、ポリシーを使用して単一の管理コンソールから管理下の製品とエンドポイントに製品を設定および配信し、組織内で一貫したウイルス/不正プログラム対策ポリシーおよびコンテンツセキュリティポリシーを実施できます。
ログ	単一の管理コンソールを使用して、個々の製品コンソールにログオンすることなく、登録済みのすべての管理下の製品の統合されたログを確認できます。
イベント通知	メール、Windows の Syslog、SNMP トラップ、アプリケーションによって通知が送信されるように Apex Central を設定することで、管理者はネットワークイベントを常に把握できます。
レポート	カスタムテンプレートまたはデフォルトテンプレートから包括的なレポートを作成すると、ネットワーク保護とセキュリティコンプライアンスの実現に必要な実用的な情報を入手できます。
コンポーネントアップデート	パターンファイル、スパムメール判定ルール、検索エンジン、およびその他のウイルス対策/コンテンツセキュリティコンポーネントを安全にダウンロードおよび配信して、すべての管理下の製品を最新の状態にします。
Connected Threat Defense	Apex Central では、トレンドマイクロのさまざまな製品やソリューションを統合することで、標的型攻撃や高度な脅威を検出して分析し、被害が拡大する前に対処することができます。
安全な通信インフラストラクチャ	Apex Central には、SSL (Secure Socket Layer) プロトコルに基づいた通信インフラストラクチャが使用されており、認証を使用してメッセージを暗号化することもできます。
役割ベースの管理	特定の Web コンソール権限を管理者に割り当て、特定のタスクを実行するために必要なツールと権限だけを提供することにより、Apex Central 管理コンソールへのアクセス権の付与と管理を実行します。

機能	利点
コマンド追跡	コマンド追跡を使用すると、Apex Central 管理コンソールを使用して実行されたコマンド (パターンファイルの更新やコンポーネントの配信など) が正常に完了したかどうかを継続的に監視できます。
ライセンス管理	新しいアクティベーションコードを配信するか、管理下の製品の既存のアクティベーションコードを再アクティベートします。
セキュリティエージェントのインストール	Apex One または Apex One (Mac) 向けのセキュリティエージェントのインストールパッケージを、Apex Central 管理コンソールから直接ダウンロードします。
2 要素認証	2 要素認証はユーザアカウントの安全性を強化します。そのためには、ユーザは Apex Central にログオンするために、Google Authenticator アプリで生成された認証コードを入力する必要があります。
ブラウザのサポート	このバージョンの Apex Central では、以下がサポートされています。 • Microsoft™ Internet Explorer™ • Microsoft™ Edge™ • Google™ Chrome™

Apex Central アーキテクチャ

Trend Micro Apex Central™は、トレンドマイクロの製品やサービスを 1 か所から集中管理する機能を提供します。Apex Central を使用することにより、企業におけるウイルス/不正プログラム対策ポリシーやコンテンツセキュリティポリシーを一貫して実施できます。

次の表は、Apex Central が使用するコンポーネントについて説明しています。

コンポーネント	説明
Apex Central サーバ	エージェントから収集したすべてのデータを保存する格納先として機能します。Apex Central サーバでは次の機能が提供されます。 • 管理下の製品の設定やログを保存する SQL データベース Apex Central は、ログ、管理下の製品の情報、ユーザアカウント、ネットワーク環境、通知設定などのデータの保存に Microsoft SQL Server データベース (`db_ApexCentral.mdf`) を使用します。 • Apex Central の Web コンソールをホストする Web サーバ • メールメッセージでイベントに関する通知を送信するメールクライアント Apex Central は、個々の受信者または受信者グループに Apex Central システム内で発生したイベントに関する通知を送信します。メール、SNMP トラップ、Syslog、または組織が通知の送信に使用する組織内のアプリケーションまたは業界標準のアプリケーションを使用して、イベントに関する通知を送信します。 • ウイルス対策/コンテンツセキュリティ製品に関するレポートを生成するレポートサーバ Apex Central レポートは、Apex Central ネットワークで発生したセキュリティの脅威およびコンテンツセキュリティ関連イベントのデータをオンラインで収集します。
Trend Micro Management Communication Protocol (MCP)	MCP は、Apex Central サーバと次世代エージェントをサポートする管理下の製品間の通信を処理します。 MCP は管理下の製品と共にインストールされ、一方向または双方向通信を使用して Apex Central と通信します。MCP エージェントは、Apex Central に対して、指示とアップデートをポーリングします。
Web サービスの統合通信	Apex Central と管理下の製品との通信を可能にするエージェントレスの統合モデル

コンポーネント	説明
Web ベースの管理コンソール	このコンソールにより、管理者はインターネット接続と Web ブラウザを利用して、すべてのコンピュータから Apex Central を管理できるようになります。 Apex Central 管理コンソールは、Microsoft Internet Information Server (IIS) を経由してインターネット上に公開され、Apex Central サーバのサービスを提供する Web ベースのコンソールです。管理者は、対応する Web ブラウザがインストールされた任意のコンピュータから、Apex Central システムを管理できるようになります。
ウィジェットフレームワーク	管理者はウィジェットフレームワークを使用して、Apex Central システムを監視するためにカスタマイズしたダッシュボードを作成できます。

第 2 章

インストールの計画

本章では、Apex Central の配置計画の作成とテストインストールの実施について説明します。

次のトピックがあります。

- 8 ページの「インストール形態の決定」
- 14 ページの「Apex Central のセットアップの流れ」
- 15 ページの「テストインストール」
- 16 ページの「サーバの配置計画」
- 18 ページの「ネットワークトラフィックの計画」
- 20 ページの「ネットワークトラフィックの発生元」
- 23 ページの「アップデートの配信」
- 24 ページの「データベースの計画」
- 26 ページの「Web サーバの設定」

インストール形態の決定

Apex Central サーバをネットワーク環境に戦略的に分散して、ウイルス対策/コンテンツセキュリティ製品を適切に管理するためのインストール形態を決定します。

Apex Central のような企業規模のクライアント/サーバ統合管理製品をネットワークに導入するためには、入念な計画と評価が必要になります。

計画を容易に作成できるように、次の 2 種類のインストール形態を推奨します。

- 集中管理 — メインオフィスにある 1 つの Apex Central から、サーバ、管理下の製品、およびエンドポイントを管理します。組織が複数のオフィスを持っていても、拠点間に高速で信頼性の高いローカルおよびワイドエリアネットワーク接続がある場合は、集中管理を適用できます。
- 分散管理 — 地理的に離れた複数のメインオフィスがある組織において、複数の Apex Central サーバから管理します。

集中管理について

集中管理では、メインオフィスにある 1 つの Apex Central から、サーバ、管理下の製品、およびエンドポイントを管理します。

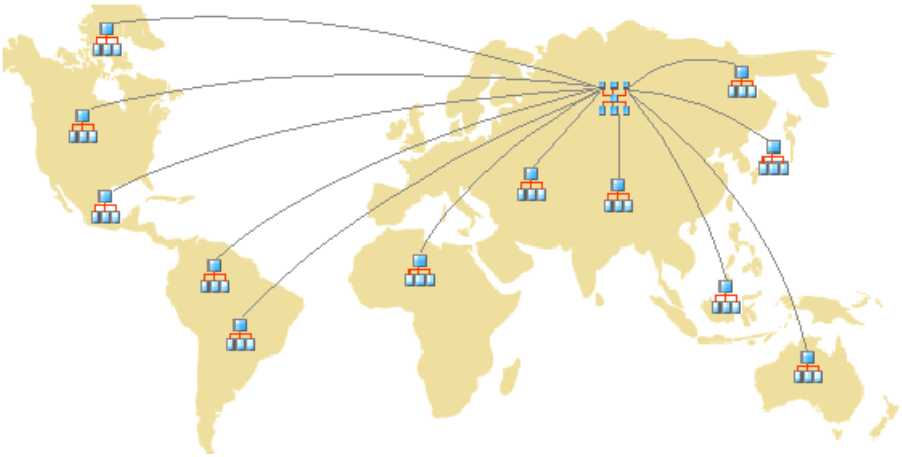

図 2-1. 単一の Apex Central サーバを使用した集中管理

Apex Central の集中管理を実施する前に、次のタスクを実行する必要があります。

1. 管理下の製品およびエンドポイントの数の決定
2. サーバ、管理下の製品、エンドポイントの最適な比率の計画
3. Apex Central サーバの指定

管理下の製品およびエンドポイントの数を決定する

Apex Central で管理しようとする、管理下の製品およびエンドポイントの構造の数を決定します。この情報は、最適な通信や管理のために配置すべき Apex Central サーバの種類と数、またそれらのサーバをネットワーク上のどこに配置するのかを決定する上で必要になります。

サーバと管理下の製品の最適な比率を計画する

1 台の Apex Central サーバで管理可能な、ローカルネットワーク上の管理下の製品およびエンドポイントの数を決定する上で最も重要な要素は、エージェントとサーバ間の通信です。

Apex Central システムの CPU および RAM の要件を決める際には、システム要件を参考にしてください。

Apex Central サーバを指定する

管理下の製品およびエンドポイントの数に基づいて、Apex Central サーバを決定および指定します。

さらに、Windows サーバの中から、Apex Central サーバとして設定するものを選択します。専用サーバをインストールする必要があるかどうかについても検討します。

Apex Central,をインストールするサーバを選択するときは、次の点を考慮します。

- CPU 負荷
- サーバが実行している他の機能

アプリケーションサーバなどの他の用途にも使用されているサーバに Apex Central をインストールする場合、基幹アプリケーションやリソースを大量に

消費するアプリケーションを実行中していないサーバへのインストールを推奨します。

各ネットワークの構成に応じて、上記以外に処置すべきことが発生する場合もあります。

分散管理について

集中管理と同様に、関連するネットワーク情報を収集して、この情報が Apex Central サーバの分散管理にどのように関わるかを判別する必要があります。

それぞれのネットワークの特性を考慮して、Apex Central サーバの最適な数を決定してください。

DMZ や専用ネットワークを含む、さまざまな場所に Apex Central サーバを配置できます。インターネットを介して管理下の製品、エンドポイント、またはその他のサーバを管理し、Apex Central Web コンソールにアクセスするには、公開されたネットワーク上の DMZ に Apex Central サーバを配置します。

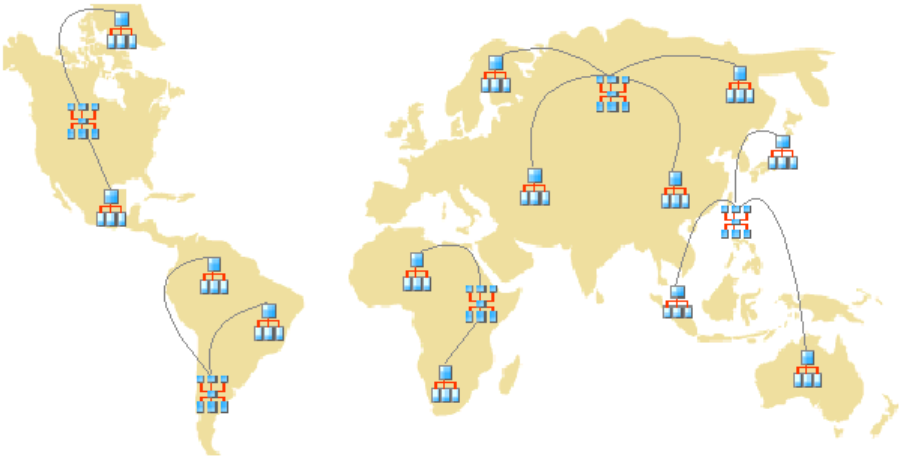

図 2-2. 複数の Apex Central サーバを使用した分散管理

分散管理においては次の点を考慮します。

- 管理下の製品、エンドポイント、またはサーバのグループ化
- 拠点数の決定
- 管理下の製品、エンドポイント、およびサーバの数の決定
- ネットワークトラフィックの計画
- Apex Central サーバのインストール場所の決定

管理下の製品をグループ化する

管理下の製品をグループ化する場合、次の点に注意してください。

表 2-1. 管理下の製品のグループ化に関する注意点

注意点	説明
社内のネットワークポリシーおよびセキュリティポリシー	社内のネットワークにアクセス権や共有権を適用する場合、社内のネットワークポリシーとセキュリティポリシーに従って管理下の製品、エンドポイント、およびサーバをグループ化します。
組織と機能	会社の組織上および機能上の分割に従って、管理下の製品、エンドポイント、およびサーバをグループ化します。たとえば、2 台の Apex Central サーバで製品グループとテスト担当グループを管理します。
所在地	管理下の製品、エンドポイント、およびサーバの位置が Apex Central サーバと管理下の製品、エンドポイント、またはサーバ間の通信に影響する場合には、グループ化の判断基準として地理的な位置を考慮します。
管理責務	管理下の製品、エンドポイント、およびサーバを、それぞれのシステムまたはセキュリティの担当者に合わせてグループ化します。これにより、グループ設定が可能になります。

拠点数の決定

Apex Central 配置内の拠点の数を決定します。この情報は、インストールが必要なサーバの数とサーバのインストール先を決定する上で必要になります。

以上の情報は、組織の WAN または LAN 構成図を基にします。

管理下の製品およびエンドポイントの数を決定する

Apex Central で管理しようとする、管理下の製品およびエンドポイントの総数についても知る必要があります。拠点ごとに、管理下の製品およびエンドポイントの総数に関するデータを収集することをお勧めします。この情報を取得できない場合は、概算の数でも役立ちます。この情報は、インストールするサーバの数を決定する上で必要になります。

サーバと管理下の製品の最適な比率を計画する

WAN 上に Apex Central を配置する場合、メインオフィスの Apex Central サーバによって、リモートオフィスの管理下の製品、エンドポイント、およびその他のサーバが管理されます。WAN を経由して Apex Central サーバに接続する場合、リモートオフィスの管理下の製品、エンドポイント、およびサーバがそれぞれ必要とするネットワーク帯域幅が異なる場合があります。Apex Central では、管理下の製品、エンドポイント、およびサーバのうち、早く接続したものが優先されます。

Apex Central システムの CPU および RAM の要件を決める際には、システム要件を参考にしてください。

Apex Central サーバを指定する

管理下の製品およびエンドポイントの数に基づいて、Apex Central サーバを決定および指定します。

さらに、Windows サーバの中から、Apex Central サーバとして設定するものを選択します。専用サーバをインストールする必要があるかどうかについても検討します。

Apex Central,をインストールするサーバを選択するときは、次の点を考慮します。

- CPU 負荷
- サーバが実行している他の機能

アプリケーションサーバなどの他の用途にも使用されているサーバに Apex Central をインストールする場合、基幹アプリケーションやリソースを大量に消費するアプリケーションを実行していないサーバへのインストールを推奨します。

Apex Central サーバのインストール場所を決定する

クライアントの数とインストールが必要なサーバの数を把握した後に、次に Apex Central サーバのインストール先を決定します。メインオフィスにすべてのサーバをインストールする必要があるか、一部をリモートオフィスにインストールする必要があるかを判断します。

通信の速度を高め、管理下の製品、エンドポイント、およびサーバを最も効果的に管理するためには、環境内の特定の場所に戦略的にサーバを配置します。

- メインオフィス —メインオフィスとは、組織内の管理下の製品、エンドポイント、およびサーバの大部分が配置されている施設です。メインオフィスは、「本社」、「本店」などとも呼ばれます。メインオフィスは、他の場所に小規模なオフィスや支店を持つこともあります。ここでは、「リモートオフィス」と呼びます。

  ヒント

  メインオフィスにサーバをインストールすることをお勧めします。

- リモートオフィス —リモートオフィスは、大規模な組織の一部である小規模で専門的なオフィスのことで、メインオフィスとの WAN 接続があります。リモートオフィスの管理下の製品、エンドポイント、またはサーバから中央オフィスの Control Manager サーバにレポートが送信される場合、この Control Manager サーバへの接続が難しい場合があります。帯域幅の制限により、Apex Central サーバと適切に通信できない場合があります。

  メインオフィスとリモートオフィス間のネットワーク帯域幅が、設定の変更の通知やステータスの送信といったルーチン的なクライアント/サーバ通信には十分でも、コンポーネント配信や他の作業には不十分である場合があります。

ネットワークトラフィックの計画

Apex Central では、サーバと管理下の製品/エンドポイントの通信時にネットワークトラフィックが発生します。組織のネットワークへの影響を最小限に抑えるように、Apex Central のネットワークトラフィックを計画します。

Apex Central 関連のネットワークトラフィックの発生元として、次のものがあります。

- 接続ステータス
- ログ
- Apex Central サーバへの管理下の製品の登録

  初期設定では、Apex Central サーバには、リリース時の製品情報が含まれます。しかし、新バージョンの製品を Apex Central に登録するときに、そのバージョンが既存の製品プロファイルに対応しない場合は、その新しい製品の製品情報が Apex Central サーバにアップロードされます。

  製品プロファイルがない新しいトレンドマイクロ製品の場合、Apex Central がこの製品を識別できるようにトレンドマイクロからアップデートが配信されます。
- 最新コンポーネントのダウンロードと配信
- ポリシーの配信
- 不審オブジェクトの同期

Apex Central のセットアップの流れ

Apex Central システムのセットアップには、次の作業に関連する複数の手順が必要です。

1. Apex Central システムのインストールの計画 (サーバの分散、ネットワークトラフィック、データストレージ、および Web サーバの検討)
2. Apex Central サーバのインストール

注意

Apex Central サーバのインストール時に、バックアップおよび復元ファイルの場所を指定します。

テストインストール

テストインストールによって、各機能がどのように動作するか、完全な導入後にどのようなレベルのサポートが必要になるかを判断するためのフィードバックを得ることができます。

ヒント

全面的にインストールする前に、限定的な環境で試験的にインストール (テストインストール) することを推奨します。

Apex Central のテストインストールにより、次のことを実現できます。

- Apex Central および管理下の製品に対する理解
- 社内のネットワークポリシーの策定または改善

テストインストールは、改良の必要な設定箇所を判断するために便利です。これにより、IT 部門またはインストールチームは導入手順を事前に実践して改善したり、組織の業務上の要件を満たすかどうかを確認する機会を得ることができます。

Apex Central のテストインストールを行うには、次のタスクを実行します。

- テストインストールの準備
- テストサイトの選定
- テストインストールの開始
- テストインストールの評価

テストインストールの準備

準備段階では、次の処理を完了します。

手順

1. テスト環境における、Apex Central サーバとエージェントの構成を決定します。
   - テスト構成におけるすべてのシステム間で TCP/IP 接続を確立させます。

- Control Manager システムから各エージェントシステムに、またその逆方向に ping コマンドを発行することにより、双方向の TCP/IP 通信を確認します。

2. どのような配置が環境に適しているかを知るために、さまざまな配置方法を評価します。
3. テストインストールに使用するシステムチェックリストに記入します。

テストサイトの選定

実際の稼働環境に類似したテスト用のサイトを選定します。構成をできる限り実稼働環境に近い形に近づけます。

テストインストールの開始

準備作業とシステムチェックリストの記入が完了したら、Apex Central サーバとエージェントをインストールし、テストインストールを開始します。

テストインストールの評価

試験の開始から終了までに確認された成功点と失敗点のリストを作成します。潜在的な問題を特定し、導入を成功させるための対応策を検討します。

このテスト評価計画は、実際のインストールおよび配置計画全体に組み込むことができます。

サーバの配置計画

サーバの配置を計画するときは次の点を考慮します。

- 管理モデル
- Apex Central サーバの配置
- 単一サーバによる運用
- 複数サーバによる運用

管理計画について

Apex Central の配信の初期段階で、Apex Central サーバへのアクセスを許可するユーザ数を決定しておきます。ユーザの数は、管理をどの程度集中させ

るかによって異なります。集中化の度合いは、ユーザ数と反比例するという法則を考慮してください。

次の管理モデルのいずれかに従います。

- 集中管理計画 —集中管理モデルでは、Apex Central へのアクセス権を必要最低限のユーザにのみ与えます。高度な集中管理においては、管理者は 1 人だけです。ネットワーク上のウイルス対策サーバやコンテンツセキュリティサーバはすべて、1 人の管理者によって管理されます。

  集中管理では、ネットワーク上のウイルス対策ポリシーやコンテンツセキュリティポリシーの管理が最も厳密になります。しかし、ネットワークが複雑になるに従って、管理者の作業負荷が大きくなり、1 人では対応できなくなる可能性があります。

- 分散管理計画 —この計画は、システム管理者の責任範囲が明確に定義、確立されている大規模なネットワークの場合に便利です。たとえば、メールサーバ管理者がメール関連のウイルス対策製品を担当したり、ある支店の管理者がその支店全体のウイルス対策を担当するというように、製品別や拠点別に責任を分担します。

  分散管理モデルを選択した場合でも、Apex Central の主となる管理者を設定する必要がありますが、管理者間で責任を分担することができます。

  各管理者には、担当する製品や拠点の設定のみを表示したり変更できるように権限を与えます。

上記のいずれかの管理モデルを土台とし、製品ディレクトリと必要なユーザアカウントを設定することによって Apex Central ネットワークを管理することができます。

Apex Central サーバの配置について

Apex Central は実際のインストール場所に関係なく製品を管理できます。したがって、1 つの Apex Central サーバからすべてのウイルス対策製品やコンテンツセキュリティ製品を管理することができます。

しかし、Apex Central ネットワークの管理を何台かのサーバ間で分割する方が好都合な場合もあります。各ネットワークの特徴に基づいて、Apex Central サーバの最適な数を決定する必要があります。

単一サーバによる運用

単一サーバによる運用は、中小規模の、1 つのサイトからなる企業に適しています。このトポロジでは、1 人の管理者による管理が容易になりますが、管理計画に応じて必要とされる追加の管理者アカウントを作成することも可能です。

さらに、この構成では、エージェントによるポーリング、データ転送、アップデート配信などのネットワークトラフィック負荷が 1 つのサーバ、およびこのサーバを収容する LAN に集中します。ネットワークの規模が拡大すると、パフォーマンスへの影響も大きくなります。

複数サーバによる運用

複数の拠点からなる大規模な企業では、Apex Central サーバを地域ごとに設置して、ネットワーク負荷を分散しなければならない場合があります。

Apex Central システムで発生するトラフィックの詳細については、18 ページの「Apex Central のネットワークトラフィックについて」を参照してください。

ネットワークトラフィックの計画

ネットワークへの Apex Central の影響を最小限に抑える計画を作成するには、Apex Central システムで発生するトラフィックについて理解することが重要です。

ここでは、Apex Central システムで発生するネットワークトラフィックを理解し、ネットワークに負荷のかからない運用を計画するために必要な情報について説明します。さらに、トラフィックの発生間隔に関する項では、Apex Central システム上にトラフィックを頻繁に生じさせる発生元について説明します。

Apex Central のネットワークトラフィックについて

ネットワークへの Apex Central の影響を最小限に抑える計画を作成するには、Apex Central システムで発生するトラフィックについて理解することが重要です。

ネットワークトラフィックの発生元

Apex Central のネットワークトラフィックを生じさせる発生元を次に示します。

- ログのトラフィック
- MCP ポリシー
- 製品登録
- 最新コンポーネントのダウンロードと配信
- ポリシー設定の配信

トラフィックの発生間隔

Apex Central ネットワークでは、次の要因によりトラフィックが頻繁に発生します。

- 管理下の製品によって生成されたログ
- MCP ポーリングおよびコマンド

ログ

管理下の製品は、それぞれのログの設定に従ったさまざまな間隔で Apex Central にログを送信します。

管理下の製品エージェントの接続ステータス

初期設定では、管理下の製品のエージェントは 60 分ごとに接続ステータスメッセージを送信します。管理者はこの値を 5 分から 480 分までの間で指定することができます。コミュニケータ接続ステータスの実行間隔を指定するときは、ステータス情報の更新頻度と、システムリソースの消費の抑制の両方を考慮する必要があります。

多くの場合、初期設定で十分な結果が得られますが、これらの設定を変更する必要がある場合には、次の点を考慮してください。

- 長い間隔の接続ステータス (60 分以上) —接続ステータスの実行間隔を長く設定するほど、Apex Central サーバの管理コンソールにステータスが表示されるまでに発生するイベントの数が多くなります。

たとえば、次の送信時間に達するまでの間にエージェントとの接続の問題が解決された場合、ステータスが「停止中」または「異常」と表示されていたとしても、エージェントとの通信が回復している可能性があります。

- 短い間隔の接続ステータス (60 分未満) —接続ステータスの実行間隔を短く設定すると、Apex Central サーバの管理コンソールに、より最新のステータスが表示されるようになります。ただし、短い間隔の接続ステータスの場合、消費されるネットワークの帯域幅が増加します。

注意

間隔を 15 分以下に設定したい場合には、まず既存のネットワークトラフィックを調べて、ネットワーク帯域幅の使用が増えることによる影響について理解する必要があります。

ネットワークプロトコル

Apex Central の通信は、主に UDP プロトコルと TCP プロトコルに基づいて行われます。

ネットワークトラフィックの発生元

ログのトラフィック

Apex Central サーバと管理下の製品間には、常に「製品ログ」によるネットワークトラフィックが発生します。製品ログは、各管理下の製品が Apex Central サーバに対して定期的に送信するログです。

表 2-2. Apex Central ログのトラフィック

ログの種類	含まれる情報
ウイルス/スパイウェア/グレーウェアのログ	検出されたウイルス/不正プログラム、スパイウェア/グレーウェアなどのセキュリティ上の脅威
セキュリティログ	コンテンツセキュリティ製品から報告された違反
Web セキュリティ	Web セキュリティ製品から報告された違反

ログの種類	含まれる情報
イベントログ	コンポーネントのアップデート、一般的なセキュリティ違反などのイベント
ステータス	管理下の製品の環境。この情報は製品ディレクトリのステータス概要ページに表示されます。
ネットワークウイルス	ネットワークパケット内で検出されたウイルス
パフォーマンス測定	旧バージョンの製品で使用
URL アクセス	Web セキュリティ製品から報告された違反
セキュリティ違反	Network VirusWall 製品から報告された違反
セキュリティ遵守	Network VirusWall 製品から報告されたエンドポイントのセキュリティ遵守
セキュリティ統計	Network VirusWall 製品から計算、報告されたクライアントのセキュリティ遵守数とセキュリティ違反数の差異
エンドポイント	Web セキュリティ製品から報告された違反
情報漏えい対策ログ	情報漏えい対策ポリシー違反に関連した検出
挙動監視ログ	悪意あるアクティビティを挙動に基づいて検出
ネットワーク検査ログ	IP アドレスまたはドメインの検出を含む
機械学習型検索ログ	機械学習型検索の検出
仮想アナライザログ	不審なサンプルの送信について仮想アナライザによって報告された検出
ファイルハッシュ検出ログ	ファイルまたはファイル SHA-1 不審オブジェクトによってトリガされた検出

Trend Micro Management Communication Protocol ポリシー

Trend Micro Management Communication Protocol (MCP) は、Apex Central の通信用コンポーネントです。MCP は次のポリシーを適用します。

- MCP 接続ステータス —Apex Central への MCP 接続ステータスにより、Apex Central に最新の情報が表示されるようにし、管理下の製品と Apex Central サーバ間の接続が正常に保たれます。
- MCP コマンドポーリング — MCP エージェントが Apex Central へのコマンドポーリングを開始すると、Apex Central はエージェントに管理下の製品のログを送信するよう通知するか、管理下の製品にコマンドを発行します。また、Apex Central ではコマンドポーリングを、Apex Central と管理下の製品の間の接続を確認するパッシブな接続ステータスとして解釈します。

製品登録によるトラフィック

製品情報は、特定の製品をどのように管理するかに関する情報を Apex Central に提供します。管理下の製品をはじめて Apex Central サーバに登録するときに、製品情報はサーバに送信されます。

製品情報は製品ごとにあり、通常、複数のバージョンがある製品の場合、バージョン別の製品情報があります。製品情報には次の情報が含まれます。

- カテゴリ (ウイルス対策など)
- 製品名
- 製品バージョン
- メニューバージョン
- ログ形式
- コンポーネント情報 — この製品で使用されるコンポーネントの情報 (パターンファイルなど)
- コマンド情報

初期設定では、Apex Central サーバには、Web サービスの統合通信を使用する管理下の製品のすべての製品プロファイルが含まれています。Trend Micro Management Communication Protocol (MCP) を使用する管理下の製品は、Apex Central サーバへの初期登録中に製品プロファイルをアップロードします。

ポリシーの配信

Apex Central では、管理下の製品およびエンドポイントへのポリシー設定の配信時にネットワークトラフィックが発生します。このトラフィックの発生元は次のとおりです。

- 定期的なポリシー適用

  Apex Central では、24 時間ごとに管理下の製品およびエンドポイントにポリシー設定が適用されます。

- 配信済みの情報

  1 つのポリシーには、各エンドポイントのグローバル一意識別子 (GUID) 情報と設定情報が含まれます。50,000 の対象と設定一式が含まれる 1 つのポリシーによって、最大 1.8MB のネットワークトラフィックが発生する可能性があります。

アップデートの配信

Apex Central ネットワークのアップデートは 2 つの手順で実施されます。

1. トレンドマイクロから最新コンポーネントを取得します。

   Apex Central で、トレンドマイクロのアップデートサーバから直接または別の場所からコンポーネントをダウンロードできます。

2. これらのコンポーネントを管理下の製品に配信します。

   Apex Central で、次のコンポーネントを管理下の製品に配信できます。

   - パターンファイル/クリーンナップテンプレート
   - 各種エンジン (検索エンジン、ダメージクリーンナップエンジン)
   - スパムメール判定ルール
   - Apex One プラグインマネージャプラグインプログラム
   - 製品プログラム (製品によって異なる)

ヒント

トレンドマイクロでは、管理下の製品が新たなウイルスの脅威に対応できるよう、それらのコンポーネントを定期的にアップデートすることをお勧めします。製品プログラムのアップデートについては、それぞれの製品のマニュアルを参照してください。

管理下の製品へのコンポーネントの配信によって、帯域幅が多く消費されます。可能な場合は、ネットワークへの影響が最小限に抑えられる時間帯に配信することが重要です。

配信計画を使用して、コンポーネントをスケジュールに従って配信することができます。

また、Apex Central サーバと管理下の製品とのネットワーク接続がアップデートに対処できることを確認します。接続は、ネットワークに必要な Apex Central サーバの数を決定する際に考慮される要素です。

データベースの計画

Apex Central のデータは SQL データベースに格納する必要があります。Apex Central がインストールされているサーバに専用のデータベースがない場合、インストールプログラムから Microsoft SQL Express をインストールするためのオプションが提示されます。ただし、SQL Express の制約により、大規模なネットワークでは SQL Server を使用する必要があります。

注意

Apex Central は SQL Server へのアクセスに、SQL Server 認証と Windows 認証を使用します。

データベースの推奨設定

ここでは、1 台のコンピュータに Apex Central と SQL Server の両方をインストールする場合の管理者向けの推奨設定を説明します。

- 実稼働環境

- 10GB を超える空きディスク容量があるコンピュータを使用します。

  注意

  Apex Central のインストールに必要な最小空きディスク容量は 10GB ですが、推奨されるのは 80GB です。Apex Central と SQL Server を同じコンピュータにインストールする際は、少なくとも 80GB の空きディスク容量を確保しておくことをお勧めします。

- SQL Server で使用される最大メモリを設定します。

  Apex Central とシステムで使用するためのメモリを少なくとも 8GB 残します。

  たとえば、コンピュータのメモリが 80GB の場合、SQL Server の最大メモリ使用量を 72GB に設定します。この場合、Apex Central とシステムで 8GB のメモリを使用できます。

- テスト環境

  Apex Central とシステムで使用するためのメモリを少なくとも 8GB 残します。

注意

SQL Server のメモリ使用量を設定する方法の詳細については、https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/server-memory-server-configuration-options を参照してください。

ヒント

- 1,000 を超える製品 (Apex One セキュリティエージェントや ServerProtect 一般サーバを含む) を管理する Apex Central では、専用の SQL Server を使用することを推奨します。
- Apex Central と SQL Server が異なるコンピュータにインストールされている場合は、両方のコンピュータに同じタイムゾーンを設定します。
- Microsoft SQL Server Standard または Enterprise Edition の使用を強く推奨します。SQL Express はテスト目的には適していますが、実稼働環境には向いていません。

ODBC ドライバ

Apex Central は、Microsoft SQL Server 通信および Transport Layer Security (TLS) 1.2 をサポートするために、Open Database Connectivity (ODBC) Driver 13 for SQL Server をインストールします。

認証

Apex Central は、SQL データベース認証と Windows 認証の両方をサポートします。

Web サーバの設定

Apex Central セットアッププログラムの [Web サーバ情報の指定] 画面では、Web サーバをホスト名、FQDN、IP アドレスのいずれかで指定します。Web サーバ名を決定する上での考慮事項は、次と同じです。

- ホスト名または FQDN を使用すると、Apex Central サーバの IP アドレスの変更に容易に対応できますが、システムは DNS サーバに依存するようになります。
- IP アドレスを使用する場合、固定 IP アドレスが必要です。

この Web サーバアドレスを使用し、コンポーネントのアップデートサーバを識別します。この情報は `SystemConfiguration.xml` ファイルに保存され、Apex Central サーバからアップデートを取得できるようにエージェントへの

通知の一部に含められます。アップデートサーバに関連する設定は次のように記述されます。

```
Value=http://<Web サーバのアドレス>:<ポート>/TvcsDownload/
ActiveUpdate/<コンポーネント>
```

ここでは次を意味します。

- ポート —アップデート元に接続するポート。Web サーバアドレス画面で指定することもできます。初期設定のポート番号は 80 です。
- TvcsDownload/ActiveUpdate —Apex Central セットアッププログラムは、対応するこの仮想ディレクトリを IIS 指定の Web サイトに作成します。
- コンポーネント —アップデートされたコンポーネントに応じて異なります。たとえば、パターンファイルがアップデートされる場合、ここには次の値が含められます。

  ```
  Pattern/Vsapixxx.zip
  ```

  「Pattern」は、Control Manager サーバの¥¥. . .Control Manager¥WebUI¥download¥activeupdate¥pattern フォルダに対応します。「Vsapi.zip」は圧縮形式でのウイルスパターンです。

第 3 章

インストール

本章では、Trend Micro Apex Central (以下、Control Manager) サーバのインストール方法について説明します。また、インストール後の設定や、製品のアクティベーション手順についても説明します。

次のトピックがあります。

- 30 ページの「システム要件」
- 35 ページの「Apex Central サーバをインストールする」

システム要件

Apex Central は Windows Server 上で動作し、インストールするには Windows の特定の機能と更新プログラムが必要です。また、Apex Central には、サポートされるバージョンの Microsoft SQL Server、8 GB 以上の RAM、10 GB 以上の使用可能な空きディスク容量も必要です。

- すべてのシステム要件およびサポートされる Windows Server および Microsoft SQL Server のバージョンについては、Apex Central システム要件 PDF ドキュメントを https://docs.trendmicro.com/ja-jp/documentation/apex-central/からダウンロードしてください。
- 管理下の製品とセキュリティエージェントの詳細なシステム要件については、管理下の製品のドキュメントを参照してください。

次の表は、Apex Central インストールプログラムの実行に必要な、Windows Server の最小要件をまとめたものです。

- 31 ページの Windows Server 2012
- 32 ページの Windows Server 2012 R2
- 33 ページの Windows Server 2016
- 34 ページの Windows Server 2019
- 34 ページの Windows Server 2022

注意

- 次の Windows の更新プログラムは Windows Update では自動的にインストールされませんが、Apex Central をインストールする前に各 OS に必須です。
  - KB2999226
  - KB2919355
  - KB2919442
- 次の Windows の更新プログラムは、個々の OS で TLS 1.2 をサポートする場合に限り必要です。
  - KB2975331
  - KB3000850

表 3-1. Windows Server 2012

項目	要件
エディション (Service Pack は不要)	• Standard • Datacenter
プロセッサ	• 2.3 GHz 以上の Intel™ Core™ i5 または互換性のある CPU • AMD™ 64 プロセッサ • Intel™ 64 プロセッサ
RAM	• 8 GB 以上
使用可能な空きディスク容量	• 10 GB 以上 • 80GB 推奨 (SAS)

項目	要件
Windows の機能	• Microsoft IIS 8.0 • Microsoft IIS Windows 認証 • Microsoft IIS ASP • Microsoft IIS ASP.NET 4.5 • Microsoft IIS ASP.NET 拡張性 4.5 • Microsoft IIS CGI • メッセージキュー
Windows の更新プログラム	• KB2999226 • KB2975331

表 3-2. Windows Server 2012 R2

項目	要件
エディション (Service Pack は不要)	• Standard • Datacenter
プロセッサ	• 2.3 GHz 以上の Intel™ Core™ i5 または互換性のある CPU • AMD™ 64 プロセッサ • Intel™ 64 プロセッサ
RAM	• 8 GB 以上
使用可能な空きディスク容量	• 10 GB 以上 • 80GB 推奨 (SAS)
Windows の機能	• Microsoft IIS 8.5 • Microsoft IIS Windows 認証 • Microsoft IIS ASP • Microsoft IIS ASP.NET 4.5 • Microsoft IIS ASP.NET 拡張性 4.5 • Microsoft IIS CGI • メッセージキュー

項目	要件
Windows の更新プログラム	• KB2919355 • KB2919442 • KB3000850

表 3-3. Windows Server 2016

項目	要件
エディション (Service Pack は不要)	• Standard • Datacenter
プロセッサ	• 2.3 GHz 以上の Intel™ Core™ i5 または互換性のある CPU • AMD™ 64 プロセッサ • Intel™ 64 プロセッサ
RAM	• 8 GB 以上
使用可能な空きディスク容量	• 10 GB 以上 • 80GB 推奨 (SAS)
Windows の機能	• Microsoft IIS 10.0 • Microsoft IIS Windows 認証 • Microsoft IIS ASP • Microsoft IIS ASP.NET 4.6 • Microsoft IIS ASP.NET 拡張性 4.6 • Microsoft IIS CGI • メッセージキュー
Windows の更新プログラム	• N/A

表 3-4. Windows Server 2019

項目	要件
エディション (Service Pack は不要)	• Standard • Datacenter
プロセッサ	• 2.3 GHz 以上の Intel™ Core™ i5 または互換性のある CPU • AMD™ 64 プロセッサ • Intel™ 64 プロセッサ
RAM	• 8 GB 以上
使用可能な空きディスク容量	• 10 GB 以上 • 80GB 推奨 (SAS)
Windows の機能	• Microsoft IIS 10.0 • Microsoft IIS Windows 認証 • Microsoft IIS ASP • Microsoft IIS ASP.NET 4.7 • Microsoft IIS ASP.NET 拡張性 4.7 • Microsoft IIS CGI • メッセージキュー
Windows の更新プログラム	• N/A

表 3-5. Windows Server 2022

項目	要件
エディション (Service Pack は不要)	• Standard • Datacenter
プロセッサ	• 2.3 GHz 以上の Intel™ Core™ i5 または互換性のある CPU • AMD™ 64 プロセッサ • Intel™ 64 プロセッサ
RAM	• 8 GB 以上

項目	要件
使用可能な空きディスク容量	• 10 GB 以上 • 80GB 推奨 (SAS)
Windows の機能	• Microsoft IIS 10.0 • Microsoft IIS Windows 認証 • Microsoft IIS ASP • Microsoft IIS ASP.NET 4.8 • Microsoft IIS ASP.NET 拡張性 4.8 • Microsoft IIS CGI • メッセージキュー
Windows の更新プログラム	• N/A

Apex Central サーバをインストールする

Apex Central のインストール計画を作成したら、Control Manager サーバのインストールを開始できます。

92 ページの「サーバアドレスのチェックリスト」を確認してください。このリストにはインストールに必要なシステム関連情報を記録することができます。

インストールには次の情報が必要です。

- 関連するサーバアドレスとポート情報
- Apex Central アクティベーションコード
- サーバ/エージェント間の通信で使用するセキュリティのレベル

データベースに関連して、あらかじめ次の情報を確認してください。

- Apex Central で SQL Server を使用するかどうか。Apex Central サーバと異なるサーバに SQL Server がある場合は、そのサーバの IP アドレス、FQDN (Fully Qualified Domain Name)、または NetBIOS 名が必要です。SQL Server のインスタンスが複数存在する場合は、使用するインスタンスについての情報が必要です。

- Apex Central で使用する SQL データベースの認証情報
  - ユーザ名
  - パスワード

注意

Apex Central では SQL Server へのアクセスに、Windows 認証または SQL Server 認証を使用できます。

- Apex Central が扱う管理下の製品の数。サーバ上に SQL Server が検出されない場合、Apex Central は SQL Server 2017 Express をインストールします。SQL Server Express では、一定の数の接続しか扱うことができません。

Apex Central のインストールの流れ

Apex Central をインストールするには、次の手順を実行する必要があります。

1. すべての必須コンポーネントをインストールします。
2. インストール先を指定します。
3. 製品およびサービスを登録し、アクティベーションを実行します。
4. バックアップ設定を指定します。
5. root アカウントを設定します。
6. データベース情報を設定します。

ヒント

Trend Micro では、新規インストールではなく、最新バージョンの Apex Central にアップグレードすることを推奨しています。

すべての必須コンポーネントのインストール

手順

1. サーバで Apex Central のインストールプログラムを実行します。

インストールプログラムにより、システム上の必須コンポーネントのチェックが行われます。

- .Net Framework 4.6.1 以降がまだインストールされていない場合は、手順 2 に進んでください。
- .Net Framework 4.6.1 以降がすでにインストールされている場合は、手順 3 に進んでください。

2. [同意する] をクリックして Microsoft のライセンス条項に同意し、[インストール] をクリックして、フレームワークをインストールします。

   インストールプログラムにより、.NET Framework 4.6.1 がインストールされます。

   注意

   不足しているコンポーネントをインストールした後にサーバを再起動することが必要になる場合があります。

3. インストールを続行するには [はい] をクリックします。

[ようこそ] 画面が表示されます。

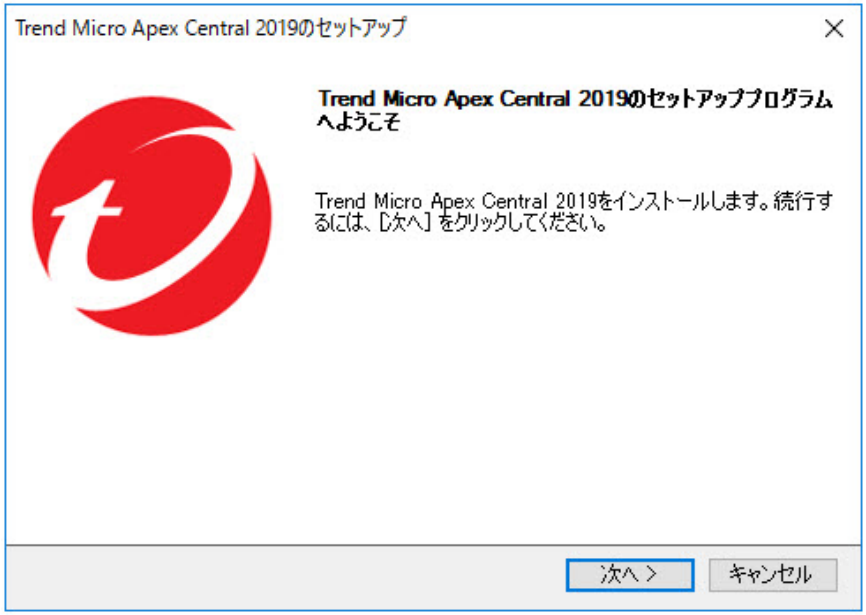

図 3-1. [ようこそ] 画面

インストールプログラムにより、システム上に現在あるコンポーネントのチェックが行われます。インストールを進める前に、Microsoft 管理コンソール (MMC) のすべてのインスタンスを停止します。

4. [次へ] をクリックします。

ソフトウェア使用許諾契約書の画面が表示されます。

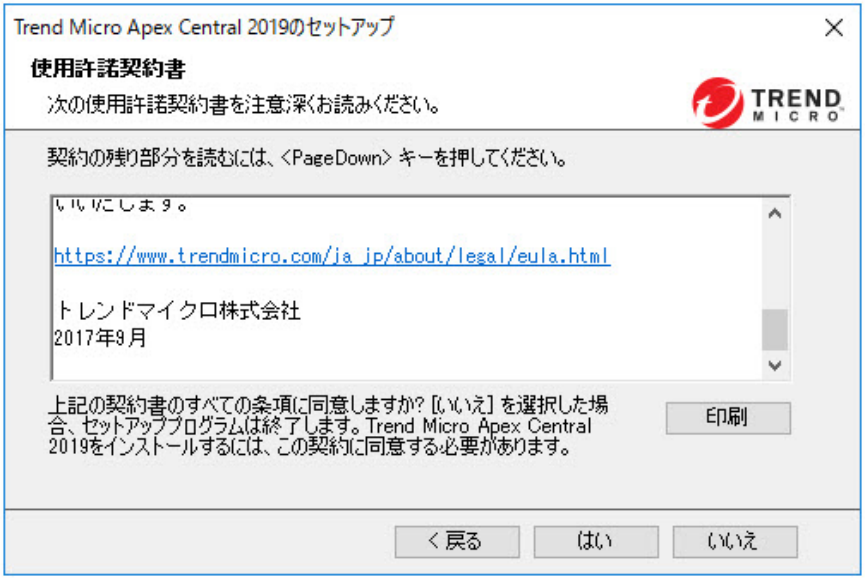

図 3-2. 契約事項の同意

5. 使用許諾契約書の条件を読み、以下のいずれかを選択します。
   - 契約事項に同意しない場合は [いいえ] をクリックします。

     インストールが中止されます。
   - インストールを続行する場合は [はい] をクリックします。

     ローカルシステム環境の解析画面が表示されます。

注意

SQL Server データベースがまだインストールされていない場合、インストールプログラムは手順の最後に Microsoft SQL Server 2017 Express をインストールします。

詳細については、47 ページの「データベース情報の設定」を参照してください。

インストール先の指定

手順

1. [次へ] をクリックします。

   [インストール先フォルダの選択] 画面が表示されます。

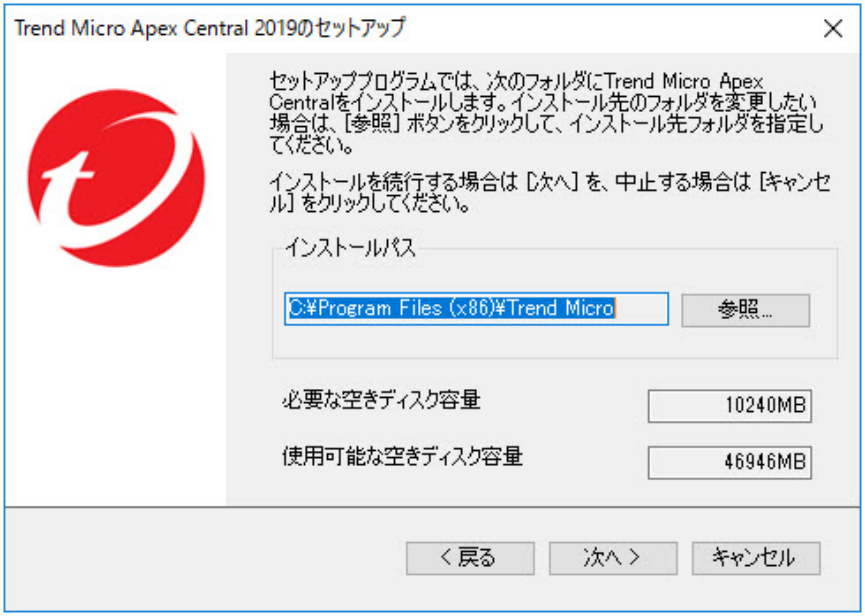

図 3-3. インストール先フォルダの選択

2. Apex Central のインストールディレクトリを指定します。別の場所を指定するには、[参照] をクリックします。

注意

- 64 ビット OS の初期設定では、`C:¥Program Files (x86)¥Trend Micro` にインストールされます。
- 初期設定以外のディレクトリを選択した場合でも、Apex Central の通信 (MCP) 関連のファイルは `Program Files` フォルダ内の既定の場所にインストールされます。

製品とサービスのアクティベーション

手順

1. [次へ] をクリックします。

[製品のアクティベーション] 画面が表示されます。

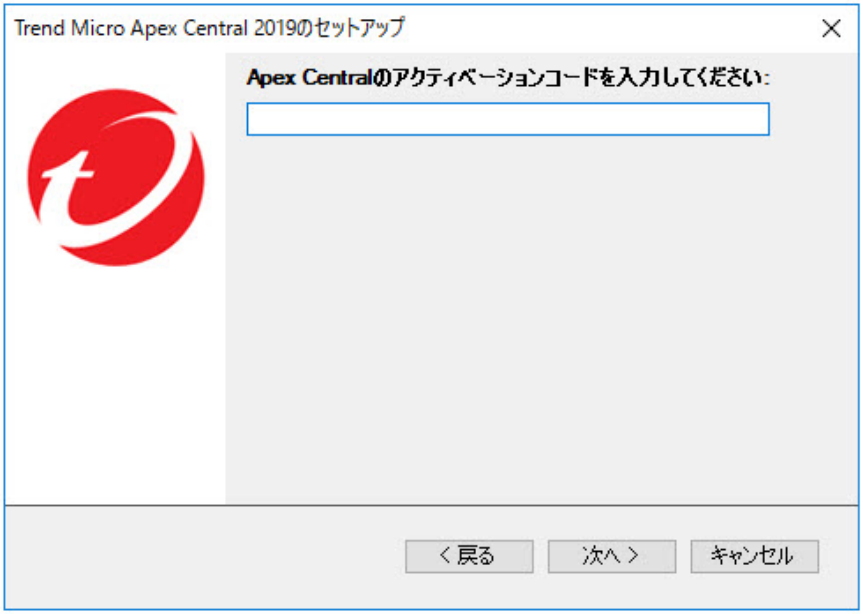

図 3-4. サービスを有効にするアクティベーションコードの入力

2. 表示されたボックスに Apex Central のアクティベーションコードを入力します。

Apex Central の Web サーバ設定を指定する

手順

1. [次へ] をクリックします。

   [Web サーバ情報の指定] 画面が表示されます。

[Web サーバ情報の指定] 画面の設定では、通信のセキュリティ設定とサーバの識別方法を指定します。

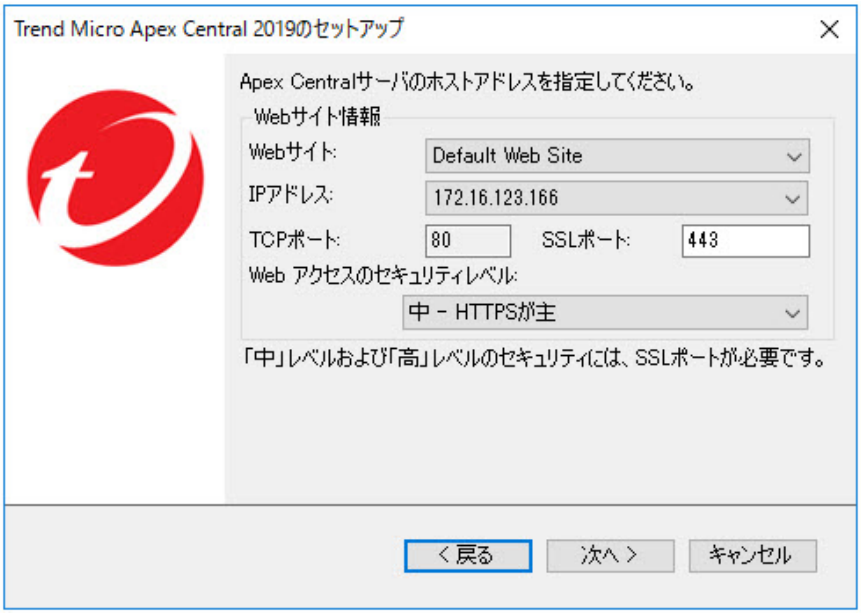

図 3-5. Web サーバ情報の指定

2. [Web サイト] リストから、Apex Central にアクセスする Web サイトを選択します。

3. [IP アドレス] リストから、Apex Central の管理コンソールで使用する、FQDN/ホスト名、IPv4、または IPv6 アドレスを選択します。この設定では、Apex Central の通信システムにおける Apex Central サーバの識別方法を指定します。セットアッププログラムは、サーバの FQDN と IP アドレスの両方を検索し、検出された場合は、これらをフィールドに表示します。

   サーバで複数のネットワークインタフェースカードが使用されている場合、またはサーバに複数の FQDN が割り当てられている場合は、その名前と IP アドレスが表示されます。リストを使用して、最適なアドレスまたは名前を選択します。

サーバの識別にホスト名または FQDN を使用する場合、製品がインストールされているコンピュータ上でこの名前を解決できることを確認してください。解決できない場合、製品は Apex Central サーバと通信することができません。

4. [セキュリティレベル] リストで、Apex Central の通信のセキュリティレベルを次のいずれかから選択します。

   - 高 — HTTPS のみ — すべての Apex Central の通信に HTTPS プロトコルを使用します。Apex Central と他の製品との間の通信として最も安全な通信方法です。
   - 中 — HTTPS が主 — HTTPS がサポートされている場合は、すべての Apex Central の通信に HTTPS プロトコルを使用します。HTTPS が利用できない場合は、エージェントは HTTP を使用します。これは、Apex Central インストール時の初期設定です。
   - 低 — HTTP が基本 — すべての Apex Central の通信に HTTP プロトコルを使用します。Apex Central と他の製品との間の通信として最も安全性が低い通信方法です。

   注意

   このオプションの選択はお勧めしません。

バックアップ設定の指定

手順

1. [次へ] をクリックします。

[インストール先の選択] 画面が表示されます。

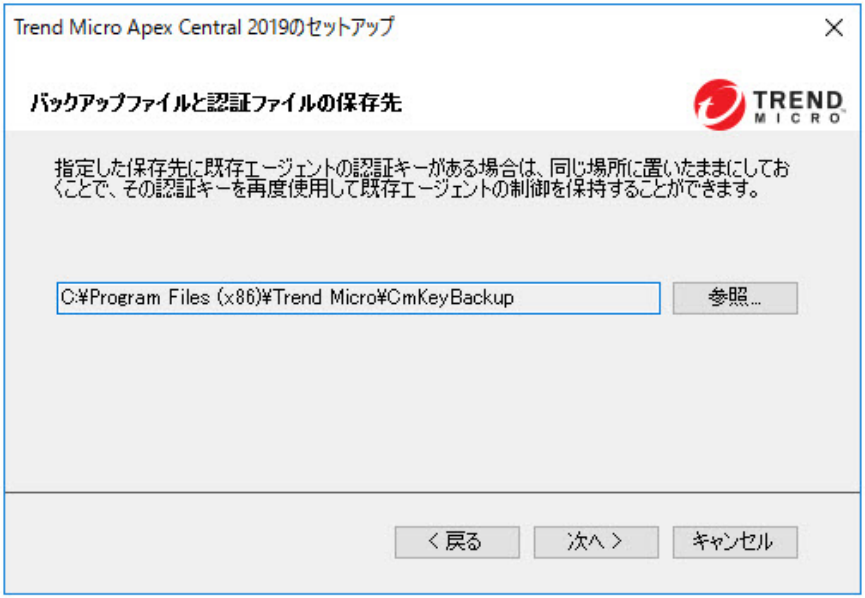

図 3-6. バックアップファイルと認証ファイルの保存場所の選択

2. Apex Central のバックアップファイルと認証ファイルの保存先を指定してください。別の場所を指定するには、[参照] をクリックします。

注意

64 ビット OS の初期設定では、`C:¥Program Files (x86)¥Trend Micro¥CmKeyBackup` にインストールされます。

詳細については、63 ページの「移行前にバックアップするサーバファイル」参照してください。

---

root アカウントをセットアップする

手順

1. [次へ] をクリックします。

   次の画面が表示されます。

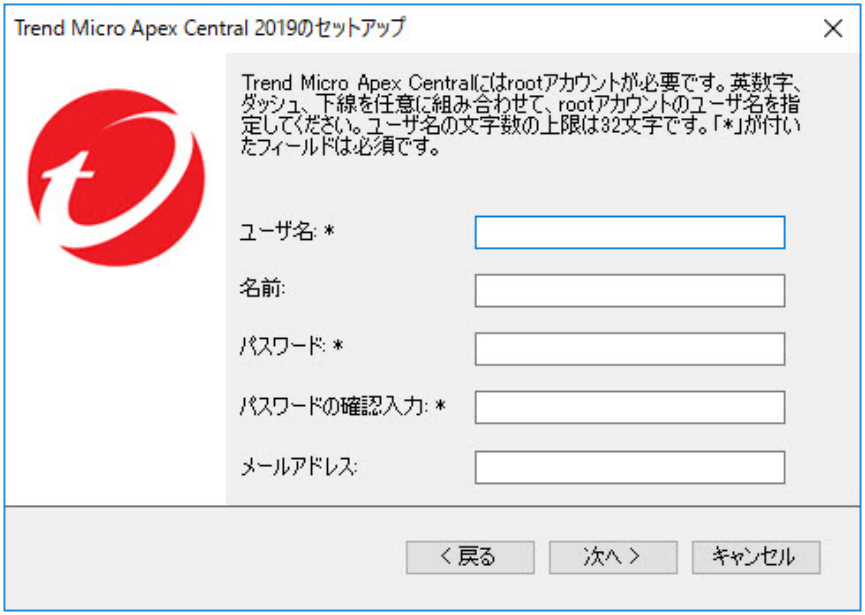

図 3-7. Apex Central root アカウントのセットアップ

2. 次のアカウント情報を入力します。
   - ユーザ名 (必須)
   - 名前
   - パスワード (必須)
   - パスワードの確認入力 (必須)
   - メールアドレス

データベース情報の設定

手順

1. [次へ] をクリックします。

   [Apex Central データベースのセットアップ] 画面が表示されます。

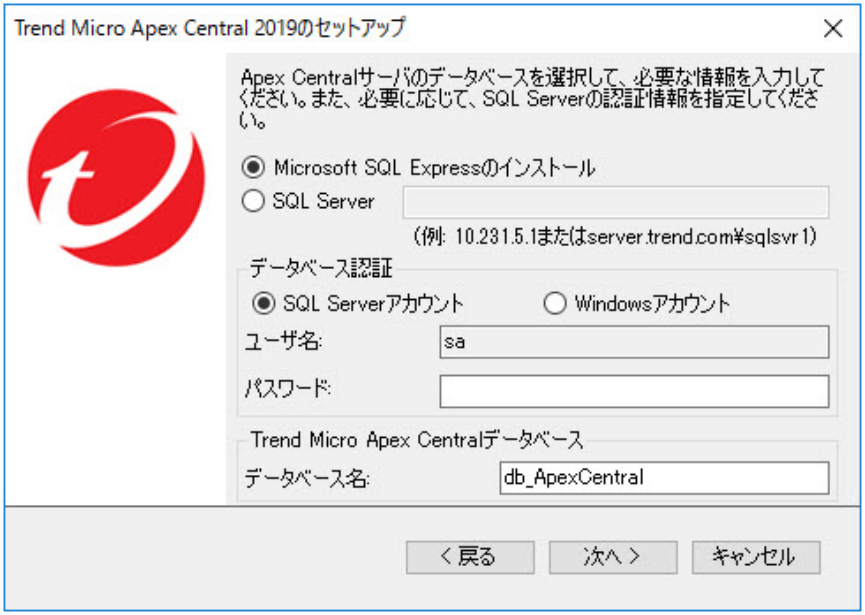

図 3-8. Apex Central データベースを選択します。

2. Apex Central で使用するデータベースを選択します。

   - Microsoft SQL Express のインストール —SQL Server がこのコンピュータにインストールされていない場合、このオプションが自動的に選択されます。データベースには必ずパスワードを指定してください。

ヒント

Microsoft SQL Server Express は、管理下のネットワーク規模が小さい場合に適しています。大規模な Apex Central ネットワークの場合、SQL Server の使用をお勧めします。

- SQL Server —サーバ上で SQL Server が検出された場合、このオプションが自動的に選択されます。次の項目を入力してください。
  - SQL Server (\Instance) —Apex Central で使用する SQL Server のホストサーバです。使用しているサーバに SQL Server が存在する場合は、このオプションが自動的に選択されます。

    別のサーバを指定する場合は、FQDN、IPv4 アドレス、または NetBIOS 名を指定してください。

    SQL Server のホストサーバは、Apex Central がインストールされているサーバ、または別のサーバのどちらでも指定することができますが、パフォーマンスを考慮し、別のサーバにインストールすることをお勧めします。複数の SQL Server インスタンスが存在する場合は、特定のインスタンスを指定する必要があります。次に例を示します。`your_sql_server.com¥instance`

    注意

    ユーザがリモートの SQL Server の使用を選択した場合は、[SQL Server] フィールドに IPv6 アドレスを指定しないでください。Apex Central では、IPv6 アドレスでリモートデータベースを識別できません。

3. [データベース認証] に、SQL Server にアクセスするための認証情報を入力します。

警告!

セキュリティ保護のため、SQL データベースには必ずパスワードを設定してください。

重要

SQL Server アカウントと Windows アカウントは両方とも次の要件を満たしている必要があります。

- 「管理者グループ」に属する
- 「「サービスとしてログオン」」のユーザ権限を持っている
- 「db_creator」または「db_owner」のデータベースの役割を持っている
  - 新しいデータベースを作成する場合 (対象データベースがまだ存在しない場合) には、「db_creator」の役割が必要です。
  - 対象データベースがすでに存在する場合には、「db_owner」の役割があれば問題ありません。

ヒント

既存のデータベースを使用する場合は、Apex Central のインストール用に空のデータベースを用意しておくことを強くお勧めします。

- SQL Server アカウント

  初期設定のユーザ名は「sa」です。

- Windows アカウント

  「ドメイン名\ユーザ名」の形式でユーザ名を入力します。

4. [Trend Micro Apex Central データベース] に Apex Central データベースの名前を入力します。

   初期設定の名前は「db_ApexCentral」です。

5. データベースを作成するには、[次へ] をクリックします。既存の Apex Central データベースが検出された場合には、次のオプションを使用できます。

   - 既存のレコードを削除して、新しいデータベースを作成: 既存のデータベースは削除され、同じ名前の新しいデータベースが作成されます。

- 別名で新規データベースを作成: 前の画面に戻ります。ここで Apex Central データベースの名前を変更することができます。

6. [次へ] をクリックします。
7. [完了] をクリックしてインストールを終了します。

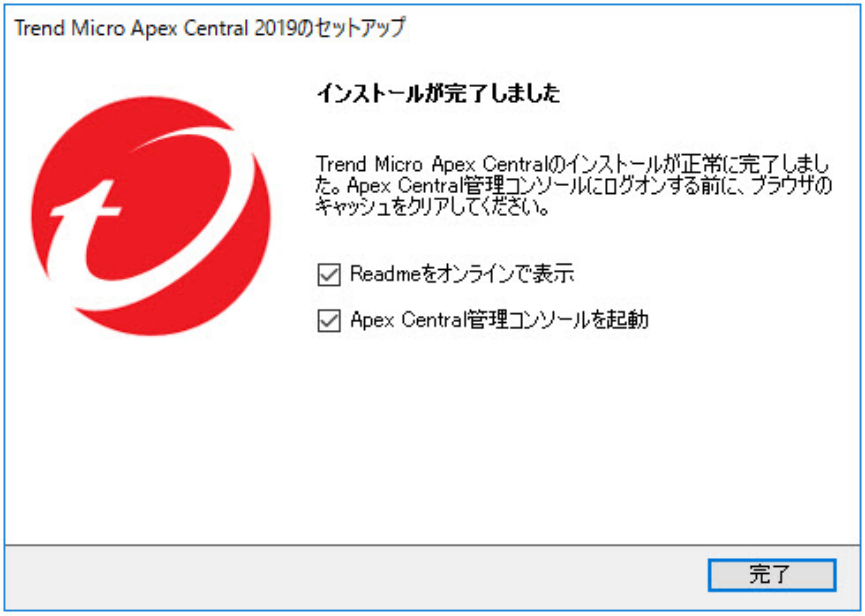

図 3-9. セットアップの完了

第 4 章

インストール後のタスク

この章では、Apex Central インストールの完了後にトレンドマイクロが推奨するタスクについて説明します。

次のトピックがあります。

- 52 ページの「インストール後の自動タスク」
- 52 ページの「サーバのインストールまたはアップグレードを確認する」
- 53 ページの「製品のアクティベーション」
- 55 ページの「Active Directory 接続を設定する」
- 58 ページの「ユーザアカウントの設定」
- 58 ページの「最新コンポーネントのダウンロード」
- 59 ページの「イベント通知を設定する」

インストール後の自動タスク

Apex Central では、Control Manager 6.0 Service Pack 3 Patch 2 からのアップグレードまたは移行が正常に完了すると、次のタスクが自動的に実行されます。

- 以前に行われた Active Directory サーバ設定の移行
- Active Directory サーバデータの同期

サーバのインストールまたはアップグレードを確認する

インストールやアップグレードが完了したら、次の項目を確認します。

項目	説明
プログラムのリスト	次のプログラムがサーバコンピュータの [プログラムの追加と削除] リスト ([コントロール パネル] > [プログラムの追加と削除]) に表示されます。 • Trend Micro Apex Central • Microsoft Visual C++ 2005、2008、2012、2015 再頒布可能パッケージ • Microsoft Report Viewer 2012 Runtime • Microsoft SQL Server 2017 • Microsoft SQL Server 2017 Native Client • Microsoft SQL Server 2017 Setup • Microsoft SQL Server 2017 Setup Support Files • Microsoft SQL Server Browser • Microsoft SQL Server VSS Writer
ディレクトリフォルダ	次のフォルダがサーバコンピュータの `C:¥Program Files (x86)` ディレクトリに表示されます。 • `Trend Micro¥CmKeyBackup` • `Trend Micro¥COMMON¥TMI` • `Trend Micro¥Control Manager`

項目	説明
Apex Central データベースファイル	• db_ApexCentral.mdf • db_ApexCentral_Log.LDF
次のサービスおよびプロセスが実行されていること	
Apex Central サービス	• Trend Micro Apex Central • Trend Micro Management Infrastructure
Microsoft Internet Information Server プロセス	• w3wp.exe (Internet Information Services)
ISAPI フィルタ	• ReverseProxy • TmcmRedirect
Apex Central プロセス	• CasProcessor.exe • CMEFScheduler.NET.exe • CmdProcessor.exe • CmdProcessor.NET.exe • LogForwarder.exe • LogProcessor.exe • LogReceiver.exe • LogRetriever.exe • MDRProcessor.NET.exe • MsgReceiver.exe • ProcessManager.exe • ReportServer.exe • sCloudProcessor.NET.exe • TICAgentForMDR.exe

製品のアクティベーション

アクティベーションコードによって Apex Central の機能が有効化されます。

詳細については、次のトピックを参照してください。

- 54 ページの「Apex Central のアクティベーションを実行する」
- 54 ページの「製品版へのアップグレード」

Apex Central のアクティベーションを実行する

トレンドマイクロの営業担当者や法人カスタマーサイトなどからアクティベーションコードを入手したら、[ライセンス管理] 画面で Apex Central をアクティベートできます。

Apex One Sandbox as a Service のライセンスを購入した場合、[ライセンス管理] 画面からライセンスをアクティベートすることもできます。

重要

Apex Central のアクティベーション後、変更を有効にするには、Apex Central 管理コンソールからログオフして再びログオンしてください。

手順

1. [運用管理] > [ライセンス管理] > [Apex Central] に移動します。

   [ライセンス情報] 画面が表示され、現在のライセンス情報が示されます。

2. [新しいアクティベーションコードを入力してください] リンクをクリックします。
3. アクティベーションコードを入力します。
4. [アクティベート] をクリックします。
5. Apex Central 管理コンソールからログオフして再びログオンすると、変更が有効になります。

製品版へのアップグレード

体験版の試用期間が過ぎた後も Apex Central を引き続き使用するには、Control Manager のアクティベーションを実行します。アップデート済みのプログラムコンポーネントのダウンロードなどのサポートサービスを含む、

全機能を使用するためには、Apex Central のアクティベーションを実行してください。

手順

1. 製品版を購入します。購入については、トレンドマイクロの営業部または販売代理店にお問い合わせください。
2. 製品版パッケージに付属のアクティベーションコードを用意します。
3. 上記の手順に従って Apex Central のアクティベーションを行ってください。

Active Directory 接続を設定する

Apex Central が Active Directory サーバからのエンドポイントおよびユーザの情報を同期できるように接続設定を指定します。

注意

Apex Central は、複数の Active Directory フォレストとの同期をサポートしています。Active Directory ドメインを追加すると、同じフォレストのすべてのドメインが自動的に同期されます。

フォレストの信頼の詳細については、Active Directory 管理者にお問い合わせください。

手順

1. [運用管理] > [設定] > [Active Directory とコンプライアンスの設定] に移動します。
2. [Active Directory の設定] タブをクリックします。
3. [Active Directory との同期と認証を有効にする] を選択します。
4. Active Directory サーバにアクセスするための接続を設定します。

フィールド	説明
サーバアドレス	Active Directory サーバの FQDN または IP アドレス (IPv4 または IPv6) を入力します。
ユーザ名	Active Directory サーバへのアクセスに必要なドメイン名とユーザ名を入力します。 形式の例: ドメイン\ユーザ名
パスワード	Active Directory サーバへのアクセスに必要なパスワードを入力します。

- 他の Active Directory サーバを追加するには、追加アイコン (+) をクリックします。
- Active Directory サーバを削除するには、削除アイコン (–) をクリックします。

5. [同期の頻度 (時間単位)] ドロップダウンリストから、Apex Central が Active Directory サーバとデータを同期する頻度を選択します。

注意

Active Directory の同期時間は、Active Directory データベースのサイズと複雑さに応じて異なります。同期が完了するまでに 1 時間以上かかる場合もあります。

---

6. (オプション) [詳細設定] を展開して、[同期元] または [接続モード] を設定します。

   a. 同期元として次のいずれかを選択します。

      - [ドメインコントローラ]: 信頼関係で結ばれた複数のフォレストのすべてのドメインを同期します。
      - [グローバルカタログ]: 単一のフォレストのすべてのドメインを同期します。

重要

初期設定のグローバルカタログを同期元とした場合、グローバルグループまたはドメインローカルグループでの地理的な位置やユーザのメンバーシップなど、Apex Central が使用する一部の情報を同期できません。グローバルカタログを同期元に選択するのは、ネットワークポリシーによって Apex Central がすべてのドメインコントローラに接続できない場合のみにしてください。

b. 接続モードとして次のいずれかを選択します。

- SSL

重要

SSL 接続を使用するには、Active Directory 証明書を Apex Central サーバにインポートします。

- 非 SSL

7. (オプション) [接続テスト] をクリックして、サーバ接続をテストします。

注意

接続をテストしても、Active Directory サーバの設定は保存されません。

サーバアドレスの前に、Active Directory サーバの接続ステータスアイコン (または) が表示されます。

8. [保存] をクリックします。

Apex Central が、同期の頻度に従って Active Directory サーバからエンドポイントとユーザ情報を同期します。

9. (オプション) 次の場所にある `ADSyncOUList.config` 設定ファイルを変更して、Apex Central の同期対象になる Active Directory ドメインと OU を設定します。

`<Apex Central インストールディレクトリ>\ADSyncOUList.config`

10. (オプション) [今すぐ同期]をクリックして、Active Directory のデータを手動で同期します。

    サーバアドレスの前に、Active Directory サーバの接続ステータスアイコン (または) が表示されます。

11. 同期した Active Directory サーバを削除するには、次の手順を行います。

    a. [Active Directory との同期を有効にする] チェックボックスをオフにします。

    b. [データのクリア] をクリックして、削除された Active Directory サーバのデータを Apex Central サーバから削除します。

       Apex Central によって、同期された Active Directory サーバが削除されます。

       注意

       [データのクリア] をクリックすると、2 分ごとに実行されるようにスケジュールされたタスクがトリガされ、削除された Active Directory サーバのすべてのデータが Apex Central のデータベースから削除されます。

ユーザアカウントの設定

必要に応じて Apex Central ユーザアカウントを作成します。アカウントを作成するときは次の点を考慮します。

- ユーザの役割それぞれの数 (Administrator、Power User、Operator)
- ユーザの役割それぞれへの適切な許可および権限の割り当て
- ユーザがさらに高度な機能を利用するためには、「Power User」以上の権限が必要になります。

最新コンポーネントのダウンロード

インストール完了後、トレンドマイクロのアップデートサーバから手動で最新のコンポーネントをダウンロードします。トレンドマイクロのアップデートサーバは、最新のセキュリティ保護を継続できるよう最新のコンポーネン

トを提供しています。トレンドマイクロのサーバとインターネットの間にプロキシサーバがある場合には、プロキシサーバを設定する必要があります (管理コンソールで [運用管理] > [設定] > [プロキシの設定] の順に選択します)。

イベント通知を設定する

インストール完了後、通知を送信するイベントを設定し、重大なウイルス攻撃やセキュリティに関わるアクティビティを監視できるようにします。通知の受信者を指定するほか、通知チャネルを選択し、通知の送信が期待どおりに実行されるかどうかをテストします。Web コンソールから [検出] > [通知] > [イベント通知] に移動します。

第 5 章

アップグレードと移行

この章では、以前のバージョンの Apex Central または Control Manager から、Apex Central にアップグレードまたは移行する方法について説明します。

次のトピックがあります。

- 62 ページの「Apex Central にアップグレードする」
- 64 ページの「アップグレードと移行のシナリオ」
- 68 ページの「Apex Central エージェントの移行を計画する」
- 69 ページの「Apex Central データベースを移行する」

Apex Central にアップグレードする

Control Manager のインストールを Apex Central に移行した場合、それまでのすべての設定、ログ、レポート、製品ディレクトリ構造、および統合された Active Directory 構造は保持されます。

重要

- Apex Central では、Control Manager 6.0 Service Pack 3 Patch 3、Control Manager 7.0、または Control Manager 7.0 Patch 1 からのアップグレードまたは移行のみがサポートされます。
- Apex Central に移行する前に、サーバに十分なシステムリソースがあることを確認してください。

  詳細については、63 ページの「移行前のチェックリスト」を確認するか、http://docs.trendmicro.com/ja-jp/enterprise/apex-central.aspx から Apex Central システム要件 PDF ドキュメントをダウンロードしてください。

警告!

アップグレードを実行する前に、必ず既存のサーバをバックアップしてください。

詳細については、63 ページの「移行前にバックアップするサーバファイル」を参照してください。

アップグレードがサポートされているバージョン

Apex Central では、次のバージョンからのアップグレードがサポートされています。

- Control Manager 6.0 Service Pack 3 Patch 2
- Control Manager 7.0
- Control Manager 7.0 Patch 1

警告!

アップグレードを実行する前に、必ず既存のサーバをバックアップしてください。

移行前にバックアップするサーバファイル

以前のバージョンの Control Manager から Apex Central にアップグレードまたは移行する前に、サーバファイルのバックアップを作成します。バックアップするファイルの詳細は次の Web サイトを参照してください。

https://success.trendmicro.com/dcx/s/solution/1096680?language=ja

移行前のチェックリスト

Control Manager を Apex Central にアップグレードまたは移行する前に、システムが次の最小要件を満たしていることを確認してください。

重要

- Apex Central では、Control Manager 6.0 Service Pack 3 Patch 3、Control Manager 7.0、または Control Manager 7.0 Patch 1 からのアップグレードまたは移行のみがサポートされます。
- すべてのシステム要件およびサポートされる Windows Server および Microsoft SQL Server のバージョンについては、Apex Central システム要件 PDF ドキュメントを https://docs.trendmicro.com/ja-jp/documentation/apex-central/からダウンロードしてください。

項目	最小要件
OS:	Windows Server 2012 重要 Windows Server 2012 より前の OS で Control Manager を実行している場合は、Windows Server 2012 またはその他のサポートされるバージョンにアップグレードまたは移行する必要があります。
使用可能な空きディスク容量	10 GB 以上 80GB 推奨 (SAS) 注意 使用可能な空きディスク容量が 10 GB 未満のサーバで Control Manager を実行している場合は、使用可能な空きディスク容量が 10 GB 以上 (80 GB を推奨) のサーバに移行する必要があります。
SQL Server	Microsoft SQL Server 2008 重要 移行前に SQL Server が実行中であることを確認してください。
トレンドマイクロのサービス	移行前に次のサービスが実行中であることを確認してください。 • Trend Micro Control Manager • Trend Micro Management Infrastructure

アップグレードと移行のシナリオ

Apex Central では、次のような移行シナリオがサポートされています。

- 65 ページの「シナリオ 1: Control Manager サーバを Apex Central へアップグレードする」

- 67 ページの「シナリオ 2: エージェント移行ツールを使用して Apex Central の新規インストールへ移行する」

アップグレードの流れ

以前のバージョンの Control Manager を Apex Central にアップグレードするには、36 ページの「すべての必須コンポーネントのインストール」の手順 1 の説明に従ってインストールプログラム (`Trend Micro Apex Central.exe`) を実行します。

重要

Apex Central では、Control Manager 6.0 Service Pack 3 Patch 3、Control Manager 7.0、または Control Manager 7.0 Patch 1 からのアップグレードまたは移行のみがサポートされます。

シナリオ 1: Control Manager サーバを Apex Central へアップグレードする

Control Manager の以前のバージョンを Apex Central に直接アップグレードする際に、管理者は以前にインストールした Control Manager をバックアップするか、Control Manager がインストールされているサーバの OS 全体をバックアップするかを選択できます。OS のバックアップにはより多くの作業が必要になりますが、データの損失を防止する上でより高度なセキュリティを提供します。

重要

Apex Central では、Control Manager 6.0 Service Pack 3 Patch 3、Control Manager 7.0、または Control Manager 7.0 Patch 1 からのアップグレードまたは移行のみがサポートされます。

既存の Control Manager サーバとデータベースをバックアップしてアップグレードする

重要

Apex Central では、Control Manager 6.0 Service Pack 3 Patch 3、Control Manager 7.0、または Control Manager 7.0 Patch 1 からのアップグレードまたは移行のみがサポートされます。

手順

1. 既存の Control Manager データベースをバックアップします。
2. `¥Trend Micro¥CmKeyBackup¥*.*`以下のすべてのファイルをバックアップします。
3. 既存の Control Manager サーバのすべてのフォルダをバックアップします。
4. 既存の Control Manager サーバのレジストリをバックアップします。
5. Control Manager を介して Apex Central をインストールします。

サーバの OS 全体と Apex Central データベースをバックアップしてアップグレードする

重要

Apex Central では、Control Manager 6.0 Service Pack 3 Patch 3、Control Manager 7.0、または Control Manager 7.0 Patch 1 からのアップグレードまたは移行のみがサポートされます。

手順

1. 既存の Control Manager サーバの OS をバックアップします。
2. 既存の Control Manager データベースをバックアップします。

3. Control Manager を介して Apex Central をインストールします。

シナリオ 2: エージェント移行ツールを使用して Apex Central の新規インストールへ移行する

このシナリオには、既存の Apex Central サーバまたは Control Manager サーバとは別のサーバに、Apex Central をインストールする作業が含まれます。この方法により、以前のサーバの使用を徐々に停止することができます。エージェントの移行の詳細については、68 ページの「Apex Central エージェントの移行を計画する」を参照してください。

重要

Apex Central では、Control Manager 6.0 Service Pack 3 Patch 3、Control Manager 7.0、または Control Manager 7.0 Patch 1 からのアップグレードまたは移行のみがサポートされます。

Control Manager サーバを Apex Central の新規インストールに移行する

重要

Apex Central では、Control Manager 6.0 Service Pack 3 Patch 3、Control Manager 7.0、または Control Manager 7.0 Patch 1 からのアップグレードまたは移行のみがサポートされます。

手順

1. 既存の Control Manager データベースをバックアップします。
2. 別のコンピュータに Apex Central を新規インストールします。
3. エージェント移行ツールを使用して、Control Manager サーバから Apex Central サーバにエンティティを移行します。

Apex Central エージェントの移行を計画する

Apex Central サーバにエージェントを移行するには、次の 2 つの方法があります。

- 一括アップグレード
- 段階的アップグレード

一括アップグレード

一括アップグレードは、次の表に示す方法で行われます。

表 5-1. 一括アップグレード

移行元	処理
Control Manager 6.0 Service Pack 3 Patch 2 (エージェント: MCP)	MCP エージェントを Apex Central サーバに登録し、製品ディレクトリ構造を再構成します。
Control Manager 7.0 (エージェント: MCP)	
Control Manager 6.0 Service Pack 3 Patch 2 (エージェント: 混在) Control Manager 7.0 (エージェント: 混在)	MCP エージェントを Apex Central サーバに登録し、製品ディレクトリ構造を再構成します。

この方法は、出荷時の設定で使用している場合や比較的小規模なネットワークで運用しているエージェントの移行 (できれば、テスト環境) に推奨します。15 ページの「テストインストール」を参照してください。しかし、一度開始した移行処理は中止できないため、この方法は小規模の配信に最適で、ネットワークの規模が大きいほど難度も高くなります。

段階的アップグレード

単一サーバを大規模な Control Manager 6.0 Service Pack 3 Patch 2 または 7.0 システムで運用している場合、トレンドマイクロでは段階的アップグレードをお勧めします。また、複数のサーバが存在するネットワークの場合にはこ

の方法が必須です。この方法では、より体系的にシステムを移行することができます。移行作業は、次の方針に基づいて進めます。

- 既存のネットワークの中で最も移行の影響が小さいと思われるシステムで、まず移行を実施します。その後、より影響が大きいシステムの移行を順次実行します。
- 十分に計画を立てた後、1 度にすべての移行手順を実行するのではなく、1 つずつ手順を実行します。

  そうすることによって、移行中に問題が発生した場合に問題解決のための作業を最小限にすることができます。

段階的アップグレードを実施するには、次の手順に従ってください。

1. 以前のバージョンの Control Manager がインストールされていないサーバに Apex Central をインストールします。
2. Apex Central サーバで `AgentMigrateTool.exe` ツールを実行します。

Apex Central エージェントインストールとエージェント移行ツールを併せて利用し、既存の Apex Central システム上でのエージェントアップグレード計画を立ててください。エージェント移行ツールの利用により、Apex Central エージェントが登録されているサーバのリストを生成できます。これにより、移行元サーバを手動で選択する必要がなくなります。

Apex Central データベースを移行する

Control Manager 6.0 SP3 Patch 3 または 7.0 の既存のデータベースを移行するには、Control Manager サーバに Apex Central をインストールします。

Apex Central のセットアッププログラムにより、データベースのバージョンが自動的にアップグレードされます。

Apex Central SQL データベースを他の SQL Server に移行する

Apex Central データベースを SQL Server から別の SQL Server に移動するには、DBConfig ツールを使用して移行します。

データベース設定ツールを使用する (DBConfig.exe)

`DBConfig.exe` ツールにより、ユーザは Apex Central データベース用のユーザアカウント、パスワード、およびデータベース名を変更できます。

このツールには次のオプションがあります。

- DBName: データベース名
- DBAccount: データベースのアカウント
- DBPassword: データベースのパスワード
- Mode: データベース認証モード (SQL Server 認証または Windows 認証)

注意

データベース認証モードの初期設定は、SQL Server 認証モードです。ただし、Windows 認証を設定する際には、Windows 認証モードで行う必要があります。

手順

1. Apex Central サーバでコマンドプロンプトを開きます。
2. 次のコマンドを使用して、`DBConfig.exe` ファイルが含まれるディレクトリに移動します。

   ```
   cd <Apex Central インストールディレクトリ>\DBConfig
   ```

3. `dbconfig` と入力し、`ENTER` キーを押します。

   DBConfig ツールインタフェースが表示されます。

4. 変更する設定を指定します。
   - 例 1: `DBConfig -DBName="db_<データベース名>" -DBAccount="sqlAct" -DBPassword="sqlPwd" -Mode="SQL"`
   - 例 2: `DBConfig -DBName="db_<データベース名>" -DBAccount="winAct" -DBPassword="winPwd" -Mode="WA"`
   - 例 3:`DBConfig -DBName="db_<データベース名>" -DBPassword="sqlPwd"`

詳細については、次の Web サイトを参照してください。

https://success.trendmicro.com/dcx/s/solution/1306559?language=ja

第 6 章

移行後のタスク

アップグレードまたは移行が正常に完了したことの確認、Apex One サーバからの設定のインポート、追加機能の有効化と設定を行うために、次のタスクを実行します。

- 72 ページの「成功したアップグレードまたは移行を確認する」
- 72 ページの「Apex Central に Apex One サーバ設定を移行する」
- 74 ページの「アプリケーションコントロールを有効にする」
- 75 ページの「仮想パッチを有効にする」
- 77 ページの「Endpoint Sensor を有効にする」
- 79 ページの「Endpoint Sensor 向けに Apex One サーバを設定する」

成功したアップグレードまたは移行を確認する

Control Manager の以前のバージョンが Apex Central に正常にアップグレードされたことを確認するには、次の手順を実行します。

手順

1. Apex Central Web コンソールにログオンします。

   Apex Central Web コンソールに正常にログオンすると、[ダッシュボード] が表示されます。

2. [ヘルプ] > [バージョン情報] に移動します。

   [バージョン情報] 画面が開き、Apex Central の製品名とバージョンが表示されます。

3. Apex Central サーバで、次のサービスが実行中であることを確認します。
   - Trend Micro Apex Central
   - Trend Micro Management Infrastructure

Apex Central に Apex One サーバ設定を移行する

既存の Apex One サーバから Apex Central に既存の設定を移行するには、次の手順を実行します。

手順

1. Apex One サーバから設定をエクスポートします。
   a. Apex One サーバから Apex One Web コンソールにログオンします。
   b. [運用管理] > [設定] > [サーバ移行] に移動します。
   c. Apex One サーバに Apex One 設定エクスポートツールをダウンロードします。
   d. `ApexOneSettingsExportTool.exe` プログラムを実行して、Apex One サーバから設定をエクスポートします。
   e. Apex Central サーバがアクセスできる場所にエクスポートパッケージ (`*.zip` ファイル) をコピーします。
2. Apex One サーバ設定をインポートします。
   a. Apex Central サーバから Apex Central Web コンソールにログオンします。
   b. [ポリシー] > [ポリシー管理] に移動します。
   c. [製品] で [Apex One セキュリティエージェント] を選択します。
   d. [設定のインポート] をクリックします。
   e. Apex One サーバからエクスポートされた`*.zip` ファイルを選択し、アップロードします。

      画面の表示が更新され、インポートされたポリシーがリストの一番上に表示されます。
   f. (オプション) ポリシーをクリックして、設定を編集するか、次のタスクを実行します。
      - 74 ページの「アプリケーションコントロールを有効にする」
      - 75 ページの「仮想パッチを有効にする」
      - 77 ページの「Endpoint Sensor を有効にする」

アプリケーションコントロールを有効にする

重要

アプリケーションコントロール機能を使用するには専用のライセンスが必要です。アプリケーションコントロールポリシーをエンドポイントに配信する前に、アクティベーションコードが正しいことを確認してください。アクティベーションコードの入手方法の詳細については、販売代理店にお問い合わせください。

手順

1. 管理下の製品サーバにアクティベーションコードを配信します。
   a. [運用管理] > [ライセンス管理] > [管理下の製品] に移動します。

      [ライセンス管理] 画面が表示されます。

   b. [追加と配信] をクリックします。

      [新しいライセンスの追加と配信]>[手順 1 :アクティベーションコードの入力] 画面が表示されます。

   c. アクティベートする製品のアクティベーションコードを [新しいアクティベーションコード] フィールドに入力します。

   d. [次へ] をクリックします。

      [新しいライセンスの追加と配信]>[手順 2 :対象の選択] 画面が表示されます。

   e. アクティベーションコードの配信先となる対象 Apex One サーバを選択します。

   f. [配信] をクリックします。

      [ライセンス管理] 画面が表示され、アクティベーションコードが正常に配信された管理下の製品サーバの数が [アクティベート済み製品] 列に表示されます。

2. [ポリシー] > [ポリシー管理] に移動します。

   [ポリシー管理] 画面が表示されます。

3. [製品] で [Apex One セキュリティエージェント] を選択します。
4. [ポリシー名] を指定または編集します。
5. 対象を指定します。
6. ポリシーを作成または編集します。
   a. ポリシーを作成するには、[作成] をクリックします。
   b. ポリシーを編集するには、[ポリシー] 列のポリシー名をクリックします。
7. [アプリケーションコントロールの設定] を展開します。
8. [アプリケーションコントロールを有効にする] を選択します。
9. [配信] または [保存] をクリックします。

   [ポリシー管理] 画面が表示され、ポリシーの配信ステータスが表示されます。

注意

配信にかかる時間は、ネットワーク環境の規模に応じて異なります。指定した対象すべてにポリシーの配信が完了するまでには、しばらく時間がかかることがあります。

仮想パッチを有効にする

重要

仮想パッチ機能を使用するには専用のライセンスが必要です。仮想パッチポリシーをエンドポイントに配信する前に、アクティベーションコードが正しいことを確認してください。アクティベーションコードの入手方法の詳細については、販売代理店にお問い合わせください。

手順

1. 管理下の製品サーバにアクティベーションコードを配信します。

a. [運用管理] > [ライセンス管理] > [管理下の製品] に移動します。

   [ライセンス管理] 画面が表示されます。

b. [追加と配信] をクリックします。

   [新しいライセンスの追加と配信]>[手順 1 :アクティベーションコードの入力] 画面が表示されます。

c. アクティベートする製品のアクティベーションコードを [新しいアクティベーションコード] フィールドに入力します。

d. [次へ] をクリックします。

   [新しいライセンスの追加と配信]>[手順 2 :対象の選択] 画面が表示されます。

e. アクティベーションコードの配信先となる対象 Apex One サーバを選択します。

f. [配信] をクリックします。

   [ライセンス管理] 画面が表示され、アクティベーションコードが正常に配信された管理下の製品サーバの数が [アクティベート済み製品] 列に表示されます。

2. [ポリシー] > [ポリシー管理] に移動します。

   [ポリシー管理] 画面が表示されます。

3. [製品] で [Apex One セキュリティエージェント] を選択します。

4. [ポリシー名] を指定または編集します。

5. 対象を指定します。

6. ポリシーを作成または編集します。

   a. ポリシーを作成するには、[作成] をクリックします。

   b. ポリシーを編集するには、[ポリシー] 列のポリシー名をクリックします。

7. [仮想パッチの設定] を展開します。

8. [仮想パッチを有効にする] を選択します。

9. [配信] または [保存] をクリックします。

   [ポリシー管理] 画面が表示され、ポリシーの配信ステータスが表示されます。

注意

配信にかかる時間は、ネットワーク環境の規模に応じて異なります。指定した対象すべてにポリシーの配信が完了するまでには、しばらく時間がかかることがあります。

Endpoint Sensor を有効にする

重要

- Endpoint Sensor 機能を使用するには、専用のライセンスが必要であるほか、追加のシステム要件を満たす必要があります。Endpoint Sensor のポリシーをエンドポイントに配信する前に、正しいライセンスがあることを確認してください。ライセンスの入手方法の詳細については、サポートプロバイダにお問い合わせください。
- 接続された Apex One サーバで Endpoint Sensor 機能を使用するには、ハードウェアとソフトウェアに関する追加要件を満たす必要があります。詳細については、Apex One のインストールおよびアップグレードガイドを参照してください。

手順

1. 管理下の製品サーバにアクティベーションコードを配信します。

   a. [運用管理] > [ライセンス管理] > [管理下の製品] に移動します。

      [ライセンス管理] 画面が表示されます。

   b. [追加と配信] をクリックします。

      [新しいライセンスの追加と配信]>[手順 1 :アクティベーションコードの入力] 画面が表示されます。

c. アクティベートする製品のアクティベーションコードを [新しいアクティベーションコード] フィールドに入力します。

d. [次へ] をクリックします。

[新しいライセンスの追加と配信]>[手順 2 :対象の選択] 画面が表示されます。

e. アクティベーションコードの配信先となる対象 Apex One サーバまたは Apex One (Mac) サーバを選択します。

f. [配信] をクリックします。

[ライセンス管理] 画面が表示され、アクティベーションコードが正常に配信された管理下の製品サーバの数が [アクティベート済み製品] 列に表示されます。

2. [ポリシー] > [ポリシー管理] に移動します。

[ポリシー管理] 画面が表示されます。

3. [製品] で [Apex One セキュリティエージェント] を選択します。

4. [ポリシー名] を指定または編集します。

5. 対象を指定します。

6. ポリシーを作成または編集します。

a. ポリシーを作成するには、[作成] をクリックします。

b. ポリシーを編集するには、[ポリシー] 列のポリシー名をクリックします。

7. [Endpoint Sensor 設定] を展開します。

8. [Endpoint Sensor を有効にする] を選択します。

9. [配信] または [保存] をクリックします。

[ポリシー管理] 画面が表示され、ポリシーの配信ステータスが表示されます。

注意

配信にかかる時間は、ネットワーク環境の規模に応じて異なります。指定した対象すべてにポリシーの配信が完了するまでには、しばらく時間がかかることがあります。

Endpoint Sensor 向けに Apex One サーバを設定する

重要

- Endpoint Sensor 機能を使用するには、専用のライセンスが必要であるほか、追加のシステム要件を満たす必要があります。Endpoint Sensor のポリシーをエンドポイントに配信する前に、正しいライセンスがあることを確認してください。ライセンスの入手方法の詳細については、サポートプロバイダにお問い合わせください。
- 接続された Apex One サーバで Endpoint Sensor 機能を使用するには、ハードウェアとソフトウェアに関する追加要件を満たす必要があります。詳細については、Apex One のインストールおよびアップグレードガイドを参照してください。
- 次の手順は、事前に Apex One セキュリティエージェントポリシーを作成または編集し、Endpoint Sensor を有効にしてあることを前提としたものです。

  詳細については、77 ページの「Endpoint Sensor を有効にする」を参照してください。

手順

1. [ポリシー] > [ポリシー管理] に移動します。

   [ポリシー管理] 画面が表示されます。

2. [製品] で [Apex One サーバ] を選択します。

3. [ポリシー名] を指定または編集します。
4. 対象を指定します。
5. ポリシーを作成または編集します。
   a. ポリシーを作成するには、[作成] をクリックします。
   b. ポリシーを編集するには、[ポリシー] 列のポリシー名をクリックします。
6. [Endpoint Sensor] を展開して、次の設定を行います。

オプション	説明
最大メタデータストレージ	メタデータストレージで許容される最大サイズを指定します。サイズは 20〜20,480GB の間で指定します。ストレージサイズの初期設定は 1,024GB です。メタデータストレージがこのサイズに達すると、サーバは新しいレコードに対応するために古いレコードを削除します。
最大メモリ割り当て	メタデータキャッシュに割り当てられる最大メモリ容量を指定します。サイズは 4〜48GB の間で指定します。現在よりも大きいサイズを新しいサイズとして指定する必要があります。割り当てサイズの初期設定は 4GB です。 注意 メモリサイズは、データアップロードのパフォーマンスや調査速度に影響します。パフォーマンスを向上させるには、該当するサーバのメモリサイズを増やしてください。

7. [配信] または [保存] をクリックします。

   [ポリシー管理] 画面が表示され、ポリシーの配信ステータスが表示されます。

注意

配信にかかる時間は、ネットワーク環境の規模に応じて異なります。指定した対象すべてにポリシーの配信が完了するまでには、しばらく時間がかかることがあります。

第 7 章

アンインストール

本章には、Apex Central をアンインストールし、関連ファイルを削除する方法について説明します。

次のトピックがあります。

- 84 ページの「Apex Central のアンインストール」
- 85 ページの「Apex Central を手動でアンインストールする」

Apex Central のアンインストール

サーバから Apex Central をアンインストールするには、次のいずれかの方法を使用します。

手順

- 方法 1: Windows の [スタート] メニューを使用し、[スタート] > [Trend Micro Apex Central] > [Trend Micro Apex Central のアンインストール] の順に選択します。
- 方法 2: Windows の [プログラムの追加と削除] を使用

  a. [スタート] > [コントロール パネル] > [プログラムの追加と削除] に移動します。

  b. [Trend Micro Apex Central] を選択し、[アンインストール] をクリックします。

     確認ダイアログが表示されます。

  c. Apex Central をアンインストールする場合は [はい] をクリックしてください。

  d. Apex Central データベースをアンインストールするかどうかを選択します。

     注意
     データベースを保持しておくと、サーバに Apex Central を再インストールする際にエージェントの登録やユーザアカウントのデータなどのシステム情報を再使用することができます。

     - データベースをアンインストールするには、[Apex Central データベースの削除] チェックボックスをオンにします。
     - データベースを保持するには、[Apex Central データベースの削除] チェックボックスをオフにします。

  e. [次へ] をクリックします。

     - アンインストールプログラムにより、サーバから Apex Central が削除されます。

- [Apex Central データベースの削除] をオンにすると、データベースも削除されます。
- Apex Central を再インストールしても、元のデータベースが削除されず、前の Apex Central にレポートしていた管理下の製品も削除されていない場合、次のタイミングで管理下の製品が Apex Central に再登録されます。
  - MCP エージェントのサービスを再起動したとき
  - 再インストール後に Apex Central に製品が登録されたとき

Apex Central を手動でアンインストールする

ここでは、Apex Central を手動でアンインストールする方法について説明します。ここで説明する手順は、Windows の「プログラムの追加と削除」、または Apex Central のアンインストールプログラムを使用して正常にアンインストールできなかった場合にのみ使用してください。

注意

Windows での手順は、使用している OS のバージョンによって異なる場合があります。ここでは Windows Server 2012 を使用していることを前提に説明しています。

Apex Central のアンインストールでは、次のコンポーネントを削除する必要があります。これらのコンポーネントは任意の順序でアンインストールできます。また、一括でアンインストールすることもできます。ただし、ここでは、説明の便宜上、節ごとに各モジュールのアンインストール手順を個別に説明します。各コンポーネントは以下のとおりです。

- Apex Central アプリケーション
- データベースコンポーネント (任意)

注意

すべてのコンポーネントをアンインストールしたら、サーバを再起動してください。各コンポーネントをアンインストールするたびに再起動する必要はありません。

Apex Central アプリケーションをアンインストールする

Apex Central アプリケーションを手動でアンインストールするには、次の手順に従ってください。

1. 86 ページの「Apex Central サービスを停止する」
2. 87 ページの「Apex Central の IIS 設定を削除する」
3. 88 ページの「Apex Central のファイル/ディレクトリおよびレジストリキーを削除する」
4. 89 ページの「データベースコンポーネントの削除」
5. 90 ページの「Apex Central サービスを削除する」

Apex Central サービスを停止する

次の Apex Central サービスのすべて、および IIS サービスを停止する場合は、Windows の [サービス] 画面を使用します。

- Trend Micro Apex Central

注意

これらのサービスは、Windows OS のバックグラウンドで動作するものです。アクティベーションコードを必要とするトレンドマイクロのサービスではありません。

Windows のサービス画面から Apex Central サービスを停止する

手順

1. [スタート] > [プログラム] > [管理ツール] > [サービス] をクリックして、[サービス] 画面を開きます。

2. Trend Micro Apex Central を右クリックして、[停止] をクリックします。

コマンドプロンプトから Apex Central および IIS サービスを停止する

手順

- コマンドプロンプトからサービスを停止するには、コマンドプロンプトで次のコマンドを実行します。

```
net stop w3svc
```

```
net stop tmcm
```

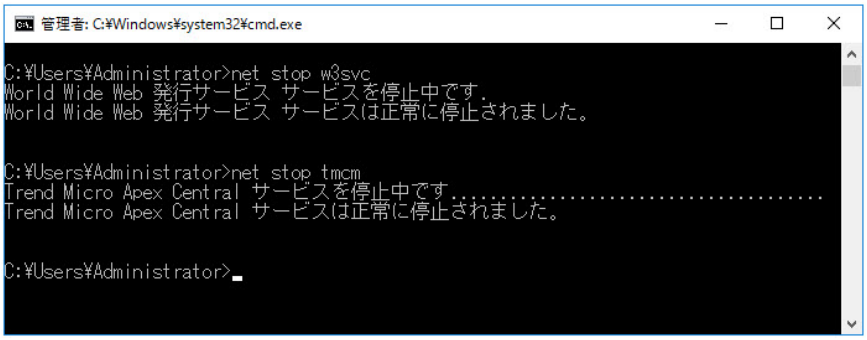

図 7-1. 対象のサービスを停止したコマンドラインのビュー

Apex Central の IIS 設定を削除する

IIS (Internet Information Service) 設定の削除は、Apex Central サービスを停止した後に実行します。

手順

1. Apex Central サーバで、Windows の [スタート] > [ファイル名を指定して実行] の順に選択します。

   [ファイル名を指定して実行] ダイアログボックスが表示されます。

2. [名前] ボックスに次のように入力します。

`%SystemRoot%\System32\Inetsrv\iis.msc`

3. 左側のメニューでサーバ名をダブルクリックしてコンソールツリーを展開します。
4. [Default Web Site] をダブルクリックします。
5. 次の仮想ディレクトリを削除します。
   - `ControlManager`
   - `TVCSDownload`
   - `TVCS`
   - `WebApp`
6. [ISAPI フィルター] タブを選択します。
7. 次の ISAPI フィルタを削除します。
   - TmcmRedirect
   - ReverseProxy

Apex Central のファイル/ディレクトリおよびレジストリキーを削除する

手順

1. 次のディレクトリを削除します。
   - `.Trend Micro¥Control Manager`
   - `.PHP`
   - `C:¥Documents and Settings¥All Users¥Start Menu¥Programs¥PHP 7`
   - `C:¥Documents and Settings¥All Users¥Start Menu¥Programs¥Trend Micro Apex Central`
2. レジストリエディタを起動し、次の Apex Central レジストリキーを削除します。

- HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\MCPAgent
- HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OPPTrustPort
- HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\TMI
- HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\TVCS
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TMCM

データベースコンポーネントの削除

ここでは、Apex Central サーバから次のデータベースコンポーネントを削除する方法について説明します。

- 89 ページの「Apex Central の ODBC 設定を削除する」
- 90 ページの「SQL Server 2017 Express データベースを削除する」

Apex Central の ODBC 設定を削除する

手順

1. Apex Central サーバで、Windows の [スタート] > [ファイル名を指定して実行] の順に選択します。

   [ファイル名を指定して実行] ダイアログボックスが表示されます。

2. [名前] ボックスに次のように入力します。

   ```
   odbcad32.exe
   ```

3. [ODBC データ ソース アドミニストレータ] 画面で、[システム DSN] タブをクリックします。
4. [名前] から [ControlManager_Database] を選択します。
5. [削除] をクリックし、[はい] をクリックして削除を確定します。

SQL Server 2017 Express データベースを削除する

手順

1. Apex Central サーバで、[スタート] > [コントロール パネル] > [プログラムの追加と削除] (または、[プログラムと機能]) をクリックします。
2. 画面を下へスクロールして [SQL Server 2017] を選択し、[削除] (または、[アンインストールと変更]) をクリックします。これで、関連する各ファイルが自動的に削除されます。

ヒント

SQL Server 2017 Express を削除する方法の詳細については、Microsoft のドキュメントを参照してください。

Apex Central サービスを削除する

手順

1. Microsoft のサービスツールである `Sc.exe` を実行します。
2. 次のコマンドを入力します。

```
sc delete "TMCM"
```

第 8 章

Apex Central のシステムチェックリスト

このセクションでは、システム関連情報を記入するためのチェックリストを参考として提供します。

次のトピックがあります。

- 92 ページの「サーバアドレスのチェックリスト」
- 93 ページの「ポートのチェックリスト」
- 93 ページの「Apex Central 入力規則」
- 94 ページの「コアプロセスおよび設定ファイル」
- 96 ページの「通信ポートおよびサービスポート」

サーバアドレスのチェックリスト

インストール処理の実行中、およびネットワークで使用する Trend Micro Apex Central サーバの設定時には、次のサーバアドレス情報を入力する必要があります。必要なときにいつでも参照できるように、ここに記録しておくことをお勧めします。

表 8-1. サーバアドレスのチェックリスト

必要な情報	EXAMPLE	設定する値
Apex Central サーバ情報		
IP アドレス	10.1.104.255	
FQDN (完全修飾ドメイン名)	server.example.com	
NetBIOS (ホスト) 名	yourserver	
Web サーバ情報		
IP アドレス	10.1.104.225	
FQDN (完全修飾ドメイン名)	server.example.com	
NetBIOS (ホスト) 名	yourserver	
Apex Central の SQL データベース情報		
IP アドレス	10.1.104.225	
FQDN (完全修飾ドメイン名)	server.example.com	
NetBIOS (ホスト) 名	sqlserver	
コンポーネントダウンロード用のプロキシサーバ		
IP アドレス	10.1.174.225	
FQDN (完全修飾ドメイン名)	proxy.example.com	
NetBIOS (ホスト) 名	proxyserver	
SMTP サーバ情報 (任意: メールメッセージ通知用)		
IP アドレス	10.1.123.225	

必要な情報	EXAMPLE	設定する値
FQDN (完全修飾ドメイン名)	mail.example.com	
NetBIOS (ホスト) 名	mailserver	
SNMP トラップ情報 (任意: SNMP トラップ通知用)		
コミュニティ名	trendmicro	
IP アドレス	10.1.194.225	
Syslog サーバ情報 (任意: Syslog 通知用)		
IP アドレス	10.1.194.225	
サーバポート番号	514	

ポートのチェックリスト

Apex Central では、次のポートをそれぞれの目的に使用します。

ポート	例	設定する値
SMTP	25	
プロキシ	8088	
管理コンソールおよびアップデート/配信コンポーネント	443	

Apex Central 入力規則

Apex Central のインストールまたは管理コンソールの設定には、次の規則が適用されますので注意してください。

- ユーザ名
  - 最大長: 32 文字
  - 使用できる文字: `A～Z`、`a～z`、`0～9`、「`-`」、「`_`」、「`.`」、「`$`」
- フォルダ名

- 最大文字数: 32 文字
- 使用できない文字: 「/」、「>」、「&」、「"」、「%」、「^」、「=」

注意

Apex Central サーバのホスト名については、インストール時にアンダースコア (_) を使用できます。

コアプロセスおよび設定ファイル

Apex Central では、システム設定および一時ファイルが XML 形式で保存されます。

次の表は、Apex Central で使用される設定ファイルおよびプロセスを示しています。

表 8-2. Apex Central 設定ファイル

設定ファイル	説明
AuthInfo.ini	プライベートキーファイル名、公開鍵ファイル名、証明書ファイル名、プライベートキーの暗号化されたパスフレーズ、ホスト ID、およびポートに関する情報を含む設定ファイルです。
aucfg.ini	アップデート設定ファイル
TVCS_Cert.pem	SSL 認証で使用される証明書です。
TVCS_Pri.pem	SSL で使用されるプライベートキーです。
TVCS_Pub.pem	SSL で使用される公開鍵です。
ProcessManager.xml	ProcessManager.exe で使用されます。
CmdProcessorEventHandler.xml	CmdProcessor.exe で使用されます。
DMRegisterinfo.xml	CasProcessor.exe で使用されます。
DataSource.xml	Apex Central のプロセスの接続パラメータを保存します。

設定ファイル	説明
SystemConfiguration.xml	Apex Central システム設定ファイル
agent.ini	MCP エージェントのファイルです。

表 8-3. Apex Central コアプロセス

プロセス	説明
ProcessManager.exe	Apex Central のコアプロセスを起動および停止します。
CmdProcessor.exe	他のプロセスによって作成された XML 命令の管理下の製品への送信、製品の登録の処理、アラートの送信、スケジュールされたタスクの実行、大規模感染予防ポリシーの適用などを行います。
LogReceiver.exe	過去のバージョンとの互換性のためにのみに使用します。
LogProcessor.exe	管理下の製品からログを受信し、管理下の製品からエンティティ情報を受信します。
LogRetriever.exe	ログを受信し、Apex Central データベースに保存します。
ReportServer.exe	Apex Central レポートを生成します。
MsgReceiver.exe	Apex Central サーバおよび管理下の製品からメッセージを受信します。
CasProcessor.exe	Apex Central サーバが他の Apex Central サーバを管理できるようにします。
inetinfo.exe	Microsoft Internet Information Service プロセスです。
cm.exe	dmserver.exe および mrf.exe を管理します。
dmserver.exe	Apex Central 管理コンソールのログオンページを提供し、製品ディレクトリ (Apex Central 側) を管理します。
sCloudProcessor.NET.exe	ステータスの照会、結果の照会、要求のキャンセルを行うために、Apex Central 管理コンソールまたはその他のプロセスに発行者のジョブ ID を提供するように要求します。ユーザ/エンドポイントディレクトリによって使用されます。

通信ポートおよびサービスポート

初期設定の Apex Central 通信ポートおよびサービスポートは次のとおりです。

サービス	サービスポート
ProcessManager.exe	20501
CmdProcessor.exe	20101
comdProcessor.NET.exe	21003
LogReceiver.exe	20201
LogProcessor.exe	21001
LogRetriever.exe	20301
ReportServer.exe	20601
MsgReceiver.exe	20001
CasProcessor.exe	20801
sCloudProcessor.NET.exe	21002

索引

アルファベット

Active Directory
- 手動同期, 55
- 接続の設定, 55
- 同期の頻度, 55

Apex Central, 1, 2, 5
- MCP, 5
- SQL データベース, 5
- Web サーバ, 5
- Web サービスの統合, 5
- Web ベースの管理コンソール, 6
- アクティベーション, 53, 54
- インストール, 29, 35, 36
- インストール手順, 36
- ウィジェットフレームワーク, 6
- Control Manager, 1
- について, 2
- コマンドプロンプト、サービスの停止, 87
- しすてむようけん, 30
- 手動アンインストール, 85, 86
- メールサーバ, 5
- ライセンス情報, 54
- レポートサーバ, 5

Control Manager
- セキュリティレベル, 44
- テストインストールの実施, 15
- データベースの移行, 69

DBConfig ツール, 69

MCP, 5
- コマンドポーリング, 22
- 接続ステータス, 22
- ポリシー, 21

ODBC
- 設定、Control Manager, 89

Web サーバ
- 計画, 26
- 設定, 26

Web サーバ設定, 42

Windows Server 2012, 31

Windows Server 2012 R2, 32

Windows Server 2016, 33

Windows Server 2019, 34

Windows Server 2022, 34

あ

アクティベーション
- Apex Central, 53, 54

アクティベーションコード, 53

アップグレード, 62
- 製品版, 54

アップデート
- 配信, 23

アンインストール
- Apex Central 手動, 85
- 手動
  - Apex Central, 86

移行, 68
- Control Manager SQL 2000, 69
- 一括アップグレード, 68
- 計画, 68
- 段階的アップグレード, 68
- データベース, 69

一括アップグレード, 68

インストール
- Apex Central, 29, 36
- 正常確認, 52
- 手順, 36
- フロー, 14

インストール手順

Apex Central, 36

か

概要
集中管理, 8
分散管理, 10
コマンドプロンプト
Apex Central、サービスの停止, 87
コマンドポーリング
MCP, 22

さ

削除
手動
Microsoft Data Engine, 89
サーバ
アドレスのチェックリスト, 92
サーバアドレスのチェックリスト, 92
サーバの配置計画, 16
システム要件, 30
集中管理
概要, 8
手動
Apex Central のアンインストール, 86
手動アンインストール, 85
推奨設定
データベース, 24
正常なインストールの確認, 52
製品登録
トラフィック, 22
製品版
アップグレード, 54
接続ステータス, 19
MCP, 22
設定
Web サーバ, 26
ユーザアカウント, 58

た

段階的アップグレード, 68
チェックリスト
サーバアドレス, 92
ポート, 93
ツール
DBConfig ツール, 69
テストインストール
テスト, 15
データベース
計画, 24
推奨設定, 24
ドキュメント, 2
トラフィック、ネットワーク, 18

な

ネットワークトラフィック
発生元, 20
ネットワークトラフィックの計画, 18

は

配置
アーキテクチャと戦略, 8
集中, 8
複数の拠点, 10
分散管理
概要, 10
ポリシー
MCP, 21
ポート
チェックリスト, 93

や

ユーザアカウント

設定, 58
用語, 4

ら

ライセンス情報, 54
レジストレーションキー, 55
ログ
トラフィック, 20