ESET Endpoint Security for Android

ユーザーズマニュアル

目次

■本書について

○本書は、ESETセキュリティ ソフトウェア シリーズ ライセンス製品の共通ガイドとしてまとめています。

■お断り

○本書は、本書作成時のソフトウェアおよびハードウェアの情報に基づき作成されています。ソフトウェアのバージョンアップなどにより、記載内容とソフトウェアに搭載されている機能が異なっている場合があります。また本書の内容は、改訂などにより予告なく変更することがあります。

[Chapter 1]
はじめに

1.1 ESET Endpoint Security for Androidについて

ESET Endpoint Security for Androidは、ウイルス・スパム対策機能のほか、紛失／盗難時の盗難対策機能や、各種設定を保護するパスワード保護機能などを搭載したAndroid端末向けの総合セキュリティプログラムです。ESET Remote Administratorと接続することにより、ネットワークに接続された任意のコンピューターから、Android端末を管理でき、ポリシーとルールの適用、検出の監視、リモート設定が可能になります。ESET Endpoint Security for Androidには、以下の機能が搭載されています。

ウイルス対策

常駐検査（リアルタイム検査）および手動検査（オンデマンド検査）で、マルウェアや不正なアプリケーションを検知します。

スパム対策※

定義したルールに基づいてSMSの受信、電話の着信／発信をブロックできます。非通知着信をブロックすることもできます（電子メールは対象外となります）。

盗難対策（リモート制御／SIMカード認証）※

Android端末を紛失した際、SMSによってAndroid端末のリモートロック／リモートワイプ／リモートファインドが行えます。登録したSIMカード以外では、Android端末を使用不可にすることもできます。

セキュリティ監査

バッテリー残量、インストールしたアプリケーション、空きディスク容量などの状態をチェックできます。

パスワード保護

各種設定を許可なく変更できないようにパスワードで保護できます。

リモート管理

ESET Remote Administratorを利用して、ESET Endpoint Security for Androidをリモート管理することが可能です。ログの表示や、リモートからの設定変更などが行えます。

※SIMカードを利用しないAndroid端末ではこの機能をご利用になれません。また、SMSを利用できないAndroid端末では、盗難対策機能はご利用になれません。

1.2 保護の種類

ESET Endpoint Security for Androidには、Android端末をさまざまな脅威から保護するために以下のような機能を搭載しています。

ウイルス対策

常駐検査（リアルタイム検査）および手動検査（オンデマンド検査）で、マルウェアや不正なアプリケーションを検知します。手動検査は、デバイス（Android端末）またはフォルダー単位で行え、検査を行う拡張子などを指定することもできます。なお、手動検査（オンデマンド検査）はバックグラウンド検査に対応していますので、検査中に別のタスクを実行することができます。

スパム対策

定義したルールに基づいて、SMSの受信、電話の着信／発信をブロックしたり、非通知の着信をブロックしたりできます。既定値では、非通知の着信をブロックするように設定されています。なお、この機能は、電子メールは対象外です。また、SIMカードを利用しないAndroid端末ではこの機能をご利用になれません。
※MMS受信ブロックは、日本の携帯電話事業者を利用した場合、対応しておりません。

盗難対策（リモート制御／SIMカード認証）

Android端末を紛失した際、SMSをAndroid端末に送ることでリモートロック、リモートワイプ、リモートファインドなどの機能を使って、Android端末を遠隔操作できます。

・リモートロック
Android端末を操作できないようにロックする機能です。
・リモートワイプ
Android端末内のデータおよびセットされているSDメモリーカードなどのリムーバブルメディアに記録されたデータをすべて消去します。
・リモートファインド
Android端末のGPS座標を取得する機能です。

これらの機能は、SIMカードを利用しないAndroid端末ではご利用になれません。また、SMSを利用できないAndroid端末では、盗難対策機能はご利用になれません。

セキュリティ監査

バッテリー残量、インストールしたアプリケーション、空きディスク容量などの状態をチェックする機能です。

パスワード保護

ESET Endpoint Security for Androidの各種設定を許可なく変更できないようにパスワードで保護できます。この設定は、各機能単位で設定でき、既定値では、ESET Endpoint Security for Androidをアンインストールする場合のみパスワード入力を求めるように設定されています。

USSDコントロール

USSDコントロールは、悪意のあるSMS、QRコード、URLリンクなどによって実行されたUSSDコード攻撃からAndroid端末を保護する機能です。USSDコードとは、通信会社のオペレーターが携帯電話の遠隔サポートを提供するためのもので、携帯電話内のすべてのデータを消去し工場出荷時の状態に戻すコードなどがあります。USSDコントロールを利用すると、有害なUSSDコードが実行されようとしたときに警告画面を表示し、USSDコード攻撃からAndroid端末を保護できます。

1.3 ESET Endpoint Security for Androidの画面構成

本プログラムが各種保護を行っているときは、ステータスバーにアイコンが表示されます。また、Android端末の取扱説明書を参考にアプリケーション一覧を表示し、「ESET Endpoint」アイコンをタップすると、基本画面が表示され、各種操作や設定を行えます。

1

本プログラムが各種保護を行っているときは、ステータスバーにアイコンが表示されます。本プログラムの設定を変更するには、アプリケーション一覧を表示し、「ESET Endpoint」アイコンをタップします。

2

基本画面が表示されます。基本画面には現在の保護レベルが表示されています。また、各種項目をタップすると、設定の変更などを行えます。

[Chapter 2]
インストール

2.1 インストールについて

ESET Endpoint Security for Androidのインストールは、手動で行います。また、本製品のインストールの前に以下のものをご準備ください。

インストーラー(.apk)

ESET Endpoint Security for Androidのインストールは、弊社ユーザーズサイトからダウンロードしたインストーラー(.apk)を利用して行います。インストーラーは、社内に設置したWebサーバーなどを利用して配布できるほか、SDメモリーカードなどのリムーバブルメディアにコピーして配布することもできます。ただし、リムーバブルメディアからインストールを行うには、ファイル操作アプリをAndroid端末にインストールしておく必要があります。

ユーザー名とパスワード

ESET Endpoint Security for Androidのアクティベーションに必要です。ESET Endpoint Security for Androidは、アクティベーションを行わないと利用できません。

2.2 インストール要件

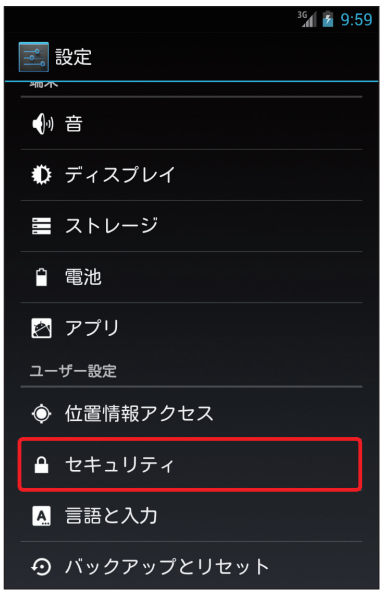
ESET Endpoint Security for Androidは、Android端末専用のプログラムです。動作環境については、弊社ホームページをご参照ください。

2.3 ESET Endpoint Security for Androidのインストール

ここではESET Endpoint Security for Androidのインストール方法を紹介します。
他社製のアンチウイルスソフトがインストールされている場合は、必ずあらかじめアンインストールを行ってください。

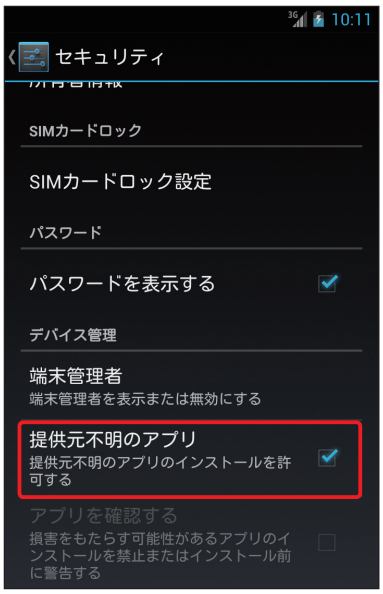
2.3.1 インストール手順

1



設定画面を起動し、提供元不明のアプリケーションのインストールを許可する設定を行います。設定画面を起動したら、[アプリケーション]または[セキュリティ]、[その他]などをタップします。

2

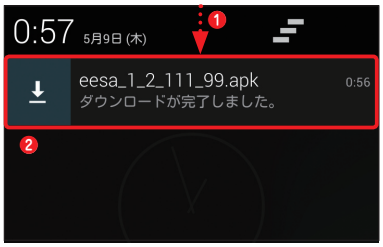


[提供元不明のアプリ]をタップしてチェックを入れます。
※本設定は、「ESET Endpoint Security for Android」のインストール完了後に元に戻してください。

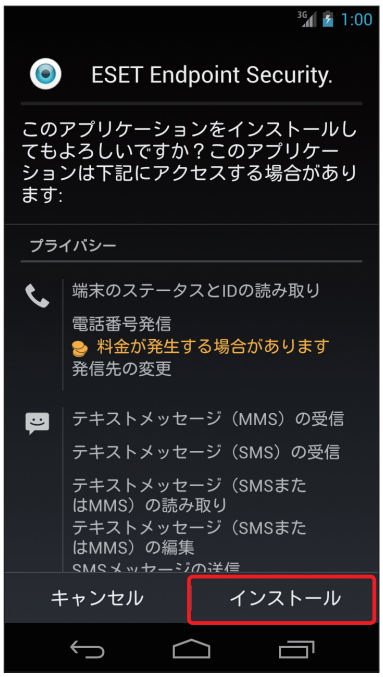
POINT

提供元不明のアプリケーションのインストールを許可する設定は、ご利用の機種によって設定手順が異なる場合があります。その場合は、ご利用の機種の取扱説明書を参考に設定を行ってください。

3 弊社ユーザーズサイトなどからインストーラー(.apk)をダウンロードします。

4 

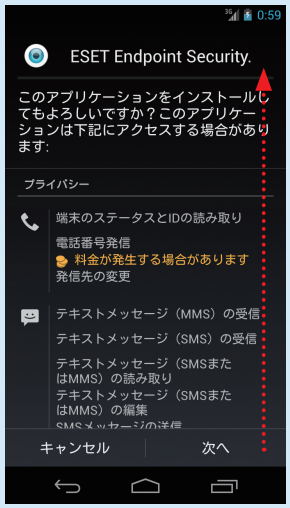
インストーラーのダウンロードが完了したら、❶[ステータスバー(通知バー)]を下方向にドラッグして、通知領域を表示します。❷ダウンロードしたインストーラー(.apk)をタップします。

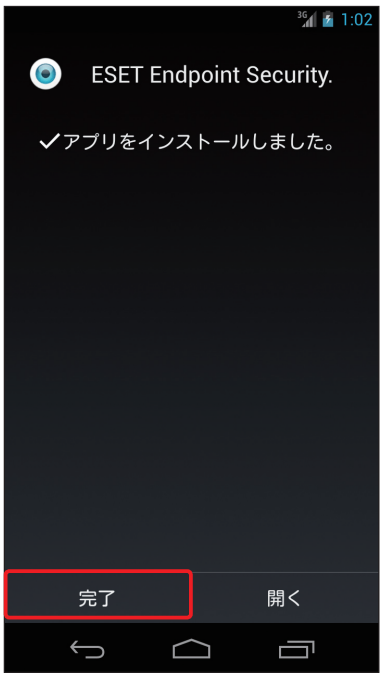
5 

[インストール]をタップします。

POINT

画面下に[インストール]ボタンが表示されていないときは、画面を最後までスクロールさせ、説明文をすべて表示すると[インストール]ボタンが表示されます。



6 

「アプリケーションをインストールしました」と表示されたら、本プログラムのインストールは完了です。[完了]をタップします。
※引き続き、アクティベーションを行う場合は[開く]をタップしてください。

POINT

本プログラムを利用するには、アクティベーションを行う必要があります。アクティベーションの手順については、16ページをご参照ください。

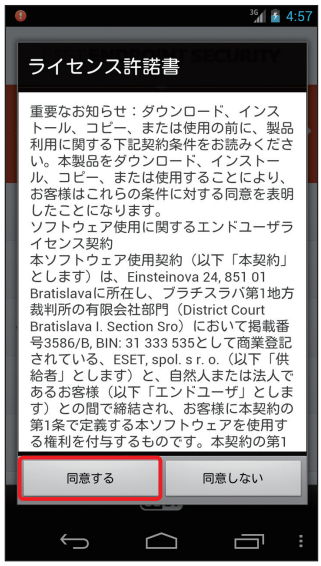
2.4 インストール後の初期セットアップ

ESET Endpoint Security for Androidのインストールが完了したら、アクティベーションを行って各種設定を行います。ここでは、インストール後の初期セットアップについて説明します。

2.4.1 アクティベーションと初期設定を行う

ESET Endpoint Security for Androidのアクティベーションは、以下の手順で行います。

1



ライセンス許諾書が表示されます。内容をご一読のうえ、同意いただけましたら［同意する］をタップします。

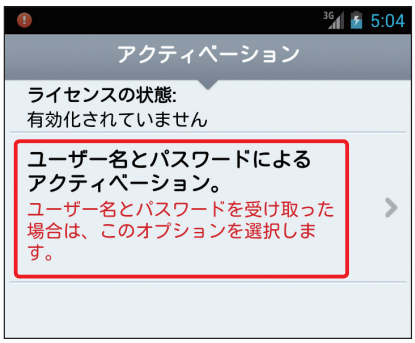
2

［今すぐアクティベーション］をタップします。

CAUTION

アクティベーションには、Android端末か直接インターネットに接続できる環境が必要です。

3



[ユーザー名とパスワードによるアクティベーション。] をタップします。

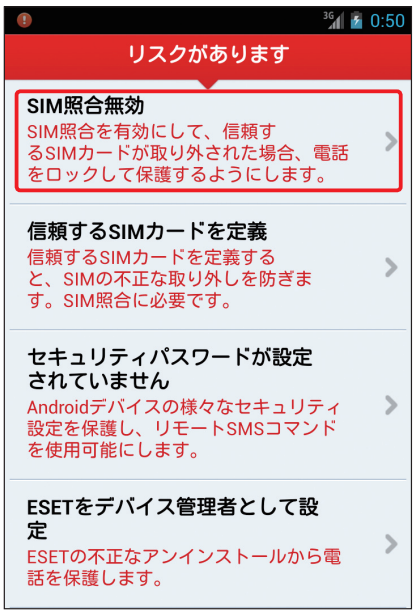
4

❶ユーザー名を入力し、❷パスワードを入力します。❸ [アクティベーション] をタップします。

5

アクティベーションが完了すると基本画面に戻ります。続いて、初期設定を行います。[リスクがあります] をタップします。

6



[SIM照合無効] をタップします。

7

❶ [SIM照合有効] をタップし、チェックを入れます。❷ ⮌ をタップします。

[SIM照合無視] にチェックした場合は8、[SIM照合有効] にチェックした場合は、SMS警告テキストの空欄にメールアドレスを入力して次に進みます。

[SIM照合] を有効にすると、[信頼するSIMカード] に登録されていない別のSIMカードに差し替えられると自動的にAndroid端末をロックします。その際に管理者連絡先に登録された電話番号に差し替えられたSIMカードから警告SMSが送信されます

※この警告SMSの本文にSMS警告テキストの内容が含まれます。空欄には警告SMSを受け取った人が連絡するためのメールアドレスを入力してください。

CAUTION

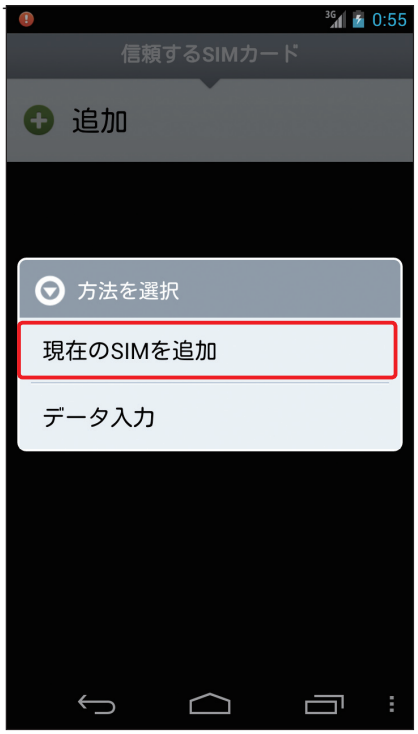
SMSの本文に全角文字（2Byte）を使用すると日本の携帯電話事業者の制限によりSMSで送信できる文字数が大幅に減り、警告SMSが送信できなくなります。そのため、SMS警告テキストの空欄には半角英数字および半角記号でメールアドレスを入力してください。

8

[信頼するSIMカードを定義] をタップします。

9 

[追加] をタップします。

10 

[現在のSIMを追加] をタップします。

11 

❶任意のSIMカード名を入力し、❷ [追加] をタップします。

12

❶SIMカードが登録されます。❷ をタップします。

13

［セキュリティパスワードが設定されていません］をタップします。

14

❶設定したいパスワードを入力し、❷パスワードを再入力します。
※パスワードは半角英数字で入力してください。また大文字と小文字も区別しますの正確に入力してください。

15

画面を上方向にスクロールし、❶秘密の言葉を入力し、❷[次へ] をタップします。

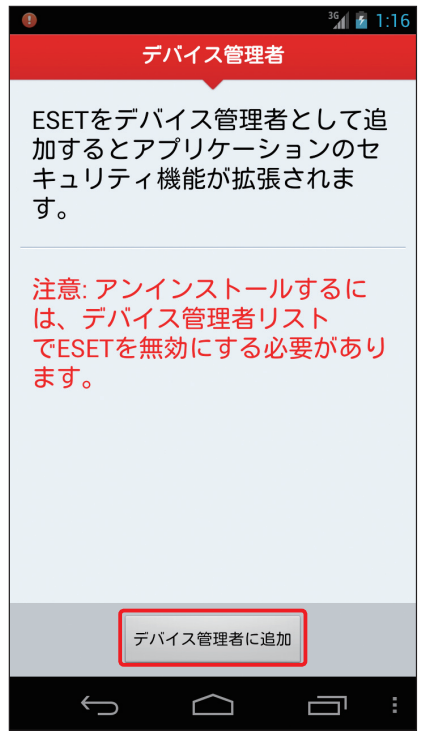
POINT

秘密の言葉は、パスワードのヒントです。秘密の言葉は、パスワードの入力を3回ミスしたときに表示されます。

16

❶手順14で設定したパスワードを入力しないと、設定変更などが行えないようにする項目をタップしてチェックを入れます。❷[適用] をタップします。

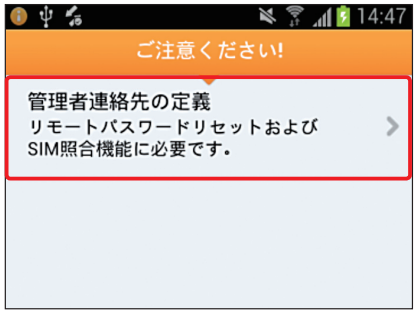
17



[デバイス管理者に追加] をタップします。

18 

[有効にする] をタップします。

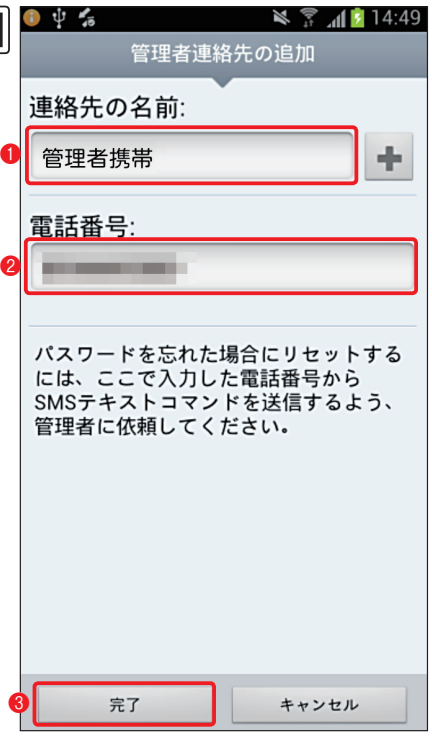
19 

[管理者連絡先の定義] をタップします。
セキュリティパスワードを忘れたときに、[管理者連絡先] に登録した携帯電話からのみ、パスワードリセットコマンドをSMSで送信し、パスワードのリセットを行えます。また、[SIM照合有効] を設定した場合、管理者連絡先に登録した携帯電話の番号に警告SMSが送信されます。

20 

[追加] をタップします。

21



❶連絡先の名前を入力し、❷電話番号を入力します。❸[完了]をタップします。

POINT

をタップすると、電話帳から管理者連絡先に登録したい情報を選択できます。

22

管理者連絡先が登録されます。複数の管理者連絡先を登録したいときは、手順20からの作業を繰り返し行います。

POINT

登録されている管理者連絡先を削除したいときは、削除したい情報を長押しして、画面が表示されたら[削除]をタップします。確認画面が表示されるので、[はい]をタップします。

23 

保護レベルが最大に設定されました。

2.5 設定読み込み型インストール

設定読み込み型インストールは、設定ファイルを事前にERA付属のESET コンフィグレーションエディターで作成し、その設定ファイルとインストーラー（.apk）を組み合わせてインストールを行います。設定ファイルの内容をインストール時に適用できるので、インストール後の設定を最小限にすることができます。設定読み込み型インストールは以下の方法で行います。

設定ファイルの作成

設定ファイルの作成は、ERA付属のESET コンフィグレーションエディターで行います。なお。設定ファイルは、「settings.xml」というファイル名で保存する必要があります。設定ファイルの詳細な作成方法は「ユーザーズガイド導入・運用編」をご参照ください。

インストール方法

設定読み込み型インストールでは、設定ファイルをAndroid端末の「/mnt/sdcard」フォルダーにコピーしてインストール作業を実施します。ファイル操作を伴うため、Android端末用のファイル操作アプリを事前にインストールしておく必要があります。

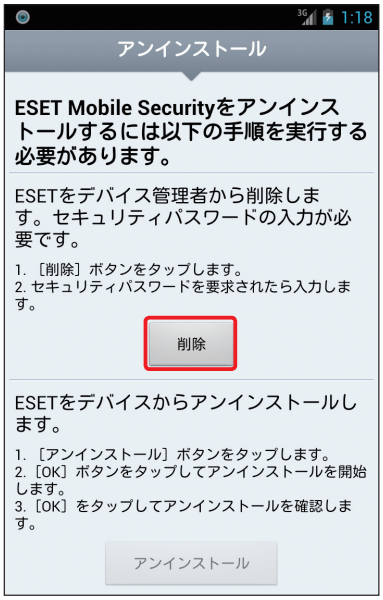
2.6 アンインストール

ESET Endpoint Security for Androidのアンインストール方法を説明します。ESET Endpoint Security for Androidのアンインストールは、以下の手順で行います。

2.6.1 アンインストール手順

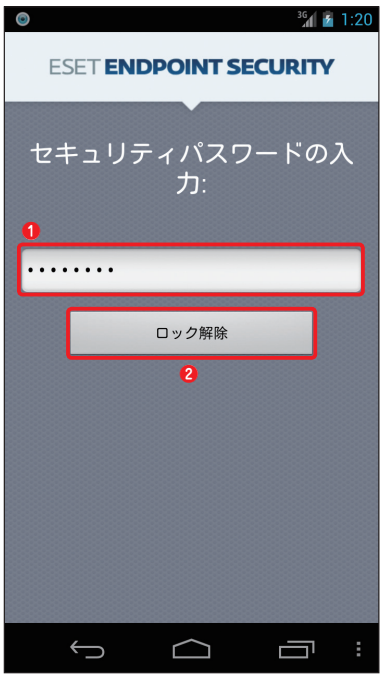
1 

[アンインストール] をタップします。

2 

アンインストール画面が表示されます。[削除] をタップします。

3



パスワードの設定で「アンインストール防止」を有効にしている場合は、❶Androidのセキュリティパスワードを入力して、❷[ロック解除] をタップします。

4

アンインストール画面に戻ります。[アンインストール] をタップします。

5

確認画面が表示されます。[OK] をタップするとESET Endpoint Security for Androidがアンインストールされます。

[Chapter 3]
操作・設定ガイド

3.1 ウイルス対策

ウイルス対策では、常駐検査（リアルタイム検査）および手動検査（オンデマンド検査）によってマルウェアや不正なアプリケーションの侵入を阻止します。ここでは、ウイルス対策の設定や手動検査の実施方法、隔離されたファイルの履歴や復元方法などについて説明します。

3.1.1 ウイルス対策の設定

ウイルス対策には、常駐検査（リアルタイム検査）および手動検査（オンデマンド検査）があります。常駐検査（リアルタイム検査）では、ユーザーが操作するファイルをリアルタイムでチェックし、マルウェアや不正なアプリケーションの侵入を阻止します。自動的に検査される対象は、SDメモリーカード上のDownloadフォルダー内のファイルとインストールファイル（.apk）内のファイルで、ブラウザーでファイルをダウンロードした時やアプリケーションをインストールしたときに検査が実行されます。手動検査（オンデマンド検査）では、手動でマルウェアや不正なアプリケーションがないかを検査でき、デバイス（Android端末）全体または指定フォルダー内のファイルを検査できます。常駐検査、手動検査ともに検査を行うファイル形式を設定できます。ウイルス対策の設定は、以下の手順で行います。

1

［ウイルス対策］をタップします。

2

ウイルス対策オプション画面が開きます。［設定］をタップします。

3

「オンデマンド」タブが選択された状態で設定画面が開きます。「オンデマンド」タブでは、手動検査（オンデマンド検査）に関する設定が行えます。設定項目の詳細については、本書32ページをご参照ください。

4

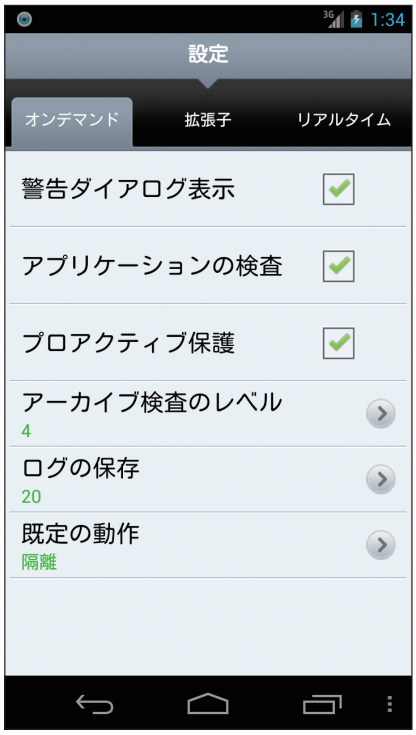
「拡張子」をタップすると、常駐検査または手動検査を行うときのファイルの拡張子の設定が行えます。設定項目の詳細については、本書33ページをご参照ください。

5

「リアルタイム」をタップすると、常駐検査（リアルタイム検査）に関する設定が行えます。設定項目の詳細については、本書34ページをご参照ください。

3.1.1.1 手動検査（オンデマンド検査）の設定

手動検査（オンデマンド検査）では、手動検査を行うときの各種動作の設定が行えます。以下の項目について設定できます。



設定項目	内容
警告ダイアログ表示	この設定にチェックを入れオンにすると、手動検査（オンデマンド検査）によって脅威が検出されるたびに警告画面を表示します。この設定の既定値は、オンに設定されています。
アプリケーションの検査	この設定にチェックを入れオンにすると、Android端末にインストールされているすべてのアプリケーション（.apkファイル）の検査が実施されます。この設定の既定値は、オンに設定されています。
プロアクティブ保護	この設定にチェックを入れオンにすると、現在のウイルス定義データベースに登録されていない悪意のあるソフトウェアを特定できるアルゴリズムベースの検出方法で検査を行います。この設定の既定値は、オンに設定されています。
アーカイブ検査のレベル	圧縮ファイルの階層をどこまで検査するかを設定します。1～4までの範囲で設定できます。既定値では、最大階層数の「4」が設定されています。
ログの保存	保存するログの最大個数を設定します。既定値では、20が設定されています。
既定の動作	感染ファイルが検出されたときの動作を設定します。感染ファイルに対してなんの処置も行わない「無視」、感染ファイルの削除を行う「削除」、感染ファイルの隔離を行う「隔離」の中から動作を設定できます。既定値では、「隔離」が設定されています。

3.1.1.2 拡張子の設定

拡張子は、常駐検査（リアルタイム検査）および手動検査（オンデマンド検査）の共通の設定となります。常駐検査（リアルタイム検査）または手動検査（オンデマンド検査）を行うときのファイル形式の設定が行えます。以下の項目について設定できます。

項目	内容
拡張子を指定	この設定にチェックを入れオンにすると、指定した拡張子のファイルのみが検査され、検査時間を短縮できます。この設定のチェックを外しオフにすると、すべてのファイルが検査対象になります。この設定の既定値はオンに設定されています。
DEX（実行可能形式ファイル）	この設定にチェックを入れオンにすると、拡張子「DEX（実行可能形式ファイル）」のファイルを検査対象とします。この設定の既定値はオンに設定されています。
SO（ライブラリ）	この設定にチェックを入れオンにすると、ファイルシステム上の指定された場所に保存されている共有ライブラリのある拡張子「SO（ライブラリ）」のファイルを検査対象とします。この設定の既定値はオンに設定されています。
アーカイブ（Zipファイル）	この設定にチェックを入れオンにすると、拡張子「Zip（圧縮ファイル、apkファイルを含む）」のファイルを検査対象とします。この設定の既定値はオンに設定されています。
その他	この設定にチェックを入れオンにすると、上記のDEX、SO、Zip（圧縮ファイル、apkファイルを含む）以外のファイルを検査対象とします。この設定の既定値はオフに設定されています。

3.1.1.3 常駐検査（リアルタイム検査）の設定

リアルタイムでは、常駐検査（リアルタイム検査）を行うときの各種動作の設定が行えます。

設定項目	内容
リアルタイム保護	この設定にチェックを入れオンにすると、常駐検査（リアルタイム検査）機能が有効になり、ユーザーが操作するファイルをリアルタイムで検査します。この設定の既定は、オンに設定されています。
警告ダイアログ表示	この設定にチェックを入れオンにすると、常駐検査（リアルタイム検査）によって脅威が検出されるたびに警告画面を表示します。この設定の既定値は、オンに設定されています。
SDカードを検査	この設定にチェックを入れオンにすると、SDメモリーカードに保存されたファイルを開いたり、SDメモリーカードにファイルを保存するときに検査を行います。この設定をオンにすると検査時間が長くなる可能性があります。この設定の既定値は、オフに設定されています。
プロアクティブ保護	この設定にチェックを入れオンにすると、現在のウイルス定義データベースに登録されていない悪意のあるソフトウェアを特定できるアルゴリズムベースの検出方法で検査を行います。この設定をオンにすると、検査時間が長くなります。この設定の既定値は、オンに設定されています。
アーカイブ検査のレベル	圧縮ファイルの階層をどこまで検査するかを設定します。1 ～ 4までの範囲で設定できます。既定値では、最大階層数の「4」が設定されています。
既定の動作	感染ファイルが検出されたときの動作を設定します。感染ファイルに対してなんの処置も行わない「無視」、感染ファイルの削除を行う「削除」、感染ファイルの隔離を行う「隔離」の中から動作を設定できます。既定値では、「隔離」が設定されています。

3.1.2 デバイスの検査を行う

手動検査（オンデマンド検査）によって、デバイス（Android端末）の検査を行うときは、以下の手順で操作します。

1 

［ウイルス対策］をタップします。

2 

ウイルス対策オプション画面が開きます。［デバイスを検査］をタップします。

3 

Android端末内のファイルの検査が実施されます。

POINT

［キャンセル］をタップすると検査を中止できます。

4

検査が完了すると、検査結果が表示されます。をタップすると、ウイルス対策オプション画面に戻ります。

※ESET Endpoint Security for Androidはバックグランド検査に対応していますので、手動検査（オンライン検査）中に別のタスクを実行することができます。

3.1.3 フォルダーの検査を行う

手動検査（オンデマンド検査）によって、デバイス（Android端末）内の特定のフォルダーの検査を行いたいときは、以下の手順で操作します。

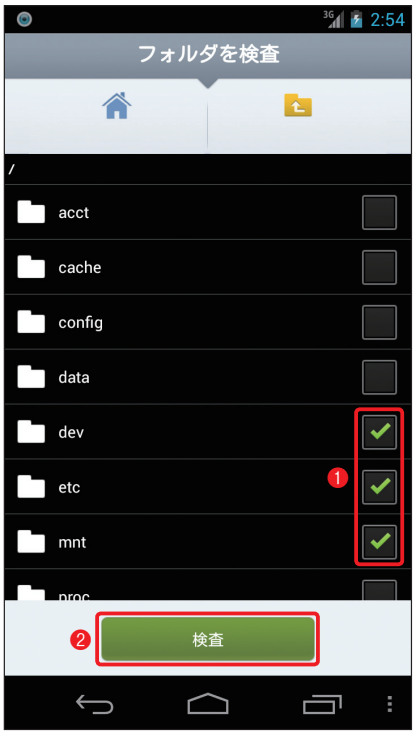
1

［ウイルス対策］をタップします。

2

ウイルス対策オプション画面が開きます。[フォルダを検査] をタップします。

3



❶検査を行いたいフォルダーをタップしてチェックを入れ、❷[検査] をタップします。

4

検査が完了すると、検査結果が表示されます。 をタップすると、フォルダーの検査画面に戻ります。

※ESET Endpoint Security for Androidはバックグランド検査に対応していますので、手動検査（オンライン検査）中に別のタスクを実行することができます。

3.1.4 常駐検査（リアルタイムスキャン）

常駐検査（リアルタイムスキャン）は、ユーザーが操作するファイルをリアルタイムでチェックし、マルウェアや不正なアプリケーションの侵入を阻止する機能です。ウイルス検査オプションの設定画面にある［リアルタイム］の設定で、［リアルタイム保護］がオンに設定されている場合に、この機能が有効になります。既定値は、オンに設定されています。常駐検査（リアルタイムスキャン）で自動的に検査される対象は、SDメモリーカード上のDownloadフォルダー内のファイルとインストールファイル（.apk）内のファイルで、ブラウザーでファイルをダウンロードした時やアプリケーションをインストールした時に検査が実行されます。また、ウイルス検査オプションの設定画面にある［リアルタイム］の設定で［SDカードを検査］をオンに設定している場合は、SDメモリーカードのマウント後、カード上のファイルを自動的に検査します。常駐検査（リアルタイムスキャン）は、システム起動時に自動的に開始されます。

3.1.5 検査ログを閲覧する

手動検査（オンデマンド検査）の結果や常駐検査（リアルタイムスキャン）によって検出されたマルウェアや不正なアプリケーションは、検査ログで確認できます。検査ログは、以下の手順で表示できます。

1 

［ウイルス対策］をタップします。

2

ウイルス対策オプション画面が開きます。[検査ログ] をタップします。

3

[オンデマンドログ] タブが選択された状態で検査ログ画面が表示されます。

POINT

手順3の画面で閲覧したいログをタップすると、ログの詳細な内容が表示されます。

4

[リアルタイムログ] をタップすると、常駐検査（リアルタイムスキャン）によって検出されたマルウェアや不正なアプリケーションが一覧表示されます。

3.1.6 隔離されたファイルを復元する

ここでは、ESET Endpoint Security for Androidでウイルスとして検出後、隔離されたファイルの復元手順を説明します。

1 

[ウイルス対策] をタップします。

2 

[隔離] をタップします。

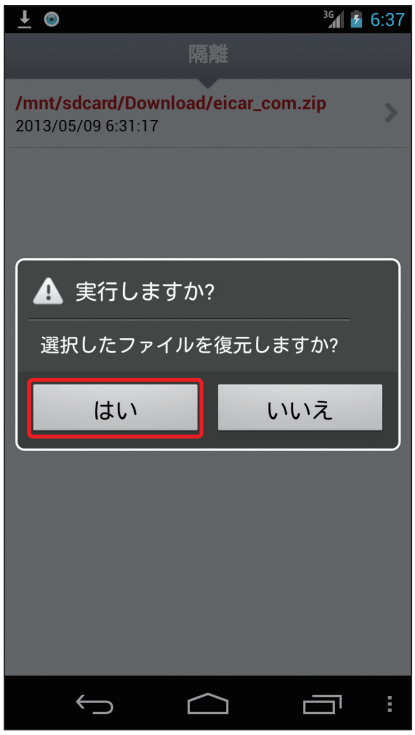
3

隔離されたファイルの一覧が表示されます。復元したいファイルをタップします。

4

ダイアログが表示されます。[復元] をタップします。

5



確認画面が表示されます。[はい] をタップします。

3.2 スパム対策

スパム対策は、SMSの受信や電話の着信／発信を、指定した設定に基いてブロックする機能です。ここでは、スパム対策の設定について説明します。

3.2.1 スパム対策の設定

スパム対策を利用すると、特定のユーザーに対してSMSの受信や電話の発着信を行えるようにできるほか、非通知の着信や電話帳に登録されていない未知の相手からのSMSの受信や電話の発着信をブロックできます。設定は、SMSの受信、電話の着信、発信それぞれで行います。たとえば、SMSは受信するが、電話の発着信はブロックするという設定も行えます。スパム対策は、以下の4項目で設定を行います。なお、スパム対策の設定を行うときは、本書66ページを参考にパスワード保護の設定を行っておくことをお勧めします。

設定項目	内容
電話/SMSルールリスト※	登録した相手からのSMSの受信や電話の発着信をブロックまたは許可するためのリストです。このリストの設定が、もっとも優先度が高い設定となります。たとえば、SMSの受信や電話の発着信を許可する相手をこのリストに登録し、「既知の相手をブロック」の設定をすべてオンにすると、リストに登録した相手からのSMSの受信や電話の発着信のみを許可できます。
非通知の着信をブロック	電話番号の非通知の着信について設定を行います。この設定をオンにすると、電話番号の非通知の着信をブロックします。この設定の既定値はオンに設定されています。
既知の相手をブロック※	電話帳に登録されている既知の相手からの、SMSの受信や電話の発着信のブロックまたは許可の設定を行います。SMS受信、MMS受信、電話の発信、着信の4項目について設定できます。各項目の設定をオンにすると、電話帳に登録されている既知の相手からのSMSの受信や電話の発着信をブロックします。この設定の既定値は、すべての項目がオフに設定されています。特定の相手からのSMSの受信や電話の発着信のみを許可したいときは、その情報を「電話/SMSルールリスト」に登録し、本設定をオンに設定します。逆に特定の相手からのSMSの受信や電話の発着信のみをブロックしたいときは、その情報を「電話/SMSルールリスト」に登録します。
未知の相手をブロック※	電話帳に登録されていない未知の相手からの、SMSの受信や電話の発着信のブロックまたは許可の設定を行います。SMS受信、MMS受信、電話の発信、着信の4項目について設定できます。設定をオンにすると、電話帳に登録されていない未知の相手からのSMSの受信や電話の発着信をブロックします。この設定の既定値は、すべての項目がオフに設定されています。

※MMS受信ブロックは、日本の携帯電話事業者を利用した場合、対応しておりません。

CAUTION

Android端末によってはSMS受信の優先度を設定できるものがあります。これが有効になっている場合、ESET Endpoint Security for AndroidのSMSを利用する機能が利用できなくなる可能性がありますのでESET Endpoint Security for Androidが優先的にSMSを受信できるように設定してください。

3.2.1.1 非通知の着信をブロックする設定を行う

電話番号の非通知の着信に関する設定を行うときは、以下の手順で行います。この設定の既定値は、非通知の着信をブロックする「オン」に設定されています。

1

[スパム対策] をタップします。

2

[設定] をタップします。

3

[非通知の着信をブロック] にチェックを入れると、この機能が「オン」に設定されます。チェックを外すと、この機能が「オフ」に設定され、非通知の着信が許可されます。

3.2.1.2 既知の相手をブロックする設定を行う

電話帳に登録された既知の相手からのSMSの受信や電話の発着信の設定は、以下の手順で行います。この設定の既定値は、SMSの受信や電話の発着信を許可する「オフ」に設定されています。

1 

[スパム対策] をタップします。

2 

[設定] をタップします。

3 

[既知の相手をブロック] をタップします。

4

❶ブロックしたい項目をタップし、チェックを入れます。❷[完了]をタップします。
※MMS受信ブロックは、日本の携帯電話事業者を利用した場合、対応しておりません。

5

既知の相手のブロックが設定され、チェックを入れた項目が「ブロック」と表示されます。

3.2.1.3 未知の相手をブロックする設定を行う

電話帳に登録されていない未知の相手からのSMSの受信や電話の発着信の設定は、以下の手順で行います。この設定の既定値は、SMSの受信や電話の発着信を許可するが「オフ」に設定されています。

1

[スパム対策]をタップします。

2

[設定] をタップします。

3

[未知の相手をブロック] をタップします。

4

❶ブロックしたい項目をタップし、チェックを入れます。❷ [完了] をタップします。

※MMS受信ブロックは、日本の携帯電話事業者を利用した場合、対応しておりません。

5

未知の相手のブロックが設定され、チェックを入れた項目が「ブロック」と表示されます。

3.2.1.4 「電話/SMSルールリスト」に登録する

SMSの受信や電話の発着信のブロックまたは許可をユーザーごとに設定したいときは、「電話/SMSルールリスト」に登録します。この設定は、「既知の相手をブロック」または「未知の相手をブロック」の設定よりも優先されます。また、このリストに登録するユーザーは、電話帳に登録されている必要はありません。「電話/SMSルールリスト」への登録は、以下の手順で行います。

1

[スパム対策] をタップします。

2

[電話/SMSルールリスト] をタップします。

3

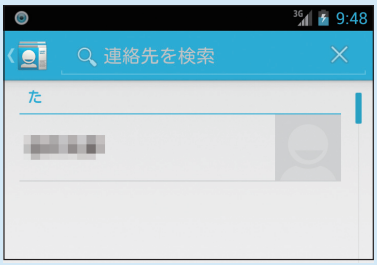
[新規追加] をタップします。

4

ルールリスト項目画面が表示されます。❶ルール名を入力し、❷電話番号を入力します。❸ [SMS受信] をタップします。

※海外の電話番号を登録するときは、国番号付きで入力する必要があります。(例 +01 12 3456 XXXX)

POINT



手順5の画面で ✚ をタップすると、電話帳に登録された情報を利用して電話/SMSルールリストにルールを登録できます。

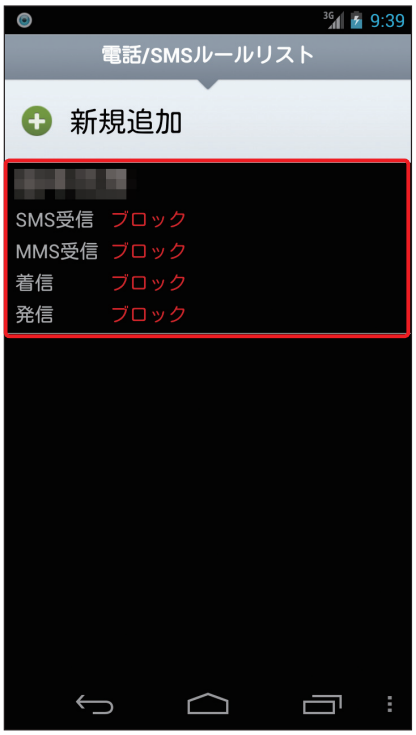
5

SMS受信時の動作をタップして選択します。

6

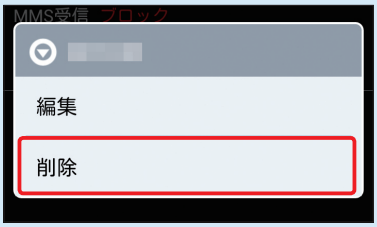
❶[着信]または[発信]をタップし、電話の着信および発進時の動作を手順5を参考に設定します。設定が終わったら、❷[完了]をタップします。
※MMS受信ブロックは、日本の携帯電話事業者を利用した場合、対応しておりません。

7



「電話/SMSルールリスト」に設定が登録されます。

POINT



電話/SMSルールリストに登録したルールを削除したいときは、手順7の画面で削除したいルールを長押し、画面が表示されたら[削除]をタップします。確認画面が表示されるので[はい]をタップします。

3.2.2 スパム対策ログを閲覧する

スパム対策によってブロックされたSMSや電話の発着信履歴を確認したいときは、以下の手順でスパム対策ログを表示します。

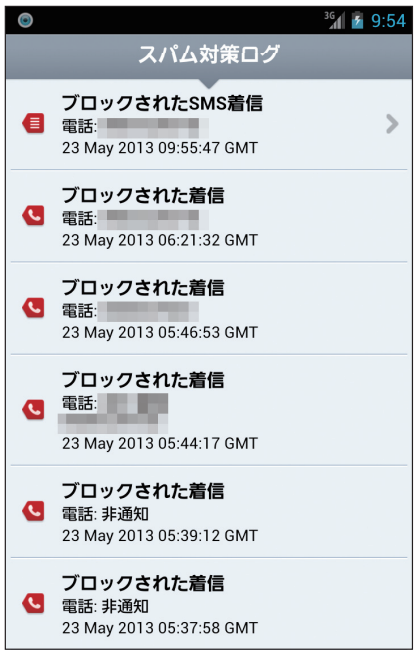
1

[スパム対策] をタップします。

2

[スパム対策ログ] をタップします。

3



スパム対策によってブロックされたSMSや電話の発着信履歴の一覧が表示されます。

POINT

SMSがブロックされた場合は、その履歴をタップするとSMSの内容を確認できます。

3.3 盗難対策

盗難対策は、SIMカードを交換すると携帯電話を使用できないようにロックする機能や、携帯電話からSMSをAndroid端末に送ることで遠隔操作する機能を搭載しています。遠隔操作機能には、Android端末を操作できないようにロックする「リモートロック」、Android端末内のデータおよびセットされているSDメモリーカードのデータをすべて消去する「リモートワイプ」、Android端末のGPS座標を取得する「リモートファインド」の3つがあります。これらの機能は、SIMカードを利用しないAndroid端末ではご利用になれません。

■盗難対策の機能一覧

機能	概要
信頼するSIMカード(SIMカードのチェック機能)	この機能は、事前に信頼するSIMカードの情報を登録しておき、それ以外のSIMカードが携帯電話にセットされると、携帯電話が利用できないようにロックする機能です。その際、警告SMSが管理者登録されている携帯電話に送信されます。また、この警告SMSには、現在セットされているSIMカードの電話番号、IMSI番号(ユーザー固有番号)、IMEI番号(電話固有の番号)が含まれます。
リモートロック	この機能は、SMSを送信できる端末からSMSを送信することで、Android端末を使用できないように遠隔操作でロックする機能です。
リモートワイプ	この機能は、SMSを送信できる端末からSMSを送信することで、Android端末内のデータおよびセットされているSDメモリーカードなどのリムーバブルメディアに記録されたデータを遠隔操作ですべて消去する機能です。
リモートファインド	この機能は、SMSを送信できる端末からSMSを送信することで、Android端末のGPS座標をSMSによって遠隔操作で取得する機能です。

CAUTION

Android端末によってはSMS受信の優先度を設定できるものがあります。これが有効になっている場合、ESET Endpoint Security for AndroidのSMSを利用する機能が利用できなくなる可能性がありますのでESET Endpoint Security for Androidが優先的にSMSを受信できるように設定してください。

3.3.1 盗難対策の設定

盗難対策の機能をすべて利用するには、利用を許可するSIMカードの情報（信頼するSIMカードの登録）や管理者の連絡先を事前に登録する必要があります。SMSコマンドを利用してのリモートロック、リモートワイプ、リモートファインドを利用する場合は信頼するSIMカードや管理者連絡先を登録する必要はありません。SIMカードの情報や管理者の連絡先は、本書16ページを参考に初期設定を行うときに登録し、SMSを利用した遠隔操作機能も有効に設定されます。これらの設定は、後から追加したり、機能の有効／無効を切り替えられます。

3.3.1.1 信頼するSIMカードの情報を登録／追加する

信頼するSIMカードの情報を登録／追加するときは、以下の手順で行います。信頼するSIMカードの登録には、「IMSI（International Mobile Subscriber Identity）」と呼ばれるSIMカード固有の情報の入力が必要となります。この情報はSIMカードに保存されていますので登録したいSIMカードのIMSIを確認の上、登録してください。また登録したいSIMカードをAndroid端末にセットしてから作業を行う場合、本書18ページの手順を参考に「SIM照合有効」のチェックを外してから作業を行うとスムーズに登録を行えます。

1 

［盗難対策］をタップします。

2 

盗難対策オプション画面が開きます。［信頼するSIMカード］をタップします。

3 本書19ページからの⑨～⑫の手順をご参照ください。

POINT

登録されているSIMカードの情報を削除したいときは、削除したい情報を長押しして、画面が表示されたら[削除] をタップします。確認画面が表示されるので、[はい] をタップします。

3.3.1.2 管理者連絡先を登録／追加する

ESET Endpoint Security for Androidで設定したセキュリティパスワードをSMSを利用してリセットを行うには、[管理者連絡先] を事前に登録しておく必要があります。パスワードリセットは、管理者連絡先に登録された電話番号でのみ行えます。また、[SIM照合] を有効にした場合、[信頼するSIMカード] に登録されていない別のSIMカードに差し替えられると管理者連絡先に登録された電話番号に警告SMSが送信されます。管理者連絡先は、複数登録できます。管理者連絡先（電話番号）の登録／追加は、以下の手順で行います。

1 

[盗難対策] をタップします。

2 

盗難対策オプション画面が開きます。[管理者連絡先] をタップします。

3 本書22ページからの⑳～㉒の手順をご参照ください。

3.3.1.3 SIM照合の有効／無効を設定する

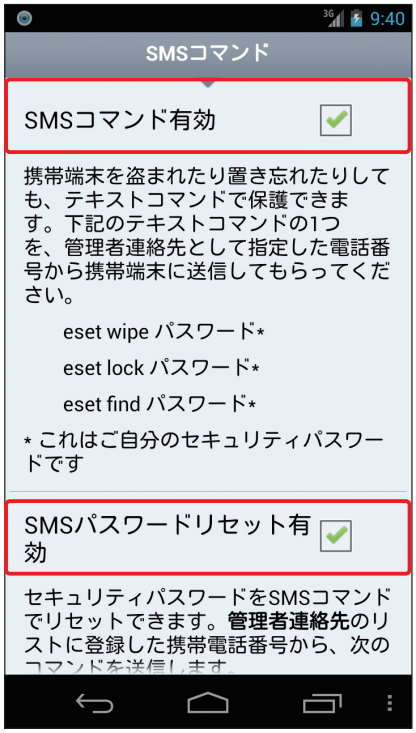
未登録のSIMカードをセットしたときに、Android端末をロックする機能であるSIM照合有効／無効の切り替えは、盗難対策の設定画面で行います。「SIM照合有効」にチェックを入れるとこの機能が有効になり、外すと無効になります。「SMS警告テキスト」は、未登録のSIMカードをセットしたときに、管理者連絡先に送信される警告SMSのメッセージです。

※空欄には警告SMSを受け取った人が連絡するためのメールアドレスを入力してください。

CAUTION

SMSの本文に全角文字（2Byte）を使用すると日本の携帯電話事業者の制限によりSMSで送信できる文字数が大幅に減り、警告SMSが送信できなくなります。そのため、SMS警告テキストの空欄には半角英数字および半角記号でメールアドレスを入力してください。

3.3.1.4 SMSによる遠隔操作の有効／無効を設定する



SMSによる遠隔操作の有効／無効の切り替えは、盗難対策のSMSコマンド画面で行います。「SMSコマンド有効」にチェックを入れると、SMSを利用した遠隔操作が有効になり、外すと無効になります。「SMSパスワードリセット有効」にチェックを入れると、管理者連絡先に登録された携帯電話からSMSを利用してセキュリティパスワードをリセットできます。セキュリティパスワードとは、本プログラムの設定を変更できないように保護するためのパスワードでSMSコマンドにも利用します。詳細については、本書66ページをご参照ください。

3.3.2 SMSコマンドの利用法

Android端末の遠隔操作を行うときは、SMSを送信できる端末から以下のようなテキストコマンドを本文としたSMSを送信します。なお、テキストコマンドの最後につけるパスワードは、本書20ページで登録したセキュリティパスワードを入力します。メッセージの入力は半角英数字、スペースも半角で一度だけ入力してください。また、大文字と小文字も区別しますので設定したパスワードを正確に入力してください。
なお、セキュリティパスワードのリセットのみ、管理者連絡先に登録した携帯電話からのSMSの送信が必要となります。

リモートロック

Android端末にロックをかけます。
テキストコマンド:eset lock パスワード

リモートワイプ

Android端末本体のデータおよびSDカードのデータを消去します。
テキストコマンド:eset wipe パスワード

リモートファインド

Android端末の位置情報を取得します。Android端末の位置情報サービス(GPS機能)がオンに設定していないと利用できません。
テキストコマンド:eset find パスワード

セキュリティパスワードのリセット

セキュリティパスワードをリセットします。こちらは管理者連絡先に登録した携帯電話からテキストコマンドを送信する必要があります。
テキストコマンド:eset remote reset

3.4 セキュリティ監査

セキュリティ監査は、バッテリー残量、インストールしたアプリケーション、ディスクの空き容量などの状態をチェックし、問題があれば警告を表示する機能です。ここでは、セキュリティ監査の設定や使い方について説明します。

3.4.1 セキュリティ監査の設定

セキュリティ監査では、監査を行う項目をユーザーが選択できます。また、セキュリティ監査は、定期的に実行するように既定値で設定されており、実行間隔を選択できます。警告を表示するバッテリーの残量やディスクの空き容量のしきい値は、ユーザーが自由に設定できます。セキュリティ監査の設定は、以下の手順で行います。

1 

[セキュリティ監査] をタップします。

2 

セキュリティ監査オプション画面が開きます。[設定] をタップします。

3

「メイン」タブが選択された状態で設定画面が開きます。「メイン」タブでは、セキュリティ監査を行う間隔やログの保存、空き記録容量のしきい値やバッテリーレベルのしきい値などに関する設定が行えます。設定項目の詳細については、下のコラムをご参照ください。

4

[監査する項目] をタップすると、監査を行う項目を設定できます。既定値では、すべての項目の監査が有効になっています。チェックを外すとその項目を監査の対象外に設定できます。

コラム

「メイン」タブの設定について

「メイン」タブでは、以下の項目について設定を行えます。

項目	内容
定期的に監査	この項目にチェックを入れオンに設定すると、セキュリティ監査を定期的に実行します。定期的な監査を行いたくないときは、この項目のチェックを外します。また、監査を行う間隔は、「監査間隔」で設定します。この項目の既定値は、オンです。
自動的に修正	この項目にチェックを入れオンにすると、監査でリスクのある項目を検出したときにユーザーとのやり取りを行うことなく、本製品が自動的に検出した項目の修正を行います。この設定は、定期的な監査にのみ適用されます。この項目の既定値は、オフです。
ログの保存	監査ログの最大保存個数を設定します。既定値では、ログの保存個数が「20」に設定されています。
監査間隔	監査を実行する間隔を設定します。既定値では、「24時間」ごとに監査を実行するように設定されています。この設定は、「定期的に監査」がオンに設定されている場合に、有効な設定です。
空き記憶容量しきい値	空き記憶容量が少ないと判断するためのしきい値を全容量の「%」単位で指定します。空き記憶容量がここで指定した容量よりも少なくなると警告が表示されます。既定値では、「10%」が設定されています。
バッテリーレベルしきい値	バッテリー残量が少ないと判断するためのしきい値を「%」単位で指定します。バッテリーの残量がここで指定した容量よりも少なくなると警告が表示されます。既定値では、「20%」が設定されています。

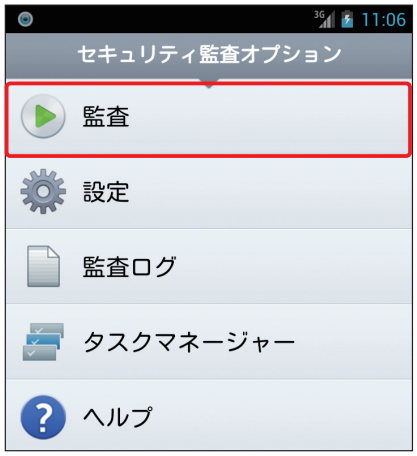
3.4.2 セキュリティ監査を手動で実行する

セキュリティ監査は、指定した間隔で自動的に実行できるほか、必要に応じて手動で実行することもできます。セキュリティ監査の手動実行は、以下の手順で行います。

1

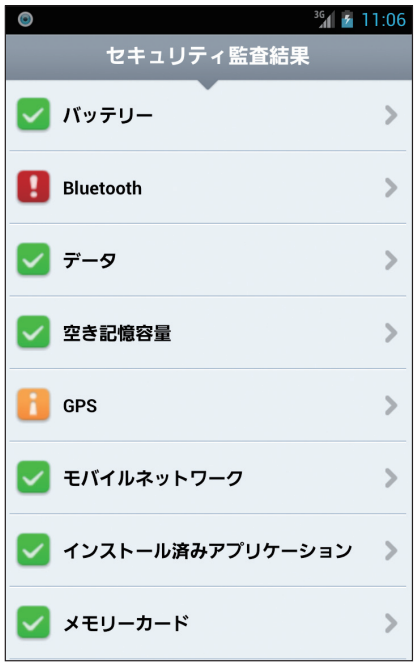
[セキュリティ監査] をタップします。

2



セキュリティ監査オプション画面が開きます。[監査] をタップします。

3



セキュリティ監査が実施され、監査結果が表示されます。

POINT

セキュリティ監査に問題がない項目には、アイコンが付き、セキュリティリスクが存在する可能性がある項目には、アイコンが付きます。また、修正の必要があるセキュリティリスクが見つかった項目には、アイコンが付きます。アイコンが付いた項目の修正を行いたいときは、その項目をタップします。詳細な監査結果が表示されるので、項目名をタップします。確認画面が表示されるので、[はい] をタップします。

3.4.3 監査ログを確認する

セキュリティ監査のログを閲覧したいときは、以下の手順で行います。

1 

[セキュリティ監査] をタップします。

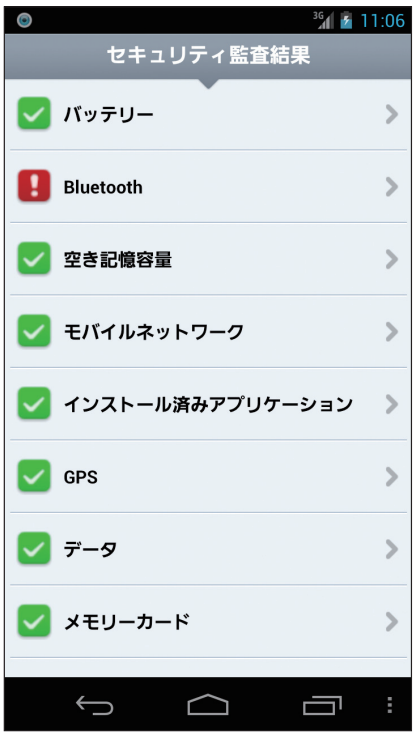
2 

セキュリティ監査オプション画面が開きます。[監査ログ] をタップします。

3 

セキュリティ監査のログが表示されます。ログの詳細を閲覧したいときは、そのログをタップします。

4



選択したログの詳細が表示されます。

POINT

セキュリティに問題がない項目には、アイコンが付きます。また、リスクが見つかった項目には、アイコンが付きます。監査結果の詳細な内容を確認したいときは、その項目をタップします。

3.4.4 タスクマネージャー

タスクマネージャーを利用すると、Android端末で動作しているすべてのプロセス、サービス、タスクを確認できます。また、本プログラムを使ってシステムで実行されていないプロセスやサービス、タスクを停止することもできます。タスクマネージャーは、以下の手順で利用できます。

1

[セキュリティ監査] をタップします。

2

セキュリティ監査オプション画面が開きます。[タスクマネージャー] をタップします。

3

「プロセス」タブを選択した状態でタスクマネージャーが開き、実行中のすべてのプロセスが表示されます。

4

［サービス］をタップすると、実行中のすべてのサービスが表示されます。

5

［タスク］をタップすると、実行中のすべてのタスクが表示されます。

コラム

プロセス／サービス／タスクを停止するには

タスクマネージャーに表示されたプロセス／サービス／タスクの内、停止可能なプロセス／サービス／タスクには✖アイコンが付けられています。これらのプロセス／サービス／タスクを停止したいときは、停止したい項目をタップし、確認画面が表示されたら［はい］をタップします。

3.5 ウイルス定義データベースのアップデート

悪意のあるプログラムは日々増加しているため、本プログラムをインストールしたAndroid端末を常に安全な環境で利用するには、ウイルス定義データベースのアップデートが欠かせません。本プログラムは、ユーザーが指定した間隔で定期的にウイルス定義データベースのアップデートが行えるほか、手動でウイルス定義データベースのアップデートを行えます。ただし、本プログラムのウイルス定義データベースは、PC向けのウイルス定義データベースとは互換性がありません。そのため、社内に設置したミラーサーバーに設置してウイルス定義データベースのアップデートを行うことはできません。

3.5.1 アップデート間隔を設定する

本プログラムは、本書16ページの手順で初期設定を行うと、既定値では1日に1回ウイルス定義データベースのアップデートを自動的に行うように設定されます。この設定は、ユーザーが自由に変更できます。ウイルス定義データベースのアップデート間隔を設定するときは、以下の手順で行います。なお、ウイルス定義データベースのアップデートは、インターネット接続環境が必要です。Wi-Fi接続中以外の環境でアップデートを行うと、パケット料金がかかりますのでご注意ください。

1 

[アップデート] をタップします。

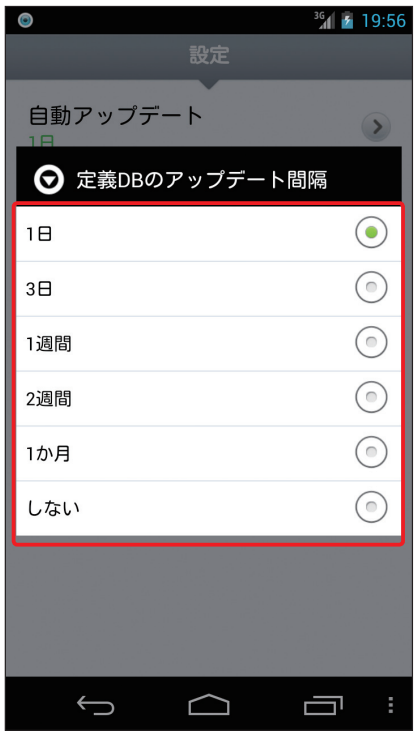
2

アップデートオプション画面が開きます。[設定] をタップします。

3

[自動アップデート] をタップします。

4



設定したいアップデート間隔をタップします。

▸▸▸ POINT

アップデート間隔を長く設定すると、長期間ウイルス定義データベースがアップデートされないためウイルス感染のリスクが高くなります。そのため、短めのアップデート間隔の設定を推奨します。

3.5.2 手動でアップデートを行う

ウイルス定義データベースのアップデートは、指定した間隔で自動アップデートが行えるほか、任意のタイミングで手動でアップデートを行えます。手動アップデートは、以下の手順で行います。

1 

[アップデート] をタップします。

2 

アップデートオプション画面が開きます。[今すぐアップデート] をタップします。

3 

ウイルス定義データベースのアップデートが実施されます。アップデートが完了すると手順2の画面に戻ります。

3.6 パスワード

パスワードを設定すると、本プログラムの各種設定をパスワードで保護できます。パスワードは、「セキュリティパスワード」とも呼ばれ、盗難対策のSMSを利用した遠隔操作を行うときにも利用されます。セキュリティを向上させるためにも、忘れずにパスワードを設定しておいてください。

3.6.1 パスワードや保護項目を変更するには

設定済みのパスワードを変更したり、パスワードで保護する設定項目を変更したいときは、以下の手順で行います。

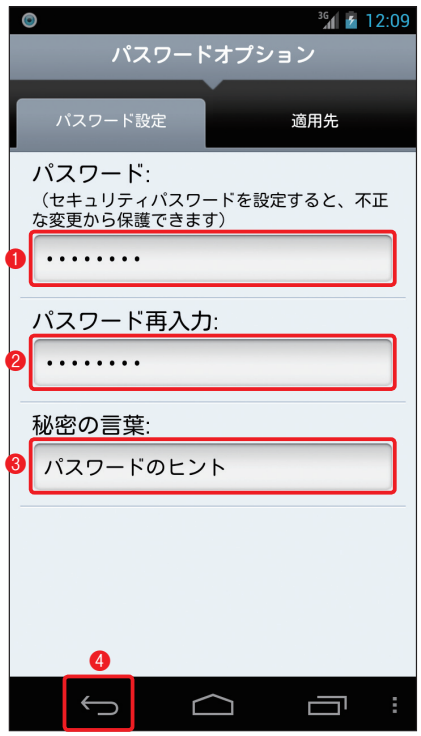
1 

[パスワード] をタップします。

2 

セキュリティパスワード入力画面が開きます。❶パスワードを入力し、❷ [ロック解除] をタップします。

3



「パスワード設定」タブを選択した状態でパスワードオプション画面が表示されます。パスワードを変更したいときは、❶新しいパスワードを入力し、❷“❶”で入力したパスワードを再入力します。❸秘密の言葉を入力します。❹設定を終えるときは、⮌をタップします。

4

パスワードで保護したい設定を変更したいときは、❶［適用先］をタップし、❷適用したい項目にチェックを入れます。❸設定を終えるときは、⮌をタップします。

3.6.2 パスワードをリセットするには

設定したパスワードがわからなくなったときは、パスワードをリセットする必要があります。パスワードをリセットするには、SMSを利用する方法、ERAを利用して設定を書き換える方法、パスワードリセット申請を利用する方法の3種類があります。

3.6.2.1 SMSでパスワードをリセットする

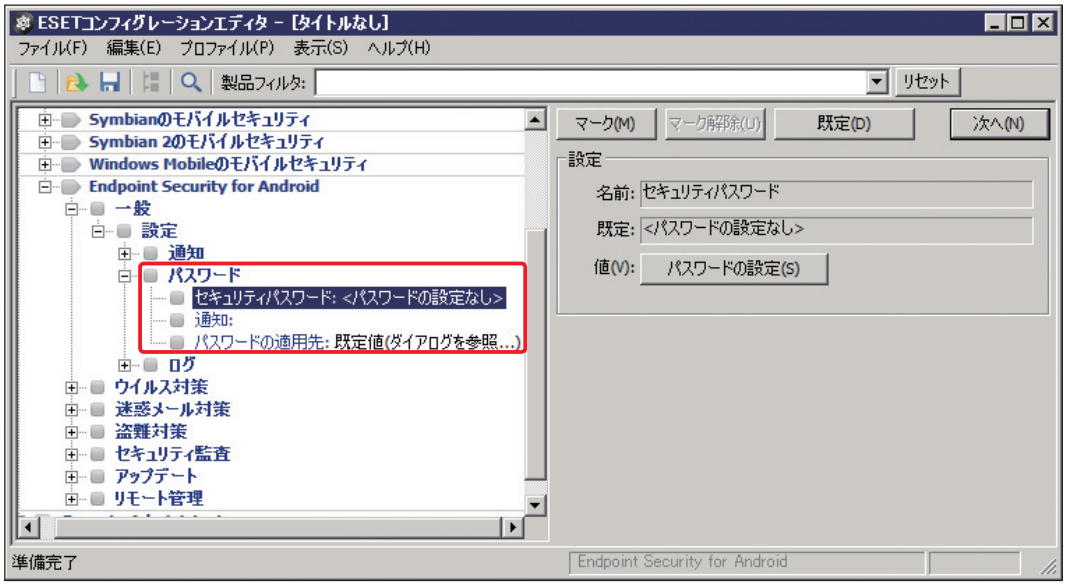
SMSでパスワードをリセットするには、盗難対策の設定で管理者連絡先に設定された携帯電話から以下のSMSを送信します。盗難対策の設定の詳細については、本書51ページを参照してください。

セキュリティパスワードのリセット

eset remote reset

3.6.2.2 ERAでパスワードを書き換える

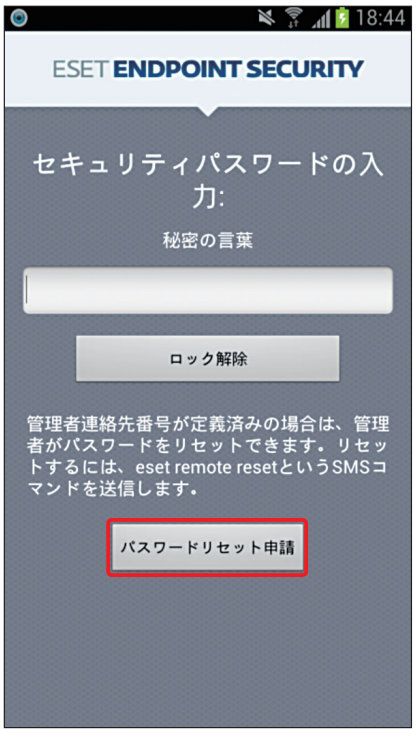
ERAを利用してパスワードを書き換えるときは、ERAでコンフィグレーションタスクを作成し、その設定をAndroid端末に配布します。ERAを利用したコンフィグレーションタスクの配布方法は、「ESET Remote Administrator ユーザーズマニュアル」をご参照ください。また、Android端末にERAでコンフィグレーションタスクを配布するには、「リモート管理」の設定が有効になっている必要があります。Android端末のリモート管理の設定については、本書73ページをご参照ください。



3.6.2.3 パスワードリセット申請を行う

パスワードのリセットは、パスワードのリセット申請でも行えます。パスワードのリセット申請を行うと、ライセンスを購入したときに登録したメールアドレスにロック解除コードが記載されたメールが送信されますので、ロック解除コードを利用してパスワードのリセットを行います。パスワードリセット申請は、以下の手順で行います。

1



パスワードの入力画面でパスワードの入力を4回ミスしたとき、左の画面が表示されますので[パスワードリセット申請]をタップします。
※パスワードのリセット申請は、Android端末が直接インターネットに接続できる環境が必要です。

2

パスワードリセット申請が終了すると左の画面に切り替わります。

3 メールでロック解除コードが送信されます。指示に従ってパスワードをリセットします。

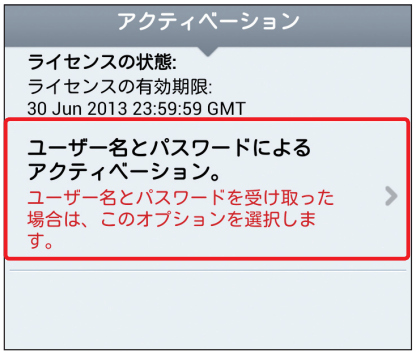
3.7 アクティベーション

本プログラムの利用には、アクティベーションが必要です。アクティベーションには、ユーザー名とパスワードが必要になります。アクティベーションは、以下の手順で行います。

1

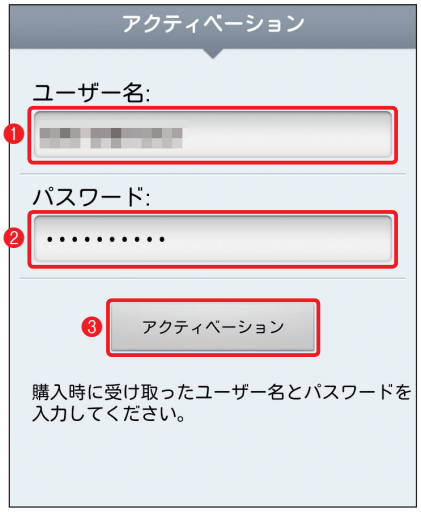
[アクティベーション] をタップします。

2



アクティベーション画面が開きます。[ユーザー名とパスワードによるアクティベーション。] をタップします。

3



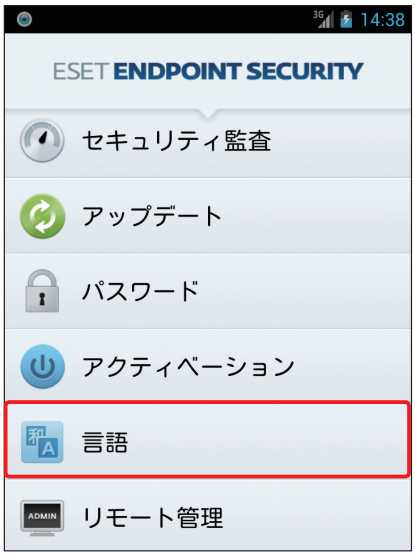
❶ユーザー名を入力し、❷パスワードを入力します。❸ [アクティベーション] をタップします。

※アクティベーションには、Android端末が直接インターネットに接続できる環境が必要です。

3.8 言語の設定

本プログラムは、言語の設定を変更することで他国の言語で利用できます。使用する言語は、以下の手順で変更できます。

1



[言語] をタップします。

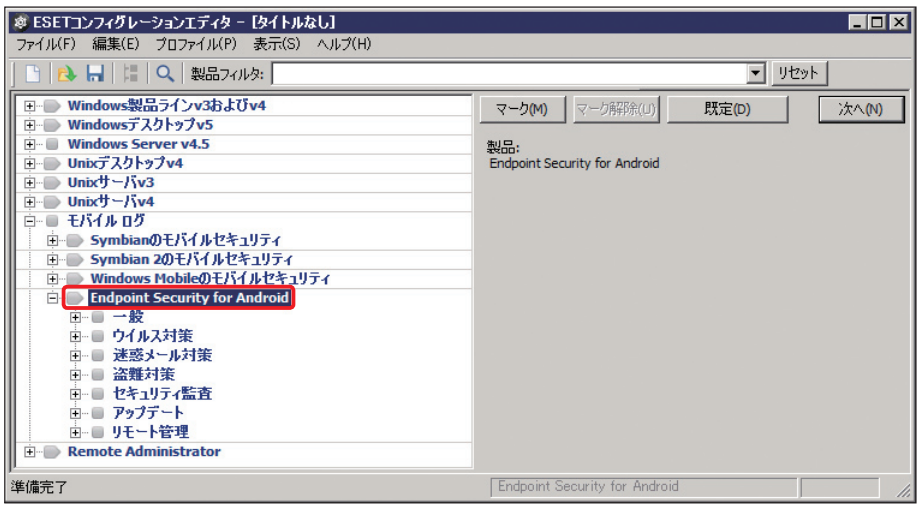
2

言語画面が開きます。❶使用したい言語をタップして選択します。❷ をタップします。

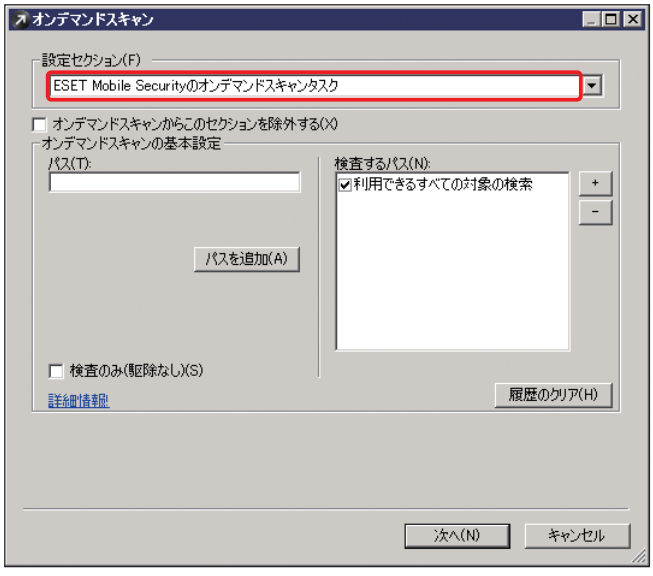
3.9 リモート管理

ESET Endpoint Security for Androidは、ERAを利用することでリモート管理を行えます。リモート管理の設定を行うと、ESET Endpoint Security for Androidの設定をリモート操作で変更したり、オンデマンドスキャンやウイルス定義データベースのアップデートなどのタスクをリモート操作で実施できます。ERAを利用したリモート管理の詳細については、ESET Remote Administrator ユーザーズマニュアルをご参照ください。なお、ERAのリモート管理でESET Endpoint Security for Androidの設定の変更を行うときは、ESET コンフィグレーションエディターで「Endpoint Security for Android」の項目を編集します。また、オンデマンドスキャンやウイルス定義データベースのアップデートなどのタスクの実施する場合は、「ESET Mobile Security」のタスクを選択します。

設定を変更する場合に利用する項目



オンデマンドスキャンなどを行う場合に選択する項目



3.9.1 リモート管理の設定

ERAでESET Endpoint Security for Androidをリモート管理するには、ERAへの接続設定を行う必要があります。ERAへの接続設定は、以下の手順で行います。

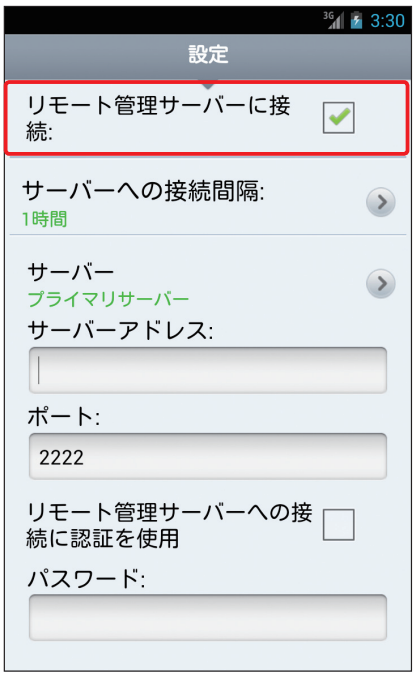
1

[リモート管理] をタップします。

2

ERAのオプション画面が開きます。[設定] をタップします

3

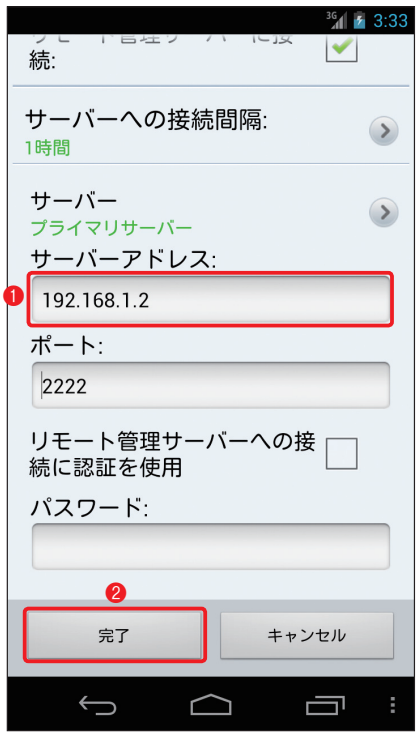


[リモート管理サーバーに接続] をタップしてチェックを入れます。

POINT

[サーバーへの接続間隔] をタップすると、ERAに自動接続する間隔を設定できます。この設定の既定値は、「1時間」が設定されています。

4



❶サーバーアドレスにリモート管理サーバーのアドレスを入力し、❷[完了]をタップします。

※リモート管理サーバーとの接続構成については「ユーザーズガイド 導入・運用編」をご参照ください。

POINT

本プログラムでは、プライマリサーバーとセカンダリサーバーの2台のサーバーへの接続設定を行えます。既定値では、プライマリサーバーが選択されていますが、[サーバー]をタップすると、セカンダリサーバーの設定を行えます。また、リモート管理サーバーへの接続にパスワード認証が設定されているときは、[リモート管理サーバーへの接続に認証を使用]にチェックを入れ、パスワード欄にパスワードを入力します。

3.9.2 リモート管理サーバーに手動で接続する

リモート管理サーバーへの接続は、指定した間隔での自動接続のほか、手動で接続することもできます。手動で接続を行うときは、以下の手順で行います。

1

[リモート管理]をタップします。

2

ERAのオプション画面が開きます。[ERAに接続]をタップします。

3.10 サポート

ESET Endpoint Security for Androidには、お客様からのお問い合わせの際にサポート対応を迅速にするためにバージョン情報の確認や動作ログの取得機能などが搭載されています。

3.10.1 バージョン情報の確認

サポートセンターへのご質問の際に本プログラムのバージョン情報が、必要になる場合があります。バージョン情報の確認は、以下の手順で行います。

1

Android端末の取扱説明書を参考にメニューボタンをタップし、メニューが表示されたら [バージョン情報] をタップします。

2

バージョン情報が表示されます。
※ESET Endpoint Security for Androidのバージョンの他に、ライセンスの有効期限、ウイルス定義データベースのバージョンと前回のアップデートの時間が確認できます。

3.10.2 ログ設定

サポートセンターへのご質問の際に本プログラムの動作ログが必要になる場合があります。弊社カスタマーサポートから動作ログ取得の要望があった場合は、以下の手順で動作ログの取得設定を行ってください。

1

Android端末の取扱説明書を参考にメニューボタンをタップし、メニューが表示されたら [ログ設定] をタップします。

2

設定画面が表示されます。❶取得したいログをタップしてチェックを入れます。❷をタップすると設定が保存され基本画面に戻ります。

3.10.3 カスタマーサポート

弊社カスタマーサポートから動作ログ提出の要望があった場合は、以下の手順でリクエストフォームから動作ログの送信を行います。なお、リクエストフォームは、弊社カスタマーサポートから要求があった場合のみご利用ください。

1

Android端末の取扱説明書を参考にメニューボタンをタップし、メニューが表示されたら［カスタマーサポート］をタップします。

2

サポートリクエストフォームが表示されます。必要な情報を入力し、［送信］をタップするとカスタマーサポートにメールが送信されます。

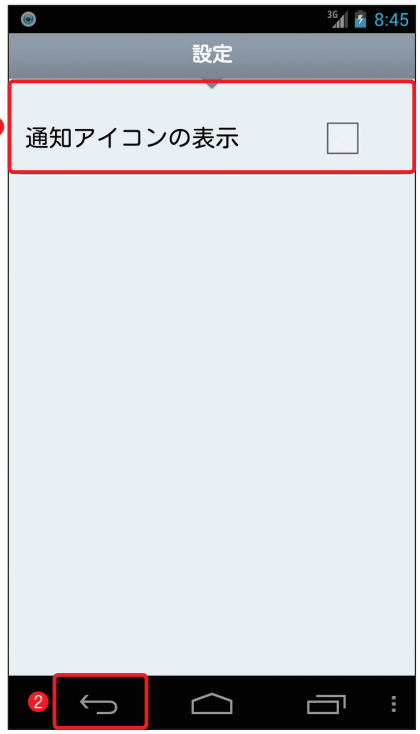
3.10.4 通知

ESET Endpoint Security for Androidをインストールすると、ステータスバーにアイコンが表示されます。このアイコンを表示したくないときは、以下の手順で設定を変更します。

1

Android端末の取扱説明書を参考にメニューボタンをタップし、メニューが表示されたら [通知] をタップします。

2



❶ [通知アイコンの表示] をタップしてチェックを外します。❷ をタップすると設定が保存され基本画面に戻ります。