



Trend Micro Mobile Security™ 9.8

インストールおよびクライアント配信ガイド



Endpoint Security

※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/jp/support-policies>

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、およびSmart Check 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 © 2020 Trend Micro Incorporated. All rights reserved.

P/N: TSEM98073/171018_JP_R1 (2020/09)

目次

はじめに

はじめに	7
対象読者	8
Mobile Security ドキュメント	8
ドキュメントの表記規則	9

第 1 章 : サーバインストールの計画

Mobile Security システムのアーキテクチャ	12
クラウドコミュニケーションサーバを使用するセキュリティ強化モデル (デュアルサーバ環境)	13
ローカルコミュニケーションサーバを使用するセキュリティ強化モデル (デュアルサーバ環境)	14
基本的なセキュリティモデル (単一サーバ環境)	15
Mobile Security のコンポーネント	15
ローカルコミュニケーションサーバとクラウドコミュニケーションサーバの比較	19
システム要件	19
インストールの概要	20

第 2 章 : 環境の設定

Mobile Security をインストールするための環境を設定する	28
iOS デバイス用の環境を設定する (オプション)	29
Microsoft IIS Web サーバをインストールする	32
SQL Server をインストールする (オプション)	33
Active Directory アカウントのアクセス権を設定する (オプション)	34
Microsoft Exchange Server 管理ツールをインストールする (オプション)	35

Mobile Security のネットワークアクセスルールを適用する	36
---	----

第 3 章 : サーバコンポーネントのインストール、アップデート、削除

サーバコンポーネントをインストールする	39
インストールする前に	39
Trend Micro Mobile Security のインストールワークフロー	39
マネージメントサーバをインストールする	40
ローカルコミュニケーションサーバをインストールする ..	50
Exchange Server との統合を設定する	52
コンポーネントのアップデート	58
Mobile Security のアップグレードについて	58
Mobile Security コンポーネントのアップデート	59
ローカルのアップデート元の手動アップデート	62
サーバコンポーネントを削除する	63

第 4 章 : サーバコンポーネントの設定

初期サーバセットアップ	67
データベースを設定する	69
コミュニケーションサーバを設定する	70
配信を設定する	75
デバイス登録の設定を行う	76
Mobile Security の利用条件をカスタマイズする	78
AD (Active Directory) の設定	79
マネージメントサーバを設定する	80
Exchange Server との統合を設定する	81
通知とレポートを設定する	83
管理者への通知を設定する	84
Mobile Security の設定を検証する	85

第 5 章 : Mobile Device エージェントの操作

サポート対象のモバイルデバイスとプラットフォーム	88
デバイスのストレージとメモリ	88
Mobile Device エージェントを設定する	89
サーバで登録依頼のメールを設定する (オプション)	90

モバイルデバイスに MDA をインストールする	95
Mobile Security マネージメントサーバに MDA を登録する ..	99
モバイルデバイスの MDA をアップグレードする	105

付録 A : ネットワークポートの設定

クラウドコミュニケーションサーバを使用するセキュリティ強化モデルのネットワークポートの設定	108
ローカルコミュニケーションサーバを使用するセキュリティ強化モデルのネットワークポートの設定	110
基本的なセキュリティモデルのネットワークポートの設定	114

付録 B : オプションの設定

SQL Server に Windows 認証を使用する	120
コミュニケーションサーバのポートを設定する	122
SCEP を設定する	123

付録 C : APNs 証明書の生成と設定

APNs 証明書について	128
APNs 証明書を生成する	128
Windows Server から APNs 証明書を生成する	129
Mac OS X ワークステーションから APNs 証明書を生成する	142
Mobile Security マネージメントサーバに APNs 証明書をアップロードする	148
APNs 証明書を更新する	150

索引


索引	153
----------	-----

はじめに

はじめに

Trend Micro Mobile Security 9.8 (以下、Mobile Security)インストールおよびクライアント配信ガイドをお読みいただきありがとうございます。このガイドは、管理者が Mobile Security を配置して管理する際に役立つ情報を提供します。また、さまざまな Mobile Security コンポーネント、および Mobile Device エージェントの設定やインストール方法について説明します。

モバイルデバイスのサポートや最新のビルドなどの Mobile Security の最新情報については、次の Web サイトをご覧ください。https://www.trendmicro.com/ja_jp/business/products/user-protection/sps/mobile.html

 **注意**

このガイドには、Mobile Security 9.8 に関する説明のみが含まれており、以前のバージョンに関する記載は含まれていません。トレンドマイクロでは、Mobile Security の使用に関するサポートのみを提供します。このガイドに記載されているサードパーティ製のアプリケーションのサポートを受けるには、それぞれのベンダーにお問い合わせください。

ここでは、次のトピックについて説明します。

- 8 ページの「対象読者」
- 8 ページの「Mobile Security ドキュメント」
- 9 ページの「ドキュメントの表記規則」

対象読者

Mobile Security のドキュメントは、企業環境で Mobile Device エージェントの管理を担当する管理者と、モバイルデバイスユーザの両方を対象としています。

管理者には、次のような Windows システム管理とモバイルデバイスのポリシーに関する中級～上級レベルの知識が必要です。

- Windows サーバのインストールと設定
- Windows サーバへのソフトウェアのインストール
- モバイルデバイスの設定と管理
- ネットワーク概念 (IP アドレス、ネットマスク、トポロジ、および LAN の設定など)
- 各種のネットワークテクノロジー
- ネットワークデバイスとその管理
- ネットワーク設定 (VLAN、HTTP、および HTTPS の使用など)

Mobile Security ドキュメント

Mobile Security ドキュメントは、次の内容で構成されています。

- **インストールおよびクライアント配信ガイド:** このガイドでは、Mobile Security について紹介し、ネットワークのプランニング、インストール、配信の準備、および稼働をサポートします。
- **管理者ガイド:** このガイドでは、Mobile Security 設定ポリシーおよびテクノロジーの詳細について説明します。
- **オンラインヘルプ:** オンラインヘルプでは、製品の主な機能の操作手順、使用方法のアドバイス、および有効なパラメータ範囲や最適値などのフィールド固有の情報を提供します。
- **Readme:** 他のドキュメントには記載されていない可能性のある最新の製品情報を提供します。トピックには、機能の説明、インストールの説明、既知の制限事項、および製品のリリースの履歴などが含まれます。

- サポートポータル: サポートポータルは、問題解決およびトラブルシューティングに関する情報を集めたオンラインデータベースです。製品の既知の問題に関する最新情報が提供されています。サポートポータルには、次の URL からアクセスできます。

<https://success.trendmicro.com/jp/technical-support>






ヒント

最新のドキュメントファイルは、弊社ダウンロードサイト (http://downloadcenter.trendmicro.com/index.php?clk=left_nav&clkval=all_download®s=jp) から入手できます。

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
 警告!	避けるべき操作や設定についての注意

第 1 章

サーバインストールの計画

この章では、管理者が Trend Micro Mobile Security 9.8 のサーバコンポーネントに関する計画を立てる際に役立つ情報を提供します。

この章には、次のセクションが含まれています。

- 12 ページの「Mobile Security システムのアーキテクチャ」
- 13 ページの「クラウドコミュニケーションサーバを使用するセキュリティ強化モデル (デュアルサーバ環境)」
- 14 ページの「ローカルコミュニケーションサーバを使用するセキュリティ強化モデル (デュアルサーバ環境)」
- 15 ページの「基本的なセキュリティモデル (単一サーバ環境)」
- 15 ページの「Mobile Security のコンポーネント」
- 19 ページの「システム要件」
- 20 ページの「インストールの概要」

Mobile Security システムのアーキテクチャ

企業のニーズに応じて、さまざまなクライアント/サーバ間の通信手段を使用して Mobile Security を実装できます。ネットワーク内で1つまたは任意の組み合わせのクライアント/サーバ通信手段を選択することもできます。

Trend Micro Mobile Security は3つの異なる配置モデルをサポートしています。

- クラウドコミュニケーションサーバを使用するセキュリティ強化モデル (デュアルサーバ環境)
- ローカルコミュニケーションサーバを使用するセキュリティ強化モデル (デュアルサーバ環境)
- 基本的なセキュリティモデル (単一サーバ環境)

クラウドコミュニケーションサーバを使用するセキュリティ強化モデル (デュアルサーバ環境)

本モデルでは、コミュニケーションサーバをクラウドに配置できます。次の図に、本モデルにおける、各 Mobile Security コンポーネントの配置を示します。

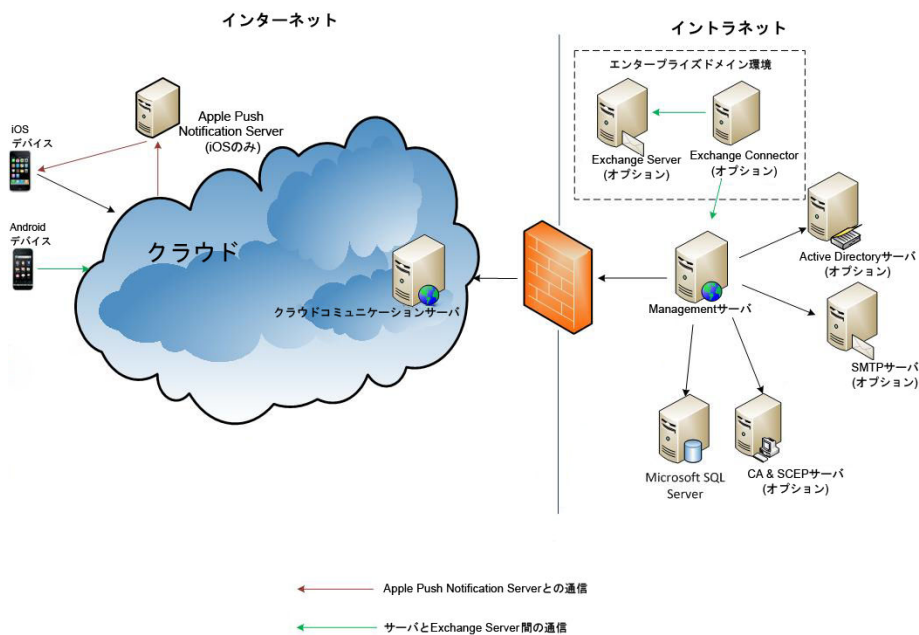


図 1-1. クラウドコミュニケーションサーバを使用するセキュリティ強化モデル

ローカルコミュニケーションサーバを使用するセキュリティ強化モデル (デュアルサーバ環境)

本モデルでは、コミュニケーションサーバとマネジメントサーバをそれぞれのコンピュータにインストールできます。次の図に、本モデルにおける、各 Mobile Security コンポーネントの配置を示します。

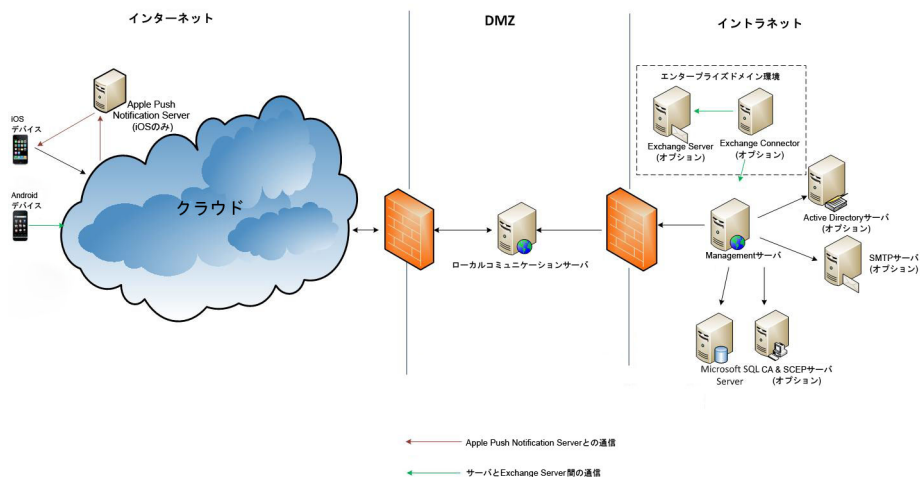


図 1-2. ローカルコミュニケーションサーバを使用するセキュリティ強化モデル

基本的なセキュリティモデル (単一サーバ環境)

本モデルでは、同じコンピュータにコミュニケーションサーバとマネジメントサーバをインストールできます。次の図に、本モデルにおける、各 Mobile Security コンポーネントの配置を示します。

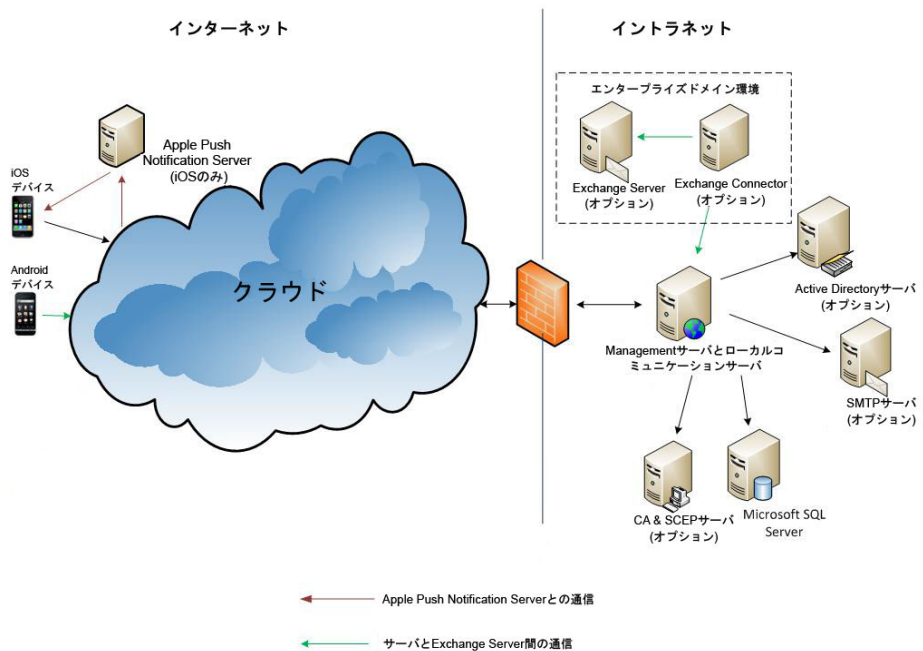


図 1-3. 基本的なセキュリティモデル


Mobile Security のコンポーネント

次の表は、Mobile Security コンポーネントの説明をまとめたものです。

表 1-1. Mobile Security のコンポーネント

コンポーネント	説明	必須/オプション
マネージメントサーバ	<p>マネージメントサーバでは、Web 管理コンソールから Mobile Device エージェントを管理できます。モバイルデバイスをサーバに登録すると、Mobile Device エージェントのポリシーを設定してアップデートを実行できます。</p>	必須
コミュニケーションサーバ	<p>コミュニケーションサーバはマネージメントサーバと Mobile Device エージェント間の通信を処理します。</p> <p>Trend Micro Mobile Security には、次の 2 種類のコミュニケーションサーバが用意されています。</p> <ul style="list-style-type: none"> • ローカルコミュニケーションサーバ (LCS): ネットワーク内にローカルに配置されたコミュニケーションサーバです。 • クラウドコミュニケーションサーバ (CCS): クラウドに配置されたコミュニケーションサーバです。インストールは必要ありません。クラウドコミュニケーションサーバはトレンドマイクロが管理します。ユーザはマネージメントサーバからこのサーバに接続するだけです。 <p>詳細については19 ページの「ローカルコミュニケーションサーバとクラウドコミュニケーションサーバの比較」を参照してください。</p>	必須

コンポーネント	説明	必須/オプション
Exchange Connector	<p>Trend Micro Mobile Security は Exchange Connector を使用して Microsoft Exchange Server と通信し、Exchange ActiveSync サービスを利用するデバイスをすべて検出して Mobile Security の Web コンソールに表示します。</p> <p>Microsoft Exchange Server と統合することにより、Microsoft Exchange Server にアクセスするモバイルデバイスを Mobile Security で監視できるようになります。この機能を有効にして設定すると、Mobile Security 管理者が Microsoft Exchange Server にアクセスするモバイルデバイスに対してリモート消去を実行したり、Microsoft Exchange Server へのアクセスをブロックしたりできます。</p> <p>Microsoft Exchange Server と Mobile Security の統合により、企業データ (メール、カレンダー、連絡先など) へのアクセスも制御できるようになります。</p>	オプション
Mobile Device エージェント (MDA)	<p>Mobile Device エージェントは、管理対象の Android および iOS デバイ스에インストールされます。このエージェントは、Mobile Security コミュニケーションサーバと通信し、モバイルデバイスでコマンドやポリシー設定を実行します。</p>	必須
Microsoft SQL Server	<p>Microsoft SQL Server は、Mobile Security マネージメントサーバ用のデータベースです。</p>	必須
Active Directory	<p>Mobile Security マネージメントサーバは、Active Directory からユーザとグループをインポートします。</p>	オプション
CA (証明機関)	<p>CA (証明機関) は、セキュリティで保護された通信を行うためのセキュリティ認証情報および公開鍵/秘密鍵を管理します。</p>	オプション

コンポーネント	説明	必須/オプション
SCEP	<p>SCEP (Simple Certificate Enrollment Protocol) は、プライベート証明機関へのネットワークフロントエンドを提供する通信プロトコルです。</p> <p>環境によっては、企業の設定やポリシーが外部から見られないように保護することが重要になります。このような保護を提供するために、iOS では、そのデバイスでしか読めないようにプロファイルを暗号化できます。暗号化されたプロファイルは、デバイスの X.509 ID に関連付けられた公開鍵を使用してペイロードが暗号化されている点を除き、通常の設定プロファイルと同じです。</p> <p>大規模な企業で証明書を発行するには、SCEP を CA とともに使用します。SCEP は、デジタル証明書の発行および失効を処理します。SCEP と CA は同じサーバにインストールできます。</p>	オプション
APNs 証明書	<p>(フル機能配信モードと指定以外の MDM ベンダーを使用するセキュリティ対策限定配信モード)。</p> <p>Mobile Security コミュニケーションサーバは、Apple Push Notification サービス (APNs) を利用して iOS デバイスと通信します。</p> <hr/> <p> 注意</p> <p>APNs 証明書は毎年更新する必要があります。詳しくは、以下をご参照ください。</p> <p>https://success.trendmicro.com/jp/solution/1096556</p>	iOS デバイスを管理する場合は必須
SSL 証明書	<p>(フル機能配信モードと指定以外の MDM ベンダーを使用するセキュリティ対策限定配信モード)。</p> <p>Trend Micro Mobile Security で、HTTPS を使用してモバイルデバイスとコミュニケーションサーバ間のセキュリティで保護された通信を実現するには、パブリック CA から発行された SSL サーバ証明書が必要です。</p>	iOS デバイスを管理する場合は必須

コンポーネント	説明	必須/オプション
SMTP サーバ	管理者が Mobile Security マネージメントサーバからレポートを取得したり、ユーザに登録依頼のメールを送信したりするには、SMTP サーバに接続します。	オプション

ローカルコミュニケーションサーバとクラウドコミュニケーションサーバの比較

次の表では、ローカルコミュニケーションサーバ (LCS) とクラウドコミュニケーションサーバ (CCS) を比較します。

表 1-2. ローカルコミュニケーションサーバとクラウドコミュニケーションサーバの比較

機能	クラウドコミュニケーションサーバ	ローカルコミュニケーションサーバ
インストールの必要性	なし	あり
ユーザ認証方式のサポート	登録キー	Active Directory または登録キー
Android 用エージェントのカスタマイズ	サポートあり	サポートあり

システム要件

Mobile Security をインストールする前に、システム要件を確認してください。最新のシステム要件については、次の Web サイトを参照してください。

<http://www.go-tm.jp/tmms/req>

インストールの概要

Trend Micro Mobile Security のインストール手順は次のとおりです。

1. Mobile Security をインストールするための環境を準備する。
詳細については、[28 ページの「Mobile Security をインストールするための環境を設定する」](#)を参照してください。
 - a. マネージメントサーバのインストール先となるコンピュータに Microsoft IIS Web サーバをインストールする。
詳細については、[32 ページの「Microsoft IIS Web サーバをインストールする」](#)を参照してください。
 - b. (オプション) データベースをインストールする。
この手順を省略した場合、Mobile Security のインストール時に Microsoft SQL Server 2017 Express Edition が自動的にインストールされます。
詳細については、[33 ページの「SQL Server をインストールする \(オプション\)」](#)を参照してください。
 - c. (オプション) Active Directory アカウントのアクセス権を設定する。
企業の Active Directory サーバからユーザをインポートする場合は、この手順を実行してください。
詳細については、[34 ページの「Active Directory アカウントのアクセス権を設定する \(オプション\)」](#)を参照してください。
 - d. (オプション) Microsoft Exchange Server 管理ツールをインストールする。
Exchange Server とマネージメントサーバが統合され、Android および iOS デバイスを管理できるようになります。
詳細については、[35 ページの「Microsoft Exchange Server 管理ツールをインストールする \(オプション\)」](#)を参照してください。
 - e. ネットワークのアクセス設定を適用する。

詳細については、36 ページの「[Mobile Security のネットワークアクセスルールを適用する](#)」を参照してください。

2. (オプション) iOS デバイス用の環境を準備する。

詳細については、29 ページの「[iOS デバイス用の環境を設定する \(オプション\)](#)」を参照してください。

3. サーバコンポーネントをインストールする。

詳細については、39 ページの「[サーバコンポーネントをインストールする](#)」を参照してください。

- a. Mobile Security マネージメントサーバをインストールする。

詳細な手順については、40 ページの「[マネージメントサーバをインストールする](#)」を参照してください。

- b. Mobile Security の Web 管理コンソールにログオンする。

詳細な手順については、46 ページの「[Web 管理コンソールにアクセスする](#)」を参照してください。

- c. 製品を登録する。

詳細な手順については、48 ページの「[製品を登録する](#)」を参照してください。

- d. (オプション) ローカルコミュニケーションサーバ (LCS) をダウンロードしてインストールする。

クラウドコミュニケーションサーバ (CCS) を使用する場合は、この手順を省略できます。

詳細な手順については、50 ページの「[ローカルコミュニケーションサーバをインストールする](#)」を参照してください。

- e. (オプション) Exchange Server との統合を設定する。

Exchange ActiveSync を使用するモバイルデバイスを管理しない場合は、この手順を省略できます。

詳細な手順については、55 ページの「[Exchange Connector をインストールする](#)」を参照してください。

- i. Microsoft Exchange Server 管理ツールがインストールされていることを確認する。

インストール手順については、35 ページの「[Microsoft Exchange Server 管理ツールをインストールする \(オプション\)](#)」を参照してください。
- ii. Exchange Connector のアカウントを設定する。

Exchange Connector 用のアクセス権が提供されます。

詳細な手順については、53 ページの「[Exchange Connector のアカウントを設定する](#)」を参照してください。
- iii. Exchange Connector をインストールする。

マネージメントサーバと Exchange Server 間の通信が確立されません。

詳細な手順については、55 ページの「[Exchange Connector をインストールする](#)」を参照してください。
- iv. Exchange Server との統合を設定する。

詳細な手順については、81 ページの「[Exchange Server との統合を設定する](#)」を参照してください。

4. サーバコンポーネントを設定する。

詳細については、67 ページの「[初期サーバセットアップ](#)」を参照してください。

- a. サーバの配置を設定する。

詳細な手順については、75 ページの「[配信を設定する](#)」を参照してください。
- b. データベースを設定する。

詳細な手順については、69 ページの「[データベースを設定する](#)」を参照してください。
- c. コミュニケーションサーバを設定する。

詳細な手順については、70 ページの「コミュニケーションサーバの共通項目を設定する」を参照してください。

- d. (オプション) Android 用のコミュニケーションサーバを設定する。

Android デバイスを管理しない場合は、この手順を省略できます。

詳細な手順については、72 ページの「Android のコミュニケーションサーバを設定する」を参照してください。

- e. (オプション) iOS 用のコミュニケーションサーバを設定する。

iOS デバイスを管理しない場合は、この手順を省略できます。

詳細な手順については、73 ページの「iOS のコミュニケーションサーバを設定する」を参照してください。

- f. デバイスの登録設定を構成する。

詳細な手順については、76 ページの「デバイス登録の設定を行う」を参照してください。

- g. (オプション) Mobile Security の利用条件をカスタマイズする。

Mobile Security の利用条件を初期設定のまま使用する場合は、この手順を省略できます。

詳細な手順については、78 ページの「Mobile Security の利用条件をカスタマイズする」を参照してください。

- h. (オプション) Active Directory を設定する

Active Directory サーバからユーザをインポートしない場合は、この手順を省略できます。

詳細な手順については、79 ページの「AD (Active Directory) の設定」を参照してください。

- i. (オプション) マネージメントサーバの設定を構成する。

マネージメントサーバがインターネットへのアクセスにプロキシを使用せず、初期設定のサーバ IP アドレスおよびポート番号を使用する場合は、この手順を省略できます。

詳細な手順については、[80 ページの「マネージメントサーバを設定する」](#)を参照してください。

- j. (オプション) Exchange Server との統合を設定する。

Exchange ActiveSync を使用するモバイルデバイスを管理しない場合は、この手順を省略できます。

詳細な手順については、[81 ページの「Exchange Server との統合を設定する」](#)を参照してください。

- k. (オプション) 通知とレポートを設定する。

登録依頼のメールをユーザに送信しない場合は、この手順を省略できます。

全体の手順を確認したい場合は、[83 ページの「通知とレポートを設定する」](#)を参照してください。

- l. (オプション) 管理者への通知を設定する。

エラーメッセージの通知と通常の定期レポートをメールで受信しない場合は、この手順を省略できます。

詳細な手順については、[84 ページの「管理者への通知を設定する」](#)を参照してください。

- m. Mobile Security の設定を検証する (推奨)。

手順については、[85 ページの「Mobile Security の設定を検証する」](#)を参照してください。

- n. Web 管理コンソールで使用する管理者アカウントのパスワードを変更する。

手順については、「[管理者ガイド](#)」の「[管理者アカウントを編集する](#)」を参照してください。

- 5. Mobile Device エージェントを設定する。

[89 ページの「Mobile Device エージェントを設定する」](#)

- a. (オプション) モバイルデバイス向けの通知を設定する

詳細な手順については、[83 ページの「通知とレポートを設定する」](#)を参照してください。

- b. (オプション) Mobile Security で、ユーザに送信するインストールメッセージを設定する。

インストールメッセージには、ユーザが MDA のセットアップパッケージをダウンロードしてインストールするための URL が含まれます。

詳細な手順については、[90 ページの「インストールメッセージを設定する」](#)を参照してください。

- c. (オプション) ユーザに登録依頼のメールを送信する。

詳細な手順については、[91 ページの「ユーザに登録を依頼する」](#)を参照してください。

- d. モバイルデバイスに MDA をインストールする。

詳細な手順については、[95 ページの「モバイルデバイスに MDA をインストールする」](#)を参照してください。

- e. マネージメントサーバに MDA を登録する。

詳細な手順については、[99 ページの「Mobile Security マネージメントサーバに MDA を登録する」](#)を参照してください。

第 2 章

環境の設定

この章では、Trend Micro Mobile Security 9.8 をインストールする前の環境設定に必要な情報を提供します。

この章には、次のセクションが含まれています。

- 28 ページの「Mobile Security をインストールするための環境を設定する」
- 29 ページの「iOS デバイス用の環境を設定する (オプション)」
- 32 ページの「Microsoft IIS Web サーバをインストールする」
- 33 ページの「SQL Server をインストールする (オプション)」
- 34 ページの「Active Directory アカウントのアクセス権を設定する (オプション)」
- 36 ページの「Mobile Security のネットワークアクセスルールを適用する」
- 35 ページの「Microsoft Exchange Server 管理ツールをインストールする (オプション)」

Mobile Security をインストールするための環境を設定する

次の表に、Mobile Security をインストールする際の設定手順を記載します。

表 2-1. Mobile Security をインストールするための環境を設定するプロセス

手順	操作	説明
手順 1	マネージメントサーバのインストール先となるコンピュータに Microsoft IIS Web サーバをインストールする。	詳細については、 32 ページの「Microsoft IIS Web サーバをインストールする」 を参照してください。
手順 2	(オプション) データベースをインストールする。	この手順を省略した場合、Mobile Security のインストール時に Microsoft SQL Server 2017 Express Edition が自動的にインストールされます。 詳細については 33 ページの「SQL Server をインストールする (オプション)」 を参照してください。
手順 3	(フル機能配信モードと指定以外の MDM ベンダーを使用するセキュリティ対策限定配信モード)。 (オプション) Active Directory アカウントのアクセス権を設定する。	企業の Active Directory サーバからユーザをインポートする場合は、この手順を実行してください。 詳細については 34 ページの「Active Directory アカウントのアクセス権を設定する (オプション)」 を参照してください。
手順 4	(フル機能配信モードのみ)。 (オプション) Microsoft Exchange Server 管理ツールをインストールする。	Exchange Server と Mobile Security マネージメントサーバが統合され、Android および iOS デバイスを管理できるようになります。 詳細については 35 ページの「Microsoft Exchange Server 管理ツールをインストールする (オプション)」 を参照してください。

手順	操作	説明
手順 5	ネットワークのアクセス設定を適用する。	<p>詳細については36 ページの「Mobile Security のネットワークアクセスルールを適用する」を参照してください。</p> <p>ネットワークポートの設定全体を確認するには、107 ページのネットワークポートの設定を参照してください。</p>
手順 6	(オプション) iOS デバイスを管理するための環境を設定する。	<p>iOS デバイスを管理する場合は、必ずこの手順を実行してください。</p> <p>詳細については29 ページの「iOS デバイス用の環境を設定する (オプション)」を参照してください。</p>

iOS デバイス用の環境を設定する (オプション)



警告!


iOS デバイスを管理する環境を設定する前に、次の表に記載したすべての手順を完了してください。

次の表に、iOS デバイスを管理する際の設定手順を記載します。

表 2-2. iOS デバイス用の環境を設定するプロセス

手順	操作	説明
手順 1	<p>(フル機能配信モードと指定以外の MDM ベンダーを使用するセキュリティ対策限定配信モード)。</p> <p>APNs (Apple Push Notification サービス) 証明書を設定する。</p>	<p>iOS デバイスを管理する場合、APNs 証明書を設定する必要があります。</p> <p>詳細な手順については、127 ページの APNs 証明書の生成と設定を参照してください。</p>

手順	操作	説明
手順 2	(フル機能配信モードのみ)。 (オプション)パブリック CA から SSL サーバ証明書を取得する。	<p>SSL 証明書によって、モバイルデバイスとコミュニケーションサーバ間の通信がセキュリティで保護されません。</p> <p>iOS デバイスを管理する場合、またはローカルコミュニケーションサーバを使用する場合は、必ずこの手順を実行してください。ローカルコミュニケーションサーバのインストール中に、パブリック SSL 証明書をインポートする必要があります。</p> <p>次の場合は、この手順を省略できません。</p> <ul style="list-style-type: none">• プライベート SSL 証明書を使用する場合。ローカルコミュニケーションサーバのインストール中、Mobile Security によってこの証明書が作成されます。• クラウドコミュニケーションサーバを使用する場合。

手順	操作	説明
手順 3	(フル機能配信モードのみ)。 (オプション) SCEP (Simple Certificate Enrollment Protocol) を設定してセキュリティを強化する	<p>モバイルデバイスとコミュニケーションサーバ間の通信がセキュリティで保護されます。</p> <p>詳細については、123 ページの「SCEP を設定する」を参照してください。</p> <p>環境内に SCEP が設定されている場合は、この手順を省略できます。</p> <hr/> <p> 注意</p> <p>iOS デバイスで SCEP を使用しない場合は、マネージメントサーバとコミュニケーションサーバをインストールした後、コミュニケーションサーバの設定で SCEP を無効にする必要があります。手順については、73 ページの「iOS のコミュニケーションサーバを設定する」を参照してください。</p>

手順	操作	説明
手順 4	ローカルコミュニケーションサーバでネットワークポート 2195 (TCP) を設定し、Wi-Fi ネットワークで 5223 を設定する	<p>TCP ポート 2195 を使用すると、コミュニケーションサーバから APNs への送信接続が可能になります。APNs のホスト名は「gateway.push.apple.com」です。</p> <p>ポート 5223 を使用すると、iOS デバイスで Apple のサーバからプッシュ通知を受信できます。接続時に経由する Wi-Fi ネットワークでポート 5223 がブロックされている場合は、このポートを設定してください。モバイルデバイスが 3G ネットワークに接続している場合は、このポートを設定する必要はありません。</p> <p>ネットワークポートの設定全体を確認するには、107 ページのネットワークポートの設定を参照してください。</p>

Microsoft IIS Web サーバをインストールする

この項目は、マネージメントサーバに Microsoft IIS Web サーバをインストールする際の手順を記載します。

全体の手順を確認したい場合は、[28 ページの「Mobile Security をインストールするための環境を設定する」](#)を参照してください。

手順

- 次のいずれかの URL にアクセスして、IIS をインストールします。
 - Windows 2008 または Windows Server 2008 R2 (IIS 7.0 または 7.5) の場合
<http://www.iis.net/learn/install/installing-iis-7>
 - Windows 2012 (IIS 8.0) の場合

<http://www.iis.net/learn/get-started/whats-new-in-iis-8/installing-iis-8-on-windows-server-2012>

**注意**

マネージメントサーバに IIS 7.0 以降を使用する場合、初期設定を変更せずに、アプリケーション開発で CGI と ISAPI 拡張機能、HTTP 共通機能で HTTP リダイレクト、管理ツールで IIS6 管理互換をそれぞれオンにして、インストールします。

SQL Server をインストールする (オプション)

**注意**

特定のバージョンの SQL Server をインストールしない場合は、この手順を省略できます。Mobile Security のインストール時には、Microsoft SQL Server 2017 Express Edition が自動的にインストールされます。

この項目は、任意の SQL Server をインストールする際の手順です。

全体の手順を確認したい場合は、[28 ページの「Mobile Security をインストールするための環境を設定する」](#)を参照してください。

手順

- 次のいずれかの URL にアクセスして、SQL Server をインストールします。
 - Microsoft SQL Server 2008/2008 R2 (または Express Edition) の場合
[http://msdn.microsoft.com/ja-jp/library/ms143219\(v=SQL.100\).aspx](http://msdn.microsoft.com/ja-jp/library/ms143219(v=SQL.100).aspx)
 - Microsoft SQL Server 2012 (または Express Edition) の場合
[http://msdn.microsoft.com/ja-jp/library/bb500395\(v=SQL.110\).aspx](http://msdn.microsoft.com/ja-jp/library/bb500395(v=SQL.110).aspx)



SQL Server には、Windows 認証方式でなく SQL Server 認証方式を使用することをお勧めします。ただし、SQL Server に Windows 認証を設定することもできます。詳細については、[120 ページの「SQL Server に Windows 認証を使用する」](#)を参照してください。

Active Directory アカウントのアクセス権を設定する (オプション)



このトピックは、フル機能配信モードと指定以外の MDM ベンダーを使用するセキュリティ対策限定配信モードに該当します。



この手順を実行する必要があるのは、ユーザ認証に Active Directory を使用する場合、または Active Directory からユーザをインポートする場合のみです。それ以外の場合は、この手順を省略してください。

Active Directory をまだインストールしていない場合は、次の URL で詳細なインストール手順を参照してください。

[http://technet.microsoft.com/ja-jp/library/cc757211\(WS.10\).aspx](http://technet.microsoft.com/ja-jp/library/cc757211(WS.10).aspx)

この項目は、Active Directory アカウントのアクセス権を設定する際の手順です。

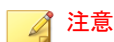
全体の手順を確認したい場合は、[28 ページの「Mobile Security をインストールするための環境を設定する」](#)を参照してください。

手順

- Mobile Security 9.8 用の Active Directory サービスアカウントを作成し、Active Directory に対する読み取り専用以上のアクセス権を割り当てます。Windows 2008 用の Active Directory アカウントの作成については、次のサイトを参照してください。

[http://technet.microsoft.com/ja-jp/library/dd894463\(WS.10\).aspx](http://technet.microsoft.com/ja-jp/library/dd894463(WS.10).aspx)

Microsoft Exchange Server 管理ツールをインストールする (オプション)



注意

このトピックは、フル機能配信モードにのみ該当します。

Microsoft Exchange Server 管理ツールを使用すると、Exchange Server とマネジメントサーバを統合して、Android デバイスと iOS デバイスを管理できます。

この項目は、Mobile Security をインストールするための環境を準備する手順の 1 つです。

詳細については [28 ページの「Mobile Security をインストールするための環境を設定する」](#) を参照してください。

手順

- 次のいずれかの URL にアクセスして、Exchange Server 管理ツールをインストールします。
 - Exchange Server 2007 管理ツール
[http://technet.microsoft.com/ja-jp/library/bb232090\(v=EXCHG.80\).aspx](http://technet.microsoft.com/ja-jp/library/bb232090(v=EXCHG.80).aspx)
 - Exchange Server 2010 管理ツール
[http://technet.microsoft.com/ja-jp/library/bb232090\(v=exchg.141\).aspx](http://technet.microsoft.com/ja-jp/library/bb232090(v=exchg.141).aspx)
 - Exchange Server 2013 管理ツール
[http://technet.microsoft.com/ja-jp/library/bb232090\(v=exchg.150\).aspx](http://technet.microsoft.com/ja-jp/library/bb232090(v=exchg.150).aspx)
-

Mobile Security のネットワークアクセスルールを適用する

この項目は、Mobile Security のネットワークアクセスルールを設定する際の手順です。

全体の手順を確認したい場合は、[28 ページの「Mobile Security をインストールするための環境を設定する」](#)を参照してください。

手順

- 次のネットワークアクセスルールを適用します。
 - Active Directory を使用する場合は、マネージメントサーバを、Active Directory サーバに接続できるようにします。ファイアウォールを使用している場合は、マネージメントサーバのファイアウォールの設定で除外を追加してください。
 - マネージメントサーバを、Mobile Security データベースがインストールされた SQL Server に接続できるようにします。ファイアウォールを使用している場合は、SQL Server とマネージメントサーバのファイアウォールの設定で除外を追加してください。
 - ポート 4343 の除外を追加して、マネージメントサーバとコミュニケーションサーバ間の HTTPS 接続を許可します。

このポート番号をカスタマイズする必要がある場合、詳細については[122 ページの「コミュニケーションサーバのポートを設定する」](#)を参照してください。

- ポート 80 および 443 の除外を追加して、すべてのモバイルデバイスがコミュニケーションサーバに接続できるようにします。
-

第 3 章

サーバコンポーネントのインストール、アップデート、削除

この章では、管理者が Trend Micro Mobile Security 9.8 のサーバコンポーネントをインストールする方法について説明します。また、サーバコンポーネントの削除方法についても説明します。

この章には、次のセクションが含まれています。

- 39 ページの「サーバコンポーネントをインストールする」
- 39 ページの「インストールする前に」
- 39 ページの「Trend Micro Mobile Security のインストールワークフロー」
- 40 ページの「マネージメントサーバをインストールする」
- 46 ページの「Web 管理コンソールにアクセスする」
- 48 ページの「製品を登録する」
- 50 ページの「ローカルコミュニケーションサーバをインストールする」
- 52 ページの「Exchange Server との統合を設定する」
- 53 ページの「Exchange Connector のアカウントを設定する」
- 55 ページの「Exchange Connector をインストールする」

- 58 ページの「Mobile Security のアップグレードについて」
- 63 ページの「サーバコンポーネントを削除する」

サーバコンポーネントをインストールする

インストールする前に

Mobile Security マネージメントサーバコンポーネントをインストールする前に、次のことを確認する必要があります。

- Mobile Security コンポーネントが、指定されたシステム要件を満たしていることを確認します。

詳細については [19 ページの「システム要件」](#) を参照してください。また、使用しているネットワークテクノロジーを評価してから、インストールする Mobile Security マネージメントサーバコンポーネントを決定する必要もあります。

- [27 ページの環境の設定](#)に記載されている、前提条件となるすべての手順が実行されていることを確認します。

Trend Micro Mobile Security のインストールワークフロー

次の表に、Trend Micro Mobile Security の基本的なインストール方法を示します。

表 3-1. Trend Micro Mobile Security のインストールワークフロー

手順	操作	説明
手順 1	Mobile Security マネージメントサーバをインストールする。	詳細な手順については、 40 ページの「マネージメントサーバをインストールする」 を参照してください。
手順 2	Mobile Security の Web 管理コンソールにログオンする。	詳細な手順については、 46 ページの「Web 管理コンソールにアクセスする」 を参照してください。
手順 3	製品を登録する。	詳細な手順については、 48 ページの「製品を登録する」 を参照してください。

手順	操作	説明
手順 4	(オプション) ローカルコミュニケーションサーバをダウンロードしてインストールする。	クラウドコミュニケーションサーバ (CCS) を使用する場合は、この手順を省略できます。 詳細な手順については、 50 ページ の「ローカルコミュニケーションサーバをインストールする」を参照してください。
手順 5	(フル機能配信モードのみ)。 (オプション) Exchange Server との統合を設定する。	Exchange ActiveSync を使用するモバイルデバイスを管理しない場合は、この手順を省略できます。 詳細な手順については、 55 ページ の「Exchange Connector をインストールする」を参照してください。

マネージメントサーバをインストールする



注意

マネージメントサーバ上のアプリケーション管理モジュールから.apk ファイルをアップロードするには、Mobile Security に JRE (Java Runtime Environment) が必要です。JRE は、マネージメントサーバのインストール時に自動的にインストールされます。ただし、マネージメントサーバをインストールするコンピュータに JRE がすでにインストールされている場合、マネージメントサーバのセットアップでは JRE がインストールされません。既存の JRE のバージョンが 1.6 より古い場合は、その JRE を手動でアンインストールし、1.6 以上の JRE をインストールする必要があります。

手順

1. 次の場所からマネージメントサーバのインストールプログラムをダウンロードします。

http://downloadcenter.trendmicro.com/index.php?clk=left_nav&clkval=all_download®s=JP

2. ダウンロードしたファイルを解凍し、次のマネージメントサーバのインストールプログラムを実行します。MdmServerSetup.exe

[ようこそ] 画面が表示されます。

3. [次へ] をクリックします。

[使用許諾契約] 画面が表示されます。

4. [使用許諾契約の条項に同意します] チェックボックスをオンにして、[次へ] をクリックします。



注意

Microsoft Visual C++ 2005 再頒布可能ファイルをインストールするよう求められます。すでにコンピュータにインストールされている場合、マネージメントサーバのインストール時に、Microsoft Visual C++ 2005 再頒布可能ファイルのインストール手順は表示されません。Microsoft Visual C++ 2005 再頒布可能ファイルのインストール画面が表示された場合は、画面で [次へ] をクリックして、インストールを続行します。

[データベースのオプション] 画面が表示されます。



図 3-1. [データベースのオプション] 画面

5. 次のいずれかを実行します。
 - データベースがインストールされていない場合や、Mobile Security 用の新しいデータベースを作成する場合は、次の手順を実行します。
 - a. [このコンピュータに Microsoft SQL server 2008 Express をインストールしてください。] を選択し、[次へ] をクリックします。

[データベースセットアップ] 画面が表示されます。

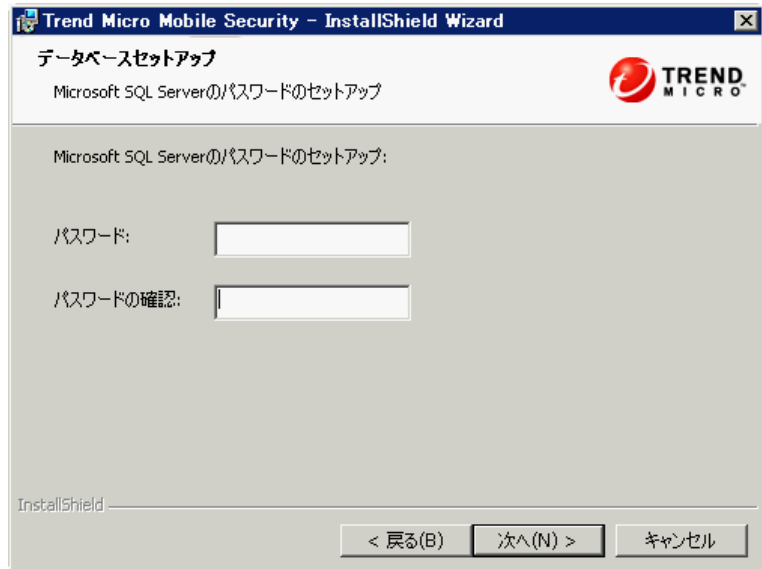


図 3-2. 新しいデータベースを作成するための [データベースセットアップ] 画面

- b. 新しいデータベースのパスワードを入力して、[次へ] をクリックします。

[セットアップの進行状況] 画面が表示され、現在のインストールのステータスを確認できます。

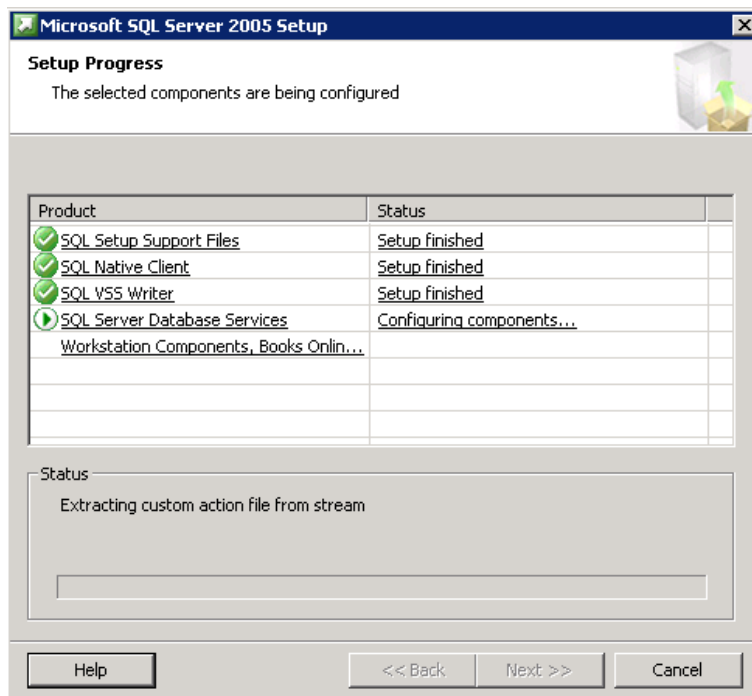


図 3-3. [セットアップの進行状況] 画面

- c. セットアップが完了したら、[次へ] をクリックします。
[サーバの接続設定] 画面が表示されます。
- データベースがすでにインストールされており、その既存のデータベースを使用する場合は、次の手順を実行します。
 - a. [既存のデータベースへの接続] を選択し、[次へ] をクリックします。

[既存のデータベース] 画面が表示されます。

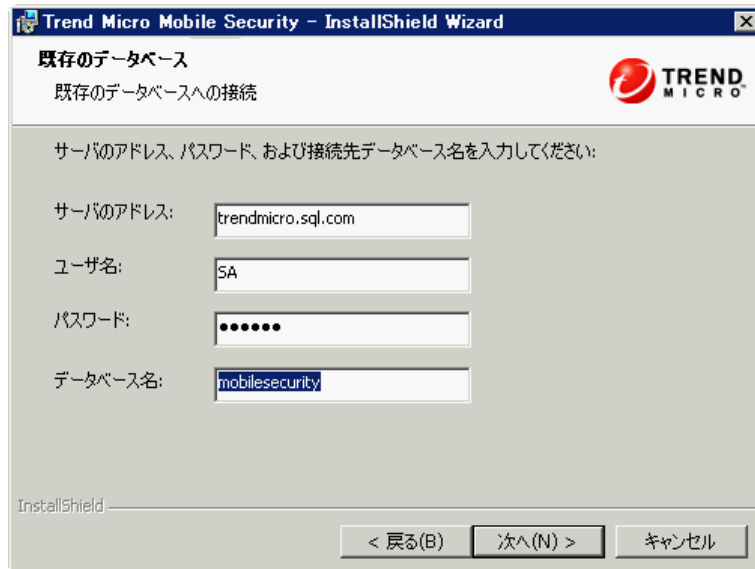


図 3-4. 既存のデータベースサーバの情報

- b. 既存のデータベースサーバの情報を入力して、[次へ] をクリックします。

[サーバの接続設定] 画面が表示されます。

6. リストから IP アドレスを選択し、サーバのポート番号を入力して、[次へ] をクリックします。
7. Mobile Security のインストール先を選択して、[次へ] をクリックします。



注意

別のインストール先を選択するには、[変更] をクリックします。

8. [インストール] をクリックしてインストールを開始します。

インストールの進捗状況を示す画面が表示されます。インストールが完了すると、[Trend Micro Mobile Security のインストールが完了しました] と表示されます。

9. [完了] をクリックします。

次に進む前に

全体的な手順を確認したい場合は、39 ページの「Trend Micro Mobile Security のインストールワークフロー」を参照してください。

Web 管理コンソールにアクセスする

手順

1. 次の URL 構造を使用して Web 管理コンソールにログインします。

`https://<外部ドメイン名または IP アドレス>:<HTTPS ポート>/mdm/web`



<外部ドメイン名または IP アドレス>は、実際の IP アドレスで置き換えます。<HTTPS ポート>は、マネージメントサーバの実際のポート番号で置き換えます。

次の画面が表示されます。



図 3-5. Web 管理コンソールのログイン画面

- 表示されるフィールドにユーザ名とパスワードを入力し、[ログオン] をクリックします。

**注意**

Web 管理コンソールの初期設定のユーザ名は「root」、パスワードは「mobilesecurity」です。

初回のログイン後に「root」ユーザの管理者パスワードを変更してください。手順については、*管理者ガイド*の「*管理者アカウントを編集する*」を参照してください。

**重要**

Internet Explorer を使用して Web 管理コンソールにアクセスする場合、次のことを確認します。

- Web サイトの互換表示のオプションが無効になっている。詳細については、[47 ページの「Internet Explorer の互換モードを無効にする」](#)を参照してください。
- ブラウザで JavaScript が有効になっている。

**注意**

Windows 2012 で、Metro モードの Internet Explorer 10 を使用して Web 管理コンソールにアクセスできない場合は、Internet Explorer の拡張保護モードのオプションが無効になっていることを確認してください。

Internet Explorer の互換モードを無効にする

Trend Micro Mobile Security では Internet Explorer の互換表示をサポートしていません。Internet Explorer を使用して Mobile Security の Web 管理コンソールにアクセスする場合は、Web サイトに対して Web ブラウザの [互換表示] を無効にします。有効になっている場合は、下記手順を実施してください。

手順

- Internet Explorer を開いて、[ツール] > [互換表示設定] をクリックします。

[互換表示設定] 画面が表示されます。

2. 管理コンソールが互換表示のリストに追加されている場合は、その Web サイトを選択して [削除] をクリックします。
 3. [イントラネットサイトを互換表示で表示する] チェックボックスと [すべての Web サイトを互換表示で表示する] チェックボックスをオフにして、[閉じる] をクリックします。
-

製品を登録する

トレンドマイクロでは、サポート契約期間中のお客さまに、テクニカルサポート、不正プログラムパターンファイルのダウンロード、およびプログラムのアップデートを提供しています。この期間の終了後にサポート契約を継続して希望される場合には、サポート契約の更新が必要となります。Mobile Security マネージメントサーバを登録して、最新のセキュリティアップデートや、その他の製品およびサポートサービスを受けられるようにしてください。

必要なのは、アクティベーションコードを使用してマネージメントサーバに Mobile Security マネージメントサーバを登録することのみです。モバイルデバイスがサーバに接続されて登録されると、Mobile Device エージェントは、Mobile Security マネージメントサーバからライセンス情報を自動的に取得します。

アクティベーションコードは、次の形式で表示されます。

XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX

手順

1. Web 管理コンソールにログオンします。

管理コンソールにはじめてアクセスする場合は、[製品ライセンス] 画面が表示されます。はじめての入力ではない場合、[管理] > [製品ライセンス] をクリックしてから、[新しいコード] をクリックします。

2. 表示されるフィールドにアクティベーションコードを入力し、[保存] をクリックします。

製品ライセンス

Trend Micro Mobile Securityはモバイルデバイス向けの包括的なセキュリティソリューションです。Webコンソールを使用して、モバイルデバイスにインストールされたモバイルデバイスエージェントを管理したり、各種のレポートを生成したりできます。

ユーザー登録することで、アカウントはサポート、不正プログラム（ランサムウェアのダウンロード、およびプログラム）のアップデートを一定期間ご利用いただけます。この期間が終了した後は継続してサービスを利用するには、契約を更新する必要があります。最新のセキュリティアップデートやその他の製品、およびメンテナンスサービスを受けたい場合は、Mobile Securityユーザー登録または、アクティベーションコードの入手法については、[トレンドマイクロの営業部](#)または[販売代理店](#)にお問合わせください。

購入コード

サービス: Trend Micro Mobile Security

購入コード:

ここをクリックして、移動先のアクティベーションコードを取得します。

保存 キャンセル

図 3-6. インストール後の Mobile Security の登録

- 登録が正常に実行されたことを確認します。[ダッシュボード] をクリックして、[ダッシュボード] 画面を表示します。

製品の登録が成功している場合、[Trend Micro Mobile Security 9.8 のアクティベーションが完了しました] というメッセージが表示されます。

登録が完了すると、初期設定を完了するための手順が [Mobile Security の設定および検証] 画面に表示されます。

現在の位置: 管理 > [設定および検証](#)

Mobile Securityの設定および検証

Trend Micro Mobile Securityの設定を構成し、検証するために、この画面で以下の手順について説明します。

1	データベース設定の構成	✓
2	コミュニケーションサーバーの設定のダウンロードおよび構成	✓
3	認証設定の構成	✓
4	iOSの設定の構成 (オプション)	✗
<small>iOSデバイスを管理する場合は、iOSの設定を構成します。iOSデバイス名APNs (Apple Push Notificationサービス) を介して管理するためのCSEPP (Single Certificate Enrollment Protocol) を使用する場合は、CSEPPサービスを設定し、APNsの証明書をアップロードしてiOSデバイスがMobile Securityからの通知を受け取ることができます。SSL証明書をアップロードして、コミュニケーションサーバーとの通信のためのCSEPPデバイスHTPSを使用できるようにします。これは、iOSでも必要です。</small>		
	<input type="checkbox"/> 使用しない	
5	通知とレポート設定の実行 (オプション)	✓
<input type="checkbox"/> 使用しない		
6	Exchange Serverとの統合の設定 (オプション)	✗
<small>Microsoft Exchange Serverへのアクセスを拒絶するには、Exchange Serverとの統合を有効にします。Exchange Serverへのアクセスが許可されるのは、正しくモバイルデバイスまたはエンタープライズ環境のモバイルデバイスだけです。この機能を有効にするには、Exchange Connectorパッケージをダウンロードして、Exchange Serverに適切に構成されているWebサービスエンドポイントが必要です。</small>		
<input type="checkbox"/> 使用しない		

Mobile Securityの設定の検証

図 3-7. [Mobile Security の設定および検証] 画面

次に進む前に

全体の手順を確認したい場合は、39 ページの「[Trend Micro Mobile Security のインストールワークフロー](#)」を参照してください。

ローカルコミュニケーションサーバをインストールする

手順

1. コミュニケーションサーバをインストールするコンピュータで、Web 管理コンソールにログオンします。
2. [管理] > [コミュニケーションサーバの設定] をクリックします。
3. [共通設定] タブをクリックします。
4. リストから [ローカルコミュニケーションサーバ] を選択し、[ここをクリックしてダウンロード] をクリックします。
5. セットアップファイルをダブルクリックして、インストール処理を開始します。

[よろこぞ] 画面が表示されます。

6. [次へ] をクリックします。
[使用許諾契約] 画面が表示されます。
7. 内容に同意される場合は、[使用許諾契約の条項に同意します] を選択して [次へ] をクリックします。

[モバイルデバイス用のコミュニケーションサーバの接続設定] 画面が表示されます。

8. リストから IP アドレスを選択し、コミュニケーションサーバの HTTP ポート番号と HTTPS ポート番号を入力します。

この画面で指定する IP アドレスおよびポート番号は、コミュニケーションサーバがモバイルデバイスと通信するために使用されます。

**注意**

IP アドレスは「すべて」選択することをお勧めします。

9. [次へ] をクリックします。

[マネージメントサーバ用のコミュニケーションサーバの接続設定] 画面が表示されます。

10. リストから IP アドレスを選択し、コミュニケーションサーバの HTTPS ポート番号を入力します。

この画面で指定する IP アドレスおよびポート番号は、コミュニケーションサーバがマネージメントサーバと通信するために使用されます。

**注意**

IP アドレスは「すべて」選択することをお勧めします。

11. [次へ] をクリックします。

[サーバ証明書] 画面が表示されます。

12. 次のいずれかを実行します。

- iOS デバイス登録用の SSL 証明書をお持ちの場合は、次の手順を実行します。
 - a. [既存の.pfx または.p12 証明書ファイルをインポートする] を選択し、[次へ] をクリックします。
[証明書のインポート] 画面が表示されます。
 - b. [参照] をクリックし、ハードドライブ上のパブリック証明書を選択します。
 - c. [パスワード] に証明書のパスワードを入力します。証明書のパスワードが設定されていない場合、このフィールドは空白のまま残しておきます。
 - d. [次へ] をクリックします。
- iOS デバイス登録用の SSL 証明書がない場合や、新しい SSL 証明書を作成する必要がある場合は、次の手順を実行します。

- a. [新しいプライベート証明書の作成] を選択し、[次へ] をクリックします。
[証明書の作成] 画面が表示されます。
- b. [一般名] にコミュニケーションサーバの IP アドレスを入力し、[パスワード] に証明書のパスワードを入力します。
- c. [次へ] をクリックします。

13. Mobile Security のインストール先を選択して、[次へ] をクリックします。



別のインストール先を選択するには、[変更] をクリックします。

14. [インストール] をクリックしてインストールを開始します。

インストールの進捗状況を示す画面が表示されます。インストールが完了すると、[インストールが完了しました] と表示されます。

15. [完了] をクリックします。

次に進む前に

全体の手順を確認したい場合は、[39 ページ](#)の「[Trend Micro Mobile Security のインストールワークフロー](#)」を参照してください。

Exchange Server との統合を設定する



このトピックは、フル機能配信モードにのみ該当します。

マネージメントサーバと Exchange Server 間の通信を確立するには、Exchange Server との統合が必要です。



Trend Micro Mobile Security では、Exchange Server 2007 以降のみがサポートされ、iOS および Android デバイスで、Exchange Server との統合がサポートされます。

次の表に、Trend Micro Mobile Security に Exchange Server を統合する設定手順を記載します。

表 3-2. Exchange Server との統合を設定するプロセス

手順	操作	説明
手順 1	Microsoft Exchange Server 管理ツールをインストールする。	Exchange Server 設定を構成する前に、Exchange Connector のインストール先となるコンピュータに Microsoft Exchange Server 管理ツールがインストールされていることを確認してください。 インストール手順については、 35 ページの「Microsoft Exchange Server 管理ツールをインストールする (オプション)」 を参照してください。
手順 2	Exchange Connector のアカウントを設定する。	Exchange Connector 用のアクセス権が提供されます。 詳細な手順については、 53 ページの「Exchange Connector のアカウントを設定する」 を参照してください。
手順 3	Exchange Connector をインストールする。	マネージメントサーバと Exchange Server 間の通信が確立されます。 詳細な手順については、 55 ページの「Exchange Connector をインストールする」 を参照してください。
手順 4	Exchange Server との統合を設定する。	詳細な手順については 81 ページの「Exchange Server との統合を設定する」 を参照してください。

Exchange Connector のアカウントを設定する



注意

このトピックは、フル機能配信モードにのみ該当します。

手順

1. Active Directory サーバでユーザアカウントを作成します。
2. Exchange Connector をインストールするコンピュータで、[スタート] > [管理ツール] > [コンピューターの管理] の順に選択し、次の手順を実行します。
 - a. 左側のツリーで [ローカル ユーザーとグループ] フォルダを展開し、[グループ] をダブルクリックします。
 - b. [Administrators] を右クリックし、[プロパティ] をクリックします。
 - c. [全般] タブの [追加] ボタンをクリックして、次の手順を実行します。
 - i. 54 ページの手順 1 で作成したユーザ名を [ログイン名] に入力し、[検索] をクリックします。
[ユーザーの選択] 画面が表示されます。
 - ii. [選択するオブジェクト名を入力してください] にユーザ名とドメイン名 (例: domainname\username) を入力し、[名前の確認] をクリックします。
 - iii. [OK] をクリックします。
 - d. [Administrator のプロパティ] 画面で [OK] をクリックします。
3. Active Directory サーバで、次の手順を実行します。
 - a. [スタート] > [管理ツール] > [Active Directory ユーザーとコンピューター] の順に選択します。
 - b. 左側のツリーで [Users] フォルダを展開します。
 - c. 54 ページの手順 1 で作成したアカウント (ユーザ名) を右クリックし、[グループに追加] をクリックします。
 - d. 次のいずれかを実行します。
 - Exchange Server 2007 の場合は、[選択するオブジェクト名を入力してください] に「Exchange Organization Administrators」と入力し、[名前の確認] をクリックします。

- Exchange Server 2010 および 2013 の場合は、[選択するオブジェクト名を入力してください]に「**Organization Management**」と入力し、[名前の確認]をクリックします。
 - e. [OK] をクリックし、確認画面で [OK] をクリックします。
4. Active Directory サーバで、次の手順を実行します。
- a. [スタート] > [管理ツール] > [Active Directory ユーザーとコンピューター] の順に選択します。
 - b. メニューバーの [表示] > [拡張機能] をクリックします。
 - c. 左側のツリーで [Users] フォルダを展開します。
 - d. [54 ページの手順 1](#) で作成したアカウント (ユーザ名) を右クリックし、[プロパティ] をクリックします。
 - e. [セキュリティ] タブの [追加] をクリックします。
 - f. [選択するオブジェクト名を入力してください] に、[54 ページの手順 1](#) で作成したユーザ名とドメイン名 (例: domainname\username) を入力し、[名前の確認] をクリックして、[OK] をクリックします。
 - g. [グループ名またはユーザー名] リストでユーザ名を選択し、[詳細設定] をクリックします。
 - h. [このオブジェクトの親からの継承可能なアクセス許可を含める] を選択し、[OK] をクリックします。
 - i. [プロパティ] 画面で [OK] をクリックします。

Exchange Connector をインストールする



注意

このトピックは、フル機能配信モードにのみ該当します。



注意

Exchange Connector は次のコンピュータにインストールする必要があります。

- Microsoft Exchange Server 管理ツールがインストールされているコンピュータ
 - Exchange Server と同じドメインにあるコンピュータ
 - マネージメントサーバに接続可能なコンピュータ
-

手順

1. Web 管理コンソールにログオンします。
2. [管理] > [Exchange Server との統合] をクリックします。
3. [ここをクリックしてダウンロード] をクリックして、ExchangeConnector.zip ファイルをコンピュータに保存します。
4. ExchangeConnector.zip ファイルの内容を解凍し、ExchangeConnector.exe ファイルを実行します。
Exchange Connector のセットアップウィザードが開きます。
5. [よろこそ] 画面の [次へ] をクリックします。
6. 内容に同意される場合は、[使用許諾契約の条項に同意します] を選択して [次へ] をクリックします。

Microsoft Exchange Server 管理ツールがコンピュータにインストールされているかどうかを確認されます。インストールされている場合は、次の画面が表示されます。

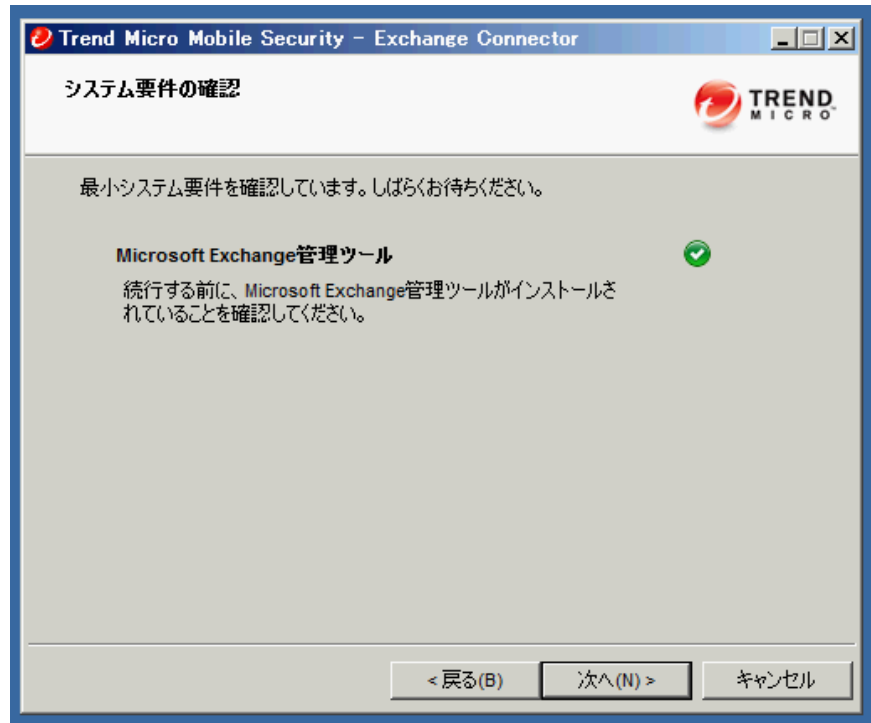


図 3-8. Exchange Server 管理ツールのインストールチェックが成功した場合に表示される画面

7. [システム要件の確認] 画面の [次へ] をクリックします。
8. [参照] をクリックし、Exchange Connector のインストール先のフォルダを選択して、[次へ] をクリックします。
[サービスアカウント] 画面が表示されます。
9. 53 ページの「Exchange Connector のアカウントを設定する」で作成したユーザ名、パスワード、およびドメイン名を入力して Exchange Server 管理ツールにアクセスし、[次へ] をクリックします。

10. [設定の確認] 画面で設定を確認し、[インストール] をクリックします。
Exchange Connector のインストールが開始されます。
11. インストールが完了したら、[次へ] をクリックし、[完了] をクリックします。



モバイルデバイスの情報を Exchange Server からマネージメントサーバにインポートする処理にかかる時間は、インポートするモバイルデバイスの数によって異なります。たとえば、5000 台のモバイルデバイスの情報を Exchange Server からマネージメントサーバにインポートする場合、数時間かかる可能性があります。

次に進む前に

その他の設定タスクについては、[39 ページの「Trend Micro Mobile Security のインストールワークフロー」](#)を参照してください。

Exchange Server との統合を設定するための次のタスクについては、[52 ページの「Exchange Server との統合を設定する」](#)を参照してください。

コンポーネントのアップデート

Mobile Security のアップグレードについて

Trend Micro Mobile Security でサポートされるのは、9.0 以降のバージョンからのアップグレードのみです。

Mobile Security では、アップデートを介して次のコンポーネントまたはファイルをアップデートします。アップデートはトレンドマイクロのインターネットベースのコンポーネントアップデート機能です。

- Mobile Security マネージメントサーバ: Mobile Security のマネージメントサーバとコミュニケーションサーバのプログラムインストールパッケージ。

- 不正プログラムパターンファイル: 多数の不正プログラムのシグニチャを含み、Mobile Security でこれらの危険なファイルを検出できるようにするファイル。トレンドマイクロでは、パターンファイルを定期的にアップデートして最新の脅威からシステムを保護します。
- Mobile Device エージェントのインストールプログラム: Mobile Device エージェントのプログラムインストールパッケージ。

Trend Micro Mobile Security でサポートされるのは、9.0 以降のバージョンからのアップグレードのみです。9.0 より前のバージョンからアップグレードする場合は、移行ツールを使用して 9.0 にデータを移行してから、Mobile Security 9.8 にアップグレードできます。

9.0 より前のバージョンから 9.8 にデータを移行する手順の詳細については、次の URL を参照してください。

http://tmqa.jp/tmms_migrationguide

Mobile Security コンポーネントのアップデート

Mobile Security マネージメントサーバで予約または手動のコンポーネントアップデートを設定して、アップデートサーバから最新のコンポーネントファイルを取得できます。マネージメントサーバに新しいバージョンのコンポーネントがダウンロードされると、マネージメントサーバはモバイルデバイスにコンポーネントをアップデートするように自動で通知を送信します。

手動アップデート

[アップデート] 画面の [手動] タブで、サーバおよび Mobile Device エージェントを手動でアップデートできます。[アップデート元] 画面 (詳細については、[61 ページの「ダウンロード元を指定する」](#)を参照) でダウンロード元をあらかじめ設定しておく必要があります。

手順

1. Mobile Security の Web 管理コンソールにログオンします。
2. [管理] > [アップデート] をクリックします。

[アップデート] 画面が表示されます。

3. [手動] タブをクリックします。
4. アップデートするコンポーネントのチェックボックスをオンにします。
[不正プログラム対策コンポーネント]、[エージェントインストールパッケージ]、[サーババージョン] のいずれか (またはすべて) のチェックボックスをオンにして、各グループのすべてのコンポーネントを選択します。この画面には、各コンポーネントの現在のバージョンおよびコンポーネントの前のアップデート日時が表示されます。各アップデートコンポーネントの詳細については、を参照してください。
5. [アップデート] をクリックして、コンポーネントのアップデート処理を開始します。


予約アップデート

予約アップデートを使用すると、ユーザの介入なしに定期的なアップデートを実行できるようになり、ユーザによる処理を削減できます。[アップデート元] 画面 (詳細については、[61 ページの「ダウンロード元を指定する」](#)を参照) でダウンロード元をあらかじめ設定しておく必要があります。

手順

1. Mobile Security の Web 管理コンソールにログオンします。
2. [管理] > [アップデート] をクリックします。

[アップデート] 画面が表示されます。
3. [予約] タブをクリックします。
4. アップデートするコンポーネントのチェックボックスをオンにします。
[不正プログラム対策コンポーネント]、[エージェントインストールパッケージ]、[サーババージョン] のいずれか (またはすべて) のチェックボックスをオンにして、各グループのすべてのコンポーネントを選択します。この画面には、各コンポーネントの現在のバージョンおよびコンポーネントの前のアップデート日時が表示されます。

5. [アップデートスケジュール] で、サーバアップデートを実行する頻度を設定します。オプションは、[毎時]、[毎日]、[毎週]、および [毎月] です。
 - 毎週アップデートする場合は、曜日を指定してください (日曜日、月曜日など)。
 - 毎月アップデートする場合は、日付を指定してください (毎月 1 日、または 01 のようにします)。
-
-  **注意**

[毎日]、[毎週]、および [毎月] のオプションには、[開始時刻] 機能を使用できます。これは、[開始時刻] フィールドで選択した時刻の後、指定した時間内のいつかにアップデートが実行されることを意味します。この機能は、アップデートサーバでの負荷分散に役立ちます。
-
- Mobile Security でアップデート開始時刻を指定する場合は、[開始時刻] を選択します。
6. [保存] をクリックして設定を保存します。

ダウンロード元を指定する

Mobile Security では、サーバアップデートの際に初期設定のアップデートサーバを使用するか、指定したダウンロード元を使用するかを設定できます。

手順

1. Mobile Security の Web 管理コンソールにログオンします。
2. [管理] > [アップデート] をクリックします。

[アップデート] 画面が表示されます。アップデートの詳細については、[59 ページの「手動アップデート」](#)を参照してください。予約アップデートについては、[60 ページの「予約アップデート」](#)を参照してください。
3. [アップデート元] タブをクリックします。
4. 次のいずれかのダウンロード元を選択します。

- トレンドマイクロのアップデートサーバ: 初期設定のアップデート元です。
- その他のアップデート元: HTTP または HTTPS Web サイト (ローカルのイントラネット Web サイトなど) を指定します。Mobile Device エージェントがアップデートをダウンロードする際に使用するポート番号も指定します。

**注意**

アップデート済みのコンポーネントが、アップデート元 (Web サーバ) で利用可能である必要があります。ホスト名または IP アドレス、およびディレクトリ (例: 「`https://10.1.123.123:14943/source`」) を入力してください。

- 現在のファイルのコピーが保存されているイントラネット上の場所: ローカルのイントラネットのアップデート元です。次のオプションを指定します。
 - UNC パス: ソースファイルが保存されているパスを入力します。
 - [ユーザ名] および [パスワード]: アップデート元で認証が必要な場合は、ユーザ名とパスワードを入力します。

ローカルのアップデート元の手動アップデート

サーバやモバイルデバイスがローカルのアップデート元を使用してアップデートされるものの、マネージメントサーバがインターネットに接続できない場合、サーバやモバイルデバイスのアップデートを実行する前に、手動でローカルのアップデート元をアップデートします。

手順

1. トレンドマイクロ販売代理店からインストールパッケージを入手します。
2. インストールパッケージを解凍します。
3. ローカルのアップデート元にフォルダー一式をコピーします。

**注意**

ローカルのアップデート元を使用している場合、定期的にアップデートを確認する必要があります。

サーバコンポーネントを削除する

ここでは、マネージメントサーバとコミュニケーションサーバの削除を実行する手順を示します。

手順

1. Windows のコントロールパネルから [プログラムと機能] をダブルクリックします。
[プログラムのアンインストールまたは変更] 画面が表示されます。
2. 次のいずれかを選択します。
 - トレンドマイクロのローカルコミュニケーションサーバ: コミュニケーションサーバをアンインストールします。
 - Trend Micro Mobile Security: マネージメントサーバをアンインストールします。
3. [アンインストール] をクリックします。
画面が表示されます。
4. [セットアップの完了後、アプリケーションを自動的に終了して、再起動する] を選択し、[OK] をクリックします。

第 4 章

サーバコンポーネントの設定

この章では、管理者が Trend Micro Mobile Security 9.8 のサーバコンポーネントを設定する際に役立つ情報を提供します。

この章には、次のセクションが含まれています。

- 67 ページの「初期サーバセットアップ」
- 69 ページの「データベースを設定する」
- 70 ページの「コミュニケーションサーバを設定する」
- 70 ページの「コミュニケーションサーバの共通項目を設定する」
- 72 ページの「Android のコミュニケーションサーバを設定する」
- 73 ページの「iOS のコミュニケーションサーバを設定する」
- 76 ページの「デバイス登録の設定を行う」
- 78 ページの「Mobile Security の利用条件をカスタマイズする」
- 79 ページの「AD (Active Directory) の設定」
- 80 ページの「マネージメントサーバを設定する」
- 81 ページの「Exchange Server との統合を設定する」
- 83 ページの「Exchange Connector のステータス」

- 83 ページの「通知とレポートを設定する」
- 84 ページの「管理者への通知を設定する」
- 85 ページの「Mobile Security の設定を検証する」

初期サーバセットアップ

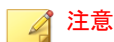
次の表に、Trend Micro Mobile Security をインストールした後の初期サーバセットアップを示します。

表 4-1. Mobile Security マネージメントサーバの初期セットアップ

手順	操作	説明
手順 1	データベースを設定する。	詳細な手順については、69 ページの「データベースを設定する」を参照してください。
手順 2	コミュニケーションサーバを設定する。	詳細な手順については、70 ページの「コミュニケーションサーバの共通項目を設定する」を参照してください。
手順 3	(フル機能配信モードのみ)。 (オプション) Android 用のコミュニケーションサーバを設定する。	Android デバイスを管理しない場合は、この手順を省略できます。 詳細な手順については、72 ページの「Android のコミュニケーションサーバを設定する」を参照してください。
手順 4	(フル機能配信モードのみ)。 (オプション) iOS 用のコミュニケーションサーバを設定する。	iOS デバイスを管理しない場合は、この手順を省略できます。 詳細な手順については、73 ページの「iOS のコミュニケーションサーバを設定する」を参照してください。
手順 5	配信モードを設定する。	詳細な手順については、75 ページの「配信を設定する」を参照してください。
手順 6	デバイスの登録設定を構成する。	詳細な手順については、76 ページの「デバイス登録の設定を行う」を参照してください。
手順 7	(フル機能配信モードのみ)。 (オプション) Mobile Security の利用条件をカスタマイズする。	Mobile Security の利用条件を初期設定のまま使用する場合は、この手順を省略できます。 詳細な手順については、78 ページの「Mobile Security の利用条件をカスタマイズする」を参照してください。

手順	操作	説明
手順 8	(フル機能配信モードと指定以外の MDM ベンダーを使用するセキュリティ対策限定配信モード)。 (オプション) Active Directory を設定する	Active Directory サーバからユーザをインポートしない場合は、この手順を省略できます。 詳細な手順については、 79 ページの「AD (Active Directory) の設定」 を参照してください。
手順 9	(オプション) マネージメントサーバの設定を構成する。	マネージメントサーバがインターネットへのアクセスにプロキシを使用せず、初期設定のサーバ IP アドレスおよびポート番号を使用する場合は、この手順を省略できます。 詳細な手順については、 80 ページの「マネージメントサーバを設定する」 を参照してください。
手順 10	(フル機能配信モードのみ)。 (オプション) Exchange Server との統合を設定する。	Exchange ActiveSync を使用するモバイルデバイスを管理しない場合は、この手順を省略できます。 詳細な手順については、 81 ページの「Exchange Server との統合を設定する」 を参照してください。
手順 11	(オプション) 通知とレポートを設定する。	登録依頼のメールをユーザに送信しない場合は、この手順を省略できます。 詳細については 83 ページの「通知とレポートを設定する」 を参照してください。
手順 12	(オプション) 管理者への通知を設定する。	エラーメッセージの通知と通常の定期レポートをメールで受信しない場合は、この手順を省略できます。 詳細な手順については、 84 ページの「管理者への通知を設定する」 を参照してください。
手順 13	Mobile Security の設定を検証する (推奨)。	Mobile Security の設定を検証するには、[設定および検証] 画面を使用します。 手順については、 85 ページの「Mobile Security の設定を検証する」 を参照してください。

手順	操作	説明
手順 14	Web 管理コンソールで使用する管理者アカウントのパスワードを変更する。	Web 管理コンソールにログインし、[管理者アカウント管理] 画面を使用します。 手順については、「 管理者ガイド 」の「 管理者アカウントの編集 」を参照してください。

**注意**

Mobile Security マネージメントサーバの初期サーバセットアップを完了させてから、モバイルデバイスに Mobile Device エージェントをインストールしてください。

データベースを設定する

手順

1. Web 管理コンソールにログオンします。
2. [管理] > [データベースの設定] をクリックします。
3. サーバの名前または IP アドレス、ユーザ名、パスワード、およびデータベース名を入力します。

**注意**

SQL Server または SQL Server Express の特定のポートを使用している場合は、次の形式を使用します。

`<SQL server name or IP address>,<Port>`

4. [保存] をクリックします。

次に進む前に

全体の手順を確認したい場合は、[67 ページ](#)の「[初期サーバセットアップ](#)」を参照してください。

コミュニケーションサーバを設定する

[コミュニケーションサーバの設定] 画面では、次の項目を設定します。

- 共通設定: コミュニケーションサーバの基本設定
- Android の設定: Android デバイスを管理するための通知の設定およびエージェントのカスタマイズ設定
- iOS の設定: SCEP の設定と、iOS デバイスの管理に使用する APNs および SSL 証明書のアップロード



注意

[Android の設定] および [iOS の設定] は、フル機能配信モードでのみ利用できません。

コミュニケーションサーバの共通項目を設定する

手順

1. Web 管理コンソールにログオンします。
2. [管理] > [コミュニケーションサーバの設定] をクリックします。
3. [共通設定] タブをクリックします。
4. [コミュニケーションサーバの種類] で、次のいずれかのオプションを選択します。
 - ローカルコミュニケーションサーバ: ネットワーク内でローカルに、コミュニケーションサーバをインストールしている場合。
 - クラウドコミュニケーションサーバ: クラウドに展開されるコミュニケーションサーバを使用する場合。
5. [コミュニケーションサーバとモバイルデバイスの通信設定] で、次の項目を設定します。(この項目は、ローカルコミュニケーションサーバを選んだ場合にのみ、表示されます。)
 - 外部ドメイン名/IP アドレス: ローカルコミュニケーションサーバのドメイン名または IP アドレス。

- HTTP ポート番号および HTTPS ポート番号: ローカルコミュニケーションサーバがモバイルデバイスと通信する場合に使用します。

初期設定の HTTP ポートおよび HTTPS ポートは、それぞれ 8080 と 4343 です。

**注意**

これらのポートを両方とも設定した場合、モバイルデバイスは HTTPS ポートを使用してコミュニケーションサーバと通信します。モバイルデバイスで HTTP ポートが使用されるのは、HTTPS ポートを使用して通信できない場合のみです。

6. [コミュニケーションサーバとマネジメントサーバの通信設定] で次の項目を設定します。(この項目は、ローカルコミュニケーションサーバを選んだ場合にのみ、表示されます。)
 - 公開サーバ名/IP アドレス: ローカルコミュニケーションサーバのドメイン名または IP アドレス。
 - HTTPS ポート番号: ローカルコミュニケーションサーバがマネジメントサーバと通信する場合に使用します。

**注意**

HTTPS ポート番号をカスタマイズする必要がある場合、詳細については [122 ページの「コミュニケーションサーバのポートを設定する」](#) を参照してください。

7. (フル機能配信モードのみ) [情報を収集する頻度] で次の項目を設定します。
 - 情報を収集する頻度: モバイルデバイスにインストールされたアプリケーションに関する情報を Mobile Security が収集する頻度を選択します。
 - モバイルデバイスのローミング時の情報収集の頻度: モバイルデバイスのローミング中にモバイルデバイスにインストールされたアプリケーションに関する情報を Mobile Security が収集する頻度を選択します。



注意

この設定は Android デバイスと iOS デバイスにのみ適用されます。

Mobile Security は、モバイルデバイスの登録時に、ユーザが選択した頻度で、モバイルデバイスにインストールされたアプリケーションに関する情報を収集します。

頻度を変更すると、タイマーがリセットされます。

8. (フル機能配信モードのみ) root 化または Jailbreak されたモバイルデバイスを自動的に選択消去する場合は、[root 化/Jailbreak されたデバイスの検出] で [root 化/Jailbreak されたデバイスの選択消去] を選択します。
 9. [保存] をクリックします。
-

次に進む前に

全体の手順を確認したい場合は、[67 ページの「初期サーバセットアップ」](#)を参照してください。

Android のコミュニケーションサーバを設定する



注意

このトピックは、フル機能配信モードにのみ該当します。

手順

1. Web 管理コンソールにログオンします。
2. [管理] > [コミュニケーションサーバの設定] をクリックします。
3. [Android の設定] タブをクリックします。
4. Android デバイスに通知を配信する場合は、[プッシュ通知の設定] で、[プッシュ通知を有効にする] を選択します。

**注意**

この設定を有効にしない場合は、Android デバイスのユーザが手動でデバイス上の企業のポリシーをアップデートする必要があります。

- [エージェントのカスタマイズ] で、[エージェントのカスタマイズを有効にする] チェックボックスをオンにして、ユーザが Mobile Security コミュニケーションサーバからダウンロードする場合、MDA インストール時にサーバ IP アドレスとポート番号を追加します。これにより、[デバイス登録設定] で [設定済みの登録キーを有効化] オプションが選択されている場合、設定済みの登録キーも自動的に Android クライアントアプリに追加されます。

つまり、サーバ IP アドレス、ポート番号、および設定済みの登録キーが自動的にクライアントアプリケーションに入力されるため、ユーザはこの情報を手動で入力する必要はありません。
- モバイルデバイスのシステム設定をパスワードで保護する場合は、[システム設定のパスワード保護] で [システム設定のパスワード保護を有効にする] を選択し、[パスワード] にパスワードを入力します。
- [保存] をクリックします。

次に進む前に

全体的な手順を確認したい場合は、[67 ページの「初期サーバセットアップ」](#)を参照してください。

iOS のコミュニケーションサーバを設定する**注意**

このトピックは、フル機能配信モードにのみ該当します。

手順

- Mobile Security の Web 管理コンソールで、[管理] > [コミュニケーションサーバの設定] > [iOS の設定] の順に選択します。

[iOS の設定] タブが表示されます。

2. [APNs (Apple Push Notification サービス) の設定] で次の項目を設定します。
 - 証明書の種類: 証明書の種類を選択します。
 - 証明書: リストから APNs 証明書を選択するか、新しい証明書をアップロードします。
3. [SCEP (Simple Certificate Enrollment Protocol) の設定] で次の項目を設定します。
 - a. [SCEP の有効化] を選択します。
 - b. 有効にする場合は、次の情報を入力する必要があります。
 - SCEP ユーザの URL:
http://SCEP_IP/certsrv/mscep
 - SCEP 管理者の URL:
Windows Server 2008 の場合:
http://SCEP_IP/certsrv/mscep_admin



注意

SCEP については、15 ページの「Mobile Security のコンポーネント」を参照してください。

4. [クライアントプロファイル署名用認証情報] で次の項目を設定します。
 - クライアントプロファイル署名用認証情報: リストから署名用認証情報の証明書を選択するか、新しい証明書をアップロードします。

**注意**

iOS デバイスに Mobile Device エージェントを設定するために、Mobile Security はモバイルデバイスにインストールプロファイルをインストールします。インストールプロファイルのステータスが「認証済み」になるためには、クライアントプロファイル署名証明書が必要です。この設定を行わないと、インストールプロファイルのステータスは「認証されていません」と表示されます。

この設定を行うと、モバイルデバイスでインストールプロファイルのステータスが「検証済み」と表示されます。

5. [保存] をクリックします。

次に進む前に

全体の手順を確認したい場合は、[67 ページの「初期サーバセットアップ」](#)を参照してください。

配信を設定する

Mobile Security は、他の MDM ソリューションと統合できます。[配信設定] 画面を使用して、次のいずれかのモードで Mobile Security を配信できます。

- フル機能: モバイルデバイス管理 (MDM) とセキュリティ対策機能を提供します。
- セキュリティ対策限定: セキュリティ対策機能のみを提供し、他社のモバイルデバイス管理 (MDM) ソリューションと統合できます。

手順

1. Mobile Security の Web 管理コンソールで、[管理] > [配信設定] の順に選択します。
2. [サーバ] タブで、Mobile Security の配信モードを選択します。
 - フル機能
 - セキュリティ対策限定: このモードを選択した場合、続けて [MDM ソリューション] リストからソリューションを選択します。

[MDM ソリューション] リストから [AirWatch] または [MobileIron] を選択した場合は、画面に表示される AirWatch または MobileIron の設定で Mobile Security との統合を有効にします。

3. (指定以外の MDM ベンダーを使用するセキュリティ対策限定配信モード) [Android エージェント] タブで、次のオプションを選択します。
 - Mobile Security マネージメントサーバからダウンロード: このオプションを選択した場合、ユーザは通知メールに記載された URL からクライアントアプリをダウンロードできます。

また、[自動登録] を選択して、サーバの IP アドレス、ポート番号、および設定済みの登録キーでクライアントアプリを事前に設定しておくこともできます。
4. (指定以外の MDM ベンダーを使用するセキュリティ対策限定配信モード) [iOS エージェント] タブで、[iOS (7.1 以降) で不正アプリ対策を使用できるようにする] を選択し、画面に表示される手順に従って設定を完了します。
5. [保存] をクリックします。

デバイス登録の設定を行う

手順

1. Web 管理コンソールにログオンします。
2. [管理] > [デバイス登録設定] をクリックします。
3. [認証情報] タブをクリックします。
4. [ユーザ認証] で、次のいずれかを選択します。
 - Active Directory を使用して認証: Active Directory のユーザ情報を使用してユーザを認証します。
 - 登録キーを使用して認証: 登録キーを使用してユーザを認証します。

Mobile Security は登録キーを自動的に生成します。この登録キーは、登録依頼メールでユーザに送信されます。

- 登録キーの使用制限: 次のいずれかを選択します。
 - 複数回使用: 複数のデバイスの登録に同じ登録キーを使用できるようにするには、このオプションを選択します。
 - [1回のみ使用]: 登録キーの再利用を禁止するには、このオプションを選択します。複数のデバイスを登録する必要があるユーザには、登録依頼を複数送信する必要があります。
- 自動生成の登録キーの有効期限: 特定の期間が経過した後、自動的に生成された登録キーの使用を中止する場合は、この設定を選択し、リストから期間を選択します。
- 設定済みの登録キーを使用: 登録キーを手動で生成する場合は、この設定を選択し、[生成] をクリックして登録キーを生成します。この登録キーは、登録依頼メールでユーザに送信されません。
- 手動生成の登録キーの有効期限: 手動で生成された登録キーの使用を特定の日に中止する場合は、この設定を選択し、カレンダーから日付を選択します。

**注意**

[Active Directory を使用して認証] 設定は、フル機能配信モードと指定以外の MDM ベンダーを使用するセキュリティ対策限定配信モードで利用できません。

5. (フル機能配信モードのみ) [デバイス認証] で、次のいずれかを選択します。
- この設定を無効にする: モバイルデバイスのデバイス認証を無効にします。
 - IMEI/MEID 番号または Wi-Fi MAC アドレスを使用して認証: 認証するモバイルデバイスのリストをアップロードできます。
 - a. [ここをクリックして、許可デバイスリストのテンプレートをダウンロードします。] をクリックしてテンプレートをダウンロードし、許可デバイスリストを作成します。
 - b. リストを作成したら、[参照] をクリックし、前の手順で作成したモバイルデバイスのリストを選択し、インポートします。

- c. [データ形式の確認] をクリックして、許可デバイスリストのデータ形式を確認します。確認が終了すると、すべてのモバイルデバイスが [許可デバイスのステータス] リストに表示されます。
- d. 次のいずれかのオプションを選択します。
 - 未認証デバイスを削除: デバイス管理画面に表示されているが、インポートする許可デバイスリストには含まれていないモバイルデバイスを削除します。(モバイルデバイス側において、登録に成功したメッセージが表示されますが、マネージメントサーバ側で自動的に削除されるため、モバイルデバイス側も未登録の状態になります。)
 - 未認証デバイスを「未認証」グループに表示: デバイス管理画面に表示されているが、インポートする許可デバイスリストには含まれていないすべての登録済みモバイルデバイスを、「未認証」グループに移動します。

**注意**

デバイス認証を使用する場合、使用する許可デバイスリストに基づいて、すべてのモバイルデバイスが再度グループ分けされます。

6. [保存] をクリックします。

次に進む前に

全体の手順を確認したい場合は、[67 ページの「初期サーバセットアップ」](#)を参照してください。

Mobile Security の利用条件をカスタマイズする

Mobile Device エージェントをダウンロード、インストール、および使用するユーザ向けに利用条件をカスタマイズできます。

手順

1. Web 管理コンソールにログオンします。
2. [管理] > [デバイス登録設定] をクリックします。

3. [利用条件のカスタマイズ] タブで、[利用条件のサンプルのダウンロード] をクリックし、Eula_agreement.zip ファイルをコンピュータに保存します。
4. Eula_agreement.zip ファイルの内容を解凍します。
5. HTML エディタを使用して、Eula_agreement.html ファイルを開き、必要に応じて変更を加えて保存します。
6. [デバイス登録設定] 画面の [利用条件のカスタマイズ] タブで、[参照] をクリックし、前の手順 (79 ページの手順 5) で変更したファイルを選択し、[開く] をクリックします。

[利用条件のプレビュー] に、アップロードされたファイルの内容が表示されます。
7. [保存] をクリックします。

次に進む前に

全体の手順を確認したい場合は、[67 ページの「初期サーバセットアップ」](#)を参照してください。

AD (Active Directory) の設定



注意

このトピックは、フル機能配信モードと指定以外の MDM ベンダーを使用するセキュリティ対策限定配信モードに該当します。

Mobile Security を使用すると、Active Directory (AD) に基づいてユーザ認証を設定できます。設定が完了すると、企業の Active Directory を使用してモバイルデバイスリストにモバイルデバイスを追加することもできます。

ユーザ認証に Active Directory を使用しない場合や、Active Directory からユーザを追加しない場合、この設定を実行する必要はありません。

手順

1. Web 管理コンソールにログオンします。
 2. [管理] > [Active Directory の設定] をクリックします。
 3. ホスト名または IP アドレス、ポート番号、ドメインユーザ名、およびパスワードを入力します。
 4. [保存] をクリックします。
-

次に進む前に

全体的な手順を確認したい場合は、[67 ページの「初期サーバセットアップ」](#)を参照してください。

マネージメントサーバを設定する

手順

1. Web 管理コンソールにログオンします。
 2. [管理] > [マネージメントサーバの設定] をクリックします。
 3. [接続] タブをクリックし、マネージメントサーバの名前または IP アドレスとポート番号を指定します。マネージメントサーバの初期設定のポートは 443 です。
-



注意

この画面で指定する IP アドレスとポート番号は、Web ブラウザで Web 管理コンソールにアクセスするために使用されます。

4. マネージメントサーバでプロキシサーバを使用してインターネットに接続する場合は、[プロキシの設定] タブでプロキシの設定を指定します。
 - a. [プロキシの設定] タブで、[マネージメントサーバで次のプロキシ設定を使用] を選択し、次の情報を指定します。
 - プロキシサーバの名前または IP アドレス

- ポート番号
 - プロキシのプロトコル
 - 除外設定: プロキシ設定をバイパスする Web アドレスを追加します。
- b. プロキシサーバで認証が必要な場合は、[プロキシ認証] にユーザ ID とパスワードを入力します。
5. [保存] をクリックします。
- これにより、設定した IP アドレスとポート番号を使用して、Web 管理コンソールにログオンします。

次に進む前に

全体的な手順を確認したい場合は、[67 ページの「初期サーバセットアップ」](#)を参照してください。

Exchange Server との統合を設定する



注意

このトピックは、フル機能配信モードにのみ該当します。

手順

1. Mobile Security の Web 管理コンソールで、[管理] > [Exchange Server との統合] の順に選択します。

[Exchange Server との統合] 画面が表示されます。

2. [Exchange Connector] で、[有効化] を選択し、コンプライアンスに準拠していないモバイルデバイスから Exchange Server へのアクセスをブロックします。

[Exchange Server との統合] 画面に表示される Exchange Connector のさまざまなステータスについては、[83 ページの「Exchange Connector のステータス」](#)を参照してください。

3. [Exchange のアクセス制御] で、必要に応じて次の項目を更新します。
 - [管理対象外のデバイスによる Exchange Server へのアクセスを自動的にブロックする] を選択します。

**注意**

Mobile Security サーバに登録されていないデバイスのことを「管理対象外のデバイス」と呼びます。これには、Exchange Server に登録されたばかりのデバイスも含まれます。

- [次のデバイスから企業データ(メール、カレンダー、連絡先など)へのアクセスを許可する] を選択し、次のいずれかを選択します。
 - 最新のデバイスのみ
 - 正常なデバイスとコンプライアンス違反のデバイス

**注意**

モバイルデバイスのさまざまな登録ステータスについては、管理者ガイドの「ダッシュボード情報」を参照してください。

- [すべての管理対象デバイスに対して [アクセスを自動許可/ブロック] オプションを自動的に有効にする] を選択します。

**注意**

このオプションを有効にすると、Exchange Server へのアクセスが管理対象デバイスのステータスに応じて自動的に許可またはブロックされます。

- Exchange Server へのアクセスをブロックするまでの日数をリストから選択します。

4. [保存] をクリックします。

次に進む前に

全体の手順を確認したい場合は、67 ページの「初期サーバセットアップ」を参照してください。

Exchange Server との統合を設定するその他の手順については、52 ページの「Exchange Server との統合を設定する」を参照してください。

Exchange Connector のステータス



注意

このトピックは、フル機能配信モードにのみ該当します。

次の表に、[Exchange Server との統合] 画面に表示される、Exchange Connector のステータスを示します。

表 4-2. Exchange Connector のステータス

ステータス	説明
正常	Exchange Connector はマネージメントサーバに接続されています。
Exchange Connector への接続を待機しています	マネージメントサーバは、Exchange Connector がマネージメントサーバに接続されるのを待機しています。
警告	Exchange Connector とマネージメントサーバが 5 分以上接続されていない状態です。
切断	Exchange Connector とマネージメントサーバが 9 分以上接続されていない状態です。
無効	Exchange Connector はマネージメントサーバに接続されていますが、Mobile Security の Exchange Server との統合の設定が無効になっています。

通知とレポートを設定する

通知メールを管理者に送信するように通知元を設定できます。

手順

1. Web 管理コンソールにログオンします。

2. [通知とレポート] > [設定] をクリックします。
3. [差出人] のメールアドレス、SMTP サーバの IP アドレス、およびそのポート番号を入力します。SMTP サーバが認証を必要とする場合は、[認証情報] を選択して、ユーザ名およびパスワードを入力します。

次に進む前に

全体の手順を確認したい場合は、67 ページの「初期サーバセットアップ」を参照してください。

また、Mobile Device エージェントの設定手順に戻るには、89 ページの「Mobile Device エージェントを設定する」を参照してください。

管理者への通知を設定する

エラーメッセージの通知と通常の定期レポートをメールで受信するように、管理者への通知およびレポートを設定できます。

手順

1. Web 管理コンソールにログオンします。
2. [通知とレポート] > [管理者への通知とレポート] をクリックします。
3. メールで受信する通知とレポートを選択し、その内容を変更します。完了したら、[保存] をクリックして [管理者への通知/レポート] に戻ります。



注意

受信するレポートを選択する際に、各レポートの後ろにあるリストから受信頻度を個々に調整することもできます。

-
4. [保存] をクリックします。

次に進む前に

全体の手順を確認したい場合は、67 ページの「初期サーバセットアップ」を参照してください。

Mobile Security の設定を検証する

[設定および検証] では、すべての設定が正しく行われているかどうかを検証することができます。

手順

1. Web 管理コンソールにログオンします。
2. [管理] > [設定および検証] をクリックします。
3. [Mobile Security の設定の検証] をクリックします。

次に進む前に

全体的な手順を確認したい場合は、[67 ページの「初期サーバセットアップ」](#)を参照してください。

第 5 章

Mobile Device エージェントの操作

この章では、Mobile Device エージェントでサポートされるモバイルデバイスの要件とモデルを示し、プラットフォームに応じた Mobile Device エージェントの配置方法について説明します。

この章には、次のセクションが含まれています。

- 88 ページの「サポート対象のモバイルデバイスとプラットフォーム」
- 88 ページの「デバイスのストレージとメモリ」
- 89 ページの「Mobile Device エージェントを設定する」
- 90 ページの「サーバで登録依頼のメールを設定する (オプション)」
- 90 ページの「インストールメッセージを設定する」
- 91 ページの「ユーザに登録を依頼する」
- 95 ページの「モバイルデバイスに MDA をインストールする」
- 99 ページの「Mobile Security マネージメントサーバに MDA を登録する」
- 105 ページの「モバイルデバイスの MDA をアップグレードする」

サポート対象のモバイルデバイスとプラットフォーム



注意

モバイルデバイスが、Wi-Fi、3G、またはホストコンピュータでのネットワーク接続を使用して、コミュニケーションサーバに接続できることを確認してください。

Mobile Security Mobile Device エージェントプログラム (Mobile Device エージェント) をインストールして使用する前に、モバイルデバイスが要件を満たしていることを確認してください。

デバイスのストレージとメモリ

最新のシステム要件については、次の Web サイトを参照してください。

<http://www.go-tm.jp/tmms/req>

Mobile Device エージェントを設定する

表 5-1. Mobile Device エージェントの設定プロセス

手順	操作	説明	
手順 1	(オプション) モバイルデバイス向けの通知を設定する	メールを使用して、インストールと登録の詳細をユーザに通知する場合は、これらの手順を実行します。	詳細な手順については、 83 ページの「通知とレポートを設定する」 を参照してください。
手順 2	(オプション) Mobile Security からユーザに送信するインストールメッセージを設定する。		インストールメッセージには、ユーザが MDA のセットアップパッケージをダウンロードしてインストールするための URL が含まれます。 詳細な手順については、 90 ページの「インストールメッセージを設定する」 を参照してください。
手順 3	(フル機能配信モードと指定以外の MDM ベンダーを使用するセキュリティ対策限定配信モード)。 (オプション) ユーザに登録依頼のメールを送信する。		詳細な手順については、 91 ページの「ユーザに登録を依頼する」 を参照してください。
手順 4	モバイルデバイスに MDA をインストールする。	詳細な手順については、 95 ページの「モバイルデバイスに MDA をインストールする」 を参照してください。	
手順 5	Mobile Security マネージメントサーバに MDA を登録する。	詳細な手順については、 99 ページの「Mobile Security マネージメントサーバに MDA を登録する」 を参照してください。	

サーバで登録依頼のメールを設定する (オプション)

インストールおよび登録の詳細をユーザにメールで送信するための、登録依頼メールを設定します。

MDA のインストールおよび登録に登録依頼メールを使用しない場合は、このセクションを省略できます。

インストールメッセージを設定する

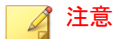
表示するメッセージを入力するには、[インストールメッセージ] 画面を使用します。

この項目は、Mobile Device エージェントを設定する手順の一部です。

全体の手順を確認したい場合は、[89 ページの「Mobile Device エージェントを設定する」](#)を参照してください。

手順

1. Web 管理コンソールにログオンします。
2. [通知とレポート] > [ユーザへの通知] をクリックします。
3. [モバイルデバイスの登録] をクリックして、モバイルデバイスの登録の設定画面を開きます。
4. 記載されている初期設定の件名、メールのメッセージを確認し、必要に応じて変更します。



注意

[メッセージ] フィールドでトークン変数 <%DOWNLOADURL%> を使用すると、Mobile Device エージェントのセットアップファイルをユーザがサーバからダウンロードする実際の URL に置き換えられます。

例: <a href=<%DOWNLOADURL%>><%DOWNLOADURL%>

**注意**

メール通知で送信されるのは、クライアントのセットアップファイルをダウンロードするためのダウンロードリンクのみです。サーバの IP アドレスおよびポート番号は登録画面に自動入力されません。

5. [保存] をクリックします。
6. [通知とレポート] > [ユーザへの通知] をクリックします。
7. [モバイルデバイスの登録] を選択し、[保存] をクリックします。

ユーザに登録を依頼する

**注意**

このトピックは、フル機能配信モードと指定以外の MDM ベンダーを使用するセキュリティ対策限定配信モードに該当します。

この項目は、Mobile Device エージェントを設定する手順の一部です。

全体の手順を確認したい場合は、[89 ページの「Mobile Device エージェントを設定する」](#)を参照してください。

手順

1. Mobile Security の Web 管理コンソールで、[ユーザ] を選択します。
[ユーザ] 画面が表示されます。
2. [ユーザ] タブで、[ユーザに登録依頼] をクリックし、次のいずれかのオプションを選択します。

方法	説明
手動でユーザに登録依頼	フォームに 1 件ずつユーザ情報を入力します。

方法	説明
	詳細については、92 ページの「 手動でユーザに登録を依頼する 」を参照してください。
CSV からユーザに登録依頼	ユーザ情報を CSV ファイルからコピーします。 詳細については、93 ページの「 CSV ファイルからユーザに登録を依頼する 」を参照してください。
Active Directory からユーザに登録依頼	Active Directory からユーザを選択します。 詳細については、94 ページの「 Active Directory のユーザに登録を依頼する 」を参照してください。

手動でユーザに登録を依頼する

この方法では、フォームに 1 件ずつユーザ情報を入力して登録を依頼します。


手順

- Mobile Security の Web 管理コンソールで、[ユーザ] > [ユーザに登録依頼] > [手動] の順に選択します。
[手動でユーザに登録依頼] 画面が表示されます。
- [手動でユーザに登録依頼] 画面で次のフィールドを設定します。
 - 電話番号: ユーザに関連付けられている電話番号を入力します。
 - メール: 通知メールを送信するメールアドレスを入力します。
 - ユーザ名: デバイスツリーでデバイスを識別するためのユーザの名前を入力します。
 - グループ: リストからグループを選択します。



ヒント

ユーザは、[モバイルデバイス] 画面で後で別のグループに再割り当てできます。

3. 他のユーザにも登録を依頼する場合は、 ボタンをクリックして手順 2 を繰り返します。
4. [保存] をクリックします。
確認メッセージが表示されます。

CSV ファイルからユーザに登録を依頼する

この方法では、所定のデータ形式を使用した CSV ファイルからユーザ情報をコピーします。データが自動的に検出されて変換され、ユーザ情報フォームに入力されます。

手順

1. Mobile Security の Web 管理コンソールで、[ユーザ] > [ユーザに登録依頼] > [CSV から] の順に選択します。

[CSV からユーザに登録依頼] 画面が表示されます。

2. 次の形式でユーザ情報を入力します。

電話番号 1, メール 1, ユーザ名 1, グループ名 1



注意

情報は、ユーザごとにセミコロン (;) または改行で区切ります。

3. [検証] をクリックして、ユーザ情報が指定の形式に従っているかどうかを検証します。

ポップアップメッセージに検証結果が表示されます。



注意

形式に誤りがある場合は、修正してやりなおします。

4. [保存] をクリックします。
確認メッセージが表示されます。

Active Directory のユーザに登録を依頼する



注意

このトピックは、フル機能配信モードと指定以外の MDM ベンダーを使用するセキュリティ対策限定配信モードに該当します。

この方法では、Active Directory からユーザまたはグループを選択します。

手順

1. Mobile Security の Web 管理コンソールで、[ユーザ] > [ユーザに登録依頼] > [Active Directory から] の順に選択します。
[Active Directory からユーザに登録依頼] 画面が表示されます。
 2. 表示される検索フィールドにユーザ情報を入力し、[検索] をクリックします。
 3. 検索結果からユーザまたはグループを選択し、[登録依頼] をクリックします。
選択したユーザが登録依頼リストに表示されます。
-



注意

グループを選択した場合は、そのグループに属するすべてのユーザが登録依頼リストに表示されます。

4. 登録依頼リストに手動でユーザを追加するには、[操作] 列の追加ボタン (+) をクリックします。ユーザを削除するには、削除ボタン (-) をクリックします。
5. 最初のユーザのグループ設定をすべてのユーザに適用するには、次の手順を実行します。

- a. 最初のユーザの [グループ] リストでオプションを選択します。
 - b. [すべてに適用] をクリックします。
 - c. [OK] をクリックします。
6. [保存] をクリックします。
確認メッセージが表示されます。
-

モバイルデバイスに MDA をインストールする

この項目は、Mobile Device エージェントを設定する際の手順です。

詳細については [89 ページの「Mobile Device エージェントを設定する」](#) を参照してください。

iOS デバイス

手順

1. Mobile Security iOS アプリのバージョンに応じてインストールを実行します。
 - フル機能
 - a. App Store を開き、Trend Micro Mobile Security アプリを検索します。
 - b. [インストール] をタップします。
 - セキュリティ対策限定
 - a. 登録依頼メールに記載されたダウンロード URL にアクセスします。
 - b. Mobile Security iOS アプリをダウンロードしてインストールします。
2. Mobile Security の使用を開始する前に、次の手順を実行する必要があります。

- a. iOS デバイスで、[一般] > [プロファイルとデバイス管理] の順に選択します。
 - b. [Trend Micro Incorporate (Ent)] をタップします。
 - c. ["Trend Micro Incorporate (Ent)"] を信頼] をタップします。
-

Android デバイス

MDA は次のいずれかの方法で Android デバイスにインストールします。

- インストール方法 I: モバイルデバイスで、マネージメントサーバから MDA を直接ダウンロードしてインストールします。手順については、[96 ページの「インストール方法 I」](#)を参照してください。
- インストール方法 II: Web ブラウザを使用して MDA のインストールパッケージをコンピュータにダウンロードした後、それをモバイルデバイスに転送してインストールします。手順については、[97 ページの「インストール方法 II」](#)を参照してください。
- インストール方法 III: モバイルデバイス管理コンソールを使用して MDA のインストールパッケージをコンピュータにダウンロードした後、それをモバイルデバイスに転送してインストールします。手順については、[98 ページの「インストール方法 III」](#)を参照してください。

ユーザに送信される初期設定の登録依頼メールには、マネージメントサーバから MDA を直接ダウンロードしてインストールする方法 (方法 I) が記載されています。アプリを別の方法でインストールするようにユーザに指示する場合は、ユーザに送信する登録依頼メールを変更してください。「[管理者ガイド](#)」の「[ユーザへの通知を設定する](#)」を参照してください。

インストール方法 I

この方法では、MDA を Mobile Security マネージメントサーバからモバイルデバイスに直接ダウンロードしてインストールします。

他の方法については、[96 ページの「Android デバイス」](#)を参照してください。

手順

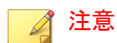
1. 次のいずれかを実行します。

- ローカルコミュニケーションサーバまたはクラウドコミュニケーションサーバを使用している場合、MDA をインストールするモバイルデバイスで、Mobile Security から受信したメールを開いて URL にアクセスし、インストールパッケージをダウンロードします。
- ローカルコミュニケーションサーバを使用している場合、MDA をインストールするモバイルデバイスで、Web ブラウザを使用して次のいずれかの URL にアクセスし、インストールパッケージをダウンロードします。

`http://<外部ドメイン名または IP アドレス>:HTTP ポート/jp/mobile`

または

`https://<外部ドメイン名または IP アドレス>:HTTPS ポート/jp/mobile`



- <外部ドメイン名または IP アドレス>、<HTTP ポート>、および <HTTPS ポート>は、[管理] > [コミュニケーションサーバの設定] > [共通設定] > [コミュニケーションサーバとモバイルデバイスの通信設定] で設定した内容に置き換えます。

2. インストールが自動的に開始されない場合は、インストールパッケージを起動してインストールを完了します。

インストール方法 II

ローカルコミュニケーションサーバを使用している場合は、Web ブラウザを使用して MDA のインストールパッケージをコンピュータにダウンロードし、それをモバイルデバイスに転送してインストールします。

他の方法については、96 ページの「Android デバイス」を参照してください。

手順

1. コンピュータで、次のどちらかの URL にアクセスしてインストールパッケージをダウンロードします。

`http://<外部ドメイン名または IP アドレス>:HTTP ポート/jp/mobile`

または

`https://<外部ドメイン名または IP アドレス>:HTTPS ポート/jp/mobile`



注意

- <外部ドメイン名または IP アドレス>、<HTTP ポート>、および <HTTPS ポート> に割り当てた値を使用します。これらの値を確認するには、[管理] > [コミュニケーションサーバの設定] > [共通設定] > [コミュニケーションサーバとモバイルデバイスの通信設定] を選択します。
-

2. インストールパッケージをダウンロードするモバイルデバイスの OS を選択します。
 3. モバイルデバイスにインストールパッケージをコピーします。
 4. インストールパッケージを起動して、インストールを完了します。
-

インストール方法 III

このトピックは、フル機能配信モードにのみ該当します。

この方法では、Web 管理コンソールを使用して MDA のインストールパッケージをコンピュータにダウンロードし、それをモバイルデバイスに転送してインストールします。

他の方法については、[96 ページの「Android デバイス」](#)を参照してください。

手順

1. Web 管理コンソールにログオンします。
2. [管理] > [デバイス登録設定] をクリックします。

3. [エージェントのインストール] タブで、エージェントのインストールパッケージを選択し、[ダウンロード] をクリックして ZIP ファイルをコンピュータにダウンロードします。
4. ZIP ファイルを解凍して、インストールパッケージをモバイルデバイスにコピーします。
5. インストールパッケージを起動して、インストールを完了します。

Mobile Security マネージメントサーバに MDA を登録する

MDA を手動でインストールする場合、または自動登録プロセスが失敗した場合は、MDA を Mobile Security に手動で登録する必要があります。

この項目は、Mobile Device エージェントを設定する際の手順です。

Android デバイス

MDA を登録するには、次のいずれかの方法で行います。

- QR コードを使用して登録する
ローカルコミュニケーションサーバまたはクラウドコミュニケーションサーバを使用している場合は、この方法で行います。
- サーバのアドレスを使用して登録する
ローカルコミュニケーションサーバを使用している場合は、この方法で行います。
- サーバのアドレスを使用せずに登録する
クラウドコミュニケーションサーバを使用している場合は、この方法で行います。

QR コードを使用して登録する

手順

1. モバイルデバイスで Mobile Device エージェントプログラムを起動します。
2. [QR コードを使用して登録] をタップします。
3. コンピュータまたは別のモバイルデバイスで登録依頼のメールを開き、モバイルデバイスのカメラを使用して、登録依頼のメールに添付された QR コードを読み取ります。
4. 必要に応じて、表示されるフィールドにユーザ名とパスワードを入力し、[OK] をタップします。

Mobile Device エージェントが Mobile Security マネージメントサーバに登録されます。

サーバのアドレスを使用して登録する

手順

1. モバイルデバイスで Mobile Device エージェントプログラムを起動します。
2. [手動で登録] をタップします。
3. [ローカルサーバ] タブをタップし、該当するフィールドにサーバのアドレスとポート番号を入力して、[次へ] をタップします。
4. 該当するフィールドに登録キーまたはユーザ名とパスワードを入力し、[次へ] をタップします。

Mobile Device エージェントが Mobile Security マネージメントサーバに登録されます。

サーバのアドレスを使用せずに登録する

手順

1. モバイルデバイスで Mobile Device エージェントプログラムを起動します。
2. [手動で登録] をタップします。
3. [クラウドサーバ] タブで、登録依頼メールに記載された登録キーを入力し、[次へ] をタップします。

Mobile Device エージェントが Mobile Security マネージメントサーバに登録されます。

iOS デバイス

iOS デバイスを Mobile Security マネージメントサーバから管理するには、モバイルデバイスにプロビジョニングプロファイルをインストールする必要があります。このプロビジョニングプロファイルはユーザ自身およびユーザのモバイルデバイスを識別する必要があります。ユーザ自身の識別には開発証明書を使用し、モバイルデバイスの識別にはデバイス ID のリストを使用します。



警告!

登録するには、iOS デバイスで Safari の JavaScript を有効にする必要があります。有効にしないと、登録は失敗します。

MDA を登録するには、次のいずれかの方法で行います。

- QR コードを使用して登録する
ローカルコミュニケーションサーバまたはクラウドコミュニケーションサーバを使用している場合は、この方法で行います。
- サーバのアドレスを使用して登録する
ローカルコミュニケーションサーバを使用している場合は、この方法で行います。

- サーバのアドレスを使用せずに登録する
クラウドコミュニケーションサーバを使用している場合は、この方法を使用します。

QR コードを使用して登録する

手順

1. モバイルデバイスで Mobile Device エージェントプログラムを起動します。
2. [QR コードを使用して登録] をタップします。
3. コンピュータまたは別のモバイルデバイスで登録依頼のメールを開き、モバイルデバイスのカメラを使用して、登録依頼のメールに添付された QR コードを読み取ります。



注意

ローカルコミュニケーションサーバ用に設定されたルート CA のインストールを求めるポップアップ画面が表示される場合があります。この画面が表示されない場合は、手順 4~6 を省略し、手順 7 に進みます。

4. [OK] をタップします。
TMMSMDM-CA の [プロファイルのインストール] が表示されます。
5. [プロファイルのインストール] で [インストール] をタップしてから、[警告] 画面で [インストール] をタップします。
6. プロファイルのインストールが完了したら、[プロファイルがインストールされました] の [完了] をクリックします。
7. 必要に応じて、表示されるフィールドにユーザ名とパスワードを入力し、[ログイン] をタップします。
MDM 登録プロファイルの [プロファイルのインストール] が表示されます。
8. [プロファイルのインストール] で [インストール] をタップしてから、確認のポップアップ画面で [インストール] をタップします。

9. モバイルデバイスにパスコードが必要な場合は、表示された [パスコードの入力] にパスコードを入力してから、[完了] をタップします。
[プロフィールのインストール] が表示されます。
10. [警告] 確認画面で [インストール] をタップします。
プロフィールのインストールプロセスが開始します。プロセスが完了すると、[プロフィールがインストールされました] と表示されます。
11. [完了] をタップします。

サーバのアドレスを使用して登録する

手順

1. モバイルデバイスで Mobile Device エージェントプログラムを起動します。
2. [手動で登録] をタップします。
3. [ローカルサーバ] タブで、サーバのアドレスとポート番号を入力し、[登録] をタップします。
4. 登録キーまたはユーザ名とパスワードを入力し、[次へ] をタップします。
ローカルコミュニケーションサーバ用に設定されたルート CA のインストールを求めるポップアップ画面が表示される場合があります。この画面が表示されない場合は、手順 5~7 を省略し、手順 8 に進みます。
5. [OK] をクリックします。
TMMSMDM-CA の [プロフィールのインストール] が表示されます。
6. [プロフィールのインストール] 画面で、[インストール] をタップします。
7. モバイルデバイスにパスコードが必要な場合は、表示された [パスコードの入力] にパスコードを入力してから、[完了] をタップします。
8. 表示された [警告] 画面で、[インストール] をタップします。
[プロフィールのインストール] 確認メッセージが表示されます。

9. [インストール] をタップします。
 10. プロファイルのインストールが完了したら、[完了] をタップします。
MDM 登録プロファイルの [プロファイルのインストール] が表示されます。
 11. [インストール] をタップします。
 12. モバイルデバイスにパスコードが必要な場合は、表示された [パスコードの入力] にパスコードを入力してから、[完了] をタップします。
 13. 表示された [警告] 画面で、[インストール] をタップします。
[リモート管理] 確認メッセージが表示されます。
 14. [信頼] をタップします。
 15. プロファイルのインストールが完了したら、[完了] をタップします。
-

サーバのアドレスを使用せずに登録する

手順

1. モバイルデバイスで Mobile Device エージェントプログラムを起動します。
2. [手動で登録] をタップします。
3. [クラウドサーバ] タブで、認証コードを入力し、[登録] をタップします。
MDM 登録プロファイルの [プロファイルのインストール] が表示されます。
4. [プロファイルのインストール] で [インストール] をタップしてから、確認のポップアップ画面で [インストール] をタップします。
5. モバイルデバイスにパスコードが必要な場合は、表示された [パスコードの入力] にパスコードを入力してから、[完了] をタップします。
[プロファイルのインストール] が表示されます。
6. [警告] 確認画面で [インストール] をタップします。

プロファイルのインストールプロセスが開始します。プロセスが完了すると、[プロファイルがインストールされました]と表示されます。

7. [完了]をタップします。
-

モバイルデバイスの MDA をアップグレードする

Mobile Security マネージメントサーバをアップグレードした後、次の手順に従ってモバイルデバイスの MDA をアップグレードします。

Android デバイス

Mobile Security マネージメントサーバのアップグレード後、サーバから Android デバイスに自動的にアップグレード通知が送信されます。

手順

1. Android デバイスで、サーバから受信したアップグレード通知をタップします。
 2. ポップアップ画面で [OK] をタップしてアップグレードを開始します。
-

iOS デバイス

iTunes Store で新しいバージョンが公開されると、iOS デバイスに自動アップグレード通知が送信されます。

手順

1. iOS デバイスで App Store を開きます。
 2. [アップデート]をタップします。
 3. [Mobile Security]、[アップデート]の順にタップしてアップデートを開始します。
-

付録 A

ネットワークポートの設定


この付録では、Trend Micro Mobile Security のインストール時に必要なすべてのネットワークポートの設定を示します。

この付録には、次のセクションが含まれています。


- 108 ページの「クラウドコミュニケーションサーバを使用するセキュリティ強化モデルのネットワークポートの設定」
- 110 ページの「ローカルコミュニケーションサーバを使用するセキュリティ強化モデルのネットワークポートの設定」
- 114 ページの「基本的なセキュリティモデルのネットワークポートの設定」

クラウドコミュニケーションサーバを使用するセキュリティ強化モデルのネットワークポートの設定

クラウドコミュニケーションサーバを使用するセキュリティ強化モデル (デュアルサーバ環境) を使用している場合、Mobile Security コンポーネント用に次のネットワークポートを設定します。

コンポーネント	ネットワークポート	詳細
マネージメントサーバ	<p>次のポートを開きます。</p> <ul style="list-style-type: none"> HTTPS ポート 443: <ul style="list-style-type: none"> マネージメントサーバへの受信接続用。 Google Play から外部アプリを追加する場合。 Google Play ストアのホスト名は「play.google.com」です。 トレンドマイクロの MARS (Mobile Application Reputation Service) を利用する場合は、アップロードされた APK ファイルのセキュリティ情報を参照してください。 MARS サーバのホスト名は「rest.mars.trendmicro.com」です。 <hr/> <p> 注意 これは、初期設定の HTTPS ポート番号です。マネージメントサーバ用の HTTPS ポート番号を変更する場合は、80 ページの「マネージメントサーバを設定する」で詳細を参照してください。</p>	Mobile Security の Web 管理コンソールにアクセスするために使用します。


コンポーネント	ネットワークポート	詳細
	<ul style="list-style-type: none"> • HTTP ポート 80: <ul style="list-style-type: none"> • ライセンスサーバ ライセンスサーバのホスト名は「licenseupdate.trendmicro.com」です。 • トレンドマイクロのアップデートサーバをアップデート元として使用する場合。 アップデートサーバのホスト名は「mobilesecurity.activeupdate.trendmicro.com」です。 	
マネージメントサーバ	次のポートを開きます。 <ul style="list-style-type: none"> • HTTP ポート 80 および HTTPS ポート 443: <ul style="list-style-type: none"> • クラウドコミュニケーションサービスへの送信接続用。 • Apple 社のアプリストアから外部の iOS アプリを追加する場合。 Apple 社のアプリストアのホスト名は「itunes.apple.com」です。 • iOS デバイスに対してカテゴリベースのアプリケーション制御を使用する場合。 ファイアウォールの除外設定に次の 2 つのクラウドコミュニケーションサービスホストを追加します。 <ul style="list-style-type: none"> • ccs.trendmicro.com • ccs01.trendmicro.com • ccs02.trendmicro.com 	Mobile Security の Web 管理コンソールにアクセスするために使用します。
SCEP (Simple Certificate	コミュニケーションサーバと iOS デバイス用に、HTTP ポート 80 を開きます。	(フル機能配信モードのみ)。



コンポーネント	ネットワークポート	詳細
Enrollment Protocol) サーバ		iOS デバイスの登録に使用します。 SCEP サーバを使用して iOS デバイスを管理しない場合、このポートは不要です。
SQL Server	次のポートを開きます。 <ul style="list-style-type: none"> マネージメントサーバで TCP ポート 1433 マネージメントサーバで UDP ポート 1434 <hr/>  注意 これは、SQL Server に接続する初期設定の TCP ポートです。ただし、必要に応じて SQL Server に別のポートを使用することもできます。	マネージメントサーバとリモート SQL Server 間の接続を確立します。

ローカルコミュニケーションサーバを使用するセキュリティ強化モデルのネットワークポートの設定


ローカルコミュニケーションサーバを使用するセキュリティ強化モデル (デュアルサーバ環境) を使用している場合、Mobile Security コンポーネント用に次のネットワークポートを設定します。

コンポーネント	ネットワークポート	詳細
マネージメントサーバ	次のポートを開きます。 <ul style="list-style-type: none"> HTTPS ポート 443: <ul style="list-style-type: none"> マネージメントサーバへの受信接続用。 	Mobile Security の Web 管理コンソールにアクセスするために使用します。

コンポーネント	ネットワークポート	詳細
	<ul style="list-style-type: none"> • Google Play から外部アプリを追加する場合。 Google Play ストアのホスト名は「play.google.com」です。 • トレンドマイクロの MARS (Mobile Application Reputation Service) を利用する場合は、アップロードされた APK ファイルのセキュリティ情報を参照してください。 MARS サーバのホスト名は「rest.mars.trendmicro.com」です。 <hr/> <p> 注意 これは、初期設定の HTTPS ポート番号です。マネージメントサーバ用の HTTPS ポート番号を変更する場合は、80 ページの「マネージメントサーバを設定する」で詳細を参照してください。</p> <hr/> <ul style="list-style-type: none"> • HTTP ポート 80: <ul style="list-style-type: none"> • ライセンスサーバ ライセンスサーバのホスト名は「licenseupdate.trendmicro.com」です。 • トレンドマイクロのアップデートサーバをアップデート元として使用する場合。 アップデートサーバのホスト名は「mobilesecurity.activeupdate.trendmicro.com」です。 	
マネージメントサーバ	次のポートを開きます。	Mobile Security の Web 管理コンソールに

コンポーネント	ネットワークポート	詳細
	<ul style="list-style-type: none"> • HTTP ポート 80 および HTTPS ポート 443: • Apple 社のアプリストアから外部の iOS アプリを追加する場合。 Apple 社のアプリストアのホスト名は「<code>itunes.apple.com</code>」です。 • iOS デバイスに対してカテゴリベースのアプリケーション制御を使用する場合。 	アクセスするために使用します。
コミュニケーションサーバ	<p>HTTP ポート 8080 を開きます。</p> <hr/> <p> 注意 これは、デュアルサーバ設定の初期設定の HTTP ポート番号です。インストール時にモバイルデバイスとコミュニケーションサーバ間の通信に使用する HTTP ポート番号を変更する場合は、70 ページの「コミュニケーションサーバの共通項目を設定する」で詳細を参照してください。</p>	モバイルデバイスとコミュニケーションサーバ間の通信に使用しません。
	<p>HTTPS ポート 4343 を開きます。</p> <hr/> <p> 注意 これは、デュアルサーバ設定の初期設定の HTTPS ポート番号です。</p>	モバイルデバイスとコミュニケーションサーバ間のセキュリティで保護された通信に使用します。
	<p>Apple プッシュ通知サービス (APNs) サーバ用に TCP ポート 2195 を開きます。APNs のホスト名は「<code>gateway.push.apple.com</code>」です。</p>	<p>Apple の APNs サーバで iOS デバイスを管理できるようになります。</p> <p>APNs サーバを使用しないで iOS デバイスを管理しない場合、このポートは不要です。</p>


コンポーネント	ネットワークポート	詳細
	<p>TCP ポート 4343 を開きます。これは、マネージメントサーバからコミュニケーションサーバへの受信接続を許可するための初期設定のポートです。インストール時にモバイルデバイスとコミュニケーションサーバ間の通信に使用する HTTP ポート番号を変更する場合は、70 ページの「コミュニケーションサーバの共通項目を設定する」で詳細を参照してください。</p> <p>TCP ポート 443 を開きます。</p>	<p>マネージメントサーバとコミュニケーションサーバ間の接続を確立します。</p> <p>ローカルコミュニケーションサーバとクラウドコミュニケーションサーバの間の接続を確立します。</p>
Active Directory	<p>次のいずれかのポートを開きます。</p> <ul style="list-style-type: none"> • TCP ポート 389 (ドメインコントローラ): マネージメントサーバ用 • TCP ポート 3268 (グローバルカテゴリ): マネージメントサーバ用 	<p>Active Directory によるユーザ認証に使用します。</p> <p>Active Directory を使用してユーザを認証またはインポートしない場合、このポートは不要です。</p>
SCEP (Simple Certificate Enrollment Protocol) サーバ	<p>コミュニケーションサーバと iOS デバイス用に、HTTP ポート 80 を開きます。</p>	<p>iOS デバイスの登録に使用します。</p> <p>SCEP サーバを使用して iOS デバイスを管理しない場合、このポートは不要です。</p>
SQL Server	<p>次のポートを開きます。</p> <ul style="list-style-type: none"> • マネージメントサーバで TCP ポート 1433 • マネージメントサーバで UDP ポート 1434 	<p>リモート SQL Server を使用してコミュニケーションサーバとマネージメントサーバ間の接続を確立します。</p>

コンポーネント	ネットワークポート	詳細
	 注意 TCP ポート 1433 は、SQL Server に接続する初期設定のポートです。ただし、必要に応じて SQL Server に別の TCP ポートを使用することもできます。	


基本的なセキュリティモデルのネットワークポートの設定

基本的なセキュリティモデル (単一サーバ環境) を使用している場合、Mobile Security コンポーネント用に次のネットワークポートを設定します。

コンポーネント	ネットワークポート	詳細
マネージメントサーバとローカルコミュニケーションサーバ	次のポートを開きます。 <ul style="list-style-type: none"> HTTPS ポート 443: <ul style="list-style-type: none"> Mobile Security マネージメントサーバへの受信接続用。 Google Play から外部アプリを追加する場合。 Google Play ストアのホスト名は「play.google.com」です。 トレンドマイクロの MARS (Mobile Application Reputation Service) を利用する場合は、アップロードされた APK ファイルのセキュリティ情報を参照してください。 MARS サーバのホスト名は「rest.mars.trendmicro.com」です。 	Mobile Security の Web 管理コンソールにアクセスするために使用します。

コンポーネント	ネットワークポート	詳細
	<p> 注意</p> <p>これは、初期設定の HTTPS ポート番号です。マネージメントサーバ用の HTTPS ポート番号を変更する場合は、80 ページの「マネージメントサーバを設定する」で詳細を参照してください。</p> <hr/> <ul style="list-style-type: none"> • HTTP ポート 80: <ul style="list-style-type: none"> • ライセンスサーバ ライセンスサーバのホスト名は「licenseupdate.trendmicro.com」です。 • トレンドマイクロのアップデートサーバをアップデート元として使用する場合。 アップデートサーバのホスト名は「mobilesecurity.activeupdate.trendmicro.com」です。 	
マネージメントサーバとローカルコミュニケーションサーバ	<p>次のポートを開きます。</p> <ul style="list-style-type: none"> • HTTP ポート 80 および HTTPS ポート 443: <ul style="list-style-type: none"> • Apple 社のアプリストアから外部の iOS アプリを追加する場合。 Apple 社のアプリストアのホスト名は「itunes.apple.com」です。 • iOS デバイスに対してカテゴリベースのアプリケーション制御を使用する場合。 	Mobile Security の Web 管理コンソールにアクセスするために使用します。
マネージメントサーバとローカルコミュニケーションサーバ	HTTP ポート 8080 を開きます。	モバイルデバイスと Mobile Security コミュニケーションサーバ間の通信に使用します。

コンポーネント	ネットワークポート	詳細
	 注意 これは、デュアルサーバ設定の初期設定の HTTP ポート番号です。	
	HTTPS ポート 4343 を開きます。	モバイルデバイスと Mobile Security コミュニケーションサーバ間のセキュリティで保護された通信に使用しません。
	 注意 これは、デュアルサーバ設定の初期設定の HTTPS ポート番号です。インストール時にモバイルデバイスとコミュニケーションサーバ間の通信に使用する HTTP ポート番号を変更する場合は、70 ページの「コミュニケーションサーバの共通項目を設定する」で詳細を参照してください。	
	Apple プッシュ通知サービス (APNs) サーバ用に TCP ポート 2195 を開きます。APNs のホスト名は「 <code>gateway.push.apple.com</code> 」です。	Apple の APNs サーバで iOS デバイスを管理できるようになります。 iOS デバイスを管理しない場合、このポートは不要です。
TCP ポート 443 を開きます。	ローカルコミュニケーションサーバとクラウドコミュニケーションサーバの間の接続を確立します。	
Active Directory	次のいずれかのポートを開きます。 <ul style="list-style-type: none"> • TCP ポート 389 (ドメインコントローラ): マネージメントサーバ用 • TCP ポート 3268 (グローバルカテゴリ): マネージメントサーバ用 	Active Directory によるユーザ認証に使用しません。 Active Directory を使用してユーザを認証またはインポートしない場合、このポートは不要です。

コンポーネント	ネットワークポート	詳細
SCEP (Simple Certificate Enrollment Protocol) サーバ	コミュニケーションサーバと iOS デバイス用に、HTTP ポート 80 を開きます。	iOS デバイスの登録に使用します。 SCEP サーバを使用して iOS デバイスを管理しない場合、このポートは不要です。
SQL Server	<p>次のポートを開きます。</p> <ul style="list-style-type: none"> • TCP ポート 1433: Mobile Security マネージメントサーバ用 • TCP ポート 1434: Mobile Security マネージメントサーバ用 <hr/> <p> 注意 これは、SQL Server に接続する初期設定の TCP ポートです。ただし、必要に応じて SQL Server に別のポートを使用することもできます。</p>	Mobile Security マネージメントサーバとリモート SQL Server 間の接続を確立します。

付録 B

オプションの設定

この付録では、Trend Micro Mobile Security のインストール中に実行できるオプションの設定手順を示します。

この付録には、次のセクションが含まれています。

- 120 ページの「SQL Server に Windows 認証を使用する」
- 122 ページの「コミュニケーションサーバのポートを設定する」
- 123 ページの「SCEP を設定する」

SQL Server に Windows 認証を使用する

SQL Server には、Windows 認証方式でなく SQL Server 認証方式を使用することをお勧めします。ただし、SQL Server に Windows 認証を設定することもできます。

手順

1. Mobile Security データベースへのアクセス権を持つユーザアカウントを Active Directory サーバに作成します。必要なアクセス権を持つユーザアカウントを作成済みの場合は、この手順を省略できます。
 - a. Active Directory サーバでユーザアカウントを作成します。
 - b. SQL Server Management Studio を起動して、Mobile Security データベースに接続します。
 - c. オブジェクト エクスプローラーのツリーで [セキュリティ] フォルダを展開します。
 - d. [ログイン] を右クリックし、[新しいログイン] をクリックします。
 - e. 左側の [ページの選択] にある [全般] をクリックして、次の手順を実行します。
 - i. [120 ページの手順 a](#) で作成したユーザ名を [ログイン名] に入力し、[検索] をクリックします。
[ユーザーまたはグループの選択] 画面が表示されます。
 - ii. ユーザ名とドメイン名 (例: domainname\username) を [選択するオブジェクト名を入力してください] に入力し、[名前の確認] をクリックします。
 - iii. [OK] をクリックします。
 - f. 左側の [ページの選択] で [サーバー ロール] を選択し、次のロールを選択します。
 - public
 - sysadmin

- g. [OK] をクリックします。
オブジェクトエクスプローラーの [ログイン] フォルダにユーザアカウントが表示されます。
2. Active Directory サーバと同じドメインに Mobile Security マネージメントサーバを追加します。
3. マネージメントサーバで、[スタート] > [管理ツール] > [コンピューターの管理] の順に選択して、次の手順を実行します。
 - a. 左側のツリーで [ローカル ユーザーとグループ] フォルダを展開し、[グループ] をダブルクリックします。
 - b. [Administrators] を右クリックし、[プロパティ] をクリックします。
 - c. [全般] タブの [追加] ボタンをクリックして、次の手順を実行します。
 - i. [120 ページの手順 a](#) で作成したユーザ名を [ログイン名] に入力し、[検索] をクリックします。
[ユーザーの選択] 画面が表示されます。
 - ii. ユーザ名とドメイン名 (例: domainname\username) を [選択するオブジェクト名を入力してください] に入力し、[名前を確認] をクリックします。
 - iii. [OK] をクリックします。
 - d. [Administrator のプロパティ] 画面で [OK] をクリックします。
4. マネージメントサーバで、次の場所に移動します。
C:\¥Program Files¥Trend Micro¥ Mobile Security¥
または
C:\¥Program Files(x86)\¥Trend Micro ¥Mobile Security¥)
5. TmDatabase.ini をテキストエディタで開きます。TmDatabase.ini ファイルが存在しない場合は、テキストエディタを使用してファイルを作成し、TmDatabase.ini という名前を付けます。
6. TmDatabase.ini ファイルに次のテキストを追加します。

```
ConnectionStringFormat=Provider=sqloledb;Data Source=%server%;Initial Catalog=%database%;Integrated Security=SSPI;
```

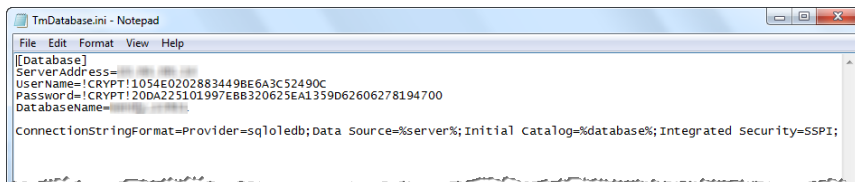


図 B-1. TmDatabase.ini ファイル

7. マネージメントサーバで Windows サービスを開き、[マネージメントサーバサービス] をダブルクリックします。
8. [ログオン] タブで、[現在のアカウント:] を選択し、データベースにアクセスするアカウント名を入力します。パスワードを [パスワード] および [パスワードの確認] に入力し、[OK] をクリックします。
9. サービスリストで [マネージメントサーバサービス] を右クリックし、[再起動] をクリックします。
10. Web 管理コンソールでデータベースを設定します。
 - a. Web 管理コンソールにログオンします。
 - b. [管理] > [データベースの設定] をクリックします。
 - c. データベースサーバの IP アドレス、ユーザ名、パスワード、およびデータベース名を入力します。
 - d. [保存] をクリックします。

コミュニケーションサーバのポートを設定する

Trend Micro Mobile Security 9.8 を使用すると、マネージメントサーバとの接続を確立するために使用されるコミュニケーションサーバのポートをカスタマイズできます。

手順

1. コミュニケーションサーバがインストールされているコンピュータで、C:\Program Files\Trend Micro\Communication ServerまたはC:\Program Files(x86)\Trend Micro\Communication Serverにある configuration.xml ファイルをテキストエディタで開きます。
 2. mdms_https_port の値を、必要なポート番号に変更します。
 3. configuration.xml ファイルを保存して、閉じます。
 4. Windows サービスを開いて、[Mobile Security コミュニケーションサービス] を右クリックし、[再起動] をクリックします。
 5. Web 管理コンソールにログオンします。
 6. [管理] > [コミュニケーションサーバの設定] > [共通設定] をクリックします。
 7. [コミュニケーションサーバとマネージメントサーバの通信設定] で、[HTTPS ポート番号] の値を、[123 ページの手順 2](#) で設定したポート番号に変更します。
 8. [保存] をクリックします。
-

SCEP を設定する



注意

このトピックは、フル機能配信モードにのみ該当します。

SCEP (Simple Certificate Enrollment Protocol) を設定すると、iOS デバイスのセキュリティが強化されます。

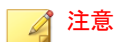
詳細については [29 ページの「iOS デバイス用の環境を設定する \(オプション\)」](#) を参照してください。

手順

1. CA (証明機関) をインストールします。

CA の詳細なインストール手順については、次の URL を参照してください。

<http://msdn.microsoft.com/ja-jp/library/ff720354.aspx>



SCEP を使用しない場合、CA をインストールする必要はありません。

2. SCEP (Simple Certificate Enrollment Protocol) を設定します。

Windows Server 2008 で SCEP が設定されている場合は、Windows サーバ用のネットワークデバイス登録サービスをインストールします。ネットワークデバイス登録サービスのインストールおよび配置手順については、次の URL を参照してください。

<https://success.trendmicro.com/solution/1060187-deploying-the-scep-server-for-mobile-security-tmms-for-ios-on-a-windows-server-2008>

または

[http://technet.microsoft.com/ja-jp/library/ff955646\(WS.10\).aspx](http://technet.microsoft.com/ja-jp/library/ff955646(WS.10).aspx)



SCEP は Windows Server 2008 で使用することをお勧めします。

3. システム時計を検証します。
SCEP サーバ、コミュニケーションサーバ、およびマネージメントサーバのシステム時計が正しい時刻に設定されていることを確認します。
4. 次の手順に従って、CA のポリシーモジュールプロパティを変更します。
 - a. CA がインストールされたコンピュータで、CA の管理コンソールを開きます。
 - b. [ポリシーモジュール] タブ→[プロパティ] の順にクリックします。
 - c. [証明書テンプレートに操作が設定されている場合はそれに従い、設定されていない場合は自動的に証明書を発行する] を選択します。
 - d. [OK] をクリックします。
5. 次のルールと設定を適用します。
 - iOS デバイスを、コミュニケーションサーバに接続できるようにします。
 - コミュニケーションサーバを、SCEP サーバに接続できるようにします。
 - iOS デバイスを、Mobile Security マネージメントサーバに登録するときに SCEP サーバに直接接続できるようにします。
6. SCEP のインストールを検証します (オプション)。

Windows Server 2008 で SCEP が実行されている場合は、コミュニケーションサーバから次の URL にアクセスします。

http://<SCEPServerIP>/certsrv/mscep_admin

**注意**

URL 内の<SCEPServerIP>は、実際の SCEP サーバの IP アドレスで置き換えてください。

次のような Web ページが表示されていれば、サーバは適切に設定されています。

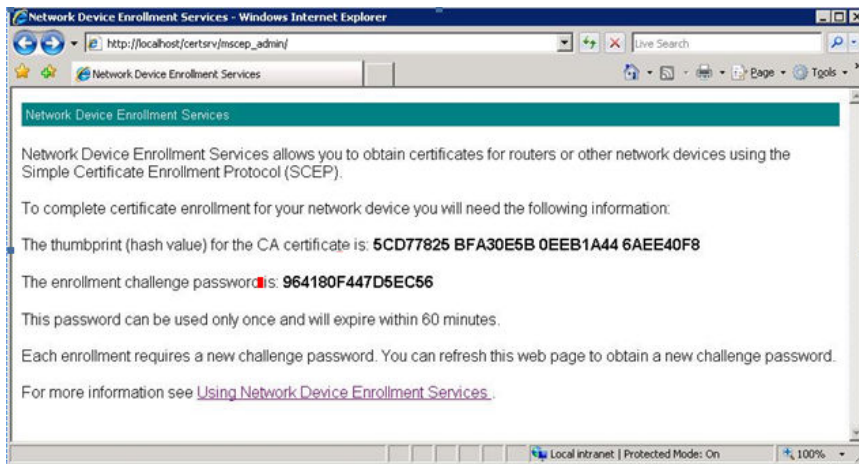
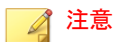


図 B-2. 設定の検証



注意

iOS デバイスを登録すると、次の URL にアクセスできるようになります。

<http://<SCEPServerIP>/certsrv/mscep>

iOS デバイスを SCEP に接続する必要があるのは、登録する場合のみです。それ以外の用途には、この接続は不要です。

付録 C

APNs 証明書の生成と設定

Trend Micro Mobile Security で iOS デバイスを管理するには、Apple Push Notification サービス (APNs) 証明書が必要です。この付録では、APNs 証明書を生成して Mobile Security マネージメントサーバにアップロードする詳細な手順を示します。

その他のセットアップ要件については、[29 ページの「iOS デバイス用の環境を設定する \(オプション\)」](#)を参照してください。

この付録には、次のセクションが含まれています。

- [128 ページの「APNs 証明書について」](#)
- [128 ページの「APNs 証明書を生成する」](#)
- [129 ページの「Windows Server から APNs 証明書を生成する」](#)
- [142 ページの「Mac OS X ワークステーションから APNs 証明書を生成する」](#)
- [148 ページの「Mobile Security マネージメントサーバに APNs 証明書をアップロードする」](#)

APNs 証明書について

Mobile Security マネージメントサーバからモバイルデバイスへの通信には、OTA (Over The Air) を使用します。Apple Push Notification サービス (APNs) を使用することにより、セキュリティで保護された通信を実行できます。Apple 社のプッシュ通知ネットワークを通じてモバイルデバイスと安全に通信するためには、APNs 証明書が必要です。

管理者が iOS デバイスに対して情報を要求したり、iOS デバイスを管理したりする場合、Mobile Security は、APNs 証明書を使用してモバイルデバイスに通知を送信します。APNs サーバを介して送信されるのは通知のみです。

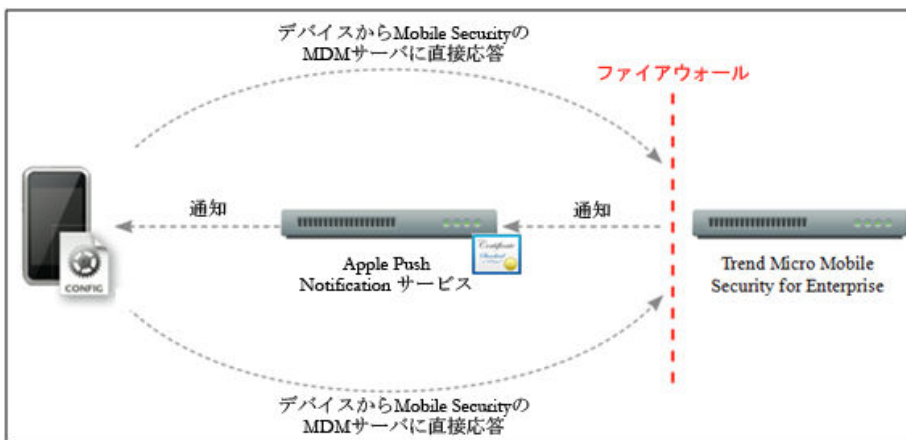


図 C-1. 通知プロセス

APNs 証明書を生成する

このセクションでは、iOS デバイス管理用の Apple Push Notification サービス証明書を生成するプロセスについて説明します。

手順

1. Windows Server または Mac ワークステーションから CSR (Certificate Signing Request) を生成します。
2. トレンドマイクロまたは Apple 社に、CSR への署名を依頼します。

- サポート担当者に依頼し、署名済みの CSR を取得します。
- 正式な Apple ID を使用して、署名済みの CSR を Apple Push Certificates Portal にアップロードします。

Apple 社によって APNs 証明書が生成されます。

- Apple 社が署名した証明書を使用する: Apple 社が署名した証明書を使用する場合は、続行する前に、次のものが用意されていることを確認してください。
 - Apple 社の iOS Developer Enterprise Program の既存のアカウント (<http://developer.apple.com/programs/ios/enterprise>)
 - Agent ロールとして割り当てられた Developer アカウント (Admin ロールでは機能しません)
 - Windows Server または Mac OS X ワークステーションの管理者権限

Apple 社が署名した証明書を使用するには、Windows の場合は136ページの「Apple 社が署名した証明書を使用する」、Mac の場合は144ページの「Apple 社が署名した証明書を使用する」を参照してください。

3. Windows Server または Mac ワークステーションに APNs 証明書をインストールし、証明書をエクスポートしてコンピュータに保存します。

エクスポートした証明書は Trend Micro Mobile Security マネージメントサーバにアップロードします。

Windows Server から APNs 証明書を生成する

Windows Server を使用して APNs 証明書を生成するには、次の手順を実行します。すでに Mac OS X ワークステーションから証明書を生成済みの場合、この

セクションを省略して Mobile Security の MDM サーバに証明書をアップロードする手順に進んでください。

手順 1: CSR (Certificate Signing Request) を生成する

手順

1. [スタート]→[管理ツール]→[インターネット インフォメーション サービス (IIS) マネージャ] の順に選択し、サーバ名を選択します。
2. [サーバ証明書] アイコンをダブルクリックします。

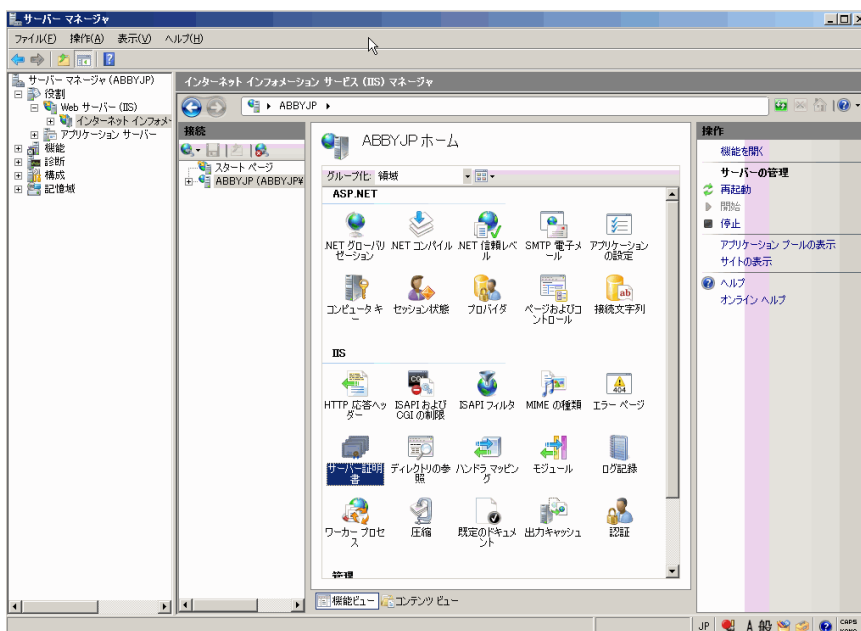


図 C-2. サーバ証明書へのアクセス



注意

このドキュメントでは、IIS バージョン 7.0 を使用して APNs 証明書を設定します。

3. 右側の [操作] ペインで [証明書の要求の作成] をクリックします。
[証明書の要求] ウィザードが開きます。

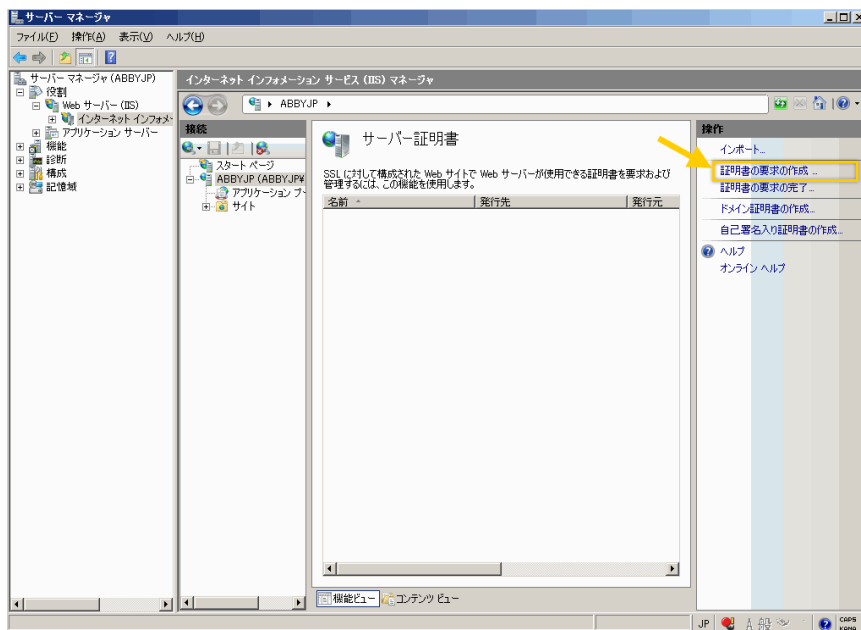


図 C-3. [証明書の要求] ウィザードの起動

4. [識別名プロパティ] で、次の項目を入力します。
 - 一般名: Apple Developer のアカウントに関連する名前
 - 組織: 法的に登録されている組織名または企業名
 - 組織単位 (OU): 組織内の部門名
 - 市区町村: 組織の所在地 (市区町村)
 - 都道府県: 組織の所在地 (都道府県)

- 国/地域: 組織の所在地 (国または地域)

証明書要求

識別名プロパティ

証明書に必要な情報を指定します。都道府県および市区町村に関する情報は、公式なものを指定してください。省略形を使用しないでください。

一般名(M): mobile_dev

組織(O): Trend Micro

組織単位 (OU)(U): TMMS

市区町村(L): Nan.Jing

都道府県(S): JiangSu

国/地域(R): CN

前に戻る(B) 次へ(N) 終了(F) キャンセル

図 C-4. [識別名プロパティ] 画面

5. [次へ] をクリックします。
[暗号化サービス プロバイダのプロパティ] が開きます。
6. [暗号化サービス プロバイダ] で [Microsoft RSA SChannel Cryptographic Provider] を選択し、[ビット長] フィールドで [2048] を選択して、[次へ] をクリックします。

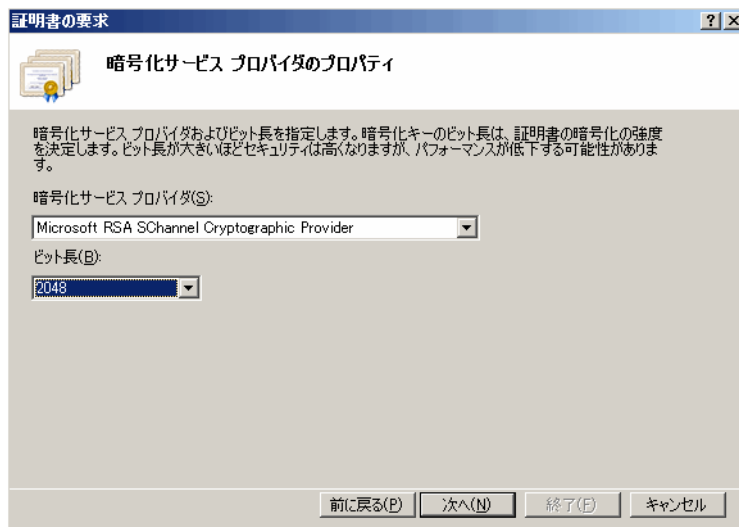


図 C-5. [暗号化サービス プロバイダのプロパティ] 画面

7. 証明書要求ファイルの保存場所を選択します。
ファイル名およびファイルの保存場所は忘れないようにしてください。

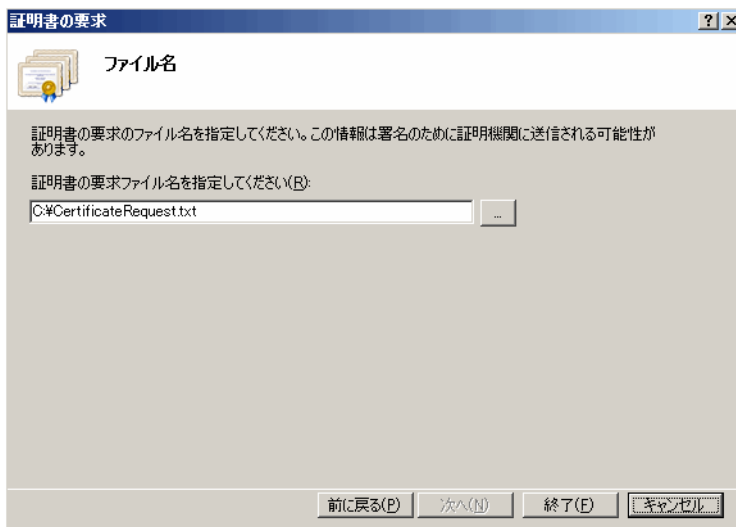


図 C-6. [ファイル名] 画面

8. [終了] をクリックします。

これで、CSR を作成して、Apple 社の開発ポータルにアップロードする準備ができました。

手順 2: CSR をアップロードして APNs 証明書を生成する

CSR を生成すると、次のいずれかを実行できます。

- 生成した CSR をトレンドマイクロ販売代理店またはサポートセンターに送信し、その後返送された CSR を使用して APNs 証明書を生成する
- Apple 社の開発ポータルに CSR をアップロードして、Apple 社が署名した CSR を取得し、この CSR を使用して APNs 証明書を生成する

**注意**

次の手順は、トレンドマイクロが署名した APNs 証明書を使用していることを前提としています。

Apple 社が署名した APNs 証明書を使用する場合はこの手順を省略し、Windows の場合は136 ページの「Apple 社が署名した証明書を使用する」、Mac の場合は144 ページの「Apple 社が署名した証明書を使用する」を参照してください。

手順

1. 以下の製品 Q&A を参照し、作成した CSR に署名します。
<https://success.trendmicro.com/jp/solution/1108633>
2. 署名した CSR を Apple Push Certificates Portal にアップロードします。
 - a. Web ブラウザを開いて、次の URL に移動します。
<https://identity.apple.com/pushcert/>
 - b. Apple ID とパスワードを使用してログインします。
[Get Started] 画面が表示されます。
 - c. [Create a Certificate] ボタンをクリックします。
[Terms of Use] 画面が表示されます。
 - d. [Accept] をクリックして使用条件に同意します。
[Create a New Push Certificate] 画面が表示されます。
 - e. [Browse] をクリックして、トレンドマイクロが署名したファイルを選択し、[Upload] をクリックします。APNs 証明書 (.pem) ファイルが生成されるまで待ちます。
 - f. [Download] をクリックして .pem ファイルをコンピュータに保存します。
 - g. ダウンロードした .pem ファイルの拡張子を .cer に変更し、138 ページの「手順 3: APNs 証明書をインストールする」に進みます (Windows の場合)。

Apple 社が署名した証明書を使用する

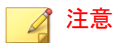


注意

トレンドマイクロが署名した APNs 証明書を取得済みの場合は、この手順を省略してください。

手順

1. Web ブラウザで次の URL に移動します。
<https://developer.apple.com/jp/>
2. [メンバーセンター] リンクをクリックします。
3. Apple ID とパスワードを使用してログインします。
4. [iOS Provisioning Portal] をクリックします。



注意

Developer のアカウントが iOS 開発用に設定されていない場合、[iOS Provisioning Portal] は表示されません。

5. 左側のペインで [App IDs] をクリックし、[New App ID] をクリックします。
6. 該当するフィールドに入力します。[Bundle Identifier (App ID Suffix)] に次のように入力します。com.apple.mgmt.mycompany.tmms
 - 「mycompany」は会社名に置き換えます。
 - [Bundle Identifier (App ID Suffix)] の値は書き留めておいてください。この値は、Mobile Security マネージメントサーバを設定する際に必要になります。
7. [Submit] をクリックします。
追加した App ID がリストに表示されます。
8. [Configure] をクリックします。



ヒント

[Configure] が表示されない場合、またはクリックできない場合は、Agent の役割でログインしていることを確認してください。

9. [Enable for Apple Push Notification service] をオンにして、[Production Push SSL Certificate] の横にある [Configure] をクリックします。

[Enable for Apple Push Notification service] をオンにできない場合は、Safari または Firefox の Web ブラウザを使用してやりなおしてください。また、Agent の役割でログインしていることを確認してください。
 10. [SSL Certificate Assistant] ウィザードが開きます。CSR (Certificate Signing Request) を作成するように記載されていますが、[142 ページの「手順 1: CSR \(Certificate Signing Request\) を生成する」](#)で作成済みです。[Continue] をクリックします。
 11. [Choose File] をクリックし、[142 ページの「手順 1: CSR \(Certificate Signing Request\) を生成する」](#)で作成した CSR ファイルをアップロードします。この例では、CertificateSigningRequest.certSigningRequest2 です。
 12. [Generate] をクリックします。

完了すると、APNs SSL 証明書が生成されたことを確認する画面が表示されます。
 13. [Continue] をクリックします。

[Download & Install Your Apple Push Notification server SSL Certificate] 画面が表示されます。
 14. [Download] をクリックして .cer ファイルをコンピュータに保存し、[146 ページの「手順 3: APNs 証明書をインストールする」](#)に進みます (Mac の場合)。
-

手順 3: APNs 証明書をインストールする

手順

1. [スタート] > [管理ツール] > [インターネット インフォメーション サービス (IIS) マネージャ] の順に選択します。次に、サーバ名を選択し、[サーバー証明書] をダブルクリックします。
2. 右側の [操作] ペインで [証明書の要求の完了] をクリックします。

[証明書の要求の完了] ウィザードが開きます。

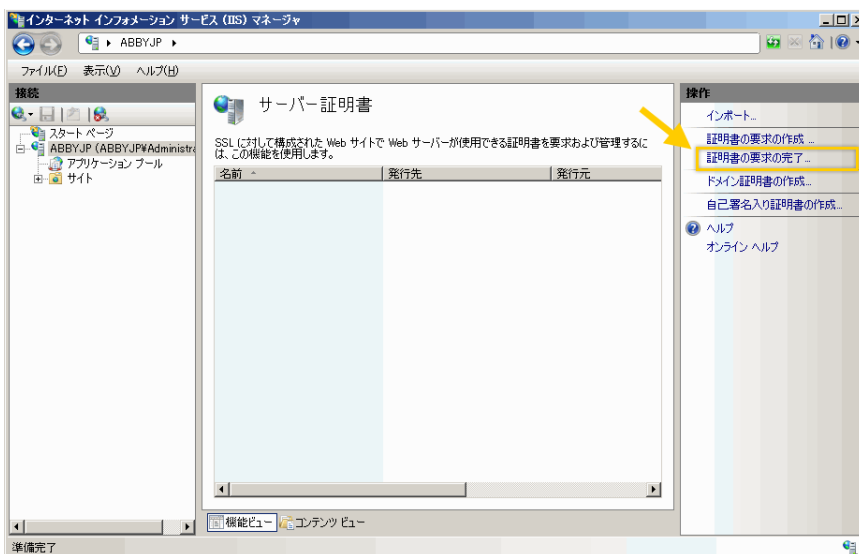


図 C-7. [証明書の要求の完了]

注意

IIS 7.5 を使用する場合は、[証明書の要求の完了] をクリックすると、次のエラーメッセージが表示される可能性があります。

証明書チェーンを、信頼されたルート機関に対して構築できませんでした。

この問題を解決するには、141 ページの「APNs 証明書をインストールするために IIS 7.5 を設定する」を参照してください。

- Apple Developer ポータルからダウンロードした .cer 証明書ファイルを選択し、[フレンドリ名] に **Mobile Security の MDM サーバの APNs** を入力します。

**注意**

Mac ワークステーションから証明書ファイルを生成するには、ファイルの拡張子を .pem から .cer に手動で変更する必要があります。

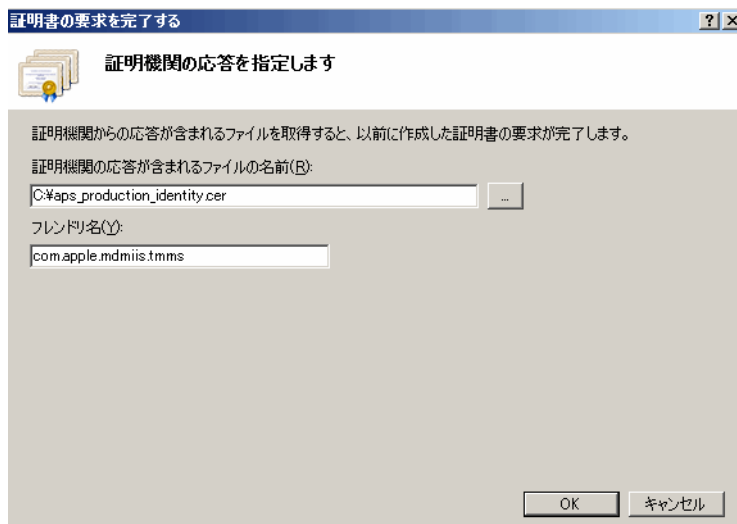


図 C-8. [証明機関の応答を指定します] 画面

**ヒント**

フレンドリ名は証明書の名前または名前の一部ではありません。サーバ管理者が証明書を簡単に識別できるようにするための名前です。

- [OK] をクリックします。
サーバに証明書がインストールされます。
- [サーバー証明書] リストに Apple Production Push Services の証明書が表示されていることを確認します。証明書が表示された場合、以降の手順に

従って証明書をエクスポートし、Mobile Security のマネージメントサーバにアップロードします。

6. [サーバー証明書] リスト内の証明書を右クリックし、[エクスポート] をクリックします。

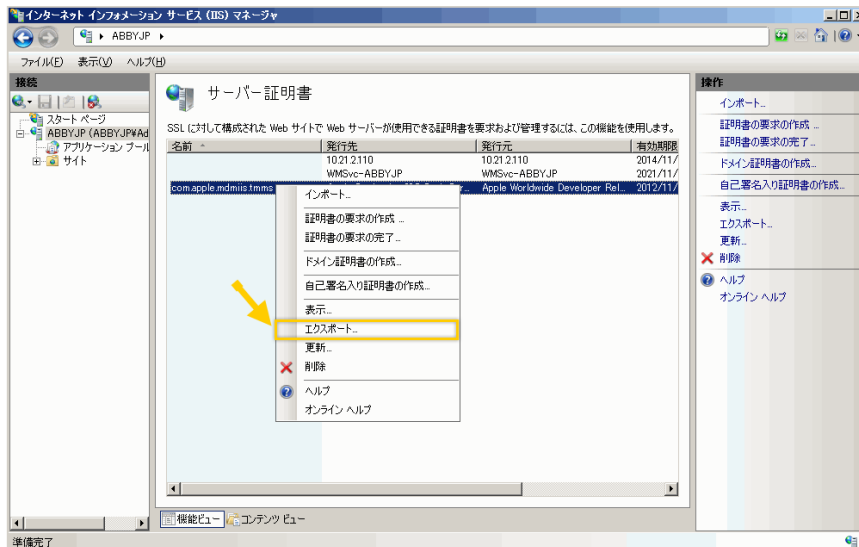


図 C-9. 証明書のエクスポート

7. ファイルの保存場所を選択し、エクスポート用のパスワードを入力して、[OK] をクリックします。

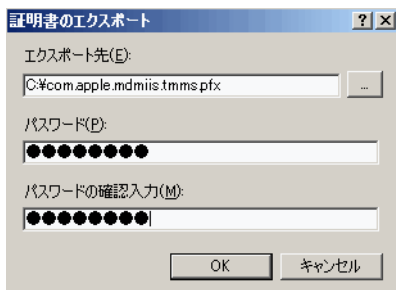


図 C-10. 証明書のエクスポート用のパスワードの指定



ヒント

ファイルの保存オプションに .pfx ではなく .cer のみが表示される場合は、証明書を正しくエクスポートしていません。エクスポート対象として正しいファイルが選択されていることを確認してください。



注意

パスワードは覚えておくか、安全な場所に保管してください。証明書を Mobile Security のマネージメントサーバにアップロードするときに、このパスワードが必要になります。

すべての手順が完了したら、次のものがあることを確認してください。

- APNs 証明書 (.pfx 形式。 .cer 形式ではない)
- 証明書をエクスポートするときに設定したパスワード

これで、証明書を Mobile Security マネージメントサーバにアップロードする準備ができました。手順については、[148 ページの「Mobile Security マネージメントサーバに APNs 証明書をアップロードする」](#)を参照してください。

APNs 証明書をインストールするために IIS 7.5 を設定する

IIS 7.5 を使用する場合は、IIS への証明書のアップロードの際に次のメッセージが表示されて、アップロードが失敗する可能性があります。

証明書チェーンを、信頼されたルート機関に対して構築できませんでした。

このエラーの原因は次のいずれかです。

- APNs 証明書への署名が、公的 CA ではなく Apple 社のルート CA によって行われている。
- IIS 7.5 による信頼されたルート CA の高度なチェック。

手順

1. Apple Root 証明書と Application Integration 証明書を次の URL からダウンロードします。

<http://www.apple.com/certificateauthority/>

2. Apple Root 証明書をダブルクリックし、[証明書] の [証明書のインストール] をクリックします。
3. ウィザードの開始画面で、[次へ] をクリックします。
4. [証明書をすべて次のストアに配置する] を選択し、[参照] をクリックします。
5. [証明書ストアの選択] で、[物理ストアを表示する] チェックボックスをオンにして、[信頼されたルート証明機関] > [ローカル コンピュータ] を選択し、[OK] をクリックします。
6. [証明書のインポート ウィザード] で [次へ] をクリックし、[完了] をクリックします。
7. Application Integration 証明書について、[142 ページの手順 2](#)～[142 ページの 5](#) を繰り返します。ただし、[142 ページの手順 4](#) では、[信頼されたルート証明機関] > [ローカル コンピュータ] ではなく、[中間証明機関] > [ローカル コンピュータ] を選択します。

Mac OS X ワークステーションから APNs 証明書を生成する

Mac OS X ワークステーションを使用して APNs 証明書を生成するには、次の手順を実行します。Windows Server を使用する場合は、このセクションを省略して [129 ページの「Windows Server から APNs 証明書を生成する」](#) に進んでください。

手順 1: CSR (Certificate Signing Request) を生成する

手順

1. Mac コンピュータで、[アプリケーション] > [ユーティリティ] > [キーチェーンアクセス] の順に選択します。
2. 左側のペインの [キーチェーン] で [ログイン] を選択し、[分類] で [証明書] を選択します。

3. 上のメニューバーから [キーチェーンアクセス] > [証明書アシスタント] > [認証局に証明書を要求] の順に選択します。
[証明書アシスタント] ウィザードが開きます。
4. [ユーザのメールアドレス] にメールアドレスを入力し、[通称] に Apple Developer に登録したアカウント名を入力します。[ディスクに保存] を選択し、[続ける] をクリックします。
5. ファイルの保存場所を選択し、[保存] をクリックします。
これで、CSR を作成して、Apple 社の開発ポータルにアップロードする準備ができました。

手順 2: CSR をアップロードして APNs 証明書を生成する

CSR を生成すると、次のいずれかを実行できます。

- 生成した CSR をトレンドマイクロ販売代理店またはサポートセンターに送信し、その後返送された CSR を使用して APNs 証明書を生成する
- Apple 社の開発ポータルに CSR をアップロードして、Apple 社が署名した CSR を取得し、この CSR を使用して APNs 証明書を生成する

注意

次の手順は、トレンドマイクロが署名した APNs 証明書を使用していることを前提としています。

Apple 社が署名した APNs 証明書を使用する場合はこの手順を省略し、Windows の場合は 136 ページの「Apple 社が署名した証明書を使用する」、Mac の場合は 144 ページの「Apple 社が署名した証明書を使用する」を参照してください。

手順

1. 以下の製品 Q&A を参照し、作成した CSR に署名します。
<https://success.trendmicro.com/jp/solution/1108633>
2. 署名した CSR を Apple Push Certificates Portal にアップロードします。

- a. Web ブラウザを開いて、次の URL に移動します。
<https://identity.apple.com/pushcert/>
 - b. Apple ID とパスワードを使用してログインします。
[Get Started] 画面が表示されます。
 - c. [Create a Certificate] ボタンをクリックします。
[Terms of Use] 画面が表示されます。
 - d. [Accept] をクリックして使用条件に同意します。
[Create a New Push Certificate] 画面が表示されます。
 - e. [Browse] をクリックして、トレンドマイクロが署名したファイルを選択し、[Upload] をクリックします。APNs 証明書 (.pem) ファイルが生成されるまで待ちます。
 - f. [Download] をクリックして .pem ファイルをコンピュータに保存します。
 - g. ダウンロードした .pem ファイルの拡張子を .cer に変更し、[146 ページの「手順 3: APNs 証明書をインストールする」](#)に進みます (Mac の場合)。
-

Apple 社が署名した証明書を使用する



注意

トレンドマイクロが署名した APNs 証明書を取得済みの場合は、この手順を省略してください。

手順

1. Web ブラウザで次の URL に移動します。
<https://developer.apple.com/jp/>
2. [メンバーセンター] リンクをクリックします。

- Apple ID とパスワードを使用してログインします。
- [iOS Provisioning Portal] をクリックします。

**注意**

Developer のアカウントが iOS 開発用に設定されていない場合、[iOS Provisioning Portal] は表示されません。

- 左側のペインで [App IDs] をクリックし、[New App ID] をクリックします。
- 該当するフィールドに入力します。[Bundle Identifier (App ID Suffix)] に次のように入力します。com.apple.mgmt.mycompany.tmms
 - 「mycompany」は会社名に置き換えます。
 - [Bundle Identifier (App ID Suffix)] の値は書き留めておいてください。この値は、Mobile Security マネージメントサーバを設定する際に必要になります。
- [Submit] をクリックします。
追加した App ID がリストに表示されます。
- [Configure] をクリックします。

**ヒント**

[Configure] が表示されない場合、またはクリックできない場合は、Agent の役割でログインしていることを確認してください。

- [Enable for Apple Push Notification service] をオンにして、[Production Push SSL Certificate] の横にある [Configure] をクリックします。

[Enable for Apple Push Notification service] をオンにできない場合は、Safari または Firefox の Web ブラウザを使用してやりなおしてください。また、Agent の役割でログインしていることを確認してください。
- [SSL Certificate Assistant] ウィザードが開きます。CSR (Certificate Signing Request) を作成するように記載されていますが、[142 ページの「手順 1: CSR \(Certificate Signing Request\) を生成する」](#)で作成済みです。[Continue] をクリックします。

11. [Choose File] をクリックし、142 ページの「[手順 1: CSR \(Certificate Signing Request\) を生成する](#)」で作成した CSR ファイルをアップロードします。この例では、CertificateSigningRequest.certSigningRequest2 です。
12. [Generate] をクリックします。
完了すると、APNs SSL 証明書が生成されたことを確認する画面が表示されます。
13. [Continue] をクリックします。
[Download & Install Your Apple Push Notification server SSL Certificate] 画面が表示されます。
14. [Download] をクリックして .cer ファイルをコンピュータに保存し、138 ページの「[手順 3: APNs 証明書をインストールする](#)」に進みます (Windows の場合)。



Windows コンピュータに APNs 証明書をインストールするには、ファイルの拡張子を .pem から .cer に手動で変更する必要があります。

手順 3: APNs 証明書をインストールする

手順

1. ファイルをダウンロードした場所に移動します。ファイルをダブルクリックすると、ファイルが [キーチェーンアクセス] に自動的にアップロードされ、署名要求が完了します。
2. [アプリケーション] > [ユーティリティ] > [キーチェーンアクセス] の順に選択します。
3. 左側のペインの [キーチェーン] で [ログイン] を選択し、[分類] で [証明書] を選択します。
4. リストに Apple Production Push Services の証明書が表示されます。表示された証明書を展開すると、その下に関連する秘密鍵が表示されます。証

明書が表示された場合、以降の手順に従って証明書をエクスポートし、Mobile Security マネージメントサーバにアップロードします。



注意

APNs 証明書または秘密鍵が表示されない場合は、[キーチェーン] で [ログイン] が選択されていること、[分類] で [証明書] が選択されていること、および証明書の秘密鍵が展開されていることを確認してください。それでも証明書が表示されない場合は、これまでの手順をすべて繰り返してください。

5. 秘密鍵を右クリックするか、<Ctrl> キーを押しながら秘密鍵をクリックし、[<秘密鍵名> を書き出す] をクリックします。
6. ファイルの保存先の名前と場所を選択し、ファイル形式に [個人情報交換 (.p12)] を選択します。



ヒント

ファイルの保存オプションに .p12 ではなく .cer のみが表示される場合は、証明書を正しくエクスポートしていません。最後の手順でエクスポート対象に秘密鍵を選択したことを確認し、ファイル形式が [個人情報交換 (.p12)] であることを確認してください。

7. [保存] をクリックします。
8. エクスポート用のパスワードを入力して、[OK] をクリックします。



ヒント

パスワードは覚えておくか、安全な場所に保管してください。証明書を Mobile Security マネージメントサーバにアップロードするときに、このパスワードが必要になります。

すべての手順が完了したら、次のものがあることを確認してください。

- APNs 証明書 (.p12 形式。 .cer 形式ではない)
- 証明書をエクスポートするときに設定したパスワード

これで、証明書を Mobile Security マネージメントサーバにアップロードする準備ができました。手順については、148 ページの「[Mobile Security マネージメントサーバに APNs 証明書をアップロードする](#)」を参照してください。

Mobile Security マネージメントサーバに APNs 証明書をアップロードする

このセクションでは、iOS デバイスの管理を開始するために、Apple プッシュ通知サービス (APNs) 証明書を Mobile Security マネージメントサーバにアップロードするプロセスについて説明します。



注意

開始する前に、次のものが用意されていることを確認してください。

- APNs 証明書ファイル (.pfx 形式または .p12 形式。 .cer 形式ではない)
 - 証明書をエクスポートするときに設定したパスワード
 - Mobile Security の MDM サーバの管理者アカウント
-

手順

1. Web 管理コンソールにログオンします。
2. 次のいずれかを実行します。

- [管理] > [証明書の管理] の順にクリックし、[追加] をクリックします。ハードディスク内の Apple プッシュ通知サーバの証明書を選択し、[保存] をクリックします。



図 C-11. [証明書の管理] からの証明書の追加

- [管理] > [コミュニケーションサーバの設定] の順にクリックし、[iOS の設定] タブを選択します。[証明書] でハードディスク内の Apple Push Notification サーバの証明書を選択し、[保存] をクリックします。

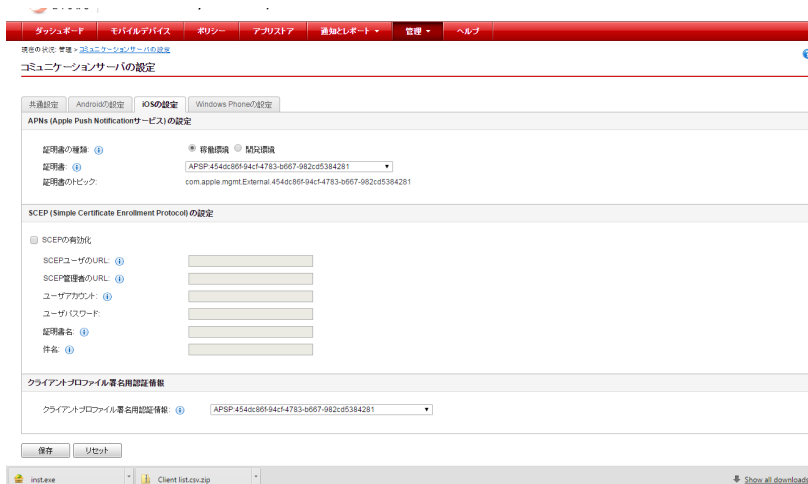


図 C-12. [コミュニケーションサーバの設定] からの証明書の追加

すべての手順が完了したら、iOS デバイスを管理できます。

APNs 証明書を更新する

iOS デバイスを継続して管理するには、APNs 証明書の有効期限が切れる前に、証明書を更新する必要があります。

APNs 証明書を更新するには、新しい証明書を作成する場合と同じ手順を実行します。その後、Apple Push Certificates Portal にアクセスして新しい証明書をアップロードします。

ポータルにログインすると、既存の証明書が表示されます。Apple Developer の以前のアカウントからインポートされた証明書が表示される場合もあります。Certificates Portal で証明書を更新する場合、作成する場合と違って[Renew] をクリックします。

**注意**

Certificates Portal にアクセスするには、Apple Developer のアカウントが必要です。

索引

シンボル

.apk ファイル, 40

アルファベット

Active Directory

サービスアカウント, 34
設定, 79

Android の設定

プッシュ通知, 72

APNs (Apple Push Notification サービス)

ホスト名, 32

APNs 証明書

Apple Push Certificates Portal, 129
CSR (Certificate Signing Request), 129
概要, 128
ホスト名, 116

Apple 社の開発ポータル, 134, 143

App Store, 95

configuration.xml ファイル, 123

Eula_agreement.zip ファイル, 79

Exchange Connector

ステータス, 83

Exchange Server

ExchangeConnector.zip ファイル, 56
管理ツール, 53, 56
サポートされるバージョン, 52

iOS の設定

APNs 証明書, 74
SCEP の設定, 74

Java Runtime Environment, 40

LCS 環境

SSL 証明書, 51
証明書のインポート, 51
証明書の作成, 52

MDA のインストール方法, 96

MDA の登録

Android, 99
iOS, 101

MDM サーバ, 140

Microsoft Exchange Server 管理ツール, 35

Mobile Security

Active Directory, 17
Exchange Connector, 17
Microsoft SQL Server, 17
Mobile Device エージェント, 17
SMTP サーバ, 19
アーキテクチャ, 12
基本的なセキュリティモデル, 12, 15
クラウドコミュニケーションサーバ, 16
コミュニケーションサーバ, 16
コミュニケーションサーバの種類, 16
コンポーネント, 15
最新情報, 7
システム要件, 19

証明書

APNs 証明書, 18
SCEP, 18
SSL 証明書, 18
機関, 17
公開鍵/秘密鍵, 17
セキュリティ認証情報, 17

セキュリティ強化モデル

クラウドコミュニケーションサーバ, 12, 13
ローカルコミュニケーションサーバ, 12, 14

通信手段, 12

- 配置モデル, 12
- マネージメントサーバ, 16
- ローカルコミュニケーションサーバ, 16
- SCEP
 - CA (証明機関), 124
 - ネットワークデバイス登録サービス, 124
- SQL Server
 - 認証方式, 34
- TmDatabase.ini, 121
- Web 管理コンソール, 47
 - URL, 46
 - ユーザ名とパスワード, 47

あ

- アクティベーションコードの形式, 48
- エラーメッセージ, 138

か

環境

- iOS デバイス, 29
- インストール, 28

共通設定

- コミュニケーションサーバの種類, 70
- 情報を収集する頻度, 71

互換表示, 47

- コミュニケーションサーバの接続設定, 50, 51

- コミュニケーションサーバの設定, 70

- Android の設定, 70
- iOS の設定, 70
- 共通設定, 70

コンポーネントのアップデート

- 概要, 58
- 手動, 59

- ダウンロード元, 61
- 予約, 60
- ローカル AU サーバ, 62

さ

- [識別名プロパティ] 画面, 131
- 証明書のパスワード, 140, 147
- 製品ライセンス画面, 48

た

通知とレポート

- トークン変数, 90

- 登録依頼のメール, 90

登録設定

- 登録キー, 76
- 認証, 76

な

- ネットワークアクセスルール, 36

は

パスワード

- Web 管理コンソール, 47

- フレンドリ名, 139

ポートの設定

基本的なセキュリティモデル

- Active Directory, 116

- SCEP サーバ, 117

- SQL Server, 117

- マネージメントサーバ, 114, 115

- ローカルコミュニケーションサーバ, 114, 115

- クラウドコミュニケーションサーバ

- SCEP サーバ, 109

- SQL Server, 110

- マネージメントサーバ, 108, 109

ローカルコミュニケーションサーバ

Active Directory, 113

SCEP サーバ, 113

SQL Server, 113

コミュニケーションサーバ,

112

マネージメントサーバ, 110, 111

ま

マネージメントサーバ

インストールプログラム, 40

初期設定のポート番号, 80

