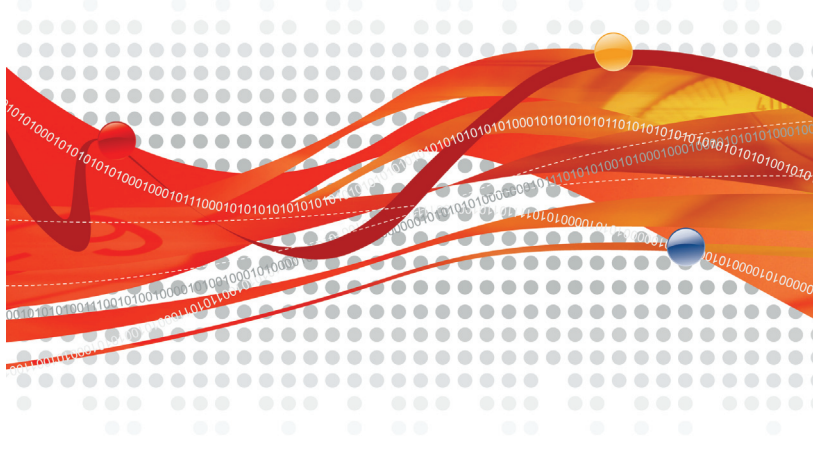
Trend Micro Mobile Security™
Smartphone/Standard 版



安心を、ひとつ上のステージへ。

TREND MICRO™

ユーザガイド

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-AE0300_51 (2009/5)

目次

第 1 章

はじめに

Trend Micro Mobile Security (以下、Mobile Security) は、モバイルデバイス向けの強力なセキュリティソリューションです。この章では、Mobile Security でモバイルデバイスを保護する方法について説明します。

この章は次のトピックで構成されています。

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、従来のラップトップやデスクトップコンピュータなどの、より大型のコンピュータデバイスにのみ関連付けられていたネットワーク接続と同じ接続を使用しているため、今やそのような脅威の対象となっています。

モバイルデバイスを保護する

安全性を考慮したコンピュータの使用を実践しているユーザは、不正プログラムによる重要なデータを喪失や、不正行為の犠牲に遭遇する可能性が低い傾向があります。自分自身を守るため、モバイルデバイスを使用する際は、次の安全対策を実施してください。

- モバイルデバイスおよびモバイルデバイスに接続するコンピュータに不正プログラム対策製品を使用します。
- モバイルデバイスをネットワークやインターネットに接続する場合は、モバイルデバイスでファイアウォールを実行します。
- コンテンツの許可およびインストールを求める、未承諾 WAP プッシュメッセージに警戒します。送信者になじみがなく、そのようなコンテンツを要求したこともなければ、受信する事前承諾もしていない場合は、そのコンテンツを許可しないでください。
- 何かに当選したという SMS メッセージに警戒します。これらのメッセージに送金や個人情報の開示が指示されている場合は、特に注意してください。
- 未承諾の Bluetooth メッセージから受信したアプリケーションをインストールしたり実行しないでください。公の場では、Bluetooth 無線をオンにしたままにしないでください。

Mobile Security の概要

Mobile Security は、モバイルデバイス向けの包括的なセキュリティソリューションです。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。

さらに、ファイアウォール機能とフィルタ機能を統合することにより、モバイルデバイスに対する不要なネットワーク通信 (SMS メッセージや WAP プッシュメールなど) を効果的にブロックします。Windows Mobile デバイスでは、Mobile Security の暗号化モジュールにより、ログオンパスワードの保護およびデータの暗号化が追加のセキュリティ機能として提供されます。

Mobile Security の機能

Mobile Security では次の機能を提供します。

- 最新の検索エンジン、パターンファイル、セキュリティポリシー、およびプログラムバージョンを確保するための、ウイルスバスター Corp. サーバからの予約または手動でのコンポーネントのアップデート
- 他人がモバイルデバイスにアクセスするのを防ぐログオン認証
- データがモバイルデバイスまたは装着されたメモリカードのどちらに格納されているのかにかかわらず、データを保護するデータの暗号化
- モバイル不正プログラムがないか検索する、実績のある不正プログラム検索テクノロジ
- 自動および定期的なコンポーネントのアップデート
- 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したり、Dos 攻撃を防ぐ、堅牢なファイアウォールおよび IDS (侵入検知システム) 機能
- 匿名のスパムメールが受信ボックスで受信されるのを防ぐ SMS スパムメール対策
- モバイルデバイスが不要なコンテンツを受信するのを防ぐ WAP プッシュ保護
- 検索結果、検出された不正プログラム、ポリシーに沿ったファイアウォールルール、および実行された処理に関するイベントログ

Mobile Security 5.1 にアップグレードする

モバイルデバイスの 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しておく必要はありません。セットアッププログラムにより、自動的に、Mobile Security 5.0 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。

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

第 2 章

インストール

Trend Micro Mobile Security (以下、Mobile Security) のインストールは、多くの準備を必要としない簡単なプロセスです。この章では、Mobile Security をモバイルデバイスに手動でインストールするための準備と実行方法について説明します。

この章は次のトピックで構成されています。

インストールする前に

ネットワーク管理者により、Mobile Security がすでにモバイルデバイスにインストールおよび設定されている場合は、インストールセクションを省略できます。

開始する前に、次の情報をネットワーク管理者から入手します。

- インストール方式
- 初期パワーオンパスワード (暗号化モジュールをインストールする場合)
- 登録情報 (手動登録が必要な場合)

注意： 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。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が有効な場合は、暗号化モジュールはインストールされません。
- 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。

手動インストール方式

Mobile Security を手動でインストールするように求められた場合は、ネットワーク管理者から使用するインストール方法が指示され、必要な情報が提供されます。次のいずれかの方法で、Mobile Security をモバイルデバイスに手動でインストールできます。

- SMS メッセージまたは WAP プッシュメッセージ内の URL をクリック(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)
- メモリカードを使用
- セットアップファイルを実行 (この方法では、ウイルスバスター Corp. サーバへの手動登録が必要です)

インストール方式に応じて、ネットワーク管理者から必要な情報を入手しておく必要があります。

方式	必須情報
インストール メッセージ	・モバイルデバイスの受信ボックス内の SMS および WAP プッシュのインストールメッセージ ・初期パワーオンパスワード
メモリカード	・root フォルダ内に Mobile Security セットアップファイルが格納されたメモリカード ・初期パワーオンパスワード
セットアップ ファイルの実行	・Mobile Security のセットアップファイル ・ActiveSync 4.2 (Windows Mobile 5 用)、4.5 (Windows Mobile 6 用)、またはそれ以降がインストールされたホストコンピュータ ・初期パワーオンパスワード ・登録情報 (サーバの IP アドレスおよびサービスポート番号など)

表 2-1.　手動インストールの必須情報

システム要件

Mobile Security をインストールして使用する前に、モバイルデバイスが次の要件を満たしていることを確認します。

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 6/6.1 Classic/Professional	1.7	5	2.2	9
Windows Mobile 5 Smartphone	2	5	3	10
Windows Mobile 6/6.1 Standard	2	5	3	10

表 2-2.　OS およびモバイルデバイスメモリの要件

注意： Mobile Security はモバイルデバイスの内部ストレージ領域にのみインストールできます。メモリカードにはインストールできません。

暗号化モジュール対応のモバイルデバイス

以下に記載されるモバイルデバイスモデルには、Mobile Security と共に暗号化モジュールもインストールできます。

http://jp.trendmicro.com/jp/products/enterprise/mobile-security/index.html

モバイルデバイスのプラットフォームを確認する

Smartphone 上で動作する Windows Mobile のバージョンを確認するには

1. [スタート]→[設定]→[次へ ...] の順に選択します。
2. [バージョン情報] を選択します。
3. [バージョン情報] 画面で、Windows Mobile のバージョンを確認します。

ホストコンピュータ

Mobile Security のインストールにはホストコンピュータは必要ありませんが、次の理由で、モバイルデバイスのコンピュータへの接続が必要になる場合があります。

- インストールファイルをモバイルデバイスにコピーするため
- Mobile Security のコンポーネントおよび設定をコンピュータのインターネット接続経由でアップデートするため

このような理由から、ActiveSync を実行する Microsoft Windows ベースのコンピュータが必要です。

ActiveSync を使用する

Mobile Security をインストールする前に、Microsoft ActiveSync (Windows Vista の場合はデバイスセンター) 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しておく必要がある場合があります。アクティブなインターネット接続を使用してモバイルデバイスをコンピュータに接続すると、Mobile Security のアップデートをダウンロードできます。

インストールファイルをコンピュータからコピーするには、モバイルデバイスをゲストとしてコンピュータに接続します。ただし、コンピュータのインターネット接続を使用して Mobile Security をアップデートするには、モバイルデバイスとコンピュータ間に「標準の同期関係」が必要です。詳細については、ActiveSync のドキュメントを参照してください。

コンピュータのインターネット接続を使用してアップデートを入手するには、モバイルデバイスのプロキシサーバの設定がコンピュータの Internet Explorer のプロキシ設定と一致していることを確認します。ActiveSync では、この確認を自動的に実行できますが、Internet Explorer でプロキシサーバの定義にスクリプトを使用している場合は、失敗する可能性があります。必要に応じて、サービスプロバイダまたはネットワーク管理者に正しいプロキシサーバ設定について相談の上、モバイルデバイスを手動で設定してください。

表 2-3 に、一般的なタスクに関する ActiveSync の必須設定を示します。

タスク	ActiveSync の必須設定
インストール ファイルのコピー	ゲストとして接続
コンポーネントの アップデート	標準の同期関係、つまり、プロキシサーバの設定がモバイルデバイスとコンピュータで同じである

表 2-3. ActiveSync の必須設定

図 2-1 に示すように、標準の同期関係にある場合は、モバイルデバイス名が表示され、自動的に同期されます。

図 2-1. 標準の同期関係で接続されている Microsoft ActiveSync およびデバイスセンター

モバイルデバイスがゲストとして接続されている場合は、図 2-2 に示すように、「ゲスト」と表示されます。

図 2-2.　モバイルデバイスがゲストとして接続されている Microsoft ActiveSync およびデバイスセンター

ヒント： ActiveSync 同期関係の詳細については、Microsoft ActiveSync のヘルプトピックの「同期関係の概要」を参照してください。

Mobile Security をインストールする

この節では、モバイルデバイスに Mobile Security を手動でインストールする方法について説明します。インストールが完了すると、Mobile Security が [スタート] メニューに追加されます。

注意： モバイルデバイスによっては、ファイアウォールや WAP プッシュ保護ドライバをロードするのに Mobile Security を再起動する必要があります。

SMS 通知メッセージを使用して Mobile Security を手動でインストールするには

1. モバイルデバイスがウイルスバスター Corp. サーバに接続できることを確認します。
2. モバイルデバイスの受信ボックスを確認します。ウイルスバスター Corp. サーバからの SMS メッセージを受信しているか確認します。
   a. モバイルデバイスで WAP プッシュメッセージを処理できる場合は、自動的に Mobile Security セットアップパッケージがダウンロードされ、Mobile Security がインストールされます。
   b. モバイルデバイスで WAP プッシュメッセージがサポートされていない場合は、SMS メッセージを開き、URL にアクセスして Mobile Security セットアップパッケージをダウンロードする必要があります。プロンプトが表示されたら、モバイルデバイスのプラットフォームを選択します。ダウンロード完了後に、Mobile Security が自動的にモバイルデバイスにインストールされます。

注意： 登録 SMS メッセージを受信ボックスから削除しないでください。Mobile Security では、ウイルスバスター Corp. サーバへの登録に SMS メッセージの情報を使用します。この SMS メッセージを誤って削除した場合は、ネットワーク管理者に相談してください。

3. インストールプロセス完了後、モバイルデバイスは、TMMS 管理サーバに自動的に登録されます（モバイルデバイスの仕様によってはウイルスバスター Corp. サーバに手動登録が必要です）。製品の登録に成功すると、暗号化モジュールをインストールするように求められます。詳細については、23 ページの「暗号化モジュールをインストールする」を参照してください。

メモリカードを使用して Mobile Security を手動でインストールするには

注意： ネットワーク管理者から、Mobile Security セットアップファイルを格納したメモリカードが提供されます。または、ネットワーク管理者がセットアップファイルをメモリカードに保存する場合もあります。

モバイルデバイスにメモリカードを挿入します。セットアッププログラムにより、Mobile Security が自動的にインストールされます。インストールプロセス完了後、モバイルデバイスは、ウイルスバスター Corp. サーバに自動的に登録されます。

製品の登録に成功すると、暗号化モジュールをインストールするように求められます。詳細については、23 ページの「暗号化モジュールをインストールする」を参照してください。

セットアップファイルを実行して Mobile Security を手動でインストールするには

1. セットアップファイル MobileSecurity_SP.cab をモバイルデバイスにコピーします。ActiveSync 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ことが必要になる場合があります。または、メモリカードを使用してファイルを転送することもできます。
2. モバイルデバイスで、セットアップファイルの場所へ移動します。
3. セットアップファイルを開いて Mobile Security のインストールを開始します。インストールが完了すると、Mobile Security が [スタート] メニューに追加されます。
4. モバイルデバイスをウイルスバスター Corp. サーバに手動で登録します (詳細については、22 ページの「手動登録」を参照してください)。製品の登録に成功すると、暗号化モジュールをインストールするように求められます。詳細については、23 ページの「暗号化モジュールをインストールする」を参照してください。

手動登録

モバイルデバイスをウイルスバスター Corp. サーバに登録し、モバイルデバイスの Mobile Security と暗号化モジュールのライセンスを取得します。使用するインストール方式によっては、Mobile Security のインストール後、モバイルデバイスがウイルスバスター Corp. サーバに自動的に登録される場合があります。

モバイルデバイスがウイルスバスター Corp. サーバに登録されていない場合は、初回ログオン後に [登録] 画面が表示されます。ネットワーク管理者から、ウイルスバスター Corp. サーバのホストおよびポート番号などの登録情報を入手しておく必要があります。

ウイルスバスター Corp. サーバにモバイルデバイスを登録しない場合は、30 日間の体験版ライセンスを使用して、モバイルデバイスで Mobile Security を使用できます。体験版ライセンスでは、コンポーネントのアップデートを除くすべての機能を使用できます。

モバイルデバイスをウイルスバスター Corp. サーバに登録するには

1. [登録] 画面 ([メニュー]→[登録]) で次のフィールドを設定します。
   - **モバイルデバイス名** — モバイルデバイスを示すわかりやすい名前を入力します。ウイルスバスター Corp. サーバ上では、この名前でモバイルデバイスが識別されます。
   - **ホスト** — ウイルスバスター Corp. サーバのホストを入力します。この情報は、ネットワーク管理者から入手します。
   - **ポート番号** — ウイルスバスター Corp. サーバの Web サーバポート番号を入力します。たとえば、80 と入力します。この情報は、ネットワーク管理者から入手します。
2. [登録] をタップします。確認を求めるポップアップ画面が表示されます。[OK] を選択して続行します。ネットワーク接続によっては、登録プロセスに数分かかる場合があります。
3. 登録が正常に完了したら、Mobile Security のメイン画面が表示されます。

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。

- Mobile Security がインストールされていること
- Mobile Security がウイルスバスター Corp. サーバに正常に登録されていること
- 暗号化ライセンスが製品ライセンスに含まれていること
- 暗号化モジュールで、使用しているモバイルデバイスのモデルがサポートされていること

暗号化モジュールをインストールするには

Mobile Security をインストールしてウイルスバスター Corp. サーバに登録した後で、モバイルデバイスへの暗号化モジュールのインストールを確認するプロンプトが表示されたら、それを許可します。

モバイルデバイスが自動的に再起動し、暗号化モジュールが利用可能になります。モバイル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。

注意： 暗号化モジュールのインストールおよびアンインストールは、モバイルデバイスエージェントによって完全に管理されます。[プログラムの削除] リストからアンインストール機能を使用できますが、トレンドマイクロでは、暗号化モジュールのアンインストールを手動で実行しないことをお勧めします。アンインストールが必要な場合は、暗号化管理者パスワードを管理者に要求してください。

初回ログオン

モバイルデバイスへの暗号化モジュールのインストール後、[パスワード] 画面に初期パワーオンパスワードを入力してログオンする必要があります。初回ログオン後に、パワーオンパスワードの変更を求められたり、パスワードリセットの質問の選択と回答の設定を求められる場合があります。

注意： 初期パワーオンパスワードを持っていない場合は、ログオンしないでください。ネットワーク管理者に連絡して情報を入手してください。

モバイルデバイスに初めてログオンするには

1. [パスワード] 画面で、ネットワーク管理者から指定された初期ログオンパスワードを入力します。
2. [ロック解除] をタップします。

初回ログオン後にパスワードを変更する

ネットワークのセキュリティポリシーによっては、初回ログオン後に初期パワーオンパスワードの変更を要求される場合があります。

初回ログオン後にパスワードを変更するには

1. 初回ログオン後、画面にパスワードの変更を求めるプロンプトが表示されます。[パスワード] フィールドに新しいパワーオンパスワードを入力します。
2. [パスワードの確認] フィールドに新しいパワーオンパスワードを再度入力します。
3. [終了] をタップします。パスワード変更が成功したかどうかを示す画面が表示されます。

注意： パワーオンパスワードの設定後、ActiveSync を使用してホストコンピュータからモバイルデバイスに接続する前に、同じパスワードをホストコンピュータに入力しておく必要があります。

パスワードを忘れた場合の質問と回答を設定する

パスワードを忘れた場合の質問と回答を指定するように求められる場合があります。パワーオンパスワードを忘れた場合、選択した質問に正しい回答を入力することにより、モバイルデバイスのロックを解除することができます。

初回ログオン後に、パスワードを忘れた場合の質問と回答を設定するには

1. 初回ログオン後、画面に質問の選択を求めるプロンプトが表示されます。質問のリストをスクロールし、[終了] をタップして質問を選択します。
2. 選択した質問の回答を設定するように求めるプロンプトが表示されます。[パスワード] フィールドと [パスワードの確認] フィールドに回答を入力します。
3. [終了] をタップします。パスワードを忘れた場合の質問と回答の設定に成功したことを示す画面が表示されます。ポップアップ画面を閉じてモバイルデバイスにログオンします。

アンインストール

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、またはホストコンピュータを通じてアンインストールできます。

モバイルデバイス上で直接アンインストールするには

1. モバイルデバイスで、[設定]→[プログラムの削除] の順に選択します。
2. [Trend Micro Mobile Security] を選択します。
3. [削除] をタップするか、[メニュー]→[削除] の順に選択します。
4. 要求された場合は、管理者パスワードを入力し、[OK] をタップして続行します。

注意： 必要に応じて、システム管理者からパスワードを受け取ることができます。

警告： アンインストールをキャンセルした、またはアンインストールに失敗した場合は、ダイアログから [いいえ] を選択してください。
Mobile Security は完全には削除されていません。インストールされているプログラムのリストから Mobile Security を削除する必要があります。
[はい] を選択すると、アンインストールが予期せず完了してしまう場合があります。

5. 確認を求められた場合は、[はい] を選択します。
6. ポリシーの保存を求められた場合は、次のいずれかを選択します。
   - はい— ファイアウォールルール、スパムメール対策リストなどの現在のポリシーを保存し、Mobile Security の再インストール時に使用できるようにします。
   - いいえ — 現在のポリシーを削除します。

ホストコンピュータを介してアンインストールするには

1. モバイルデバイスをホストコンピュータに接続します。
2. ホストコンピュータで Microsoft ActiveSync を開きます。
3. ActiveSync パネルで、[ツール]→[アプリケーションの追加と削除] をクリックします。
4. 要求された場合は、管理者パスワードを入力し、[OK] をクリックして続行します。
5. プログラムのリストで、[Trend Micro Mobile Security] を選択して [削除] をクリックします。
6. 確認を求められた場合は、[OK] をクリックします。
7. ポリシーの保存を求められた場合は、次のいずれかを選択します。
   - はい — ファイアウォールルール、スパムメール対策リストなどの現在のポリシーを保存し、Mobile Security の再インストール時に使用できるようにします。
   - いいえ — 現在のポリシーを削除します。

第 3 章

基本の操作

Trend Micro Mobile Security (以下、Mobile Security) は、インストール後すぐに使用できます。この章では、基本のタスク、メイン画面とそのメニュー項目、および製品の初期設定のポリシーについて説明します。

この章は次のトピックで構成されています。

パワーオンパスワード

Mobile Security および暗号化モジュールをインストールした後で、モバイルデバイスのログオンパスワード (パワーオンパスワードとしても知られる) を設定する必要があります。パワーオンパスワードは、モバイルデバイスへの不正アクセスを防ぎます。

ネットワーク管理者から、以下のパスワードポリシーに関する情報が提供されます。

- パスワードに使用できる文字の種類。たとえば、パスワードには、数字のみが使えるか、数字と英字両方が使用できるか、などです。
- パスワードに英数字を使用できる場合のパスワードの複雑さ。たとえば、大文字と小文字を混合して入力する必要があるかどうか、または英数字以外の文字を少なくとも 1 文字使用する必要があるかどうかなどです。
- 現在のパスワードの有効期限。有効期限が過ぎたら、新しいパスワードを設定する必要があります。
- 間違ったパスワードを入力できる回数。

注意： 間違ったパスワードを何度も入力すると、モバイルデバイスは次のように動作します。

- 再起動し、パワーオンパスワードを入力するように求めます。
- モバイルデバイスのロックを解除し、パワーオンパスワードをリセットするために管理者パスワードが必要となります。
- モバイルデバイスおよび装着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。
- モバイルデバイスを出荷時の初期設定ポリシーにリセットし、モバイルデバイスのすべてのデータを削除します。

パスワードを変更する

現在のパスワードの有効期限が切れたり、管理者がモバイルデバイスのロックをリモートで解除した場合は、パスワードの変更が必要になる場合があります。

パワーオンパスワードを変更するには

1. [パスワード] 画面で、[メニュー]→[パスワードの変更] の順に選択します。
2. 現在のパスワードを表示されたフィールドに入力し、[ロック解除] を選択します。画面にパスワードの変更を求めるプロンプトが表示されます。
3. [パスワード] フィールドに新しいパスワードを入力します。
4. 確認のため、[パスワードの確認] フィールドに同じパスワードを入力します。パスワードの変更に成功すると、メッセージが表示されます。
5. [終了] をクリックしてモバイルデバイスにログオンします。

パスワードをリセットする

パスワードを忘れた場合は、次の方法のいずれかを使用し、モバイルデバイスのロックを解除してパスワードをリセットできます。

- 選択したパスワードリセットの質問に答えを入力します。
- 管理者にリモートでモバイルデバイスのロックを解除し、パスワードをリセットするための応答コードを提供してもらいます。

パスワードリセットの質問に回答してパスワードを変更するには

1. [パスワード] 画面で、[メニュー]→[パスワードの紛失] の順に選択します。パスワードリセットの質問が表示されます。
2. 回答を入力して [ロック解除] を選択します。
3. 新しいパスワードを設定するように求められます。[パスワード] フィールドと [パスワードの確認] フィールドに新しいパスワードを入力します。

4. [終了] を選択します。パスワードのリセットに成功すると、モバイルデバイスにアクセスできるようになります。

モバイルデバイスのロックをリモートで解除するには

1. [パスワード] 画面で、[メニュー]→[リモートによるロック解除] の順に選択します。
2. モバイルデバイスでパスコードが自動的に生成されます。[表示更新] をタップして、新しいコードを生成できます。
3. このパスコードをネットワーク管理者に渡します。[リモートによるロック解除] 画面を閉じたり、何らかのボタンを選択しないでください。
4. ネットワーク管理者からの指示を受けたら、[次へ] をクリックします。
5. 応答コードを入力し、[次へ] をクリックします。
6. パスワードのリセットに成功すると、新しいパスワードを設定するように求められます。[パスワード] フィールドと [パスワードの確認] フィールドに新しいパスワードを入力します。
7. [終了] をクリックします。パスワードのリセットに成功すると、モバイルデバイスにアクセスできるようになります。

モバイルデバイスをロックする

非アクティブ状態で一定の期間が経過すると、モバイルデバイスは自動的にセキュアモードになります。つまり、モバイルデバイスからログアウトされ、[パスワード] 画面または電話画面が表示されるようになります。非アクティブ状態のタイムアウト期間は、企業の方針に応じて異なります。この情報については、ネットワーク管理者にお問い合わせください。

モバイルデバイスを手動でロックできます。[Today] 画面で、ロックアイコンをクリックします。

モバイルデバイスがロックされた場合でも、電話をかけることはできますが、モバイルデバイスのファイルやプログラムにアクセスすることはできません。

モバイルデバイスのロックを解除する

モバイルデバイスのロックを解除するには、パワーオンパスワードを入力し、[ロック解除] を選択します。

注意： 間違ったパスワードを何度も入力すると、モバイルデバイスは次のように動作します。

- 再起動し、パワーオンパスワードを入力するように求めます。
- モバイルデバイスのロックを解除し、パワーオンパスワードをリセットするために管理者パスワードが必要となります。
- モバイルデバイスおよび装着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。
- モバイルデバイスを出荷時の初期設定ポリシーにリセットし、モバイルデバイスのすべてのデータを削除します。

データ暗号化

モバイルデバイス上でデータが確実に保護されるようにするため、Mobile Security の暗号化モジュールにより、モバイルデバイス上のファイルやデータが暗号化されます。企業の方針によっては、メモリカードに保存されたデータも暗号化され、社外の人間がメモリカード内の暗号化されたファイルを開くことができないようにする場合があります。詳細については、ネットワーク管理者にお問い合わせください。

たとえば、メモリカードのデータの暗号化が有効な場合に、モバイルデバイスを使用してメモリカード上のファイルを開いて保存すると、そのファイルは暗号化されます。ただし、変更を加えずに、モバイルデバイスからメモリカード上のファイルを表示するだけの場合は、ファイルは暗号化されません。

注意： 暗号化ライセンスの有効期限が切れると、モバイルデバイスおよび装着されているメモリカード内の暗号化されたすべてのファイルやデータが自動的に復号化されます。

Mobile Security のインタフェースについて

Mobile Security には、製品のさまざまな機能を容易に理解してアクセスできるようにする、簡便なインタフェースが用意されています。メインインタフェースの構成は次のとおりです。

- 「メイン画面」
- 「メニュー項目」

メイン画面

Mobile Security が起動すると、メイン画面が表示されます。メイン画面では、次の処理が可能です。

図 3-1. メイン画面

インタフェースの項目	処理
1	リアルタイム検索を有効 / 無効にします
2	ファイアウォールの事前定義の保護レベルを選択したり、ファイアウォールを無効にします
3	製品をアップデートします

表 3-1. メイン画面のインタフェース項目

メニュー項目

メイン画面のメニューから製品のすべての機能にアクセスできます。メイン画面のメニュー項目および実行可能な処理は、次のとおりです。

メニュー項目	処理
検索	不正プログラムがないかモバイルデバイスを検索します
オプション	製品のオプションにアクセスします
隔離リスト	隔離ファイルにアクセスします
イベントログ	イベントログを表示します
不正プログラムの定義	既知のモバイル不正プログラムの定義を表示します
ヘルプ	ヘルプを表示します
登録	製品を登録します
バージョン情報	[バージョン情報] 画面を表示します

表 3-2.　メイン画面のメニュー項目

製品ライセンス

Mobile Security および暗号化モジュールのライセンスの種類に応じて、ライセンスの有効期限が切れた後で使用可能な機能が異なります。

Mobile Security がウイルスバスター Corp. サーバに登録されておらず、体験版のライセンスの有効期限が切れた場合は、モバイルデバイスで Mobile Security のすべての機能が無効になります。

Mobile Security の製品版ライセンスの有効期限が切れた場合は、ファイアウォールと不正プログラム検索機能を引き続き使用できます。ただし、不正プログラム検索には期限切れの不正プログラム対策コンポーネントが使用されるため、最新のセキュリティリスクを検出できない可能性があります。

モバイルデバイスの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は、暗号化モジュールが自動的にアンインストールされます。さらに、モバイルデバイスおよび装着されているメモリカードに保存されている暗号化されたデータが復号化されます。

[バージョン情報] 画面

製品ライセンス情報を表示するには、[メニュー]→[バージョン情報] の順にクリックして [バージョン情報] 画面を表示します。標準ライセンスと暗号化ライセンスの終了日を確認できます。

標準 (製品版) ライセンスは、Mobile Security の不正プログラム対策機能とファイアウォール機能を対象としています。暗号化ライセンスは、ログオン認証とデータ暗号化のための暗号化モジュールを利用可能にします。

初期設定の保護ポリシーを確認する

Mobile Security をインストールすると、モバイル不正プログラムやその他の脅威からモバイルデバイスを保護できるようになります。

注意： ネットワーク管理者が、お使いのモバイルデバイス上での Mobile Security ポリシーの変更を禁じている場合があります。
ウイルスバスター Corp. サーバが、お使いのモバイルデバイスの SMS スパムメール対策機能および WAP プッシュ保護機能を制御している場合があります。

表 3-3 に表示されている初期設定の保護ポリシーを確認し、変更が必要かどうかを判断します。

機能	初期設定のポリシー	実行される処理
リアルタイム検索サービス	有効	アクセス中のファイルを検索します。
リアルタイム処理	隔離	感染ファイルまたは疑わしいファイルを暗号化し、移動します。
カード検索	無効	メモリカードの挿入時に、カードの自動検索を実行しません。
検索するファイルタイプ	すべて	不正プログラムがないかすべてのファイルを検索します。
検索する CAB/ZIP 階層	3 (最大)	不正プログラムを検索する前に、最大で 3 圧縮階層まで圧縮ファイル (CAB/ZIP) を展開します。ファイルが 4 階層以上圧縮されている場合は、ファイルは検索不能と見なされます。
ワイヤレス接続の警告	有効	GPRS またはその他のワイヤレス接続を開いてインターネットにアクセスする前に、確認メッセージを表示します。

表 3-3.　初期設定の保護ポリシー

機能	初期設定のポリシー	実行される処理
自動アップデート	有効	自動的にアップデートを確認、ダウンロード、およびインストールします。
アップデート間隔	8 時間	前回のアップデートの確認から 8 時間後にアップデートを確認します。
指定期間後に強制的にアップデート	30 日	30 日ごとにアップデートを実行します。その際、必要に応じてワイヤレス接続を開きます。このアップデートは、他のアップデートの実行に関係なく、30 日ごとに実行されます。
ファイアウォール	有効	ネットワークの送受信トラフィックをフィルタリングします。初期設定のファイアウォールルールについては、57 ページの「ファイアウォールルール」を参照してください。
IDS (侵入検知システム)	有効	DoS 攻撃から保護します。
ファイアウォールの保護レベル	中	ファイアウォールにより、すべての送信トラフィックが許可され、すべての受信トラフィックがブロックされます。Mobile Security には、事前定義のファイアウォールルールが用意されています。このルールは選択した保護レベルより優先されます。
SMS スパムメール対策	無効	SMS メッセージをフィルタせず、すべてのメッセージがメッセージ受信ボックスで受信されることを許可します。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	無効	WAP プッシュメッセージをフィルタせず、すべてのメッセージのモバイルデバイスでの受信を許可します。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。

表 3-3.　初期設定の保護ポリシー (続き)

不正プログラム対策コンポーネントをアップデートする

モバイル不正プログラムに対する最新の保護を確保するために、インストール後に Mobile Security をアップデートします。

Mobile Security をアップデートするには

1. モバイルデバイスがウイルスバスター Corp. サーバに接続できることを確認します。
2. メイン画面で、[アップデート] を選択します。[アップデート] 画面にコンポーネントのバージョンが表示されます。バーはアップデートのステータスを示しています。アップデートをキャンセルするには、[キャンセル] を選択します。

注意： 製品のアップデートの詳細については、41 ページの「不正プログラム対策コンポーネントのアップデート」を参照してください。
モバイルデバイスがウイルスバスター Corp. サーバに登録されていない場合は、アップデート機能は無効です。

不正プログラムを検索する

モバイルデバイスの不正プログラムをすばやく確認するには、メイン画面で [メニュー]→[検索] の順に選択します。検出されたファイルや検索不能なファイルを削除または隔離できます。

モバイルデバイスで不正プログラムが検出された場合は、セキュリティリスクログが生成されてウイルスバスター Corp. サーバに送信されます。モバイルデバイスのウイルスバスター Corp. サーバへの接続の許可を求めるプロンプトが画面に表示される場合があります。

注意： Mobile Security の不正プログラム対策機能の詳細については、45 ページの「不正プログラムの検索」を参照してください。

第 4 章

不正プログラム対策コンポーネントのアップデート

最新のモバイル不正プログラムに対する保護を維持するには、不正プログラム対策コンポーネントを定期的にアップデートします。

この章は次のトピックで構成されています。

ウイルスバスター Corp. サーバに接続する

Trend Micro Mobile Security (以下、Mobile Security) のコンポーネントをアップデートするには、モバイルデバイスがウイルスバスター Corp. サーバに接続している必要があります。必要に応じて、[登録] 画面にウイルスバスター Corp. サーバの IP アドレスとポート番号を入力します (22 ページの「手動登録」を参照してください)。

アップデートの種類

コンポーネントを自動的にアップデートしたり、手動でアップデートするように Mobile Security を設定できます。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。モバイル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 4-1.　アップデートの種類

自動アップデートと強制アップデート

自動アップデートは、指定した間隔で実行されます。この間隔を設定するには、[アップデートオプション] 画面にアクセスします。

自動アップデートと強制アップデートの間隔を設定するには

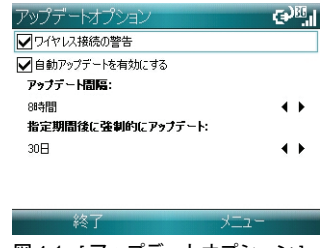


図 4-1. [アップデートオプション] 画面

1. [メニュー]→[オプション]→[アップデートオプション] の順に選択します。図 4-1 に示すように、[アップデートオプション] 画面が表示されます。
2. [アップデートオプション] 画面で、[自動アップデートを有効にする] が選択されていることを確認します。
3. [アップデート間隔] で適切な間隔を選択します。前回アップデートを確認した時点からこの間隔が経過すると、アップデートが確認されます。モバイルデバイスがインターネットに接続している場合にのみ、このアップデートは実行されます。
4. [指定期間後に強制的にアップデート] で、強制アップデートの間隔を選択します。他のアップデートが実行されたかどうかにかかわらず、この間隔で初期設定のインターネット接続が開かれ、アップデートが確認されます。
5. [終了] を選択します。

注意： 強制アップデート中、GPRS、CDMA2000、またはその他のワイヤレス接続が開かれる可能性があります。ワイヤレス接続を開く前にメッセージを表示する場合は、[アップデートオプション] 画面で [ワイヤレス接続の警告] を選択します。

手動アップデート

手動アップデートを実行するには

1. モバイルデバイスが TMMS 管理サーバに接続可能なこと、もしくはインターネットに接続されていることを確認します。
2. メインメニューの [アップデート] を選択します。[アップデート] 画面にコンポーネントのバージョンが表示されます。バーはアップデートのステータスを示しています。アップデートをキャンセルするには、[キャンセル] を選択します。

注意： プログラムコンポーネントのアップデート後すぐに手動検索を実行することを強くお勧めします。手動検索の実行の詳細については、46 ページの「手動検索」を参照してください。

第 5 章

不正プログラムの検索

Trend Micro Mobile Security (以下、Mobile Security) では、モバイル不正プログラムがないかモバイルデバイスが検索されます。この章では、Mobile Security の不正プログラム対策機能について説明します。

この章は次のトピックで構成されています。

不正プログラム検索の種類

Mobile Security に用意されている不正プログラム検索の種類は次のとおりです。

検索の種類	説明
手動検索	手動で、ユーザが開始する検索
リアルタイム検索	アクセス中のファイルの自動検索
カード検索	メモリカード挿入時に実行されるカードの自動検索

表 5-1.　不正プログラム検索の種類

手動検索

手動検索では、モバイルデバイス上のすべてのファイルについて、不正プログラムがないか検索されます。手動検索を実行するには、メイン画面で [メニュー]→[検索] の順に選択します。

検索結果の画面に、感染ファイルまたは疑わしいファイルと検索不能ファイルのリストが表示されます。これらのファイルは削除または隔離できます。詳細については、50 ページの「感染または疑わしいファイルや検索不能ファイルを処理する」を参照してください。

リアルタイム検索

リアルタイム検索サービスにより、ユーザやモバイルデバイス上のアプリケーションがファイルにアクセスする際にそのファイルが検索されます。この検索により、モバイルデバイスのユーザが不正プログラムを誤って実行することを防止できます。

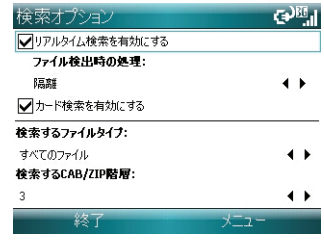


図 5-1. [検索オプション] 画面

リアルタイム検索を有効にする

リアルタイム検索を有効にすると、モバイルデバイスの不正プログラム保護が強化されます。

リアルタイム検索を有効にするには

1. メイン画面で [メニュー]→[オプション]→[検索オプション] の順に選択します。図 5-1 に示すように、[検索オプション] 画面が表示されます。
2. [リアルタイム検索を有効にする] を選択します。
3. [終了] を選択します。

注意： リアルタイム検索サービスを無効にするには、[検索オプション] 画面で [リアルタイム検索を有効にする] をクリアします。リアルタイム検索サービスを無効にすると、事前予防がモバイルデバイスで使用できなくなります。

ファイル検出時の処理を設定する

初期設定では、リアルタイム検索で検出されたファイルは、自動的に隔離、つまり暗号化され移動されます。ただし、検出されたファイルを自動的に削除するように、リアルタイム検索を設定することもできます。

[検索オプション] 画面の [ファイル検出時の処理] で、適切なリアルタイム処理を選択します。

カード検索

カード検索機能は、初期設定では無効です。メモリカードに不正プログラムがないか自動的に確認するには、カード検索を有効にします。カード検索が有効な場合にメモリカードがモバイルデバイスに挿入されると、不正プログラムの検索が自動的に開始されます。

カード検索を有効にするには

1. メイン画面で [メニュー]→[オプション]→[検索オプション] の順に選択します。
2. [カード検索を有効にする] を選択します。
3. [終了] を選択します。

検索結果

Mobile Security では、カード検索および手動検索の結果を表示して、ユーザが検出されたファイルや検索不能ファイルごとに処理を指定できるようにします。

検索結果を表示する

手動検索またはカード検索後、図 5-2 に示すように、感染ファイルまたは疑わしいファイルと検索不能ファイルのリストが表示されます。これらのファイルは削除または隔離できます。

表 5-2 に示すとおり、検索結果項目は、感染または疑わしいファイルか検索不能ファイルのどちらかになります。

図 5-2. 検索結果の画面

検索結果項目	説明
疑わしいファイル	不正プログラムが含まれていることが検出されたファイル
検索不能ファイル	アクセス不能なアーカイブに圧縮されたファイル。このようなファイルには、圧縮階層が多すぎる圧縮ファイル、パスワードで保護されている圧縮ファイル、またはモバイルデバイス上で展開するには大きすぎるファイルなどがあります。

表 5-2. 検索結果項目

疑わしいファイルまたは検索不能ファイルの詳細を表示するには、目的のファイルを選択し、処理ボタンを押します。

ヒント： 検索する圧縮階層数の設定の詳細については、51 ページの「不正プログラム対策ポリシーの詳細設定」を参照してください。

感染または疑わしいファイルや検索不能ファイルを処理する

疑わしいファイルや検索不能ファイルを隔離または削除せずに検索結果の画面を終了すると、これらのファイルはモバイルデバイスに残り、他のファイルを損傷したり、モバイルデバイスの動作に影響を与えます。

感染または疑わしいファイルや検索不能ファイルを削除するには

1. 検索結果の画面で、疑わしいファイルまたは検索不能ファイルを選択します。
2. メニューで、次の処理のいずれかを選択します。
   - **削除** — 感染または疑わしいファイルや検索不能ファイルをモバイルデバイスから恒久的に削除します。
   - **隔離** — 感染または疑わしいファイルや検索不能ファイルを暗号化して隔離フォルダに移動します。

注意： 感染または疑わしいファイルや検索不能ファイルをすべて隔離または削除するには、[すべて削除] または [すべて隔離] を選択します。

隔離ファイル

[隔離リスト] 画面で隔離ファイルにアクセスできます。このリストには、リアルタイム検索中に自動的に隔離されたファイルや、手動検索やカード検索後に手動で隔離したファイルが含まれています。

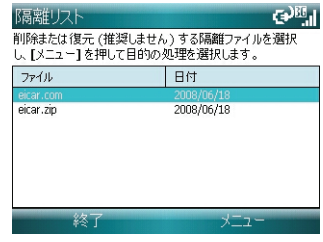


図 5-3. [隔離リスト] 画面

リストを開くには、メイン画面で [メニュー]→[隔離リスト] の順に選択します。図 5-3 に、[隔離リスト] 画面を示します。

通常のファイルのように隔離ファイルにアクセスするには、隔離ファイルを元の状態に復元します。隔離ファイルを復元すると、モバイルデバイスが有害なファイルにさらされる可能性があります。

ファイルを隔離から復元するには

1. [隔離リスト] 画面で、復元するファイルを選択します。
2. [メニュー]→[復元] の順に選択します。

注意： 感染ファイルまたは疑わしいファイルは、復元後に開かないでください。

不正プログラム対策ポリシーの詳細設定

検索するファイルタイプを選択できます。圧縮ファイルの場合は、圧縮ファイルが検索不能と見なされるまでにサポートされる圧縮階層数の上限 (最大で 3) を指定できます。

検索するファイルタイプ

Mobile Security では、すべてのファイル、実行可能ファイルと圧縮ファイル、または実行可能ファイルのみの検索が可能です。

オプション	説明
すべてのファイル	ROM に保存された OS ファイルを除く、モバイルデバイス上のすべてのファイル
実行可能ファイルおよび ZIP/CAB ファイル	.EXE および .DLL の拡張子を持つファイルと .ZIP および .CAB フォーマットの圧縮ファイル。.CAB ファイルは、一般的にアプリケーションのインストールに使用されます。
実行可能ファイルのみ	.EXE および .DLL の拡張子を持つファイル

表 5-3.　検索するファイルタイプのオプション

検索する圧縮階層数

圧縮ファイルを検索する場合は、まず、ファイルが展開されます。そのため、圧縮ファイルの検索には、余分の時間とリソースが必要になります。

ファイルを展開するように設定できるのは、圧縮階層が 3 つまでのファイルです。ファイルが設定より多い階層で圧縮されている場合は、そのファイルは検索不能と見なされます。

圧縮階層の数を決定する前に、次のことを考慮してください。

- 複数の圧縮階層のファイルを誤って開くことはまずありません。
- 意図的に複数の圧縮階層のファイルを準備するかまたは使用するのでないかぎり、そのようなファイルの大半は、不正プログラム対策の検索を避けるために準備されたものと考えられます。圧縮階層数の上限に低い値を選択した場合は、これらのファイルは検索されませんが、検索不能というタグが付き、削除または隔離できるようになります。

検索ポリシーの詳細を設定する

[検索オプション] 画面で、検索するファイルタイプや圧縮階層数など、検索ポリシーの詳細を設定します。

検索ポリシーの詳細を設定するには

1. メインメニューから [メニュー]→[オプション]→[検索オプション] の順に選択します。
2. [検索するファイルタイプ] で、不正プログラムを検索するファイルタイプを選択します。ファイルタイプオプションの詳細については、表 5-3 を参照してください。
3. [すべてのファイル] または [実行可能ファイルおよび CAB/ZIP ファイル] を選択した場合は、[検索する CAB/ZIP 階層] で、CAB ファイルと ZIP ファイルの階層数を選択します。
4. [終了] を選択します。

注意： 項目 [ファイル検出時の処理] は、リアルタイム検索にのみ適用されます。48 ページの「ファイル検出時の処理を設定する」を参照してください。

モバイル不正プログラム情報

既知のモバイル不正プログラムの情報を表示するには、メイン画面で [メニュー]→[不正プログラムの定義] の順に選択します。図 5-4 に示すように、[不正プログラムの定義] 画面が表示されます。

不正プログラムの詳細を追加で表示するには、目的の不正プログラムを選択し、[表示] を選択します。

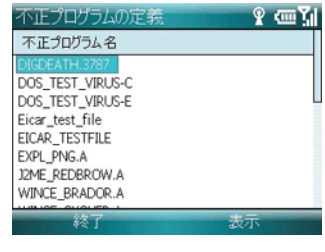


図 5-4. [不正プログラムの定義] 画面

第 6 章

不正侵入への対策

Trend Micro Mobile Security (以下、Mobile Security) のファイアウォールを使用すると、ネットワークの送受信トラフィックをフィルタできます。この章では、ファイアウォールでモバイルデバイスを保護する方法について説明します。

この章は次のトピックで構成されています。

ファイアウォールについて

ファイアウォールはネットワーク接続されたコンピュータおよびモバイルデバイスのポートへのアクセスを制御します。Mobile Security のファイアウォールを使用すると、外部アプリケーションがモバイルデバイスへの接続に使用できるポートを制御できます。また、モバイルデバイス上で動作するアプリケーションが外部システムへの接続に使用できるポートも制御できます。ポートへのアクセスの制御に加え、モバイルデバイスに接続可能な IP アドレスおよびモバイルデバイスから接続可能なアドレスも制御できます。

ファイアウォールは、モバイルデバイス上で動作する外部システムやアプリケーションによって開始された不要な接続を防止することにより、ネットワークに接続されたモバイルデバイスのセキュリティを高めます。たとえば、ハッカーが特に脆弱なポートからモバイルデバイスにアクセスするのを防ぐため、そのポートをブロックできます。

注意： ポートは、通常、特定のアプリケーションやサービスに関連付けられています。詳細については、57 ページの「ファイアウォールルール」を参照してください。

Mobile Security のファイアウォールによるフィルタについて

Mobile Security のファイアウォールには、次の 2 つのフィルタ方法が用意されています。

- 事前定義の保護レベル
- ファイアウォールルール

注意： 事前定義の保護レベルとファイアウォールルールに加え、Mobile Security では、ファイアウォールポリシーをバックグラウンドに実装することにより、基本のネットワーク通信、ActiveSync 通信、およびコンポーネントのアップデートが影響を受けないようにしています。

事前定義の保護レベル

事前定義の保護レベル (表 6-1 を参照) を使用すると、ファイアウォールをすばやく設定できます。各レベルは、Mobile Security で受信および送信接続を処理する一般的なルールに対応しています。

保護レベル	モード	説明
低	オープン	すべての送受信トラフィックが許可されます。
中	ステルス	すべての送信トラフィックが許可され、すべての受信トラフィックがブロックされます。
高	ロック	すべての送受信トラフィックがブロックされます。

表 6-1. 事前定義の保護レベル

注意： ファイアウォールルールは事前定義の保護レベルに優先するので、保護レベルの調整で変更されるのは、ファイアウォールルールの対象外であるネットワーク通信の処理方法のみです。

ファイアウォールルール

ファイアウォールルールでは、特定のポートおよび IP アドレスの保護ポリシーを定義します。このルールは、事前定義の保護レベルよりも優先されます。図 6-1 に示すように、[ファイアウォールルールリスト] 画面に現在のファイアウォールルールが一覧表示されます。

Mobile Security には、Web の参照やメールなどの機能に使用される共通ポートを対象とする初期設定のファイアウォールルールセットが用意されています。表 6-2 に、初期設定のファイアウォールルールを示します。

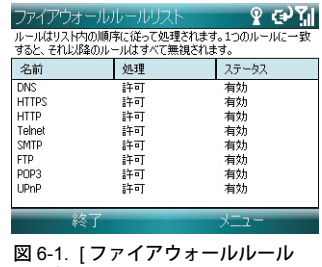


図 6-1. [ファイアウォールルールリスト] 画面

ルール	ポート	一般的な使用方法	初期設定のファイアウォールポリシー
DNS	53	ドメイン名の解決	このポートを経由するすべての送受信トラフィックが許可されます
HTTPS	443	セキュアな Web 参照	このポートを経由するすべての送受信トラフィックが許可されます
HTTP	80	Web 参照	このポートを経由するすべての送受信トラフィックが許可されます
Telnet	23	サーバ通信	このポートを経由するすべての送受信トラフィックが許可されます
SMTP	25	メール	このポートを経由するすべての送受信トラフィックが許可されます
FTP	21	ファイル転送	このポートを経由するすべての送受信トラフィックが許可されます
POP3	110	メール	このポートを経由するすべての送受信トラフィックが許可されます
UPnP	1900	ネットワーク接続性	このポートを経由するすべての受信トラフィックが許可されます

表 6-2.　初期設定のファイアウォールルール

ヒント：初期設定のファイアウォールルールを変更したり、独自のルールを作成することができます。詳細については、61 ページの「ファイアウォールポリシーの詳細設定」を参照してください。

ファイアウォールを有効にする

ネットワークに接続するたびにファイアウォールで保護されるようにするには、ファイアウォールを有効にします。

ファイアウォールを有効にするには

1. メイン画面で [メニュー]→[オプション]→[ファイアウォールオプション] の順に選択します。図 6-2 に示すように、[ファイアウォールオプション] 画面が表示されます。
2. [ファイアウォールを有効にする] を選択します。
3. [終了] を選択します。

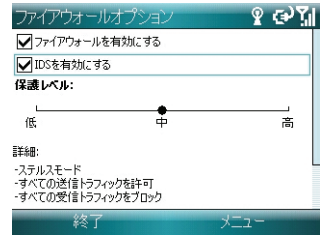


図 6-2. [ファイアウォールオプション] 画面

ファイアウォールの保護レベルを設定する

事前定義の保護レベルにより、Mobile Security のファイアウォールをすばやく設定できます。

ヒント： 事前定義の保護レベルの詳細については、57 ページの「事前定義の保護レベル」を参照してください。

ファイアウォールの保護レベルを設定するには

1. メイン画面で [メニュー]→[オプション]→[ファイアウォールオプション] の順に選択します。
2. [ファイアウォールを有効にする] が選択されていることを確認します。
3. [保護レベル] で、適切な保護レベルを選択します。
4. [終了] を選択します。

ヒント： メイン画面でファイアウォールの保護レベルを選択することもできます。

ファイアウォールポリシーの詳細設定

事前定義の保護レベルと初期設定のルールに加え、独自のルールを作成し、侵入検知を有効にしてファイアウォールによる保護を強化できます。

ファイアウォールルールを作成する

ファイアウォールルールでは、選択した保護レベルにカスタムのフィルタポリシーが追加されます。このルールを使用すると、特定のポート、ポート範囲、特定の IP アドレス、および IP アドレスの範囲に対する処理を設定できます。たとえば、特定のコンピュータの IP アドレスを設定し、モバイルデバイスとそのコンピュータ間のすべてのトラフィックを許可することができます。

ファイアウォールルールを作成するには

1. メイン画面で [メニュー]→[オプション]→[ファイアウォールオプション] の順に選択します。
2. [ファイアウォールを有効にする] が選択されていることを確認します。
3. [メニュー]→[ルールリストの設定] の順に選択します。[ファイアウォールルールリスト] 画面が表示されます。
4. [メニュー]→[新規ルール] の順に選択します。図 6-3 に示すように、[ルールの詳細] 画面が表示されます。

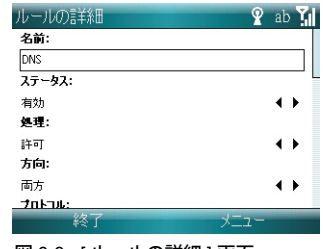


図 6-3. [ルールの詳細] 画面

注意： 新規ルールに既存のルールと類似する特徴が多数ある場合は、既存のルールを選択し、[メニュー]→[複製] の順に選択して、次に、複製されたルールを適宜変更できます。

5. ルールに一意の名前を付けます。

6. [ルールの詳細] 画面で該当する詳細を設定します。この画面の項目の詳細については、表 6-3 を参照してください。

項目	オプション	定義
ステータス	有効 無効	ルールのオンとオフを切り替えます。
処理	拒否 許可 ログのみ	ルールに一致する接続の試行を許可、拒否、またはログのみにするかを決定します。
方向	受信 送信 両方	このルールを受信、送信、または送受信のいずれの接続に適用するかを決定します。
プロトコル	すべて TCP/UDP TCP UDP ICMP	このルールを適用するネットワークプロトコルを決定します。
ポート	すべてのポート ポート範囲 特定のポート	アクセスを許可または拒否するモバイルデバイス (受信接続用) またはリモートシステム (送信接続用) のポートを決定します。すべてのネットワークポート、ポート範囲、または 32 個までの特定のポートについて、アクセスを許可または拒否できます。 ポートを指定する場合は、各ポートをカンマで区切ります。 注意： [プロトコル] で ICMP が選択されている場合は、ポートを指定できません。

表 6-3. [ルールの詳細] 画面の項目

項目	オプション	定義
IP アドレス	すべての IP アドレス 単一 IP IP アドレスの範囲 サブネット	アクセスを許可または拒否する IP アドレスを決定します。すべての IP アドレス、特定の IP アドレス、IP アドレスの範囲、またはサブネットに対して、アクセスを許可または拒否できます。 注意： ルールをサブネットに適用するには、ホストまたはネットワークの IP アドレスとサブネットマスクを指定する必要があります。

表 6-3. [ルールの詳細] 画面の項目 (続き)

7. [終了] を選択します。

ファイアウォールルールのリスト順序を設定する

複数のファイアウォールルールが同じポートまたは同じ IP アドレスに指定されている場合、重複する可能性があります。重複すると、リストの一番上のルールがそれよりも下のルールより優先されます。

ルールをリスト内で上下に移動するには

1. メイン画面で [メニュー]→[オプション]→[ファイアウォールオプション] の順に選択します。
2. [ファイアウォールを有効にする] が選択されていることを確認します。
3. [メニュー]→[ルールリストの設定] の順に選択します。[ファイアウォールルールリスト] 画面が表示されます。
4. ルールを選択し、次に [メニュー]→[移動] の順に選択します。図 6-4 に示すように、[ルールの移動] 画面が表示されます。
5. 適切な位置を選択します。
6. [終了] を選択します。

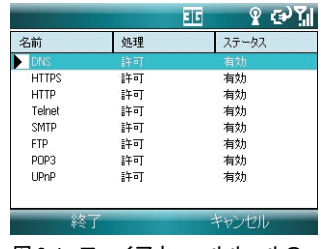


図 6-4. ファイアウォールルールの移動

注意： 複数のポートおよび複数の IP アドレスを対象とするルールは作成しないでください。特定のポートや特定の IP アドレスを対象とするファイアウォールルールの方が管理しやすく、重複する可能性も少なくなります。

ファイアウォールルールを削除する

ルールリストが雑然とならないように、不要なルールを削除します。

ファイアウォールルールを削除するには

1. メイン画面で [メニュー]→[オプション]→[ファイアウォールオプション] の順に選択します。
2. [ファイアウォールを有効にする] が選択されていることを確認します。
3. [メニュー]→[ルールリストの設定] の順に選択します。[ファイアウォールルールリスト] 画面が表示されます。
4. ルールを選択し、次に [メニュー]→[削除] の順に選択します。確認プロンプトが表示されます。
5. 確認プロンプトで [はい] を選択します。

注意： ファイアウォールルールを削除せずに無効にするには、[ルールの詳細] 画面でルールを開き、[無効] を選択します。

侵入検知を有効にする

IDS (侵入検知システム) は、Mobile Security のファイアウォールに組み込まれています。IDS を使用すると、モバイルデバイスに複数のパケットを連続的に送信しようとする外部ソースによる試行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。

侵入検知を有効にするには

1. メイン画面で [メニュー]→[オプション]→[ファイアウォールオプション] の順に選択します。
2. [IDS を有効にする] を選択します。
3. [終了] を選択します。

注意： IDS は SYN フラッド攻撃のみをブロックします。

第 7 章

SMS メッセージのフィルタリング

電話機能を備えたモバイルデバイスで Trend Micro Mobile Security (以下、Mobile Security) を使用すると、不要な SMS メッセージをフィルタしてスパムメールフォルダに移動できます。この章では、SMS メッセージフィルタの設定方法について説明します。

この章は次のトピックで構成されています。

SMS スパムメール対策フィルタの種類

SMS メッセージをフィルタするのに、次のフィルタリストのいずれかを使用できます。

- **除外リスト** — 有効にすると、このリストにある番号からのメッセージを除くすべてのメッセージがブロックされます。
- **ブロックリスト** — 有効にすると、このリストにある番号からのメッセージを除くすべてのメッセージが許可されます。

注意： Mobile Security は、ブロックされた SMS メッセージをすべて受信ボックスのスパムメールフォルダに移動します。詳細については、74 ページの「ブロックされた SMS メッセージを処理する」を参照してください。

SMS スパムメール対策の設定

スパムメール対策ポリシーを設定するには、メイン画面で [メニュー]→[オプション]→[SMS スパムメール対策] の順に選択します。図 7-1 に示すように、[SMS スパムメール対策] 画面が表示されます。

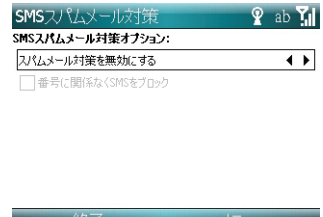


図 7-1. [SMS スパムメール対策] 画面

SMS スパムメール対策フィルタを有効にする

不要な SMS メッセージをフィルタするには、除外リストまたはブロックリストのどちらかを有効にします。

- 既知の番号のリストからのみメッセージを受信する場合は、除外リストを有効にします。
- 特定のユーザからのメッセージをブロックし、その他すべてのメッセージを許可する場合は、ブロックリストを有効にします。

スパムメール対策フィルタリストを有効にするには

1. メイン画面で [メニュー]→[オプション]→[SMS スパムメール対策] の順に選択します。
2. [SMS スパムメール対策オプション] で、[除外リストを有効にする] または [ブロックリストを有効にする] のいずれかを選択します。

スパムメール対策リストに送信者を追加する

送信者をスパムメール対策リストに追加するには、次の 2 つの方法があります。

- 送信者の詳細を手動で入力
- モバイルデバイスの連絡先リストから送信者をインポート

送信者の詳細を手動で入力するには

1. メイン画面で [メニュー]→[オプション]→[SMS スパムメール対策] の順に選択します。
2. スパムメール対策リストが有効であることを確認します。
3. [メニュー]→[除外リスト]/[ブロックリストの設定] の順に選択します。

   図 7-2 に示すように、現在のリストエントリが表示されます。
4. [メニュー]→[追加] の順に選択します。

   図 7-3 に示すように、[送信者の追加] 画面が表示されます。
5. 送信者の名前と電話番号を入力します。
6. [終了] を選択し、送信者リストに戻ります。エントリがリストに表示されます。
7. [終了] を選択して変更を保存し、[SMS スパムメール対策] 画面に戻ります。

図 7-2. SMS スパムメール対策 ブロックリスト

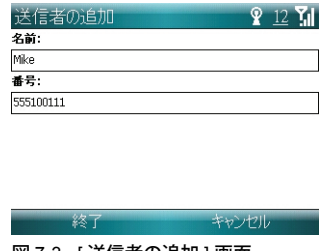


図 7-3. [送信者の追加] 画面

モバイルデバイスの連絡先リストから送信者をインポートするには

1. メイン画面で [メニュー]→[オプション]→[SMS スパムメール対策] の順に選択します。
2. スパムメール対策リストが有効であることを確認します。

3. [メニュー]→[除外リスト]/[ブロックリストの設定] の順に選択します。

   図 7-4 に示すように、現在のリストエントリが表示されます。

4. [メニュー]→[インポート] の順に選択します。

   図 7-5 に示すように、[インポートウィザード] 画面が表示されます。

5. [番号が存在する場合] で、次のオプションのいずれかを選択します。

   - **要求** — 番号がすでにスパムメール対策フィルタリストに存在することを通知します。ユーザはその番号に対する処理を指定できます。
   - **置換** — 現在スパムメール対策フィルタリストにあるエントリを置換します。
   - **無視** — 元のエントリを保持し、新しい番号を無視します。

6. [電話の種類] で、インポートする番号を選択します。図 7-5。

7. [次へ] を選択します。
   図 7-6 に示すように、一致するすべての連絡先が一覧表示されます。

8. [連絡先の選択] でインポートする連絡先を選択して、[インポート] を選択します。

9. 連絡先がインポートされたことを確認します。図 7-6。

10. [終了] を選択して変更を保存し、[SMS スパムメール対策] 画面に戻ります。

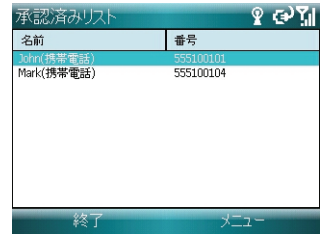


図 7-4. SMS スパムメール対策除外リスト

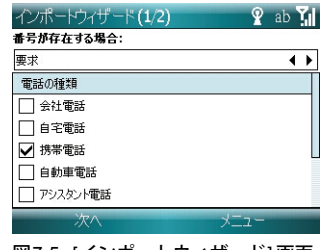


図7-5. [インポートウィザード] 画面 (1/2)

図7-6. [インポートウィザード] 画面 (2/2)

スパムメール対策リストを編集する

送信者の名前または番号を変更するには、スパムメール対策リストに一覧表示されている送信者を編集します。

送信者情報を編集するには

1. メイン画面で [メニュー]→[オプション]→[SMS スパムメール対策] の順に選択します。
2. [メニュー]→[除外リスト]/[ブロックリストの設定] の順に選択します。現在のエントリがリストに表示されます。
3. 送信者の名前を選択します。
4. [メニュー]→[編集] の順に選択します。[送信者の編集] 画面が開きます。
5. 送信者情報を変更し、[終了] を選択します。
6. 再度 [終了] を選択して変更を保存し、[SMS スパムメール対策] 画面に戻ります。

スパムメール対策リストから送信者を削除する

スパムメール対策フィルタリストから送信者を削除する前に、除外リストまたはブロックリストを有効にしたかどうかを確認します。

- 除外リストを有効にした状態で、送信者をスパムメール対策フィルタリストから削除すると、その送信者からの SMS メッセージはブロックされます。
- ブロックリストを有効にした状態で、送信者をスパムメール対策フィルタリストから削除すると、その送信者からの SMS メッセージは許可されます。

送信者を削除するには

1. メイン画面で [メニュー]→[オプション]→[SMS スパムメール対策] の順に選択します。
2. [メニュー]→[除外リスト]/[ブロックリストの設定] の順に選択します。現在のエントリがリストに表示されます。

3. 送信者の名前を選択します。
4. [メニュー]→[削除] の順に選択します。
5. 確認プロンプトが表示されます。[はい] を選択します。
6. [終了] を選択して変更を保存し、[SMS スパムメール対策] 画面に戻ります。

ヒント： 全送信者を削除するには、リストの任意のセクションをタップアンドホールドして、[すべて選択] を選択し、次に [削除] をタップします。

識別されていない送信者からの SMS メッセージをブロックする

ブロックリストが有効な場合は、送信者番号情報がない SMS メッセージをブロックできます。

識別されていない送信者からのメッセージをブロックするには

1. メイン画面で [メニュー]→[オプション]→[SMS スパムメール対策] の順に選択します。
2. [ブロックリストを有効にする] が選択されていることを確認します。
3. 図 7-7 に示すように、[番号に関係なく SMS をブロック] を選択します。
4. [終了] を選択します。

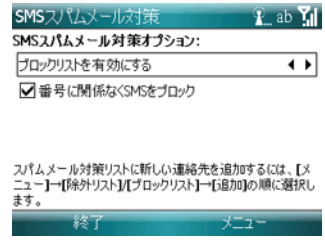


図 7-7. [SMS スパムメール対策] 画面

注意： 送信者番号情報のない SMS メッセージをブロックすると、必要なメッセージが除外される可能性があります。スパムメールフォルダを定期的にチェックし、現在の SMS スパムメール対策ポリシーで、受信する必要のあるメッセージがブロックされていないことを確認します。74 ページの「ブロックされた SMS メッセージを処理する」を参照してください。

SMS スパムメール対策フィルタを無効にする

すべての SMS メッセージを受信ボックスで受信するには、SMS フィルタを無効にします。

SMS フィルタをすべて無効にするには

1. メイン画面で [メニュー]→[オプション]→[SMS スパムメール対策] の順に選択します。
2. [SMS スパムメール対策オプション] で、[スパムメール対策を無効にする] を選択します。
3. [終了] を選択します。

ブロックされた SMS メッセージを処理する

ブロックされた SMS メッセージは、メッセージ受信ボックスのスパムメールフォルダに移動されます。これらのメッセージは、受信ボックスフォルダ内のメッセージと同様に処理できます。

スパムメールフォルダにアクセスするには、受信ボックスフォルダにアクセスする際に [Folder] ビューを選択します。

第 8 章

WAP プッシュメッセージのフィルタリング

WAP プッシュメッセージにより、不要な WAP プッシュコンテンツのモバイルデバイスへの配信が開始される可能性があります。この章では、Trend Micro Mobile Security (以下、Mobile Security) を使用して、不要な WAP プッシュメッセージをブロックする方法について説明します。

この章は次のトピックで構成されています。

WAP プッシュメッセージについて

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。着信メロディ、ニュース、メール、およびデバイスポリシーなど、モバイルに関連するコンテンツの配信に使用されます。コンテンツをモバイルデバイスに配信する機能を備えていることから、WAP プッシュにより、不正プログラムや広告などの未承諾のコンテンツや不要なコンテンツが配信される可能性があります。

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 SMS メッセージがユーザに送信されます。このメッセージは、通常、モバイルデバイスで受信されると同時に警告を表示します。この警告で、WAP サイトに直接接続するか、コンテンツをモバイルデバイスにダウンロードするかを選択できます。

不正なユーザは、誤った情報や役に立たない情報を入れた WAP プッシュメッセージを送信し、ユーザをだまして不要なコンテンツを許可させることが知られています。不明な送信者からの WAP プッシュメッセージをブロックすることにより、不要な WAP プッシュコンテンツを誤ってダウンロードしたりインストールするのを防ぐことができます。

WAP プッシュ保護を有効にする

WAP プッシュ保護を使用すると、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できます。

WAP プッシュ保護を有効にするには

1. メイン画面で [メニュー]→[オプション]→[WAP プッシュ保護] の順に選択します。図 8-1 に示すように、[WAP プッシュ保護] 画面が表示されます。
2. [保護を有効にする] を選択します。
3. [終了] を選択します。

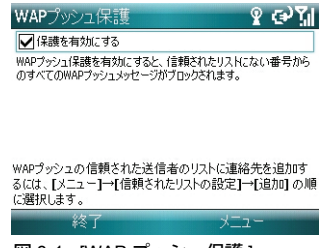


図 8-1. [WAP プッシュ保護] オプション画面

WAP プッシュの信頼された送信者のリストの管理

信頼された送信者のリストに記載されている送信者からのメッセージは、自動的に許可されます。不明な送信者からの WAP プッシュメッセージを受信すると、メッセージの許可またはブロックを確認するプロンプトが表示されます。

信頼された WAP プッシュ送信者を追加する

同じ番号から WAP プッシュメッセージを頻繁に受信する場合は、その番号を信頼された送信者のリストに追加します。

送信者を信頼された送信者のリストに追加するには

1. メイン画面で [メニュー]→[オプション]→[WAP プッシュ保護] の順に選択します。

2. [保護を有効にする] が選択されていることを確認します。
3. [メニュー]→[信頼されたリストの設定] の順に選択します。

   図 8-2 に示すように、現在のエントリを示す信頼されたリストが表示されます。
4. [追加] を選択します。[送信者の追加] 画面が表示されます。
5. 送信者の名前と電話番号を入力します。
6. [終了] を選択します。

図 8-2. [信頼された送信者のリスト] 画面

信頼された WAP プッシュ送信者に関する情報を変更する

信頼された送信者の情報を編集するには

1. メイン画面で [メニュー]→[オプション]→[WAP プッシュ保護] の順に選択します。
2. [保護を有効にする] が選択されていることを確認します。
3. [メニュー]→[信頼されたリストの設定] の順に選択します。現在のエントリがリストに表示されます。
4. 編集するエントリを選択します。
5. [メニュー]→[編集] の順に選択します。[送信者の編集] 画面が開きます。
6. 送信者情報を変更し、[終了] を選択します。

信頼された WAP プッシュ送信者を削除する

信頼されたリストから送信者を削除するには

1. メイン画面で [メニュー]→[オプション]→[WAP プッシュ保護] の順に選択します。
2. [保護を有効にする] が選択されていることを確認します。
3. [メニュー]→[信頼されたリストの設定] の順に選択します。現在のエントリがリストに表示されます。
4. 送信者の名前を選択します。
5. [メニュー]→[削除] の順に選択します。

ヒント： 全送信者を削除するには、[すべて削除] を選択します。

6. 確認プロンプトが表示されます。[はい] を選択します。
7. [終了] を選択して変更を保存し、[WAP プッシュ保護] 画面に戻ります。

ブロックされた WAP プッシュメッセージを処理する

信頼されたリストに含まれていない送信者からの WAP プッシュメッセージを受信すると、警告が表示されます。

WAP プッシュメッセージをモバイルデバイスで受信しない場合は、[いいえ] を選択します。このブロックされたメッセージは、モバイルデバイスには保存されません。

ヒント： 不明な WAP プッシュメッセージの送信者を信頼されたリストに追加するには、WAP プッシュ警告メッセージで [信頼されたリストに追加] を選択し、[はい] を選択します。

第 9 章

トラブルシューティングとサポート情報

Trend Micro Mobile Security (以下、Mobile Security) の使用中に何らかの問題が発生する場合があります。この章では、一般的な問題とその回避策をリスト形式で記載すると共に、テクニカルサポートへの問い合わせ方法について説明します。

この章は次のトピックで構成されています。

トラブルシューティング

ここでは、Mobile Security のインストール、設定、および使用時に発生する可能性がある問題の対処方法について説明します。

問題	推奨処理
Mobile Security のインストール中にモバイルデバイスでバッテリ不良が発生しました。インストールプロセスが停止しました。	モバイルデバイスに適切な電源が供給されていることを確認し、インストールプロセスを再度実行します。
Mobile Security のアンインストール中にバッテリが故障しました。それ以降インストールを試みても、すべて失敗に終わりました。	アンインストールが完了していません。使用しているモバイルデバイスに適したツールを使用して、不完全な状態でインストールされているソフトウェアを削除します。
暗号化モジュールをモバイルデバイスにインストールできません。	まず、次のことを確認してください。 ・Mobile Security がウイルスバスター Corp. サーバに正常に登録されていること。 ・Mobile Security のライセンスに暗号化モジュールが含まれていること。この情報については、ネットワーク管理者にお問い合わせください。 ・Windows Mobile の組み込みのパスワードセキュリティ機能が無効になっていること。 ・サードパーティ製の暗号化ソフトウェアをモバイルデバイスからアンインストールしてあること。 ・暗号化モジュールでご使用のモバイルデバイスモデルがサポートされていること。 次に、モバイルデバイスに Mobile Security を再インストールします。

問題	推奨処理
Mobile Security がウイルスバスター Corp. サーバに正常に登録されましたが、モバイルデバイスで Mobile Security のポリシーを設定できません。	ネットワーク管理者が、Mobile Security のポリシーをモバイルデバイス上でカスタマイズするオプションを無効にしている可能性があります。詳細については、ネットワーク管理者にお問い合わせください。
隔離ファイルを開くことができません。	Mobile Security でファイルが隔離されると、ファイルが暗号化されます。隔離ファイルは復元できますが、この処理はお勧めしません。
Mobile Security の動作が遅くなっています。	モバイルデバイスのストレージ領域の空きを確認します。モバイルデバイスのメモリ上限に近づいている場合は、不要なファイルやアプリケーションを削除することを検討します。
モバイルデバイスがホストコンピュータに接続されているときに、アップデートを実行できません。	次のことを確認してください。 ・Mobile Security がウイルスバスター Corp. サーバに正常に登録されていること。 ・モバイルデバイスのプロキシ設定がホストコンピュータのプロキシ設定と同じであること。 ・ホストコンピュータがウイルスバスター Corp. サーバに接続できること。 ・Mobile Security コンポーネントのアップデートオプションがモバイルデバイスで有効になっていること。モバイルデバイス上で Mobile Security のポリシーを変更できない場合は、ネットワーク管理者にお問い合わせください。

問題	推奨処理
GPRS を使用したアップデートを実行できません。	次のことを確認してください。 ・Mobile Security がウイルスバスター Corp. サーバに正常に登録されていること。 ・モバイルデバイスが GPRS 接続を使用してインターネットに接続できること。ホストコンピュータに接続している場合は、モバイルデバイスで GPRS 接続を使用できない場合があります。詳細については、モバイルデバイスのマニュアルを参照してください。 ・ネットワーク管理者に問い合わせて、パブリックアクセス用にサーバが適切に設定されていることを確認します。
モバイルデバイスの連絡先リストから自分のスパムメール対策フィルタリストに連絡先をインポートできません。	インポートウィザードを再度実行し、インポートオプションが正しく設定されていることを確認します。インポートする電話の種類が、連絡先で使用されている電話の種類と一致していることを確認します。
Mobile Security のインストール後に、SMS メッセージを受信できません。	送信者の除外リストが有効になっているものの、リストが空である場合は、SMS メッセージはすべてブロックされ、スパムメールフォルダに移動されます。スパムメールフォルダとスパムメール対策ポリシーを確認します。
WAP プッシュメッセージの許可を選択しても、メッセージを受信できません。	モバイルデバイスで、WAP プッシュメッセージの受信をサポートしていない可能性があります。モバイルデバイスのマニュアルで、WAP プッシュメッセージの解析がモバイルデバイスでサポートされているかどうかを確認します。
ワイヤレス接続を開くよう求めるポップアップメッセージが表示されます。	[アップデートオプション] 画面で [ワイヤレス接続の警告] を選択した場合は、この現象は正常です。このオプションは無効にできますが、アップデートの確認でワイヤレス接続が開かれる場合に、警告が表示されなくなります。

問題	推奨処理
Mobile Security のインストールに成功しました。しかし、コピー中のセキュリティリスクを検出できませんでした。	ネットワーク管理者に問い合わせ、Mobile Security のライセンスの有効期限が切れていないことを確認します。
ファイルをモバイルデバイスにコピーできません。	ファイルが感染している可能性があるため、Mobile Security によりブロックされました。リアルタイム検索は無効にできますが、モバイルデバイスの予防セキュリティを損なう可能性があります。
インターネットやその他のネットワークリソースにアクセスできません。	ファイアウォールポリシーを確認します。ファイアウォールの保護レベルが高に設定されている場合は、すべての送受信トラフィックがブロックされます。55 ページの「不正侵入への対策」を参照してください。
ファイアウォール機能や WAP プッシュ保護機能を使用できません。ファイアウォールまたは WAP プッシュ保護ドライバがロードされていませんというメッセージを受信しました。	モバイルデバイスを再起動します。モバイルデバイスによっては、ファイアウォールや WAP プッシュ保護ドライバをロードするのに、Mobile Security をインストールした後で再起動する必要があります。
初期設定パスワードが許可されません。	モバイルデバイスを再起動します。解決しない場合は、ポリシーが適用されていません。以前の初期設定パスワードを使用してログオンします。
ストレージカード内のファイルが暗号化されていますが、Mobile Security がアンインストールされました。ファイルを復号化できません。	管理者にお問い合わせください。管理者はファイルを回復できます。

問題	推奨処理
ストレージカード内のファイルが暗号化されていますが、モバイルデバイスを紛失しました。ファイルの復号化を希望しています。	管理者にお問い合わせください。管理者はファイルを回復できます。
ファイルを隔離しようとすると、常に処理が失敗します。 ファイルを隔離するとき、常に次のようなメッセージが表示されます。「ファイル「%s」を隔離できません。このファイルは、読み取り専用か、使用できないか、サイズが大きすぎるか、他のアプリケーションによって使用されている可能性があります。すべてのアプリケーションを終了してから再度実行してください。」	この問題は、隔離ディレクトリに格納されているファイルが多すぎる場合に発生します。OS では各ディレクトリに約 1000 個のファイルのみを格納できます。隔離フォルダ内のファイルをいくつか削除してから再度実行してください。
Mobile Security をアンインストールしましたが、モバイルデバイスに DLL がまだいくつか残っています。	場合によっては、Mobile Security の DLL が他のアプリケーションによって使用されていたため、アンインストール時に削除されなかった可能性があります。プロンプトが表示されたら、すべてのコンポーネントをアンインストールするためにモバイルデバイスを必ず再起動してください。

よくある質問 (FAQ)

- **Mobile Security をストレージカードにインストールできますか。**

  いいえ。Mobile Security は、モバイルデバイスの内部メモリにのみインストールできます。

- **以前使用できていた機能で、使用できなくなったものがあります。なぜでしょうか。**

  管理者が特定の機能の使用可能性を無効にしている場合があります。管理者に問い合わせてから、サポートにお問い合わせください。

- **Mobile Security を他のセキュリティ製品といっしょにインストールできますか。**

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は保証できません。また、不正プログラム検索、SMS 管理、およびファイアウォール保護などの類似する機能を備えたソフトウェア製品と Mobile Security との間に互換性がない可能性もあります。Mobile Security をモバイルデバイスにインストールする前に、これらのソフトウェア製品をアンインストールするように求められる場合があります。

- **Mobile Security がモバイルデバイスに直接インストールされている場合でも、不正プログラムパターンファイルをストレージカードにダウンロードできますか。**

  いいえ。不正プログラムパターンファイルは、Mobile Security をインストールした場所と同じ場所にダウンロードおよびインストールされます。

- **Mobile Security のプログラムコンポーネントはどのくらいの頻度でアップデートする必要がありますか。**

  プログラムコンポーネントは毎週アップデートすることをお勧めします。ネットワーク管理者が、モバイルデバイスの予約アップデートをすでに設定している場合もあります。

- **Mobile Security では、圧縮ファイルを検索できますか。**

  はい。ZIP ファイルと Microsoft CAB ファイルを検索できます。3 圧縮階層まで検索するように設定できます。

- **Mobile Security で検索を実行中に電話をかけたり受けることはできますか。**

  はい。モバイルデバイスで他の機能を実行する際は、バックグラウンドで検索を実行できます。検索、検出された不正プログラム、およびセキュリティリスクに関する詳細を示すログを表示できます。

- **感染または疑わしいセキュリティリスクをクリーンできますか。**

  いいえ。Mobile Security では、感染ファイルの隔離または削除のみ実行可能です。

- **Mobile Security のログエントリは、大量のメモリ領域を消費しますか。**

  Mobile Security では、ログの種類ごとに最大で 32KB のメモリを割り当てます。

- **モバイルデバイス上で感染ファイルや疑わしいファイルを開くことはできますか。**

  いいえ。リアルタイム検索が有効な場合は、疑わしいセキュリティリスクを開いたり、コピーまたは移動することがブロックされます。リアルタイム検索は無効にできますが、モバイルデバイスの予防セキュリティを損なう可能性があります。

- **Mobile Security では、混合型の圧縮ファイル (ZIP ファイルを含む CAB ファイルなど) を検出できますか。**

  はい。Mobile Security では、混合型の圧縮ファイルの検索をサポートしています。

- **隔離ファイルを再度開くことはできますか。**

  Mobile Security では、隔離ファイルを暗号化し、ユーザが誤って開くことがないようにしています。隔離ファイルは復元できますが、この処理はお勧めしません。

- **Mobile Security では、送信者番号を SMS スパムメール対策フィルタリストと WAP プッシュの信頼されたリストにどのように照合しますか。**

  部分照合または全体照合を使用して、リストに対して送信者番号を確認しています。送信者番号が 7 桁以上である場合は、下 7 桁のみを使用し、リストに表示されている 7 桁以上の番号に照合して確認します。送信者番号が 6 桁以下の場合は、全体照合を使用します。全体照合の場合は、どちらの番号も同じ桁数であることが必要です。

- **ネットワークトラフィックがフィルタされませんが、なぜですか。**

  ActiveSync 接続でネットワークに接続している場合は、すべてのネットワークトラフィックがフィルタされません。Mobile Security のファイアウォールでは、ActiveSync 接続を経由するネットワークトラフィックは送受信ともフィルタできません。

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。

第 10 章

ログの表示

イベントログには、感染ファイルまたは疑わしいファイル、検索およびアップデートの結果、フィルタした SMS および WAP プッシュメッセージ、およびブロックされた接続の試行に関する情報が含まれています。この章では、Trend Micro Mobile Security (以下、Mobile Security) のイベントログの種類とログの使用方法について説明します。

この章は次のトピックで構成されています。

イベントログの種類

Mobile Security ではイベントログを管理します。このログを使用すると、製品のアクティビティを追跡記録したりタスク結果を表示できます。Mobile Security でサポートされているログの種類は次のとおりです。

- 94 ページの「検索ログ」
- 95 ページの「タスクログ」
- 96 ページの「ファイアウォールログ」
- 96 ページの「スパムメールログ」
- 97 ページの「WAP プッシュログ」

検索ログ

不正プログラムが検出されるたびに、検索ログにエントリ (図 10-1 を参照) が生成されます。

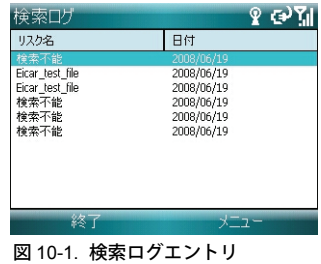


図 10-1. 検索ログエントリ

各検索ログエントリ (図 10-2 を参照) には、次の情報が含まれています。

図 10-2. 検索ログの詳細

- **日時** — 不正プログラムが検出された日時
- **リスク名** — 不正プログラムの名前
- **ファイル** — 感染または疑わしいファイルの名前
- **処理** — ファイルが隔離されたか、削除されたかを示します。
- **結果** — 処理が正常に終了したかどうかを示します。

タスクログ

手動検索、カード検索、またはアップデートが実行されるたびに、タスクログにエントリ (図 10-3 を参照) が生成されます。

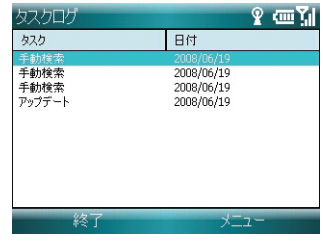


図 10-3. タスクログのエントリ

次に、タスクログのエントリの情報 (図 10-4 を参照) について説明します。

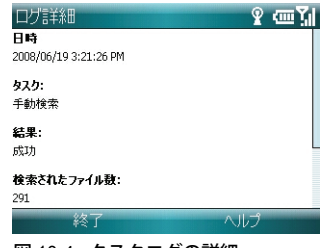


図 10-4. タスクログの詳細

- **日時** — タスクの実行日時
- **タスク** — 実行されたタスクが検索かアップデートかを示します。
- **結果** — タスクが正常に終了したかどうかを示します。
- **検索されたファイル数** — 不正プログラムがチェックされたファイルの数 (検索タスクのみ)
- **疑わしいファイル** — 不正プログラムが検出されたファイルの数 (検索タスクのみ)
- **検索されなかったファイル数** — 検出がスキップされたファイルの数 (検索タスクのみ)

ファイアウォールログ

Mobile Security では、次のいずれかの場合にファイアウォールログにエントリ (図 10-5 を参照) が生成されます。

- 接続の試行が、「ログのみ」のルール処理のファイアウォールルールと一致した場合
- 事前定義の保護レベルによって接続の試行がブロックされた場合
- IDS によって接続の試行がブロックされた場合

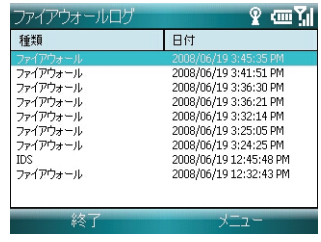


図 10-5. ファイアウォールログのエントリ

ファイアウォールログの各エントリ (図 10-6 を参照) には、次の情報が含まれています。

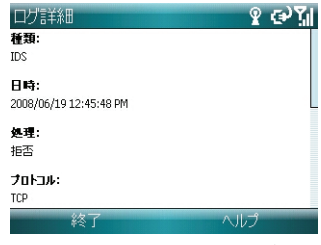


図 10-6. ファイアウォールログの詳細

- **種類** — イベントの種類。ファイアウォールまたは IDS。
- **日時** — 接続が試行された日時
- **処理** — 接続が許可されたか、ブロックされたかを示します。
- **プロトコル** — 接続で使用されたレイヤ 4 プロトコル
- **方向** — 接続は受信であったか、送信であったかを示します。
- **送信元 IP** — 接続を要求した IP アドレス
- **送信先 IP** — 接続を受信した IP アドレス
- **送信先ポート** — 接続に使用されたポート
- **説明** — ファイアウォールルールと事前定義の保護のどちらが適用されたかを示します。IDS の場合は攻撃の種類を示します。

スパムメールログ

SMS メッセージがブロックされるたびに、スパムメールログにエントリが生成されます。

注意： [スパムメールログ] メニューオプションは、電話機能を装備していないモバイルデバイスでは使用できません。

スパムメールログの各エントリには、次の情報が含まれています。

- **日時** — SMS メッセージがブロックされた日時
- **説明** — 送信者番号などのイベントに関する追加情報

WAP プッシュログ

WAP プッシュメッセージがブロックされるたびに、WAP プッシュログにエントリが生成されます。

注意： [WAP プッシュログ] メニューオプションは、電話機能を装備していないモバイルデバイスでは使用できません。

WAP プッシュログの各エントリには、次の情報が含まれています。

- **日時** — WAP プッシュメッセージがブロックされた日時
- **説明** — 送信者番号などのイベントに関する追加情報

ログを表示する

各ログを表示するには、[イベントログ] サブメニューからログを選択します。

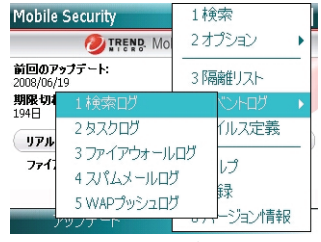


図 10-7. イベントログ

ログのエントリを表示するには

1. [メニュー]→[イベントログ] の順に選択し、次にログの種類を選択します。図 10-7 に、[イベントログ] サブメニューのログの種類を示します。
2. ログ画面で、表示するログのエントリを選択します。
3. [メニュー]→[表示] の順に選択します。

ログを削除する

ログのエントリを削除するには、ログ全体をクリアします。

ログをクリアするには

1. [メニュー]→[イベントログ] の順に選択し、次にログの種類を選択します。
2. [メニュー]→[ログのクリア] の順に選択します。確認画面が表示されます。
3. [はい] を選択します。

注意： Mobile Security では、ログの種類ごとに 32KB のメモリ領域を割り当てます。この上限に達すると、新しいエントリに対応するために自動的に最も古いエントリが削除されます。

用語集

用語	定義
ActiveSync	Windows ベースのコンピュータが Windows Mobile を実行するモバイルデバイスに接続および通信できるようにするアプリケーション
CDMA2000	CDMA (符号分割多元接続) テクノロジに基づいた一連の高速ワイヤレス通信規格。GPRS と同様に、モバイルプロバイダは、通常、メールおよび Web 参照用に CDMA2000 規格に準拠したサービスを提供しています。
GPRS	General Packet Radio Service。メールおよび Web 参照用に、モバイルプロバイダが通常提供するワイヤレス通信の一般的な規格
IDS	侵入検知システム。ネットワークアクティビティが攻撃であるかどうかを判断し、その攻撃の影響を緩和するために設計されたテクノロジ
SMS	ショートメッセージサービス。テキストベースのメッセージを携帯電話間で送受信するための一般的なプラットフォーム
SYN フラッド	攻撃元が複数の SYN パケットを送信する DoS (サービス拒否) 攻撃の 1 形態。通常は、それらのパケットは接続要求に使用され、受信コンピュータまたはモバイルデバイスのリソースを拘束します。
WAP	Wireless Application Protocol。このプロトコルは、通常、ネットワーク帯域幅、処理能力、および表示領域に制限があることの多いモバイルデバイスに、Web コンテンツを提供するのに使用されます。
WAP プッシュ	WAP を使用して、アプリケーションおよびシステムポリシーなどのコンテンツをモバイルデバイスに自動的に配信する方法
WAP プッシュ メッセージ	WAP プッシュコンテンツの配信前に、確認プロンプトとして表示される SMS メッセージ

用語	定義
アップデート	アップデートを Trend Micro サーバから適切にダウンロードしてインストールするために、Trend Micro 製品で使用しているテクノロジ
イベントログ	製品機能の実行結果を含むログ
カード検索	装着されたメモリカードに不正プログラムがないか自動的に検索する Trend Micro Mobile Security の機能
スパムメール対策	メッセージングアプリケーションまたはプラットフォームによって不要なコンテンツが受信された場合に、そのコンテンツをフィルタするためのテクノロジ
セキュリティリスク	コンピュータやモバイルデバイスおよびその通常の使用に悪影響を与える可能性があるファイルを指すのに使用される、一般的な用語
。	データを読み取り不能な形式に変換するプロセス
パターンファイル	「不正プログラムパターンファイル」を参照してください。
ファイアウォール	ポートへのアクセスを制御し、コンピュータまたはモバイルデバイスから送受信されるネットワーク通信を規制するアプリケーションまたはモバイルデバイス
ファイアウォールルール	ファイアウォールに対し、ポートへのアクセスの制御方法を指示する一連の情報
フィルタ	不要なコンテンツを区別して処理するプロセス
ポート	物理的というよりは論理的なネットワーク接続の終点。ポートには番号が付けられており、それぞれの番号が論理接続の種類を表すようになっています。たとえば、ファイアウォールで特定のポート番号がブロックされる場合は、実際には、特定の種類の論理接続がブロックされます。
リアルタイム検索	常時オンの検索サービスで、アプリケーションがファイルにアクセスすると、起動されます。
検索	ファイルまたはファイルセットに不正プログラムが含まれているかどうかを判断するプロセス

用語	定義
検索エンジン	ファイルが不正プログラムであるかどうかを判断する不正プログラム対策コンポーネント。検索エンジンは、通常、ファイルを「不正プログラムパターンファイル」として知られている不正プログラムのコードのデータベースファイルと照合します。
検索不能ファイル	パスワードで保護されているか圧縮階層が多すぎるために、Mobile Security でアクセスおよび検索できない圧縮ファイル (51 ページの「不正プログラム対策ポリシーの詳細設定」を参照してください)
検出されたファイル	不正プログラムが含まれていることが検出されたファイル
不正プログラム	ウイルスやトロイの木馬など、あらゆる種類の不正なアプリケーションを指す一般的な用語
不正プログラム	自らのコピーを配布したり、他のファイルを感染させたり、またはその両方を実行することによって増殖する不正プログラム
不正プログラム パターンファイル	検索エンジンで不正プログラムを識別する基盤として使用される、不正プログラムのコードを集めたデータベースファイル
不正プログラム対策	不正プログラムを検出および処理するために設計されたテクノロジ

索引

英数字

あ

ま

や

ら