Trend Micro Mobile Security™ 9.8

Service Pack 5 Critical Patch 3

管理者ガイド

(フル機能配信モード)

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/solution/000207383

法人向け製品のサポートについて

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

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

商標について

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

P/N: TSEM99446/211119_JP (2022/10)

プライバシーと個人データの収集に関する規定

トレンドマイクロ製品の一部の機能は、お客さまの製品の利用状況や検出にかかわる情報を収集してトレンドマイクロに送信します。この情報は一定の管轄区域内および特定の法令等において個人データとみなされることがあります。トレンドマイクロによるこのデータの収集を停止するには、お客さまが関連機能を無効にする必要があります。

Trend Micro Mobile Security により収集されるデータの種類と各機能によるデータの収集を無効にする手順については、次の Web サイトを参照してください。

https://www.go-tm.jp/data-collection-disclosure

重要

データ収集の無効化やデータの削除により、製品、サービス、または機能の利用に影響が発生する場合があります。Trend Micro Mobile Security における無効化の影響をご確認の上、無効化はお客さまの責任で行っていただくようお願いいたします。

トレンドマイクロは、次の Web サイトに規定されたトレンドマイクロのプライバシーポリシー (Global Privacy Notice) に従って、お客さまのデータを取り扱います。

https://www.trendmicro.com/ja_jp/about/legal/privacy-policy-product.html

目次

はじめに

第 1 章：製品の紹介

第 2 章：Mobile Security の使用開始

第 3 章：モバイルデバイスの管理

第 4 章：ユーザと登録依頼の管理

第 5 章：ポリシーの設定

第 10 章：コンポーネントのアップデート

第 11 章：テクニカルサポート

索引

はじめに

Trend Micro Mobile Security バージョン 9.8 SP5 Critical Patch 3 管理者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、Mobile Security のすべての設定オプションの詳細情報を提供します。ソフトウェアをアップデートして最新のセキュリティリスクから保護する方法、ポリシーを設定および使用してセキュリティ目標達成をサポートする方法、検索の設定、モバイルデバイスの同期ポリシー、およびログとレポートの使用方法に関するトピックが含まれます。

ここでは、次のトピックについて説明します。

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
- 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

ヒント

最新のドキュメントファイルは、トレンドマイクロのダウンロードサイト (https://www.trendmicro.co.jp/download/) 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、次の規則を使用しています。

表 1. ドキュメントの表記規則

規則	説明
太字	メニューおよびメニューコマンド、コマンドボタン、タブ、オプション
等幅文字	コマンドラインのサンプル、プログラムコード、Web URL、ファイル名、プログラム出力
[ナビゲーション] > [パス]	特定の画面に到達するためのナビゲーションパス たとえば、[ファイル] > [保存] は、画面上で [ファイル]、[保存] の順にクリックすることを意味します。
注意	設定上の注意
ヒント	推奨

規則	説明
 重要	必要な設定または初期設定や製品の制限に関する情報
 警告!	重要な処理と設定オプション

第 1 章

製品の紹介

Trend Micro Mobile Security 9.8 SP5 Critical Patch 3 は、モバイルデバイス向けの総合的なセキュリティソリューションです。この章では、Mobile Security コンポーネント、機能、およびモバイルデバイスを保護する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。

モバイルの脅威について

プラットフォームが標準化され、接続性が拡大するにつれ、モバイルデバイスはより多くの脅威にさらされます。モバイルプラットフォーム上で実行される不正プログラムの数は増加しており、より多くの不要なメッセージが SMS を介して送信されます。また、WAP や WAP プッシュなどの新しいコンテンツのソースが、不要なプログラムやコンテンツを配信するために使用されています。

また、モバイルデバイスの盗難も、個人または機密データの漏えいにつながります。

Trend Micro Mobile Security について

Trend Micro Mobile Security は、モバイルデバイス向けの総合的なセキュリティソリューションです。トレンドマイクロの不正プログラム対策技術を搭載し、モバイルデバイスを最新の脅威から効果的に保護します。

組み込みのフィルタ機能により、Mobile Security でモバイルデバイスに対する不要なネットワーク通信をブロックできます。不要なネットワーク通信には、SMS メッセージ、WAP プッシュメール、3G 接続経由で受信するデータなどがあります。

このバージョンの Mobile Security は、ウイルスバスター Corp.™がなくても使用でき、スタンドアロンのアプリとして Windows コンピュータに単体でインストールできます。

警告!

トレンドマイクロは、Mobile Security とファイルシステム暗号化ソフトウェアとの互換性を保証していません。不正プログラム検索や SMS 管理など、同様の機能を提供するソフトウェア製品にも、Mobile Security との互換性がない場合があります。

Trend Micro Mobile Security の機械学習型検索について

トレンドマイクロの機械学習型検索は、高度な機械学習技術を使用して脅威情報を関連付け、デジタル DNA フィンガープリントや API マッピングなどの

ファイル機能を使用した詳細なファイル分析により未知のセキュリティリスクを検出します。機械学習型検索は、特定されていない未知の脅威やゼロデイ攻撃から環境を保護するための強力なツールです。

未知のファイルや認知度の低いファイルを検出すると、Mobile Security は、次世代のモバイルエンジンでファイルを検索してファイル特性を抽出し、Trend Micro Smart Protection Network でホストされている機械学習型検索エンジンにレポートを送信します。機械学習型検索では、不正プログラムモデリングにより、サンプルを不正プログラムモデルと比較し、可能性スコアを割り当て、不正なファイルであるかどうかを判別します。Mobile Security では、該当するファイルがインストールされるのを防止し、アンインストールまたは削除するようにユーザに通知することができます。

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)

詳細については、「インストールおよびクライアント配信ガイド」を参照してください。

Mobile Security システムのコンポーネント

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 システムのコンポーネント

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	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。	必須
コミュニケーションサーバ	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。 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。 • 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。 25 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。	必須
SMS Sender この機能は現在日本では提供されていません。	SMS Sender を使用すると、ユーザに SMS を送信できます。	オプション

コンポーネント	説明	必須/オプション
Exchange Connector	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。 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。 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。	オプション
Mobile Device エージェント (MDA)	Mobile Device エージェントは、管理対象の Android および iOS デバイスに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。	必須
Microsoft SQL Server	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。	必須
Active Directory	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。	オプション
CA (証明機関)	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。	オプション

コンポーネント	説明	必須/オプション
SCEP	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。 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。 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。	オプション
APNs 証明書	(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)。 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。 注意 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。 https://success.trendmicro.com/jp/solution/1096556	iOS デバイスを管理する場合は必須
SSL 証明書	(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)。 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。	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

Trend Micro Mobile Security 9.8 SP5 Critical Patch 3 の新機能

注意

本リリースより、製品バージョン番号の記載が変更され、英語版のバージョンと同じ表記となります。

Trend Micro Mobile Security 9.8 SP5 Critical Patch 3 で追加または強化された新機能は次のとおりです。

機能	説明
Firebase Cloud Messaging を使用した通知のサポート	本バージョンの Mobile Security では、Google の Firebase Cloud Messaging (FCM) ソリューションを使用して、Android デバイスに通知を送信します。 FCM ソリューションにより、Mobile Security サーバと Android エージェント間の通信のパフォーマンスと安定性が向上します。
iOS デバイスの位置情報の特定に関する問題のバグ修正	本バージョンの Mobile Security では、iOS デバイスの位置情報を特定できない場合があるという問題が修正されます。

Trend Micro Mobile Security 9.8 SP5 Critical Patch 2 の新機能

注意

本リリースより、製品バージョン番号の記載が変更され、英語版のバージョンと同じ表記となります。

Trend Micro Mobile Security 9.8 SP5 Critical Patch 2 で追加または強化された新機能は次のとおりです。

機能	説明
セキュリティの脆弱性の修正	本バージョンの Mobile Security では、マネージメントサーバーで認証されていないファイルが削除される可能性がある問題が解決されます。

Trend Micro Mobile Security 9.8 SP5 Critical Patch 1 (日本語版では 9.8 Patch2 CP3128) の新機能

Trend Micro Mobile Security 9.8 SP5 Critical Patch 1 (日本語版では 9.8 Patch2 CP3128) で追加または強化された新機能は次のとおりです。

機能	説明
レガシーバイナリプロトコルの置換	本バージョンの Mobile Security では、2021 年 3 月 31 日に Apple がサポートを停止するレガシーバイナリプロトコルが、HTTP/2 ベースの Apple Push Notification サービス (APNs) に置き換えられています。
バグ修正	本バージョンの Mobile Security では、Android での既知のバグが一部修正されています。

Trend Micro Mobile Security 9.8 SP5 (日本語版では 9.8 Patch2 CP3111) の新機能

機能	説明
Apex Central からの MARS パターンファイルのアップデート	本バージョンの Mobile Security では、Trend Micro Apex Central からの MARS パターンファイルのアップデートがサポートされています。
PHP バージョンのアップグレード	本バージョンの Mobile Security では、組み込みの PHP バージョンが 7.0.33 から 7.4.12 にアップグレードされています。
Microsoft Exchange Server の最新バージョンのサポート	本バージョンの Mobile Security では、Microsoft Exchange Server 2016/2019 をサポートします。
サポートするエージェントのバージョンの追加	本バージョンの Mobile Security では、Android 11.0 および iPadOS 14 のサポートを追加しています。

Trend Micro Mobile Security 9.8 SP4 (日本語版では 9.8 Patch2 CP3070) の新機能

注意

Trend Micro Mobile Security 証明書をアップグレードし、セキュリティを強化しています。証明書のアップグレードによって、一部のサービスに影響が生じる場合があります。証明書のアップグレードによる影響を軽減するため、Trend Micro Mobile Security サーバを 9.8 Patch2 CP3070 にアップグレードすることを強くお勧めします。

機能	説明
Apex Central との統合	本バージョンの Mobile Security では、Trend Micro Apex Central のポリシーページがアップデートされています。
PHP バージョンのアップグレード	本バージョンの Mobile Security では、Trend Micro Mobile Security 組み込みの PHP バージョンが 5.4.38 から 7.0.33 にアップグレードされています。
iOS の最新バージョンのサポート	本バージョンの Mobile Security では、iOS 14 のサポートを追加しています。

Trend Micro Mobile Security 9.8 SP3 (日本語版では 9.8 Patch2 CP3070) の新機能

機能	説明
MARS パターンファイルツールのアップデート	本バージョンの Mobile Security では、MARS パターンファイルのバージョンがアップグレードに失敗した場合、MARS パターンファイルツールをアップデートしてログを取得します。

Trend Micro Mobile Security 9.8 SP2 Patch 1 (日本語版では 9.8 Patch2 CP2334) の新機能

機能	説明
Android および iOS の互換性の問題に対する修正	本バージョンの Mobile Security では、iOS 13 および Android 10 の互換性の問題が修正されています。
その他のバグ修正	本バージョンの Mobile Security では、サーバおよびモバイルデバイスの管理者に関するその他のバグと脆弱性の問題が修正されています。

Trend Micro Mobile Security 9.8 SP2 (日本語版では 9.8 Patch2 (B2300)) の新機能

機能	説明
新しいバージョンの Microsoft SQL Server のインストール	本バージョンの Mobile Security では、インストール時に Microsoft SQL Server 2017 がインストールされます。
JRE から OpenJDK への変更	本バージョンの Mobile Security では、JRE に代わり OpenJDK が使用されており、モバイルデバイスに.apk ファイルがインストールされます。

Trend Micro Mobile Security 9.8 SP1 (日本語版では 9.8 Patch2 (B2300)) の新機能

機能	説明
ローカルコミュニケーションサーバの高可用性のサポート	ネットワーク上のすべてのローカルコミュニケーションサーバで高可用性を確保するように、Windows サーバを設定できます。

Trend Micro Mobile Security 9.8 の新機能

機能	説明
Trend Micro Control Manager (以下、Control Manager) 7.0 との統合	Control Manager 7.0 との完全な統合がサポートされます。
セキュリティ対策と検出の強化:	モバイルデバイスに対する次の検索がサポートされます。 • 不正な SSL 証明書 • 不正な iOS プロファイル (iOS のみ) • ネットワークトラフィックの復号 • 安全でないアクセスポイント (Wi-Fi) • 開発者オプションと USB デバッグ (Android のみ) • 改ざんアプリ
新しいウィジェット、管理者への通知、レポート	新しいウィジェット、管理者への通知、レポートの導入: 不正な SSL 証明書、不正な iOS プロファイル、ネットワークトラフィックの復号、安全でないアクセスポイント (Wi-Fi)、開発者オプション、USB デバッグ、改ざんアプリ、root 化/Jailbreak されたモバイルデバイスに関する情報が提供されるようになりました。

機能	説明
承認済みアプリリスト	承認済みリストが導入され、不正プログラム、脆弱性、プライバシーリスク、改ざんが検出されたアプリのうち、安全性を確認できたアプリを管理者が承認済みリストに追加してモバイルデバイスへのインストールを許可できるようになりました。

Trend Micro Mobile Security 9.7 Patch 3 (日本語版では 9.8) の新機能

機能	説明
QR コードによるエージェントの迅速な配信 (セキュリティ対策限定配信モードのみ)	エージェント配信設定画面に表示される QR コードを使用して、登録情報をすばやく簡単にエージェントを配信できます。 この機能は、セキュリティ対策限定配信モードで、AirWatch または MobileIron と統合する場合にのみ使用できます。
機械学習型検索のサポート	機械学習型検索のサポートにより、詳細なファイル分析を実行して、最新の既知のセキュリティリスクを検出できます。

Trend Micro Mobile Security 9.7 Patch 2 (日本語版では 9.8) の新機能

機能	説明
MobileIron モバイルデバイス管理ソリューションとの統合	Android デバイスと iOS デバイスにセキュリティ対策を提供し、次の MobileIron モバイルデバイス管理ソリューションと統合します。 • MobileIron Core (ホスト) • MobileIron Core (オンプレミス)

機能	説明
オンラインヘルプの統合	すべての UI 画面から、トレンドマイクロオンラインヘルプセンターのヘルプファイルを参照できるようになりました。
iOS アクティベーションロックのサポート (セキュリティ対策限定配信モードのみ)	アクティベーションロックは、iOS 7 以降を搭載したモバイルデバイスに組み込まれている「iPhone を探す」の機能です。第三者がデバイス上で「iPhone を探す」をオフにしたり、デバイスのデータを消去したり、デバイスを再アクティベートして使おうとするときにユーザの Apple ID とパスワードが必要になるため、紛失したモバイルデバイスや盗まれたモバイルデバイスが再アクティベートされるのを防ぎます。

Trend Micro Mobile Security 9.7 の新機能

機能	説明
複数の配信モード	Trend Micro Mobile Security の配信モードを選択できます。 • フル機能配信モード: Trend Micro Mobile Security のすべての機能が含まれます。 • セキュリティ対策限定配信モード: Android および iOS のモバイルデバイスにセキュリティ対策を提供し、他社のモバイルデバイス管理 (MDM) ソリューションと統合します。
AirWatch との統合	Android デバイスと iOS デバイスにセキュリティ対策を提供し、AirWatch モバイルデバイス管理ソリューションと統合します。
[ダッシュボード] 画面のサイバーセキュリティニュースウィジェット (※日本ではこの機能は提供されていません)	[ダッシュボード] 画面に、トレンドマイクロが公開するモバイルデバイス向けサイバーセキュリティニュースを 表示するウィジェットが追加されました。
Android デバイスでのサーバ証明書の検証	Android デバイスでサーバ証明書を検証できます。

機能	説明
セキュリティ検索および不正アプリ対策用の新しい MARS API	最新の Mobile Application Reputation Service (MARS) API との統合により、脆弱性の検出機能が強化され、またより詳しい説明が表示されるようになりました。
Android と iOS の最新バージョンのサポート	Android 7 と iOS 10 のサポートが追加されました。

Trend Micro Mobile Security 9.6 SP1 (日本語版では 9.7) の新機能

機能	説明
ランサムウェア検出ウィジェット	ランサムウェア検出の統計情報を表示する新しいウィジェットがダッシュボードに追加されました。
Android アプリのバージョン選択	Android デバイスおよび iOS デバイス向けのアプリの配信で、フル機能またはセキュリティ対策限定を選択できるようになりました。
Android デバイスでのアプリの自動アクティベーション	本バージョンの Mobile Security では、Android デバイスでアプリ配信時の自動アクティベーションが可能です。
Exchange Server のデータクリーンナップ (セキュリティ対策限定配信モードのみ)	別の Exchange Server に移行する前にデータクリーンアップを実行できます。Exchange Connector および Exchange ActiveSync の既存のデバイスデータが Mobile Security から削除されます。
複数の Active Directory ユーザに対するグループ設定	複数の Active Directory ユーザにグループ設定を適用できます。
デバイスプラットフォーム別のレポートの生成	レポート生成機能が強化され、デバイスプラットフォームを選択してレポートを生成できるようになりました。
デバイス情報のアップデート	管理対象のモバイルデバイスのデバイス情報を次回の予約アップデートを待たずにアップデートできます。

Trend Micro Mobile Security 9.6 の新機能

バージョン 9.6 以降に追加または強化された新機能は次のとおりです。

機能	説明
ユーザ管理	ユーザと登録依頼を別々に管理できるようになりました。
手動レポート	必要に応じてレポートを生成できるようになりました。
予約検索	不正プログラム検索やセキュリティ検索を、毎日、毎週、毎月など、指定のスケジュールに基づいて実行できるようになりました。
Android のセキュリティ検索	セキュリティ強化のために、Mobile Security ではアプリ権限チェックに加え、脆弱性検索および改ざんアプリ検索がサポートされるようになりました。
新しいウィジェット	Android セキュリティ検索および iOS 不正プログラム検索に関する情報を表示するウィジェットが新たに 5 つ追加されました。
iOS アプリの新しいバージョン	新しいバージョンの iOS アプリを配信できるようになりました。このバージョンは、不正アプリ対策のみをサポートしており、サードパーティのモバイルデバイス管理 (MDM) アプリと連携します。

Mobile Device エージェントの主要機能

機能名	説明		Android	iOS
セキュリティ対策	Mobile Security は、トレンドマイクロの不正プログラム対策テクノロジを統合し、効果的に脅威を検出して、攻撃者がモバイルデバイスの脆弱性を利用することを防止します。Mobile Security は、モバイルの脅威を検索するよう特別に設計されています。	不正プログラム検索	●	●
		アプリ権限チェック	●	
		脆弱性検索	●	
		改ざんアプリ検索	●	●
		USB デバッグ検索	●	
		開発者オプション検索	●	
		root 化されたモバイルデバイス検索	●	
		Jailbreak されたモバイルデバイス検索		●
		不正な iOS プロファイル検索		●
		ネットワークトラフィックの復号検索	●	●
		不正な SSL 証明書検索	●	●
		安全でないアクセスポイント (Wi-Fi) 検索	●	

機能名	説明	ANDROID	IOS
Web 脅威対策	モバイルデバイスの技術が向上するにつれて、モバイルの脅威もより高度になっています。Trend Micro Mobile Security の Web レピュテーション機能は、安全ではない Web サイトからお使いのモバイルデバイスを保護します。必要に応じて、Web レピュテーションの設定レベルを変更できます。また、Mobile Security は Web レピュテーションでブロックされた Web サイトのログを記録します。	●	
認証情報	Mobile Device エージェントをインストールしたら、モバイルデバイスユーザは認証情報を入力して、モバイルデバイスを Mobile Security マネージメントサーバに登録する必要があります。	●	●
定期的なアップデート	最新の脅威に対応するために、Mobile Security を手動でアップデートするか、または自動でアップデートするように設定できます。コストを削減するため、「ローミング」中のモバイルデバイスに異なるアップデート頻度を設定することもできます。アップデートには、コンポーネントのアップデートと、Mobile Security プログラムパッチのアップデートが含まれます。	●	

機能名	説明		Android	iOS
Mobile Device エージェントログ	マネージメントサーバで使用できる Mobile Device エージェントのログです。	アプリ検索ログ	●	●
		ポリシー違反ログ	●	●
		デバイス脆弱性ログ	●	●
		ネットワーク保護ログ	●	●
		Web 脅威検出ログ	●	
	モバイルデバイスに保存される Mobile Device エージェントのユーザごとのログです。	不正プログラム検索の履歴	●	
		脆弱性検索ログ	●	
		改ざんアプリ検索ログ	●	
		アプリ権限チェックの履歴	●	
		(Android のログ): Web ブロック履歴	●	
		着信ブロックの履歴	●	
		SMS ブロックの履歴	●	
		アップデート履歴	●	

サポートされるモバイルデバイスの OS の機能

次の表は、Trend Micro Mobile Security でサポートされている機能をプラットフォーム別に示したものです。

表 1-3. Trend Micro Mobile Security9.8 SP5 Critical Patch 3 の機能

カテゴリ	機能	設定		
共通		Mobile Security エージェントのアンインストールを禁止する		●
		Mobile Security クライアントの設定を許可する		●
プロビジョニング	Wi-Fi	Wi-Fi の標準設定	●	●
		旧バージョンの Hotspot の設定	●	
		Hotspot 2.0 の設定	●	
	Exchange ActiveSync	Exchange ActiveSync の設定	●	
	VPN	VPN の設定	●	
	グローバル HTTP プロキシ	グローバル HTTP プロキシの設定	●	
	シングルサインオン	シングルサインオンの設定	●	
	証明書	証明書の設定	●	
	モバイルデータ通信ネットワーク	モバイルデータ通信ネットワークの設定	●	
	AirPlay/AirPrint	AirPlay/AirPrint の設定	●	
	テーマ (監視モードの場合のみ)	壁紙設定	●	
		フォント設定	●	
	管理対象ドメイン	マークされていないメールドメイン	●	
		管理対象 Safari Web ドメイン	●	
デバイスのセキュリティ	セキュリティ設定	リアルタイム検索		●
		パターンファイルのアップデート後に検索する		●

カテゴリ	機能	設定		
		手動検索	●	●
データ保護	Web 脅威対策	サーバ側の制御		●
		ブロックリストの使用		●
		承認済みリストの使用		●
		特定の Web サイトのみ許可		●
		限られた成人向けコンテンツのみ許可		●
データ保護	パスワード設定	ログイン時のパスワードの使用	●	●
		簡単なパスワードの許可	●	●
		英数字のパスワードの要求	●	●
		最小のパスワードの長さ	●	●
		パスワードの失効	●	●
		パスワードの履歴	●	●
		自動ロック	●	●
		パスワード失敗時の処理	●	●
	機能ロック	カメラ	●	●
		FaceTime (監視モードの場合のみ)	●	
		画面キャプチャ	●	
		アプリのインストール	●	
		ローミング中の同期	●	
		音声ダイヤル	●	

カテゴリ	機能	設定		
		アプリケーションの購入	●	
		マルチプレイヤーゲーム	●	
		Game Center の友人の追加	●	
		Game Center (監視モードの場合のみ)	●	
		暗号化バックアップの実行	●	
		不適切な音楽、ポッドキャスト、iTunes U	●	
		デバイスのロック中の Passbook	●	
		Bluetooth および Bluetooth 検出		●
		WLAN/Wi-Fi		●
		3G データネットワーク		●
		開発者モード		●
		スピーカー/スピーカーフォン/マイク		
		メモリカードの制限 (監視モードの場合のみ)		●
		Siri (監視モードの場合のみ)	●	
		デバイスのロック中の Siri (監視モードの場合のみ)	●	
		不適切な言葉に対するフィルタを有効にする (監視モードの場合のみ)	●	
		iCloud サービスへのアクセスを有効にする (監視モードの場合のみ)	●	

カテゴリ	機能	設定		
		クラウドバックアップ (監視モードの場合のみ)	●	
		クラウドでのドキュメント同期 (監視モードの場合のみ)	●	
		フォトストリーム (監視モードの場合のみ)	●	
		共有フォトストリーム (監視モードの場合のみ)	●	
		診断データ (監視モードの場合のみ)	●	
		信頼されていないトランスポート層セキュリティ (TLS) の受け入れ	●	
		iTunes Store パスワードの要求	●	
		その他のアプリ内の管理対象アプリからドキュメントを開く	●	
		管理対象アプリ内のその他のアプリからドキュメントを開く	●	
		iTunes	●	
		Safari Web ブラウザ	●	
		オートフィル	●	
		JavaScript	●	
		ポップアップ	●	
		不正行為に関する警告の表示	●	
		Cookie の許可	●	
		アプリの削除 (監視モードの場合のみ)	●	

カテゴリ	機能	設定		
		ブックストア (監視モードの場合のみ)	●	
		性描写を含む書籍 (監視モードの場合のみ)	●	
		設定プロファイルのインストール (監視モードの場合のみ)	●	
		iMessage (監視モードの場合のみ)	●	
		評価区分	●	
		ムービー	●	
		テレビ番組	●	
		アプリ	●	
		アカウントの変更 (監視モードの場合のみ)	●	
		AirDrop (監視モードの場合のみ)	●	
		アプリでのモバイルデータ通信の変更 (監視モードの場合のみ)	●	
		アシスタント (Siri) ユーザが生成したコンテンツ (監視モードの場合のみ)	●	
		クラウドキーチェーンの同期	●	
		「友達を探す」の変更 (監視モードの場合のみ)	●	
		デバイスのロック解除のための指紋認証	●	
		ホストペアリング (監視モードの場合のみ)	●	

カテゴリ	機能	設定		
		ロック画面のコントロールセンター	●	
		ロック画面の通知の表示	●	
		ロック画面の今日の表示	●	
		Over the Air Public Key Infrastructure (OTAPKI) のアップデート	●	
		追跡型広告の制限の適用	●	
		AirPlay の発信でのペアリングパスワードの要求	●	
		管理対象アプリが iCloud にデータを保存することを許可	●	
		エンタープライズブックのバックアップを許可	●	
		制限の構成を許可	●	
		[すべてのコンテンツと設定の消去] を許可	●	
		Handoff を許可	●	
		Spotlight でインターネット検索結果を許可	●	
		エンタープライズブックのメモとハイライトの同期を許可	●	
		管理対象の書類を AirDrop で共有することを許可する	●	
		iCloud フォトライブラリを許可する	●	
		デバイスからのアプリのインストールを許可する	●	

カテゴリ	機能	設定		
		キーボードショートカットを許可する	●	
		Apple Watch のペアリングを許可する	●	
		パスコードの変更を許可する	●	
		デバイス名の変更を許可する	●	
		壁紙の変更を許可する	●	
		アプリの自動ダウンロードを許可する	●	
		エンタープライズアプリの信頼を許可する	●	
		アクセスポイント		●
	コンプライアンス設定	root 化/Jailbreak	●	●
		暗号化なし	●	●
		OS バージョンチェック	●	●
アプリケーションの管理	アプリの監視および制御	必須アプリ	●	●
		許可するアプリ	●	●
		アプリのロック (監視モードの場合のみ)	●	
	Volume Purchasing Program	Volume Purchasing Program	●	
リモートコントロール	登録		●	●
	アップデート		●	●
	盗難/紛失時の対策	リモート検索	●	●

カテゴリ	機能	設定		
		リモートロック	●	●
		リモート消去	●	●
		パスワードのリセット	●	●
		メッセージの送信	●	●
	Samsung KNOX ワークスペース	コンテナの作成		●
		コンテナの削除		●
		コンテナのロック		●
		コンテナのロック解除		●
		コンテナパスワードのリセット		●
Samsung KNOX ワークスペースポリシー	コンテナのアカウント設定	ブロックリスト		●
		承認済みリスト		●
	制約の設定	ユーザによるカメラの使用を許可する		●
		アプリのリストによる共有の表示を許可		●
	ブラウザの設定	オートフィルを有効にする設定		●
		Cookie を有効にする設定		●
		ポップアップを有効にする設定		●
		不正行為に関する警告を有効にする設定		●
		JavaScript を有効にする設定		●
		Web プロキシを有効にする		●

カテゴリ	機能	設定		
Samsung KNOX ワークスペースポリシー	コンテナのパスワード設定	パスワードの可視化を有効にする		●
		パスワードの最小変更文字数		●
		最小のパスワードの長さ		●
		自動ロックするまでの待ち時間		●
		パスコードの最大入力回数		●
		パスワードの履歴		●
		パスワードの最長有効期間		●
		パスワードに必要な特殊文字の最小数		●
		パスワードの複雑さ		●
	アプリの設定	インストールの承認済みリスト		●
		インストールのブロックリスト		●
		必須アプリ		●
		無効化されたアプリ		●
Device Enrollment Program			●	
デバイス情報	ハードウェア、OS	シリアル番号	●	●
		MEID	●	●
		IMEI	●	●
		仕様		●
		ブートローダバージョン		●
	ネットワーク	Bluetooth MAC	●	●

カテゴリ	機能	設定		
		Wi-Fi MAC	●	●

第 2 章

Mobile Security の使用開始

この章では、Mobile Security の使用を開始するために役立つ情報と基本的な使用手順を示します。先に進む前に、マネージメントサーバ、コミュニケーションサーバ、および Mobile Device エージェントがモバイルデバイスにインストールされていることを確認してください。

この章には、次のセクションが含まれています。

Web 管理コンソール

Mobile Security の Web 管理コンソールから、設定画面にアクセスできます。

Web 管理コンソールは、企業ネットワークを介して Mobile Security を管理および監視するための中心点です。コンソールには、初期設定の設定および値が設定済みですが、これらの値はユーザのセキュリティ要件と仕様に応じて変更できます。

Web 管理コンソールでは、次の作業を実行できます。

- モバイルデバイスにインストールされた Mobile Device エージェントの管理
- Mobile Device エージェントのセキュリティポリシーの設定
- 単一または複数のモバイルデバイスでの検索の設定
- 設定と管理を容易にするための、各グループにおけるデバイスの 管理
- 登録情報およびアップデート情報の表示

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オンします。

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

   注意

   <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。

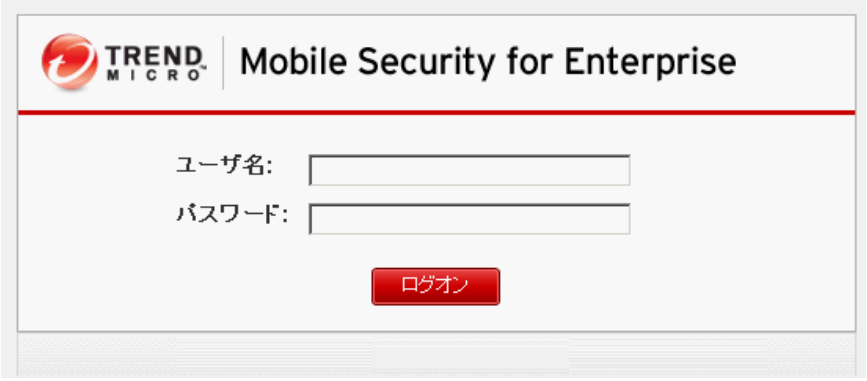

図 2-1. Web 管理コンソールのログイン画面

2. 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、52 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

1. 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。

製品ライセンス

体験版ライセンスの有効期限が切れると、すべてのプログラムの機能が無効になります。製品版ライセンスでは、サポート契約の有効期限が切れた後もすべての機能を継続して使用することができます。ただし、Mobile Device エージェントではサーバからアップデートを取得できなくなるため、不正プログラム対策コンポーネントが最新のセキュリティリスクにさらされることになります。

サポート契約の有効期限が切れた後に継続してお使いいただくには、新しいアクティベーションコードで Mobile Security マネージメントサーバを登録する必要があります。詳細については、最寄りのトレンドマイクロ販売代理店までお問い合わせください。

アップデートのダウンロードおよびリモート管理を可能にするには、Mobile Device エージェントを Mobile Security マネージメントサーバに登録する必要があります。モバイルデバイスで Mobile Device エージェントを手動で登録する手順については、「インストールおよびクライアント配信ガイド」を参照してください。

マネージメントサーバのライセンスアップグレード手順を表示するには、Mobile Security の [製品ライセンス] 画面で、[ライセンスのアップグレード方法を確認] のリンクをクリックしてください。

ダッシュボード情報

マネージメントサーバにアクセスすると、[ダッシュボード] 画面が表示されます。この画面には、モバイルデバイスの登録ステータスおよびコンポーネントの詳細が表示されます。

[ダッシュボード] には、次の 5 つのタブがあります。

- 概要: モバイルデバイスのステータスとセキュリティステータス、モバイルデバイスで使用される OS のバージョン情報を示します。
- セキュリティ :Android デバイス脆弱性検索情報、iOS デバイス脆弱性検索情報、Android ネットワーク保護情報、iOS ネットワーク保護情報、Android アプリリスク情報、iOS アプリリスク情報を示します。このカテゴリでは、次のウィジェットおよびステータスを確認できます。
    - Android/iOS 脆弱性情報:
        - root 化: (Android のみ) root 化されたモバイルデバイスの数
        - USB デバッグ: (Android のみ) USB デバッグモードが有効になっているモバイルデバイスの数
        - 開発者オプション: (Android のみ) 開発者モードが有効になっているモバイルデバイスの数

- Jailbreak あり: (iOS のみ) Jailbreak されたモバイルデバイスの数
- 不正な iOS プロファイル: (iOS のみ) 不正な iOS プロファイルがインストールされているモバイルデバイスの数

- Android/iOS ネットワーク保護情報:
  - 安全でないアクセスポイント (Wi-Fi): (Android のみ) パスワードが脆弱である、またはパスワードが設定されていない不審アクセスポイント/安全ではないアクセスポイント (Wi-Fi) に接続しているモバイルデバイスの数
  - ネットワークトラフィックの復号: ネットワークトラフィックの復号が検出されたモバイルデバイスの数
  - 不正な SSL 証明書: 不正な SSL 証明書がインストールされているモバイルデバイスの数
- Android/iOS アプリリスク情報:
  - 不正プログラム: 不正プログラムとして検出されたインストール済みアプリの数
  - 脆弱なアプリ: (Android のみ) 脆弱なアプリとして検出されたインストール済みアプリの数
  - プライバシーリスク: (Android のみ) プライバシー漏えいのあるアプリとして検出されたインストール済みアプリの数
  - 改ざんアプリ: アプリパッケージが改ざんされているインストール済みアプリの数

- ステータス:サーバコンポーネントとポリシーのアップデートステータスおよびモバイルデバイスのステータスを示します。このカテゴリでは、次の操作を実行できます。
  - モバイルデバイスのステータスを表示する。
    - 最新: デバイスが Mobile Security マネージメントサーバに登録されていて、そのコンポーネントおよびポリシーが最新の状態です。

- コンプライアンス違反: モバイルデバイスは Mobile Security マネージメントサーバに登録されていますが、サーバポリシーに違反しています。
- 非同期: デバイスが Mobile Security マネージメントサーバに登録されていますが、コンポーネントまたはポリシーが最新ではありません。
- 未登録: デバイスが Mobile Security マネージメントサーバに登録されていません。

- Mobile Security によって管理されている登録済みまたは未登録のモバイルデバイスの合計数を表示する。

  モバイルデバイスは、コミュニケーションサーバとの接続に失敗した場合、未登録のままになる可能性があります。

- モバイルデバイスのプログラムパッチおよびコンポーネントのアップデートステータスを表示する。
  - 現在のバージョン: Mobile Device エージェントまたは Mobile Security マネージメントサーバ上のコンポーネントの現在のバージョン番号
  - 最新: 最新の Mobile Device エージェントのバージョンまたはコンポーネントを使用しているモバイルデバイスの数
  - 期限切れ: 期限切れのコンポーネントを使用しているモバイルデバイスの数
  - アップデート率: 最新のコンポーネントのバージョンを使用しているモバイルデバイスの割合
  - アップグレード完了: 最新の Mobile Device エージェントのバージョンを使用しているモバイルデバイスの数
  - アップグレード未完了: 最新の Mobile Device エージェントのバージョンを使用するようアップグレードされていないモバイルデバイスの数
  - アップグレード率: 最新の Mobile Device エージェントを使用しているモバイルデバイスの割合

- サーバのアップデートステータスを表示する。
  - サーバ: マネージメントサーバの名前
  - アドレス: マネージメントサーバをホストしているコンピュータのドメイン名または IP アドレス
  - 現在のバージョン: Mobile Security マネージメントサーバモジュールの現在のバージョン番号
  - 前回のアップデート: 前回のアップデート日時
- コンプライアンス: モバイルデバイスのアプリケーション制御、暗号化、および Jailbreak または root 化のステータスを示します。このカテゴリでは、次の操作を実行できます。
  - モバイルデバイスの Jailbreak または root 化のステータスを表示する。
    - Jailbreak 有効、root 化完了: Jailbreak、root 化が完了したモバイルデバイスの数
    - Jailbreak 無効、root 化未完了: Jailbreak、root 化をしていないモバイルデバイスの数
  - モバイルデバイスの暗号化のステータスを表示する。
    - 暗号化完了: 暗号化されているモバイルデバイスの数
    - 暗号化未完了: 暗号化されていないモバイルデバイスの数
  - モバイルデバイスのアプリケーション制御のステータスを表示する。
    - コンプライアンス準拠: Mobile Security のコンプライアンスおよびアプリケーション制御ポリシーに準拠しているモバイルデバイスの数
    - コンプライアンス違反: Mobile Security のコンプライアンスおよびアプリケーション制御ポリシーに準拠していないモバイルデバイスの数
- インベントリ: モバイルデバイスで使用される OS のバージョン情報、電話のキャリアの概要、モバイルデバイスのベンダーの概要、およびモバ

イルデバイスにインストールされている主な 10 個のアプリケーションを示します。

注意

[ダッシュボード] 画面の各ウィジェットで、[すべて] を選択するか、リストからグループ名を選択して、関連デバイスの情報を表示できます。

ダッシュボードをカスタマイズする

Mobile Security では、必要に応じてダッシュボードの情報をカスタマイズできます。

新しいタブを追加する

手順

1. [ダッシュボード] 画面の + ボタンをクリックします。
2. [新規タブ] ポップアップ画面で、次の手順を実行します。
   - タイトル: タブの名前を入力します。
   - レイアウト: タブに表示されるウィジェットのレイアウトを 選択します。
   - 自動調整: タブ上のウィジェットの表示を自動で調整する場合は [オン]、手動で調整する場合は [オフ] を選択します。
3. [保存] をクリックします。

タブを削除する

手順

1. タブをクリックし、タブに表示される × ボタンをクリックします。

2. 確認のポップアップ画面で [OK] をクリックします。

ウィジェットを追加する

手順

1. [ダッシュボード] 画面で、ウィジェットを追加するタブをクリックします。
2. タブの右上にある [ウィジェットの追加] をクリックします。

   [ウィジェットの追加] 画面が表示されます。
3. 左側のメニューからカテゴリを選択するか、または検索フィールドにキーワードを入力して、該当するウィジェットのリストを表示します。
4. 追加するウィジェットを選択し、[追加] をクリックします。

   選択したウィジェットが [ダッシュボード] のタブに表示されます。

ウィジェットを削除する

手順

1. [ダッシュボード] 画面で、ウィジェットを削除するタブをクリックします。
2. 削除するウィジェットの右上にある × をクリックします。

ウィジェットの位置を変更する

手順

1. [ダッシュボード] 画面で、再配置するウィジェットを含むタブをクリックします。

2. ウィジェットのタイトルバーをクリックしたまま 新しい位置にドラッグして、ドロップします。

ウィジェット上の情報を更新する

手順

1. [ダッシュボード] 画面で、情報を更新するウィジェットを含むタブをクリックします。
2. 情報を更新するウィジェットの右上にある をクリックします。

タブの設定を表示または変更する

手順

1. [ダッシュボード] 画面で、設定を表示または変更するタブをクリックします。
2. [タブ設定] をクリックします。
3. 必要に応じて設定を変更し、[保存] をクリックします。

管理設定

AD (Active Directory) を設定する

Trend Micro Mobile Security では、AD (Active Directory) に基づいてユーザ認証を設定できます。また、AD を使用してリストにモバイルデバイスを追加することもできます。設定手順の詳細については、「インストールおよびクライアント配信ガイド」の「初期サーバセットアップ」を参照してください。

ユーザ認証を設定する

Trend Micro Mobile Security では、AD (Active Directory) または登録キーに基づいてユーザ認証を設定できます。設定手順の詳細については、「インストールおよびクライアント配信ガイド」の「初期サーバセットアップ」を参照してください。

データベースを設定する

設定手順の詳細については、「インストールおよびクライアント配信ガイド」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

設定手順の詳細については、「インストールおよびクライアント配信ガイド」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

設定手順の詳細については、「インストールおよびクライアント配信ガイド」の「初期サーバセットアップ」を参照してください。

フル機能からセキュリティ対策限定配信モードに切り替える

Mobile Security の配信モードはいつでも切り替えが可能です。

フル機能からセキュリティ対策限定モードの切り替えについては、次の製品 Q&A を参照してください。

https://success.trendmicro.com/jp/solution/1116941

管理者アカウントを管理する

[管理者アカウント管理] 画面では、マネージメントサーバに対して異なるアクセス権限を持つユーザアカウントを作成できます。

初期設定の管理者アカウントの名前と役割

初期設定の管理者アカウントは「root」です (パスワード:「mobilesecurity」)。root アカウントを削除することはできません。変更のみ可能です。詳細な手順については、65 ページの「管理者アカウントを編集する」を参照してください。

表 2-1. root アカウントのプロパティ

ROOT アカウントのプロパティ		変更
管理者アカウント	アカウント名	不可
	氏名	可
	パスワード	可
	メールアドレス	可
	携帯電話番号	可
管理者の役割	管理者の役割の変更	不可

初期設定の管理者の役割は最上位の管理者です。この役割は、すべての設定にアクセスできます。最上位の管理者この役割を削除することはできません。変更のみ可能です。詳細な手順については、67 ページの「管理者の役割を編集する」を参照してください。

表 2-2. 最上位の管理者の役割のプロパティ

最上位の管理者の役割のプロパティ		変更
役割の説明	管理者の役割	不可
	説明	可
グループ管理の制御	管理対象グループ	不可
Exchange Server ドメインの制御	ドメインの選択	不可

表 2-3. 最上位の管理者とグループ管理者のアクセス権

サーバコンポーネント	アクセス権	最上位の管理者	グループ管理者
管理	アップデート	サポートあり	サポートなし
	管理者アカウント管理	すべてのアカウントを変更可能	自分のアカウント情報のみ変更可能
	デバイス登録設定	サポートあり	サポートなし
	証明書の管理	サポートあり	サポートあり
	コマンドキュー管理	すべてのコマンドを変更可能	関連グループのコマンドのみ表示可能
	データベースの設定	サポートあり	サポートなし
	コミュニケーションサーバの設定	サポートあり	サポートなし
	Active Directory の設定	サポートあり	サポートなし
	マネージメントサーバの設定	サポートあり	サポートなし
	配信設定	サポートあり	サポートなし
	Exchange Server との統合	サポートあり	サポートなし
	設定および検証	サポートあり	サポートなし
	製品ライセンス	サポートあり	サポートなし
通知/レポート	ログクエリ	すべてのグループ	管理対象グループのみ
	ログの削除設定	すべてのグループ	管理対象グループのみ
	管理者への通知/レポート	サポートあり	サポートなし
	ユーザへの通知	サポートあり	サポートなし
	設定	サポートあり	サポートなし

サーバコンポーネント	アクセス権	最上位の管理者	グループ管理者
アプリ	エンタープライズアプリストア	サポートあり	サポートなし
	インストール済みアプリ	サポートあり	管理対象グループでのみサポート
ポリシー	ポリシーの作成	サポートあり	管理対象グループでのみサポート
	ポリシーの表示	サポートあり	管理対象グループでのみサポート
	ポリシーのコピー	サポートあり	管理対象グループでのみサポート
	ポリシーの削除	サポートあり	管理対象グループでのみサポート
デバイス	デバイスの表示	サポートあり	管理対象グループでのみサポート
	グループの追加	サポートあり	サポートあり
	Exchange ActiveSync デバイス	サポートあり	管理対象グループでのみサポート
ユーザ	ユーザに登録依頼	サポートあり	管理対象グループでのみサポート

管理者アカウントを追加する

手順

1. Mobile Security の Web 管理コンソールで、[管理] > [管理者アカウント管理] の順に選択します。
2. [管理者アカウント] タブで、[作成] をクリックして新しいアカウントを追加します。

   [管理者アカウントの作成] 画面が表示されます。

3. [アカウントの詳細] で、次のいずれかを実行します。

   - [Trend Micro Mobile Security ユーザ] を選択し、次に示すユーザアカウントの詳細を指定します。
     - アカウント名: マネージメントサーバへのログオンに使用する名前。
     - 氏名: ユーザの氏名。
     - パスワード (および [パスワードの確認])。
     - メールアドレス: ユーザのメールアドレス。
     - 携帯電話番号: ユーザの携帯電話番号。
   - [Active Directory ユーザ] を選択し、次のいずれかを実行します。
     a. 検索フィールドにユーザ名を入力し、[検索] をクリックします。
     b. 左側のリストからユーザ名を選択し、[>] をクリックして、右側の [選択したユーザ] リストにユーザを移動します。

   注意

   右側の [選択したユーザ] リストからユーザを削除するには、ユーザ名を選択し、[<] をクリックします。

   <Ctrl> キーまたは <Shift> キーを押しながらユーザ名をクリックして、複数のユーザを同時に選択することもできます。

4. [管理者の役割] で、[管理者の役割の選択:] リストから役割を選択します。

   管理者の役割の作成手順については、66 ページの「管理者の役割を作成する」を参照してください。

5. [保存] をクリックします。

管理者アカウントを編集する

手順

1. Mobile Security の Web 管理コンソールで、[管理] > [管理者アカウント管理] の順に選択します。
2. [管理者アカウント] タブで、[作成] をクリックして新しいアカウントを追加します。

   [管理者アカウントの編集] 画面が表示されます。
3. 必要に応じて、管理者アカウントの詳細と役割を変更します。
   - アカウントの詳細
     - アカウント名: マネージメントサーバへのログオンに使用する名前。
     - 氏名: ユーザの氏名。
     - メールアドレス: ユーザのメールアドレス。
     - 携帯電話番号: ユーザの携帯電話番号。
     - パスワード: [パスワードのリセット] をクリックしてユーザアカウントのパスワードを変更し、[新しいパスワード] および [パスワードの確認] に新しいパスワードを入力して、[保存] をクリックします。
   - 管理者の役割
     - 管理者の役割の選択: リストから管理者の役割を選択します。

       管理者の役割を作成する手順については、66 ページの「管理者の役割を作成する」を参照してください。
4. [保存] をクリックします。

管理者アカウントを削除する

手順

1. Mobile Security の Web 管理コンソールで、[管理] > [管理者アカウント管理] の順に選択します。
2. [管理者アカウント] タブで、削除する管理者アカウントを選択し、[削除] をクリックします。

   確認メッセージが表示されます。

管理者の役割を作成する

手順

1. Mobile Security の Web 管理コンソールで、[管理] > [管理者アカウント管理] の順に選択します。
2. [管理者の役割] タブで、[作成] をクリックします。

   [管理者の役割の作成] 画面が表示されます。
3. [役割の詳細] で、次の情報を指定します。
   - 管理者の役割
   - 説明
4. [グループ管理の制御] で、この管理者の役割が管理できるモバイルデバイスグループを選択します。
5. [保存] をクリックします。

管理者の役割を編集する

手順

1. Mobile Security の Web 管理コンソールで、[管理] > [管理者アカウント管理] の順に選択します。
2. [管理者の役割] タブで、[作成] をクリックします。

   [管理者の役割の作成] 画面が表示されます。
3. 必要に応じて役割の詳細を変更し、[保存] をクリックします。

管理者の役割を削除する

手順

1. Mobile Security の Web 管理コンソールで、[管理] > [管理者アカウント管理] の順に選択します。
2.
3. [管理者の役割] タブで、削除す管理者の役割を選択し、[削除] をクリックします。

   確認メッセージが表示されます。

管理者のパスワードを変更する

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、65 ページの「管理者アカウントを編集する」を参照してください。

コマンドキュー管理

Mobile Security では、Web コンソールから実行したすべてのコマンドの履歴が保持されます。これらのコマンドは、必要に応じてキャンセルしたり、再

送信したりできます。また、実行済みのコマンドや、リストに表示しておく必要がないコマンドを削除することもできます。

[コマンドキュー管理] 画面にアクセスするには、[管理] > [コマンドキュー管理] の順に選択します。

次の表に、[コマンドキュー管理] 画面に表示されるすべてのコマンドのステータスを示します。

コマンドのステータス	説明
送信待ち	Mobile Security マネージメントサーバがコマンドをモバイルデバイスに送信しています。 このステータスの間は、コマンドをキャンセルできます。
受信確認待ち	Mobile Security マネージメントサーバがコマンドをモバイルデバイスに送信し、モバイルデバイスからの受信確認を待機しています。
失敗	モバイルデバイスでコマンドを実行できません。
成功	モバイルデバイスでコマンドが正常に実行されました。
キャンセル済み	モバイルデバイスで実行される前に、コマンドがキャンセルされました。

ハードディスク上で容量を過剰に占有しないようにコマンドのサイズを維持するには、手動でコマンドを削除するか、または Mobile Security の Web 管理コンソールの [コマンドキュー管理] 画面で、スケジュールに基づいて自動的にコマンドを削除するように設定します。

古いコマンドの削除スケジュールを設定する

手順

1. [管理] > [コマンドキュー管理] の順にクリックします。

   [コマンドキュー管理] 画面が表示されます。

2. [コマンドキューメンテナンス] タブで [コマンドの予約削除を有効にする] を選択します。

3. 古いコマンドを削除するまでの日数を指定します。
4. コマンドキューを削除する頻度と時刻を指定します。
5. [保存] をクリックします。

古いコマンドを手動で削除する

手順

1. [管理] > [コマンドキュー管理] の順にクリックします。

   [コマンドキュー管理] 画面が表示されます。
2. [コマンドキューメンテナンス] タブで [コマンドの予約削除を有効にする] を選択します。
3. 古いコマンドを削除するまでの日数を指定します。
4. [今すぐ削除] をクリックします。

証明書の管理

`.pfx`、`.p12`、`.cer`、`.crt`、および`.der` 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には、[証明書の管理] 画面を使用します。

証明書をアップロードする

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] > [証明書の管理] をクリックします。
3. [追加] をクリックします。

   [証明書の追加] 画面が表示されます。

4. [参照...] をクリックし、.pfx、.p12、.cer、.crt、.der などの証明書ファイルを選択します。
5. [パスワード] に証明書のパスワードを入力します。
6. [保存] をクリックします。

証明書を削除する

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] > [証明書の管理] をクリックします。
3. 削除する証明書を選択し、[削除] をクリックします。

Exchange Server との統合

Exchange Server との統合を設定する

詳細な設定手順については、「インストールおよびクライアント配信ガイド」の「Exchange Server との統合を設定する」を参照してください。

Exchange Connector を設定する

新しいバージョンが入手可能になった場合に自動的にアップデートするように、Exchange Connector を設定できます。

手順

1. Exchange Connector がインストールされているコンピュータで、Windows のタスクバーのシステムトレイ (システム時計の横) にある [隠れているインジケーターを表示します] ボタンをクリックします。

2. [Exchange Connector] アイコンを右クリックし、[Trend Micro Mobile Security と Exchange Connector] をクリックします。

   [Trend Micro Mobile Security と Exchange Connector] 画面が表示されます。

3. 次の設定を行います。

   - 自動アップグレードを有効にする: このオプションを選択すると、Exchange Connector の新しいバージョンが入手可能になった場合に自動的にアップグレードされます。
   - サーバのアドレス: Mobile Security マネージメントサーバの IP アドレス。
   - HTTPS ポート番号: Web 管理コンソールにログオンするための、Mobile Security マネージメントサーバの HTTPS ポート番号。

新しい Exchange Server に移行する

新しい Exchange サーバに移行するには、次の手順を実行します:

手順

1. Exchange Connector がインストールされているコンピュータで、既存の Exchange Connector サービスを停止します。
2. Mobile Security の Web 管理コンソールにログオンします。
3. [管理] > [Exchange Server との統合] をクリックします。
4. [データクリーンナップ] をクリックします。
5. 新しい Exchange Connector をダウンロードしてコンピュータにインストールします。

   詳細については、「インストールおよびクライアント配信ガイド」を参照してください。

6. Exchange Connector を設定します。

詳細は 70 ページの「Exchange Connector を設定する」を参照してください。

第 3 章

モバイルデバイスの管理

この章では、Mobile Security の使用を開始するために役立つ情報を提供します。基本的なセットアップおよび使用方法を記載します。先に進む前に、マネージメントサーバ、コミュニケーションサーバ、および Mobile Device エージェントがモバイルデバイスにインストールされていることを確認してください。

この章には、次のセクションが含まれています。

[管理対象デバイス] タブ

[モバイルデバイス] 画面の [管理対象デバイス] タブでは、Mobile Device エージェントの設定、編成、または検索に関連するタスクを実行できます。デバイスツリービューアの上にあるツールバーから、以下のタスクを実行できます。

- デバイスツリーの設定 (グループの追加、削除、名前の変更、および Mobile Device エージェントの追加と削除など)
- Mobile Device エージェントに関する情報の設定
- Mobile Device エージェントのステータスの検索と表示
- モバイルデバイスへのメッセージの送信
- Mobile Device エージェントコンポーネントの手動アップデート、リモートデバイスの消去/ロック/検索、およびポリシーのアップデート
- 詳細分析またはバックアップのためのデータエクスポート

Mobile Security のグループ

Mobile Security マネージメントサーバは、次の 2 つのサブグループを含むルートグループ「モバイルデバイス」を自動的に作成します。

- 初期設定: このグループには、他のどのグループにも属さない Mobile Device エージェントが含まれます。Mobile Security デバイスツリーの「初期設定」グループを削除したり、名前を変更したりすることはできません。
- 未認証: Mobile Security マネージメントサーバは、[デバイス登録設定] で [デバイス認証] が有効になっており、モバイルデバイスのリストを認証に使用する場合、このグループを自動的に作成します。モバイルデバイスのリストに含まれていない登録済みのモバイルデバイスは、「未認証」グループに移動されます。また、別のグループも作成され、使用するリストに従ってすべてのモバイルデバイスが再グループ化されます。

注意

- [デバイス登録設定] で [デバイス認証] が有効になっている場合に、認証用として空白のモバイルデバイスリストをアップロードすると、現在登録されているすべてのモバイルデバイスが「未認証」グループに移動されます。
- [デバイス認証] は Android と iOS デバイスのみをサポートします。

手順については、Mobile Security マネージメントサーバの「オンラインヘルプ」を参照してください。

グループの管理

「モバイルデバイス」のルートグループに属するグループは、追加、編集、または削除することができます。ただし、「モバイルデバイス」のルートグループと「初期設定」、「未承認」グループの名前を変更したり、削除したりすることはできません。

グループの追加

手順

1. Mobile Security の Web 管理コンソールにログオンします。
2. メニューバーの [モバイルデバイス] をクリックします。

   [モバイルデバイス] 画面が表示されます。
3. [管理対象デバイス] タブで、「モバイルデバイス」というルートグループをクリックし、[グループの追加] をクリックします。
4. 次の設定を行います。
   - 親グループ: サブグループを作成するグループを選択します。
   - グループ名: グループの名前を入力します。
   - ポリシー: グループに適用するポリシーをリストから選択します。

5. [追加] をクリックします。

グループ名の変更

手順

1. Mobile Security の Web 管理コンソールにログオンします。
2. メニューバーの [モバイルデバイス] をクリックします。

   [モバイルデバイス] 画面が表示されます。
3. [管理対象デバイス] タブで、名前を変更するグループをクリックします。
4. [編集] をクリックします。
5. グループ名を変更し、[名前の変更] をクリックします。

グループの削除

手順

1. Mobile Security の Web 管理コンソールにログオンします。
2. メニューバーの [モバイルデバイス] をクリックします。

   [モバイルデバイス] 画面が表示されます。
3. [管理対象デバイス] タブで、削除するグループをクリックします。
4. [削除] をクリックし、確認画面で [OK] をクリックします。

モバイルデバイスの管理

[モバイルデバイス] 画面では、モバイルデバイス情報の編集、モバイルデバイスの削除、モバイルデバイスグループの 変更を行うことができます。

デバイスを回収する

手順

1. Mobile Security の Web 管理コンソールで、[モバイルデバイス] > [管理対象デバイス] の順に選択します。

   [モバイルデバイス] 画面が表示されます。

2. デバイスツリーで、回収するデバイスを選択します。

   デバイス情報が表示されます。

3. [ユーザの変更] をクリックし、表示されるフィールドでユーザ名を変更します。

4. [保存] をクリックします。

モバイルデバイス情報を編集する

手順

1. Mobile Security の Web 管理コンソールにログオンします。

2. メニューバーの [モバイルデバイス] をクリックします。

   [モバイルデバイス] 画面が表示されます。

3. [管理対象デバイス] タブのデバイスツリーで、情報を編集するモバイルデバイスをクリックします。

4. [編集] をクリックします。

5. 次のフィールドの情報をアップデートします。

   - 電話番号: モバイルデバイスの電話番号。モバイルデバイスが SMS Sender から確実に通知メッセージを受信できるように、国コード (長さ 1〜5 桁) を入力してください。
   - デバイス名: デバイスツリーでモバイルデバイスを識別するためのモバイルデバイスの名前。

- グループ: モバイルデバイスが属するグループの名前。リストに表示されます。
- アセット番号: モバイルデバイスに割り当てられるアセット番号。
- 説明: モバイルデバイスやユーザに関連する追加情報または注意事項。

6. [保存] をクリックします。

モバイルデバイスを削除する

Mobile Security には、モバイルデバイスを削除するためのオプションが 2 つあります。

- 78 ページの「1 台のモバイルデバイスを削除する」
- 79 ページの「複数のモバイルデバイスを削除する」

1 台のモバイルデバイスを削除する

手順

1. Mobile Security の Web 管理コンソールにログオンします。
2. メニューバーの [モバイルデバイス] をクリックします。

   [モバイルデバイス] 画面が表示されます。
3. [管理対象デバイス] タブのデバイスツリーで、削除するモバイルデバイスをクリックします。
4. [削除] をクリックし、確認画面で [OK] をクリックします。

モバイルデバイスツリーからモバイルデバイスが削除され、Mobile Security マネージメントサーバへの登録が解除されます。

複数のモバイルデバイスを削除する

手順

1. Mobile Security の Web 管理コンソールにログオンします。
2. メニューバーの [モバイルデバイス] をクリックします。

   [モバイルデバイス] 画面が表示されます。
3. [管理対象デバイス] タブのデバイスツリーで、削除するモバイルデバイスを含むグループをクリックします。
4. 右側にあるリストからモバイルデバイスを選択し、[削除] をクリックして、確認画面で [OK] をクリックします。

   モバイルデバイスツリーからモバイルデバイスが削除され、Mobile Security マネージメントサーバへの登録が解除されます。

モバイルデバイスを別のグループに移動する

モバイルデバイスを別のグループに移動できます。移動すると、Mobile Security によって、グループに適用されているポリシーの情報がユーザに自動的に送信されます。

手順

1. Mobile Security の Web 管理コンソールにログオンします。
2. メニューバーの [モバイルデバイス] をクリックします。

   [モバイルデバイス] 画面が表示されます。
3. [管理対象デバイス] タブで、別のグループに移動するモバイルデバイスを含むグループをクリックします。
4. 右側にあるリストからモバイルデバイスを選択し、[移動] をクリックします。

   [デバイスの移動] 画面が表示されます。

5. リストから対象のグループを選択し、[OK] をクリックします。

モバイルデバイスのステータス

[デバイス] 画面の [管理対象デバイス] タブでモバイルデバイスを選択すると、そのデバイスのステータス情報が右側のペインに表示されます。モバイルデバイス情報は、次のセクションに分かれています。

- 基本: 登録ステータス、電話番号、LDAP アカウント、プラットフォーム情報が表示されます。
- ハードウェア、OS: デバイスやモデルの名前、OS のバージョン、メモリ情報、セルラー技術、IMEI および MEID 番号、ファームウェアバージョン情報、前回の iCloud バックアップなど、モバイルデバイスの詳細情報が表示されます。
- セキュリティ : モバイルデバイスの暗号化、Jailbreak、root 化、開発者オプション、USB デバッグ、ネットワークトラフィックの復号の状況、不正な iOS プロファイル、不正な SSL 証明書、不正なアプリ、改ざんされたアプリ、脆弱なアプリ、プライバシー漏えいのあるアプリの数、接続しているアクセスポイント (Wi-Fi)、およびアクティブな iTunes アカウントが表示されます。
- ネットワーク: ICCID (Integrated Circuit Card ID)、Bluetooth および Wi-Fi MAC の情報が表示されます。これには、キャリア網の名前、設定バージョン、ローミングステータス、MCC (Mobile Country Code) や MNC (Mobile Network Code) 情報、およびインターネット共有のステータスが含まれます。

  注意

  USB テザリングのステータスおよび Bluetooth テザリングのステータスはサポートされなくなりました。

- ポリシー: 設定およびセキュリティポリシーの前回アップデート日時が表示されます。
- インストール済みのアプリ : モバイルデバイスにインストールされているすべてのアプリケーションのリストとコンプライアンスチェックの 結

果が表示されます。このタブは Android デバイスと iOS デバイスでのみ使用できます。

- Samsung KNOX 情報: Samsung KNOX をサポートするモバイルデバイスに関する追加情報が表示されます。

Mobile Device エージェントの基本検索

モバイルデバイス名または電話番号を使用して Mobile Device エージェントを検索するには、検索テキストボックスに情報を入力し、<Enter> キーをクリックします。検索結果は、デバイスツリーに表示されます。

Mobile Device エージェントの詳細検索

[詳細検索] 画面を使用して、Mobile Device エージェントの追加検索条件を指定できます。

手順

1. [モバイルデバイス] 画面の [詳細検索] のリンクをクリックします。ポップアップ画面が表示されます。
2. 検索条件を選択して、値をフィールドに入力します (該当する場合)。
   - デバイス名: モバイルデバイスの識別用ニックネーム
   - 電話番号: モバイルデバイスの電話番号
   - ユーザ名: モバイルデバイスのユーザ名
   - アセット番号: モバイルデバイスのアセット番号
   - IMEI: モバイルデバイスの IMEI 番号
   - シリアル番号: モバイルデバイスのシリアル番号
   - Wi-Fi の MAC アドレス: モバイルデバイスの Wi-Fi の MAC アドレス
   - 説明: モバイルデバイスの説明

- OS: モバイルデバイスで実行されている OS、または Android および iOS のバージョン番号
- グループ: モバイルデバイスが属するグループ
- エージェントのバージョン: モバイルデバイスの Mobile Device エージェントのバージョン番号
- 前回の接続: モバイルデバイスが Mobile Security サーバに前回接続されていた期間
- 不正プログラムパターンファイルのバージョン: モバイルデバイス上の不正プログラムパターンファイルのバージョン番号
- 不正プログラム検索エンジンのバージョン: モバイルデバイスの不正プログラム検索エンジンのバージョン番号
- アプリ名: モバイルデバイスにインストールされているアプリ
- ユーザがアンインストールした Mobile Device エージェント: ユーザによって Mobile Device エージェントがアンインストールされているモバイルデバイスのみに検索範囲を絞り込む
- root 化されたモバイルデバイス: root 化されたモバイルデバイスのみに検索範囲を絞り込む
- 感染した Mobile Device エージェント: 指定した数の不正プログラムが検出されたモバイルデバイスのみに検索範囲を絞り込む
- モバイルデバイスステータス: 選択したステータスのモバイルデバイスのみに検索範囲を絞り込む

3. [OK] をクリックします。検索結果は、デバイスツリーに表示されます。

Mobile Device エージェントでの操作

Trend Micro Mobile Security では、[モバイルデバイス] 画面からモバイルデバイスのさまざまな操作を実行できます。

Mobile Device エージェントをアップデートする

[モバイルデバイス] 画面の [管理対象デバイス] タブから、期限切れのコンポーネントまたはセキュリティポリシーを使用しているモバイルデバイスにアップデート通知を送信できます。

手順

1. Mobile Security の Web 管理コンソールにログオンします。
2. メニューバーの [モバイルデバイス] をクリックします。

   [モバイルデバイス] 画面が表示されます。
3. [管理対象デバイス] タブで、アップデートするモバイルデバイスを含むグループをクリックします。
4. [アップデート] をクリックします。

期限切れのコンポーネントまたはセキュリティポリシーを使用しているすべてのモバイルデバイスに、Mobile Security からアップデート通知が送信されます。

[アップデート] 画面を使用して、期限切れのコンポーネントまたはポリシーを使用しているモバイルデバイスにアップデート通知を自動的に送信するか、またはこのプロセスを手動で開始するように Mobile Security を設定することもできます。

詳細については、184 ページの「Mobile Security コンポーネントをアップデートする」を参照してください。

モバイルデバイス情報をアップデートする

Mobile Security サーバは、設定された頻度で管理対象のモバイルデバイスからデバイス情報を自動的に取得し、その情報を [モバイルデバイス] 画面に表示します。

[管理対象デバイス] タブでは、予約された次回の自動アップデートを待たずに、管理対象のモバイルデバイスのデバイス情報をアップデートできます。

手順

1. Mobile Security の Web 管理コンソールにログオンします。
2. メニューバーの [モバイルデバイス] をクリックします。

   [モバイルデバイス] 画面が表示されます。
3. [管理対象デバイス] タブのデバイスツリーで、モバイルデバイスを選択します。
4. [アップデート] をクリックします。

盗難/紛失時の対策

モバイルデバイスを紛失または置き忘れた場合に、モバイルデバイスをリモートで検索したり、ロックしたり、すべてのデータを削除したりできます。

モバイルデバイスをリモート検索する

ワイヤレスネットワークやモバイルデバイスの GPS 機能を使用してモバイルデバイスを検索できます。マネージメントサーバは、モバイルデバイスの位置情報を Google Map 上に表示します。

注意

この機能は Android デバイスと iOS デバイスでのみ使用できます。

手順

1. Mobile Security の Web 管理コンソールにログオンします。
2. メニューバーの [モバイルデバイス] をクリックします。

   [モバイルデバイス] 画面が表示されます。
3. [管理対象デバイス] タブのデバイスツリーで、検索するモバイルデバイスをクリックします。

4. [デバイス検索] をクリックし、確認画面で [OK] をクリックします。

   Mobile Security マネージメントサーバがモバイルデバイスの検索を試行し、[モバイルデバイスのリモート検索] 画面に Google Map へのリンクを表示します。

5. [モバイルデバイスのリモート検索] 画面にある Google Map へのリンクをクリックして、モバイルデバイスの最新の位置情報をマップ上で確認します。

モバイルデバイスをリモートロックする

Web 管理コンソールからモバイルデバイスをリモートでロックできます。モバイルデバイスのロックを解除するには、ユーザがパワーオンパスワードを入力する必要があります。

注意

この機能は、Android および iOS デバイスでのみサポートされます。

手順

1. Mobile Security の Web 管理コンソールにログオンします。
2. メニューバーの [モバイルデバイス] をクリックします。

   [モバイルデバイス] 画面が表示されます。

3. [管理対象デバイス] タブのデバイスツリーで、ロックするモバイルデバイスをクリックします。
4. 次のいずれかを実行します。

   Android デバイスの場合、[リモートロック] をクリックし、確認画面で [OK] をクリックします。

   iOS デバイスの場合、[リモートロック] をクリックし、ユーザの電話番号とユーザに送信するメッセージを入力してから [ロック] をクリックします。

ロックコマンドが正常に生成されると、[成功] というメッセージが画面に表示されます。モバイルデバイスが正常にロックされたかどうかは、[コマンドキュー管理] 画面のコマンドのステータスで確認できます。詳細については、67 ページの「コマンドキュー管理」を参照してください。

モバイルデバイスをリモート消去する

警告!

この処理は元に戻せないため、この機能を使用する際には注意してください。すべてのデータが消失し、復元不可能になります。

モバイルデバイスを工場出荷時の設定にリモートでリセットして、モバイルデバイスの内部メモリ/SD カードをクリアできます。この機能によって、モバイルデバイスの紛失、盗難、または置き忘れの場合に、データのセキュリティを確保できます。また、モバイルデバイスから次の企業データのみを削除することもできます。

- Android の場合: Exchange メール、カレンダー、および連絡先
- iOS の場合: MDM プロファイル、関連ポリシー、設定、およびデータ

注意

この機能は、Android および iOS デバイスでのみサポートされます。

手順

1. Mobile Security の Web 管理コンソールにログオンします。
2. メニューバーの [モバイルデバイス] をクリックします。

   [モバイルデバイス] 画面が表示されます。
3. [管理対象デバイス] タブのデバイスツリーで、消去するモバイルデバイスをクリックします。
4. [リモート消去] をクリックします。

   [モバイルデバイスのリモート 消去] 画面が表示されます。

5. 該当する [デバイス名] チェックボックスをオンにします。
6. 次のいずれかを実行します。
   - Android デバイスの場合は、次のいずれかを選択します。
     - すべてのデータを消去し、出荷時の設定に戻します (すべてのアプリおよび格納されたデータが削除されます。挿入されているメモリカードはフォーマットされます。この処理を元に戻すことはできません)。
     - メール、カレンダー、および連絡先リストを消去します:「選択消去」とも呼ばれます。

       このオプションを選択する場合は、[選択消去に失敗した場合、すべてのデータを消去し、出荷時の設定に戻します。] も選択できます。
   - iOS デバイスの場合は、次のいずれかを選択します。
     - すべてのデータを消去し、出荷時の設定に戻します (すべてのアプリおよび格納されたデータが削除されます。挿入されているメモリカードはフォーマットされます。この処理を元に戻すことはできません)。
     - プロビジョニングされたプロファイル、ポリシー、設定、およびその関連データをすべて消去します。
7. [モバイルデバイスのリモート消去] をクリックします。

   選択したデータがモバイルデバイスから削除され、Mobile Device エージェントがサーバから登録解除されます。

リモートによるパスワードのリセット

ユーザがパワーオンパスワードを忘れた場合、マネージメントサーバからリモートでパワーオンパスワードをリセットしてモバイルデバイスのロックを解除できます。モバイルデバイスのロック解除が正常に行われると、ユーザはパワーオンパスワードを変更できるようになります。

注意

この機能は、Android および iOS デバイスでのみサポートされます。

Android デバイスのパスワードをリセットする

手順

1. Mobile Security の Web 管理コンソールにログオンします。
2. メニューバーの [モバイルデバイス] をクリックします。

   [モバイルデバイス] 画面が表示されます。
3. ツリーからモバイルデバイスを選択し、[パスワードのリセット] をクリックします。
4. 表示されるポップアップ画面に 6 桁の新しいパスワードを入力して確認します。

iOS デバイスのパスワードを削除する

手順

1. Mobile Security の Web 管理コンソールにログオンします。
2. メニューバーの [モバイルデバイス] をクリックします。

   [モバイルデバイス] 画面が表示されます。
3. ツリーからモバイルデバイスを選択し、[パスワードのリセット] をクリックします。
4. 表示される確認画面で [OK] をクリックします。選択した iOS デバイスのパワーオンパスワードが削除されます。

Samsung KNOX ワークスペースをリモートで管理する

Samsung KNOX ワークスペースを管理するためのコマンドを Mobile Security の Web 管理コンソールから送信できます。これらのコマンドには、コンテナの作成、コンテナの削除、コンテナのロック、コンテナのロック解除、およびコンテナのパスワードのリセットなどが含まれます。この機能は Samsung デバイスでのみ使用できます。

手順

1. Mobile Security の Web 管理コンソールにログオンします。
2. メニューバーの [モバイルデバイス] をクリックします。

   [モバイルデバイス] 画面が表示されます。
3. [管理対象デバイス] タブのデバイスツリーで、管理対象の Samsung デバイスを選択します。
4. 次のいずれかを実行します。
   - モバイルデバイス上に KNOX ワークスペースを作成するには、[KNOX の操作] > [コンテナの作成] をクリックします。
   - モバイルデバイスから KNOX ワークスペースを削除するには、[KNOX の操作] > [コンテナの削除] をクリックします。
   - ユーザがワークスペースのパスワードをリセットできるようにするには、[KNOX の操作] > [パスワードのリセット] をクリックします。
   - モバイルデバイスでワークスペースをロックするには、[KNOX の操作] > [コンテナのロック] をクリックします。
   - モバイルデバイスでワークスペースをロック解除するには、[KNOX の操作] > [コンテナのロック解除] をクリックします。

iOS の設定をリモートで変更する

iOS デバイスの設定を Web 管理コンソールからリモートで変更できます。これらの設定には、データローミング、音声ローミング、インターネット共有などが含まれます。

手順

1. Mobile Security の Web 管理コンソールにログオンします。
2. メニューバーの [モバイルデバイス] をクリックします。

   [モバイルデバイス] 画面が表示されます。
3. [管理対象デバイス] タブのデバイスツリーで、管理対象の iOS デバイスを選択します。
4. 次のいずれかを実行します。
   - データローミングを有効にするには、[iOS の操作] > [データローミングを有効にする] をクリックします。
   - データローミングを無効にするには、[iOS の操作] > [データローミングを無効にする] をクリックします。
   - 音声ローミングを有効にするには、[iOS の操作] > [音声ローミングを有効にする] をクリックします。
   - 音声ローミングを無効にするには、[iOS の操作] > [音声ローミングを無効にする] をクリックします。
   - インターネット共有を有効にするには、[iOS の操作] > [インターネット共有を有効にする] をクリックします。
   - インターネット共有を無効にするには、[iOS の操作] > [インターネット共有を無効にする] をクリックします。
   - AirPlay ミラーリングを開始するには、[iOS の操作] > [AirPlay ミラーリングの要求] をクリックします。
   - AirPlay ミラーリングを停止するには、[iOS の操作] > [AirPlay ミラーリングの停止] をクリックします。

データをエクスポートする

[モバイルデバイス] 画面の [管理対象デバイス] タブからデータをエクスポートし、分析またはバックアップに使用できます。

手順

1. Mobile Security の Web 管理コンソールにログオンします。
2. メニューバーの [モバイルデバイス] をクリックします。

   [モバイルデバイス] 画面が表示されます。
3. エクスポートするデータを含むモバイルデバイスグループをデバイスツリーから選択します。
4. [エクスポート] をクリックします。
5. 必要に応じて、表示されたポップアップ画面の [保存] をクリックし、.zip ファイルをコンピュータに保存します。
6. ダウンロードした.zip ファイルの内容を解凍し、.csv ファイルを開いてモバイルデバイスの情報を確認します。

モバイルデバイスにメッセージを送信する

[モバイルデバイス] 画面の [管理対象デバイス] タブから、ユーザやグループにメッセージを送信できます。

注意

iOS デバイスに SMS を送信した場合、[コマンドキュー管理] 画面には情報が表示されません。

手順

1. Mobile Security の Web 管理コンソールにログオンします。
2. メニューバーの [モバイルデバイス] をクリックします。

   [モバイルデバイス] 画面が表示されます。
3. デバイスツリーで、メッセージを送信するモバイルデバイスまたはデバイスグループを選択します。

4. [メッセージの送信] をクリックします。

   [メッセージの送信] 画面が表示されます。

5. 表示されるフィールドにメッセージを入力し、[送信] をクリックします。

[Exchange ActiveSync デバイス] タブ

Mobile Security マネージメントサーバで Exchange Server との統合を有効にすると、[モバイルデバイス] 画面の [Exchange ActiveSync デバイス] タブに、ActiveSync サービス経由で Exchange Server に接続するデバイスのリストが表示されます。

[Exchange ActiveSync デバイス] タブでは、次の操作を実行できます。

- Exchange Server へのアクセスの許可またはブロック
- オンデマンドのリモート消去
- リモート消去コマンドのキャンセル
- リストからのモバイルデバイスの削除

注意

Mobile Security サーバによって、デバイスモデルとメールアドレスに基づき、Exchange Server のモバイルデバイスが照合されます。事前設定された登録キーを使用して登録されているデバイスの場合、Mobile Security サーバが Exchange Server のデバイスを正常に照合できない場合があります。

Exchange ActiveSync ユーザに登録を依頼する

Exchange ActiveSync ユーザに登録を依頼する前に、マネージメントサーバで通知とレポートを設定する必要があります。「インストールおよびクライアント配信ガイド」の「通知とレポートを設定する」を参照してください。

手順

1. Mobile Security の Web 管理コンソールにログオンします。
2. メニューバーの [モバイルデバイス] をクリックします。

   [モバイルデバイス] 画面が表示されます。
3. [Exchange ActiveSync デバイス] タブをクリックします。
4. Mobile Security への登録を依頼するユーザに割り当てられているモバイルデバイスを選択します。
5. [登録依頼] をクリックし、表示された確認画面で [OK] をクリックします。

   登録依頼したユーザにメールメッセージが送信されます。モバイルデバイスを Mobile Security マネージメントサーバに登録すると、Mobile Device エージェントのステータスが [管理対象デバイス] 列に表示されます。

Exchange Server へのアクセスを許可またはブロックする

手順

1. Mobile Security の Web 管理コンソールにログオンします。
2. メニューバーの [モバイルデバイス] をクリックします。

   [モバイルデバイス] 画面が表示されます。
3. [Exchange ActiveSync デバイス] タブをクリックします。
4. Exchange Server へのアクセスを許可またはブロックするモバイルデバイスを選択します。
5. [アクセスを許可] または [アクセスをブロック] をクリックし、確認画面で [OK] をクリックします。

モバイルデバイスと Exchange Server との同期が完了した後に、[Exchange のアクセス状態] 列のモバイルデバイスのステータスに新しいステータスが表示されます。

ActiveSync モバイルデバイスをリモート消去する

警告!

この処理は元に戻せないため、この機能を使用する際には注意してください。すべてのデータが消失し、復元不可能になります。

ActiveSync モバイルデバイスを工場出荷時の設定にリモートでリセットして、モバイルデバイスの内部メモリ/SD カードをクリアできます。この機能によって、モバイルデバイスの紛失、盗難、または置き忘れの場合に、データのセキュリティを確保できます。

ActiveSync を使用しないモバイルデバイスを消去する手順については、86 ページの「モバイルデバイスをリモート消去する」を参照してください。

手順

1. Mobile Security の Web 管理コンソールにログオンします。
2. メニューバーの [モバイルデバイス] をクリックします。

   [モバイルデバイス] 画面が表示されます。
3. [Exchange ActiveSync デバイス] タブをクリックします。
4. 消去するモバイルデバイスを選択します。
5. [リモート消去] をクリックします。

   [モバイルデバイスのリモート消去] ポップアップ画面が表示されます。
6. デバイスを選択し、[モバイルデバイスのリモート消去] をクリックします。

ActiveSync モバイルデバイスを削除する

Mobile Security マネージメントサーバからリモート消去したモバイルデバイスは Exchange Server にアクセスできなくなります。このようなモバイルデバイスの情報を、[モバイルデバイス] 画面の [Exchange ActiveSync デバイス] タブから削除できます。

注意

削除できるのは、Mobile Security マネージメントサーバからリモート消去したモバイルデバイスのみです。

手順

1. Mobile Security の Web 管理コンソールにログオンします。
2. メニューバーの [モバイルデバイス] をクリックします。

   [モバイルデバイス] 画面が表示されます。
3. [Exchange ActiveSync デバイス] タブをクリックします。
4. リストから削除するモバイルデバイスを選択します。
5. [削除] をクリックし、確認画面で [OK] をクリックします。

[Device Enrollment Program] タブ

Device Enrollment Program (DEP) は、会社所有の iOS デバイスをすばやく効率的に導入するための Apple が提供するプログラムです。DEP プログラムに自分の会社を登録することができます。

Trend Micro Mobile Security は Device Enrollment Program と統合されているため、Apple から直接購入した会社支給の iOS 7～iOS 11 デバイスを効率的に登録することができます。管理者が Device Enrollment Program との統合を設定した場合、会社所有の iOS デバイスを支給された社員が iOS のアクティベーションプロセスでデバイスを 設定しようとすると、Mobile Security への登録画面が表示されます。

Mobile Security を DEP と統合しておけば、登録手順をユーザに指示しなくても、初回使用時にすべてのモバイルデバイスが登録されます。これは、関連するサポートコストの削減にもつながります。

Device Enrollment Program のユーザ操作

管理者が Mobile Security と Apple の Device Enrollment Program との統合を設定している場合、ユーザ (社員) の操作は次のようになります。

- ユーザが会社支給の新しい iOS デバイスを受け取り、箱から出して電源を入れます。
- デバイスが Apple のサーバに接続されます。
- デバイス ID からデバイスが会社の Device Enrollment Program アカウントに追加されていることが Apple サーバ側で検出され、Mobile Security の導入に必要なデバイスの設定と接続の詳細が送信されます。
- ユーザが iOS 設定アシスタントを使用してデバイスアクティベーションを実行すると、Mobile Security への登録も完了します。

Device Enrollment Program との統合を設定する際に、iOS 設定アシスタントに表示される画面を指定できます。デバイス管理で設定する項目の画面を省略することで、アクティベーションプロセスをさらにシンプルにすることができます。たとえば、ジオフェンシング設定の一環としてすべてのデバイスで位置情報サービスを有効にする必要がある場合、位置情報サービスを有効にするかどうかを選択する画面を省略します。

デバイスをアクティベーションすると 、Mobile Security への登録画面が表示されます。認証情報やメールアドレスをユーザが入力する必要はなく、Mobile Security の接続の詳細も必要ありません。Device Enrollment Program との統合時に管理者が作成した専用の Device Enrollment Program プロファイルが、自動的にデバイスに展開されます。

Device Enrollment Program 用に Mobile Security を設定する

Device Enrollment Program (DEP) 用に Mobile Security を設定する前に、Apple の次の Web サイトで、組織を DEP プログラムに登録してあることを確認してください。

http://deploy.apple.com/

手順

1. Mobile Security の Web 管理コンソールにログオンします。
2. メニューバーの [モバイルデバイス] をクリックします。

   [モバイルデバイス] 画面が表示されます。
3. [Device Enrollment Program] タブをクリックします。
4. [設定] をクリックします。
5. [公開鍵] の前にある [ダウンロード] リンクをクリックして、Mobile Security マネージメントサーバからローカルコンピュータに公開鍵をダウンロードします。
6. [配信] の前にある [Apple Deployment Programs] リンクをクリックします。

   Apple Deployment Programs Web ポータルが Web ブラウザで開きます。
7. Device Enrollment Program アカウントにログインし、Mobile Security マネージメントサーバからダウンロードした公開鍵を使用して新しい MDM サーバを作成します。
8. MDM サーバで、アクセストークンを生成して適切な場所にトークンファイルを保存してから、登録するモバイルデバイスを MDM サーバに割り当てます。
9. Apple Deployment Programs Web ポータルで生成したトークンファイルを Mobile Security マネージメントサーバにアップロードします。アップロードが完了するまで待ちます。

   アップロードが完了すると、[Device Enrollment Program 設定] 画面が表示されます。
10. [Device Enrollment Program の詳細] で、モバイルデバイス用のセットアッププロファイルを設定します。
    - プロファイル名: モバイルデバイスに表示されるセットアッププロファイルの名前です。

- 監視が必要: Device Enrollment Program で登録したモバイルデバイスを監視モードにします。
- 削除可能な設定: Device Enrollment Program で登録したデバイスからユーザがデバイス管理設定を削除できるようにします。
- ペアリングを許可: Device Enrollment Program で登録したデバイスを Apple の iTunes や Apple Configurator などのツールで管理できるようにします。
- 必須設定: デバイスのアクティベーションプロセスでユーザが Mobile Security の登録手順を省略できないようにします。
- 事業部門: モバイルデバイスの割り当て先の部門名です。
- 一意のサービス ID: Mobile Security を複数展開している場合に、対象の Mobile Security を一意に識別するサービス ID を入力します。
- サポートの電話番号: 問い合わせ先の電話番号です。
- 必要な設定項目: ユーザが設定する必要がある設定項目です。初期設定では、すべての設定項目が必須です。項目を無効にすると、その項目を設定時に省略できるようになります。

11. [Enterprise Mobile Security エージェントのライセンス] セクションで、モバイルデバイスへの Enterprise Mobile Security エージェントのライセンスの割り当てに関する使用可能なオプションを選択します。Enterprise Mobile Security アプリケーションが Volume Purchase Program に含まれている場合は、DEP による登録時にアプリケーションライセンスが割り当てられます。それ以外の場合は、iTunes アカウントを使用してライセンスが割り当てられます。

注意

この機能を使用するには、まず Volume Purchase Program の設定を行う必要があります。Volume Purchase Program を設定するには、「147 ページの「Volume Purchase Program ライセンスを設定する」」を参照してください。

DEP を介して iOS モバイルデバイスで Enterprise Mobile Security MDA の展開と登録を行う手順については、「インストールおよびクライアント配信ガイド」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。

12. [保存] をクリックします。

    Mobile Security マネージメントサーバのモバイルデバイスのリストが Apple 社の Device Enrollment Programs サーバと同期され、[モバイルデバイス] 画面の [Devices Enrollment Program] タブにモバイルデバイスが表示されます。

Trend Micro Control Manager との統合

Trend Micro Mobile Security では、Trend Micro Control Manager (Control Manager) との統合機能が提供されます。この統合により、Control Manager の管理者は次のことができます。

- Mobile Security 用のセキュリティポリシーの作成、編集、または削除
- 登録済みモバイルデバイスへのセキュリティポリシーの配信
- の [ダッシュボード] 画面の表示

Trend Micro Control Manager の詳細と、Control Manager における Mobile Security ポリシーの管理の詳細については、次の URL にある製品ドキュメントを参照してください。

https://docs.trendmicro.com/ja-jp/enterprise/control-manager-70/introduction/introducing-control-/about-control-manage.aspx

Control Manager でセキュリティポリシーを作成する

Trend Micro Control Manager の Web コンソールでは、Mobile Security で提供されるものと同じセキュリティポリシーが表示されます。Control Manager の管理者が Mobile Security 用のセキュリティポリシーを作成した場合、Mobile Security によってこのポリシー用の新しいグループが作成され、すべての対象モバイルデバイスがこのグループに移動します。Mobile Security で作成されたポリシーを、Control Manager で作成されたポリシーと区別するため、Mobile Security はグループ名の接頭辞に TMCM_を付加します。

セキュリティポリシーを削除または変更する

Control Manager の管理者はいつでもポリシーを変更できます。変更されたポリシーは、すぐにモバイルデバイスに展開されます。

Trend Micro Control Manager は、24 時間ごとにポリシーを Trend Micro Mobile Security と同期します。Control Manager で作成し、Control Manager から展開したポリシーを削除または変更した場合、そのポリシーは元の設定に戻されるか、同期の実行後にもう一度作成されます。

Control Manager におけるセキュリティポリシーのステータス

Trend Micro Control Manager の Web コンソールには、セキュリティポリシーのステータスが表示されます。

- 保留中: Control Manager の Web コンソールでポリシーが作成されましたが、まだモバイルデバイスに配信されていません。
- 配信済み: ポリシーはすべての対象モバイルデバイスに配信および展開されています。

第 4 章

ユーザと登録依頼の管理

この章では、Mobile Security でのユーザと登録依頼リストの管理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。

[ユーザ] タブ

[ユーザ] タブでは、次のタスクを実行できます。

- ユーザへの登録依頼
- 登録依頼の再送と割り当てグループの変更
- ユーザ情報の編集
- ユーザの削除
- ユーザの検索

ユーザリストを表示する

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. リストを並べ替えるには、次のいずれかの列の見出しをクリックします。
   - ユーザ名
   - メール
   - デバイス
   - 登録依頼の送信日
3. ユーザを検索するには、[検索] バーにユーザ名またはメールアドレスを入力し、<Enter> キーを押します。

   該当するユーザがリストにあれば、Mobile Security に情報が表示されます。

登録依頼を再送する

注意

このトピックは、指定以外の MDM ソリューションを使用するセキュリティ 検索モードの Mobile Security に該当します。

Mobile Security を AirWatch または MobileIron と統合している場合、この機能は無効になります。

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. ユーザを選択し、[登録依頼を再送] をクリックします。

   [登録依頼を再送] 画面が表示されます。

3. リストからグループを選択します。

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。

ユーザ情報を編集する

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. リストからユーザ名をクリックします。

   [ユーザ情報の編集] 画面が表示されます。

3. 必要に応じて、ユーザ名やメールアドレスを変更します。

4. [保存] をクリックします。

   ユーザ情報が更新されます。

ユーザを削除する

注意

削除できるのは、Mobile Security サーバにデバイスが登録されていないユーザだけです。

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. リストからユーザを選択し、[削除] をクリックします。
3. 表示された確認メッセージで、[OK] をクリックします。

   選択したユーザが削除されます。

[登録依頼] タブ

[ユーザ] 画面の [登録依頼] タブでは、次のタスクを実行できます。

- 登録依頼リストの表示
- 登録依頼の再送信
- アクティブな登録依頼のキャンセル
- リストからの登録依頼の削除
- 登録依頼の検索

登録依頼リストを表示する

手順

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

   [登録依頼] タブが表示されます。

2. リストをフィルタするには、リストから登録依頼のステータスを選択します。

登録依頼のステータス	説明
アクティブ	登録依頼は有効で、ユーザは登録依頼メールの情報を使用して登録できます。
使用期間終了日時	登録依頼の期間が終了しているため、ユーザは登録依頼メールの情報を使用して登録することはできません。
使用済み	ユーザは登録依頼メールの情報を使用して登録済みであり、登録キーは無効になっています。 **注意** このステータスは、[デバイス登録設定] の [登録キーの使用制限] オプションが [1 回のみ使用] に設定されている場合のみ表示されます。
キャンセル済み	サーバで登録依頼がキャンセルされたため、ユーザは登録依頼メールの情報を使用して登録することはできません。

3. 登録依頼を検索するには、[検索] バーにユーザ名、電話番号、またはメールアドレスを入力し、<Enter> キーを押します。

   該当する登録依頼がリストにあれば、Mobile Security に情報が表示されます。

登録依頼を再送信する

手順

1. Mobile Security の Web 管理コンソールで、[ユーザ] > [登録依頼] の順に選択します。
2. リストから登録依頼を選択します。
3. [登録依頼の再送信] をクリックします。

   Mobile Security によって、選択したユーザに登録依頼が再送信されます。

アクティブな登録依頼をキャンセルする

手順

1. Mobile Security の Web 管理コンソールで、[ユーザ] > [登録依頼] の順に選択します。
2. リストから登録依頼を選択します。
3. [登録依頼のキャンセル] をクリックします。

   選択した登録依頼がキャンセルされます。

リストから登録依頼を削除する

注意

削除できるのは、ステータスが [使用済み] または [キャンセル済み] の登録依頼だけです。

手順

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

2. リストから登録依頼を選択します。
3. [登録依頼の削除] をクリックします。

   選択した登録依頼がリストから削除されます。

第 5 章

ポリシーの設定

この章では、Mobile Security グループのモバイルデバイスにセキュリティポリシーを設定して適用する方法を説明します。プロビジョニング、モバイルデバイスのセキュリティ、およびデータ保護に関連するポリシーを使用できます。

この章には、次のセクションが含まれています。

ポリシーについて

マネージメントサーバの Mobile Security グループに対するポリシーや Mobile Security に登録されたすべてのモバイルデバイスに対するポリシーを設定できます。

表 5-1. Mobile Security のデバイスポリシー

ポリシー	レファレンス/参照情報
承認済みリスト	詳細は 113 ページの「承認済みアプリリスト」を参照してください。
ネットワークトラフィックを復号する信頼された証明書リスト	詳細は 113 ページの「ネットワークトラフィックを復号する信頼された証明書リスト」を参照してください。

表 5-2. Mobile Security のグループポリシー

ポリシーグループ	ポリシー	レファレンス/参照情報
一般	共通ポリシー	詳細は 117 ページの「共通ポリシー」を参照してください。

ポリシーグループ	ポリシー	レファレンス/参照情報
プロビジョニング	Wi-Fi ポリシー	詳細は 118 ページの「Wi-Fi ポリシー」を参照してください。
	Exchange ActiveSync ポリシー	詳細は 118 ページの「Exchange ActiveSync ポリシー」を参照してください。
	証明書ポリシー	詳細は 119 ページの「証明書ポリシー」を参照してください。
	VPN ポリシー	詳細は 118 ページの「VPN ポリシー」を参照してください。
	グローバル HTTP プロキシポリシー	詳細は 118 ページの「グローバル HTTP プロキシポリシー」を参照してください。
	シングルサインオンポリシー	詳細は 119 ページの「シングルサインオンポリシー」を参照してください。
	モバイルデータ通信ネットワークポリシー	詳細は 120 ページの「モバイルデータ通信ネットワークポリシー」を参照してください。
	AirPlay/AirPrint ポリシー	詳細は 120 ページの「AirPlay/AirPrint ポリシー」を参照してください。
	テーマポリシー	詳細は 120 ページの「テーマポリシー」を参照してください。
	管理対象ドメインポリシー	詳細は 121 ページの「管理対象ドメインポリシー」を参照してください。

ポリシーグループ	ポリシー	レファレンス/参照情報
デバイスのセキュリティ	セキュリティポリシー	詳細は 121 ページの「セキュリティポリシー」を参照してください。
	迷惑メール対策ポリシー	詳細は 125 ページの「迷惑メール対策ポリシー」を参照してください。
	着信フィルタポリシー	詳細は 128 ページの「着信フィルタポリシー」を参照してください。
デバイス	パスワードポリシー	詳細は 130 ページの「パスワードポリシー」を参照してください。
	機能ロックポリシー	詳細は 130 ページの「機能ロックポリシー」を参照してください。
	コンプライアンスポリシー	詳細は 131 ページの「コンプライアンスポリシー」を参照してください。
アプリケーションの管理	アプリの監視および管理ポリシー	詳細は 131 ページの「アプリの監視および制御ポリシー」を参照してください。
	Volume Purchasing Program ポリシー	詳細は 134 ページの「Volume Purchasing Program ポリシー」を参照してください。
Samsung KNOX	コンテナポリシー	詳細は 135 ページの「コンテナポリシー」を参照してください。

すべてのデバイスのポリシー

このセクションでは、すべてのモバイルデバイスに対して Mobile Security で使用できるポリシーについて説明します。

承認済みアプリリスト

[承認済みアプリリスト] には、セキュリティリスク (不正プログラム、脆弱性、プライバシーリスク、改ざん) が検出されたアプリのうち、管理者がモバイルデバイスへのインストールを承認したすべてのアプリが含まれます。

[承認済みアプリリスト] を管理するには、[ポリシー] > [すべてのデバイスのポリシー] の順にクリックします。

ネットワークトラフィックを復号する信頼された証明書リスト

Mobile Security で不正な SSL 証明書が検出された場合、それらの証明書が [検出数] > [不正な SSL 証明書] 画面に表示されます。それらの証明書に問題がない場合は、[ネットワークトラフィックを復号する信頼された証明書リスト] に追加すると Mobile Security による検索の対象から除外することができ、[不正な SSL 証明書] 画面に表示されなくなります。

[ネットワークトラフィックを復号する信頼された証明書リスト] を管理するには、[ポリシー] > [すべてのデバイスのポリシー] の順にクリックします。

すべてのデバイスのポリシーの 管理

Mobile Security では、アプリケーションの承認済みリストとネットワークトラフィックを復号する証明書の信頼済みリストに基づいて、それらのアプリケーションやネットワークを復号する証明書を制約や警告なしでユーザが使用できるように管理できます。

モバイルデバイスのポリシーを作成、編集、コピー、または削除するには、[すべてのデバイスのポリシー] 画面を使用します。

アプリを承認済みリストに追加する

手順

1. Mobile Security の 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。

   - Mobile Security で検索されたインストール済みのアプリを [承認済みリスト] に追加します。

     a. メニューバーの [検出数] > [アプリのセキュリティステータス] または [アプリ] > [インストール済みアプリ] をクリックします。

     b. [Android] タブまたは [iOS] タブをクリックし、[承認済みリスト] に追加する検出済みまたはインストール済みのアプリをリストから選択します。

     c. [承認済みリストに追加] をクリックします。

   - アプリを手動で [承認済みリスト] に追加します。

     a. メニューバーの [ポリシー] > [すべてのデバイスのポリシー] をクリックします。

     b. [承認済みアプリリスト] で、[Android] タブまたは [iOS] タブをクリックし、[承認済みリストに追加] をクリックします。

        [アプリのインポート] 画面が表示されます。

     c. パッケージ名、アプリ名、および説明を該当するフィールドに入力します。各アプリ情報はセミコロン (;) で区切ります。

     d. [アプリのインポート] 画面で [保存] をクリックします。

     e. [すべてのデバイスのポリシー] 画面で [保存] をクリックします。

アプリを承認済みリストから削除する

手順

1. Mobile Security の 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。

   - Mobile Security で検索されたインストール済みのアプリを [承認済みリスト] から削除します。

a. メニューバーの [検出数] > [アプリのセキュリティステータス] または [アプリ] > [インストール済みアプリ] をクリックします。

b. [Android] タブまたは [iOS] タブをクリックし、[承認済みリスト] から削除する検出済みまたはインストール済みのアプリをリストから選択します。

c. [承認済みリストから削除] をクリックします。

- アプリを [承認済みリスト] から直接削除します。

a. メニューバーの [ポリシー] > [すべてのデバイスのポリシー] をクリックします。

b. [承認済みアプリリスト] で、[Android] タブまたは [iOS] タブをクリックし、リストから削除するアプリを選択します。

c. [承認済みリストから削除] をクリックします。

d. [すべてのデバイスのポリシー] 画面で [保存] をクリックします。

ネットワークトラフィックを復号する信頼された証明書を追加する

手順

1. Mobile Security の Web 管理コンソールにログオンします。
2. メニューバーの [ポリシー] > [すべてのデバイスのポリシー] をクリックします。

   [すべてのデバイスのポリシー] 画面が表示されます。
3. [ネットワークトラフィックを復号する信頼された証明書リスト] で [追加] をクリックします。

   [証明書の追加] 画面が表示されます。
4. ローカルハードドライブから 証明書ファイルを選択し、[説明] に証明書ファイルの説明を入力します。

5. [OK] をクリックします。
6. [すべてのデバイスのポリシー] 画面で [保存] をクリックします。

ネットワークトラフィックを復号する信頼された証明書を削除する

手順

1. Mobile Security の Web 管理コンソールにログオンします。
2. メニューバーの [ポリシー] > [すべてのデバイスのポリシー] をクリックします。

   [すべてのデバイスのポリシー] 画面が表示されます。
3. [ネットワークトラフィックを復号する信頼された証明書リスト] で、削除する証明書ファイルを選択し、[削除] をクリックします。
4. [すべてのデバイスのポリシー] 画面で [保存] をクリックします。

すべてのグループのポリシー

このセクションでは、すべてのグループに対して Mobile Security で使用できるポリシーについて説明します。

最上位のユーザアカウントを使用すると、任意のポリシーをテンプレートとして指定することができます。グループ管理者は、このテンプレートに基づいて Mobile Security のセキュリティポリシーを作成できます。ただし、テンプレートとして指定したセキュリティポリシーは、どのグループにも割り当てることができなくなります。

共通ポリシー

共通ポリシーは、モバイルデバイスに共通のセキュリティポリシーを提供します。共通セキュリティポリシーを設定するには、[ポリシー] をクリックし、ポリシー名をクリックして [共通ポリシー] をクリックします。

- ユーザ権限: ユーザによる Mobile Device エージェントのアンインストールを許可する機能を有効または無効にできます。また、ユーザによる Mobile Device エージェントの設定を許可するかどうかも選択できます。

  次に、アンインストール防止に関連する機能の一覧を示します。

  - アンインストール防止のオン/オフは管理コンソールで切り替えます。
  - パスワードの長さは最小 6 文字、最大 12 文字にする必要があります。パスワードには、数字、文字、または記号を使用できます。
  - 管理コンソールからパスワードをグループごとに設定できます。

  [ユーザに Mobile Security クライアントの設定を許可する] チェックボックスをオンにしないと、ユーザは Mobile Device エージェントの設定を変更できません。ただし、このオプションを選択しても、[迷惑メール対策ポリシー]、[着信フィルタポリシー]、および [Web 脅威検出ポリシー] のフィルタリストには影響がありません。詳細については、125 ページの「迷惑 SMS 対策ポリシー」、127 ページの「迷惑 WAP プッシュ対策ポリシー」、および 121 ページの「セキュリティポリシー」を参照してください。

- アップデート設定: 新しいコンポーネントのアップデートを入手できるようになると、Mobile Security マネージメントサーバから Mobile Device エージェントに通知するよう選択できます。または、自動チェックのオプションを選択して、Mobile Security マネージメントサーバのコンポーネントまたは設定のアップデートを Mobile Device エージェントで定期的にチェックできます。

- ログの設定: Mobile Device エージェントが Android OS 上で不正プログラムなどのセキュリティリスクを検出すると、モバイルデバイスでログが生成されます。

Wi-Fi ポリシー

Wi-Fi ポリシーを使用すると、ネットワーク名、セキュリティタイプ、パスワードなどの組織の Wi-Fi ネットワーク情報を Android および iOS デバイスに配信できます。

Wi-Fi ポリシーを設定するには、[ポリシー] をクリックし、ポリシー名をクリックして [Wi-Fi ポリシー] をクリックします。

Exchange ActiveSync ポリシー

Exchange ActiveSync ポリシーを使用すると、組織に合った Exchange ActiveSync ポリシーを作成し、iOS デバイスに配信できます。

Exchange ActiveSync ポリシーを設定するには、[ポリシー] をクリックし、ポリシー名をクリックして [Exchange ActiveSync ポリシー] をクリックします。

VPN ポリシー

VPN ポリシーの設定を使用すると、組織に合った VPN ポリシーを作成し、iOS デバイスに配信できます。

VPN ポリシーを設定するには、[ポリシー] をクリックし、ポリシー名をクリックして [VPN ポリシー] をクリックします。

グローバル HTTP プロキシポリシー

グローバル HTTP プロキシポリシーを使用して、組織のプロキシ情報をモバイルデバイスに配信できます。このポリシーは、監視モードの iOS デバイスにのみ適用されます。

グローバル HTTP プロキシポリシーを設定するには、[ポリシー] をクリックし、ポリシー名をクリックして [グローバル HTTP プロキシポリシー] をクリックします。

証明書ポリシー

証明書ポリシーを使用すると、iOS デバイスに配置する必要がある証明書をインポートできます。

証明書ポリシーを設定するには、[ポリシー] をクリックし、ポリシー名をクリックして [証明書ポリシー] をクリックします。

シングルサインオンポリシー

シングルサインオン (SSO) ポリシーを使用すると、Mobile Security やアプリストアのアプリケーションなど、複数のアプリケーション間で同じ認証情報を使用できます。SSO 証明書が設定された新規アプリケーションではエンタープライズリソースに対してユーザの権限が検証されるため、ユーザは、各アプリケーションにログインするたびにパスワードを 入力する必要がなくなります。

シングルサインオンポリシーには次の情報が含まれます。

- 名前: Kerberos プリンシパル名。
- レルム: Kerberos レルム名。

  Kerberos レルム名は大文字を正しく入力する必要があります。
- URL 接頭辞 (オプション): HTTP を使用した Kerberos 認証用アカウントを使用するために一致する必要のある URL のリスト。このフィールドが空白の場合、すべての http および https の URL がアカウントに一致します。URL の一致パターンは http または https で始まる必要があります。

  このリストの各エントリには URL 接頭辞が必要です。アカウントのいずれかの文字列で始まる URL のみが Kerberos チケットへのアクセスを許可されます。URL の一致パターンにはスキームを含める必要があります。たとえば「http://www.example.com/」などです。一致パターンの末尾が「/」でない場合は、URL に自動的に「/」が追加されます。
- アプリケーション ID (オプション): アカウントの使用が許可されるアプリケーション識別子のリスト。このフィールドが空白の場合、すべてのアプリケーション識別子がアカウントに一致します。

アプリケーション識別子の配列には、アプリケーションバンドル ID に一致する文字列を含める必要があります。これらの文字列には、com.mycompany.myapp のような完全一致を指定することも、ワイルドカード文字「*」を使用してバンドル ID に一致する接頭辞を指定することもできます。ワイルドカード文字はピリオド (.) の後に使用する必要があり、文字列の末尾にのみ使用できます (例: com.mycompany.*)。ワイルドカードを使用すると、バンドル ID がその接頭辞で始まるすべてのアプリケーションがアカウントへのアクセスを許可されます。

iOS 用にシングルサインオンポリシーを設定するには、[ポリシー]、ポリシー名、[シングルサインオンポリシー] の順にクリックします。

AirPlay/AirPrint ポリシー

AirPlay/AirPrint ポリシーの設定を使用すると、組織に合った AirPlay および AirPrint ポリシーを作成し、iOS デバイスに配信できます。

AirPlay/AirPrint ポリシーを設定するには、[ポリシー] をクリックし、ポリシー名をクリックして [AirPlay/AirPrint ポリシー] をクリックします。

モバイルデータ通信ネットワークポリシー

モバイルデータ通信ネットワークポリシーの設定を使用すると、組織に合ったモバイルデータ通信ネットワークを設定し、iOS デバイスに配信できます。

モバイルデータ通信ネットワークポリシーを設定するには、[ポリシー] をクリックし、ポリシー名をクリックして [モバイルデータ通信ネットワークポリシー] をクリックします。

テーマポリシー

テーマポリシー設定を使用すると、iOS デバイスのホーム画面およびロック画面のフォントや壁紙を設定できます。このポリシーは、監視モードの iOS デバイスにのみ適用されます。

テーマポリシーを設定するには、[ポリシー] をクリックし、ポリシー名をクリックして [テーマポリシー] をクリックします。

管理対象ドメインポリシー

管理対象ドメインポリシーでは、組織が管理するメールドメインや Web ドメインを設定できます。

- マークされていないメールドメイン: ユーザがシステムのメールクライアントを使用してメールを作成し、指定されたドメイン以外のメールアドレスを入力すると、メールアドレスが赤色で強調表示 (マーク) されます。この機能を使用すると、信頼されていないメールアドレスにユーザが不注意で機密情報を送信しようとした場合に警告することができます。
- 管理対象の Safari Web ドメイン: Safari を使用して特定のドメインからダウンロードされたファイルを管理対象アプリでしか開けないように指定することができます。たとえば、internal.example.com からダウンロードした PDF を Adobe Reader (管理対象アプリ) では開けるようにし、Dropbox (非管理対象アプリ) では開けないように設定できます。これにより、Safari のセキュリティを強化し、エンタープライズブラウザとして幅広く使用できるようになります。

重要

機能ロックポリシーで以下の iOS 機能を無効にする必要があります。これらの設定を無効にしないと、ダウンロードしたファイルを他のアプリで開くことができるため、管理対象 Safari Web ドメインの設定は効果がありません。

- その他のアプリ内の管理対象アプリからドキュメントを開く (7.0 以降)
- 管理対象アプリ内のその他のアプリからドキュメントを開く (7.0 以降)

管理対象ドメインポリシーを設定するには、[ポリシー] をクリックし、ポリシー名をクリックして [管理対象ドメインポリシー] をクリックします。

セキュリティポリシー

セキュリティ設定は [セキュリティポリシー] 画面で設定できます。

[セキュリティポリシー] 画面では、Android デバイスの Web 脅威検出ポリシーも管理できます。また、Web 脅威検出ログを Android デバイスからサーバに戻すこともできます。

注意

Mobile Security での Web 脅威検出でサポートされるのは、Android モバイルデバイスの初期設定のブラウザと Google Chrome のみです。

セキュリティ保護ポリシーを設定するには、[ポリシー] をクリックし、ポリシー名をクリックして [セキュリティポリシー] をクリックします。

次の表に、このポリシーで設定できる項目を示します。

表 5-3. セキュリティポリシーの設定

セクション	項目	説明	サポートされるモバイルデバイスの OS
セキュリティ設定	インストールされているアプリのみを検索する	インストールされているアプリのみを検索する場合はこのオプションを選択します。	
	インストールされているアプリとファイルを検索する	インストールされているアプリに加え、モバイルデバイスに保存されている他のファイルも検索する場合はこのオプションを選択します。 このオプションを選択する場合は、APK ファイルだけを検索するかすべてのファイルを検索するかを指定します。	
	パターンファイルのアップデート後に検索	パターンファイルのアップデート後に不正プログラム検索を毎回実行する場合はこのオプションを有効にします。 Android デバイスのパターンファイルのアップデート後、	

セクション	項目	説明	サポートされるモバイルデバイスのOS
		Mobile Security が自動的に検索を実行します。	
	アプリ検索	不正プログラム、プライバシーリスク、脆弱なアプリ、改ざん (偽装) されたアプリを検索する場合はこのオプションを有効にします。	
	ネットワークセキュリティ検索	ネットワークトラフィックの復号、安全でないアクセスポイント (Wi-Fi)、インストールされた不正な SSL 証明書を検索するための設定です。このカテゴリのオプションは初期設定ですべて有効になっており、変更することはできません。	
	脆弱なアプリ検索	USB デバッグ、開発者オプション、不正なプロファイル、root 化、Jailbreak など、モバイルデバイスの脆弱性を検索するための設定です。	
	ネットワークトラフィックの復号が検出されたときにネットワークをブロック	通信中にデータの漏えいが検出されたときにネットワークトラフィックの復号を中止する場合はこのオプションを有効にします。	
	危険度が高い不審アクセスポイント (Wi-Fi) が検出されたときにネットワークをブロック	偽装されている可能性がある不審ネットワーク接続が検出されたときにモバイルデバイスをネットワークから切断する場合はこのオプションを有効にします。	
	予約検索を有効にする (検索スケジュール)	検索を毎日、週 1 回、または月 1 回のいずれの頻度で実行する	

セクション	項目	説明	サポートされるモバイルデバイスの OS
		かに応じて、[毎日]、[毎週]、または [毎月] のいずれかを選択します。	
Web 脅威検出の設定	Web 脅威検出ポリシーのサーバ側の制御を有効にする	この機能により、Web 脅威検出ポリシーをサーバ側で制御できます。要件に応じて、次の保護レベルを設定できます。 • 低: この設定では、オンライン詐欺や、Web サイトから実行されるその他の悪意あるアクティビティに 対する最低限の保護が提供されます。 • 正常: この設定では、オンラインのセキュリティの脅威に対する保護が提供されます。ほとんどの Web サイトはブロックされません。この初期設定を選択することをお勧めします。 • 高: この設定では、オンライン詐欺や、その他の Web サイトに対するほとんどの保護が提供されます。評価が高い Web サイトの表示は許可され、その他のサイトはすべてブロックされます。	
	フィルタリスト	Mobile Security では、ブロックリストに追加されたすべての URL をブロックし、承認済みリストに追加されたすべての URL を許可します。	

セクション	項目	説明	サポートされるモバイルデバイスの OS
	URL の再評価	URL の分類に誤りがあると思われる場合、それらの URL を次の Web サイトからトレンドマイクロに連絡できます。 https://jp.sitesafety.trendmicro.com/	

迷惑メール対策ポリシー

Mobile Security の迷惑メール対策ポリシーを使用すると、迷惑 WAP プッシュや迷惑 SMS から保護できます。

迷惑メール対策ポリシーを設定するには、[ポリシー] をクリックし、ポリシー名をクリックして [迷惑メール対策ポリシー] をクリックします。

迷惑 SMS 対策ポリシー

注意

この機能はサポートされなくなりました。

この機能により、迷惑 SMS 対策ポリシーをサーバ側で制御できます。迷惑 SMS 対策ポリシーの設定時に指定できる機能は、次のとおりです。

- モバイルデバイスの迷惑 SMS 対策を有効または無効にする。
- ブロックリスト、除外リストを使用するようにモバイルデバイスを設定する、またはモバイルデバイスの迷惑 SMS 対策機能を無効にする。
- 管理コンソールから除外リストを設定する。
- 管理コンソールからブロックリストを設定する。

承認済みフィルタリストまたはブロックフィルタリストの 設定に関する詳細については、次の表を参照してください。

表 5-4. 迷惑 SMS 対策ポリシーのフィルタリストに関する設定

中央制御	ユーザ制御	説明
無効	有効	ユーザは Mobile Device エージェントの承認済み/ブロックリストを編集できます。 Mobile Security では、次の優先順位に基づいてメッセージが許可またはブロックされます。 1. Mobile Device エージェントの承認済みリスト 2. Mobile Device エージェントのブロックリスト
有効	無効	ユーザは Mobile Device エージェントの承認済み/ブロックリストのみを編集できます。 Mobile Security では、次の優先順位に基づいてメッセージが許可またはブロックされます。 1. サーバの承認済みリストまたはブロックリスト 2. Mobile Device エージェントの承認済みリスト 3. Mobile Device エージェントのブロックリスト
有効	有効	ユーザは管理者によって定義された承認済み/ブロックリストを表示または編集でき、Mobile Device エージェントの承認済み/ブロックリストも使用できます。 セキュリティポリシーが Mobile Device エージェントと同期されると、フィルタリストは同期されず、他のすべての 設定がポリシーに従ってアップデートされます。 Mobile Security では、次の優先順位に基づいてメッセージが許可またはブロックされます。 1. Mobile Device エージェントの承認済みリスト 2. Mobile Device エージェントのブロックリスト 3. サーバの承認済みリストまたはブロックリスト

注意

SMS 除外リストおよびブロックリストでは、「[name1]:number1;[name2]:number2;...」の形式を使用する必要があります。

name の長さは 30 文字以内です。電話番号の長さは 4〜20 文字で、0〜9、+、-、#、(、)、スペースを使用できます。最大エントリ数は 200 です。

迷惑 WAP プッシュ対策ポリシー

注意

この機能はサポートされなくなりました。

この機能により、WAP プッシュ対策をサーバ側で制御できます。有効になっている場合、WAP 除外リストを使用するかどうかを選択できます。

注意

WAP 除外リストでは、「[name1]:number1;[name2]:number2;...」の形式を使用する必要があります。

name の長さは 30 文字以内です。電話番号の長さは 4〜20 文字で、0〜9、+、-、#、(、)、スペースを使用できます。最大エントリ数は 200 です。

次に、WAP プッシュ対策ポリシーの設定時に指定可能な機能の一覧を示します。

- モバイルデバイスの WAP プッシュ対策を有効または無効にする。
- 除外リストを使用するようにモバイルデバイスを設定する、またはモバイルデバイスの WAP プッシュ対策を無効にする。
- 管理コンソールから除外リストを設定する。
- 管理者がサーバ側の制御を有効にしている場合、ユーザは管理者によって定義されている種類の WAP プッシュ対策を変更することはできない。
- 管理者がサーバ側の制御を無効にし、モバイルデバイスでのユーザによる Mobile Security の設定を許可している場合、ユーザは管理者によって設定されている WAP プッシュ対策リストの表示または編集を行うこと

はできないが、モバイルデバイス側の個人の WAP プッシュ対策リストを編集することはできる。

注意

不要なメッセージに対するユーザの個人設定は、迷惑メール対策ポリシーが Mobile Device エージェントに適用された後にクリアされます。

着信フィルタポリシー

注意

この機能はサポートされなくなりました。

この機能により、着信フィルタポリシーをサーバ側で制御できます。着信フィルタポリシーを設定するには、[ポリシー] をクリックし、ポリシー名をクリックして [フィルタポリシー] をクリックします。

着信フィルタポリシーの設定時に指定できる機能は、次のとおりです。

- モバイルデバイスの着信フィルタ機能を有効または無効にする。
- モバイルデバイスでブロックリストまたは承認済みリストを使用するように設定する。
- 管理コンソールから除外リストを設定する。
- 管理コンソールからブロックリストを設定する。

承認済みフィルタリストまたはブロックフィルタリストの 設定に関する詳細については、次の表を参照してください。

表 5-5. 着信フィルタポリシーのフィルタリストに関する設定

中央制御	ユーザ制御	説明
無効	有効	ユーザは Mobile Device エージェントの承認済み/ブロックリストを編集できます。 Mobile Security では、次の優先順位に基づいて URL が許可またはブロックされます。 1. Mobile Device エージェントの承認済みリスト 2. Mobile Device エージェントのブロックリスト
有効	無効	ユーザは Mobile Device エージェントの承認済み/ブロックリストのみを編集できます。 Mobile Security では、次の優先順位に基づいて着信が許可またはブロックされます。 1. サーバのブロックリスト 2. Mobile Device エージェントの承認済みリスト 3. Mobile Device エージェントのブロックリスト Android デバイスでは、発信に対するサーバ側制御も設定できます。
有効	有効	ユーザは管理者によって定義された承認済み/ブロックリストを表示または編集でき、Mobile Device エージェントの承認済み/ブロックリストも使用できます。 セキュリティポリシーが Mobile Device エージェントと同期されると、フィルタリストは同期されず、他のすべての設定がポリシーに従ってアップデートされます。 Mobile Security では、次の優先順位に基づいて着信が許可またはブロックされます。 1. Mobile Device エージェントの承認済みリスト 2. Mobile Device エージェントのブロックリスト 3. サーバのブロックリスト Android デバイスでは、発信に対するサーバ側制御も設定できます。

注意

着信フィルタ承認済みリストおよびブロックリストでは、「[name1:]number1; [name2:]number2;...」の形式を使用する必要があります。

name の長さは 30 文字以内です。電話番号の長さは 4〜20 文字で、0〜9、+、-、#、(、)、スペースを使用できます。最大エントリ数は 200 です。

パスワードポリシー

パスワードポリシーを使用すると、モバイルデバイスのデータへの不正アクセスを阻止できます。

パスワードポリシーを設定するには、[ポリシー] をクリックし、ポリシー名をクリックして、左側のメニューにある [パスワードポリシー] をクリックします。

機能ロックポリシー

この機能を使用すると、モバイルデバイスの特定の機能またはコンポーネントの使用を制限 (無効化) または許可 (有効化) することができます。たとえば、特定のグループ内にあるすべてのモバイルデバイスのカメラを無効にできます。

注意

テザリング機能はサポートされなくなりました。

機能ロックポリシーを設定するには、[ポリシー] をクリックし、ポリシー名をクリックして、左側のメニューにある [機能ロックポリシー] をクリックします。

サポートされる機能/コンポーネントについては、37 ページの「サポートされるモバイルデバイスの OS の機能」を参照してください。

警告!

WLAN/WIFI および Microsoft ActiveSync を無効にするときは注意が必要です。これらのオプションが両方とも使用できない場合、モバイルデバイスはサーバと通信できません。

Android デバイスの場合、アクセスポイントを追加し、これらのアクセスポイントの範囲内でモバイルデバイスの機能を使用可能にするかどうかを制御できます。

コンプライアンスポリシー

コンプライアンスポリシーを使用すると、モバイルデバイスのコンプライアンス条件を設定できます。いずれかのモバイルデバイスが条件に一致しない場合、Mobile Security のサーバ UI にはコンプライアンス違反のステータスが表示されます。また、Mobile Security では、コンプライアンスに違反している iOS デバイスにメールを送信します。一方、コンプライアンスに違反している Android デバイスには通知が表示されます。コンプライアンスチェックリストには、次のものが含まれています。

- root 化/Jailbreak: モバイルデバイスが root 化されているかどうか、またはモバイルデバイスが Jailbreak しているかどうかを確認します。
- 暗号化なし: モバイルデバイスで暗号化が有効になっているかどうかを確認します。
- OS バージョンチェック: OS のバージョンが定義済みの条件に一致するかどうかを確認します。

コンプライアンスポリシーを設定するには、[ポリシー] をクリックし、ポリシー名をクリックして [コンプライアンスポリシー] をクリックします。

アプリの監視および制御ポリシー

アプリの監視および制御ポリシーを使用すると、モバイルデバイスにインストールされているアプリケーションをサーバ側で制御したり、必須のアプリケーションをモバイルデバイスに配信したりできます。

アプリの監視および制御ポリシーを設定するには、[ポリシー]をクリックし、ポリシー名をクリックして [アプリの監視および制御ポリシー] をクリックします。

- 必須アプリ: このオプションを使用すると、リストに追加するすべてのアプリケーションがモバイルデバイスに配信されます。VPN とアプリケーションをリンクして、アプリケーションが常にその VPN を使用してネットワークに接続するように設定することもできます。
- 許可するアプリ: 承認済みリストおよびブロックリストを使用して、モバイルデバイスにインストールするアプリケーションを 制御します。

  iOS デバイスの場合、Mobile Security は、管理者とポリシーに準拠していないアプリケーションのユーザに通知を送信します。

  Android デバイスの場合、Mobile Security は、ポリシーに準拠していないアプリケーションをブロックし、その他のアプリケーションをすべて許可します。

  - システムアプリのブロックを 有効にする (Android のみ):

    Android デバイスのすべてのシステムアプリをブロックします 。
  - アプリのカテゴリを有効にする: モバイルデバイスで有効または無効にするアプリのカテゴリを選択します。これらのカテゴリに属するアプリケーションを承認済みリストまたはブロックリストに追加して、例外を作成することもできます。たとえば、[ゲーム] カテゴリを無効にした場合、このカテゴリに属するすべてのアプリケーションは、承認済みリストに入っていない限り Mobile Security によってブロックされます。

    Mobile Security では、次の優先順位に従ってアプリケーションが許可またはブロックされます。

    1. 承認済みリスト: 無効化されたカテゴリに属するアプリケーションであっても、承認済みリスト内にあるアプリケーションは許可されます。
    2. ブロックリスト: 有効化されたカテゴリに属するアプリケーションであっても、ブロックリスト内にあるアプリケーションはブロックされます。

3. アプリの許可: アプリケーションが属するカテゴリに対してユーザが選択した許可ステータスに基づいて、アプリケーションを許可またはブロックします。

- アプリの許可を有効にする (Android のみ): Android デバイスで有効または無効にするアプリケーションサービスを選択します。これらのサービスを使用するアプリケーションを承認済みリストまたはブロックリストに追加して、除外することもできます。たとえば、[データの読み取り] サービスタイプを無効にした場合、データの読み取りサービスを使用するすべてのアプリケーションは、承認済みリストに入っていない限り Mobile Security によってブロックされます。

  Mobile Security では、次の優先順位に従ってアプリケーションが許可またはブロックされます。

  1. 承認済みリスト: 無効化されているサービスを使用するアプリケーションであっても、承認済みリスト内にあるアプリケーションの場合、そのアプリケーションの使用は許可されます。
  2. ブロックリスト: 有効化されているサービスを使用するアプリケーションであっても、ブロックリスト内にあるアプリケーションの場合、そのアプリケーションの使用はブロックされます。
  3. アプリケーション許可: アプリケーションで使用されるサービスに対してユーザが選択した許可ステータスに基づいて、アプリケーションを許可またはブロックします。

- 次のアプリのみを許可する: ユーザにモバイルデバイスでの使用を許可するアプリケーションを承認済みリストに追加します。有効にすると、次のようになります。
  - 承認済みリストにないアプリケーションが検出された場合、Android デバイスではポップアップ警告メッセージが表示されます。
  - iOS デバイスではユーザにメール通知が送信されます。
- 次のアプリのみをブロックする: ユーザにモバイルデバイスでの使用を許可しないアプリケーションをブロックリストに追加します。有効にすると、次のようになります。

- ブロックリストにあるアプリケーションが検出された場合、Android デバイスではポップアップ警告メッセージが表示されます。
- iOS デバイスではユーザにメール通知が送信されます。

- アプリのロック (監視モードの場合のみ): iOS デバイスで使用するアプリケーションを特定のものに制限します。

Mobile Security は、次のいずれかの方法で、禁止されたアプリケーションを検索してユーザにメールアラートを送信します。

- [管理] > [コミュニケーションサーバの設定] > [共通設定] タブにある [情報を収集する頻度] の設定に従って自動的に実行
- [管理] > [コミュニケーションサーバの設定] > [共通設定] タブにある [情報を収集する頻度] の設定をアップデートしたときに実行

Volume Purchasing Program ポリシー

このポリシーを使用すると、管理者は、Apple の Volume Purchase Program から購入した iOS アプリを、Mobile Security の Web 管理コンソールにインポートできます。Mobile Security は、Volume Purchasing Program リストに含まれるすべてのアプリを、グループ内のモバイルデバイスに配信します。

Volume Purchasing Program ポリシーを設定するには、次の手順を実行します。

1. アプリをエンタープライズアプリストアに 追加します。手順については、142 ページの「アプリケーションを追加する」を参照してください。
2. [ポリシー] をクリックし、ポリシー名をクリックして [Volume Purchasing Program ポリシー] をクリックします。
3. [インポート] をクリックし、インポートするアプリをエンタープライズアプリストアから選択します。
4. [保存] をクリックして、すべてのアプリを iOS デバイスに配信します。

コンテナポリシー

このポリシーを使用すると、Samsung KNOX コンテナのセキュリティ設定を管理できます。アカウントの承認済みリストまたはブロックリストの設定、制約の適用、およびブラウザ、パスワード、アプリの設定を行うことができます。

注意

このポリシーを有効にする前に、Mobile Security で KNOX のライセンスを設定する必要があります。KNOX のライセンスを設定するには、Web 管理コンソールで [管理] > [製品ライセンス] の順に選択します。

- アカウントの設定: 承認済みリストとブロックリストを使用して、Samsung KNOX コンテナへの追加を許可または制限するアカウントを指定します。
- 制約の設定: Samsung KNOX コンテナでのカメラまたはファイル共有を無効にします。
- ブラウザの設定: Samsung KNOX コンテナのネイティブの Android Web ブラウザのセキュリティ設定を行います。
- パスワード設定: Samsung KNOX コンテナのパスワードのセキュリティ設定を行います。
- アプリの設定: 次のリストを設定します。
  - フィルタアプリリスト : 承認済みリストまたはブロックリストを設定して、Samsung KNOX コンテナへのアプリのインストールを制限します。
  - 必須アプリ : 必須アプリリストを設定して、Samsung KNOX にインストールする必要があるアプリを指定します。
  - 無効化されたアプリ : 無効化されたアプリリストを設定して、モバイルデバイスで特定のアプリを無効にします。このリストのアプリがモバイルデバイスにインストールされた場合、削除はされませんが、ユーザがそれらのアプリを使用することはできません。

コンテナポリシーを設定するには、[ポリシー] をクリックし、ポリシー名をクリックして [コンテナポリシー] をクリックします。

すべてのグループのポリシーの 管理

Mobile Security では、初期設定のポリシーテンプレートを使用して、ポリシーを簡単に作成できます。

モバイルデバイスのポリシーを作成、編集、コピー、または削除するには、[すべてのグループのポリシー] 画面を使用します。

ポリシーを作成する

手順

1. Mobile Security の Web 管理コンソールにログオンします。
2. メニューバーの [ポリシー] > [グループのポリシー] をクリックします。

   [ポリシー] 画面が表示されます。
3. [作成] をクリックします。

   [ポリシーの作成] 画面が表示されます。
4. 該当するフィールドにポリシーの名前と説明を入力し、[保存] をクリックします。

   Mobile Security では、初期設定を使用してポリシーが作成されます。ただし、グループにはポリシーが割り当てられません。グループにポリシーを割り当てるには、137 ページの「グループのポリシーを割り当てまたは削除する」を参照してください。
5. (最上位の管理者のみ) このポリシーをテンプレートとして使用する場合は、[ポリシー] 画面の [種類] 列にある矢印ボタンをクリックします。グループ管理者は、最上位の管理者が作成したテンプレートを使用して担当するグループのポリシーを作成できます。

注意

- テンプレートをグループに割り当てることはできません。
- テンプレートをポリシーに変換することもできます。ただし、ポリシーに変換できるのは、どのグループにも割り当てられていないテンプレートだけです。

ポリシーを編集する

手順

1. Mobile Security の Web 管理コンソールにログオンします。
2. メニューバーの [ポリシー] > [グループのポリシー] をクリックします。

   [ポリシー] 画面が表示されます。
3. ポリシーリストで、編集する詳細を含むポリシー名をクリックします。

   [ポリシーの編集] 画面が表示されます。
4. ポリシーの詳細を変更し、[保存] をクリックします。

グループのポリシーを割り当てまたは削除する

手順

1. Mobile Security の Web 管理コンソールにログオンします。
2. メニューバーの [ポリシー] > [グループのポリシー] をクリックします。

   [ポリシー] 画面が表示されます。
3. ポリシーの [適用するグループ] 列で、グループ名をクリックします。グループにポリシーが割り当てられていない場合は、[なし] をクリックします。
4. 次のいずれかを実行します。

- グループにポリシーを割り当てるには、左側の [使用できるグループ] リストでポリシーを適用するグループを選択し、[>] をクリックしてグループを右側に移動します。
- グループからポリシーを削除するには、右側のグループリストで削除するグループを選択し、[<] をクリックしてグループを左側の [使用できるグループ] リストに移動します。

5. [保存] をクリックします。

ポリシーをコピーする

手順

1. Mobile Security の Web 管理コンソールにログオンします。
2. メニューバーの [ポリシー] > [グループのポリシー] をクリックします。

   [ポリシー] 画面が表示されます。
3. コピーするポリシーを選択し、[コピー] をクリックします。

ポリシーを削除する

初期設定ポリシーおよびグループに適用されているポリシーを削除することはできません。ポリシーを削除する前に、すべてのグループからポリシーを削除してください。手順については、137 ページの「グループのポリシーを割り当てまたは削除する」を参照してください。

手順

1. Mobile Security の Web 管理コンソールにログオンします。
2. メニューバーの [ポリシー] > [グループのポリシー] をクリックします。

   [ポリシー] 画面が表示されます。

3. 削除するポリシーを選択し、[削除] をクリックします。

アプリの使用可能状況を設定する

Mobile Security では、特定のポリシーに応じて、iOS および Android デバイスで使用可能にするアプリを設定できます。

手順

1. Mobile Security の Web 管理コンソールにログオンします。
2. メニューバーの [ポリシー] > [グループのポリシー] をクリックします。

   [ポリシー] 画面が表示されます。
3. [使用可能なアプリ] 列で、ポリシーに対するアプリの数をクリックします。

   [使用可能なアプリ] 画面が表示されます。
4. [iOS アプリ] タブまたは [Android アプリ] タブをクリックします。
5. 次のいずれかを実行します。
   - アプリを有効または無効にするには、そのアプリの [許可] 列にあるボタンをクリックして切り替えます。
   - すべてのアプリを有効または無効にするには、[すべてを有効にする] または [すべてを無効にする] をクリックします。
6. [許可] 列のアプリの使用可能状況が切り替わります。

第 6 章

アプリケーションの管理

この章では、iOS モバイルデバイスおよび Android モバイルデバイスでの、検出された不正なアプリケーションの管理方法と、SSL 証明書および iOS プロファイルの表示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。

エンタープライズアプリストアについて

エンタープライズアプリストアでは、Android デバイスや iOS デバイスにダウンロードしてインストールするための、ファイルおよびアプリのリストを作成できます。

また、Mobile Security の Web 管理コンソールで、Apple の Volume Purchase Program から購入した iOS アプリをエンタープライズアプリストアにアップロードすることもできます。

エンタープライズアプリの管理

アプリケーションを追加する

手順

1. Mobile Security の Web 管理コンソールで、[アプリ] > [エンタープライズアプリストア] の順に選択します。

   [エンタープライズアプリストア] 画面が表示されます。

2. [Android] タブまたは [iOS] タブをクリックします。

3. [追加] をクリックします。

   [アプリの追加] 画面が表示されます。

4. 次のいずれかのオプションを使用して、リストにアプリケーションを追加できます。

   - ローカルコンピュータから追加: Android デバイスと iOS デバイスのインストールファイルを選択します。
   - Web クリップの追加: アプリケーションの URL を入力すると、アプリケーションのアイコンがユーザのモバイルデバイスのホーム 画面に表示され、モバイルデバイスの初期設定の Web ブラウザでリンクが開きます。
   - (Android) 外部のアプリストアから追加: 外部のアプリストアのアプリケーションへのリンクを入力します。アプリケーションのアイコ

ンがユーザのモバイルデバイスのホーム画面に表示され、モバイルデバイスの初期設定の Web ブラウザでリンクが開きます。

- (iOS) iTunes Store のアプリへのリンクを追加: Apple の App Store で検索する VPP アプリケーションの名前を入力し、アプリケーションを検索する国を選択して、追加するアプリケーションを検索結果から選択します。追加した VPP アプリケーションは、Mobile Security の Web 管理コンソールの [アプリストア] でのみ使用できます。アプリケーションをモバイルデバイスに配信するには、そのアプリケーションを Volume Purchasing Program ポリシーに追加する必要があります。手順については、134 ページの「Volume Purchasing Program ポリシー」を参照してください。

5. [Continue] をクリックします。

   [アプリの編集] 画面が表示されます。

6. 次の設定を行います。

   - アプリ名: アプリケーションの名前を入力します。
   - アプリのアイコン : アプリケーションのアイコンが 表示されない場合は、[アプリのアイコンのアップロード] をクリックし、アイコンを選択してアップロードします。
   - パッケージ名: パッケージ名が表示されない場合は、パッケージ名を入力します。
   - VPP コードファイル: iOS VPP アプリケーションの場合は、Apple から送信された Volume Purchase Code のファイルをアップロードします。
   - カテゴリ : アプリケーションのカテゴリを選択します。

     注意

     リストからカテゴリを選択する必要があります。カテゴリを追加または削除するには、[カテゴリ] ボタンをクリックします。

   - 説明: アプリケーションの説明を入力します。
   - 公開方法: 次のいずれかを選択します。

- 公開しない: サーバにアプリケーションをアップロードしますが、モバイルデバイスには公開しません。
- 製品版として公開: サーバにアプリケーションをアップロードして、モバイルデバイスからダウンロードできるように公開します。
- ベータ版として公開: サーバにアプリケーションをアップロードして、ベータ版としてモバイルデバイスからダウンロードできるように公開します。

- スクリーンショット: アプリケーションのスクリーンショットを選択してアップロードします。

7. [Continue] をクリックします。

   アプリケーションのリストにアプリケーションが 表示されます。

アプリケーション情報を編集する

手順

1. Mobile Security の Web 管理コンソールで、[アプリ] > [エンタープライズアプリストア] の順に選択します。

   [エンタープライズアプリストア] 画面が表示されます。

2. [Android] タブまたは [iOS] タブをクリックします。
3. 情報を編集するアプリケーションの名前をクリックします。

   [アプリの編集] 画面が表示されます。

4. 画面上で詳細を変更します。
5. [Continue] をクリックします。

アプリストアからアプリケーションを削除する

手順

1. Mobile Security の Web 管理コンソールで、[アプリ] > [エンタープライズアプリストア] の順に選択します。

   [エンタープライズアプリストア] 画面が表示されます。

2. [Android] タブまたは [iOS] タブをクリックします。
3. 削除するアプリケーションを選択します。
4. [削除] をクリックし、確認画面で [OK] をクリックします。

アプリケーションのカテゴリの管理

アプリケーションのカテゴリを追加する

手順

1. Mobile Security の Web 管理コンソールで、[アプリ] > [エンタープライズアプリストア] の順に選択します。

   [エンタープライズアプリストア] 画面が表示されます。

2. [Android] タブまたは [iOS] タブをクリックします。
3. [カテゴリの管理] をクリックします。
4. [追加] をクリックします。

   [カテゴリの追加] 画面が表示されます。

5. カテゴリの名前と説明を入力し、[保存] をクリックします。

アプリケーションのカテゴリを編集する

手順

1. Mobile Security の Web 管理コンソールで、[アプリ] > [エンタープライズアプリストア] の順に選択します。

   [エンタープライズアプリストア] 画面が表示されます。

2. [iOS アプリ] タブまたは [Android アプリ] タブをクリックします。
3. [カテゴリの管理] をクリックします。
4. 編集するカテゴリ名をクリックします。

   [カテゴリの編集] 画面が表示されます。

5. カテゴリの詳細を変更し、[保存] をクリックします。

アプリケーションのカテゴリを削除する

手順

1. Mobile Security の Web 管理コンソールで、[アプリ] > [エンタープライズアプリストア] の順に選択します。

   [エンタープライズアプリストア] 画面が表示されます。

2. [Android] タブまたは [iOS] タブをクリックします。
3. [カテゴリの管理] をクリックします。
4. 削除するカテゴリを選択して、[削除] をクリックし、表示される確認画面で [OK] をクリックします。

Volume Purchase Program で購入したアプリの管理

重要

VPP は、地域によっては利用できないことがあります。利用可能な地域などの詳細については、次のサイトを参照してください。

http://www.apple.com/business/vpp/

Apple では、アプリをまとめて購入する際の方法として、引き換えコードと Volume Purchase Program (VPP) ライセンスの 2 種類の方法を採用しています。引き換えコードを VPP ライセンスに変更することはできないため、Mobile Security では両方のオプションをサポートしています。

Volume Purchase Program に登録すると、iOS アプリの VPP ライセンスをユーザやデバイスに配布できます。

残りのライセンス数を監視したり、ライセンスの割り当てを変更したりして、VPP アプリを管理することができます。ユーザは、自分のモバイルデバイスに Mobile Security クライアントアプリがインストールされていなくても VPP アプリを使用できます。

注意

Mobile Security では、モバイルデバイスに VPP アプリを自動配信しません。ユーザが Apple の App Store から各自のモバイルデバイスに手動でダウンロードする必要があります ([App Store] > [アップデート] > [購入済み] にあります)。

Volume Purchase Program ライセンスを設定する

手順

1. 次の URL に移動します。

   http://www.apple.com/business/vpp/

2. Apple アカウントでログインし、Apple Volume Purchase Program Web ポータルからサービストークンファイルをダウンロードします。

3. Mobile Security の Web 管理コンソールで、[アプリ] > [エンタープライズアプリストア] > [iOS] の順に選択します。

   [iOS エンタープライズアプリストア] 画面が表示されます。

4. [Volume Purchase Program (VPP) 管理] > [VPP 設定] の順に選択します。

5. Apple Web ポータルからダウンロードしたトークンファイルをアップロードし、処理が完了するまで待ちます。

6. [今すぐ同期] をクリックします。

VPP ライセンスの割り当てと回収を行う

Mobile Security では、Volume Purchase Program で購入したアプリのライセンスをユーザやデバイスに割り当てたり回収したりできます。

重要

アプリの割り当てや回収を行うには、Volume Purchase Program ライセンスの設定を完了しておく必要があります。

詳細については、147 ページの「Volume Purchase Program ライセンスを設定する」を参照してください。

手順

1. Mobile Security の Web 管理コンソールで、[アプリ] > [エンタープライズアプリストア] > [iOS] > [Volume Purchase Program (VPP) 管理] の順に選択します。

2. [アプリリスト] でアプリを探し、[割り当て/回収] をクリックします。

   [ライセンスの割り当て/回収] 画面が表示されます。

3. ライセンスを割り当てるには、次の手順を実行します。

   - ライセンスをデバイスに割り当てる場合

     a. [モバイルデバイス] タブで、ステータスが割り当て解除済みのデバイスを選択します。

b. [割り当て] をクリックします。

注意

Volume Purchasing Program には、デバイスへのアプリの割り当てに関して次の制限があります。

- VPP アプリを割り当てることができるのは、iOS 9 以降を実行しているデバイスのみです。
- アプリ開発者がデバイスへの割り当てを許可している必要があります。

- ライセンスをユーザに割り当てる場合

  a. [ユーザ] タブで、ステータスが割り当て解除済みのユーザを選択します。

  b. [割り当て] をクリックします。

注意

VPP ライセンスが割り当てられると、Mobile Security からユーザに通知が送信されます。

ユーザへの通知の設定を変更するには、[通知とレポート] > [ユーザへの通知] > [VPP ユーザ通知] に移動します。

ライセンスが正常に割り当てられます。

4. ライセンスを回収するには、次の手順を実行します。

   - ライセンスをデバイスから 回収する場合

     a. [モバイルデバイス] タブで、ステータスが割り当て済みのデバイスを選択します。

     b. [回収] をクリックします。

   - ライセンスをユーザから回収する場合

     a. [ユーザ] タブで、ステータスが割り当て済みのユーザを選択します。

b. [回収] をクリックします。

ライセンスが正常に回収されます。

VPP ユーザのステータスを確認する

手順

1. Mobile Security の Web 管理コンソールで、[アプリ] > [エンタープライズアプリストア] > [iOS] の順に選択します。

   [iOS エンタープライズアプリストア] 画面が表示されます。

2. [Volume Purchase Program (VPP) 管理] > [VPP ユーザリスト] の順に選択します。

3. [ステータス] 列でユーザのステータスを確認します。

   [ステータス] 列には、次のいずれかのステータスが表示されます。

   - -: ユーザにアプリがまだ割り当てられていません。
   - 登録済み: ユーザに少なくとも 1 つのアプリが割り当てられていますが、ユーザの Apple ID とメールアドレスがまだ関連付けられていません。
   - 割り当て済み: ユーザに少なくとも 1 つのアプリが割り当てられており、ユーザの Apple ID とメールアドレスがすでに関連付けられています。
   - 回収済み: ユーザに割り当てられたすべてのライセンスを回収済みです。

ユーザからすべてのライセンスを回収する

Mobile Security では、ユーザからすべてのライセンスを回収することができます。

手順

1. Mobile Security の Web 管理コンソールで、[アプリ] > [エンタープライズアプリストア] > [iOS] の順に選択します。

   [iOS エンタープライズアプリストア] 画面が表示されます。

2. [Volume Purchase Program (VPP) 管理] > [VPP ユーザリスト] の順にクリックします。

3. リストからユーザを選択し、[回収] をクリックします。

4. [ユーザリスト] 画面で [閉じる] をクリックします。

インストール済みアプリについて

[インストール済みアプリ] 画面には、管理対象の Android デバイスおよび iOS デバイスにインストールされているすべてのアプリのリストが 表示されます。

この画面に表示されたアプリが安全である場合は、それらのアプリを [承認済みリスト] に追加することもできます。同様に、以前に [承認済みリスト] に追加したアプリを安全でないと判断した場合は、それらのアプリをリストから削除することもできます。

手順については、113 ページの「アプリを承認済みリストに追加する」および 114 ページの「アプリを承認済みリストから削除する」を参照してください。

テーブルの右上にある [承認済みリストの管理] リンクをクリックすると、[承認済みリスト] 画面に移動してリストを管理できます。

次の表に、Android および iOS のアプリについて確認できる情報を示します。

表 6-1. インストール済みアプリの情報

情報	説明	ANDROID	IOS
アプリ名	アプリの名前	●	●
バージョン	アプリのバージョン番号	●	●

情報	説明	ANDROID	IOS
インストール数	アプリがインストールされているデバイスの数	●	●

インストール済みアプリを表示する

手順

1. Mobile Security の Web コンソールで、[アプリ] > [インストール済みのアプリ] の順に選択します。

   [インストール済みのアプリ] タブが表示されます。

2. [Android] タブまたは [iOS] タブをクリックします。

3. アプリがインストールされたデバイスを確認するには、[インストール数] 列の数字をクリックします。

   [モバイルデバイス] 画面が表示され、[管理対象デバイス] タブにデバイスのリストが表示されます。

4. 特定のアプリの情報を確認するには、[検索] バーにアプリ名を入力し、<Enter> キーを押します。

   該当するアプリがリストにあれば、そのアプリの情報がテーブルに表示されます。

第 7 章

検出項目の表示と管理

この章では、iOS モバイルデバイスおよび Android モバイルデバイスでの、検出された不正なアプリケーションの管理方法と、SSL 証明書および iOS プロファイルの表示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。

[不審アプリ] 画面について

[不審アプリ] 画面には、モバイルデバイスにインストールされているすべてのアプリについて、アプリの名前、バージョン、セキュリティ検索ステータス、インストール数、および前回検索した日時が表示されます。

この画面に表示されたアプリが安全である場合は、それらのアプリを [承認済みリスト] に追加することもできます。同様に、以前に [承認済みリスト] に追加したアプリを安全でないと判断した場合は、それらのアプリをリストから削除することもできます。

手順については、113 ページの「アプリを承認済みリストに追加する」および114 ページの「アプリを承認済みリストから削除する」を参照してください。

テーブルの右上にある [承認済みリストの管理] リンクをクリックすると、[承認済みリスト] 画面に移動してリストを管理できます。

次の表に、Android および iOS のアプリについて確認できる情報を示します。

表 7-1. アプリのセキュリティステータス

情報	説明	ANDROID	IOS
アプリ名	アプリの名前	●	●
バージョン	アプリのバージョン番号	●	●

情報	説明	ANDROID	IOS
不正プログラム検索の結果	不正プログラム検索の結果として、次のいずれかが表示されます。 • 正常: 不正プログラムは検出されませんでした。 • PUA: Potentially Unwanted Application (PUA) は、ユーザのセキュリティやプライバシーに高いリスクをもたらす可能性があるグレーウェアアプリです。 詳細については、https://www.trendmicro.com/vinfo/jp/security/definition/potentially-unwanted-app を参照してください。 • 不正プログラム: 既知の不正プログラムです。 • 不明: 情報がありません。	●	●
脆弱性検索の結果	脆弱性検索の結果として、次のいずれかの危険度が表示されます。 • 正常 • 中 • 高 • 不明: 情報がありません。	●	
アプリ権限チェックの結果	アプリ権限チェックの結果として、次のいずれかの危険度が表示されます。 • 正常 • 中 • 高 • 不明: 情報がありません。	●	

情報	説明	ANDROID	iOS
改ざんあり	改ざんアプリ検索の結果として、次のいずれかが表示されます。 • はい: 正規のアプリが不正な目的で改ざんまたは偽装されています。 • いいえ: 正規のアプリに対して改ざんは行われていません。 • 不明: 情報がありません。	●	●
インストール数	アプリがインストールされているデバイスの数	●	●
前回の検索	前回の検索日時	●	●

Mobile Security は、アプリのセキュリティリスクを検索した後、セキュリティ検索の結果に基づいて次の処理を行います。

- [Android/iOS アプリリスク情報] ウィジェットの [ダッシュボード] 画面に検出情報を表示する
- [モバイルデバイス] 画面の該当するカテゴリにモバイルデバイスで検出されたセキュリティリスクの数を表示する
- ログエントリを生成する

不審 Android アプリを表示する

手順

1. Mobile Security の Web コンソールで、[検出数] > [不審アプリ] > [Android] タブの順に選択します。

   [Android] タブが表示されます。

2. アプリに対する検索結果の詳細を確認するには、次の列の結果をクリックします。
   - 脆弱性検索の結果

- アプリ権限チェックの結果

選択した項目の検索結果の詳細画面が表示されます。

3. アプリがインストールされたデバイスを 確認するには、[インストール数] 列の数字をクリックします。

   [モバイルデバイス] 画面が表示され、[管理対象デバイス] タブにデバイスのリストが表示されます。

4. 特定のアプリの情報を確認するには、[検索] バーにアプリ名を入力し、<Enter> キーを押します。

   該当するアプリがリストにあれば、そのアプリの情報がテーブルに表示されます。

不審 iOS アプリを表示する

手順

1. Mobile Security の Web コンソールで、[検出数] > [不審アプリ] > [iOS] タブの順に選択します。

   [iOS] タブが表示されます。

2. アプリがインストールされたデバイスを 確認するには、[インストール数] 列の数字をクリックします。

   [モバイルデバイス] 画面が表示され、[管理対象デバイス] タブにデバイスのリストが表示されます。

3. 特定のアプリの情報を確認するには、[検索] バーにアプリ名を入力し、<Enter> キーを押します。

   該当するアプリがリストにあれば、そのアプリの情報がテーブルに表示されます。

不正な SSL 証明書を表示する

[不正な SSL 証明書] 画面には、Mobile Security で不正な SSL 証明書として検出された、Android デバイスまたは iOS デバイスにインストールされている証明書が表示されます。[不正な SSL 証明書] 画面に表示された証明書が信頼できる場合は、その証明書を 113 ページの「ネットワークトラフィックを復号する信頼された証明書リスト」に追加できます。追加した証明書は [不正な SSL 証明書] 画面に表示されなくなります。

Mobile Security は、不正な証明書を検出すると次の処理を行います。

- 不正な SSL 証明書を [不正な SSL 証明書] 画面に表示する
- [ネットワーク保護情報] ウィジェットの [ダッシュボード] 画面に検出情報を表示する
- デバイスのセキュリティステータスを [危険] に変更する
- 管理者に通知メールを送信する
- ログエントリを生成する

[不正な SSL 証明書] 画面に表示される証明書の詳細には、証明書の名前と詳細、モバイルデバイスへのインストール数、および前回検索した日時の情報が含まれます。

手順

1. Mobile Security の Web コンソールで、[検出数] > [不正な SSL 証明書] の順に選択します。

   [不正な SSL 証明書] 画面が表示されます。

2. [Android] タブまたは [iOS] タブをクリックします。

3. 特定のアプリの情報を確認するには、[検索] バーにアプリ名を入力し、<Enter> キーを押します。

   該当するアプリがリストにあれば、そのアプリの情報がテーブルに表示されます。

不正な iOS プロファイルを表示する

[不正な iOS プロファイル] 画面には、Mobile Security で不正な iOS プロファイルとして検出された、iOS デバイスにインストールされているプロファイルが表示されます。

Mobile Security は、不正な iOS プロファイルを検出すると次の処理を行います。

- 不正な iOS プロファイルを [不正な iOS プロファイル] 画面に表示する
- [iOS ネットワーク保護情報] ウィジェットの [ダッシュボード] 画面に検出情報を表示する
- デバイスのステータスを [危険] に変更する
- 管理者に通知メールを送信する
- ログエントリを生成する

[不正な iOS プロファイル] 画面に表示されるプロファイルの詳細には、プロファイルの名前、種類、検索結果、モバイルデバイスへのインストール数、および前回検索した日時の情報が含まれます。

手順

1. Mobile Security の Web コンソールで、[検出数] > [不正な iOS プロファイル] の順に選択します。

   [不正な iOS プロファイル] 画面が表示されます。

2. 特定の iOS プロファイルの情報を確認するには、[検索] バーに証明書名を入力し、<Enter> キーを押します。

   該当する証明書がリストにあれば、そのアプリの情報がテーブルに表示されます。

第 8 章

ログの表示と管理

この章では、Mobile Security の Web 管理コンソールでログを表示する方法と、ログの削除を設定する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。

ログについて

Mobile Security では、次の種類のログが記録されます。

- 管理者ログ: 管理者が Web 管理コンソールで設定を行うと、マネージメントサーバに Mobile Security のログが生成されます。
- Mobile Device エージェントログ: Mobile Device エージェントがアプリ検索ログ、ポリシー違反ログ、デバイス脆弱性ログ、ネットワーク保護ログ、または Web 脅威検出ログを生成すると、そのログが Mobile Security マネージメントサーバに送信されます。これにより、Mobile Device エージェントのログを中央の場所に格納できるようになるため、組織の保護ポリシーを評価したり、感染や攻撃を受ける可能性が高いモバイルデバイスを特定したりできます。

注意

モバイルデバイスに迷惑 SMS 対策ログ、WAP プッシュ保護ログ、および着信フィルタログを表示できます。

Mobile Device エージェントのログを表示する

モバイルデバイスで Mobile Device エージェントのログを表示したり、Mobile Security マネージメントサーバ上で Mobile Device エージェントのすべてのログを表示したりできます。マネージメントサーバでは、Mobile Device エージェントの次のログを表示できます。

- アプリ検索ログ: Mobile Device エージェントで不正プログラム、プライバシーの脅威、脆弱性、改ざんアプリが検出された場合に生成されます。
- ポリシー違反ログ: Mobile Device エージェントのポリシー準拠ステータス情報が含まれます。
- デバイス脆弱性ログ: 開発者オプションまたは USB デバッグモードが有効になっている場合、モバイルデバイスで不正な iOS プロファイルが検出された場合、root 化または Jailbreak されているモバイルデバイスが検出された場合に生成されます。

- ネットワーク保護ログ: モバイルデバイスでネットワークトラフィックの復号、安全でないアクセスポイント (Wi-Fi)、不正な SSL 証明書が検出された場合に生成されます。
- Web 脅威検出ログ: Mobile Device エージェントは、危険な Web ページや不正プログラムに感染した Web ページをブロックすると Web 脅威検出ログを生成し、そのログをサーバにアップロードします。

手順

1. Mobile Security の Web 管理コンソールにログオンします。
2. [通知とレポート] > [ログクエリ] をクリックします。

   [ログクエリ] 画面が表示されます。

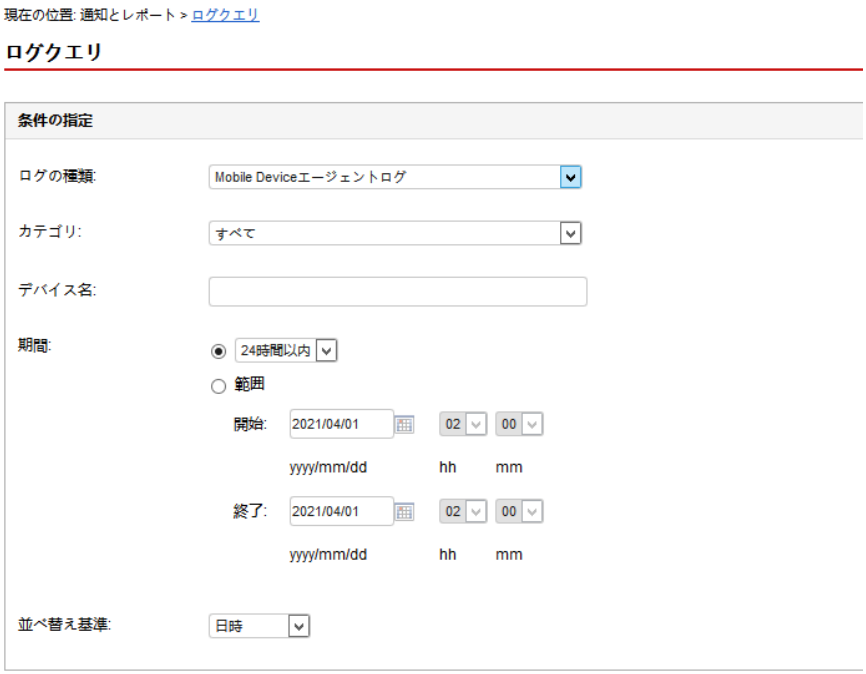

図 8-1. [ログクエリ] 画面

3. 表示するログの検索条件を指定します。次のパラメータがあります。
   - ログの種類: ログの種類をメニューから選択します。
   - カテゴリ: ログのカテゴリをメニューから選択します。
   - 管理者名またはデバイス名: 検索するログに関連する管理者またはデバイスの名前を入力します。
   - 期間:事前定義された日付範囲を選択します。選択肢は、[すべて]、[24 時間以内]、[過去 7 日間]、および [過去 30 日間] です。その他の期間を指定する場合は、[範囲] を選択して、日付範囲を指定してください。
     - 開始: 表示する最初のログの日付を選択します。アイコンをクリックしてカレンダーから日付を選択します。
     - 終了: 表示する最後のログの日付を選択します。アイコンをクリックしてカレンダーから日付を選択します。
   - 並べ替え基準: ログの順序およびグループ化を指定します。
4. [クエリ] をクリックして検索を開始します。

ログの削除設定

Mobile Device エージェントがセキュリティリスクの 検出に関するイベントログを生成した場合、そのログはマネージメントサーバに送信されて格納されます。これらのログを使用して組織の保護ポリシーを評価したり、感染または攻撃される可能性が高いモバイルデバイスを識別したりできます。

ハードディスク上で容量を過剰に占有しないように Mobile Device エージェントのログのサイズを維持するには、手動でログを削除するか、または Mobile Security の Web 管理コンソールの [ログの削除設定] 画面で、スケジュールに基づいて自動的にログを削除するように設定します。

ログを予約削除する

手順

1. [通知とレポート] > [ログの削除設定] をクリックします。

   [ログの削除設定] 画面が表示されます。

2. [ログの予約削除を有効にする] を選択します。
3. 削除するログの種類を選択します。
4. 選択した種類のログをすべて削除するか、または指定した日数より古いログを削除するかを選択します。
5. ログを削除する頻度と時刻を指定します。
6. [保存] をクリックします。

ログを手動で削除する

手順

1. [通知とレポート] > [ログの削除設定] をクリックします。

   [ログの削除設定] 画面が表示されます。

2. 削除するログの種類を選択します。
3. すべての選択した種類のログを削除するか、または指定した日数より古いログのみを削除するかを選択します。
4. [今すぐ削除] をクリックします。

第 9 章

通知とレポートの使用

この章では、Mobile Security の通知とレポートの設定方法および使用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。

通知メッセージとレポートについて

Mobile Security では、メールで管理者やユーザに通知やレポートを送信するように設定できます。

- 管理者への通知: システム異常が発生した場合、管理者にメール通知を送信します。
- レポート: 指定のメール受信者にレポートを送信します。
- ユーザへの通知: Mobile Device エージェントをダウンロードしてインストールするようにモバイルデバイスに通知するメールを送信します。

通知の設定

メール通知を設定する

ユーザにメール通知を送信する場合は、設定を行う必要があります。

手順

1. [通知とレポート] > [設定] をクリックします。

   [通知とレポートの設定] 画面が表示されます。

2. [メールの設定] セクションで、[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。
3. 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、ユーザ名とパスワードを入力します。
4. [保存] をクリックします。

SMS Sender を設定する (※この機能は現在日本では提供されていません。)

マネージメントサーバは、サーバに接続された SMS Sender を制御および監視します。SMS Sender は、Mobile Device エージェントのインストール、登録、

コンポーネントのアップデート、セキュリティポリシーの設定、リモート消去/ロック/検索を実行するように通知するメッセージをモバイルデバイスに送信します。

[SMS Sender 設定] では、次の操作を実行できます。

- SMS Sender の電話番号の設定
- SMS Sender の接続状態の確認
- Mobile Device エージェントのインストールメッセージの 設定
- SMS Sender の切断通知の設定

SMS Sender リスト

モバイルデバイスにメッセージを送信するように SMS Sender を設定するには、マネージメントサーバで SMS Sender デバイスの電話番号を設定しておく必要があります。

注意

SMS Sender リストに SMS Sender の電話番号が設定されていないと、SMS Sender からモバイルデバイスにメッセージを送信できません。

手順

1. Mobile Security の 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。

   [通知/レポート設定] 画面が表示されます。[SMS Sender 設定] に、SMS Sender の電話番号と接続状態のリストが表示されます。SMS Sender がマネージメントサーバに接続されていれば、[ステータス] に [接続] と表示されます。

注意

SMS の送信に 3 回失敗すると、モバイルデバイスに「切断」と表示されます。

SMS Sender リストを設定する

Mobile Security サーバで SMS Sender を管理できるようにするには、SMS Sender の電話番号を指定します。SMS Sender は、次の操作の実行を指示するメッセージをモバイルデバイスに送信します。

- Mobile Device エージェントのダウンロードとインストール
- Mobile Security マネージメントサーバへの登録
- Mobile Security マネージメントサーバからの登録解除
- Mobile Device エージェントの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とのセキュリティポリシー 設定の同期
- モバイルデバイスのリモート 消去
- モバイルデバイスのリモートロック
- モバイルデバイスのリモート 検索

手順

1. Mobile Security の 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。

   [通知/レポート設定] 画面が表示されます。
3. [SMS Sender 設定] で、[追加] をクリックし、SMS Sender の電話番号を入力して [保存] をクリックします。リストに SMS Sender が表示されます。
4. 設定した番号の [ステータス] に [接続] と表示されていることを確認します。[ステータス] に [切断] と表示される場合は、SMS Sender デバイスがマネージメントサーバに接続されていることを確認してください。

注意

電話番号をクリックすると既存の SMS Sender を編集できます。

SMS Sender を監視する

Mobile Security は SMS Sender のステータスを監視し、SMS Sender が 10 分以上切断されている場合にメール通知を送信します。さらに、SMS Sender デバイスに、[エージェント停止]、[エージェント実行中]、[エージェント使用中]、[エージェント切断] のいずれかの接続状態が表示されます。設定の詳細については、173 ページの「管理者への通知」を参照してください。

SMS Sender を編集する

手順

1. Mobile Security の 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。

   [通知/レポート設定] 画面が表示されます。
3. [SMS Sender 設定] で、編集する電話番号をクリックします。

   設定画面が表示されます。
4. 表示されるフィールドで電話番号を編集し、[保存] をクリックします。
5. [保存] をクリックして設定を保存します。

SMS Sender を削除する

手順

1. Mobile Security の 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。

[通知/レポート設定] 画面が表示されます。

3. [SMS Sender 設定] で、削除する SMS Sender を選択し、[削除] をクリックします。
4. [保存] をクリックして設定を保存します。

SMS Sender Client アプリの操作

SMS Sender Client アプリを設定する

手順

1. Android デバイスで SMS Sender アプリを開きます。
2. [設定] をタップして、次の項目を設定します。
   - サーバのアドレス: マネージメントサーバの名前または IP アドレスを入力し、[OK] をタップします。
   - サーバのポート: Web 管理コンソールのポート番号を入力し、[OK] をタップします。
   - 電話番号: SMS Sender の電話番号を入力します。
   - プロトコルの種類: メッセージの送信に使用するプロトコル (HTTP または HTTPS) を選択します。
3. [開始] をタップして SMS Sender を開始します。

SMS Sender を停止する

手順

1. Android デバイスで SMS Sender アプリを開きます。
2. [停止] をタップして SMS Sender を停止します。

SMS Sender のステータス

モバイルデバイスの SMS Sender のステータスは、Mobile Security で更新されます。接続状態に応じて、次のステータスがデバイスに表示されます。

- 正常: SMS Sender はマネージメントサーバに接続されています。
- 停止: SMS Sender は現在停止しています。
- 未使用: SMS Sender アプリの設定が Mobile Security マネージメントサーバの設定と一致しません。

SMS Sender の履歴を確認する

手順

1. Android デバイスで SMS Sender アプリを開きます。
2. [履歴] をタップして、モバイルデバイスに送信されたメッセージを確認します。

SMS Sender の実行ログを確認する

手順

1. Android デバイスで SMS Sender アプリを起動します。
2. [実行ログ] をタップして、SMS Sender の実行イベントログを確認します。

管理者への通知

[管理者への通知] 画面を使用して、次を設定します。

- リアルタイム不正プログラム検出に関する警告: 不正プログラムが検出されると、管理者にメール通知を送信します。

- 不正な証明書に関する警告: 不正な証明書が検出されると、管理者にメール通知を送信します。
- 不正な iOS プロファイルに関する警告: 不正な iOS プロファイルが検出されると、管理者にメール通知を送信します。
- システムエラー: システム異常が発生した場合、管理者にメール通知を送信します。トークン変数 <%PROBLEM%>、<%REASON%>、および <%SUGGESTION%> は、実際の問題、理由、および推奨されるその問題の解決方法に置き換えられます。
- Mobile Security のデバイス管理者を無効化: Android デバイスの [デバイス管理者] リストで Mobile Security が無効になると、管理者にメール通知を送信します。トークン変数 <%DEVICE%> は、メール内でモバイルデバイス名に置き換えられます。
- APNs 証明書の有効期限に関する警告: APNs 証明書の有効期限が切れる 1 ヵ月前に、管理者にメール通知を送信します。
- VPP トークンの有効期限に関する警告: VPP トークンの有効期限が切れる 15 日前に、管理者にメール通知を送信します。
- DEP トークンの有効期限に関する警告: DEP トークンの有効期限が切れる 15 日前に、管理者にメール通知を送信します。

管理者への通知を有効にする

手順

1. [通知とレポート] > [管理者への通知] の順に選択します。

   [管理者への通知] 画面が表示されます。

2. メールで受信する通知とレポートを選択します。
3. [保存] をクリックします。

管理者への通知を設定する

手順

1. [通知とレポート] > [管理者への通知] の順に選択します。

   [管理者への通知] 画面が表示されます。

2. [通知設定] で通知の名前をクリックします。

   選択した通知の [メールの設定] 画面が表示されます。

3. 必要に応じて次の項目を更新します。

   - 宛先: 管理者のメールアドレス。

     
     注意

     メールアドレスを複数指定する場合は、セミコロン「;」で区切ります。

   - 件名: 通知メールの件名。
   - メッセージ: 通知メッセージの本文。

     
     重要

     通知メッセージを変更するときは、初期設定のメールテンプレートにあるトークン変数をメッセージに含めてください。

4. [保存] をクリックします。

レポート

Mobile Security では、次のレポートを生成して送信できます。

- セキュリティレポート: 検出された不正プログラム、改ざんアプリ、プライバシーリスク、脆弱なアプリ、ネットワークトラフィックの復号、安全でないアクセスポイント (Wi-Fi)、不正な SSL 証明書、不正な iOS プロ

ファイル、開発者オプション、USB デバッグの状況、root 化/Jailbreak のステータス、およびブロックされた上位 10 個の Web サイトを表示します。

- デバイスのインベントリレポート: すべての管理対象デバイスについての包括的な情報を表示します。
- コンプライアンス違反レポート: コンプライアンス違反に関する情報を表示します。
- アプリのインベントリレポート: Android デバイスおよび iOS デバイスにインストールされた上位のアプリに関する情報を表示します。
- デバイス登録レポート: デバイスの登録に関する情報を表示します。
- デバイス登録解除レポート: デバイスの登録解除に関する情報を表示します。

[レポート] 画面から次のタスクを実行できます。

表 9-1. レポートのタスク

タスク	説明
生成	新しいレポートをいつでも生成できます。 詳細については、177 ページの「レポートを生成する」を参照してください。
表示	[手動] タブから、最後に生成されたレポートを表示できます。 詳細については、178 ページの「レポートを表示する」を参照してください。
送信	レポートをいつでもメールで送信できます。 詳細については、178 ページの「レポートを送信する」を参照してください。
予約	管理者や他のユーザにレポートを送信するスケジュールを指定できます。 詳細については、179 ページの「レポートを予約設定する」を参照してください。

レポートを生成する

注意

Mobile Security でサーバに保存されるレポートのコピーは、レポートの種類ごとに 1 つだけです。

最新のレポートのコピーを保存してから、新しいバージョンを生成するようにしてください。

手順

1. Mobile Security の Web 管理コンソールで、[通知とレポート] > [レポート][手動] の順に選択します。

   [手動] 画面が表示されます。

2. 期間を選択します。
   - 今日
   - 過去 7 日間
   - 過去 30 日間
3. すべてまたはいずれかのデバイスプラットフォームを 選択します。
   - すべての種類
   - iOS
   - Android
4. レポートに含めるユーザ情報を選択します。
   - すべて
   - 指定
5. 生成するレポートを選択します。
6. [Generate] をクリックします。

選択したレポートが生成され、既存のすべてのバージョンが上書きされます。

レポートを表示する

手順

1. Mobile Security の Web 管理コンソールで、[通知とレポート] > [レポート] の順に選択します。
2. 次のいずれかのタブで、表示するレポートを探します。
   - 手動: 手動レポートを表示する場合に選択します。
   - 予約: 定期レポートを表示する場合に選択します。
3. [表示] をクリックします。

   注意

   リンクが表示されない場合は、先にレポートを生成する必要があります。

   詳細については、177 ページの「レポートを生成する」を参照してください。

   選択したレポートが新しいタブまたは画面に表示されます。

レポートを送信する

手順

1. Mobile Security の Web 管理コンソールで、[通知とレポート] > [レポート][手動] の順に選択します。

   [手動] 画面が表示されます。
2. [レポート] テーブルで目的のレポートを探します。

3. [送信] をクリックします。

> **注意**
>
> リンクが表示されない場合は、先にレポートを生成する必要があります。
>
> 詳細については、177 ページの「レポートを生成する」を参照してください。

[レポートの送信] 画面が表示されます。

4. 受信者のメールアドレスを入力します。
5. 必要に応じて、メールの件名や本文を変更します。
6. [送信] をクリックします。

確認メッセージが表示されます。

レポートを予約設定する

手順

1. Mobile Security の Web 管理コンソールで、[通知とレポート] > [レポート] > [予約] の順に選択します。

[予約] 画面が表示されます。

2. リストからレポートの頻度を選択します。
   - 毎日
   - 毎週: レポートを送信する曜日をリストから選択します。
   - 毎月: レポートを送信する日にちをリストから選択します。
3. [保存] をクリックします。

メールテンプレートを変更する

手順

1. Mobile Security の Web 管理コンソールで、[通知とレポート] > [レポート] > [予約] の順に選択します。

   [予約] 画面が表示されます。

2. レポートの名前をクリックします。

   選択したレポートの [メールの設定] 画面が表示されます。

3. 必要に応じて次の項目を更新します。

   - 宛先: 管理者のメールアドレス。

     注意

     メールアドレスを複数指定する場合は、セミコロン「;」で区切ります。

   - [件名]: レポートメールの件名。
   - [メッセージ]: レポートのメッセージ本文。

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。

ユーザへの通知

メール通知を設定するには、[ユーザへの通知] 画面を使用します。

- モバイルデバイスの登録: Mobile Device エージェントをダウンロードしてインストールするようにモバイルデバイスに通知するメールを送信します。トークン変数 <%DOWNLOADURL%> は、セットアップパッケージの実際の URL に置き換えられます。

- ポリシー違反: コンプライアンス条件を満たしていない場合、モバイルデバイスにメール通知を送信します。トークン変数 <%DEVICE%> と <%VIOLATION%> は、メール内でモバイルデバイスの名前と違反したポリシーに置き換えられます。
- VPP ユーザ通知: 管理者がユーザに VPP アプリを割り当てたときに、モバイルデバイスにメール通知を送信します。

ユーザへの通知を設定する

手順

1. [通知とレポート] > [ユーザへの通知] をクリックします。

   [ユーザへの通知] 画面が表示されます。

2. ユーザにメールで送信する通知を選択し、個々の通知をクリックして内容を変更します。
   - メール通知のメッセージの設定では、必要に応じて次の項目を更新します。
     - 件名: メールの件名。
     - メッセージ: メールの本文。
   - SMS 通知のメッセージを設定するには、[メッセージ] 内のメールの本文を更新します。
3. 完了したら、[保存] をクリックして [ユーザへの通知] に戻ります。

第 10 章

コンポーネントのアップデート

この章では、Mobile Security のコンポーネントをアップデートする 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。

コンポーネントのアップデートについて

Mobile Security では、インターネットを介してトレンドマイクロのアップデートサーバから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。

- Mobile Security サーバ: Mobile Security 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 で危険なファイルを検出できるかどうかを決定するファイル。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。

Mobile Security コンポーネントをアップデートする

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の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、186 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回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、184 ページの「コンポーネントのアップデートについて」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、186 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回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、184 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、185 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。

第 11 章

テクニカルサポート

ここでは、次の項目について説明します。

トラブルシューティングのリソース

トレンドマイクロでは以下のオンラインリソースを提供しています。テクニカルサポートに問い合わせる前に、こちらのサイトも参考にしてください。

サポートポータルの利用

サポートポータルでは、よく寄せられるお問い合わせや、障害発生時の参考となる情報、リリース後に更新された製品情報などを提供しています。

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

脅威データベース

現在、不正プログラムの多くは、コンピュータのセキュリティプロトコルを回避するために、2 つ以上の技術を組み合わせた複合型脅威で構成されています。トレンドマイクロは、カスタマイズされた防御戦略を策定した製品で、この複雑な不正プログラムに対抗します。脅威データベースは、既知の不正プログラム、スパム、悪意のある URL、および既知の脆弱性など、さまざまな混合型脅威の名前や兆候を包括的に提供します。

詳細については、https://www.trendmicro.com/vinfo/jp/threat-encyclopedia/ をご覧ください。

- 現在アクティブまたは「in the Wild」と呼ばれている生きた不正プログラムと悪意のあるモバイルコード
- これまでの Web 攻撃の記録を記載した、相関性のある脅威の情報ページ
- 対象となる攻撃やセキュリティの脅威に関するオンライン勧告
- Web 攻撃およびオンラインのトレンド情報
- 不正プログラムの週次レポート

製品サポート情報

製品のユーザ登録により、さまざまなサポートサービスを受けることができます。

トレンドマイクロの Web サイトでは、ネットワークを脅かすウイルスやセキュリティに関する最新の情報を公開しています。ウイルスが検出された場合や、最新のウイルス情報を知りたい場合などにご利用ください。

サポートサービスについて

サポートサービス内容の詳細については、製品パッケージに同梱されている「製品サポートガイド」または「スタンダードサポートサービスメニュー」をご覧ください。

サポートサービス内容は、予告なく変更される場合があります。また、製品に関するお問い合わせについては、サポートセンターまでご相談ください。トレンドマイクロのサポートセンターへの連絡には、電話またはお問い合わせ Web フォームをご利用ください。サポートセンターの連絡先は、「製品サポートガイド」または「スタンダードサポートサービスメニュー」に記載されています。

サポート契約の有効期限は、ユーザ登録完了から 1 年間です (ライセンス形態によって異なる場合があります)。契約を更新しないと、パターンファイルや検索エンジンの更新などのサポートサービスが受けられなくなりますので、サポートサービス継続を希望される場合は契約満了前に必ず更新してください。更新手続きの詳細は、トレンドマイクロの営業部、または販売代理店までお問い合わせください。

注意

サポートセンターへの問い合わせ時に発生する通信料金は、お客さまの負担とさせていただきます。

トレンドマイクロへのウイルス解析依頼

ウイルス感染の疑いのあるファイルがあるのに、最新の検索エンジンおよびパターンファイルを使用してもウイルスを検出/駆除できない場合などに、感

染の疑いのあるファイルをトレンドマイクロのサポートセンターへ送信していただくことができます。

ファイルを送信いただく前に、トレンドマイクロの不正プログラム情報検索サイト「脅威データベース」にアクセスして、ウイルスを特定できる情報がないかどうか確認してください。

https://www.trendmicro.com/vinfo/jp/threat-encyclopedia/

ファイルを送信いただく場合は、次の URL にアクセスして、サポートセンターの受付フォームからファイルを送信してください。

https://success.trendmicro.com/jp/virus-and-threat-help

感染ファイルを送信する際には、感染症状について簡単に説明したメッセージを同時に送ってください。送信されたファイルがどのようなウイルスに感染しているかを、トレンドマイクロのウイルスエンジニアチームが解析し、回答をお送りします。

感染ファイルのウイルスを駆除するサービスではありません。ウイルスが検出された場合は、ご購入いただいた製品にてウイルス駆除を実行してください。

メールレピュテーションについて

スパムメールやフィッシングメールなどの 送信元を、脅威情報のデータベースと照合することによって判別して評価する、トレンドマイクロのコアテクノロジーです。コアテクノロジーの詳細については、次の Web ページを参照してください。

https://www.trendmicro.com/ja_jp/business/technologies/smart-protection-network.html

ファイルレピュテーションについて

不正プログラムなどのファイル情報を、脅威情報のデータベースと照合することによって判別して評価する、トレンドマイクロのコアテクノロジーです。コアテクノロジーの詳細については、次の Web ページを参照してください。

https://www.trendmicro.com/ja_jp/business/technologies/smart-protection-network.html

Web レピュテーションについて

不正な Web サイトや URL などの情報を、脅威情報のデータベースと照合することによって判別して評価する、トレンドマイクロのコアテクノロジーです。コアテクノロジーの詳細については、次の Web ページを参照してください。

https://www.trendmicro.com/ja_jp/business/technologies/smart-protection-network.html

その他のリソース

製品やサービスについてのその他の情報として、次のようなものがあります。

最新版ダウンロード

製品やドキュメントの最新版は、次の Web ページからダウンロードできます。

https://downloadcenter.trendmicro.com/index.php?clk=left_nav&clkval=all_download&regs=jp

注意

サービス製品、販売代理店経由での販売製品、または異なる提供形態をとる製品など、一部対象外の製品があります。

脅威解析・サポートセンター TrendLabs (トレンドラボ)

TrendLabs (トレンドラボ) は、フィリピン・米国に本部を置き、日本・台湾・ドイツ・アイルランド・中国・フランス・イギリス・ブラジルの 10 カ国 12 か所の各国拠点と連携してソリューションを提供しています。

世界中から選び抜かれた 1,000 名以上のスタッフで 24 時間 365 日体制でインターネットの脅威動向を常時監視・分析しています。

索引

アルファベット

あ

や

ら