

# F-Secure Mobile Security™ for Windows Mobile

## 1. インストールと認証

**旧バージョン** F-Secure Mobile Security の旧バージョンからアップグレードする場合、旧バージョンを起動していない状態にしてください。インストールを実行するときに旧バージョンが自動的に削除されます。

**インストール** 本製品は次のいずれかの方法でインストールできます。



1. .cab ファイルをデバイスに転送します。
2. .cab ファイルをファイルエクスプローラから選択します。
3. インストールの実行を確認された場合、[はい] を選択します。
4. 使用許諾契約書を確認して、[はい] を選択します。
5. インストール後、デバイスを再起動するためのメッセージが表示されます。[はい] を選択します。
6. インストールが完了したら、本製品を認証する必要があります。認証を行わない場合、本製品の保護機能は無効になります。

**認証** 本製品を認証するには

1. F-Secure Mobile Security をインストールした後、デバイスをはじめて起動するときに認証に関するメッセージが表示されます。確認されたら、[はい] を選択します。
2. 認証タイプを選択します。  
本製品を試用する場合、[試用] を選択してから [次へ] を押します。  
ライセンス版を認証する場合、[ライセンスキーコード] を選択してから、[次へ] を選択します。次の画面でライセンスキーコードを入力して、[次へ] を押します。
3. [はい] を押して、更新をダウンロードするためのアクセスポイントに接続します。更新サービスに接続して、指定のライセンスキーコードが認証されます。はじめて更新するときには最新のウイルス定義ファイルがダウンロードされます。
4. ダウンロードが完了したら、認証が完了したことを示すメッセージが表示されます。[OK] を押すと認証手続きが完了します。
5. 認証後、スキャンを実行してデバイスにウイルスが感染していないことを確認してください。詳細は、次ページの『[ウイルスのスキャン](#)』を参照してください。

試用版からライセンス版にアップグレードする場合、[購入] メニューからライセンスキーコードを入力することでライセンスを認証できます。

**Mobile Security** の起動 F-Secure Mobile Security を一度認証したら、デバイスの電源をつけるたびに本製品が自動的に起動されるようになります。

1. デバイスが Windows Mobile Professional/Classic を使用している場合、**スタート プログラム**  **Mobile Security** の順に選択します。  
デバイスが Windows Mobile Standard を使用している場合、**スタート**  **Mobile Security** の順に選択します。
2. ウイルススキャンを実行するように促されたら、[はい] を選択してください。

## 2. ウイルスのスキャン

F-Secure Mobile Security のリアルタイムスキャンを有効にしている場合、本製品は透過的に動作し、ファイルを自動的にスキャンします。

1. リアルタイムスキャンがウイルスを検出した場合、メッセージが表示されます。[はい] を押すと、感染したファイルの詳細を確認できます。[いいえ] を押すと、前の画面に戻ります。
2. 「感染」ビューには、デバイスで検出された感染ファイルの一覧と各ファイルの状態（「検疫」あるいは「解除」）が表示されます。
3. 感染したファイルの詳細を表示するには  
デバイスが Windows Mobile Professional/Classic を使用している場合、[詳細] を押します。  
デバイスが Windows Mobile Standard を使用している場合、[メニュー] [詳細] の順に押します。

**感染ファイルの**  
**処理**

**感染ファイルを処理するには**

1. 「メイン」ビューから [ウイルス保護] を開きます。
2. 「ウイルス保護」メニューで感染ファイルを選択します。
3. 「感染」ビューで、処理する感染ファイルを選択します。
4. 処理を選択します。

**削除** - 感染したファイルを削除します。通常はこのオプションを選択してください。感染したファイルがデバイスから完全に削除されます。

**検疫** - 感染したファイルを検疫します。F-Secure Mobile Security が起動している間、検疫したファイルはデバイスに脅威をさらせなくなります。

**解除** - 検疫したファイルを解除します。検疫したファイルを解除すると、ファイルに対する保護はなくなります。使用する際には十分に注意してください。

デバイスが Windows Mobile Professional/Classic を使用している場合、ソフトキーを押します。

デバイスが Windows Mobile Standard を使用している場合、[メニュー] を押してから処理を選択します。

## 3. ファイアウォール

F-Secure Mobile Security のファイアウォールは透過的に動作します。この機能はインターネットとネットワークから送受信されるデータを監視して、不正な侵入を防ぎます。保護レベルは必要に応じて変更できます。

## 保護レベル

保護レベルを選択するには

1. 「メイン」ビューから [ [ファイアウォール](#) ] を開きます。
2. 「ファイアウォール」メニューで [ [設定](#) ] を選択します。
3. 保護レベルを選択します。

[すべて拒否](#) - ネットワークトラフィックをすべて拒否します。

[高](#) - 一般的なアプリケーションを許可して、着信トラフィックをすべて拒否します。


[標準](#) - 発信接続をすべて許可して、着信トラフィックをすべて拒否します。

[すべて許可](#) - ネットワークトラフィックをすべて許可します。

[カスタム](#) - カスタムのルールに応じて、ネットワークトラフィックを許可します。カスタムのルールを編集するには、[ [カスタム](#) ] 保護レベルを選択した状態で [ [カスタムルールを編集する](#) ] を選択します。

## 4. Anti-Theft

本製品は、デバイス紛失・盗難時の悪用を防ぐ Anti-Theft (盗難防止) 機能を備えています。

-  メモリカードは簡単に取り外すことができるため、重要なデータはデバイスの本体に保存することを推奨します。

### セキュリティコード

セキュリティコードを使用して、リモートからデバイスの位置検索、ロック、データ削除を行うことができます。

セキュリティコードは8文字以上である必要があります。設定したら、大切に保管してください。

### リモート Anti-Theft

デバイスを紛失した場合、リモートロケータ機能でSMSをデバイスに送ることでデバイスの位置を検索できます。

デバイスへSMSを送ることで、デバイスのロックをリモートから実行することができます。リモートロックを使用するには、デバイスロックを有効にする必要があります。

デバイスへSMSを送ることで、デバイスのデータ削除をリモートから実行することもできます。デバイスのデータ削除を実行すると、すべてのデータが完全に削除されます。


リモート Anti-Theft を設定するには

1. 「メイン」ビューから [ [Anti-Theft](#) ] を開きます。
2. 「Anti-Theft」メニューで [ [設定](#) ] を選択します。
3. 有効にする機能を選択します。

デバイスの位置をリモートから検索できるようにするには、[ [ロケータを有効にします](#) ]。

[ [リモート削除を有効にする](#) ] を有効にします。

[ [リモートロックを有効にする](#) ] を有効にします。

-  リモートロックを有効にするには、デバイスロックが有効になっている必要があります。

4. [ [セキュリティコード](#) ] を入力および確認します。

リモートからデバイスのロケート/ロック/データ削除を実行するには

デバイスの位置検索 - デバイスに次の SMS メッセージを送ります。

#LOCATE#<セキュリティコード> (例: #locate#12345678)

デバイスのロック - デバイスに次の SMS メッセージを送ります。

#LOCK#<セキュリティコード> (例: #lock#12345678)

デバイスのデータ削除 - デバイスに次の SMS メッセージを送ります。

#WIPE#<セキュリティコード> (例: #wipe#12345678)

#### SIM 変更時に SMS を送る

デバイスの SIM カードが変更された場合、別のデバイスに SMS を送るように設定できます。[SIM 変更時に SMS を送る] を有効にし、SMS の送り先となる電話番号を指定したら、SIM カード変更時に SMS が指定のデバイス (電話番号) へ自動的に送られるようになります。

## 5. ブラウザ保護

ブラウザ保護は、デバイスを危険性のある Web サイト (クレジットカードたアカウントのパスワードなどの個人情報を盗むサイト) のアクセスから保護しません。

ブラウザ保護は Internet Explorer を利用してアクセスする Web サイトの安全性を確認します。F-Secure Mobile Security を認証した後に Internet Explorer がデフォルトのブラウザとして設定されている場合、ブラウザ保護は自動的に有効になります。ブラウザ保護はサードパーティのブラウザには対応してません。

ブラウザ保護を設定するには

1. 「メイン」ビューから [ブラウザ保護] を開きます。
2. 「ブラウザ保護」メニューで [設定] を選択します。
3. [ブラウザ保護を有効にする] を選択します。
4. [使用するネットワーク] でブラウザ保護を有効にするネットワークを設定します。

**マイプロバイダ** - 通常のネットワークに接続しているときにブラウザ保護を有効にします。

**全プロバイダ** - 接続しているプロバイダに関係なくブラウザ保護を常に有効にします。

## 6. 更新

### 自動更新

F-Secure Mobile Security は自動更新機能を搭載し、ウイルス定義ファイルを定期的に更新できます。最新のウイルス定義ファイルはデバイスを最新のウイルスから保護するために必要であります。本製品を認証したら自動更新機能は有効になります。

更新をダウンロードするにはインターネットに接続していることが必要です。Mobile Security は定期的にウイルス定義ファイルの更新をチェックし、必要な際に更新をダウンロードします。

### 手動更新

Mobile Security を手動で更新することもできます。Mobile Security を手動で更新するには

1. 「メイン」ビューから [メニュー] [更新] の順に選択します。
2. [はい] を選択して、更新の有無を確認します。
3. 新しい更新がある場合、[はい] を選択して、更新をダウンロードします。
4. 更新が完了したら、[はい] を選択することでデバイスをスキャンできます。詳細は、ページ 2 の『ウイルスのスキャン』を参照してください。

## 追加情報

本製品に関する追加情報は、<http://mobile.f-secure.com/> にあるユーザガイドでご覧になれます。

## テクニカルサポート

本ガイドや Web ページ (<http://mobile.f-secure.com/>) で取り上げていない情報がありましたら、F-Secure の代理店または F-Secure Corporation (本社) へお問い合わせください。

---

### 免責条項

「F-Secure」および三角形のシンボルは、F-Secure Corporation の登録商標です。F-Secure の製品名およびシンボル / ロゴは、F-Secure Corporation の商標または登録商標です。本書に記載されている製品名はすべて、各社の商標または登録商標です。F-Secure Corporation は、他社の商標および名前について所有権を持つものではありません。F-Secure Corporation では、本書の情報に期待して万全の努力を払っておりますが、情報に間違いや脱落があっても責任を負うことはありません。本書に記載されている仕様は、予告なしに変更されることがあります。

本書の例で使われている会社、名前、およびデータは、特に断りがない限り、事実とは関係ありません。本書のどの部分も、いかなる形態または手段（電子的または機械的）によっても、目的を問わず、F-Secure Corporation の書面による許可なしに複製または伝達することはできません。

本製品は以下の F-Secure の特許で保護されていることがあります。

GB2353372、GB2366691、GB2366692、GB2366693、GB2367933、GB2368233、GB2374260

Copyright (c) 2010 F-Secure Corporation. All rights reserved

