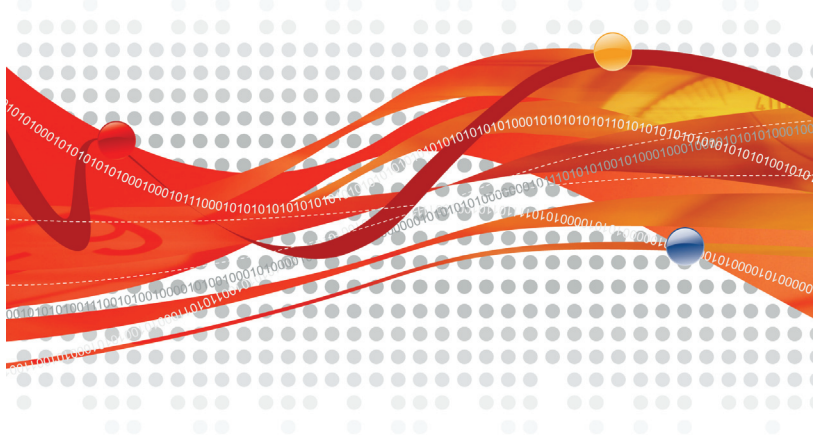
Trend Micro Mobile Security™ 5.1



管理者ガイド

安心を、ひとつ上のステージへ。

TREND MICRO™

トレンドマイクロへのお客様情報の送信について

「フィッシング詐欺対策」「URLフィルタ」では、Webサイトが安全かどうかの判定のために、お客様がアクセスしたURLの情報を暗号化してトレンドマイクロのサーバに送信します。

サーバに送信されたURL情報は、Webサイトの安全性の確認、および本機能の改良の目的にのみ利用されます。

また、これらの機能を有効にしたうえで、コモンゲートウェイインタフェースアプリケーションを使用しているサーバで構築されているWebサイトにアクセスし、ID、パスワード等を入力した場合には、お客様がアクセスしたWebページのURLにお客様が入力したID、パスワード等が含まれた状態でトレンドマイクロのサーバに送信される場合があります。この場合、トレンドマイクロでは、お客様がアクセスするWebページの安全性の確認のため、これらのお客様より受領した情報にもとづき、お客様がアクセスするWebページのセキュリティチェックを実施します。

「ソフトウェア安全性評価サービス」では、プログラムが安全かどうかの判定のために、プログラムの情報をトレンドマイクロのサーバに送信します。
「ウイルストラッキング/TrendCareプログラム」では、検出されたウイルス/脅威名、検出数、国/地域、感染元となったWebサイトのURLを、統計を取るためにトレンドマイクロのサーバに送信します。
「迷惑メール対策ツール」では、弊社製品の改良目的および迷惑メールの撲滅のため、トレンドマイクロのサーバに該当メールを送信します。また、迷惑メールの削減、迷惑メールによる被害の抑制を目指している政府関係機関に対して迷惑メール本体を開示する場合があります。

輸出規制について

本製品は、外国為替及び外国貿易法、U.S. Export Administration Regulations、およびその他の国における輸出規制品目に該当している場合があります。したがって、本製品が輸出規制品目に該当する場合、適正な政府の許可なくして、禁輸国もしくは貿易制裁国の企業、居住者、国民、または、取引禁止者、取引禁止企業に対して、輸出もしくは再輸出できません。このような規制についての情報は以下のウェブサイトから見つけることができます。

「http://www.treas.gov/ofac/」、および「http://www.bis.doc.gov/complianceandenforcement/ListsToCheck.htm」

2008年12月現在、米国により定められる禁輸国は、キューバ、イラン、北朝鮮、スーダン、シリアが含まれています。

あなたは本製品に関連した米国輸出管理法令の違法行為に対して責任があります。本契約の同意により、あなたは、あなたが米国により現時点で禁止されている国の居住者もしくは国民ではないこと、別途本製品を受け取ることが禁止されていないことを確認します。また、大量破壊を目的とした、核兵器、化学兵器、生物兵器、ミサイルの開発、設計、製造、生産を行うために使用しないことに同意します。

複数年契約について

お客様が複数年契約（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://jp.trendmicro.com/jp/support/lifecycle/index.html

著作権について

商標について

P/N: TMMSFF-AE0100_51 (2009/5)

目次

はじめに

Trend Micro Mobile Security 5.1 (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。このガイドでは、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独自のセキュリティ対策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、企業環境でモバイルデバイス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 (Smartphone や Windows Mobile/Windows Mobile Phone など) 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。

- **管理者ガイド** — このガイドは詳細な Mobile Security 設定ポリシーおよびテクノロジについて説明します。
- **クライアント配信ガイド** — このガイドは Mobile Security について紹介し、ネットワークの計画とインストールを支援して、配信の準備および稼動をサポートします。
- **ユーザガイド** — このガイドは、ユーザに Mobile Security の基本的な概念を紹介し、モバイルデバイスにおける Mobile Security 設定の手順を説明します。
- **オンラインヘルプ** — オンラインヘルプの目的は、製品の主なタスクの操作手順、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することです。

- **Readme** — Readme には、オンライン版または印刷版のドキュメントには記載されていない最新の製品情報が含まれています。トピックには、新機能の説明、インストールのヒント、既知の問題、およびリリース履歴があります。
- **製品 Q&A** — 製品 Q&A は、問題解決とトラブルシューティングに関する情報のオンラインデータベースです。ここでは、製品の既知の問題に関する情報が提供されています。製品 Q&A を調べるには、次のアドレスにアクセスしてください。

  http://esupport.trendmicro.co.jp/supportjp/smb/search.do

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://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、次の表記規則を使用しています。

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

表 1. 本書で使用している表記規則

第 1 章

製品の紹介

Trend Micro Mobile Security 5.1 (以下、Mobile Security) は、モバイルデバイス向けの統合セキュリティソリューションです。この章を読んで Mobile Security の機能とモバイルデバイスを保護する方法を理解してください。

この章には、次の節が含まれています。

モバイルの脅威について

プラットフォームの標準化と、その接続性が増大するにつれ、モバイルデバイスはより多くの脅威にさらされる可能性があります。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、より多くのスパムメールメッセージが 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。

不正プログラム、スパムメール、またはその他の不要なコンテンツによってもたらされる脅威に加えて、モバイルデバイスはハッキングやサービス拒否 (DoS) 攻撃の影響も受けやすくなっています。モバイルデバイスの多くは、従来はより大型のコンピュータデバイスであるノートブックコンピュータやデスクトップコンピュータなどにしか結びつきのなかったネットワーク接続と同じ接続性を備えているため、今やそのような脅威の対象となっています。

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洩につながります。

Trend Micro Mobile Security 5.1 について

Mobile Security は、モバイルデバイスの包括的なセキュリティソリューションです。Mobile Security にはトレンドマイクロの不正プログラム対策テクノロジが組み込まれていて、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。

組み込みのファイアウォールおよび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。これらの不要なネットワーク通信とは、SMS メッセージ、WAP プッシュメール、3G/GPRS 接続経由で受信するデータなどです。

Mobile Security の最新バージョンでは、集中的なデバイス管理および自動的なポリシー設定やコンポーネントのアップデートを行うウイルスバスター コーポレートエディション (以下、ウイルスバスター Corp.) の統合をサポートします。また Mobile Security には、サポートされるモバイルデバイスにログオンパスワード保護およびデータ暗号化機能を提供する個別の暗号化モジュールが含まれています。この個別の暗号化モジュールは、物理的なデバイスの紛失または盗難によるデータの漏洩防止に役立ちます。

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できません。不正プログラム検索、SMS 管理、ファイアウォール保護など同様の機能を提供するソフトウェア製品には、Mobile Security との互換性がない場合があります。

Mobile Security コンポーネント

この節では、一般的なネットワーク環境における各 Mobile Security コンポーネントのインストール、および他のコンポーネントと連動する仕組みについて説明します。ネットワークのトポロジやニーズによっては、オプションのコンポーネントをインストールする場合があります。

Mobile Security は、次の 4 つのコンポーネントで構成されています。TMMS 管理サーバ、TMMS アップデートサーバ、SMS Sender、およびモバイルデバイスエージェントです。次の図は、一般的なネットワークにおける各 Mobile Security コンポーネントの配置場所を示しています。

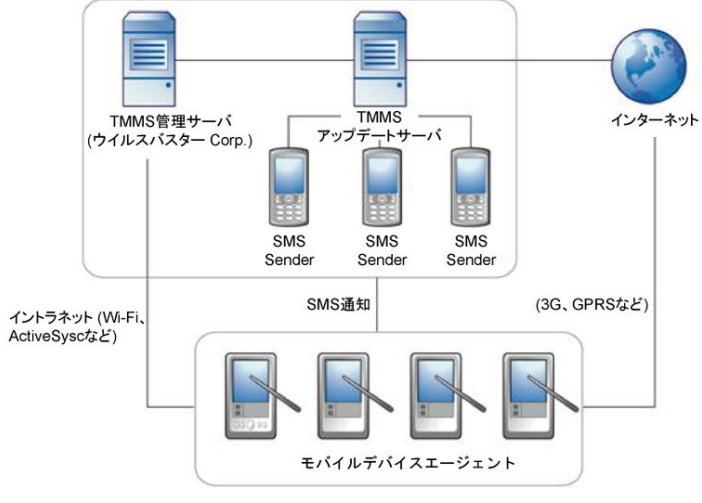


図 1-1.　Mobile Security コンポーネント

TMMS 管理サーバ

TMMS 管理サーバは、ウイルスバスターCorp. サーバのプラグインプログラムの 1 つで、これを使用するとウイルスバスター Corp. の web 管理コンソールからモバイルデバイスエージェントを制御できます。モバイルデバイスが TMMS 管理サーバに登録されたら、モバイルデバイス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。また TMMS 管理サーバを使用して、SMS Sender を制御および監視する TMMS アップデートサーバにコマンドを送信することもできます。これらのコマンドに基づいて SMS Sender からモバイルデバイスエージェントに通知が行われます。

モバイルデバイスエージェントは、イントラネットの Wi-Fi 接続または 3G/GPRS 接続経由で、TMMS 管理サーバに直接接続できます。モバイルデバイスエージェントのステータス、情報、およびログは、TMMS 管理サーバに格納されます。

TMMS アップデートサーバ

TMMS アップデートサーバは、SMS Sender を制御し、TMMS 管理サーバとモバイルデバイスエージェント間の通信を処理します。TMMS アップデートサーバを使用すると、TMMS 管理サーバで企業のイントラネット外部にあるモバイルデバイスエージェントを管理できます。モバイルデバイスエージェントを TMMS アップデートサーバのパブリック IP アドレスに接続できます。

TMMS アップデートサーバはオプションのコンポーネントの 1 つです。次のような場合、TMMS アップデートサーバをインストールする必要があります。

- モバイルデバイスのアップデートや監視に伴う TMMS 管理サーバの負荷を軽減する
- SMS Sender を介してモバイルデバイスに SMS メッセージを送信する
- ウイルスバスターCorp. サーバをパブリックアクセスに公開することなく TMMS 管理サーバにセキュリティ層を追加する

ウイルスバスター Corp. の web 管理コンソールを使用して、TMMS アップデートサーバにポリシーを設定できます。

SMS Sender

SMS Sender は、WLAN 接続または ActiveSync (バージョン 4.0 以降) を介して TMMS アップデートサーバに接続された専用モバイルデバイスです。SMS Sender はコマンドを TMMS アップデートサーバから受信し、SMS メッセージを送信することによりそれらのコマンドをモバイルデバイスへ転送します。

SMS メッセージを使用して、モバイルデバイスに次のタスクを実行するよう通知できます。

- モバイルデバイスエージェントのダウンロードおよびインストール
- TMMS 管理サーバへのモバイルデバイスエージェントの登録
- TMMS 管理サーバからのモバイルデバイスエージェントコンポーネントのアップデート
- リモートデバイスの消去
- TMMS 管理サーバとのポリシーの同期

注意： 最大 64 個の SMS Sender を同時に TMMS アップデートサーバに接続できます。

モバイルデバイスエージェント

自動インストール方式である、Service Load (SL) メッセージ、SMS メッセージ通知、メモリカード、Device Management (DM) フレームワークのうちのいずれか、または手動インストールを使用して、モバイルデバイスエージェントをサポート対象のプラットフォームにインストールします。モバイルデバイスエージェントは、不正プログラム、不要な SMS/WAP プッシュメッセージ、またはネットワークトラフィックからのシームレスな保護を提供します。ユーザはリアルタイムの検索、ファイアウォールによる保護、データ暗号化などの利点が得られると同時に、モバイルデバイスでメッセージを送受信したりファイルを開いたりすることもできます。

Mobile Security 5.1 の新機能

Mobile Security 5.1 で提供される新機能は次のとおりです。

モバイルデバイスのコンポーネントの有効化 / 無効化

管理者は Windows ベースのモバイルデバイスで特定の機能を使用可能にするかどうかを制御できます。

SMS Sender のステータス

SMS Sender のステータスが SMS Sender モバイルデバイスに表示されるようになりました。詳細については、32 ページの「SMS Sender のステータス」を参照してください。

SMS スパムメール対策ポリシー

管理者は SMS スパムメール対策ポリシーを一括、またはドメインごとに制御できます。詳細については、18 ページの「SMS スパムメール対策」を参照してください。

WAP プッシュ保護ポリシー

以前のバージョンでは、エンドユーザのみが WAP プッシュ保護を制御できました。本リリースでは、管理者とエンドユーザの両方が WAP プッシュ保護を制御できるようになりました。詳細については、19 ページの「WAP プッシュ保護」を参照してください。

アンインストール防止の有効化

以前のバージョンでは、ユーザはモバイルデバイスエージェントを管理者に知らせることなくアンインストールできました。この機能は企業のセキュリティポリシーに違反する可能性がありました。本リリースでは、管理者はアンインストーラをパスワードで保護することによってモバイルデバイスエージェントのアンインストールを制限できます。

オンデマンドのリモート消去

本リリースでは、管理者はリモートでハードディスク / メモリカードをクリアしたり、モバイルデバイスを工場出荷時の設定にリセットしたりできます。この新機能によって、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。

SMS Sender の監視

本リリースでは、いずれかの SMS Sender が切断された場合に、メールメッセージが管理者に送信されます。詳細については、33 ページの「SMS Sender の監視」を参照してください。

アップデートされた「概要」画面

「概要」画面に次の項目が表示されるようになりました。

- 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
- アップデート対象のサーバおよびコンポーネントのアップデートステータス数
- アップデート対象のサーバおよびコンポーネントのアップデートステータス

モバイルデバイスエージェントの主要機能

不正プログラム検索

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。Mobile Security を使用すると、感染ファイルを隔離および削除できます。

ファイアウォール

Mobile Security には、トレンドマイクロのファイアウォールモジュールが含まれます。これには、ネットワークトラフィックをフィルタするための事前定義されたセキュリティレベルが設定されています。独自のフィルタルールを定義し、特定の IP アドレスまたは特定のポートのネットワークトラフィックをフィルタすることもできます。IDS (侵入検知システム) を使用すると、モバイルデバイスに連続的に多数のパケットを送信しようとする試みをブロックできます。そのような試みは通常、DoS (サービス拒否) 攻撃であり、モバイルデバイスをビジー状態にさせ、他の接続を受信できないようにします。

SMS スパムメール対策

モバイルデバイスでは、SMS メッセージング経由で、しばしば迷惑メッセージやスパムメールを受信します。不要な SMS メッセージをスパムメールフォルダにフィルタするには、スパムメールと見なすすべての SMS メッセージの送信元の電話番号を指定するか、または電話番号の除外リストを指定して、Mobile Security で除外リストに存在しない送信者からのすべてのメッセージをフィルタするように設定できます。また、識別できない SMS メッセージまたは送信者の電話番号が表示されないメッセージもフィルタできます。モバイルデバイスは、これらのメッセージを自動で受信ボックスのスパムメールフォルダに格納します。

注意： SMS スパムメール対策機能は、電話機能のないモバイルデバイスでは使用できません。
このポリシーを TMMS 管理サーバからモバイルデバイスエージェントに設定することはできません。ユーザは、各自のモバイルデバイス上でこの機能を有効または無効にできます。

WAP プッシュ保護

WAP プッシュは、コンテンツをモバイルデバイスに自動的に配信する強力な機能です。コンテンツの配信を開始するには、WAP プッシュメッセージと呼ばれる特殊なメッセージがユーザに送信されます。これらのメッセージには、通常コンテンツに関する情報が含まれ、それによってユーザはコンテンツを受け入れるか拒否するかを選択できます。

悪意のあるユーザは、誤った情報や無用な WAP プッシュメッセージを送信し、ユーザにとって不要なアプリケーション、システム設定、もしくは不正プログラムを含むコンテンツを受け取るようにします。Mobile Security では、ユーザは信頼された送信者のリストを使用して、WAP プッシュメッセージをフィルタし、モバイルデバイスに不要なコンテンツが配信されることを防ぐことができます。

注意： WAP プッシュ保護機能は、電話機能のないモバイルデバイスでは使用できません。
このポリシーを TMMS 管理サーバからモバイルデバイスエージェントに設定することはできません。ユーザは、各自のモバイルデバイス上でこの機能を有効または無効にできます。

データ暗号化

Mobile Security は、モバイルデバイスおよびメモリカードに格納されたデータに対して、動的なデータ暗号化を提供します。暗号化するデータの種類および使用する暗号化アルゴリズムを指定できます。

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。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 Patch のアップデートが含まれます。

ログ

TMMS 管理サーバでは、次のモバイルデバイスエージェントログを使用できます。

- 不正プログラムログ
- 暗号化ログ
- ファイアウォールログ
- イベントログ

モバイルデバイス上で、次のログを表示できます。

- 検索ログ (不正プログラムログ)
- ファイアウォールログ
- スパムメールログ
- WAP プッシュログ
- タスクログ

第 2 章

使用開始

この章では、Trend Micro Mobile Security (以下、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示します。開始する前に、ウイルスバスターCorp. サーバに TMMS 管理サーバを、モバイルデバイスにモバイルデバイスエージェントをそれぞれインストールする必要があります。

この章には、次の節が含まれています。

Mobile Security 管理コンソールへのアクセス

TMMS 管理サーバは、ウイルスバスターCorp. サーバにインストールされているプラグインプログラムです。ウイルスバスター コーポレートエディション (以下、ウイルスバスター Corp.) Web 管理コンソールを介して、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従って構成できます。

Web 管理コンソールを使用すると、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モバイルデバイスエージェントの管理
- モバイルデバイスエージェントのセキュリティポリシーの設定
- 設定と管理を容易にするための、論理ドメインへのデバイスのグループ化
- 単一または複数のモバイルデバイスでの検索の設定
- 登録情報およびアップデート情報の表示

Mobile Security の管理コンソールにアクセスするには

1. ウイルスバスター Corp. の web 管理コンソールにログオンし、[プラグインマネージャ] をクリックします。
2. Mobile Security の [プログラムの管理] をクリックします。

概要情報

TMMS 管理サーバにアクセスすると、[概要] 画面が最初に表示されます。この画面には、モバイルデバイスの登録ステータス、待機中の SMS メッセージ、およびコンポーネントの詳細が表示されます。

[概要] 画面の [待機中の SMS メッセージ] セクションは、5 秒間隔で自動的にアップデートされます。[表示更新] をクリックすると、この画面を手動でアップデートできます。

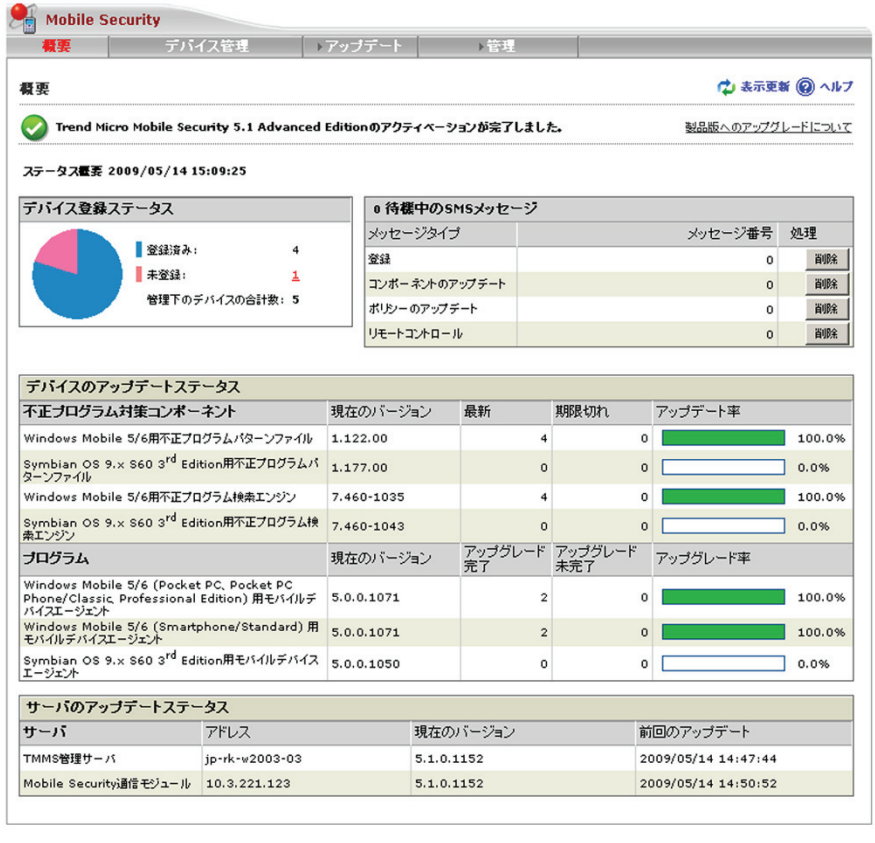


図 2-1.　[概要] 画面

[概要] 画面では、次の作業を実行できます。

- 製品登録ステータスを表示する、または [製品版へのアップグレードについて] をクリックして製品ライセンスを更新する。
- 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。使用するモバイルデバイスエージェントのインストール方法によっては、モバイルデバイスが TMMS 管理サーバに自動的に登録される場合がありますが、そうでなければ管理者が手動でデバイスを登録する必要があります。

  モバイルデバイスは、次のいずれかの場合に、非登録のままになる可能性があります。

  - TMMS 管理サーバへの接続が失敗した
  - モバイルデバイスのユーザが登録 SMS メッセージを削除した
  - 登録情報を含む SMS メッセージが、配信中に失われた

  注意： 注意 : モバイルデバイスの仕様によっては TMMS 管理サーバに手動登録が必要です。

- 配信待機中の SMS メッセージの数を表示する、または [削除] をクリックして待機中のすべての SMS メッセージを削除する。
- 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** — モバイルデバイスエージェントまたは TMMS 管理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** — 最新のモバイルデバイス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** — 最新のモバイルデバイス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** — 最新のモバイルデバイス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** — 最新のモバイルデバイス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** — TMMS 管理サーバの名前
  - **アドレス** — TMMS 管理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 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

製品ライセンス

TMMS 管理サーバに対して購入するアクティベーションコード (シリアル番号) の種類によって、使用可能な機能および機能の有効期限が異なります。

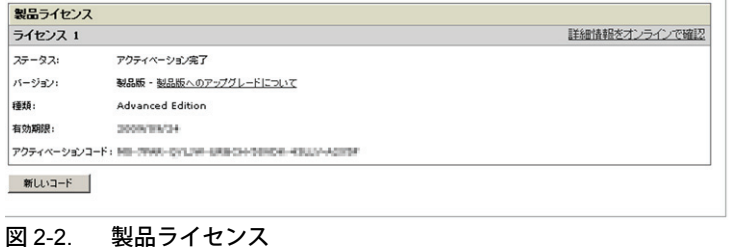


図 2-2. 製品ライセンス

Mobile Security には Standard Edition と Advanced Edition の 2 種類のライセンスがあります。Standard Edition のライセンスでは、不正プログラム対策機能、スパムメール対策機能、WAP プッシュ保護機能、およびファイアウォール機能が利用可能です。Advanced Edition のライセンスでは、Standard Edition のライセンスと同じ機能に加え、暗号化機能、機能のロック機能、およびオンデマンドのリモート消去機能も利用可能です。

体験版ライセンスの有効期限が切れると、すべての機能が無効になり、暗号化モジュールがモバイルデバイスからアンインストールされます。また、モバイルデバイス上および挿入されたメモリカード上の暗号化されたデータはすべて復号化されます。製品版ライセンスでは、ライセンス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、モバイルデバイス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。

ライセンスの有効期限が切れた場合は、新しいアクティベーションコードで TMMS 管理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。

アップデートをダウンロードしてリモート管理を可能にするには、モバイルデバイスエージェントを TMMS 管理サーバに登録する必要があります。モバイルデバイスから手動でモバイルデバイスエージェントを登録する手順については、モバイルデバイスプラットフォームの「クライアント配信ガイド」または「ユーザガイド」を参照してください。

ウイルスバスターCorp. サーバ上の TMMS 管理サーバのライセンスの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] 画面の [製品の更新について] リンクをクリックしてください。

SMS Sender の設定

TMMS 管理サーバでは、TMMS アップデート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、モバイルデバイス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、およびセキュリティポリシーの設定を実行するように、モバイルデバイスにメッセージを送信します。

[SMS Sender 設定] メニューオプションを使用すると、次のことを実行できます。

- SMS Sender の電話番号の設定
- SMS Sender の接続ステータスの表示
- モバイルデバイスエージェントのインストールメッセージの設定
- 送信を待機している SMS メッセージの削除または表示
- SMS Sender の切断通知の設定

SMS Sender リスト

TMMS 管理サーバで、モバイルデバイスへメッセージを送信するよう SMS Sender に指示するには、SMS Sender デバイスの電話番号を設定する必要があります。

警告： SMS Sender リスト内で SMS Sender の電話番号を設定しないと、その SMS Sender はモバイルデバイスにメッセージを送信できなくなります。

SMS Sender リストを表示するには

1. ウイルスバスター Corp. の web 管理コンソールにログオンし、[プラグインマネージャ] をクリックします。
2. Mobile Security の [プログラムの管理] をクリックします。

3. [管理]→[SMS Sender 設定] をクリックします。[SMS Sender リスト] 画面に、SMS Sender の電話番号および接続ステータスの一覧が表示されます。SMS Sender が TMMS アップデートサーバに正常に接続された場合、[ステータス] フィールドに [接続されました] と表示されます。

注意： SMS メッセージの送信試行に 3 回失敗すると、モバイルデバイスに [切断されました] と表示されます。

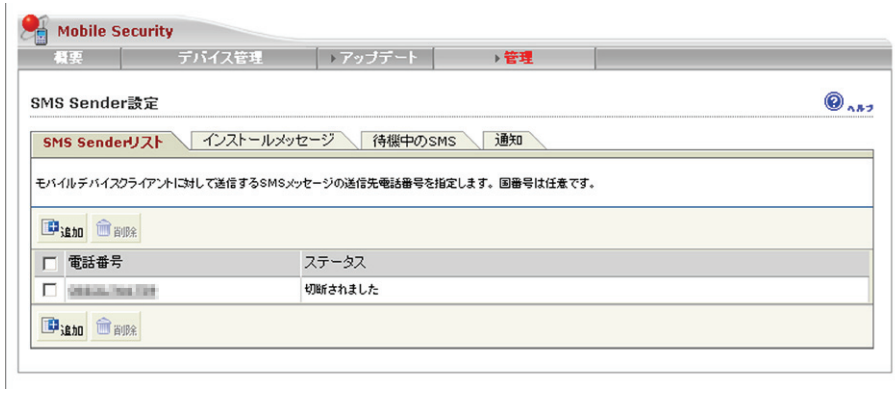


図 2-3. [SMS Sender 設定] 画面の [SMS Sender リスト] タブ

SMS Sender リストの設定

SMS Sender の電話番号を指定して、TMMS 管理サーバが SMS Sender を管理できるようにします。SMS Sender は、モバイルデバイスにメッセージを送信して、以下のことを通知します。

- モバイルデバイスエージェントのダウンロードおよびインストール
- TMMS 管理サーバへの登録
- TMMS 管理サーバからの登録解除
- モバイルデバイスエージェントコンポーネントのアップデート
- TMMS 管理サーバとのセキュリティポリシー設定の同期

SMS Sender の電話番号を設定するには

1. ウイルスバスター Corp. の web 管理コンソールにログオンし、[プラグインマネージャ] をクリックします。
2. Mobile Security の [プログラムの管理] をクリックします。
3. [管理]→[SMS Sender 設定] をクリックします。
4. [SMS Sender リスト] 画面で [追加] をクリックします。
5. [電話番号の追加] 画面で、SMS Sender の電話番号を入力して [保存] をクリックします。
6. [SMS Sender リスト] 画面が表示されます。設定した番号の [ステータス] フィールドに [接続されました] と表示されていることを確認します。[ステータス] フィールドに [切断されました] と表示されている場合は、SMS Sender デバイスが TMMS アップデー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： 既存の SMS Sender は、電話番号をクリックすることによって変更できます。

インストールメッセージの設定

モバイルデバイスエージェントのサイレントインストールを開始するために、SMS Sender はモバイルデバイスに WAP プッシュメッセージと SMS メッセージを送信して、モバイルデバイスエージェントのダウンロードとインストールを実行するように通知します。

モバイルデバイスが Service Load (SL) メッセージを処理できない場合は、ユーザは SMS メッセージを開き、メッセージ内の URL をクリックして、モバイルデバイスエージェントのセットアップパッケージをダウンロードできます。

[インストールメッセージ] 画面を使用して、SMS メッセージに表示するメッセージを入力します。

インストールメッセージを変更するには

1. ウイルスバスター Corp. の web 管理コンソールにログオンし、[プラグインマネージャ] をクリックします。
2. Mobile Security の [プログラムの管理] をクリックします。
3. [管理]→[SMS Sender 設定] をクリックします。
4. [インストールメッセージ] タブをクリックします。[インストールメッセージ] 画面が表示されます。

図 2-4. 初期設定の SMS メッセージの設定

5. テキストボックスにメッセージを入力します。

> **注意：** インストールメッセージには、「%s」文字が含まれている必要があります。この文字は自動的に、モバイルデバイスエージェントのセットアップファイルをダウンロードするための URL で置き換えられます。

6. [保存] をクリックします。

待機中の SMS メッセージ

TMMS 管理サーバでは、以下のタスクが実行されたときに自動的に SMS メッセージが生成されます。

- モバイルデバイスの追加
- 電話番号が TMMS 管理サーバに指定されているモバイルデバイスの削除
- 新しい製品アクティベーションコードの入力
- TMMS アップデートサーバのパブリック IP アドレスの変更
- ドメインポリシーの変更と全モバイルデバイスへの適用の選択
- モバイルデバイスの消去

SMS Sender によって処理可能なメッセージ数を超えると、SMS メッセージは待機中になります。

[概要] 画面または [待機中の SMS] 画面で、SMS メッセージの待機のステータスを表示することができます。

- **登録** — モバイルデバイスエージェントのインストールまたは TMMS 管理サーバへの登録をモバイルデバイスに通知します。このメッセージの待機には、登録解除およびプロビジョニングの通知も含まれます。
- **コンポーネントのアップデート** — アップデートされた Mobile Security コンポーネントを TMMS 管理サーバから取得するようにモバイルデバイスエージェントに通知します。
- **ポリシーのアップデート** — TMMS 管理サーバからセキュリティポリシー設定をアップデートするようにモバイルデバイスエージェントに通知します。

- **リモートコントロール** — 未送信で待機しているリモートコマンドの数を表示します。

図 2-5.　待機中の SMS

SMS メッセージは攻撃者に傍受されても内容の読み取りができないように常に暗号化されています。[削除] をクリックすると、選択されているメッセージの待機がクリアされます。この操作で、選択した待機中の SMS メッセージはすべてクリアされ、送信されなくなります。

SMS Sender のステータス

Mobile Security では、モバイルデバイスに表示される SMS Sender のステータスがアップデートされます。接続ステータスに応じて、次のステータスがデバイスに表示されます。

- SMS エージェントのステータス : 正常
- SMS エージェントのステータス : 停止
- SMS エージェントのステータス : 切断
- SMS エージェントのステータス : 未使用

- SMS エージェントのステータス : 不明

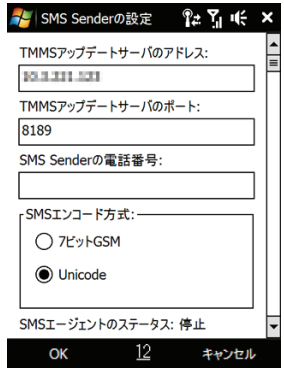


図 2-6.　SMS Sender のステータス

SMS Sender の監視

Mobile Security では、SMS Sender のステータスを監視して、10 分を超えて切断されている SMS Sender があった場合はメール通知を送信できます。また、SMS Sender デバイスには、エージェントの停止、エージェントの実行、エージェントの未使用、またはエージェントの切断の接続ステータスが表示されます。

[通知] 画面を使用して、メッセージの件名、受信者、および SMTP サーバ詳細を入力します。

ヒント： 必要に応じて、OfficeScan/Addon/Mobile Security にある TmOMSM.ini ファイルで、特定の SMS Sender のユーザ名とパスワードを変更できます。

SMS Sender を監視するには

1. ウイルスバスター Corp. の web 管理コンソールにログオンし、[プラグインマネージャ] をクリックします。
2. Mobile Security の [プログラムの管理] をクリックします。

3. [管理]→[SMS Sender 設定] をクリックします。

4. [通知] タブをクリックします。[通知] タブが表示されます。

図 2-7.　SMS Sender 通知

5. [SMS Sender のステータスが異常な場合にメール通知を送信] チェックボックスを選択します。

6. 必要に応じて次の詳細をアップデートします。

   - **SMTP サーバ** — SMTP サーバの詳細。
   - **ポート番号** — メールメッセージの送信に使用するポート。初期設定の値は 25 です。
   - **差出人** — 送信者のメールアドレス。
   - **宛先** — 受信者のメールアドレス。複数のメールアドレスは、セミコロンで区切ることができます。
   - **件名** — メールメッセージの件名。

注意： メールメッセージの本文を編集するには、必要に応じて、¥OfficeScan¥Addon¥Mobile Security にある TmOMSM.ini の MailBody セクションをアップデートします。

7. [保存] をクリックします。

ログの削除設定

モバイルデバイス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 TMMS 管理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。

ハードディスクの使用容量を抑えるために、ログを手動で削除することも、自動削除をスケジュールするように TMMS 管理サーバを設定することもできます。

ログの削除をスケジュールするには

1. ウイルスバスター Corp. の web 管理コンソールにログオンし、[プラグインマネージャ] をクリックします。
2. Mobile Security の [プログラムの管理] をクリックします。
3. [管理]→[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。
4. [ログの予約削除を有効にする] を選択します。
5. 不正プログラム、ファイアウォール、暗号化、またはイベントのうち、削除するログの種類を選択します。
6. 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。
7. ログを削除する頻度と時刻を指定します。
8. [保存] をクリックします。

手動でログを削除するには

1. ウイルスバスター Corp. の web 管理コンソールにログオンし、[プラグインマネージャ] をクリックします。
2. Mobile Security の [プログラムの管理] をクリックします。

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

Mobile Security ドメイン

ウイルスバスター Corp. と同様、Mobile Security 内のドメインとは、同じ設定を共有し、同じタスクを実行するモバイルデバイスエージェントのグループを指します。モバイルデバイスエージェントをドメインにグループ化することで、すべてのドメインメンバーに対して同様の設定内容を設定、管理、および適用することができます。

モバイルデバイスの管理

Mobile Security ドメインを設定するには、[デバイス管理] をクリックします。

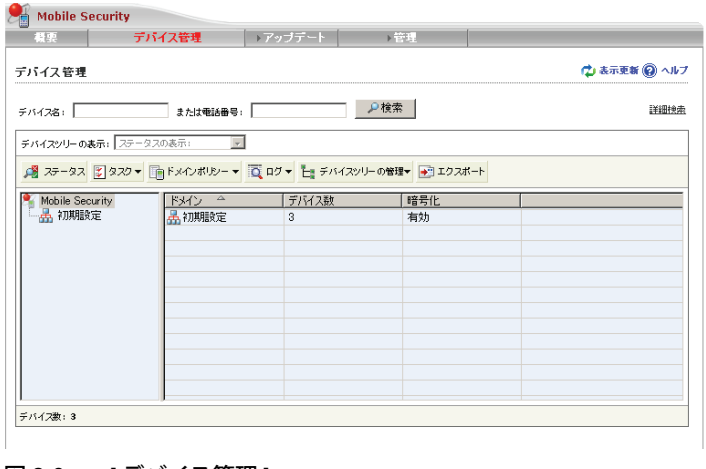


図 2-8. [デバイス管理]

[デバイス管理] 画面では、モバイルデバイス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。

- モバイルデバイスエージェントのステータスの検索と表示
- オンデマンドでのモバイルデバイスエージェントコンポーネントのアップデート、登録、リモートデバイスの消去、および設定の同期化
- 以下のドメイン固有のポリシーの設定：一般ポリシー、ファイアウォールポリシー、SMS スパムメール対策ポリシー、WAP プッシュ保護ポリシー、暗号化ポリシー、およびデバイスコンポーネントの有効化 / 無効化 (44 ページの「セキュリティポリシーについて」を参照)
- モバイルデバイスエージェントのイベントログの表示
- デバイスツリーの設定 (ドメインの追加、削除、名前変更、およびモバイルデバイスエージェントの追加、削除など)
- 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

次の表は、モバイルデバイスのアップデートステータスを示すためにデバイスツリーに表示されるアイコンの説明をまとめたものです。

アイコン	説明
	モバイルデバイスエージェントは、TMMS 管理サーバに正常に登録されています。
	モバイルデバイスエージェントは、TMMS 管理サーバに登録されていません。
	モバイルデバイスエージェントのコンポーネントの中に、アップデートされていないものがあります。
	モバイルデバイスエージェントコンポーネントはすべてアップデートされています。
	セキュリティポリシーの中に、TMMS 管理サーバと同期していないものがあります。
	すべてのセキュリティポリシーが TMMS 管理サーバと同期されています。

表 2-1.　デバイスツリーのアイコン

モバイルデバイス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に従ってモバイルデバイスエージェントを検索するには、[デバイス管理] 画面で情報を入力し、[検索] 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。

モバイルデバイスエージェントの詳細検索

[詳細検索] 画面を使用して、モバイルデバイスエージェントの追加検索条件を指定できます。

モバイルデバイスエージェントの詳細検索を実行するには

1. [デバイス管理] 画面の [詳細検索] リンクをクリックします。ポップアップウィンドウが表示されます。
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** — モバイルデバイスを特定できるわかりやすい名前
   - **電話番号** — モバイルデバイスの電話番号
   - **プラットフォーム** — モバイルデバイスで実行されている OS
   - **ドメイン** — モバイルデバイスが属するドメイン
   - **プログラムバージョン** — モバイルデバイスのモバイルデバイスエージェントのバージョン番号
   - **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
   - **感染クライアント** — 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
   - **未登録のデバイス** — 未登録のモバイルデバイスのみに検索範囲を絞り込む

- **期限切れ設定ファイル** — 期限切れの設定ファイルを持つモバイルデバイスのみに検索範囲を絞り込む
- **期限切れコンポーネント** — 期限切れのコンポーネントを持つモバイルデバイスのみに検索範囲を絞り込む

3. [検索] 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。

デバイスツリーの表示オプション

[デバイスツリーの表示] リストで、事前定義されているビューを選択できます。定義されているビューとは、[ステータスの表示]、[不正プログラム対策の表示]、[ファイアウォールの表示]、および [すべて表示] です。これによって、デバイスツリーに表示された情報をすぐに確認できます。デバイスツリーに表示される情報は、選択したオプションによって異なります。

デバイスツリーの管理

[デバイスツリーの管理] メニューオプションを使用して、Mobile Security のドメインとモバイルデバイスエージェントを設定します。

TMMS 管理サーバは、Mobile Security デバイスツリーに「Mobile Security」ドメイン (ルートドメイン) と「初期設定」ドメインの 2 つのドメインを自動的に作成します。「初期設定」ドメインには、ドメインが指定されていないモバイルデバイスエージェントが含まれています。これは、モバイルデバイスを追加した際に、そのモバイルデバイスが属する Mobile Security ドメインを指定していないためです。Mobile Security デバイスツリーの「Mobile Security」ドメインおよび「初期設定」ドメインを削除したり、名前を変更したりすることはできません。

ヒント： ルートドメイン (「Mobile Security」ドメイン) に設定を適用した場合、[[保存] をクリックして、変更をすべてのドメインに適用します] を選択することによって、他のドメインにもその設定を適用できます。

手順については、TMMS 管理サーバの「オンラインヘルプ」を参照してください。

モバイルデバイスエージェントのプロビジョニング

ユーザは、製品の登録、コンポーネントのアップデート、および設定の同期のプロセスをモバイルデバイスからいつでも開始できます。また、TMMS 管理サーバを手動で設定して、これらのプロセスを実行するように SMS メッセージをモバイルデバイスエージェントに送信することもできます。

[デバイスのアップデート] 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。詳細については、74 ページの「デバイスのアップデート」を参照してください。

手動でアップデートプロセスを開始するには、ウイルスバスターCorp. サーバで Mobile Security の [デバイス管理] 画面の [タスク] メニューを選択します。

- **アップデート** — TMMS 管理サーバで使用可能な最新のコンポーネントにアップデートするようにモバイルデバイスエージェントに通知を送信します。
- **登録** — TMMS 管理サーバに登録するようにモバイルデバイスエージェントに通知を送信します。
- **同期設定** — TMMS 管理サーバのセキュリティポリシー設定を同期するようにモバイルデバイスエージェントに通知を送信します。

注意： [ドメインポリシー] 画面でのセキュリティポリシー設定の変更後、すぐにモバイルデバイスエージェントの設定を同期することをお勧めします。

Mobile Security の SMS メッセージング機能を有効にしていない場合、モバイルデバイスまたは [一般ポリシー] 画面 (45 ページの「一般ポリシー」を参照) で、定期的にコンポーネントをアップデートするように予約アップデートを設定する必要があります。

リモートによるデバイスのロック解除

ユーザがパワーオンパスワードを忘れた場合、TMMS 管理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、ユーザはログオンしてパワーオンパスワードを変更できるようになります。

モバイルデバイスでユーザ確認のためのコード (16 桁の 16 進数) を生成するようにユーザに要求しないと、リモートでモバイルデバイスのロック解除を行うことはできません。

リモートでモバイルデバイスをリセットするには

1. モバイルデバイス名、およびユーザがモバイルデバイスで生成したユーザ確認のためのコードを取得します。ユーザ確認のためのコードの生成手順については、「クライアント配信ガイド」または「ユーザガイド」を参照してください。
2. ウイルスバスター Corp. の web 管理コンソールにログオンし、[プラグインマネージャ] をクリックします。
3. Mobile Security の [プログラムの管理] をクリックして、[管理]→[リモートによるパスワードのリセット] をクリックします。

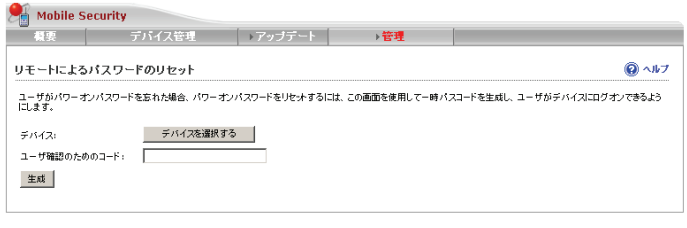


図 2-9. リモートによるパスワードのリセット

4. [リモートによるロック解除] 画面で、[デバイスを選択する] をクリックします。

5. デバイスツリーが表示されます。リモートでロック解除するモバイルデバイスを選択して、[選択] をクリックします。

図 2-10. ロック解除するモバイルデバイスの選択

6. フィールドにユーザ確認のためのコードを入力して、[生成] をクリックします。
7. TMMS 管理サーバによって応答コードが生成され、ポップアップ画面にコードが表示されます。
8. モバイルデバイスの [パスワード] 画面の [次へ] をクリックし、モバイルデバイスをロック解除するための応答コードを入力するようユーザに指示します。

第 3 章

セキュリティポリシーの設定

この章では、Trend Micro Mobile Security (以下、Mobile Security) ドメイン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。一般的なポリシーに加えて、ファイアウォール、パスワード、および暗号化に関連するポリシーも使用できます。

この章には、次の節が含まれています。

セキュリティポリシーについて

TMMS 管理サーバの Mobile Security ドメインに対して、セキュリティポリシーを設定できます。これらのポリシーは、ドメイン内のすべてのモバイルデバイスに適用されます。Mobile Security ドメイン (ルートドメイン) を選択することで、すべての Mobile Security ドメインにセキュリティポリシーを適用できます。

セキュリティポリシーには、一般ポリシー、ファイアウォールポリシー、SMS スパムメール対策ポリシー、WAP プッシュ保護ポリシー、暗号化ポリシー、およびデバイスコンポーネントの有効化 / 無効化ポリシーなどがあります。

Mobile Security ドメインにセキュリティポリシーを設定するには

1. ウイルスバスター コーポレートエディション (以下、ウイルスバスター Corp.) Web 管理コンソールにログオンし、[プラグインマネージャ] をクリックします。
2. Mobile Security の [プログラムの管理] をクリックします。
3. [デバイス管理] をクリックして、デバイスツリーで 1 つ以上のドメインを選択します。
4. [ドメインポリシー] をクリックして、[一般ポリシー]、[ファイアウォールポリシー]、[SMS スパムメール対策ポリシー]、[WAP プッシュ保護ポリシー]、[暗号化ポリシー]、または [デバイスコンポーネントの有効化 / 無効化] を選択します。

注意： [ドメインポリシー] 画面でのセキュリティポリシー設定の変更後、すぐにモバイルデバイスエージェントの設定を同期することをお勧めします。詳細については、40 ページの「モバイルデバイスエージェントのプロビジョニング」を参照してください。

一般ポリシー

一般セキュリティポリシーを設定するには、デバイスツリーでドメインを選択して、[ドメインポリシー]→[一般ポリシー] をクリックします。

ユーザ権限

ユーザによるモバイルデバイス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、ユーザによるモバイルデバイス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、数値、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ドメインごとに設定できます。

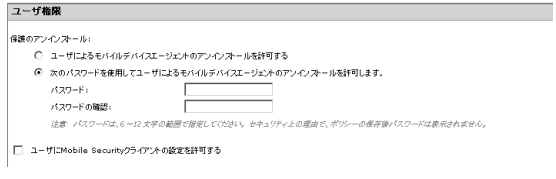


図 3-1. [一般ポリシー]、[ユーザ権限] セクション

[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、ユーザはモバイルデバイスエージェントの設定を変更することができません。ただし、SMS スパムメール対策および WAP プッシュ保護は、このオプションの選択によって影響を受けることはありません。詳細については、50 ページの「SMS スパムメール対策ポリシー」および 51 ページの「WAP プッシュ保護ポリシー」を参照してください。

不正プログラム対策ポリシー

検索の種類 (リアルタイム検索およびカード検索)、不正プログラムに対する処理、検索する圧縮階層数、およびファイルタイプなどの不正プログラム対策ポリシーを設定できます。

検索の種類

Mobile Security には、不正プログラムからモバイルデバイスを保護するためのさまざまな検索機能があります。

リアルタイム検索

モバイルデバイスエージェントは、モバイルデバイスのファイルをリアルタイムに検索します。モバイルデバイスエージェントがセキュリティリスクを検出しなかった場合、ユーザは引き続きファイルを開いたり保存したりすることができます。モバイルデバイスエージェントがセキュリティリスクを検出した場合は、検索結果が表示され、ファイル名と特定のセキュリティリスクが示されます。Mobile Security は、モバイルデバイスの検索結果を使用してログを生成します。検索ログは、TMMS 管理サーバに送信されて格納されます。

カード検索

[一般ポリシー] 画面で [カード検索] オプションを選択した場合、モバイルデバイスにメモリカードが挿入されると、Mobile Security はメモリカードのデータを検索します。これにより、メモリカードを経由した感染ファイルの蔓延を防ぎます。

検索処理

モバイルデバイスで不正プログラムが検出された場合、Mobile Security は感染ファイルを削除または隔離できます。そのファイルが使用中の場合、OS によってそのファイルへのアクセスが拒否される場合があります。

- 削除 — 感染ファイルを削除します。

- 隔離 — 感染ファイルの名前を変更して、モバイルデバイスの隔離ディレクトリ (Windows Mobile の場合は、¥TmQuarantine、Symbian OS の場合は、{ ディスクラベル }¥TmQuarantine) に移動します。
- 接続されている場合は、モバイルデバイスエージェントから TMMS 管理サーバに不正プログラムログが送信されます。

ファイルタイプおよび圧縮レベルのオプション

ZIP または CAB ファイルの場合、検索する圧縮階層の数を指定できます。ZIP/CAB ファイルの圧縮階層の数が指定された数を超えると、Mobile Security はそのファイルを検索しません。Mobile Security は、適切な圧縮階層数が指定されない限り、これ以上の処理は行いません。

Mobile Security がモバイルデバイス上の実行可能ファイル、CAB/ZIP ファイル、またはすべてのファイルの検索を実行するように選択できます。

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ったときに TMMS 管理サーバからモバイルデバイス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、TMMS 管理サーバのコンポーネントまたは設定のアップデートをモバイルデバイスエージェントで定期的にチェックできます。

ワイヤレス接続の通知オプションを有効にすると、モバイルデバイスエージェントがワイヤレス接続 (3G や GPRS など) で TMMS 管理サーバに接続する前に、モバイルデバイスにプロンプトが表示されます。ユーザは接続要求を許可または拒否できます。

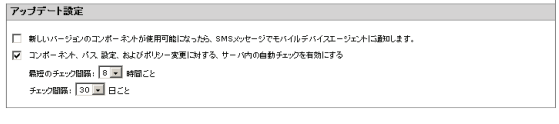


図 3-2. [一般ポリシー]、[アップデート設定] セクション

ログの設定

モバイルデバイスエージェントが感染ファイルや不正侵入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。暗号化モジュールが利用可能な場合は、暗号化ログも生成されます。これらのログを TMMS 管理サーバに送信するようにモバイルデバイスを設定できます。感染数を分析したり、潜在的なネットワーク攻撃を特定して、脅威の蔓延を防ぐための適切な措置を講じる場合に、この設定を行ってください。

通知設定

モバイルデバイスエージェントが TMMS 管理サーバと接続を確立しようとする際に、モバイルデバイスにプロンプト画面を表示するかどうかを選択します。

デバイス管理エージェント

サードパーティ製のデバイス管理ツールを使用してモバイルデバイスを管理する場合、そのデバイス管理ツールを使用してモバイルデバイスエージェントのインストール、コンポーネントのアップデート、および設定の同期を実行できるように TMMS 管理サーバを設定できます。[一般ポリシー] 画面で [デバイス管理エージェントの有効化] チェックボックスをオンにします。

ファイアウォールポリシー

Mobile Security ファイアウォールでは、ステートフルインスペクション、高パフォーマンスネットワークトラフィック制御、および侵入検知システム (IDS) を使用して、ネットワーク上のモバイルデバイスを保護します。IP アドレス、ポート番号、またはプロトコルによって接続をフィルタするルールを作成して、特定の Mobile Security ドメインのモバイルデバイスにルールを適用できます。

注意： モバイルデバイス上のその他のソフトウェアベースのファイアウォールアプリケーションをアンインストールしてから、Mobile Security ファイアウォールを配置して有効にすることをお勧めします。同じコンピュータに複数のベンダーのファイアウォールをインストールすると、予期しない結果が発生する可能性があります。

Mobile Security のファイアウォールポリシーは、[ドメインポリシー]→[ファイアウォールポリシー] で設定できます。

ファイアウォールポリシーには次のものが含まれています。

- **ファイアウォールポリシー** — Mobile Security ファイアウォールと IDS を有効 / 無効にします。モバイルデバイスのすべての受信トラフィックまたはすべての送信トラフィック (またはその両方) をブロックまたは許可する一般ポリシーも含まれています。
- **除外リスト** — 各種のネットワークトラフィックをブロックまたは許可するための設定可能なルールの一覧。

事前定義されたファイアウォールセキュリティレベル

Mobile Security ファイアウォールには、3 つの事前定義されたセキュリティレベルがあり、これらを使用して簡単にファイアウォールポリシーを設定できます。これらのセキュリティレベルは、トラフィックの方向に基づいてネットワークトラフィックを制限します。

- **低** — すべての送受信トラフィックを許可します。
- **中** — すべての送信トラフィックを許可し、すべての受信トラフィックをブロックします。
- **高** — すべての送受信トラフィックをブロックします。

侵入検知システム

Mobile Security ファイアウォールは、侵入検知システム (IDS) を統合しています。IDS を有効にすると、モバイルデバイスに対する潜在的な攻撃を示すネットワークパケットのパターンを特定することができます。

Mobile Security ファイアウォールは、あるプログラムがコンピュータに複数の TCP 同期 (SYN) パケットを送信し、モバイルデバイスが同期 / 確認 (SYN/ACK) 応答を送り続けるようにする、SYN フラッド攻撃 (DoS 攻撃の一種) を防止する場合に役立ちます。この攻撃により、システムリソースが使い尽くされ、モバイルデバイスが他の要求を処理できなくなる可能性があります。

除外ルール

除外ルールには、モバイルデバイスのポート番号および IP アドレスに従ってさまざまな種類のトラフィックを許可またはブロックする、より詳細な設定が含まれます。リスト内のルールは、[セキュリティレベル] ポリシーより優先されます。

除外ルール設定には次のものが含まれます。

- **処理** — ルール条件に合うトラフィックをブロック / 許可、またはログ記録します。
- **方向** — モバイルデバイス上の受信または送信ネットワークトラフィック。
- **プロトコル** — トラフィックタイプ (TCP、UDP、ICMP)。
- **ポート** — 処理を実行するモバイルデバイスのポート。
- **IP アドレス** — トラフィック条件を適用するネットワークデバイスの IP アドレス。

SMS スパムメール対策ポリシー

この機能を使用すると、SMS スパムメール対策ポリシーのサーバ側の制御を有効または無効にできます。SMS スパムメール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。

- Mobile Security モバイルデバイスに対する SMS スパムメール対策の制御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 Mobile Security モバイルデバイスを設定する、または Mobile Security モバイルデバイスの SMS スパムメール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。
- 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 SMS スパムメール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ブロックリストまたは除外リストの表示または編集を行うことはできない。ただし、ユーザはモバイルデバイス側の個人の SMS スパムメール対策の除外リストおよびブロックリストを編集することはできる。

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 0 ～ 30 文字で、number の長さは 4 ～ 20 文字です。電話番号には、数字、+、-、#、(,)、スペースを使用できます。CR は「;」と同じように処理されます。最大エントリ数は 200 です。

WAP プッシュ保護ポリシー

WAP プッシュ保護のサーバ側の制御を有効にできます。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。次に、WAP プッシュ保護ポリシーの設定時に指定可能な機能の一覧を示します。

- Mobile Security モバイルデバイスに対する WAP プッシュ保護の制御を有効または無効にする。
- 除外リストを使用するように Mobile Security 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 プッシュ保護を無効にする。
- 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 プッシュ保護を変更することはできない。
- 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設定されている WAP プッシュ保護リストの表示または編集を行うことはできない。ただし、ユーザはモバイルデバイス側の個人の WAP プッシュ保護リストを編集することはできる。

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 0 ～ 30 文字で、number の長さは 4 ～ 20 文字です。電話番号には、数字、+、-、#、(,)、スペースを使用できます。CR は「;」と同じように処理されます。最大エントリ数は 200 です。

暗号化ポリシー

暗号化モジュールは、モバイルデバイスでのパスワード認証およびデータ暗号化を提供します。これらの機能を使用すると、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。

モバイルデバイスエージェントに暗号化ポリシーを設定するには、[ドメインポリシー]→[暗号化ポリシー] をクリックします。

注意： 暗号化モジュールのライセンスの有効期限が切れた場合、[暗号化ポリシー] 画面のすべての設定が無効になります。ライセンスのアップグレードの詳細については、25 ページの「製品ライセンス」を参照してください。

パスワードの設定およびパスワードのセキュリティ

モバイルデバイスエージェントをインストールすると、各モバイルデバイスがそれぞれのユーザと関連付けられます。ユーザがモバイルデバイスにログオンするには、パワーオンパスワードを正しく入力する必要があります。ユーザがパワーオンパスワードを忘れた場合にデバイスのロックを解除したり、より高度な設定が可能な Mobile Security の管理画面にモバイルデバイスからアクセスしたりするには、管理者のパスワードを入力する必要があります。そのため、ログオン時に指定するパスワードの種類 (パワーオンパスワードか管理者パスワードか) によっては、使用できる Mobile Security の管理画面またはフィールドが異なります。

次の表に、設定可能なパワーオンパスワードポリシーを示します。

オプション	説明
パスワードの種類	パスワードには数字または英数字のみを指定します。
最小のパスワードの長さ	パスワードは指定された文字数よりも長くする必要があります。
パスワードの複雑さ	英数字のパスワードの場合、パスワードを推測されにくくするために、大文字、小文字、特殊文字、または数字を含むパスワードを設定する必要があります。
モバイルデバイスエージェントの初期パスワード	モバイルデバイスエージェントと暗号化モジュールのインストール後、ユーザが Windows Mobile デバイスにログオンするためのパスワード。初期設定は、「123456」です。
管理者パスワード	モバイルデバイスをロック解除するために管理者が使用するパスワード。初期設定は、「1234567890」です。
パスワードの有効期限	ログオンパスワードが有効な日数。パスワードの有効期限が切れた場合、ユーザは新しいログオンパスワードを設定する必要があります。
非アクティブ状態のタイムアウト	ユーザ操作がない状態（アイドル状態）でモバイルデバイスにパスワードロックがかかるまでの時間（分）。

表 3-1.　パスワードポリシー

オプション	説明
ログオン上限試行回数	総当たりのパスワード攻撃を防ぐために、ログオン試行回数を制限します。上限に達した場合に実行可能な処理は次のとおりです。 • ソフトリセット — モバイルデバイスを再起動します。 • 管理者アクセスのみ — 管理者パスワードを使用したログオンが必要です。 • すべてのデータをクリア — モバイルデバイスおよび挿入されているメモリカードのすべてのデータを削除します。 **警告：** [すべてのデータをクリア] のアクションを選択した場合、メモリカードに再度データを格納するには、ユーザはメモリカードを再フォーマットする必要があります。 • ハードリセット — モバイルデバイスのすべてのデータを削除して、モバイルデバイスを出荷時の初期設定にリセットします。
初期設定パワーオンパスワードの変更	初回ログオン後、パスワードを変更するようにユーザに要求します。
パスワードを忘れた場合の質問	ユーザがパワーオンパスワードを忘れた場合、この機能を使用すると、ユーザは選択した質問に回答することで、モバイルデバイスのロックを解除して新しいパスワードを設定できます。

表 3-1.　パスワードポリシー (続き)

暗号化設定

モバイルデバイスエージェントには、モバイルデバイスのデータを保護するためのオンザフライのデータ暗号化機能があります。使用できる暗号化アルゴリズムには、AES (128 ビット、192 ビット、または 256 ビットの鍵を持つ Advanced Encryption Standard) および 3DES (Triple Data Encryption Standard) の 2 種類があります。

警告： 暗号化方式または暗号鍵を変更して新しい暗号化ポリシーを適用したときに、メモリカードがモバイルデバイスに挿入されていない場合、そのメモリカードのデータは読み取れなくなります。この問題は、古い暗号化方式または暗号鍵でメモリカードのデータが暗号化された場合に発生します。新しい暗号化ポリシーの適用後は、モバイルデバイスのアプリケーションでメモリカードのデータを読み取ることはできなくなります。
トレンドマイクロでは、暗号化ポリシーを設定および適用後に、暗号化方式または暗号鍵を変更しないことをお勧めします。変更が必要な場合、新しい暗号化ポリシーを適用する前に、メモリカードがモバイルデバイスに挿入されていることを確認してください。

Windows Mobile デバイスまたは Symbian OS デバイスで暗号化する特定のファイルタイプ、使用する暗号化アルゴリズム、暗号化データにアクセスを許可する信頼されたアプリケーションを指定できます。また、モバイルデバイスに挿入されたメモリカードでデータ暗号化を適用することもできます。

モバイルデバイスエージェントは、実行可能ファイル (拡張子 .EXE のファイル) は暗号化しません。メモリカードでは、モバイルデバイスエージェントはユーザが変更したファイルのみを暗号化します。ファイルを読み取り、変更しないで閉じた場合、そのファイルは暗号化されません。

暗号化モジュールをインストールすると、一部のファイルタイプが暗号化されます (doc、txt、ppt、pdf、xls など)。暗号化モジュールでは、暗号化されたデータへのアクセスが信頼されたアプリケーションにのみ許可されます。このため、管理者は、信頼されたアプリケーションのリストにこれらのアプリケーションを追加する必要があります。信頼されたアプリケーションのリストにソフトウェアを追加するには、[暗号化されたデータへのアクセスをさらに多くのアプリケーションに許可する] の該当するリストにソフトウェアのフルパスを追加します。

注意： 詳細設定では、その他のファイルタイプを暗号化するように Mobile Security を設定できます。カスタムファイルタイプの暗号化を有効にするには、¥OfficeScan¥Addon¥Mobile Security にある TmOMSM.ini ファイルのパラメータ Enable_Custom_Extension を 1 に設定します。TmOMSM.ini ファイルのこのパラメータが「1」に設定されると、[暗号化ポリシー] 画面に [その他のファイルタイプを暗号化する] フィールドが表示されます。このフィールドにファイルタイプを指定します。

この機能を無効にするには、パラメータ Enable_Custom_Extension を 0 に設定します。TmOMSM.ini ファイルのこのパラメータが「0」に設定されると、[その他のファイルタイプを暗号化する] フィールドは [暗号化ポリシー] 画面に表示されなくなります。

警告： トレンドマイクロでは、暗号化するファイルタイプをカスタマイズしないことをお勧めします。特定のファイルタイプ (.exe、.cert、.dll など) は暗号化できません。暗号化すべきでないファイルタイプを暗号化するように Mobile Security を設定した場合、予期しないシステムエラーが発生する可能性があります。

デバイスコンポーネントの有効化 / 無効化

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、特定のドメイン内のすべてのモバイルデバイスのカメラを無効にできます。

- Bluetooth および Bluetooth 検出
- 赤外線
- USB ストレージ
- WLAN/WiFi
- シリアル
- スピーカー/ スピーカーフォン / マイク
- カメラ
- Microsoft ActiveSync
- MMS/SMS
- メモリカード
- GPS

注意： Mobile Security では、Windows ベースのモバイルデバイスで特定の機能を使用可能にするかどうかのみ制御できます。Symbian ベースのモバイルデバイスでこのような制御はできません。

サポートされる機能 / コンポーネント

Windows ベースのモバイルデバイスで次の機能を使用可能にするかどうかを制御できます。

- Bluetooth および Bluetooth 検出 — この機能を無効にすると、Bluetooth および外部 GPS 接続経由の ActiveSync も無効になります。

- 赤外線 — モバイルデバイスでこの機能を無効にすると、着信ビームサービス (すべての着信ビームを受信する) がブロックされます。
- USB ストレージ
- WLANWIFI
- シリアル — この機能を無効にすると、疑似シリアル接続および外部 GPS 接続を使用した USB 経由の ActiveSync も無効になります。これによって一部の赤外線サービスや Bluetooth サービスも無効になる場合があります。
- スピーカー/ スピーカーフォン / マイク
- カメラ
- Microsoft ActiveSync
- MMS/SMS — この機能を無効にすると、Mobile Security から送信されるメッセージを含め、すべての送受信メッセージがブロックされます。
- メモリカード
- GPS — この機能を無効にすると、内部 GPS 機能 (モバイルデバイスに GPS コンポーネントが組み込まれている場合にのみ適用) および GPSID (GPS 中間ドライバ) に基づいた外部 GPS 接続のみがブロックされます。シリアルポートを使用した外部 GPS 接続には影響はありません。

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。

特定のドメインのモバイルデバイスで機能を使用可能にするかどうかを設定するには、[ドメインポリシー]→[デバイスコンポーネントの有効化 / 無効化] をクリックします。

第 4 章

データ復元ツール

データ復元ツールは、管理者が Trend Micro Mobile Security (以下、Mobile Security) の暗号化モジュールによって暗号化されたユーザファイルを復号化するためのスタンドアロンアプリケーションです。何らかの理由で、ユーザがストレージカードに保存されている暗号化ファイルを開けない場合に使用します。

この章には、次の節が含まれています。

データ復元ツールのインストール

データ復元ツールをインストールするには

1. インストールを開始するには、データ復元ツールのインストーラファイル TmmsDataRecoverySetup.exe を開きます。

[ようこそ] 画面が表示されてインストールウィザードが開始します。[次へ] をクリックします。

図 4-1. [ようこそ] 画面

2. [使用許諾契約] 画面が表示されます。[使用許諾契約の条項に同意します] を選択して [次へ] をクリックします。

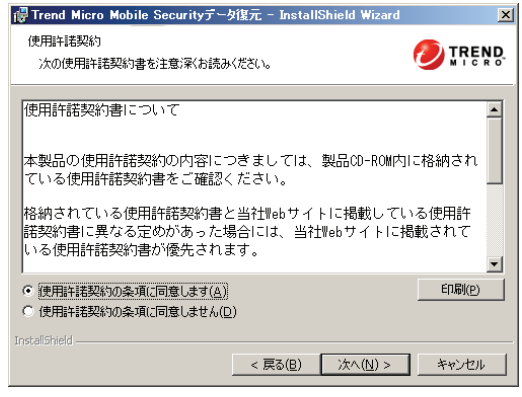


図 4-2. [使用許諾契約] 画面

3. [インストール先のフォルダ] 画面が表示されます。[変更] をクリックしてフォルダを変更します。または、[次へ] をクリックして初期設定のフォルダを受け入れます。

図 4-3. [インストール先のフォルダ] の選択

4. [プログラムをインストールする準備ができました] 画面が表示されます。[インストール] をクリックしてプログラムをインストールします。

図 4-4. [プログラムをインストールする準備ができました] 画面

5. [InstallShield ウィザードを完了しました] 画面が表示されたら、[完了] をクリックしてウィザードを終了します。

図 4-5. InstallShield ウィザードの完了画面

プログラムがインストールされました。

データ復元ツールの使用

復元ツールを使用するには、復元ファイルが必要です。管理者は、Web 管理コンソールから特定のドメインの復元ファイルをエクスポートします。エクスポートされた暗号化ファイルには、管理者パスワード (Web 管理コンソールの管理者パスワードではなく、暗号化ポリシーの管理者パスワード)、暗号鍵、および暗号化アルゴリズムが含まれています。

ユーザファイルを復号化するには

1. ユーザから復号化するファイルを取得します。
2. ウイルスバスターCorp. サーバにログオンして、UI からポリシーファイルを作成してダウンロードします。次に、[プラグインマネージャ]→[プログラムの管理]→[デバイス管理]→ { ドメイン } →[暗号化ポリシー]→[復元ファイルのダウンロード] をクリックします。

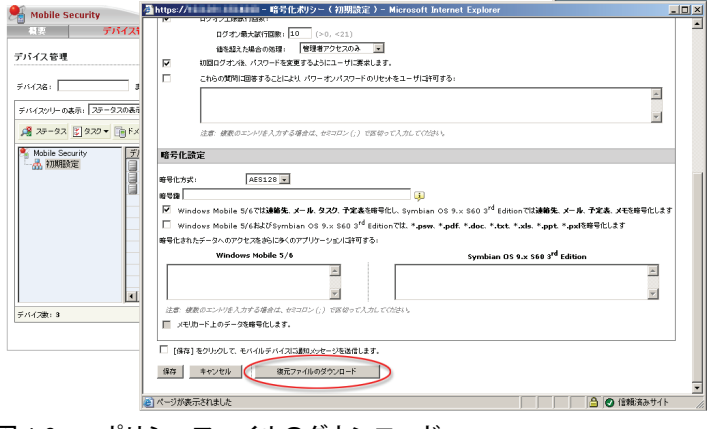


図 4-6.　ポリシーファイルのダウンロード

3. [スタート]→[すべてのプログラム]→[Trend Micro]→[Trend Micro TMMS Recovery Tool]→[Launch TmmsDataRecovery.exe] をクリックし、ツールを開きます。以下を入力します。

   - 復元ファイルの場所 (適切な復元ファイルを使用する必要があります。下の注意を参照)
   - 復号化されるユーザファイルの場所 (複数のファイルを選択できます)
   - 復号化されたファイルを配置する場所 (実行先フォルダは復号化するファイルの現在の場所と同じにはできません)

   [確認なしで上書きする] を選択して、[復号化開始] をクリックします。

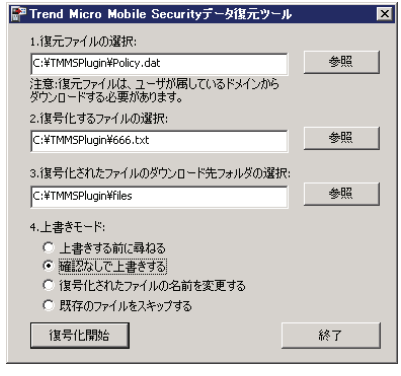


図 4-7. データ復元ツールのメインユーザインタフェース

注意： データ復元ツールの復元ファイルは、特定のドメインに関連付けられています。復元ファイルは、復号化アルゴリズム、キー、およびパスワードを指定します。復元ファイルのアルゴリズムとキーは間違っているがパスワードは正しい場合、データ復元ツールは指定されたアルゴリズムとキーを使用してファイルの復号化を続行します。ただし、復号化されたファイルは不要なデータになります。正確な復元ファイルを使用する必要があります。

4. ポップアップ画面が表示されます。管理者パスワードを入力して [OK] をクリックしてファイルの復号化を開始します。

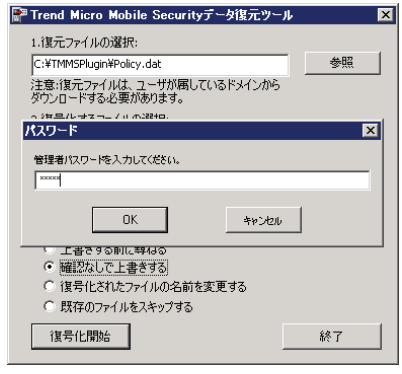


図 4-8. パスワードの入力

5. 完了すると、次の画面が表示されます。終了する場合は [OK]、復号化ログを表示する場合は [ログの表示] をクリックします。

図 4-9. 復号化の完了

6. 初期設定のテキストエディタでログファイルを開きます。

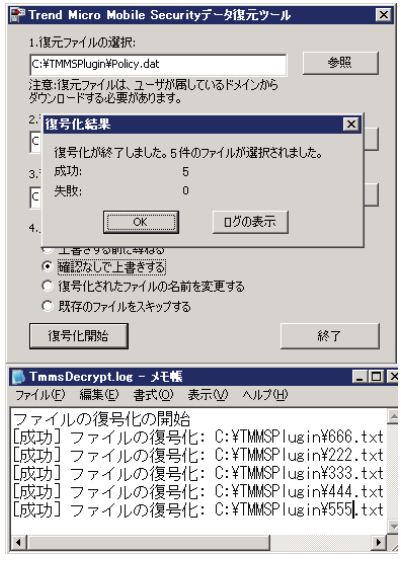


図 4-10. データ復元ログ

ログファイルには、復号化ログエントリとその結果が一覧表示されます。

第 5 章

コンポーネントのアップデート

この章では、予約および手動のサーバアップデートを設定して、アップデートのアップデート元を指定する方法を示します。また、特定のモバイルデバイスエージェントでのコンポーネントのアップデートの実行についても説明します。

この章には、次の節が含まれています。

コンポーネントのアップデートについて

Trend Micro Mobile Security (以下、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。

- 不正プログラムパターンファイル — 何千も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、ウイルスパターンファイルを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。
- 不正プログラム検索エンジン — 実際の検索および駆除の機能を実行するコンポーネント。この検索エンジンには、パターンファイルのシグニチャを使用して不正プログラムを検出するパターンマッチング技術が採用されています。トレンドマイクロでは、新技術を組み込んだ新しいウイルス検索エンジンを適宜公開しています。
- モバイルデバイスエージェントのインストールプログラム — モバイルデバイスエージェントのプログラムインストールパッケージ。
- モバイルデバイスエージェントのプログラムパッチ — モバイルデバイスにインストールされたモバイルデバイスエージェントプログラムに対する最新のアップデートを含むプログラムパッチファイル。

サーバアップデート

TMMS 管理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することができます。TMMS 管理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、TMMS 管理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。

アップデートは手動で実行することも、予約に従って Mobile Security に実行させることもできます。

手動サーバアップデート

[手動] 画面で、手動サーバアップデートを実行できます。[アップデート元] 画面 (詳細については、72 ページの「ダウンロード元の指定」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。

手動サーバアップデートを実行するには

1. ウイルスバスター コーポレートエディション (以下、ウイルスバスター Corp.) Web 管理コンソールにログオンし、[プラグインマネージャ] をクリックします。
2. Mobile Security の [プログラムの管理] ボタンをクリックします。
3. [アップデート]→[サーバアップデート] をクリックします。[手動] 画面が表示されます。
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] と、[プログラム]、または [プログラムインストールパッケージ] チェックボックス (またはこれらのうちの 2 つか、3 つすべて) 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、68 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。

[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。

図 5-1.　手動サーバアップデートの開始

予約サーバアップデート

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、ワークロードを削減できます。[アップデート元] 画面 (詳細については、72 ページの「ダウンロード元の指定」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。

予約サーバアップデートを設定するには

1. ウイルスバスター Corp. の web 管理コンソールにログオンし、[プラグインマネージャ] をクリックします。
2. Mobile Security の [プログラムの管理] ボタンをクリックします。

3. [アップデート]→[サーバアップデート] をクリックして、[予約] タブをクリックします。[予約] 画面が表示されます。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] と、[プログラム]、または [プログラムインストールパッケージ] チェックボックス (またはこれらのうちの 2 つか、3 つすべて) 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。

4. [アップデートスケジュール] の下で、サーバアップデートを実行する時間間隔を設定します。オプションは、[毎時]、[毎日]、[毎週]、および [毎月] です。

   - 毎週のスケジュールには、曜日を指定してください (日曜日、月曜日など)。
   - 毎月のスケジュールには、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： [アップデートの期間 (時間数)] 機能は、[毎日]、[毎週]、および [毎月] オプションで使用できます。これは、[開始時刻] フィールドで選択した時刻の後、指定された x 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。

5. [保存] をクリックして設定を保存します。

図 5-2. 予約サーバアップデートの設定

ダウンロード元の指定

サーバアップデートに、初期設定のアップデートサーバか、または指定したダウンロード元を使用するように Mobile Security を設定できます。

ダウンロード元をカスタマイズするには

1. ウイルスバスター Corp. の web 管理コンソールにログオンし、[プラグインマネージャ] をクリックします。
2. Mobile Security の [プログラムの管理] ボタンをクリックします。

3. [アップデート]→[サーバアップデート] をクリックします。サーバアップデートの詳細については、69 ページの「手動サーバアップデート」を参照してください。予約アップデートについては、70 ページの「予約サーバアップデート」を参照してください。

4. [アップデート元] タブをクリックし、次のダウンロード元のいずれかを選択します。

   - 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。モバイルデバイスエージェントがアップデートをダウンロードするために使用されるポート番号も含めます。

   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。

5. [保存] をクリックして設定を保存します。

図 5-3. サーバアップデートのダウンロード元の指定

デバイスのアップデート

登録済みのモバイルデバイスエージェントから、TMMS 管理サーバまたは TMMS アップデートサーバのいずれかに接続して、最新の検索エンジン、不正プログラムパターンファイル、またはプログラムパッチファイルを入手できます。

TMMS 管理サーバでアップデート済みファイルが使用可能な場合、新しいコンポーネントをインストールするように SMS アップデートメッセージがモバイルデバイスエージェントに送信されます。さらに、TMMS 管理サーバの任意のコンポーネントのアップデートを定期的に確認するように、モバイルデバイスエージェントを設定することもできます。

アップデートの種類

Mobile Security には、次の 3 種類のアップデートがあります。

種類	説明
手動	ユーザが開始します。このアップデートは随時実行できます。
自動	モバイルデバイスでネットワーク接続を開始すると、前回アップデートを確認した時点から指定のアップデート間隔が経過している場合に、アップデートが実行されます。
強制	その期間内に別のアップデートが実行されたかどうかにかかわらず、指定の間隔でアップデートが実行されます。デバイスがウイルスバスターCorp. サーバに接続していない場合は、強制アップデートにより、初期設定のワイヤレス接続が開かれます。

表 5-1. アップデートの種類

[デバイスのアップデート] 画面を使用して、期限切れのコンポーネントを使用しているすべてのモバイルデバイスまたは選択したモバイルデバイスにアップデート通知を送信します。

注意： コンポーネントの予約アップデートを実行するようにデバイスを設定することもできます。詳細については、47 ページの「アップデート設定」およびお使いのモバイルデバイスの「ユーザガイド」を参照してください。

モバイルデバイスにアップデート通知を送信するには

1. ウイルスバスター Corp. の web 管理コンソールにログオンし、[プラグインマネージャ] をクリックします。
2. Mobile Security の [プログラムの管理] ボタンをクリックします。
3. [アップデート]→[デバイスのアップデート] をクリックします。[デバイスのアップデート] 画面が表示されます。サポート対象のデバイスごとにコンポーネントの最新バージョンとコンポーネントの最終更新日時を確認できます。
4. アップデート通知を送信するデバイスを指定します。
   - コンポーネントのバージョンが古いすべてのモバイルデバイスにアップデート通知を送信するには、[期限切れのコンポーネントを使用しているすべてのデバイス] を選択します。初期設定ではこれが選択されています。
   - アップデート通知を送信して新しいコンポーネントをダウンロードするデバイスを選択できるデバイスツリーを表示するには、[手動でデバイスを選択する] を選択します。
5. [アップデート] をクリックします。TMMS 管理サーバから、選択したデバイスに通知が送信されます。

6. [アップデート] をクリックします。TMMS 管理サーバは、期限切れのコンポーネントを使用しているすべてのモバイルデバイスを検索して、それらのモバイルデバイスにコンポーネントのアップデートを実行します。

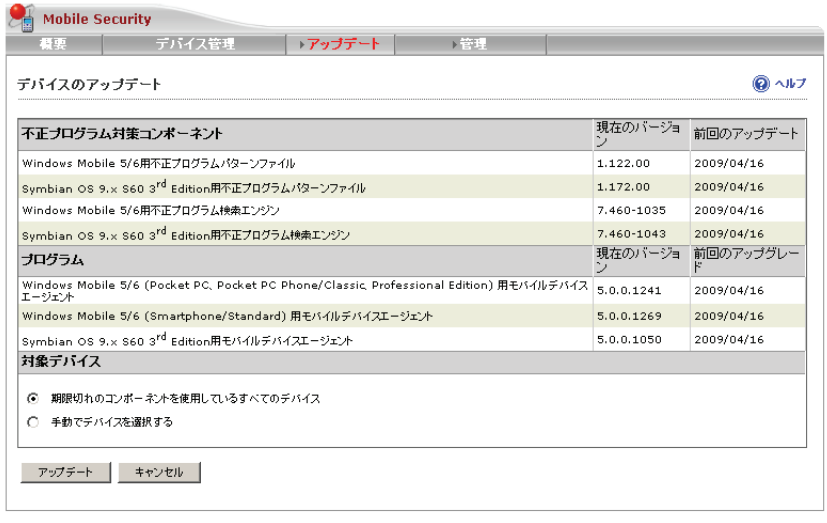


図 5-4. デバイスのアップデートの設定

ローカルのアップデート元の手動アップデート

サーバ / 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、ウイルスバスターCorp. サーバがインターネットに接続できない場合、サーバ / 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。

ローカルのアップデート元をアップデートするには

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. TmmsServerAu フォルダと TmmsClientAu フォルダを、仮想ディレクトリ TmmsAu が配置されているディレクトリにコピーします (仮想ディレクトリの作成方法については、マニュアル「Trend Micro Mobile Security クライアント配信ガイド」の第 1 章の「ローカルのアップデート元を使用してサーバコンポーネントをインストールする」節を参照)。画面に確認メッセージが表示されたら、ディレクトリの任意の既存フォルダの上書きを確定します。

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 6 章

ログの表示と管理

この章では、TMMS 管理サーバでモバイルデバイスエージェントの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、次の節が含まれています。

モバイルデバイスエージェントのログについて

モバイルデバイスエージェントが不正プログラムログ、暗号化ログ、ファイアウォールログ、またはイベントログを生成すると、そのログが TMMS 管理サーバに送信されます。これにより、モバイルデバイス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 SMS スパムメール対策ログおよび WAP プッシュ保護ログを表示できます。

モバイルデバイスエージェントのログの表示

モバイルデバイスでモバイルデバイスエージェントのログを表示したり、TMMS 管理サーバ上でモバイルデバイスエージェントのすべてのログを表示したりできます。TMMS 管理サーバでは、モバイルデバイスエージェントの次のログを表示できます。

- 不正プログラムログ — モバイルデバイスエージェントはモバイルデバイス上での不正プログラムの検出時にログを生成します。これらのログを使用して、検出された不正プログラムと、それに対して実行された処理を追跡できます。
- 暗号化ログ — 成功したユーザのログオン試行や、ログオン試行の上限に達した後に実行される処理などの情報が含まれます。
- ファイアウォールログ — これらのログは、ファイアウォールルールが一致したとき、またはファイアウォール機能 (事前定義セキュリティレベルや IDS など) が接続をブロックしたときに生成されます。
- イベントログ — これらのログは、サーバおよびモバイルデバイスエージェントによって特定の処理がされたときに生成されます (83 ページの「イベントログメッセージ」を参照)。

モバイルデバイスエージェントのログを表示するには

1. [デバイス管理] 画面で、[ログ] をクリックし、[不正プログラムログ]、[暗号化ログ]、または [ファイアウォールログ] を選択します。
2. 表示するログの検索条件を指定します。以下のパラメータがあります。
   - **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。必要な期間が上記のオプションでカバーされていない場合は、[範囲] を選択して、日付範囲を指定します。
   - **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。
3. [ログの表示] をクリックして検索を開始します。

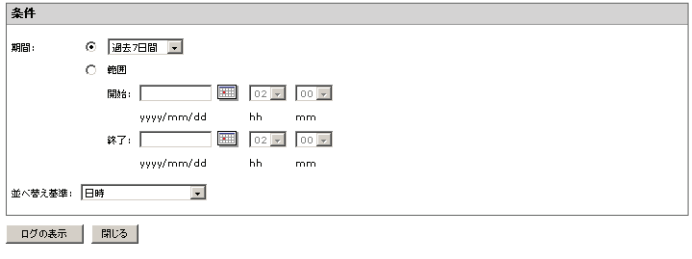


図 6-1. ログ表示のためのログ条件の設定

ログの削除

ハードディスク上で容量を過剰に占有しないようにモバイルデバイス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 TMMS 管理サーバを設定して、[ログの削除設定] 画面のスケジュールに基づいて自動的にログを削除します。

図 6-2. ログの削除設定

スケジュールに基づいてログを削除するには

1. [ログの予約削除を有効にする] を選択します。
2. 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。
3. 削除するログの種類を選択します。
4. ログ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。

手動でログを削除するには

1. 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。
2. 削除するログの種類を選択します。
3. [今すぐ削除] をクリックします。

イベントログメッセージ

表示される可能性のあるイベントログメッセージを次に示します。

表 6-1. イベントログメッセージ

イベントログメッセージ
コンソールでデバイスを追加します (モバイルデバイスが登録され、ログ記録されます)
コンソールでデバイスを削除します (モバイルデバイスが登録解除され、ログ記録されます)
管理者がモバイルデバイス名または電話番号を変更します
管理者がモバイルデバイスのドメインを変更します
マスターサービスがモバイルデバイスから登録要求を受信します
マスターサービスがモバイルデバイスから登録解除要求を受信します

イベントログで表示される可能性のあるエラーを次に示します。

表 6-2.　イベントログのエラーコード

エラーコード	エラーテキスト
-200	一般エラーが発生したため操作に失敗しました。操作を再度実行してください。
-202	デバイスは存在しません。他のセッションで削除された可能性があります。
-203	ドメインは存在しません。他のセッションで削除された可能性があります。
-204	電話番号はすでに他のモバイルデバイスに割り当てられています。別の電話番号を使用して、再度実行してください。

第 7 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、Trend Micro Mobile Security (以下、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、次の節が含まれています。

トラブルシューティング

この節では、Mobile Security の使用時に発生する可能性のある問題を処理するためのヒントを示します。

ウイルスバスター コーポレートエディション (以下、ウイルスバスター Corp.) で、Mobile Security 用のアップデートされたプラグインマネージャが表示されない

新しいバージョンの TMMS 管理サーバがアップデートサーバで入手可能であり、ウイルスバスターCorp. サーバでバージョン番号が正しく表示されない場合は、ウイルスバスターCorp. サーバでプラグインマネージャを再起動してください。

Mobile Security の [デバイス管理] 画面にアクセスするたびに、ウイルスバスター Corp. の web 管理コンソールで、TMMS_AtxConsole.cab をインストールするよう求められる

Internet Explorer で、高度なセキュリティレベルを使用するよう設定しています。この問題を解決するには、Internet Explorer のセキュリティレベルを初期設定ポリシーに戻してください。

Trend Micro Control Manager を介して、Mobile Security の管理コンソールにアクセスできない

Mobile Security では、Trend Micro Control Manager を使用したリモート管理をサポートしていません。

SMS Sender のステータスが常に切断と表示される

1. SMS Sender の電話サービスが使用可能であることを確認してください。たとえば、電話料金を支払っており、サービスが停止されていないことを確認します。

2. SMS Sender を ActiveSync を使用してホストコンピュータに接続しており、TMMS アップデートサーバにファイアウォールがインストールされている場合は、ファイアウォールルールを設定して、ポート 5721 でトラフィックを許可する必要があります。そうしないと、SMS Sender はモバイルデバイスにメッセージを送信するようにという TMMS アップデートサーバからの指示を受信することができません。

SMS Sender がメッセージを送信しない

1. SMS Sender が TMMS アップデートサーバに接続されていることを確認してください。
2. SMS Sender の電話サービスが使用可能であることを確認してください。たとえば、電話料金を支払っており、サービスが停止されていないことを確認します。
3. SMS Sender とモバイルデバイスエージェントを同じモバイルデバイスにインストールしており、TMMS アップデートサーバにファイアウォールがインストールされている場合は、ファイアウォールルールを設定して、ポート 5721 でトラフィックを許可する必要があります。そうしないと、SMS Sender はモバイルデバイスにメッセージを送信するようにという TMMS アップデートサーバからの指示を受信することができません。
4. SMS Sender のエンコード方式を変更して、再度実行してください。初期設定では、SMS Sender はメッセージの送信に Unicode エンコード方式を使用します。サービスプロバイダが Unicode エンコードをサポートしていない場合は、[7 ビット GSM] を選択してください。
5. TMMS アップデートサーバのインストール中、管理者が TMMS アップデートサーバに対し「すべて」ではなく個別の IP アドレスを選択し、その後サーバの IP アドレスが変更された場合、TMMS アップデートサーバは TMMS 管理サーバおよび SMS Sender に接続されず、SMS を送信できなくなります。

   TMMS アップデートサーバのインストールフォルダにある omsm_srv.ini ファイルの omsm_soap_ip フィールドの IP アドレスが、サーバの現在の IP アドレスと同じであることを確認してください。

ユーザがデバイスでアンインストールパスワードを入力できない

モバイルデバイスのキーボードでは、特定の文字セットのみをサポートできます。トレンドマイクロでは、管理者がデバイスでサポートされる文字のリストを作成することをお勧めします。サポートされる文字のリストを作成すると、管理者は管理コンソールからそのリストを使用してアンインストール防止パスワードを設定できます。

モバイルデバイスエージェントのセットアップパッケージをサーバからダウンロードすると、セットアップパッケージがテキストファイルとして開かれる

この問題は、Apache Web サーバの設定が原因で発生します。この問題を解決するには、次のいずれかを実行します。

- 「conf/http.conf」ファイルの「DefaultType text/plain」を「application/octet-stream」に置き換えます
- 「conf/mime.types」ファイル内の「application/octet-stream」行の後に「sis cab zip」を追加します

Mobile Security エージェントがサーバの SMS 通知を受信できない、または、パブリック DNS 経由でサーバに接続できない

DNS 名をサポートする Mobile Security エージェントのバージョンは、Windows Mobile プラットフォームでは 5.0.0.1099 以降、Symbian OS 9.x S60 3rd Edition プラットフォームでは 5.0.0.1061 以降である必要があります。それ以前のバージョンは、IP アドレス経由でのみ接続できます。

同期の正常な完了後に、新しい暗号化ポリシーをモバイルデバイスに適用できない

モバイルデバイスを再起動してください。問題が継続する場合は、管理者は暗号化ポリシーを変更し、同期を実行するようモバイルデバイスに通知する必要があります。

Syn Flood 攻撃

管理者が Mobile Security 5.1 Web 管理コンソールをリモートまたはローカルで使用すると、ファイアウォールにより SYN Flood 警告ポップアップダイアログが表示される場合があります。これは、ファイアウォールからの IDS (侵入検知システム) 警告です。この現象は、ウイルスバスター Corp. Web サーバ (IIS または Apache) で [キープアライブ] オプションを有効にしていない場合に発生します。このメッセージが再び表示されないようにするには、このオプションを有効にする必要があります。実行方法については、Web サーバのドキュメントを参照してください。

暗号化モジュールをインストールした後、アプリケーションが機能しない

ユーザが暗号化モジュールをデバイスにインストールすると、既存のアプリケーションが機能しなくなる場合があります。これは、これらの既存のアプリケーションが信頼されたリストに含まれていない可能性があることが原因です。暗号化モジュールをインストールすると、一部のファイルタイプが暗号化されます (doc、txt、ppt、pdf、xls など)。暗号化モジュールでは、暗号化されたデータへのアクセスが信頼されたアプリケーションにのみ許可されます。このため、管理者は、信頼されたアプリケーションのリストにこれらのアプリケーションを追加する必要があります。詳細については、55 ページの「暗号化設定」を参照してください。

ウイルスバスター Corp. 管理コンソールで、モバイルデバイスエージェントの正常なアップデート完了後に、デバイスのコンポーネントステータスまたは設定ステータスに「期限切れ」と表示される

アップデート時に TMMS 管理サーバまたは TMMS アップデートサーバにアクセスできない場合、モバイルデイバスエージェントはトレンドマイクロの公式アップデート元からアップデートします。この場合、アップデートは正常に実行される可能性がありますが、モバイルデバイスエージェントでは TMMS 管理サーバまたは TMMS アップデートサーバとの同期化が実行されません。このため、デバイスのコンポーネントステータスまたは設定ステータスが期限切れになります。

テクニカルサポートに問い合わせる前に

テクニカルサポートに問い合わせる前に問題の解決策が見つかるように、簡単に実行できる 2 つの方法を示します。

- ドキュメントの確認 — マニュアルおよびオンラインヘルプでは、Mobile Security に関する包括的な情報が提供されています。これら両方のドキュメントで、解決策がないか確認してください。
- テクニカルサポートの Web サイトへのアクセス — テクニカルサポートの Web サイトは製品 Q&A と呼ばれており、トレンドマイクロの全製品に関する最新情報が記載されています。サポートのこの Web サイトには、過去のユーザからの問い合わせに対する回答が記載されています。

  製品 Q&A を調べるには、次のアドレスにアクセスしてください。

  http://esupport.trendmicro.co.jp/supportjp/smb/search.do

製品サポート情報

Mobile Security 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「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、FAX、メールなどをご利用ください。サポートセンターの連絡先は、「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、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。

製品 Q&A のご案内

トレンドマイクロの Web サイトでは、製品 Q&A の情報を提供しています。これは、トレンドマイクロの製品に関する技術的な質問と、それに対する回答を集めたものです。製品 Q&A には、次の URL からアクセスできます。

http://esupport.trendmicro.co.jp/supportjp/smb/search.do

製品 Q&A では、お使いの製品名およびキーワードを指定して、知りたい情報を検索できます。たとえば製品のマニュアル、ヘルプ、Readme ファイルなどに記載されていない情報が必要な場合に、製品 Q&A を利用してください。

トレンドマイクロでは製品 Q&A の内容を常に更新し、新しい情報を追加しています。

セキュリティ情報

セキュリティ情報の入手先

トレンドマイクロでは、最新のセキュリティ情報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情報 Web サイトでは、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。セキュリティ情報 Web サイトは、次の URL からアクセスできます。

http://www.trendmicro.co.jp/vinfo/

管理コンソールからセキュリティ情報サイトにアクセスすることもできます。セキュリティ情報サイトにアクセスするには、管理コンソールの画面の右上にあるリストボックスから[セキュリティ情報] リンクを選択します。

セキュリティ情報 Web サイトでは、次の情報を閲覧できます。

- ウイルス名やキーワードから検索できるウイルスデータベース
- 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

セキュリティ情報 Web サイト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ウイルスデータベース検索サイトにアクセスして、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。

http://www.trendmicro.co.jp/vinfo/virusencyclo/default.asp

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。

http://inet.trendmicro.co.jp/esolution/attach_agreement.asp

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。

ウイルス解析サポートセンター「TrendLabs」

トレンドマイクロのウイルス解析サポートセンター「TrendLabs」(トレンドラボ) は、フィリピンセンターを本部として、米国、日本、台湾、ドイツ、アイルランド、中国、フランス、メキシコの各国センターで構成されています。24 時間体制でウイルスの活動を監視するウイルス解析エンジニアを含む 1000 名以上のスタッフが、セキュリティに関する最新の情報を収集し、高品質なサービスとソリューションを迅速かつ効果的に世界各国のトレンドマイクロのパートナーとお客さまに提供しています。

「TrendLabs」では、品質保証の ISO9001:2000 認定 (フィリピン)、国際規格 COPC-2000 規格 (フィリピン)、英国の国家規格 ITIL: BS15000 (ドイツ)、情報セキュリティマネージメントの英国規格 BS7799 (フィリピン) を取得しています。