Trend Micro Mobile Security™ 9.8

管理者ガイド

（セキュリティ対策限定配信モード）

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。
  http://esupport.trendmicro.com/ja-jp/support-lifecycle/default.aspx

P/N: TSEM98072/171018_JP (2018/03)

目次

はじめに

はじめに 9
対象読者 10
Mobile Security ドキュメント 10
ドキュメントの表記規則 11

第 1 章：製品の紹介

モバイルの脅威について 14
Trend Micro Mobile Security について 14
Trend Micro Mobile Security の機械学習型検索について 14
Mobile Security システムのアーキテクチャ 15
Mobile Security のコンポーネント 15
ローカルコミュニケーションサーバとクラウドコミュニケーションサーバの比較 18
Trend Micro Mobile Security 9.8 の新機能 18
Trend Micro Mobile Security 9.7 の新機能 19
Trend Micro Mobile Security 9.6 の新機能 21
Mobile Device エージェントの主要機能 23
サポートされるモバイルデバイスの OS の機能 24

第 2 章：使用開始

Web 管理コンソール 28
Web 管理コンソールにアクセスする 28
Internet Explorer の互換モードを無効にする 30
製品ライセンス 30
ダッシュボード情報 31
ダッシュボードをカスタマイズする 32

管理設定 35
AD (Active Directory) を設定する 35
ユーザ認証を設定する 35
データベースを設定する 35
コミュニケーションサーバを設定する 35
配信を設定する 36
管理者アカウントを管理する 36
コマンドキューを管理する 43
古いコマンドの削除スケジュールを設定する 44
古いコマンドを手動で削除する 44
証明書を管理する 45
証明書をアップロードする 45
証明書を削除する 46

第 3 章：他の MDM ソリューションと統合する

AirWatch との統合 48
統合の前提条件 48
Airwatch との統合アーキテクチャ 48
統合の機能 49
統合のための AirWatch アカウントの権限の要件 52
AirWatch との統合を設定する 54
エージェントの配信 56
MobileIron との統合 61
統合の前提条件 61
MobileIron との統合のアーキテクチャ 61
統合の機能 62
MobileIron との統合を設定する 64
エージェントの配信 65

第 4 章：モバイルデバイスの管理

[管理対象デバイス] タブ 70
Mobile Security のグループ 70
グループの管理 70
モバイルデバイスを管理する 72
モバイルデバイスのステータス 75

Mobile Device エージェントでの操作 77
Mobile Device エージェントをアップデートする 77
モバイルデバイス情報をアップデートする 78
データをエクスポートする 79
Trend Micro Control Manager との統合 79
Control Manager でセキュリティポリシーを作成する 80
セキュリティポリシーを削除または変更する 80
Control Manager におけるセキュリティポリシーのステータス 80

第 5 章：ユーザの表示

[ユーザ] タブ 82
ユーザリストを表示する 82

第 6 章：ポリシーの設定

ポリシーについて 84
すべてのデバイスのポリシー 84
承認済みアプリリスト 84
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 85
すべてのデバイスのポリシーの管理 85
すべてのグループのポリシー 88
共通ポリシー 88
セキュリティポリシー 89
Web 脅威検出ポリシー 92
すべてのグループのポリシーの管理 93

第 7 章：検出項目の表示と管理

[不審アプリ] 画面について 98
不審 Android アプリを表示する 100
不審 iOS アプリを表示する 101
不正な SSL 証明書を表示する 102
不正な iOS プロファイルを表示する 103

第 8 章：コンポーネントのアップデート

コンポーネントのアップデートについて 106
Mobile Security コンポーネントのアップデート 106
手動アップデート 106
予約アップデート 107
ダウンロード元を指定する 108
ローカルのアップデート元の手動アップデート 109

第 9 章：ログの表示と管理

ログについて 112
Mobile Device エージェントのログを表示する 112
ログの削除設定 114
ログを予約削除する 114
ログを手動で削除する 115

第 10 章：通知とレポートの使用

通知メッセージとレポートについて 118
通知の設定 118
メール通知を設定する 118
管理者への通知 119
管理者への通知を有効にする 119
管理者への通知を設定する 119
レポート 120
レポートを生成する 121
レポートを表示する 122
レポートを送信する 123
レポートを予約設定する 124
メールテンプレートを変更する 124
ユーザへの通知 125
ユーザへの通知を設定する 125

第 11 章：トラブルシューティングとサポート情報

トラブルシューティング 128

トラブルシューティングのリソース 130
サポートポータルの利用 130
脅威データベース 130
製品サポート情報 131
サポートサービスについて 131
セキュリティニュース 132
脅威解析・サポートセンター TrendLabs (トレンドラボ) 133

索引

索引 135

はじめに

Trend Micro Mobile Security 9.8 (以下、Mobile Security) 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。

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

対象読者

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

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

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

ヒント

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

ドキュメントの表記規則

このドキュメントでは、次の表記規則を使用しています。

表 1. ドキュメントの表記規則

表記	説明
注意	設定上の注意
ヒント	推奨事項
警告!	避けるべき操作や設定についての注意

第 1 章

製品の紹介

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。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。

- 14 ページの「モバイルの脅威について」
- 14 ページの「Trend Micro Mobile Security について」
- 15 ページの「Mobile Security システムのアーキテクチャ」
- 15 ページの「Mobile Security のコンポーネント」
- 18 ページの「Trend Micro Mobile Security 9.8 の新機能」
- 23 ページの「Mobile Device エージェントの主要機能」
- 24 ページの「サポートされるモバイルデバイスの OS の機能」

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

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。

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 Mobile Security と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 のコンポーネント

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

表 1-1. Mobile Security のコンポーネント

コンポーネント	説明	必須/オプション
マネージメントサーバ	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。 詳細については18 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
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

コンポーネント	説明	必須/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
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
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
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 の新機能

バージョン 9.8 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
登録依頼メール (Android のみ)	管理者が AirWatch を使用して Mobile Device エージェントを配信する際に、すべてのユーザに登録依頼メールを送信できます。
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

機能	説明
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。
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。
iOS Mobile Device エージェントのサポート	AirWatch および MobileIron のセキュリティ対策モードでのみ、iOS Mobile Device エージェントがサポートされます。
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 の新機能

バージョン 9.7 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
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)
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。

機能	説明
iOS アクティベーションロックのサポート (フル機能配信モードのみ)	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。
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: Andoird 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	Andoird 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。
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。
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。
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。
アプリの配信モード選択	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。

機能	説明
Exchange Server のデータクリーンナップ	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、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。

機能	説明
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
認証	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。		●	
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。	アプリ検索ログ	●	●
		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。	アプリ権限チェックの履歴	●	

サポートされるモバイルデバイスの OS の機能

次の表は、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 Security 9.8 の機能

ポリシー	機能	設定		
モバイル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		●
		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		●

第 2 章

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。

- 28 ページの「Web 管理コンソールにアクセスする」
- 31 ページの「ダッシュボード情報」
- 35 ページの「管理設定」
- 43 ページの「コマンドキューを管理する」
- 45 ページの「証明書を管理する」

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、40 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。

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、30 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 2 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

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]、無効にする場合は [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に配信モードを切り替える

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への配信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。

http://esupport.trendmicro.com/solution/ja-JP/1116941.aspx

AirWatch と Trend Micro Mobile Security の統合を設定する

Trend Micro Mobile Security は、AirWatch デバイス管理ソリューションと統合できます。

詳細については、48 ページの「AirWatch との統合」を参照してください。

MobileIron と Trend Micro Mobile Security の統合を設定する

Trend Micro Mobile Security は、MobileIron デバイス管理ソリューションと統合できます。

詳細については、61 ページの「MobileIron との統合」を参照してください。

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、40 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、42 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

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
	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		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
モバイルデバイス	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
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、42 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、42 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. [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、40 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。

コマンドキューを管理する

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。

コマンドのステータス	説明
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。

コマンドがハードディスクの容量を占有し過ぎないようにするには、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] 画面でのスケジュールに基づいて自動的に削除され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] をクリックします。

   [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] をクリックします。

[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。

証明書を管理する

.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。

第 3 章

他の MDM ソリューションと統合する

Trend Micro Mobile Security は、他のモバイルデバイス管理ソリューションと統合できます。

この章では、他のモバイルデバイス管理ソリューションと Mobile Security の統合を設定する手順について説明します。

この章のトピックは次のとおりです。

- 48 ページの「AirWatch との統合」
- 61 ページの「MobileIron との統合」

AirWatch との統合

Trend Micro Mobile Security は、AirWatch MDM ソリューションと統合できます。

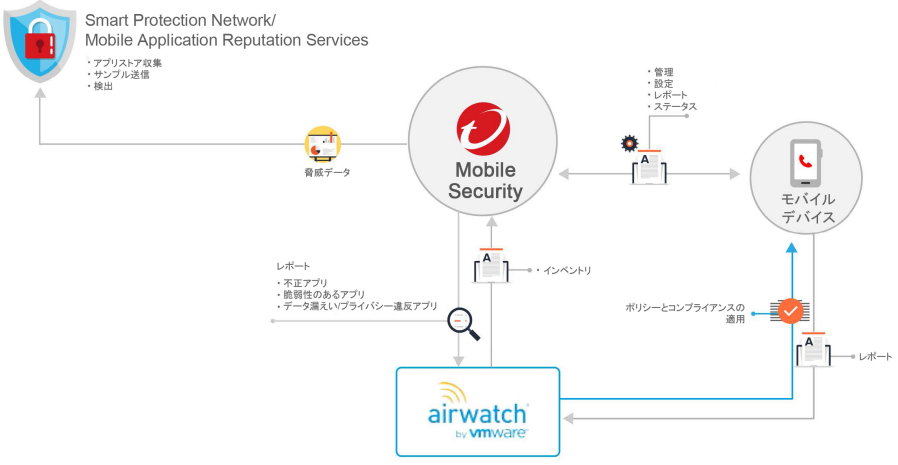
統合の前提条件

他の MDM ソリューションを Trend Micro Mobile Security に統合するには、次の製品を使用する必要があります。

- Mobile Security 9.7 以降
- Mobile Security で設定されたローカルコミュニケーションサーバまたはクラウドコミュニケーションサーバ
- AirWatch v9.1 以降
- AirWatch の Web 管理コンソールの管理者アカウント

Airwatch との統合アーキテクチャ

次の図は、AirWatch との統合アーキテクチャの概要を示しています。



Mobile Application Reputation はアプリの動作に基づいてモバイルの脅威を自動的に特定する、クラウドベースの技術です。さまざまな Android マーケットから膨大な数の Android アプリをクロールして収集し、既存および新しい不正プログラム、およびプライバシー/デバイスのリソースを不正使用する可能性のあるアプリを特定します。世界初のモバイルアプリ自動評価サービスです。

Trend Micro Smart Protection Network は、ゼロデイ攻撃に対してプロアクティブでグローバルな脅威情報を提供し、ユーザの環境を常に保護します。トレンドマイクロでは、最新の脅威情報を使用して、危害が及ぶ前にただちに攻撃を防ぎます。Trend Micro Smart Protection Network は、トレンドマイクロのすべての製品およびサービスに適用されます。

Mobile Security は、Trend Micro Smart Protection Network と Mobile Application Reputation Services を使用してモバイルデバイスのセキュリティに関する問題を検出し、AirWatch コンプライアンスポリシーを活用してモバイルデバイスを管理します。

統合の機能

Trend Micro Mobile Security には、AirWatch との統合のために次の機能が用意されています。

機能	説明
モバイルデバイスの自動グループ化	Mobile Security は、Dangerous、Risky、No_TMMS のサフィックスを追加し、リスクレベルに基づいてモバイルデバイスにタグ付けします。 詳細については、50 ページの「モバイルデバイスの自動グループ化」を参照してください。
アプリケーションの自動グループ化	Mobile Security は、Malware、Vulnerability、Privacy のプレフィックスを追加し、リスクレベルに基づいてモバイルアプリケーションをグループ化します。 詳細については、51 ページの「モバイルアプリケーションの自動グループ化」を参照してください。

機能	説明
AirWatch 拒否リストの自動アップデート (ポリシー違反のアプリの登録)	この機能を使用すると、(セキュリティ対策の結果に基づいて) AirWatch のコンプライアンスポリシーに違反するアプリを拒否リストに登録し、ユーザにメールアラートを送信できます。 詳細については、51 ページの「AirWatch 拒否リストのアプリ用コンプライアンスポリシーを設定する」を参照してください。
Mobile Security クライアントアプリの自動配信	モバイルデバイスに Mobile Device エージェントを自動的に配信するように AirWatch を設定できます。 • Android: 手順については、57 ページの「Mobile Security マネージメントサーバから Android エージェントを配信する」を参照してください。 Samsung デバイスの場合、Mobile Device エージェントを自動的に起動するように設定することもできます。詳細および手順については、58 ページの「Android デバイスの自動起動を設定する 」を参照してください。 • iOS: 手順については、59 ページの「iOS エージェントを配信する」を参照してください。

モバイルデバイスの自動グループ化

Trend Micro Mobile Security は、プレフィックスを使用して 3 つのクラス (Dangerous、Risky、NO_TMMS) を作成し、リスクのあるデバイスを次のようにタグ付けします。

- PREDEFINEDPREFIX_Dangerous
- PREDEFINEDPREFIX _Risky
- PREDEFINEDPREFIX _NO_TMMS

Mobile Security では、Web 管理コンソールを使用してプレフィックス (PREDEFINEDPREFIX) を定義できます。セキュリティレベルが異なるアプ

リケーションが検出されると、デバイスのスマートグループが自動的に変更されます。

モバイルデバイスで不正プログラムが検出されと、そのモバイルデバイスは PREDEFINEDPREFIX _Dangerous グループに移動されます。

モバイルアプリケーションの自動グループ化

Mobile Security は、リスクの高いアプリケーションをまとめて (もたらすリスクの種類に応じて)「アプリケーショングループ」として自動的にグループ化します。

- PREDEFINEDPREFIX _Malware_App_Android
- PREDEFINEDPREFIX _Privacy_App_Android
- PREDEFINEDPREFIX _Vulnerability_App_Android
- PREDEFINEDPREFIX _Malware_App_iOS

Mobile Security では、Web 管理コンソールを使用してプレフィックス (PREDEFINEDPREFIX) を定義できます。

AirWatch 拒否リストのアプリ用コンプライアンスポリシーを設定する

AirWatch との統合を設定したら、AirWatch の Web 管理コンソールでコンプライアンスポリシーを作成して、AirWatch の拒否リストに不正アプリを追加できます。

手順

1. AirWatch の Web コンソールにログオンし、[デバイス] > [順守ポリシー] > [リスト表示] の順に選択します。
2. [追加] をクリックし、プラットフォーム (Android または Apple iOS) を選択します。リストから [アプリケーションリスト] を選択し、[ブラックリストアプリが含まれている] を選択します。
3. [次へ] をクリックします。

4. [アクション] タブで処理を設定します。
   a. [非順守状態としてマーク] を選択します。
   b. リストから [通知] と [E メールをユーザに送信] を選択します。
   c. [次へ] をクリックします。
5. [割り当て] タブで次のように設定します。
   - 管理元:Trend Micro
   - 割り当てるグループ
   - 除外
6. [次へ] をクリックします。
7. [概要] タブで、名前と説明を設定します。
8. [完了してアクティブ化する] をクリックします。

モバイルデバイスで不正プログラムが検出されると、AirWatch の拒否リストに登録され、モバイルデバイスには非準拠のフラグが設定されます。

統合のための AirWatch アカウントの権限の要件

Mobile Security では AirWatch との統合がサポートされます。Mobile Security を AirWatch と統合するには、Mobile Security マネージメントサーバと AirWatch の間の通信に必要な権限を持つ AirWatch アカウントが必要です。

AirWatch で必要な権限を持つアカウントを作成する方法は 3 種類あります。

- オプション 1:すべての権限を持つ通信用の AirWatch 管理者アカウントを作成する

  AirWatch 管理コンソールで、[アカウント] > [管理者] > [リスト表示] > [追加] > [管理者を追加] の順に選択し、次の役割と権限を持つアカウントを作成します。

  ```
  AirWatch Administrator
  AirWatch Admins (Internal or External) Access to all except
  "dangerous" console features.
  ```

- オプション 2:すべての REST API 権限を持つ API ONLY のユーザを作成する

  AirWatch 管理コンソールで、[アカウント] > [管理者] > [リスト表示] > [追加] > [管理者を追加] の順に選択し、次の役割と権限を持つアカウントを作成します。

  ```
  API Only
  Only provides access to REST APIs
  ```

- オプション 3:カスタマイズされた REST API 権限を持つ API ONLY のユーザを作成する

  この方法では、Mobile Security で使用する特定の REST API を選択します。

  次の手順を実行します。

  1. AirWatch 管理コンソールで、[アカウント] > [管理者] > [役割] の順に選択し、次の表に示されるような REST API 権限から Mobile Security で使用する特定の権限を選択して役割を作成します。

カテゴリ	名前
管理者アカウントの管理	管理者を検索する
タグの管理	タグを作成する
	タグを検索する
	タグにデバイスを追加する
	タグからデバイスを削除する
	特定のタグのデバイスを取得する
スマートグループの管理	スマートグループを作成する
	スマートグループを検索する
	スマートグループを削除する

カテゴリ	名前
アプリケーショングループの管理	アプリケーショングループを作成する
	アプリケーショングループを検索する
	アプリケーショングループの詳細を取得する
	アプリケーションをアプリケーショングループに追加する
	アプリケーションをアプリケーショングループから削除する
アプリケーションの管理	社内アプリケーションのインストール: アプリケーションチャンクをアップロードする (iOS および Android)
	社内アプリケーションのインストール: 社内アプリケーションのインストールを開始する
デバイス管理	デバイスの情報を取得する
	デバイスの詳細検索
	デバイス数の情報

2. [アカウント] > [管理者] > [リスト表示] > [追加] > [管理者を追加] の順に選択し、新しく作成した役割を持つアカウントを追加します。

注意

AirWatch の REST 権限の設定画面には、API ごとの権限はありませんが、多数の API のシリーズ (Admin API、APPs API など) があります。設定ページで有効にする必要がある REST API 権限については、AirWatch のテクニカルサポートに問い合わせてください。

AirWatch との統合を設定する

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 [管理] > [コミュニケーションサーバの設定] をクリックし、コミュニケーションサーバが設定されていることを確認します。設定されていない場合は、「インストールおよびクライアント配信ガイド」の「コミュニケーションサーバを設定する」で設定手順を確認してください。
3. [管理] > [配信設定] をクリックします。
4. [サーバ] の [セキュリティ対策限定] を選択し、リストから [AirWatch] MDM ソリューションを選択します。
5. [サービスの登録] で、AirWatch の次の情報を設定します。
   - API URL
   - API キー
   - アカウント
   - パスワード
6. [設定の確認] をクリックして、Mobile Security が AirWatch サーバに接続できることを確認します。
7. [データ同期設定] で次のように設定します。
   - セキュリティカテゴリのプレフィックス

注意

Trend Micro Mobile Security は、プレフィックスを使用して 3 つのクラス (Dangerous、Risky、NO_TMMS) を作成し、リスクのあるデバイスを次のようにタグ付けします。

- XXXX_Dangerous
- XXXX_Risky
- XXXX_NO_TMMS

リスクのあるデバイスとアプリは、それぞれスマートグループとアプリケーショングループにグループ化され、アプリ名にタグとカテゴリのプレフィックスが付加されます。

- スマートグループ: XXXX_Dangerous、XXXX_Risky、XXXX_NO_TMMS
- アプリケーショングループ: XXXX_Malware_App_Android、XXXX_Privacy_App_Android、XXXX_Vulnerability_App_Android、XXXX_Malware_App_iOS

エージェントの配信

Trend Micro Mobile Security では、次の方法でエージェントを配信できます。

- Mobile Security サーバ: Mobile Device エージェントを AirWatch アプリストアからダウンロードするようにユーザに通知します。アプリ名は ENT Security です。

  この配信オプションを使用する場合は、テキストまたは QR コードの形式で登録情報をユーザに提供する必要があります。ユーザは登録情報を使用するか QR コードを読み取ってサーバに登録できます。登録情報を使用する場合は、サーバの IP アドレスとポート番号、および登録キーを [配信設定] 画面の [Android エージェント] タブで確認できます。ユーザは、Mobile Device エージェントを起動するたびにアプリを Mobile Security マネージメントサーバに登録する必要があります。自動的に登録されるようにアプリを設定することもできます。ただし、アップデートが利用可能になるたびに、モバイルデバイスユーザは Mobile Device エージェントを手動でアップデートする必要があります。

Samsung デバイスでは、AirWatch 管理コンソールから Mobile Device エージェントを自動的に配信および設定できます。

Mobile Security マネージメントサーバから Android エージェントを配信する

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 [管理] > [デバイス登録設定] をクリックします。
3. [認証情報] タブで、[登録キーを使用して認証] を選択し、[設定済みの登録キーを使用] を選択します。
4. [管理] > [配信設定] > [Android エージェント] (タブ) をクリックします。
5. [Mobile Security マネージメントサーバからダウンロード] を選択し、[自動登録] を選択します。
6. [保存] をクリックして設定を保存します。
7. [アップロード] をクリックし、変更済みの Mobile Security エージェントファイルを選択して、AirWatch サーバにアップロードします。

   Mobile Device エージェントがアップロードされて、AirWatch の Web 管理コンソールに表示されます。

次に進む前に

Android エージェントを配信したら、テキストまたは QR コードの形式で登録情報をユーザに提供します。ユーザは登録情報を使用するか QR コードを読み取ってサーバに登録できます。登録情報を使用する場合は、サーバの IP アドレスとポート番号、および登録キーを [配信設定] 画面の [Android エージェント] タブで確認できます。

Android デバイスの自動起動を設定する

始める前に

この手順を実行する前に、57 ページの「Mobile Security マネージメントサーバから Android エージェントを配信する」で説明したすべての手順を完了しておく必要があります。

手順

1. AirWatch の Web コンソールにログオンし、[デバイス] > [代理加入セットアップとプロビジョニング] > [コンポーネント] > [ファイル/アクション] の順に選択します。
2. AirWatch のコンソールから [ファイル/アクション] を設定します。次の手順を実行します。
   a. [デバイス] > [代理加入セットアップとプロビジョニング] > [コンポーネント] > [ファイル/アクション] の順に選択します。
   b. [ファイルアクションを追加] > [Android] をクリックします。
   c. [全般] タブの [名前] と [説明] に入力します。
   d. [マニフェスト] タブで、[インストールマニフェスト] の下にある [処理を追加] をクリックします。
   e. [マニフェスト] オプションで、次の情報を設定して [保存] をクリックします。
      - 実行するアクション:インデントを実行
      - 実行するコマンドラインと引数:

        ```
        mode=explicit,broadcast=false,action=android.intent.action.MAIN,package=com.trendmicro.tmmssuite.enterprise,class=com.trendmicro.tmmssuite.enterprise.ui.TmmsEnterpriseSplashScreen
        ```

      - タイムアウト:[要件に応じた期間]
   f. [ファイル/アクションを追加] 画面の [保存] をクリックします。

3. 製品を設定します。次の手順を実行します。
   a. [デバイス] > [代理加入セットアップとプロビジョニング] > [プロダクトリスト表示] の順に選択します。
   b. [プロダクトを追加] > [Android] をクリックします。
   c. [全般] タブの [名前]、[説明]、および [割り当てるグループ] に入力します。
   d. [マニフェスト] タブの [追加] をクリックしてマニフェストを追加します。
   e. [マニフェストを追加] オプションで、次の情報を設定して [保存] をクリックします。
      - 実行するアクション: ファイル/アクションをインストールする
      - ファイル/アクション:

        `TestLauncher`
   f. [プロダクトを追加] 画面の [保存] をクリックします。
4. アプリケーションを設定します。次の手順を実行します。
   a. Mobile Security エージェントをスマートグループに割り当てます。
   b. [プッシュモード] を [自動] に設定します。

iOS エージェントを配信する

手順

1. AirWatch の Web コンソールにログオンし、[アプリとブック] > [アプリケーション] > [リスト表示] の順に選択します。
2. [パブリック] タブの [アプリケーションを追加] をクリックします。
3. [アプリケーションを追加] 画面で、次のフィールドを設定します。
   - 管理元: 「`Trend Micro`」と入力します。

- プラットフォーム: [Apple iOS] を選択します。
- ソース: [アプリストアを検索] を選択します。
- 名前: 「ENT Security」と入力します。

4. [次へ] をクリックします。
5. 検索結果から、[選択] をクリックして [Mobile Security for Enterprise Agent] を選択します。
6. [割り当て] タブの [アプリケーション構成を送信] を選択し、[アプリケーション構成] でアプリケーションを設定します。

   アプリケーションの設定値を確認するには、次の図に示すように、Mobile Security の Web 管理コンソールの [配信設定] 画面を参照してください ([管理] > [配信設定])。

設定キー	値の型	設定値
CmdType	文字列	Enroll
EK	文字列	<登録キー>
ServerUrl	文字列	<実際のサーバの URL>

設定キー	値の型	設定値
ServerPort	文字列	<実際のサーバのポート番号>
DeviceSerialNumber	文字列	{DeviceSerialNumber}
DeviceWLANMac	文字列	{DeviceWLANMac}

7. [保存して公開] をクリックします。
8. [デバイス割り当て表示] 画面の [公開] をクリックします。

MobileIron との統合

Trend Micro Mobile Security は、次の MobileIron MDM ソリューションと統合できます。

- MobileIron Core (ホスト)
- MobileIron Core (オンプレミス)

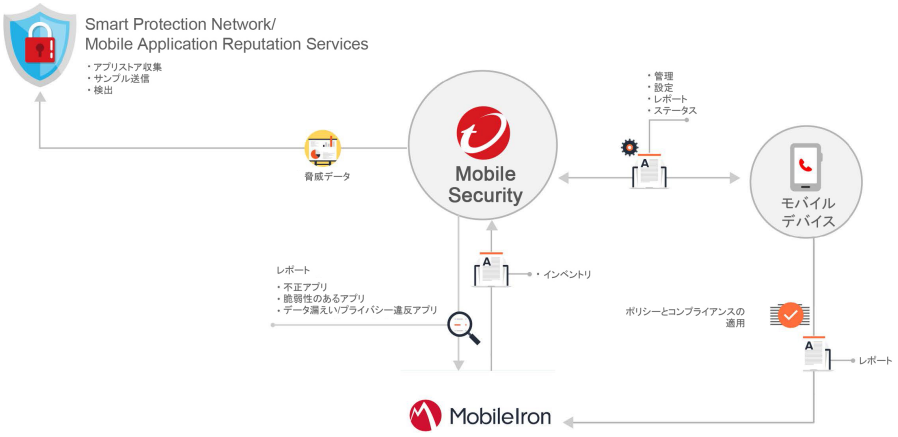
統合の前提条件

他の MDM ソリューションを Trend Micro Mobile Security に統合するには、次の製品を使用する必要があります。

- Mobile Security 9.7 以降
- Mobile Security で設定されたローカルコミュニケーションサーバまたはクラウドコミュニケーションサーバ
- MobileIron v9.3 以降
- MobileIron の Web 管理コンソールの管理者アカウント

MobileIron との統合のアーキテクチャ

次の図は、MobileIron との統合アーキテクチャの概要を示しています。



Mobile Application Reputation はアプリの動作に基づいてモバイルの脅威を自動的に特定する、クラウドベースの技術です。さまざまな Android マーケットから膨大な数の Android アプリをクロールして収集し、既存および新しい不正プログラム、およびプライバシー/デバイスのリソースを不正使用する可能性のあるアプリを特定します。世界初のモバイルアプリ自動評価サービスです。

Trend Micro Smart Protection Network は、ゼロデイ攻撃に対してプロアクティブでグローバルな脅威情報を提供し、ユーザの環境を常に保護します。トレンドマイクロでは、最新の脅威情報を使用して、危害が及ぶ前にただちに攻撃を防ぎます。Trend Micro Smart Protection Network は、トレンドマイクロのすべての製品およびサービスに適用されます。

Mobile Security は、Trend Micro Smart Protection Network と Mobile Application Reputation Services を使用してモバイルデバイスのセキュリティに関する問題を検出し、MobileIron コンプライアンスポリシーを活用してモバイルデバイスを管理します。

統合の機能

Trend Micro Mobile Security には、AirWatch との統合のための次の機能が用意されています。

機能	説明
モバイルデバイスの自動グループ化	Mobile Security は、Dangerous、Risky、NO_TMMS のサフィックスを追加し、リスクレベルに基づいてモバイルデバイスにラベルを付けます。 詳細については、63 ページの「モバイルデバイスの自動グループ化」を参照してください。
Mobile Security クライアントアプリの自動配信	モバイルデバイスに Mobile Device エージェントを自動的に配信するように MobileIron を設定できます。 • Android: 手順については、65 ページの「Mobile Security マネージメントサーバから Android エージェントを配信する」を参照してください。 • iOS: 手順については、66 ページの「iOS エージェントを配信する」を参照してください。

モバイルデバイスの自動グループ化

Trend Micro Mobile Security は、プレフィックスを使用して 3 つのクラス (Dangerous、Risky、NO_TMMS) を作成し、リスクのあるデバイスに次のようにラベルを付けます。

- PREDEFINEDPREFIX_Dangerous
- PREDEFINEDPREFIX _Risky
- PREDEFINEDPREFIX _NO_TMMS

Mobile Security では、Web 管理コンソールを使用してプレフィックス (PREDEFINEDPREFIX) を定義できます。不正なアプリケーションが検出されると、デバイスのスマートグループが自動的に変更されます。

モバイルデバイスで不正プログラムが検出されと、そのモバイルデバイスは PREDEFINEDPREFIX _Dangerous グループに移動されます。

MobileIron との統合を設定する

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 [管理] > [コミュニケーションサーバの設定] をクリックし、コミュニケーションサーバが設定されていることを確認します。設定されていない場合は、「インストールおよびクライアント配信ガイド」の「コミュニケーションサーバを設定する」で設定手順を確認してください。
3. [管理] > [配信設定] をクリックします。
4. [サーバ] の [セキュリティ対策限定] を選択し、リストから [MobileIron Core (ホスト)] または [MobileIron Core (オンプレミス)] MDM ソリューションを選択します。
5. [サービスの登録] で、MobileIron の次の情報を設定します。
   - API URL
   - アカウント名
   - パスワード
6. [設定の確認] をクリックして、Mobile Security が MobileIron サーバに接続できることを確認します。
7. [データ同期設定] で次のように設定します。
   - セキュリティカテゴリのプレフィックス

注意

Trend Micro Mobile Security は、プレフィックスを使用して 3 つのクラス (Dangerous、Risky、NO_TMMS) を作成し、リスクのあるデバイスに次のようにラベルを付けます。

- XXXX_Dangerous
- XXXX_Risky
- XXXX_NO_TMMS

エージェントの配信

Trend Micro Mobile Security では、次の方法でエージェントを配信できます。

- Mobile Security サーバ: Mobile Device エージェントを MobileIron アプリストアからダウンロードするようにユーザに通知します。アプリ名は ENT Security です。

  この配信オプションを使用する場合は、テキストまたは QR コードの形式で登録情報をユーザに提供する必要があります。ユーザは登録情報を使用するか QR コードを読み取ってサーバに登録できます。登録情報を使用する場合は、サーバの IP アドレスとポート番号、および登録キーを [配信設定] 画面の [Android エージェント] タブで確認できます。ユーザは、Mobile Device エージェントを起動するたびにアプリを Mobile Security マネージメントサーバに登録する必要があります。自動的に登録されるようにアプリを設定することもできます。ただし、アップデートが利用可能になるたびに、モバイルデバイスユーザは Mobile Device エージェントを手動でアップデートする必要があります。

Mobile Security マネージメントサーバから Android エージェントを配信する

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 [管理] > [デバイス登録設定] をクリックします。

3. [認証情報] タブで、[登録キーを使用して認証] を選択し、[設定済みの登録キーを使用] を選択します。
4. [管理] > [配信設定] > [Android エージェント] (タブ) をクリックします。
5. [Mobile Security マネージメントサーバからダウンロード] を選択し、[自動登録] を選択します。
6. [保存] をクリックして設定を保存します。
7. [アップロード] をクリックし、変更済みの Mobile Security エージェントファイルを選択して、MobileIron サーバにアップロードします。

   Mobile Device エージェントがアップロードされて、MobileIron の Web 管理コンソールに表示されます。

次に進む前に

Android エージェントを配信したら、テキストまたは QR コードの形式で登録情報をユーザに提供します。ユーザは登録情報を使用するか QR コードを読み取ってサーバに登録できます。登録情報を使用する場合は、サーバの IP アドレスとポート番号、および登録キーを [配信設定] 画面の [Android エージェント] タブで確認できます。

iOS エージェントを配信する

手順

1. MobileIron の Web コンソールにログオンし、[App Catalog] をクリックします。
2. [Add+] をクリックし、[iTunes] を選択します。
3. 検索フィールドに「`ENT Security`」と入力し、[Search] をクリックします。
4. [Mobile Security for Enterprise Agent] を選択し、[Next] をクリックします。
5. 設定を変更しないで、[Next] をクリックします。
6. [APPS@WORK CATALOG] の [Feature this App in the Apps@Work catalog] を選択し、[Next] をクリックします。

7. [Finish] をクリックします。
8. Mobile Security の Web 管理コンソールにログオンします。
9. [管理] > [配信設定] > [iOS エージェント] (タブ) をクリックします。
10. [ダウンロード] をクリックして設定ファイルをダウンロードします。

注意

[ダウンロード] ボタンがアクティブでない場合は、前の手順の設定に間違いがないことを確認してください。

11. MobileIron の Web 管理コンソールで、[Policies & Configures] に移動します。
12. [Add New] > [iOS and OS X] > [Managed App Config] をクリックします。
13. 次の情報を入力します。
    - Name
    - 説明
    - BundleId
14. [ダウンロード] をクリックして設定ファイルをダウンロードします。

15. 新しく作成した設定ファイルを選択し、[More Action] > [Apply to Label] をクリックします。
16. [Apply] をクリックします。

    「App Installation」という通知が iOS デバイスにプッシュされます。

第 4 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。

- 70 ページの「[管理対象デバイス] タブ」
- 70 ページの「グループの管理」
- 72 ページの「モバイルデバイスを管理する」
- 75 ページの「モバイルデバイスのステータス」
- 77 ページの「Mobile Device エージェントでの操作」
- 77 ページの「Mobile Device エージェントをアップデートする」
- 79 ページの「Trend Micro Control Manager との統合」

[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
- Mobile Device エージェントコンポーネントの手動アップデート、デバイスの検索、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。

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、ルートグループ「モバイルデバイス」と「初期設定」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。

モバイルデバイスを管理する

[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。
   - 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。

- 74 ページの「1 台のモバイルデバイスを削除する」
- 74 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、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 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、および接続しているアクセスポイント (Wi-Fi) 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 マネージメント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
- 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

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

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、106 ページの「Mobile Security コンポーネントのアップデート」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 マネージメントサーバは、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。

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。

Trend Micro Control Manager との統合

Trend Micro Mobile Security は、Trend Micro Control Manager (Control Manager または TMCM) と統合することができます。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
- Mobile Security 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。

http://docs.trendmicro.com/ja-jp/enterprise/control-manager-70.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。

Control Manager は、24 時間ごとにポリシーを 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 5 章

ユーザの表示

この章では、Mobile Security に登録されたユーザを表示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。

- 82 ページの「[ユーザ] タブ」
- 82 ページの「ユーザリストを表示する」

[ユーザ] タブ

[ユーザ] タブを使用して、Mobile Security に登録されたすべてのモバイルデバイスを表示できます。

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
   - モバイルデバイス
   - 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、その情報が表示されます。

第 6 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。

- 84 ページの「ポリシーについて」
- 84 ページの「すべてのデバイスのポリシー」
- 85 ページの「すべてのデバイスのポリシーの管理」
- 88 ページの「すべてのグループのポリシー」
- 93 ページの「すべてのグループのポリシーの管理」

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デバイスに対するポリシーを設定できます。

表 6-1. 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	詳細については84 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	詳細については85 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 6-2. Mobile Security のグループポリシー

ポリシーグループ	ポリシー	参照情報
一般	共通ポリシー	詳細については88 ページの「共通ポリシー」を参照してください。
モバイルデバイスのセキュリティ	セキュリティポリシー	詳細については89 ページの「セキュリティポリシー」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] 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] 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 エージェントの設定を許可するかどうかを選択できます。

[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、[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、89 ページの「セキュリティポリシー」を参照してください。

- 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。

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。

注意

Mobile Security での Web 脅威検出でサポートされるのは、Android 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 6-3. 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	

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
		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、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。	

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
	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。	

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
		• 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。	
	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/	

Web 脅威検出ポリシー

Mobile Security マネージメントサーバから Web 脅威検出ポリシーを管理して、Android デバイスに展開できます。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

Web 脅威検出でサポートされるのは、Android の初期設定のブラウザと Google Chrome のみです。

Web 脅威検出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 [Web 脅威検出ポリシー] 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、94 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、94 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。

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。

- 98 ページの「[不審アプリ] 画面について」
- 102 ページの「不正な SSL 証明書を表示する」
- 103 ページの「不正な iOS プロファイルを表示する」

[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、85 ページの「アプリを承認済みリストに追加する」および86 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	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 85 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

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。

- 106 ページの「コンポーネントのアップデートについて」
- 106 ページの「Mobile Security コンポーネントのアップデート」
- 109 ページの「ローカルのアップデート元の手動アップデート」

コンポーネントのアップデートについて

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

- Mobile Security 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 でこれらの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 コンポーネントのアップデート

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

手動アップデート

[アップデート] 画面の [手動] タブで、サーバおよび Mobile Device エージェントを手動でアップデートできます。[アップデート元] 画面 (詳細については、108 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、106 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、108 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、106 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、107 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 9 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。

- 112 ページの「ログについて」
- 112 ページの「Mobile Device エージェントのログを表示する」
- 114 ページの「ログの削除設定」

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 エージェントのログ: Mobile Device エージェントがアプリ検索ログ、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。

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。
- 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:危険な Web ページや不正プログラムに感染した Web ページをブロックした場合に生成されます。Web 脅威検出ログは、生成されるとサーバにアップロードされます。

手順

1. Mobile Security の Web 管理コンソールにログオンします。
2. [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。

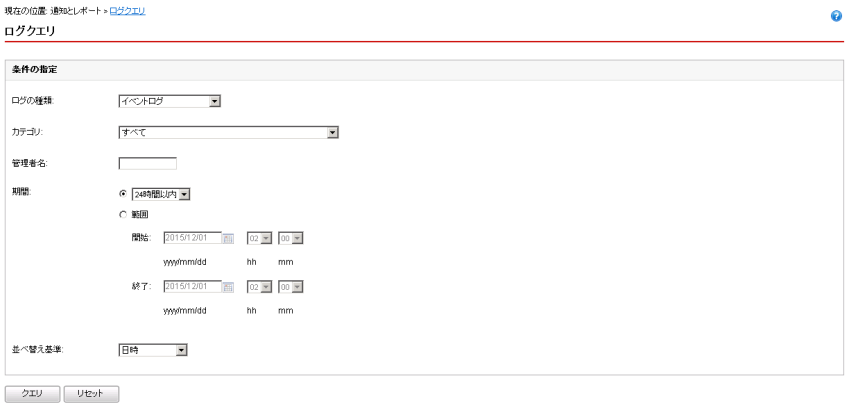


図 9-1. [ログクエリ] 画面

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. 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。
3. [ログの予約削除を有効にする] を選択します。
4. 削除するログの種類を選択します。
5. 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。
6. ログを削除する頻度と時刻を指定します。
7. [保存] をクリックします。

ログを手動で削除する

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] > [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。
3. 削除するログの種類を選択します。
4. 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。
5. [今すぐ削除] をクリックします。

第 10 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。

- 118 ページの「通知メッセージとレポートについて」
- 118 ページの「通知の設定」
- 118 ページの「メール通知を設定する」
- 119 ページの「管理者への通知」
- 120 ページの「レポート」
- 125 ページの「ユーザへの通知」

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. 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。

   [通知とレポートの設定] が表示されます。
3. [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。
4. 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。
5. [保存] をクリックします。

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、および推奨される解決方法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。

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] をクリックします。

   [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] をクリックします。

[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。

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。
- 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。

[レポート] 画面から次のタスクを実行できます。

表 10-1. 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、121 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、122 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、123 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、124 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 マネージメント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. [生成] 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、121 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、121 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。

ユーザへの通知を設定する

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] > [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。

3. 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
4. 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 11 章

トラブルシューティングとサポート情報

この章では、よくある質問の答えと、Mobile Security の追加情報を入手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。

- 128 ページの「トラブルシューティング」
- 130 ページの「トラブルシューティングのリソース」
- 131 ページの「製品サポート情報」
- 131 ページの「サポートサービスについて」
- 132 ページの「セキュリティニュース」
- 133 ページの「脅威解析・サポートセンター TrendLabs (トレンドラボ)」

トラブルシューティング

このセクションでは、Mobile Security を使用する際に生じる可能性のある問題を解決するためのヒントを提供します。

- コミュニケーションサーバのアンインストールプロセスをキャンセルすると、コミュニケーションサーバが適切に機能しなくなる

  アンインストールプロセスが起動してから停止するまでの間に、コミュニケーションサーバが適切に動作するために重要となるファイルおよびサービスの削除が開始された場合、コミュニケーションサーバが正常に機能しなくなることがあります。この問題を解決するには、コミュニケーションサーバを再びインストールして、設定します。

- SQL Server Express を使用している場合、データベースの設定を保存できない

  SQL Server Express を使用している場合は、[サーバのアドレス] で次の形式を使用します。`<SQL Server Express の IP アドレス>\sqlexpress`

  注意

  `<SQL Server Express の IP アドレス>` は、SQL Server Express の IP アドレスで置き換えます。

- SQL Server に接続できない

  この問題は、SQL Server の設定でリモート接続が許可されていない場合に発生することがあります。SQL Server Express Edition および SQL Server Developer Edition の初期設定ではリモート接続が許可されていません。リモート接続を許可するように SQL Server を設定するには、次の手順を実行します。

  1. リモートコンピュータから接続する SQL Server のインスタンスで、リモート接続を有効にします。
  2. SQL Server Browser サービスを有効にします。
  3. SQL Server および SQL Server Browser サービスに関連するネットワークトラフィックを許可するように、ファイアウォールを設定します。

- SQL Server 2008 R2 に接続できない

この問題は、初期設定の場所に Visual Studio 2008 がインストールされていないため、SQL Server 2008 セットアップで devenv.exe.config 設定ファイルを検索できない場合に発生することがあります。この問題を解決するには、次の手順を実行します。

1. <Visual Studio **インストールフォルダ**>¥Microsoft Visual Studio 9.0¥Common7¥IDE フォルダに移動し、devenv.exe.config ファイルを検索してコピーし、次のフォルダに貼り付けます (フォルダオプションで既知のファイルタイプの拡張子を表示するように設定する必要がある場合があります)。

   - 64 ビット OS の場合:

     ```
     C:¥Program Files (x86)¥Microsoft Visual Studio 9.0¥Common7¥IDE
     ```

   - 32 ビット OS の場合:

     ```
     C:¥Program Files¥Microsoft Visual Studio 9.0¥Common7¥IDE
     ```

2. SQL Server 2008 のセットアップをもう一度実行して、SQL Server 2008 の既存のインスタンスに BIDS 機能を追加します。

- デバイス管理画面でクライアントデバイスリストをエクスポートできない

  これは、Internet Explorer で暗号化ファイルのダウンロードが無効になっている場合に発生することがあります。次の手順を実行して、暗号化ファイルのダウンロードを有効にします。

  1. Internet Explorer で [ツール] > [インターネット オプション] を選択して、[インターネット オプション] の [詳細設定] タブをクリックします。
  2. [セキュリティ] で [暗号化されたページをディスクに保存しない] をオフにします。
  3. [OK] をクリックします。

- [ポリシー] ポップアップ画面の内容が表示されず、Internet Explorer でブロックされる

この問題は、.pac 自動設定ファイルを使用するように Internet Explorer が設定されている場合に発生します。この場合、Internet Explorer は、複数のフレームを含む安全な Web サイトへのアクセスをブロックします。この問題を解決するには、Internet Explorer の [信頼済みサイト] セキュリティゾーンに Mobile Security マネージメントサーバのアドレスを追加します。そのためには、次の手順を実行します。

1. Internet Explorer を起動します。
2. [ツール] > [インターネット オプション] を選択します。
3. [セキュリティ] タブで、[信頼済みサイト] をクリックし、[サイト] をクリックします。
4. [この Web サイトをゾーンに追加する] に Mobile Security マネージメントサーバの URL を入力し、[追加] をクリックします。
5. [OK] をクリックします。

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。

セキュリティニュース

トレンドマイクロ「セキュリティニュース」

トレンドマイクロでは、最新のセキュリティニュースをインターネットで公開しています。トレンドマイクロのセキュリティニュースでは、ウイルスやインターネットセキュリティに関する最新の情報を入手できます。セキュリティニュースは、次の URL からアクセスできます。

https://www.trendmicro.com/ja_jp/security-intelligence/breaking-news.html

- ウイルス名やキーワードから検索できる脅威データベース
- コンピュータウイルスの最新動向に関するニュース
- 現在流行中のウイルスや不正プログラムの情報
- デマウイルスまたは誤警告に関する情報
- ウイルスやネットワークセキュリティの予備知識

セキュリティニュースに定期的にアクセスして、流行中のウイルス情報などを入手することをお勧めします。メールによる定期的なウイルス情報配信を希望する場合は、警告メール配信の登録フォームを利用してメールアドレスを登録してください。

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専門のスタッフが解析し、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。

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

MDA のログ
- Web 脅威検出ログ, 112
- アプリ検索ログ, 112
- 概要, 112
- 検索条件, 113
- 手動削除, 115
- デバイス脆弱性ログ, 112
- ネットワーク保護ログ, 112
- 予約削除, 114
- ログの種類, 112

Mobile Security
- Active Directory, 16
- Microsoft SQL Server, 16
- Mobile Device エージェント, 16
- SMTP サーバ, 17
- 暗号化ソフトウェアの互換性, 14
- アーキテクチャ, 15
- ウイルスバスター Corp., 14
- 概要, 14
- 基本的なセキュリティモデル, 15
- クラウドコミュニケーションサーバ, 16
- コミュニケーションサーバ, 16
- コミュニケーションサーバの種類, 16
- コンポーネント, 15
- サブグループ, 70
- 証明書
  - SCEP, 17
  - SSL 証明書, 17
  - 管理, 45
  - 機関, 17
  - 公開鍵/秘密鍵, 17
  - セキュリティ認証情報, 17
- セキュリティ強化モデル
  - クラウドコミュニケーションサーバ, 15
  - ローカルコミュニケーションサーバ, 15
- 通信手段, 15
- 配置モデル, 15
- 不要なネットワーク通信, 14
- マネージメントサーバ, 16
- ローカルコミュニケーションサーバ, 16

root アカウントのプロパティ, 37

Web 管理コンソール, 28, 30
- URL, 28
- オプション, 28
- ユーザ名とパスワード, 29

か

管理者ログ
- 概要, 112

[管理対象デバイス] タブ, 70

互換表示, 30

コマンドのステータス, 43

コンポーネントのアップデート
- 概要, 106
- 手動, 106
- ダウンロード元, 108
- 予約, 107
- ローカル AU サーバ, 109

さ

最上位の管理者の役割のプロパティ, 37

新機能
- 9.6, 21

9.7, 19
9.8, 18
製品版ライセンス, 30
セキュリティ対策, 23

た

通知, 119
通知とレポート
概要, 118
トークン変数, 125
メールの設定, 125
定期的なアップデート, 24
デバイス検出ログ
ログの種類, 112
デバイス情報のアップデート, 78
トラブルシューティングのヒント, 128
.pac 自動設定ファイル, 130
devenv.exe.config 設定ファイル, 129
SQL Server 2008 R2, 128
SQL Server Express, 128
クライアントデバイスリスト, 129
コミュニケーションサーバ, 128

ま

モバイルデバイスの認証, 24
モバイルの脅威, 14
迷惑メール, 14

や

ユーザアカウントの詳細, 39

ら

レポート, 120