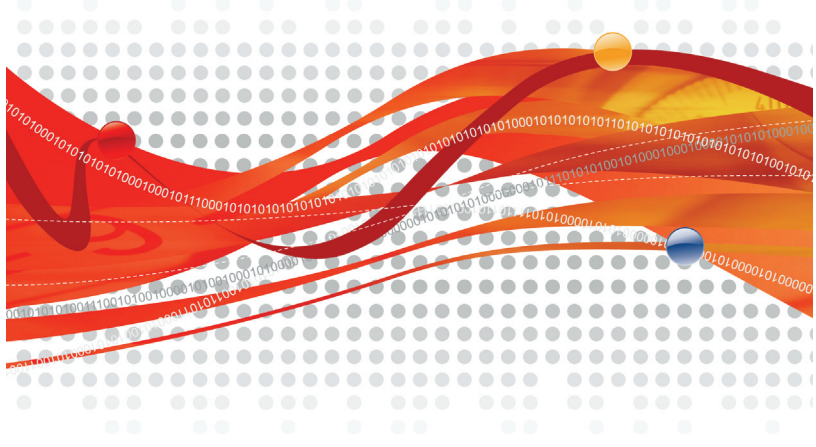
Trend Micro Mobile Security™ 5.1



クライアント配信ガイド

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

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

商標について

TRENDMICRO、ウイルスバスター、ウイルスバスター On-Line-Scan、PC-cillin、InterScan、INTERSCAN VIRUSWALL、ISVW、InterScanWebManager、ISWM、InterScan Message Security Suite、InterScan Web Security Suite、IWSS、TRENDMICRO SERVERPROTECT、PortalProtect、Trend Micro Control Manager、Trend Micro MobileSecurity、VSAPI、Trend Micro Policy Server、トレンドマイクロ・プレミアム・サポート・プログラム、License for Enterprise Information Security、LEISec、Trend Park、Trend Labs、Trend Micro Enterprise Protection Strategy、InterScan Gateway Security Appliance、Trend Micro Network VirusWall、Network VirusWall Enforcer、Trend Flex Security、EPS、Trend Micro EPS、LEAKPROOF、Trendプロテクト、Expert on Guard、InterScan Messaging Security Appliance、InterScan Web Security Appliance、InterScan Messaging Hosted Security、DataDNA、Trend Micro Threat Management Solution、Trend Micro Threat Management Services、Trend Micro Threat Management Agent、Trend Micro Threat Mitigator、およびTrend Micro USB Securityは、トレンドマイクロ株式会社の登録商標です。

本書に記載されている各社の社名、製品名およびサービス名は、各社の商標または登録商標です。

Copyright © 2004-2009 Trend Micro Incorporated. All rights reserved.

P/N: TMMSFF-AE0200_51 (2009/5)

目次

はじめに

Trend Micro Mobile Security 5.1 (以下、Mobile Security) クライアント配信ガイドをお読みいただきありがとうございます。このガイドは、管理者が Mobile Security を配置して管理するために役立つ情報を提供します。このガイドでは、さまざまな Mobie Security コンポーネント、およびモバイルデバイスエージェントのさまざまな配置方法について説明します。

モバイルデバイスのサポートおよび最新のビルドなどの Mobile Security の最新情報については、http://jp.trendmicro.com/jp/products/enterprise/mobile-security/index.html にアクセスしてください。

注意： この「クライアント配信ガイド」は、Mobile Security バージョン 5.1 にのみ適用されます。その他のバージョンの Mobile Security には適用されません。トレンドマイクロのサポートは、Mobile Security の使用に限定されています。このガイドに記載されているサードパーティ製のアプリケーションのサポートを受けるには、それぞれのベンダーにお問い合わせください。

ここでは、次のトピックについて説明します。

対象読者

Mobile Security のドキュメントは、企業環境で Mobile Security デバイスを管理する責任のある管理者と、デバイスユーザの両方を対象に準備されました。

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 (Smartphone や Pocket PC/Pocket PC 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** — このガイドでは、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** — このガイドでは、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。製品 Q&A には、次のアドレスからアクセスできます。

  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

サーバコンポーネントのインストール

この章では、管理者が Trend Micro Mobile Security 5.1 (以下、Mobile Security) のサーバコンポーネントのインストールを計画および実行するために役立つ情報を提供します。

この章には、次の節が含まれています。

サーバインストールを計画する

Mobile Security をインストールする前に、この節でシステム要件を確認してください。

ネットワーク計画

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。図 1-1 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。

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。

ヒント： イントラネット外で、TMMS アップデートサーバとモバイルデバイスエージェント間にプロキシサーバまたはファイアウォールをインストールできます。プロキシを設定するには、ウイルスバスター Corp. サーバにログオンして、[プラグインマネージャ] をクリックします。その後、Mobile Security の [プログラムの管理] をクリックして、[管理]→[接続設定] をクリックします。

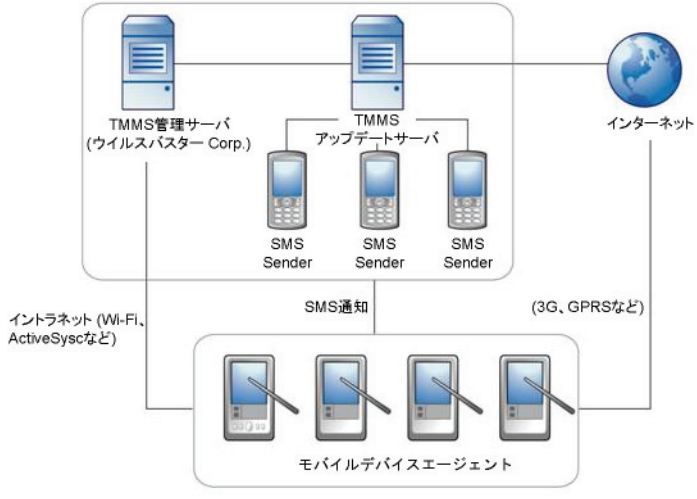


図 1-1.　Mobile Security コンポーネント

システム要件

ネットワークに各 Mobile Security をインストールする前に、次の要件を確認してください。Mobile Security コンポーネントの詳細については、「管理者ガイド」を参照してください。

コンポーネント	要件
TMMS 管理サーバ	・ ウイルスバスター Corp. サーバ 8.0 ・ プラグインマネージャ 1.0 **注意：** システムの最小要件については、ウイルスバスター Corp. 8.0 サーバのド キュメントを参照してください。 * ウイルスバスター Corp. 8.0 サーバの追加要件 - 200MB 以上のディスク空き容量
TMMS アップデートサーバ	**プラットフォーム** ・ Microsoft Windows Server 2003 Standard / Enterprise SP2 ・ Microsoft Windows Server 2003 R2 Standard / Enterprise ・ Microsoft Windows Server 2003 Standard / Enterprise x64 Edition SP2 ・ Microsoft Windows Server 2003 R2 Standard / Enterprise x64 Edition ・ Microsoft Windows 2000 Server / Advanced Server SP4 ・ Microsoft Virtual Server 2005 R2 (Microsoft Windows 2000 Server) **ハードウェア** ・ 800MHz Intel Pentium プロセッサまたは同等の CPU ・ 最小 512MB の RAM ・ 最小 40MB の使用可能なディスク空き容量 ・ USB サポート ・ 解像度 800x600、256 色以上をサポートするモニタ

表 1-1.　システム要件

コンポーネント	要件
SMS Sender	・ Windows Mobile 5 Pocket PC Phone ・ Windows Mobile 5 Smartphone ・ Windows Mobile 6 Standard ・ Windows Mobile 6 Professional
Web サーバ	・ Microsoft Internet Information Server (IIS) 5.0/6.0 ・ Apache 2.x 以降
Web ブラウザ	・ Internet Explorer 5.5 (Service Pack 1) 以降

表 1-1.　システム要件 (続き)

サーバコンポーネントをインストールする

Mobile Security コンポーネントのインストールを開始する前に、Mobile Security コンポーネントが指定されたシステム要件を満たしていることを確認してください。また、使用しているネットワークテクノロジを評価してから、インストールする Mobile Security サーバコンポーネントを決定する必要もあります。

この節では、次の Mobile Security サーバコンポーネントのインストール方法について説明します。

- TMMS 管理サーバ — ウイルスバスター Corp. サーバのプラグインプログラム
- TMMS アップデートサーバ — SMS Sender を制御して、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操作するサーバ
- SMS Sender — TMMS アップデートサーバに接続して SMS メッセージを送信するモバイルデバイス

TMMS 管理サーバをインストールする

TMMS 管理サーバをインストールする前に、ウイルスバスター Corp. サーババージョン 8.0 およびプラグインマネージャ 1.0 がインストール済みであることを確認してください。詳細については、ウイルスバスター Corp. サーバの「管理者ガイド」を参照してください。

TMMS 管理サーバをインストールするには

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ます。
2. メインメニューの [プラグインマネージャ] をクリックします。
3. [ダウンロード] をクリックして、Mobile Security プラグインパッケージを取得します。パッケージには、SMS Sender、TMMS アップデートサーバ、およびモバイルデバイスエージェントのインストールファイルも含まれています。
4. [OK] をクリックしてファイルのダウンロード処理を開始します。ダウンロードが完了するまで待機します。

5. [インストール] をクリックします。
6. エンドユーザライセンスに同意してインストール処理を開始するには、[同意する] をクリックします。

ウイルスバスター Corp. の Web 管理コンソールにアクセスする

ウイルスバスターCorp. の Web 管理コンソールを使用して、TMMS 管理サーバの管理コンソールにアクセスできます。

ウイルスバスター Corp. の Web 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。

TMMS アップデートサーバをインストールする

TMMS アップデートサーバのインストールはオプションです。次のような場合のみ、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。

- デバイスコンポーネント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 を使用してデバイスに SMS メッセージを送信する。
- モバイルデバイスエージェントがインターネットを介してコンポーネントのアップデートと設定の同期を行い、TMMS 管理サーバにセキュリティ層を追加できるようにする。

注意： TMMS アップデートサーバは別のコンピュータにインストールすることをお勧めします。
TMMS アップデートサーバのインストールを開始する前に、コンピュータに IIS または Apache Web サーバがインストール済みであることを確認してください。
IIS Web サーバを使用する場合、TMMS アップデートサーバは HTTP と HTTPS (初期設定) の両方の接続タイプをサポートします。
Apache Web サーバを使用する場合、TMMS アップデートサーバは初期設定で HTTP 接続をサポートします。HTTPS 接続を行うためには、Apache Web サーバを手動で設定する必要があります。

TMMS アップデートサーバをインストールするには

1. ウイルスバスター Corp. サーバで、¥OfficeScan¥Addon¥Mobile Security¥AgentPackage¥MSCMServer フォルダのセットアップファイルを TMMS アップデートサーバをインストールするコンピュータにコピーします。
2. セットアップファイルをダブルクリックして、インストール処理を開始します。
3. 画面の指示に従います。
4. TMMS アップデートサーバの IP アドレスを選択し、サービスポート番号を入力します。IP アドレスとポート番号は、TMMS アップデートサーバが TMMS 管理サーバおよび SMS Sender と通信するために使用されます (IP アドレスは「すべて」選択することをお勧めします。そうすると、IP が変更された場合、この値が自動でアップデートされます)。

SMS Sender をインストールする

通知に SMS メッセージング機能を使用する場合にのみ、SMS Sender をインストールする必要があります。最初に TMMS アップデートサーバをインストールしてから、SMS Sender をインストールしてください。

SMS Sender をインストールして、次のことをモバイルデバイスエージェントに通知するメッセージを送信します。

- 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 管理サーバからのコンポーネントのアップデート
- TMMS 管理サーバとの設定の同期

最大 64 の SMS Sender をインストールし、WiFi 接続を介して TMMS アップデートサーバに接続できます。

警告： 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、ポート 5721 でトラフィックを許可するようにファイアウォールルールを設定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 をインストールするには

1. ウイルスバスター Corp. サーバで、¥OfficeScan¥Addon¥Mobile Security¥AgentPackage¥SmsSender フォルダのセットアップファイルをサポート対象のデバイスプラットフォームのメモリカードにコピーします。
2. メモリカードをデバイスに挿入します。セットアップファイルを開いて、SMS Sender プログラムをインストールします。SMS Sender はメモリカードまたは電話にインストールできます。
3. [スタート] メニューから、[プログラム] フォルダの [SMS Sender 設定] を開いて、TMMS アップデートサーバと電話を設定します。[SMS Sender の設定] 画面で、TMMS アップデートサーバの DNS 名または IP アドレスとサービスポート番号を入力して、電話番号を設定し、エンコード方式を選択します。

注意： 初期設定では、SMS Sender は Unicode を使用して SMS メッセージをエンコードします。Unicode で SMS メッセージを送受信する際にエラーが発生した場合は、エンコード方式を [7 ビット GSM] に変更してください。

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

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、ウイルスバスター Corp. サーバ (ローカルホスト) に Mobile Security サーバコンポーネントをインストールして、Mobile Security のローカルアップデート元を指定する必要があります。

注意： 続行する前に、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てください。インストールパッケージには、Mobile Security エージェントとサーバのコンポーネントのセットアップファイルが含まれています。

ローカルのアップデート元を使用して Mobile Security をインストールするには

1. ウイルスバスター Corp. サーバで、仮想ディレクトリ「TmmsAu」を作成します。

   - IIS Web サーバを使用している場合は、[インターネット インフォメーション サービス (IIS) マネージャ] 画面を開いて [規定の Web サイト] を右クリックします。その後、[新規作成]→[仮想ディレクトリ] をクリックします。
   - Apache Web サーバを使用している場合は、httpd.conf ファイルに新しい仮想ディレクトリを指定して、Apache サービスを再起動します。httpd.conf ファイルの「TmmsAu」の仮想ディレクトリセクションの例を次に示します。

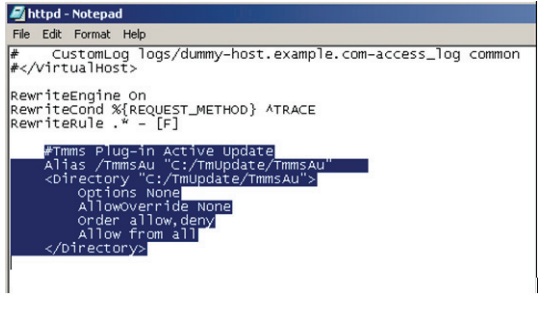


図 1-2. 新しい仮想ディレクトリを指定した Apache httpd.conf の例

2. トレンドマイクロのインストールパッケージを解凍します。

3. 「TmmsServerAu」および「TmmsClientAu」の各フォルダを仮想ディレクトリにコピーします。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。

ウイルスバスター Corp. のローカルのアップデート元を指定するには

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て、[アップデート]→[アップデート元] をクリックします。[サーバアップデート元] 画面が表示されます。

2. [その他のアップデートサーバ] を選択して、指定されたフィールドに「http://localhost/TmmsAu/TmmsServerAu」を入力します。[保存] をクリックします。

3. 変更内容を有効にするために、ウイルスバスター Corp. プラグインマネージャサービスを再起動します。

4. ウイルスバスター Corp. の Web 管理コンソールに再度ログオンして、[プラグインマネージャ] をクリックします。

5. 画面の指示に従って、Mobile Security をダウンロードしてウイルスバスター Corp. サーバにインストールします。

6. インストールが完了したら、[プログラムの管理] をクリックして Mobile Security の設定画面にアクセスします。

7. アクティベートコードを入力して製品を登録します。詳細については、20 ページの「製品を登録する」を参照してください。製品登録が正常に完了したら、Mobile Security の [概要] 画面が表示されます。

Mobile Security のローカルのアップデート元を指定するには

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。その後、Mobile Security の [プログラムの管理] をクリックします。

2. [アップデート]→[サーバアップデート] をクリックし、[アップデート元] タブをクリックして Mobile Security コンポーネントのアップデート元を設定します。

3. [その他のアップデートサーバ] を選択して、指定されたフィールドに「http://localhost/TmmsAu/TmmsClientAu」を入力します。[保存] をクリックします。

4. ポリシーを検証するには、手動アップデートを実行します ([アップデート]→[サーバアップデート]→[手動アップデート]をクリックします)。

初期サーバセットアップ

この節では、サーバをインストールした後、TMMS 管理サーバの初期セットアップを実行する手順を示します。

初期サーバセットアップの手順には、次の作業が含まれます。

- 20 ページの「製品を登録する」
- 23 ページの「接続設定」
- 25 ページの「SMS Sender リストを設定する」

注意： TMMS 管理サーバの初期サーバセットアップを完了させてから、モバイルデバイスへのモバイルデバイスエージェントのインストールを続行してください。
Trend Micro Control Manager を使用して Mobile Security の管理コンソールにアクセスすることはできません。

製品を登録する

トレンドマイクロでは、指定された期間登録されているすべてのお客さまに、テクニカルサポート、不正プログラムパターンファイルのダウンロード、およびプログラムのアップデートを提供しています。この期間の終了後に引き続きこれらのサービスを受けるには、サポート契約の更新が必要となります。TMMS 管理サーバを登録して、最新のセキュリティアップデートや、その他の製品およびサポートのサービスを受けられるようにしてください。

ご購入の Mobile Security アクティベーションコード (シリアル番号としても知られる) の種類によって、TMMS 管理サーバに暗号化モジュールが含まれるかどうかが決まります。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。

必要な作業は、アクティベーションコードを使用して、ウイルスバスター Corp. サーバ上の TMMS 管理サーバを登録することのみです。モバイルデバイスがサーバに接続されて登録されると、モバイルデバイスエージェントは、TMMS 管理サーバからライセンス情報を自動的に取得します。

TMMS 管理サーバで暗号化モジュールが有効になっており、暗号化ポリシーが設定されている場合、製品の登録が成功すると、モバイルデバイスエージェントはサポート対象のモバイルデバイスに暗号化モジュールをインストールします。

アクティベーションコードの形式

アクティベーションコードは、次の形式で表示されます。

xx-xxxx-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx

TMMS 管理サーバを登録するには

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。管理コンソールに初めてアクセスする場合は、[製品ライセンス] 画面が表示されます。そうでない場合は、[管理]→[製品ライセンス] をクリックしてから、[新しいコード] をクリックします。

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

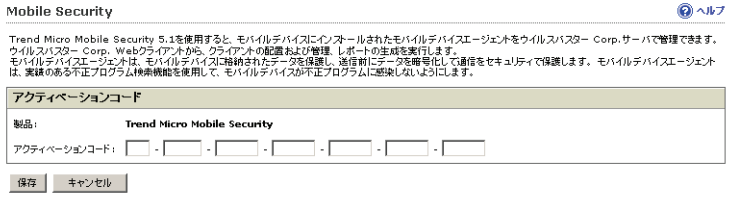


図 1-3. インストール後の Mobile Security の登録

4. 登録が正常に実行されたことを確認します。[概要] をクリックして、[概要] 画面を表示します。製品の登録が成功している場合、[Mobile Security のアクティベーションが完了しました。] というメッセージが表示されます。

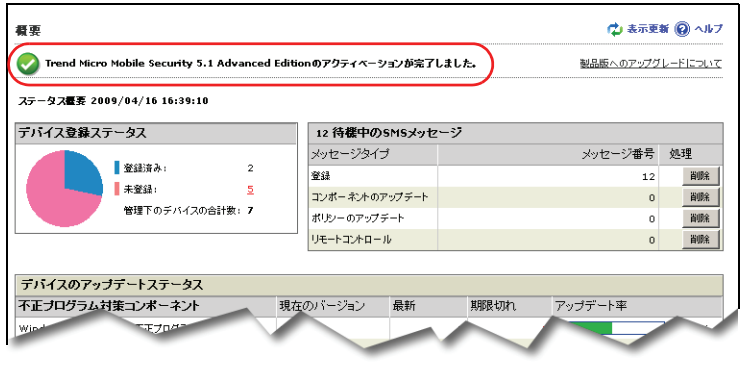


図 1-4. 成功した製品登録

接続設定

Mobile Security の次の接続の種類を設定するには、[接続設定] 画面を使用します。

- 3G/GPRS — インターネット上で、モバイルデバイス上のモバイルデバイスエージェントが TMMS 管理サーバと通信できるようにします。モバイルデバイスは、コンポーネント / ポリシーのアップデートおよびログのレポートのために、TMMS 管理サーバに直接またはプロキシ経由で接続することもできます。

  注意： 3G/GPRS 接続では、プロキシまたはウイルスバスター Corp. サーバが NAT デバイスの背後に存在する場合、ポートのマッピング設定を設定して、プライベート IP アドレスを DNS 名またはパブリック IP アドレスにマップすることが必要です。プロキシまたはウイルスバスター Corp. サーバがファイアウォールに保護されている場合は、ファイアウォールポリシーを設定してモバイルデバイスからのトラフィックを許可していることを確認してください。

- TMMS アップデートサーバ接続 — TMMS 管理サーバが、TMMS アップデートサーバに接続して、SMS Sender を管理できるようにします。TMMS アップデートサーバは、TMMS 管理サーバから、モバイルデバイスに通知メッセージを送信するよう SMS Sender を設定する指示を受け取ります。

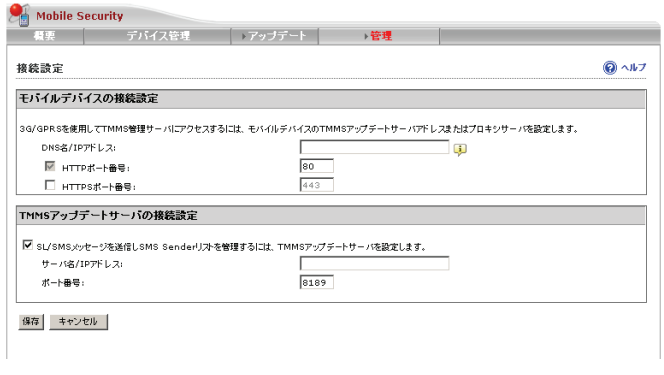


図 1-5.　接続設定

3G/GPRS 接続を設定するには

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. [管理]→[接続設定] をクリックします。
4. [DNS 名 /IP アドレス] フィールドに、TMMS 管理サーバをインストールしたプロキシまたはウイルスバスター Corp. サーバのパブリック DNS 名または IP アドレスを入力します。
5. 3G/GPRS 通信を行うためのプロトコルとポート番号を指定します。

   初期設定では、TMMS 管理サーバは、3G/GPRS 接続に、ポート 80 で **HTTP** プロトコルを使用します。別の HTTP ポートを使用する場合は、ポート番号を入力します。
   セキュリティで保護された接続には、**HTTPS** を選択し、表示されるフィールドにサービスポート番号を指定します (443 など)。
6. **[保存]** をクリックします。

警告： HTTPS 接続設定は、Symbian デバイスには適用されません。Symbian デバイスは、TMMS 管理サーバとの通信に、HTTP 接続のみを使用します。

TMMS アップデートサーバ接続を設定するには

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. [管理]→[接続設定] をクリックします。
4. [SL/SMS メッセージを送信し SMS Sender リストを管理するには、TMMS アップデートサーバを設定します] チェックボックスをオンにして、TMMS 管理サーバが TMMS アップデートサーバに指示を送信できるようにします。

5. [サーバ名 /IP アドレス] フィールドに、TMMS アップデートサーバの名前または IP アドレスを入力します。
6. [ポート番号] フィールドに、TMMS アップデートサーバが SL/SMS メッセージの送信に使用するサービスポートを入力します。
7. [保存] をクリックします。

注意： TMMS アップデートサーバと、ウイルスバスター Corp. サーバ、SMS Sender のホストコンピュータ、またはプロキシサーバとの間で、ファイアウォールがインストールされている場合、ファイアウォールポリシーを設定して、TMMS アップデートサーバ上の指定されたポートにトラフィックを許可する必要があります。

TMMS アップデートサーバへの接続を検証するには

1. TMMS アップデートサーバの設定後、ウイルスバスター Corp. の Web 管理コンソールにログオンして、メインメニューの [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] 画面が表示されます。[TMMS アップデートサーバにアクセスできませんでした] というエラーメッセージが表示されなければ、TMMS 管理サーバは、TMMS アップデートサーバに正常に接続できます。

SMS Sender リストを設定する

TMMS 管理サーバと SMS Sender 間の通信を許可するには、ウイルスバスター Corp. の Web 管理コンソールに SMS Sender 情報を入力する必要があります。

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]→[SMS Sender リスト] をクリックします。

4. [SMS Sender リスト] タブで、[追加] をクリックします。

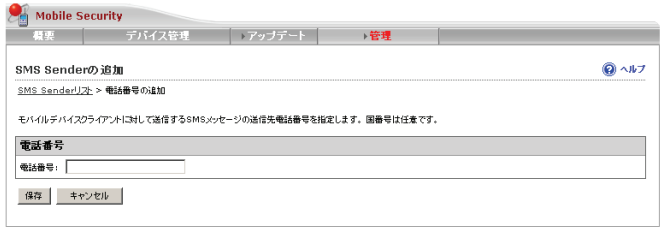


図 1-6. SMS Sender の追加

5. [SMS Sender 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。

警告： ここで使用する電話番号が、SMS Sender デバイスで設定されている電話番号と同じであることを確認してください。これらの電話番号が異なると、SMS Sender は TMMS アップデートサーバに接続できません。

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 が TMMS アップデートサーバに接続できることを確認してください。

第 2 章

モバイルデバイスエージェントコンポーネントのインストール

この章では、さまざまなモバイルデバイスエージェントの配置方法について説明します。モバイルデバイスエージェントがサポートするモバイルデバイス要件およびモデルについても示します。

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インストールを計画する

注意： モバイルデバイスが、WiFi、3G/GPRS、またはホストコンピュータでのインターネット接続を使用して、TMMS 管理サーバに接続できることを確認してください。

サポート対象のモバイルデバイスとプラットフォーム

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

デバイスストレージおよびメモリ

OS	暗号化モジュールなし		暗号化モジュールあり	
	メモリ (MB)	ストレージ (MB)	メモリ (MB)	ストレージ (MB)
Windows Mobile 5 Pocket PC/Pocket PC Phone	1.7	5	2.2	9
Windows Mobile 6 Classic/Professional	1.7	5	2.2	9
Windows Mobile 5 Smartphone	2	5	3	10
Windows Mobile 6 Standard	2	5	3	10
Symbian OS 9.x S60 3rd Edition	2.6	1	該当なし	該当なし

表 2-1.　OS およびデバイスメモリの要件

注意： サポート対象のモバイルデバイスの一覧については、次を参照してください。
http://jp.trendmicro.com/jp/products/enterprise/mobile-security/index.html

モバイルデバイスエージェントのインストール方式

次の方式のいずれかを使用して、モバイルデバイスエージェントをモバイルデバイスにインストールできます。

- SMS メッセージを使用したサイレントインストール — モバイルデバイスエージェントのインストール URL を含む SMS メッセージをモバイルデバイスに送信します。サービスプロバイダが SL メッセージを許可するかどうかによって、モバイルデバイスエージェントがモバイルデバイスに自動でインストールおよび登録されるか、ユーザが SMS メッセージの URL をクリックしてプロセスを開始する必要があるかが決まります。TMMS アップデートサーバと SMS Sender をインストールする必要があります。
- メモリカード — TMMS 管理サーバからセットアップファイルをダウンロードして、解凍後のファイルをメモリカードにコピーします。メモリカードをモバイルデバイスに挿入すると、モバイルデバイスエージェントが自動でインストールおよび登録されます。

  注意： Symbian デバイスで Mobile Security 5.1 向けモバイルデバイスエージェントを再インストールまたはアップグレードする場合は、メモリカードによるインストール方式は使用できません。この場合は、手動インストール方式を使用する必要があります。

- デバイス管理 (DM) のフレームワーク — Nokia Intellisync、Sybase iAnywhere Afaria、および Odyssey Software Athena などのサードパーティ製のソフトウェアを使用して、モバイルデバイスエージェントをインストールできます。サポート対象のモバイルデバイスのセットアップファイルを解凍して、セットアップファイルを送信 (またはプッシュ) するように DM フレームワークを設定する必要があります。手順については、DM フレームワークに付属のドキュメントを参照してください。

- 手動インストール — セットアップファイルを各モバイルデバイスに転送して、セットアッププログラムを実行する必要があります。インストールが完了したら、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。手動インストールおよび登録に関する詳細な手順については、36 ページの「手動でセットアップファイルを起動する」またはモバイルデバイスプラットフォームの「ユーザガイド」を参照してください。

Mobile Security 5.1 にアップグレードする

Windows Mobile デバイスの Mobile Security のバージョンを 5.0 から 5.1 にアップグレードできます。その際、古いバージョンをアンインストールする必要はありません。セットアッププログラムにより、自動的に前のバージョンがアンインストールされてから Mobile Security 5.1 がインストールされます。

Symbian デバイスの場合は、バージョン 5.1 をインストールする前に、前のバージョンをアンインストールする必要があります。

注意： Windows Mobile モバイルデバイスで Mobile Security 2.0 を使用している場合は、バージョン 5.1 にアップグレードする前に、この古いバージョンをアンインストールしておく必要があります。

モバイルデバイスエージェントをインストールする

Windows Mobile モバイルデバイスに暗号化モジュールをインストールするには、まず次のことを行う必要があります。

- モバイルデバイスの Windows Mobile に付属している、パスワードセキュリティまたはメモリカード暗号化機能を無効にします。
- サードパーティ製のパスワードセキュリティプログラムを削除します。インストールプロセス中に、プログラムを削除するよう求められる可能性があります。

注意： 組み込みのパスワードセキュリティまたはメモリカード暗号化機能が有効になっている場合、暗号化モジュールはインストールされません。

SMS 通知を使用したサイレントインストール

SMS 通知を使用したモバイルデバイスエージェントのインストールには、次の手順が含まれます。

- 25 ページの「SMS Sender リストを設定する」
- 31 ページの「インストールメッセージを設定する」
- 32 ページの「モバイルデバイスリストを設定する」

インストールメッセージを設定する

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には、SMS Sender がモバイルデバイスに WAP プッシュ (Service Load) 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.) 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 の設定] をクリックします。

   [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 2-1. インストールメッセージの設定

4. 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。

5. [保存] をクリックします。

モバイルデバイスリストを設定する

SMS メッセージを特定のモバイルデバイスに送信する場合、TMMS 管理サーバのモバイルデバイスリストを設定します。最初にモバイルデバイスのリストを設定しないと、SMS Sender はモバイルデバイスエージェントをインストールして登録するようにモバイルデバイスに通知できません。

デバイス管理 (DM) のフレームワークまたはメモリカードを使用して、モバイルデバイスエージェントを手動でインストールする場合、デバイスが TMMS 管理サーバに登録されたら、TMMS 管理サーバは自動でモバイルデバイスエージェント情報をリストに追加します。

デバイスを追加するには

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. [デバイス管理] をクリックします。[デバイス管理] 画面が表示されます。
4. [デバイスツリーの管理] タブをクリックして、[デバイスの追加] を選択します。

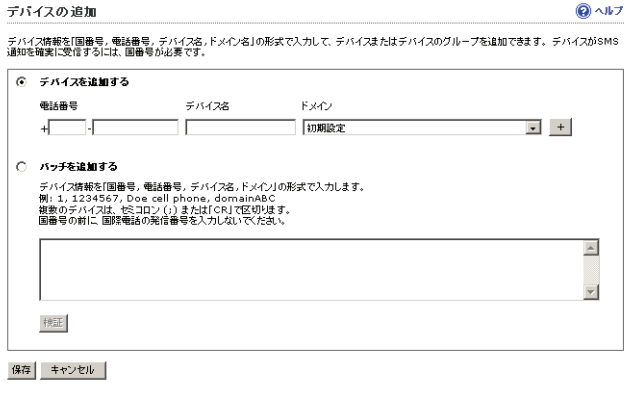


図 2-2.　デバイスの追加

5. [デバイスの追加] を選択して、次のフィールドを設定します。

   - **電話番号** — モバイルデバイスの電話番号を入力します。

   注意： モバイルデバイスが SMS Sender から確実に通知メッセージを受信できるように、国コード (長さ 1 ～ 5 桁) を入力してください。国際電話の発信番号を入力する必要はありません。

   - **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を入力します。
   - **ドメイン** — モバイルデバイスが属するドメインの名前をリストから選択します。ドメインをリストから選択しない場合、モバイルデバイスは「初期設定」ドメインに追加されます。モバイルデバイスが属するドメインはいつでも変更できます。

ヒント： さらにデバイスを追加するには、[+] ボタンをクリックします。
または、[バッチを追加する] を選択してからデバイス情報をボックスに入力します。[検証] をクリックして、デバイス情報が指定の形式に従っているかどうかを検証します。

6. [保存] をクリックします。
7. 新しいデバイスの情報がデバイスツリーに表示されていることを確認します。
   TMMS 管理サーバでモバイルデバイスの情報を追加したら、次の節を参照して、これらのモバイルデバイスにモバイルデバイスエージェントをインストールします。

モバイルデバイスエージェントのステータスを確認する

TMMS 管理サーバでモバイルデバイス情報を保存したら、SMS Sender は、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開始するようにモバイルデバイスに通知する SMS メッセージを自動で送信します。インストールが正常に完了したら、モバイルデバイスエージェントは自動的に TMMS 管理サーバに登録されます。ファイルのダウンロード、製品のインストールおよび登録には数分かかる場合があります。

ウイルスバスター Corp. サーバの Mobile Security の [概要] 画面で、モバイルデバイスエージェント登録ステータスを確認できます。

メモリカードを使用してインストールする

メモリカードを使用して、手動でモバイルデバイスエージェントをモバイルデバイスにインストールすることができます。TMMS 管理サーバからセットアップファイルをダウンロードして、解凍後のファイルをメモリカードにコピーする必要があります。

警告： Symbian デバイスでモバイルデバイスエージェントを再インストールまたはアップグレードする場合は、メモリカードによるインストール方式は使用できません。この場合は、手動インストール方式を使用する必要があります。

TMMS 管理サーバからセットアップファイルを取得するには

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. [プラグインマネージャ] 画面で、Mobile Security の [プログラムの管理] をクリックします。
3. [管理]→[デバイスのセットアップファイル] をクリックします。
4. [ダウンロード] をクリックして、コンピュータに ZIP ファイルをダウンロードします。
5. ZIP ファイルを解凍します。
6. 解凍後のファイルをメモリカードのルートフォルダにコピーします。

注意： Apache Web サーバを使用していて、セットアップパッケージをテキストファイルとして開く場合は、Apache Web サーバの設定を変更する必要があります。「conf/http.conf」ファイルの「DefaultType text/plain」を「application/octet-stream」に置き換えるか、「conf/mime.types」ファイルの「application/octet-stream」行の後に、「sis cab zip」を追加します。

解凍後のファイルがメモリカードのルートフォルダにない場合は、モバイルデバイスにカードを挿入しても自動インストールは実行されません。

モバイルデバイスにモバイルデバイスエージェントをインストールするには

1. モバイルデバイスにメモリカードを挿入します。セットアップによってモバイルデバイスエージェントが自動でインストールされます。
2. インストールが完了したら、プロンプトに従ってモバイルデバイスを再起動します。
3. モバイルデバイスは、ウイルスバスター Corp. サーバに自動で登録されます。Mobile Security が [スタート] メニューに追加されます。

登録プロセスには数分かかる場合があります。モバイルデバイスが正常に登録されたことを検証するには、TMMS 管理サーバのデバイスツリーのモバイルデバイスエージェントのステータスを確認します。

手動でセットアップファイルを起動する

モバイルデバイスのセットアップファイルを実行して、手動でモバイルデバイスエージェントをインストールすることができます。セットアップファイルをモバイルデバイスに転送するには、ActiveSync または PC Suite を使用して、モバイルデバイスをホストコンピュータに接続する必要があります。インストールが正常に完了したら、モバイルデバイスエージェントを TMMS 管理サーバに手動で登録してください。

注意： Symbian デバイスの場合は、次のようになります。
- PC Suite を備えたホストコンピュータでセットアップファイルを直接実行できます。
- バージョン 5.1 のモバイルデバイスエージェントをインストールする前に古いバージョンのモバイルデバイスエージェントをアンインストールする必要があります。

TMMS 管理サーバからセットアップファイルを取得するには

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. [プラグインマネージャ] 画面で、Mobile Security の [プログラムの管理] をクリックします。
3. [管理]→[デバイスのセットアップファイル] をクリックします。
4. [ダウンロード] をクリックして、コンピュータに ZIP ファイルをダウンロードします。
5. ZIP ファイルを解凍して、解凍後のファイルをホストコンピュータにコピーします。
6. 管理者は、このファイルをユーザに送信するための最適な手段を決定する必要があります。たとえば、メールやイントラネットのヘルプデスクサイトなどです。
7. URL にアクセスしてセットアップファイルをダウンロードし、モバイルデバイスにインストールするように、ユーザに指示できます。

   サーバにアクセス可能な内部ネットワークのユーザの場合：
   http(s)://<Office scan Server:Port>/officescan/PLS_TMMS_CGI/cgiOsmaProvision.exe

   内部ネットワークにアクセスできないスタンドアロンユーザの場合：
   http://<Public Address:Port>/officescan/PLS_TMMS_CGI/cgiOsmaProvision.exe

8. または、インストールファイルを提供することもできます。

   適切なセットアップファイルをモバイルデバイスに転送するか、PC Suite を備えたホストコンピュータでセットアップファイルを実行 (Symbian デバイスのみ) します。

   - Windows Mobile 5 for Smartphone または Windows Mobile 6 Standard の場合 : MobileSecurity_SP.cab
   - Windows Mobile 5 for Pocket PC/Pocket PC Phone または Windows Mobile 6 Professional/Classic の場合 : MobileSecurity_PPC.cab
   - Symbian OS 9.x S60 3rd Edition の場合 : MobileSecurity_S60.sis

---

注意 : Apache Web サーバを使用していて、セットアップパッケージをテキストファイルとして開く場合は、Apache Web サーバの設定を変更する必要があります。「conf/http.conf」ファイルの「DefaultType text/plain」を「application/octet-stream」に置き換えるか、「conf/mime.types」ファイルの「application/octet-stream」行の後に、「sis cab zip」を追加します。

次の場所にあるサーバから、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直接入手することもできます。http(s)://<Office scan Server: Port>/officescan/PLS_TMMS_ActiveUpdate/<Setup Package Name>

<Setup Package Name> サーバ上のセットアップパッケージ名は次のようになります。
PPC: MobileSecurity_PPC.cab
SP: MobileSecurity_SP.cab
Symbian: MobileSecurity_S60.sis

Windows Mobile デバイスにモバイルデバイスエージェントを手動でインストールするには

1. デバイスで、セットアップファイルの場所へ移動します。
2. セットアップファイルを開いて、モバイルデバイスエージェントのインストールを開始します。

3. インストールが完了したら、TmSettings.ini ファイルを次のようなデバイスの適切なディレクトリにコピーします。

   - ¥Program Files¥Trend Micro¥Mobile Security¥5.0¥ (Windows Mobile の場合)
   - C:¥data¥mobilesecurity¥ (Symbian OS の場合、このディレクトリにアクセスするにはサードパーティ製のファイルエクスプローラが必要)
   - E:¥mobilesecurity (Symbian OS の場合、このディレクトリにアクセスするにはサードパーティ製のファイルエクスプローラが必要)

4. デバイスを再起動します。デバイスは自動でサーバに登録されます。

手動登録

モバイルデバイスエージェントを手動でインストールする場合、または自動登録プロセスが失敗した場合は、モバイルデバイスエージェントを TMMS 管理サーバに手動で登録する必要があります。

モバイルデバイスエージェントを TMMS 管理サーバに手動で登録するには

1. モバイルデバイスでモバイルデバイスエージェントプログラムを開きます。Windows Mobile プラットフォームでは、ディスプレイに初めてアクセスする場合、パワーオンパスワードを入力するよう指示される可能性があります。
2. [登録] 画面が表示されます。わかりやすいデバイス名、およびウイルスバスター Corp. サーバ (TMMS 管理サーバのインストール先サーバ) または TMMS アップデートサーバの DNS 名か IP アドレス、およびポート番号を入力します。[登録] をクリックします。
3. 登録が完了したら、[バージョン情報] 画面 ([メニュー]→[バージョン情報]) でライセンス情報を確認します。TMMS 管理サーバでデバイスのステータスを表示することもできます。登録プロセスには数分かかる場合があることに注意してください。

デバイス管理のフレームワークを使用する

この節では、Nokia Intellisync、Sybase iAnywhere Afaria、および Odyssey Software Athena などのサードパーティ製のデバイス管理 (DM) のフレームワークを使用して、モバイルデバイスエージェントを配置して管理する方法について説明します。このドキュメントでは、これらのデバイス管理のフレームワークが一般的にサポートしているアプローチを示します。

デバイス管理のフレームワークを使用してモバイルデバイスエージェントを配置するには

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. [プラグインマネージャ] 画面で、Mobile Security の [プログラムの管理] をクリックします。
3. [管理]→[デバイスのセットアップファイル] をクリックします。
4. [ダウンロード] をクリックして、コンピュータに ZIP ファイルをダウンロードします。
5. ZIP ファイルを解凍します。
6. 解凍後のファイルと TmSettings.ini をデバイス管理のフレームワークサーバにコピーします。デバイス管理のフレームワークサーバで、TMsetting.ini ファイルを、¥Program Files¥Trend Micro¥Mobile Security¥5.0¥ (Windows Mobile の場合) または C:¥data¥mobilesecurity¥ (Symbian OS の場合) に保存します。
7. デバイスでセットアップファイルを実行するためのコマンドを送信して、モバイルデバイスエージェントをインストールします。
8. インストールが完了したら、モバイルデバイスエージェントは自動的に TMMS 管理サーバに登録されます。

暗号化モジュールをインストールする

暗号化モジュールは、モバイルデバイスでのパワーオンパスワードと暗号化機能を提供します。

次の要件を満たしている場合、暗号化モジュールはモバイルデバイスに自動でインストールされます。

- モバイルデバイスエージェントが正常にインストールされている。
- モバイルデバイスエージェントが TMMS 管理サーバに正常に登録されている。
- 製品ライセンスに暗号化ライセンスが含まれている。
- 暗号化モジュールがモバイルデバイスのモデルとプラットフォームをサポートしている。
- 初期設定のシステムログインパスワードセキュリティがモバイルデバイスで無効になっている。

暗号化モジュールをインストールするには

1. モバイルデバイスエージェントのインストールと TMMS 管理サーバへの登録の完了後、デバイスへの暗号化モジュールのインストールを求めるプロンプトが表示されたら、それを受け入れます。
2. デバイスを再起動して、暗号化モジュールを有効にします。デバイスの再起動が完了すると、[パスワード] 画面が表示されます。初期設定では、初期パスワードは「123456」です。

注意： ウイルスバスター Corp. の Web 管理コンソールを介してモバイルデバイスエージェントが削除されると、暗号化モジュールが自動でアンインストールされます。

第 3 章

デバイス管理のフレームワーク

この章では、デバイス管理のフレームワークを紹介し、トレンドマイクロのデバイス管理エージェントについて説明します。サードパーティ製のデバイス管理のフレームワークを使用して、モバイルデバイスにインストールされたモバイルデバイスエージェントを管理する場合は、この章をお読みください。

この章には、次のトピックが含まれています。

デバイス管理エージェントについて

デバイス管理エージェント TmDMAgent.exe を使用すると、モバイルデバイスエージェントをリモートでインストールして管理できます。適切なスイッチを使用して、このファイルをリモートで実行できるサードパーティ製のデバイス管理フレームワークであればどれでも、サポート対象のモバイルデバイスでモバイルデバイスエージェントを設定できます。

トレンドマイクロでは、デバイス管理エージェントに Trend Micro Mobile Security 5.1 (以下、Mobile Security) を提供しています。この製品のインストーラは、次の表に示すとおり、デバイスの特定の場所にエージェントをコピーします。

プラットフォーム	場所
Windows Mobile 5/6	¥Program Files¥Trend Micro¥Mobile Security¥5.0¥TmDMAgent.exe
Symbian OS 9.x S60 3rd Edition	C:¥sys¥bin¥TmDMAgent.exe

デバイス管理エージェントの機能

デバイス管理エージェントには、次の機能があります。

- **検索エンジンのアップデート** (Windows Mobile デバイスのみ) — デバイス管理のフレームワークで特定のフォルダに新しい検索エンジンを配置し、Mobile Security をアップデートするためにエージェントを呼び出すことができます。

注意： S60 バージョンの新しいエンジンのリリースは、PU タイプの SIS ファイルとしてパックされています。通常、デバイス管理のフレームワークでは、これらの SIS パッケージを直接インストールできます。

- **パターンファイルアップデート** — デバイス管理のフレームワークは、特定のフォルダに新しいパターンファイルを配置して、Mobile Security をアップデートするためにエージェントを呼び出すことができます。
- **製品ポリシー** — デバイス管理のフレームワークでは、エージェントを使用して次の製品ポリシーを設定できます。
    - リアルタイム検索ポリシー
    - アップデートポリシー
    - ファイアウォールポリシー
    - SMS スパムメール対策の有効化 / 無効化
    - WAP プッシュ保護の有効化 / 無効化
    - ロック / ロック解除ポリシー (SMS スパムメール対策ポリシーおよび WAP プッシュ保護ポリシーは対象としていません)

コマンドスイッチおよび構文

デバイス管理エージェントを使用してモバイルデバイスエージェントをアップデートまたは設定するには、デバイス管理のフレームワークを使用して正しいスイッチで TmDMAgent.exe を実行します。処理と対応するスイッチの一覧については、下の表を参照してください。

処理	スイッチ / 構文	例
検索エンジンのアップデート	/e < 新しいエンジンのパス >	.../TmDMAgent.exe /e ¥temp¥vsapice.dll **注意**： S60 デバイスでは、デバイス管理のフレームワークは通常、検索エンジンのアップデート (SIS パッケージ) を直接インストールできます。
検索パターンファイルのアップデート	/e < 新しいパターンファイルのパス >	**Windows Mobile の場合**： ¥Program Files¥Trend Micro¥Mobile Security¥ 5.0¥TmDMAgent.exe /p ¥temp¥msvpnwce.108 **S60 の場合**： C:¥sys¥bin¥TmDMAgent.exe /p c:¥data¥msvpnwce.108
製品の設定	/o <option 1>=<option value 1> ... <option n>=<option value n> **注意**：サポートされるオプションについては、「設定オプション」を参照してください。	.../TmDMAgent.exe /o SMSSpamOption=2 LockAllOption=1

注意： 複数の単語を含む値は、引用符で囲んでください。例 : /p "¥temporary files¥msvpnwce.108"

コマンドを送信する

デバイスは、デバイス管理エージェントのインスタンスを 1 つだけ実行します。エージェントがすでに実行中の場合、新しいインスタンスは自動で終了します。

通常、デバイス管理のフレームワークは、コマンドを待機して、エージェントのインスタンスが 1 つだけ実行されるようにします。コマンドが正常に実行されるために、次のベストプラクティスに留意してください。

- 可能なかぎり、複数のコマンドを実行するのではなく、1 つのコマンドで複数のオプションを使用して実行してください。
- 同じデバイスにコマンドを送信する時間間隔を十分確保してください。設定コマンドを送信する場合は最低 5 秒、アップデートコマンドを送信する場合は最低 1 分空けてください。

設定オプション

デバイス管理エージェントでは、設定スイッチ /o に対して次のオプションをサポートします。

オプション	値	説明
RealTimeScan	・ 0 — 無効 ・ 1 — 有効	リアルタイム検索を有効 / 無効にします
CompressedFileScanLayer	1, 2, 3	検索する圧縮レイヤ数を設定します
EnableAutoUpdate	・ 0 — 無効 ・ 1 — 有効	自動検索を有効 / 無効にします

オプション	値	説明
SMSSpamOption	・ 0 — SMS スパムメール対策を無効にする ・ 1 — ブロックリストを有効にする ・ 2 — 承認済みリストを有効にする	スパムメール対策を設定します
PromptWhenConnectByWireless	・ 0 — 無効 ・ 1 — 有効	ワイヤレス接続通知を有効 / 無効にします
LockAllOption	・ 0 — ロック解除 ・ 1 — すべてロック	製品のインタフェースを使用したポリシー変更を、ユーザに対して拒否 / 許可します **注意**: このコマンドオプションは、SMS スパムメール対策ポリシーおよび WAP プッシュ保護ポリシーは対象としていません。
MaxUpdateFrequency	1, 7, 14, 30	強制アップデートを実行する時間間隔 (日数) を設定します
MinUpdateFrequency	1, 2, 4, 8	自動アップデートの時間間隔 (時間数) を設定します。これはデバイスがインターネットに接続された直後に実行されます。
BlockSMSwoIDOption	・ 0 — 無効 ・ 1 — 有効	不明な送信者からの SMS メッセージのブロックを有効 / 無効にします
FileScanType	・ 0x7FFFFFFF — すべてのファイルタイプ ・ 0x3 — 実行可能ファイルのみ ・ 0x7 — 実行可能ファイルおよび CAB/ZIP ファイル	検索対象のファイルタイプを指定します **注意**: このオプションは S60 バージョンではサポートされていません。

オプション	値	説明
InstantCardScanOption	・ 0 — 無効 ・ 1 — 有効	自動メモリカード検索を有効 / 無効にします
Firewall	・ 0 — 無効 ・ 1 — 有効	ファイアウォールを有効 / 無効にします
IDS	・ 0 — 無効 ・ 1 — 有効	IDS (侵入検知システム) を有効 / 無効にします。IDS を有効にするには、ファイアウォールを有効にする必要があります。
SecurityLevel	・ 1 — 高 ・ 2 — 中 ・ 3 — 低	ファイアウォールのセキュリティレベルを設定します

設定シナリオ

一般的な設定タスクを実行する方法の例については、次のシナリオを参照してください。

シナリオ 1

タスク :

・ リアルタイム検索を有効にします
・ ファイアウォールを有効にします

コマンド :

```
TmDMAgent.exe /o RealTimeScan=1 Firewall=1
```

シナリオ 2

タスク:

- SMS スパムメール対策を有効にして、承認済みの送信者からのメッセージのみを許可します
- ユーザがモバイルデバイスエージェントのポリシーを変更できないようにします (SMS スパムメール対策ポリシーおよび WAP プッシュ保護ポリシーは対象外)
- 検索実行中すべてのファイルタイプをチェックするように製品を設定します

コマンド:

```
TmDMAgent.exe /o SMSSpamOption=2 LockAllOption=1 FileScanType= 0x7FFFFFFF
```

シナリオ 3

タスク:

- リアルタイム検索を有効にします
- 7 日ごとに強制アップデートを実行するように製品を設定します
- 検索する圧縮レイヤの最大数を 2 に設定します。Mobile Security では、ZIP ファイルと CAB ファイルについては、最大 3 つの圧縮レイヤをサポートしています。1 つの圧縮ファイルをさらに圧縮する場合に複数の圧縮レイヤが発生します。たとえば、ZIP ファイルに別の ZIP ファイルが含まれている場合などです。

コマンド:

```
TmDMAgent.exe /o RealTimeScan=1 MaxUpdateFrequency=7
CompressedFileScanLayer=2
```

シナリオ 4

タスク:

- 不明な送信者からの SMS メッセージをブロックするように製品を設定します
- メモリカードが挿入されたときに自動で検索するように製品を設定します

コマンド:

TmDMAgent.exe /o BlockSMSwoIDOption=1 InstantCardScanOption=1

シナリオ 5

タスク:

- ファイアウォールを有効にします
- 侵入検知システムを有効にします
- ユーザがモバイルデバイスエージェントのポリシーを変更できないようにします (SMS スパムメール対策ポリシーおよび WAP プッシュ保護ポリシーは対象外)

コマンド:

TmDMAgent.exe /o Firewall=1 IDS=1 LockAllOption=1