# ESET Endpoint Security for Android
# ユーザーズマニュアル

■お断り

○ 本マニュアルは、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記載されている機能が異なる場合があります。また、本マニュアルの内容は、改訂などにより予告なく変更することがあります。



○ ESET、ESET Endpoint Security、ESET Endpoint アンチウイルス、ESET File Security、ESET Remote Administratorは、ESET, spol. s r.o.の商標です。

○ Microsoft、Windows、Windows Server、Internet Explorer、Active Directoryは、米国Microsoft Corporationの米国、日本およびその他の国における登録商標または商標です。

○ Mac、Mac OS、OS X、Finderは、米国およびその他の国で登録されているApple Inc.の商標です。

改定日　2017/4/30

# 目　次

# Chapter 1 ESET Endpoint Security for Android について

この章では、ESET Endpoint Security for Android の特徴について説明しています。

## 1.1 ESET Endpoint Security for Android の特徴

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 デバイス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 デバイスを管理でき、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。
また、ESET Endpoint Security for Android は、ESET Remote Administrator 経由でのリモート管理が必要ではない中小企業でも適用でき、自分の ESET Endpoint Security for Android の設定を他のユーザーと共有できます。このプロセスにより、ESET Endpoint Security for Android のインストール直後に必要な製品のアクティベーションと各製品モジュールの手動セットアップが不要になります。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。また、Android デバイスが完全に充電され、充電器に接続している場合に検査を実施したり、指定日時などスケジュールされた検査を行ったりすることもできます。

### ■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／発信をブロックできます。この機能には、管理者ルールとユーザールールという 2 種類のルールがあり、管理者ルールが常に優先されます。また、ユーザーまたは管理者が指定した時間の間に受信した通話とメッセージをブロックできます。最後の発信元またはメッセージ送信者、電話番号、連絡先グループ、非表示または不明な番号をワンタッチでブロックできます。

### ■アンチセフト（盗難対策）

Android デバイスが紛失または盗難にあった場合に、管理者がデバイスを保護して検索できます。Android デバイスのロック、ロック解除、ワイプ、拡張初期設定リセット、警報、検索などのアンチセフト処理がリモートで行えます。アンチセフト処理は、ERA サーバーまたは SMS によるリモートコマンドによって実行できます。

### ■アプリケーション制御

アプリケーション制御を使用すると、管理者は、インストール済みアプリケーションを監視し、定義済みアプリケーションへのアクセスをブロックして、特定のアプリケーションをアンインストールするようにユーザーに通知してリスクを低減できます。

### ■デバイスセキュリティ

デバイスセキュリティでは、管理者が、複数のモバイルデバイスを対象に基本セキュリティポリシーを実行できます。例えば、管理者は次のことができます。

- 画面ロックコードの最低セキュリティレベルと複雑さを設定
- ロック解除の試行失敗が許可される最大回数を設定
- ユーザーが現在の画面ロックコード使用できる期間を設定

- ロック画面タイマーを設定
- カメラの使用を制限

### ■フィッシング対策

ユーザーがサポートされている Web ブラウザ（既定の Android ブラウザと Chrome）を使用するときに、ユーザーが悪意のある Web サイトにアクセスしないように保護します。Android デバイスが、URL にアクセスしようとすると、Anti-Phishing 技術によってその URL が既知のフィッシング詐欺サイトとして登録されていないかを ESET データベースと比較します。一致する場合、URL への接続は中断され、警告メッセージが表示されます。

### ■通知センター

ESET Endpoint Security for Android には統合された通知センターが搭載されています。ユーザーは、通知センターで注意が必要なアプリケーション機能に関するすべての通知を確認できます。通知センターは、各種イベント、企業ポリシーに準拠していない理由、これらの要件を満たすために必要な操作に関する情報を示します。通知は優先度に従って表示され、優先度が高い通知がリストの最上位に表示されます。

### ■設定のインポート / エクスポート

設定のインポート / エクスポートを行えます。管理者は手動で Android デバイスの設定をファイルにエクスポートし、エクスポートした設定ファイルを、電子メールなどを利用して共有することで任意の Android デバイスにインポートできます。ユーザーが受信した設定ファイルをインポートすると、設定が自動的に定義され、設定ファイルにライセンス情報が含まれている場合は、アプリケーションがアクティベートされます。設定は管理者パスワードによって保護されます。

※設定ファイルには、ESET Remote Administrator への接続情報は含まれません。

### ■ローカル管理

ESET Remote Administrator を使用しない場合、管理者は Android デバイスをローカルでセットアップして管理できます。また、すべてのアプリケーション設定は管理者パスワードによって保護されているため、常にアプリケーションを完全に制御できます。

### ■リモート管理

ウイルス対策、SMS と電話フィルタ、デバイスセキュリティの設定からアプリケーション制御制限まで、すべてのアプリケーション設定を ESET Remote Administrator を利用したリモートポリシー経由で構成および設定できます。これによって、管理者は、モバイルデバイスを含むネットワーク全体で、企業セキュリティポリシーを適用できます。

## 1.2 システム要件

ESET Endpoint Security for Android は、Android デバイス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。

https://eset-info.canon-its.jp/business/endpoint_protection_adv/spec.html

# Chapter 2 インストールについて

この章では、ESET Endpoint Security for Android のインストールについて説明しています。

## 2.1 ESET Endpoint Security for Android のインストール

ESET Endpoint Security for Android のインストールは、リモートインストールとローカルインストールの 2 つの方法で実行できます。

### 2.1.1 リモートインストールについて

ESET Endpoint Security for Android は、ESET Remote Administrator を利用したリモートインストールが行えます。リモートインストールを行うには、次の要件を満たしている必要があります。

- Mobile Device Connector のインストール
- ESET Remote Administrator 上でのモバイルデバイス登録

**ワンポイント**

Mobile Device Connector のインストールやモバイルデバイス登録の詳細については、「ESET Remote Administrator ユーザーズマニュアル」をご参照ください。

### 2.1.2 イントールの方法

ESET Endpoint Security for Android のインストールは、次の 2 つの方法で実行できます。

- 電子メールを利用したインストール
- ローカルインストール

**! 重 要**

ESET Endpoint Security for Android V1 がインストールされている場合、上書きインストールはできないため、事前にアンインストールしておく必要があります。

### 2.1.3 リモートインストールの方法

ESET Endpoint Security for Android のリモートインストールは、次の 2 つの方法で実行できます。

1. 管理者は、登録リンク、インストール APK ファイル、インストール手順の簡単な説明を電子メールでエンドユーザーに送信します。エンドユーザーが、受け取った電子メールに記載されている登録リンクをタップすると、Android デバイスの既定のインターネットブラウザに移動します。ESET Endpoint Security for Android が登録され、ESET Remote Administrator に移動します。ESET Endpoint Security for Android がデバイスにインストールされていない場合、自動的に Google Play Store に移動するため、アプリケーションをダウンロードします。その後、標準インストールが実行されます。ESET Endpoint Security for Android のアクティベーションは、ERA サーバーからリモート操作で行います。

2. 管理者は、アプリケーション設定ファイル、インストール APK ファイル、インストール手順の簡単な説明を電子メールでエンドユーザーに送信します。インストール APK ファイルは、ユーザーが Google Play Store からダウンロードすることもできます。各種ダウンロードリンクは、管理者が提供します。インストール後、ユーザーがアプリケーション設定ファイルを開きます。設定がインポートされ、設定ファイルにライセンス情報が含まれている場合は、アプリケーションがアクティベートされます。
※設定ファイルには、ESET Remote Administrator への接続情報は含まれません。

### 2.1.4 ローカルインストール

ERA サーバーによる管理を必要としない場合、管理者は ESET Endpoint Security for Android をローカルでセットアップして管理できます。すべてのアプリケーション設定は管理者パスワードによって保護できるため、常にアプリケーションを完全に管理制御できます。また、ESET Remote Administrator を利用しない場合にローカルで管理するための 2 つのオプションを用意しています。

1.Android デバイスを一台ずつ手動で設定します。

2. 設定ファイルを利用した各種設定の共有を行えます。管理者は、ESET Endpoint Security for Android をインストールした任意の Android デバイスから設定をファイルにエクスポートし、エクスポートした設定ファイルを電子メールなどを利用して他のユーザーに配布します。ユーザーは、受信した設定ファイルを開き許可を行うと、設定が自動的にインポートされ、ライセンス情報が含まれている場合は、アプリケーションがアクティベートされます。また、設定は管理者パスワードによって保護できます。ローカルインストールを行うときは、ユーザーズサイトまたは Google Play Store からインストール APK ファイルをダウンロードしてインストールを行います。

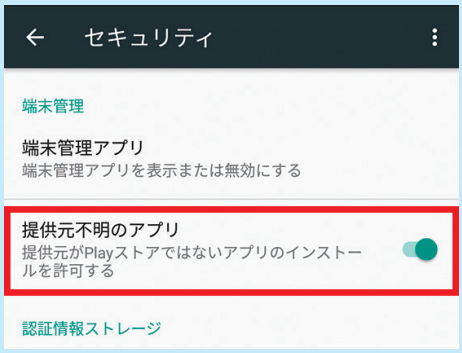
**ワンポイント**
設定のインポートとエクスポートの詳細については、「9.1 設定のインポート / エクスポート」をご参照ください。

#### 2.1.4.1 ユーザーズサイトからダウンロード

ユーザーズサイトより ESET Endpoint Security for Android をダウンロードします。不明なソースまたは提供元不明のアプリのインストールが許可されていることを確認してください。

ユーザーズサイト URL：http://canon-its.jp/product/eset/users/

**ワンポイント**
不明なソースまたは提供元不明のアプリのインストールが許可されているかどうかの確認は、ホーム画面のランチャーアイコンをタップするか、[ホーム] > [メニュー] に移動して「設定」画面を開きます。続いて、[セキュリティ] をタップし、[不明なソース] または [提供元不明のアプリ] オプションを許可する必要があります。




#### 2.1.4.2 Google Play Store からダウンロード

Android デバイスで Google Play Store アプリケーションを開き、ESET Endpoint Security（または ESET）を検索します。

## 2.2 ESET Endpoint Security for Android のインストール手順

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。

**! 重 要**

上書きバージョンアップを行う場合、Google Play から ESET Endpoint Security for Android をインストールした Android 端末は Google Play からバージョンアップを実施し、ユーザーズサイトからダウンロードしたプログラムをインストールした Android 端末はユーザーズサイトからダウンロードしたプログラムでバージョンアップを実施してください。

### 2.2.1 Google Play Store からのインストール手順

**操作手順**

1. Android デバイスで Google Play Store アプリケーションを開き、ESET Endpoint Security（または ESET）を検索して ESET Endpoint Security のページを開きます。

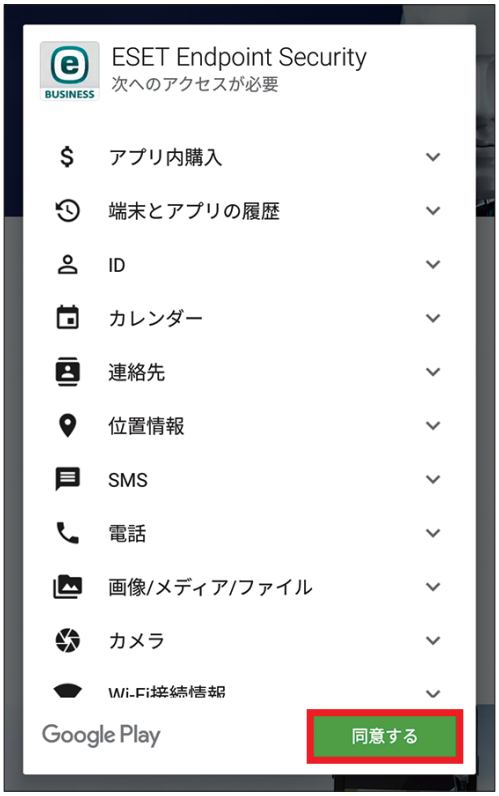
**ワンポイント**

ESET Endpoint Security をインストールしていない Android デバイスで電子メールを利用したリモートインストールを行う場合に、電子メールに記載されたリンクをタップすると、自動的に Google Play Store の ESET Endpoint Security for Android のページが表示されます。

2. ［インストール］をタップします。


続く

3 ［同意する］をタップすると、インストール作業が行われます。




4 アプリのインストールが完了すると、ESET Endpoint Security for Android のページの表示が画面のように変わります。［開く］をタップすると、ESET Endpoint Security for Android のセットアップウィザードが起動します。


**ワンポイント**

ESET Endpoint Security のセットアップウィザードの詳細については、「2.3 セットアップウィザード」をご参照ください。

### 2.2.2 インストール APK ファイルを利用したインストール手順

**操作手順**

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、［セキュリティ］または［アプリケーション］、［その他］などをタップします。

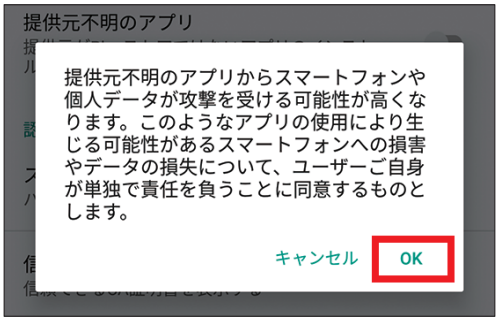

2 ［提供元不明のアプリ］をタップします。


**ワンポイント**

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。

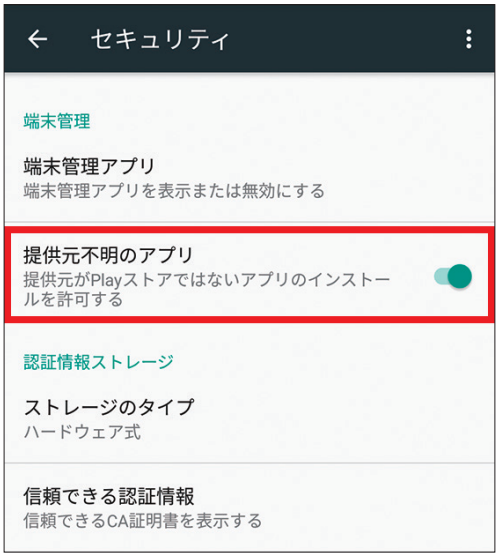
続く

3 [OK] をタップします。




4 提供元不明のアプリケーションのインストールの許可が設定されます。

※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。




5 ユーザーズサイトからインストーラー（.apk）をダウンロードします。

6 インストーラーのダウンロードが完了したら、[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。ダウンロードしたインストーラー（.apk）をタップします。

7 [インストール] をタップします。

8 「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。[開く] をタップすると、ESET Endpoint Security for Android のセットアップウィザードが起動します。

## 2.3 セットアップウィザード

ESET Endpoint Security for Android のインストール完了後、はじめて ESET Endpoint Security for Android を起動したときは、初期設定を行うためのセットアップウィザードが表示されます。セットアップウィザードを利用した初期設定には、アクティベーションが含まれます。手動でアクティベーションを行うには、製品認証キーが必要になります。ここでは、セットアップウィザードを利用した初期設定について説明します。

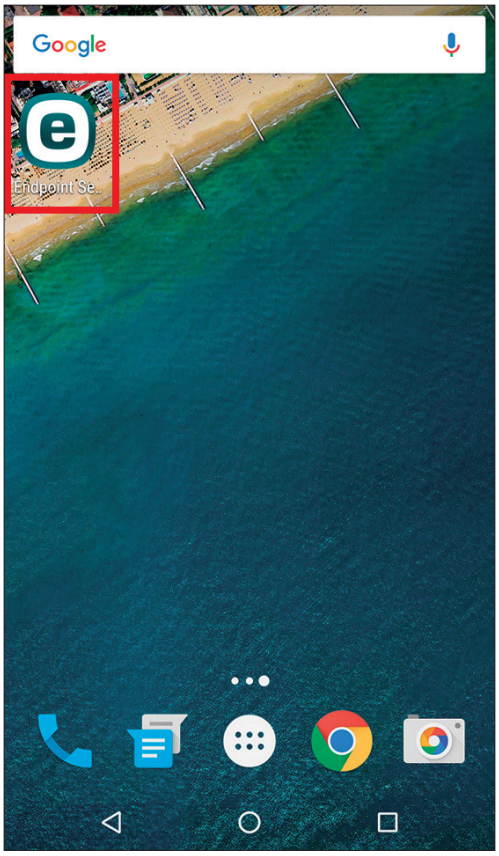
**! 重 要**

インストールする Android デバイスの OS のバージョンにより、必要な権限を有効にする設定画面が異なります。
画面の設問に従い権限を有効にしてください。

### 2.3.1 初期設定を行う

**操作手順**

1 ホーム画面の［ESET Endpoint Security for Android］のアイコンをタップして、ESET Endpoint Security for Android を起動します。




**ワンポイント**

インストール完了後に、Google Play Store の ESET Endpoint Security for Android のページ内にある［開く］をタップすることでも ESET Endpoint Security for Android を起動できます。

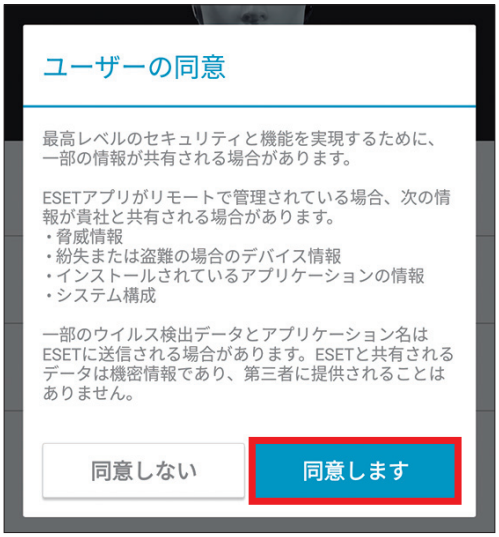
続く

2 ［管理者設定］をタップします。


3 言語と国に「日本」が選択されていることを確認し、［同意します］をタップします。


続く

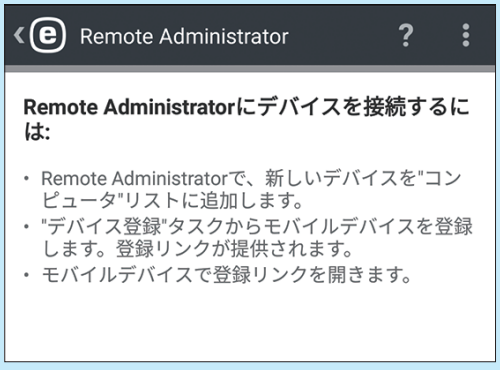
4 [同意します] をタップします。




5 ESET Endpoint Security for Android を ESET Remote Administrator に接続するか、手動セットアップを実行するかを選択します。ここでは、[いいえ、手動で設定します] をタップして手動セットアップを行います。

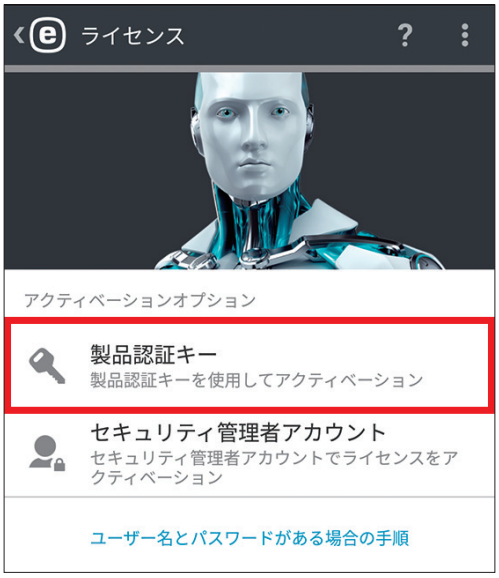

**ワンポイント**

電子メールによるリモートインストールを行っており、ESET Endpoint Security for Android を ESET Remote Administrator に接続する場合は、[はい、Remote Administrator に接続します] をタップします。次の画面が表示されたら、ホームボタンをタップして、メールアプリで登録リンクが記載されたメールを開き、リンクをタップして画面の指示に従ってセットアップを行います。
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。




続く

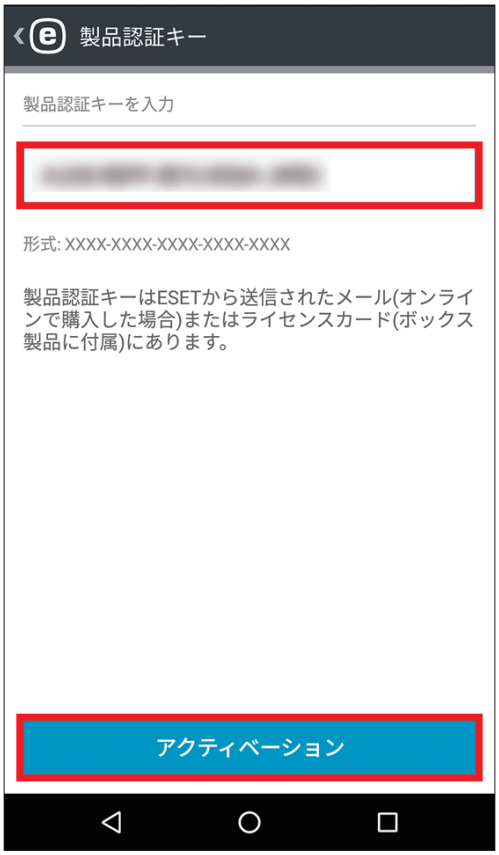
6 アクティベーションの方法を選択します。ここでは、［製品認証キー］をタップします。




**ワンポイント**

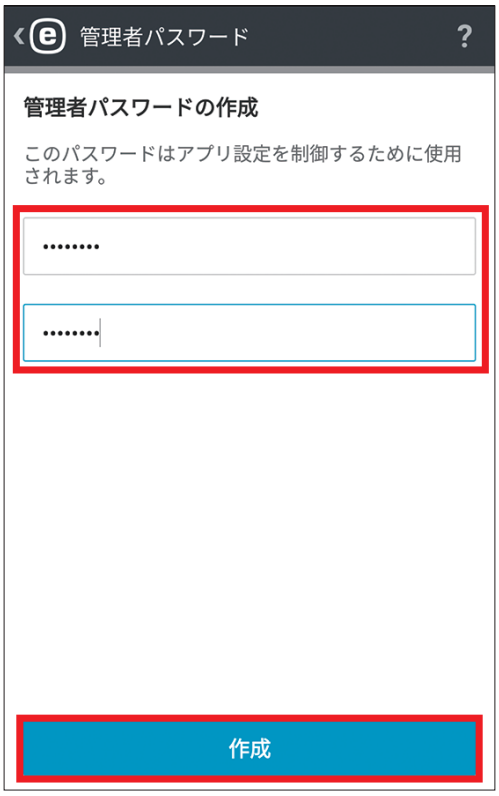
セキュリティ管理者アカウントは、日本では使用しません。

7 製品認証キーを入力し、［アクティベーション］をタップします。

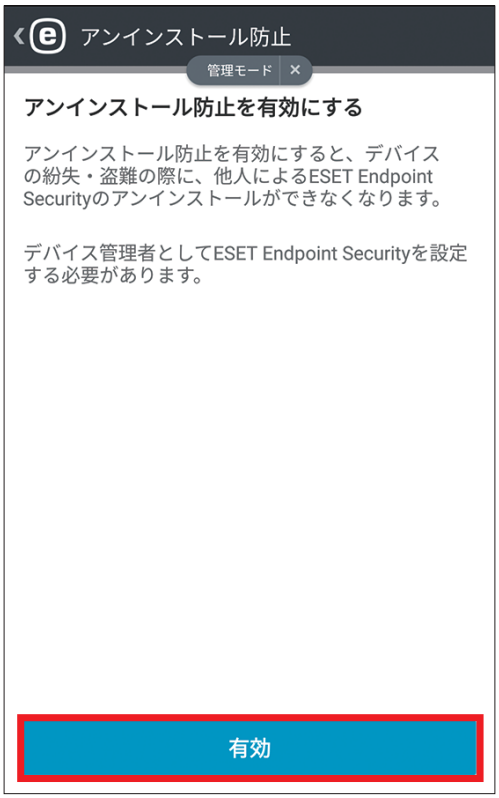



続く

8 アクティベーションが完了したら、管理者パスワードの作成画面が表示されます。管理者パスワードとして登録したいパスワードを 2 回入力し、［作成］をタップします。

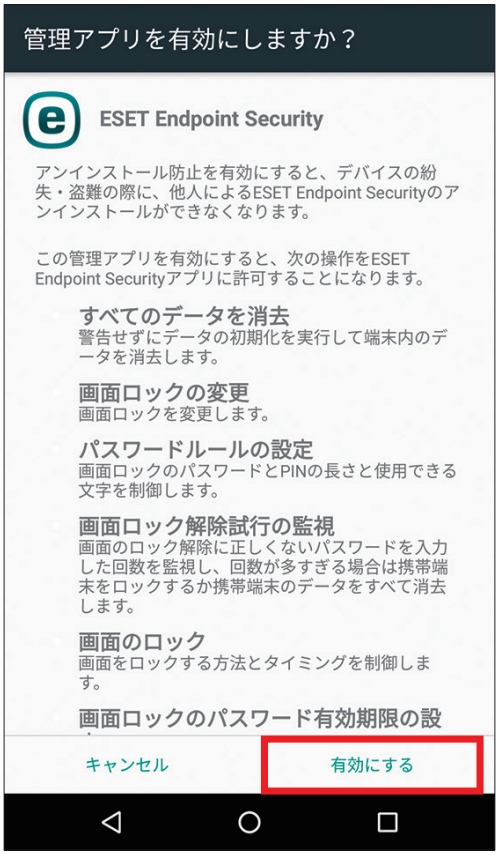



9 アンインストール防止機能の設定画面が表示されます。［有効］をタップします。

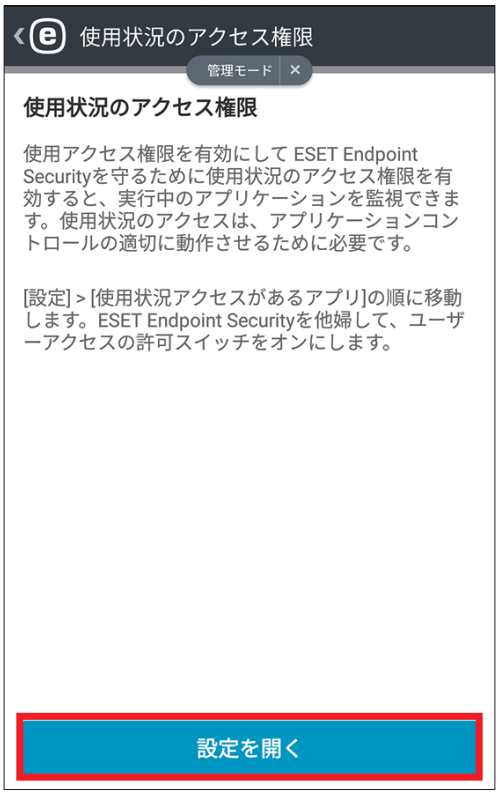



続く

10 管理アプリの設定画面が表示されます。［有効にする］をタップします。




11 ［設定を開く］をタップします。



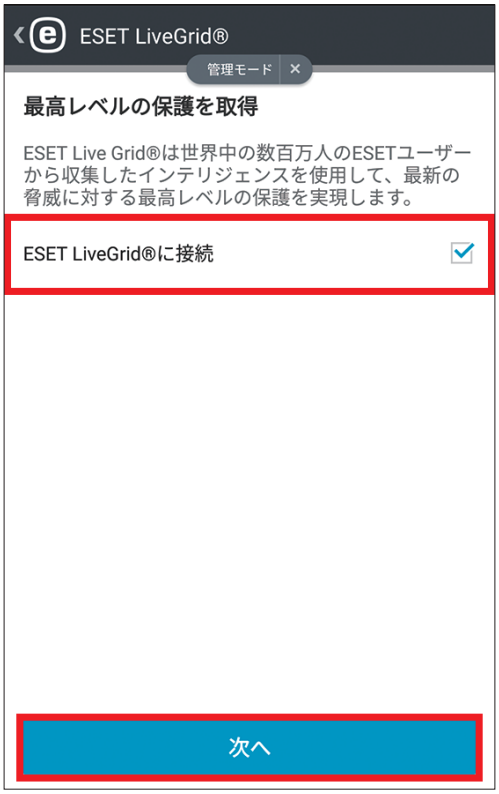

続く

⑫［ESET Endpoint Security］をタップします。

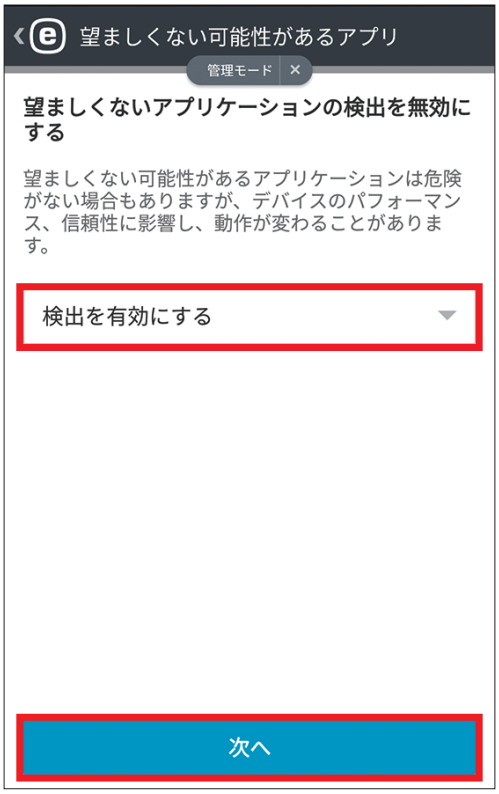

⑬使用状況へのアクセスを許可のスライドバーをタップします。


続く

14 ESET LiveGrid に接続のチェックをオンにして、［次へ］をタップします。




15 望ましくない可能性がアプリの設定画面表示されます。［検出を有効にする］を選択して、［次へ］をタップします。




続く

16 ESET Endpoint Security for Android の初期設定が完了しました。［OK］をタップします。


17 ESET Endpoint Security for Android のメインメニューが表示されます。

## 2.4 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。

### 2.4.1 アンインストール手順

**操作手順**

1 メインメニューの⋮をタップし、［設定］をタップします。


2 アンインストール保護が有効に設定されている場合、一部機能がグレーの網掛けの状態で表示されます。［アンインストール］をタップします。


続く

3 管理者パスワードを入力し、［入力］をタップします。


4 ［アンインストール］をタップします。


5 ［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 ウイルス対策

ウイルス対策モジュールは、脅威をブロックして隔離または駆除することで、悪意のあるコードから Android デバイスを保護します。ここでは、ウイルス対策について説明します。

## 3.1 ウイルス対策の画面構成

ESET Endpoint Security for Android のウイルス対策の画面構成について説明します。ウイルス対策は、メインメニューで[ウイルス対策]をタップすることで表示できます。一部の機能は、管理者パスワードを入力しない限り設定できません。


| 項目名 | 内容 | |
|---|---|---|
| **デバイスを検査** | ［デバイスを検査］をタップすると、検査レベルで設定した検査方法によって Android デバイス内の手動検査が実行されます。検査結果は、［検査ログ］セクションにあるログファイルに保存されます。 | |
| **検査レベル** | 2 つの検査レベルから選択できます。 | |
| | スマート | スマート検査は、インストールされたアプリケーションと SD カード内の DEX ファイル（AndroidOS 用の実行ファイル）、SO ファイル（ライブラリ）を検査します。 |
| | 詳細 | 拡張子などに関係なくすべてのファイルタイプの検査を内蔵メモリと SD カードの両方を対象に実施します。 |

| 項目名 | 内容 |
|---|---|
| **自動検査** | オンデマンドデバイス検査（手動デバイス検査）の他に、ESET Endpoint Security for Android には、充電中などの特定の状態にあるときに自動検査を行ったり、スケジュールされた検査を実施する機能を搭載しています。［自動検査］をタップすると、充電中の検査およびスケジュール検査の有効／無効を切り替えられます。詳細については、「3.3　自動検査」をご参照ください。 |
| **検査ログ** | ［検査ログ］をタップすると、検査を行ったときに検出されたマルウェアや不正なアプリケーションの情報などの履歴（ログファイル）を確認できます。詳細については、「3.4　検査ログ」を参照してください。 |
| **ウイルス定義データベースのアップデート** | タップすると、ウイルス定義データベースのアップデートを手動で実行します。既定では、ESET Endpoint Security for Android にあらかじめ用意されているアップデートタスクによって、ウイルス定義データベースのアップデートが定期的に実行されます。<br>**!重　要**<br>ウイルス定義データベースは、不必要な帯域幅使用を防止するために、新しい脅威が追加されたときに必要に応じて更新されます。また、ウイルス定義データベースのアップデートは無償ですが、更新されたウイルス定義データベースのダウンロードには、別途、データ転送料金が必要になる場合があります。 |
| **詳細設定** | 詳細設定では、ESET Endpoint Security for Android の詳細な保護設定を行えます。ウイルス対策詳細設定の詳細については、「3.5　詳細設定」をご参照ください。 |

## 3.2 デバイスを検査

「デバイスを検査」をタップすると、検査レベルで設定した検査方法によって Android デバイス内の手動検査が実行されます。

**操作手順**

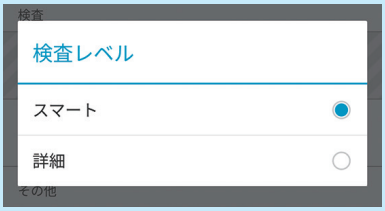
1 「ウイルス対策」を開き、［デバイスを検査］をタップします。


2 検査レベルで選択された検査方法で検査が実行され、検査結果が表示されます。


**ワンポイント**

［検査レベル］をタップすると、次の 2 種類から検査方法を選択できます。

| | |
|---|---|
| スマート | スマート検査は、インストールされたアプリケーションと SD カード内の DEX ファイル（AndroidOS 用の実行ファイル）、SO ファイル（ライブラリ）を検査します。 |
| 詳細 | 拡張子などに関係なくすべてのファイルタイプの検査を内蔵メモリと SD カードの両方を対象に実施します。 |



## 3.3 自動検査

自動検査では、充電中の検査およびスケジュール検査の有効／無効を切り替えられます。この機能は、管理者パスワードによって設定が保護されています。設定の変更には、管理者パスワードの入力を行う必要があります。以下の項目について設定できます。


| 項目名 | 内容 | |
|---|---|---|
| **検査レベル** | 検査レベルを「スマート」と「詳細」の 2 種類から選択できます。この設定は、充電中の検査とスケジュールされた検査に適用されます。 | |
| | スマート | スマート検査は、インストールされたアプリケーションと SD カード内の DEX ファイル（AndroidOS 用の実行ファイル）、SO ファイル（ライブラリ）を検査します。 |
| | 詳細 | 拡張子などに関係なくすべてのファイルタイプの検査を内蔵メモリと SD カードの両方を対象に実施します。 |
| **充電中に検査** | 充電中の検査の有効／無効を設定できます。充電中の検査が有効に設定されている場合、Android デバイスが充電器に接続された状態で完全充電され、アイドル状態にあるときに検査が自動的に実行されます。 | |
| **スケジュール検査** | スケジュールされた検査の有効／無効を設定できます。スケジュールされた検査が有効に設定されている場合、定義した時刻に自動的に検査が実行されます。スケジュールされた検査を有効にすると、検査を実行する日時を指定できます。既定では、月曜日の午前 4 時が選択されています。 | |

## 3.4 検査ログ

検査を行ったときに検出されたマルウェアや不正なアプリケーションの情報などの履歴（ログファイル）は、検査ログで確認できます。各ログには、次の情報が保存されています。

- イベントの日時
- 検査の期間
- 検査されたファイル数
- 検査結果または検査中に発生したエラー


続く

**操作手順**

1 「ウイルス対策」を開き、［検査ログ］をタップします。


2 閲覧したい検査ログをタップします。


3 検査ログの詳細が表示されます。

## 3.5 詳細設定

詳細設定では、ESET Endpoint Security for Android の詳細な保護設定を行えます。次の項目について設定を行えます。設定時、管理者パスワードの入力を行う必要があります。


| 項目名 | 内容 |
|---|---|
| **リアルタイム保護** | この設定をオンにすると、リアルタイム保護機能が有効になり、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。この設定は既定でオンに設定されています。このスキャナは、システムの起動時に自動的に実行され、操作するファイルを検査します。ダウンロードフォルダ、APKインストールファイル、およびマウント後のSDカードのすべてのファイルが自動的に検査されます。 |
| **ESET LiveGrid** | ESET LiveGrid は、先進の早期警告システムである ThreatSense.Net に基づいて構築されており、デバイスのセキュリティを向上させるように設計されています。世界各国の数百万人の ESET ユーザーから収集された最新情報を基に、システムで実行中のプログラムやプロセスを常時監視します。さらに、ESET LiveGrid データベースは時間とともに増大してゆくため、検査はより正確に処理されます。そのため、すべての ESET ユーザーに対しても、事前対策保護が強化され、検査速度が高まります。この機能の既定は、オンに設定されています。 |
| **望ましくない可能性があるアプリケーションの検出** | この設定をオンにすると、望ましくない可能性があるアプリケーションの検出を行います。望ましくない可能性あるアプリケーションとは、アドウエアを含んだり、ツールバーをインストールしたり、検索結果を追跡したり、その他の不明確なオブジェクトを含んだりするプログラムです。このタイプのアプリケーションは、場合によっては、リスクよりも使用する利点があることもあります。このため、このようなアプリケーションには、他のタイプの悪意のあるソフトウェアと比べて、低いリスクのカテゴリが割り当てられています。 |

| 項目名 | 内容 |
| --- | --- |
| **安全でない可能性があるアプリケーションの検出** | この設定をオンにすると、安全でない可能性があるアプリケーションの検出を行います。安全でない可能性があるアプリケーションとは、適正なアプリケーションでありながら、悪意のある目的で悪用される可能性があるプログラムです。この機能をオンにすると、このようなタイプのアプリケーションを監視し、必要に応じてブロックできます。安全ではない可能性があるアプリケーションは、市販の適正なソフトウェアに適用される分類です。この分類には、リモートアクセスツール、パスワード解析アプリケーション、キーロガーなどのプログラムが含まれます。 |
| **未解決の脅威をブロック** | この設定をオンにすると、ESET Endpoint Security for Android は脅威に分類されたファイルへのアクセスをブロックします。 |
| **ウイルス定義データベース更新** | このオプションは、ウイルス定義データベースの更新を行う間隔を設定します。既定では、「毎日」に設定されています。設定を変更することなく利用することをお勧めします。 |
| **最大データベース経過時間** | この設定は、ウイルス定義データベースのアップデート間隔の長さを定義します。ここで設定した時間が経過すると、ESET Endpoint Security for Android をアップデートするように通知されます。 |
| **アップデートサーバー** | この設定は、アップデートに利用するサーバーを設定できます。「公開前サーバー」「公開サーバー」「ローカルミラー」の中から選択できます。公開前サーバーを選択すると、まもなく一般に公開される予定のリリース前のプログラムにアップデートでき、最新の保護機能や修正プログラムを利用できます。ただし、リリース前アップデートは常に安全であるとは限りません。また、「ローカルミラー」を選択すると、社内などに設置されたミラーサーバーからアップデートできます。 |

# Chapter 4 アンチセフト

アンチセフト機能は、Android デバイスを不正アクセスから保護する機能です。この機能を利用することで、Android デバイスを紛失した場合や、Android デバイスが盗まれ、SIM カードを新しい（信頼できない）ものと交換された場合に、その Android デバイスを不正なアクセスから保護できます。ここでは、アンチセフト機能について説明します。

## 4.1 アンチセフトで利用できる機能

アンチセフト機能は、SIM カードを交換すると Android デバイスを使用できないようにロックしたり、ユーザーが定義した電話番号宛てにアラート SMS が送信できたりします。また、リモートコマンドを利用して紛失した Android デバイスの GPS 座標を要求したり、Android デバイスに保存されたすべてのデータを消去したりすることもできます。アンチセフトでは、次の機能を利用できます。

| 項目名 | 内容 | |
|---|---|---|
| **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 Android デバイスにセットされると、その Android デバイス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モバイルデバイスに送信されます。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。 | |
| **ロック画面カスタム情報** | Android デバイスがロックされているときに、管理者が定義したカスタム情報（会社名、電子メールアドレス、メッセージなど）をロック画面に表示できます。 | |
| **リモートコマンド** | SMS を利用して Android デバイスを遠隔操作できます。リモートコマンドは、管理者の電話番号または ERA Remote Administrator から送信できます。リモートコマンドでは、以下の機能を利用できます。 | |
| | 検索 | 現在位置の GPS 座標およびテキストメッセージを Android デバイスに要求します。また、より正確な位置情報が 10 分後に使用可能になった場合、Android デバイスはもう一度メッセージを送信します。受信した情報はコンピューター詳細に表示されます。 |
| | ロック | Android デバイスをロックします。Android デバイスは、管理者パスワードまたはロック解除コマンドを使用することでロックを解除できます。 |
| | ロック解除 | Android デバイスのロックを解除し、使用可能な状態にします。ロック解除した時点で使用されていた Android デバイスの SIM カードは信頼できる SIM として保存されます。 |
| | 警報 | Android デバイスをロックし、5 分間（またはロック解除が実行されるまで）大音量を再生します。 |
| | ワイプ | Android デバイス内のすべての使用可能なデータを完全に消去します（ファイルは上書きされます）。なお、ESET Endpoint Security for Android は Android に残ります。これには最大数時間かかる場合があります。 |
| | 拡張初期設定リセット | Android デバイスでアクセスできるすべてのデータを迅速に削除します（ファイルヘッダーは破棄されます）。Android デバイスは既定の初期設定にリセットされます。これには数分かかる場合があります。 |

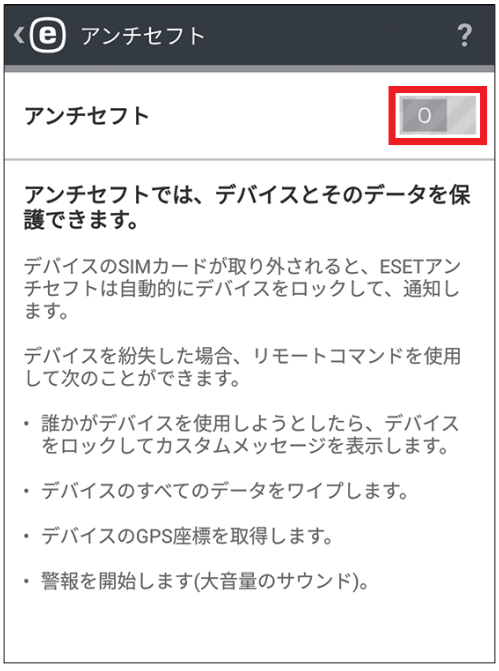
## 4.2　アンチセフトの初期設定を行う

アンチセフトを利用するにはアンチセフトを有効に設定し、アンチセフトスタートアップウィザードで管理者の連絡先の登録などの初期設定を行う必要があります。

**操作手順**

1 メインメニューの［アンチセフト］をタップします。

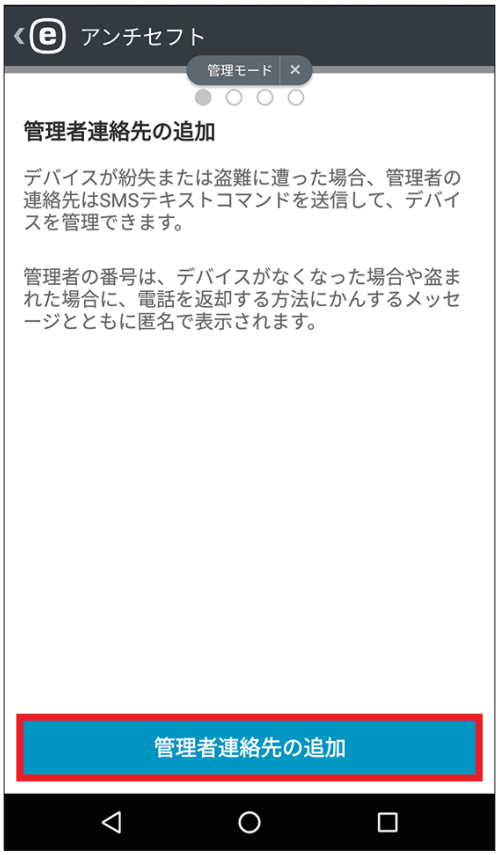

2 アンチセフトの 0 をタップします。




続く

3 「管理モードに切り替える」画面が表示されたら、管理者パスワードを入力し、[入力] をタップします。


4 [管理者連絡先の追加] をタップします。




続く

5 管理者の名前と電話番号を入力し、［保存］をタップします。

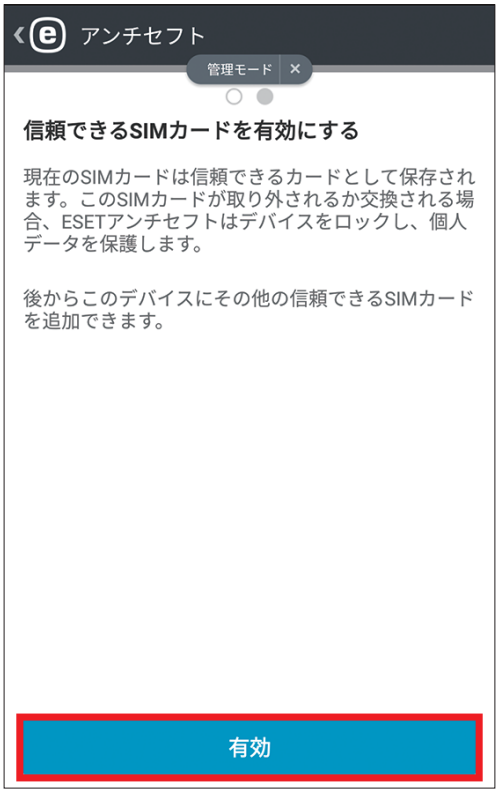

**ワンポイント**

複数の電話番号を登録したいときは、＋をタップして、別の電話番号を入力します。
すべての電話番号を登録したら、［保存］をタップしてください。


続く

6 Android デバイスをロックしたときに、ロック画面に表示される情報の入力を行います。会社名、連絡先のメールアドレス、メッセージなどの入力を行い、［次へ］をタップします。


7 信頼できる SIM カードを有効にします。［有効］をタップします。




続く

8 アンチセフトの初期設定はこれで完了です。[OK] をタップします。


9 アンチセフトの設定画面が表示されます。

## 4.3 アンチセフトの設定の変更について

アンチセフトを有効にすると、アンチセフトの有効 / 無効の切り替え、各種設定の確認や変更、追加が行えるようになります。次の項目について設定の確認や変更、追加が行えます。また、アンチセフトの設定を変更するには、管理者パスワードの入力が必要になります。


| 項目名 | 内容 |
|---|---|
| **管理者連絡先** | 管理者の連絡先（電話番号）の追加や変更が行えます。管理者の連絡先は複数登録できます。 |
| **ロック画面情報** | Android デバイスをロックしたときにロック画面に表示される情報を編集できます。 |
| **信頼する SIM カード** | 信頼する SIM カードの追加を行えます。1 台の Android デバイスで複数の SIM カードを利用する場合、信頼する SIM カードを複数登録できます。 |
| **SMS テキストコマンドの着信** | SMS テキストコマンドの着信の有効 / 無効を切り替えられます。 |
| **コマンドの送信** | 他のデバイスにコマンドを送信します。 |

### 4.3.1　管理者の連絡先の追加や編集を行う

ここでは、管理者の連絡先の新規追加や登録済みの連絡先の編集方法を説明します。

#### 4.3.1.1　管理者の連絡先を追加する

ここでは、管理者の連絡先を追加する方法を説明します。

**操作手順**

1 メインメニューの［アンチセフト］をタップし、［管理者連絡先］をタップします。


2 ＋をタップします。


続く

3 「管理モードに切り替える」画面が表示されたら、管理者パスワードを入力し、［入力］をタップします。


**ワンポイント**

管理者パスワードを入力し、管理者モードになっているときは、パスワード入力画面は表示されません。手順 4 に進んでください。

4 追加したい管理者の名前と電話番号を入力し、［保存］をタップします。


続く

**ワンポイント**

複数の電話番号を登録したいときは、電話番号の右横の＋をタップして、別の電話番号を入力します。すべての電話番号を登録したら、［保存］をタップしてください。


5 管理者の連絡先が追加されます。

### 4.3.1.2　登録済みの管理者の情報の編集を行う

ここでは、登録済みの管理者の情報を編集する方法を説明します。

**操作手順**

1. メインメニューの［アンチセフト］をタップし、［管理者連絡先］をタップします。
2. 情報の編集を行いたい管理者をタップします。


3. ［管理者として編集］をタップします。


続く

4 「管理モードに切り替える」画面が表示されたら、管理者パスワードを入力し、[入力] をタップします。

**ワンポイント**

管理者パスワードを入力し、管理者モードになっているときは、パスワード入力画面は表示されません。手順 5 に進んでください。

5 連絡先追加の編集画面が表示されます。登録情報の追加などを行って［保存］をタップします。

## 4.3.2　ロック画面の情報を編集する

ここでは、ロック画面の情報を編集する方法を説明します。

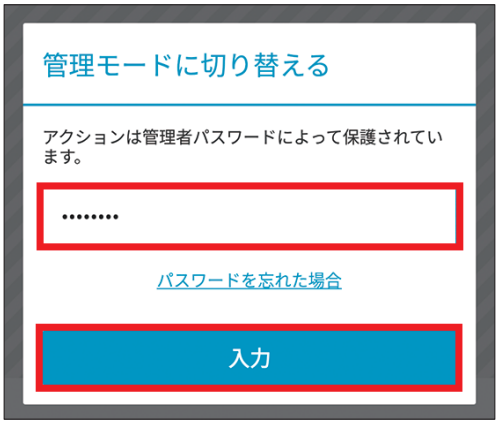
**操作手順**

1 メインメニューの［アンチセフト］をタップし、［ロック画面情報］をタップします。


2 ［管理者として編集］をタップします。


続く

3 「管理モードに切り替える」画面が表示されたら、管理者パスワードを入力し、［入力］をタップします。




**ワンポイント**

管理者パスワードを入力し、管理者モードになっているときは、パスワード入力画面は表示されません。手順 4 に進んでください。

4 ロック画面の情報の編集画面が表示されます。登録情報の編集を行って、［保存］をタップします。

### 4.3.3 信頼する SIM カードを追加する

ここでは、信頼する SIM カードを追加する方法を説明します。

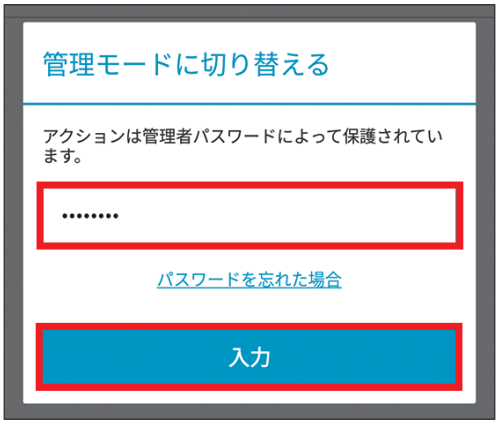
**操作手順**

1. メインメニューの［アンチセフト］をタップし、［信頼する SIM カード］をタップします。


2. ＋をタップします。


続く

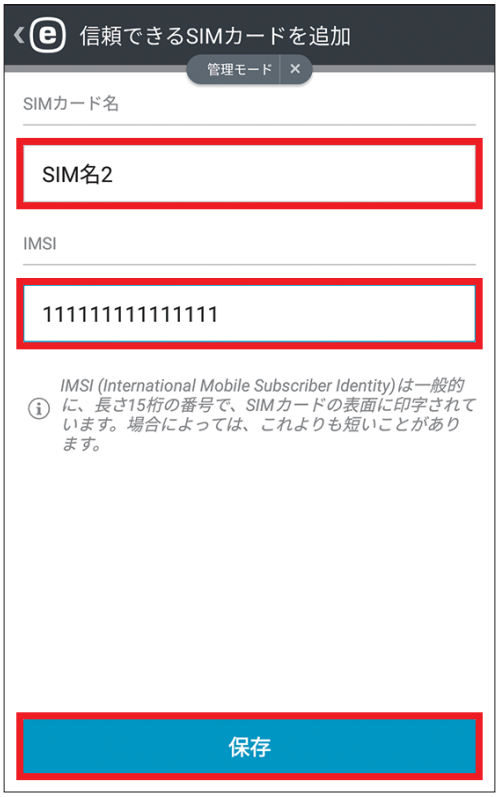
3 「管理モードに切り替える」画面が表示されたら、管理者パスワードを入力し、[入力] をタップします。




**ワンポイント**

管理者パスワードを入力し、管理者モードになっているときは、パスワード入力画面は表示されません。手順 4 に進んでください。

4 「信頼できる SIM カードを追加」画面が表示されます。SIM カードの名称を入力し、IMSI（International Mobile Subscriber Identity）番号を入力して、[保存] をタップします。




**ワンポイント**

IMSI 番号は、通常、15 桁の番号で SIM カードの表面に印刷されています。ただし、場合によっては、15 桁よりも短い場合があります。

**! 重　要**

信頼できる SIM 機能は、CDMA、WCDMA、および Wi-Fi 専用デバイスでは使用できません。

## 4.4 リモートコマンド

ここでは、Android デバイスのリモート操作について説明します。

### 4.4.1 リモート操作の方法とリモートコマンド

Android デバイスのリモート操作は、検索、ロック、ロック解除、警報、ワイプ、拡張初期設定リセットなどの操作を行えます。また、次の 3 つの方法で実行できます。

- 管理者の Android デバイスにインストールされた ESET Endpoint Security for Android のコマンドの送信機能を使用
- 管理者のモバイルデバイスから SMS テキストメッセージを送信
- ESET Remote Administrator の Web コンソールから送信

**! 重　要**

管理者のモバイルデバイス／ Android デバイスからリモート操作を行う場合は、操作される側の Android デバイスに管理者の連絡先として操作元の電話番号が登録されている必要があります。電話番号が管理者の連絡先として登録されていない場合は、リモート操作を行えません。管理者の連絡先の登録方法については「4.3.1　管理者の連絡先の追加や編集を行う」をご参照ください

| 項目名 | 内容 |
|---|---|
| **検索** | 現在位置の GPS 座標およびテキストメッセージを Android デバイスに要求します。また、より正確な位置情報が 10 分後に使用可能になった場合、Android デバイスはもう一度メッセージを送信します。受信した情報はコンピューター詳細に表示されます。 |
| **ロック** | Android デバイスをロックします。Android デバイスは、管理者パスワードまたはロック解除コマンドを使用することでロック解除できます。 |
| **ロック解除** | Android デバイスのロックを解除し、使用可能な状態にします。ロックを解除した時点で使用されていた Android デバイスの SIM カードは信頼できる SIM として保存されます。 |
| **警報** | Android デバイスをロックし、5 分間（またはロック解除が実行されるまで）大音量を再生します。 |
| **ワイプ** | Android デバイス内のすべての使用可能なデータを完全に消去します（ファイルは上書きされます）。なお、ESET Endpoint Security for Android は Android に残ります。これには最大数時間かかる場合があります。Android 6 以降に対し、ワイプを実行すると、拡張初期設定リセットの動作になります。 |
| **拡張初期設定リセット** | Android デバイスでアクセスできるすべてのデータを迅速に削除します（ファイルヘッダーは破棄されます）。Android デバイスは既定の初期設定にリセットされます。これには数分かかる場合があります |

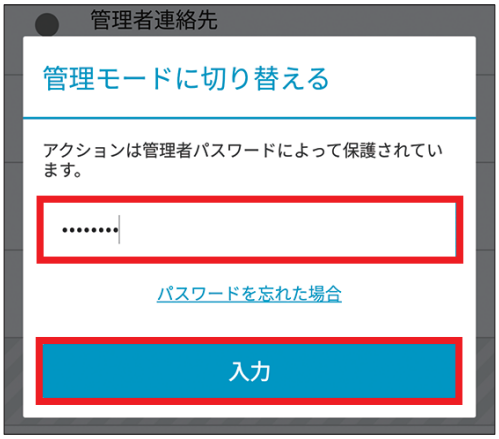
### 4.4.2 ESET Endpoint Security for Android のコマンドの送信機能で操作する

ESET Endpoint Security for Android のコマンドの送信機能で操作する場合は、メニューから行いたい操作を選択するだけでリモート操作を行えます。リモート操作は、次の手順で行います。

**操作手順**

1 メインメニューの［アンチセフト］をタップし、［コマンドの送信］をタップします。


2 「管理モードに切り替える」画面が表示されたら、管理者パスワードを入力し、［入力］をタップします。



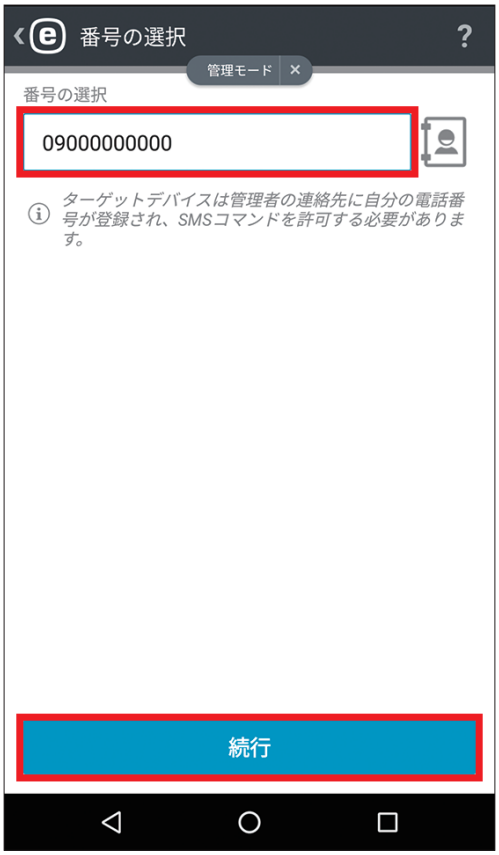

**ワンポイント**

管理者パスワードを入力し、管理者モードになっているときは、パスワード入力画面は表示されません。手順 3 に進んでください。

続く

3 ［新しいコマンドの送信］をタップします。


4 リモート操作を行いたい Android デバイスの電話番号を入力し、［続行］をタップします。

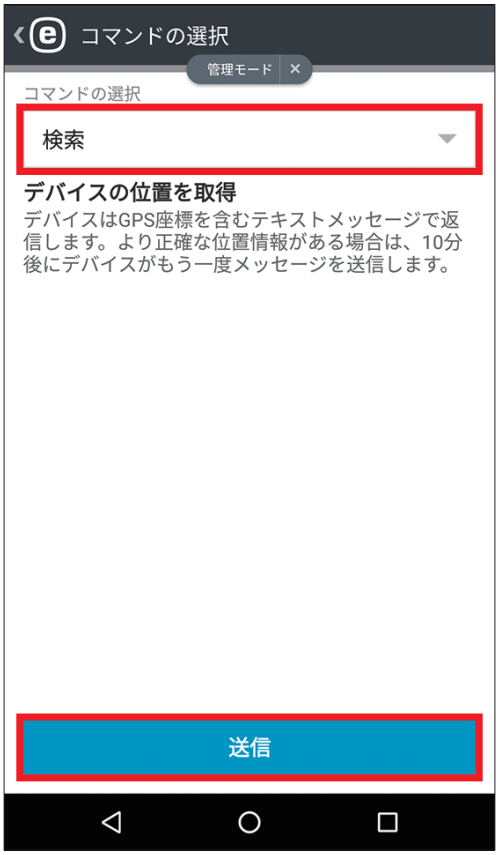



**ワンポイント**

をタップすると、アドレス帳から操作を行いたい Android デバイスの電話番号を選択できます。

続く

5 送信したいコマンドを選択し、［送信］をタップします。



### 4.4.3 管理者のモバイルデバイスから SMS テキストメッセージを送信

管理者のモバイルデバイスから SMS テキストメッセージで操作を行うときは、以下のようなテキストコマンドを本文とした SMS メッセージを送信します。

| 項目名 | SMS コマンド | 内容 |
|---|---|---|
| 検索 | eset find | Google マップ上のその場所へのリンクを含む、対象デバイスの GPS 座標が入ったテキストメッセージの送信をリクエストします。 |
| ロック | eset lock | Android デバイスを使用できないようにロックします。 |
| ロック解除 | eset unlock | Android デバイスのロックを解除し、その時点で Android デバイスに挿入されている SIM カードを信頼できる SIM として保存します。 |
| 警報 | eset siren | 大音量の警報を再生します。 |
| ワイプ | eset wipe | 既定のフォルダに保存されているすべての連絡先、メッセージ、電子メール、アカウント、SD カードの内容、画像、音楽、動画が完全に Android デバイスから消去します。ESET Endpoint Security はインストールされたまま残ります。 |
| 拡張初期設定リセット | eset factory reset | デバイスを初期設定にリセットします。すべてのアクセス可能なデータが消去されます。 |

### 4.4.4 ESET Remote Administrator の Web コンソールから送信

ESET Remote Administrator でリモート操作を行う場合は、ERA Web コンソールから操作を行います。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。

# Chapter 5 アプリケーション制御

アプリケーション制御は、管理者がユーザーが利用できるアプリケーションを制限する機能です。管理者が定義したアプリケーションへのアクセスをブロックし、特定のインストール済みアプリケーショオンをアンインストールするようにユーザーに通知できます。これによって、アプリケーションを利用する上でのリスクを低減できます。管理者は、次のフィルタリング方法を用いて、アプリケーションの管理を行えます。

- ブロックするアプリケーションを手動で定義
- 分類に基づくブロック（ゲームまたはソーシャルなど）
- 権限に基づくブロック（位置情報を追跡するアプリケーションなど）
- ソースによってブロック（Google Play Store 以外のソースからインストールされたアプリケーションなど）

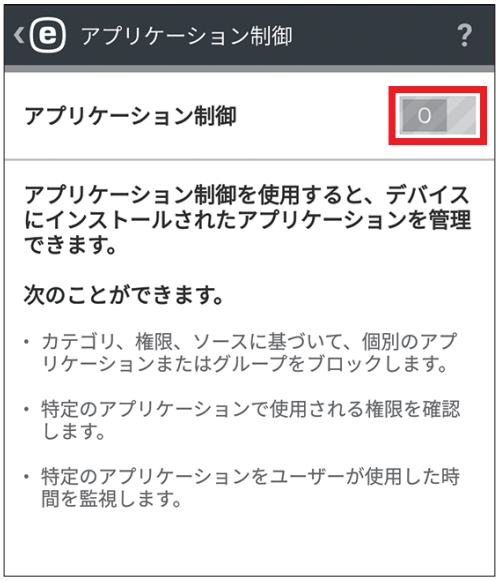
## 5.1 アプリケーション制御を有効する

アプリケーション制御を利用するには、アプリケーション制御を有効に設定し、各種設定を行う必要があります。アプリケーション制御は、次の手順で有効にできます。

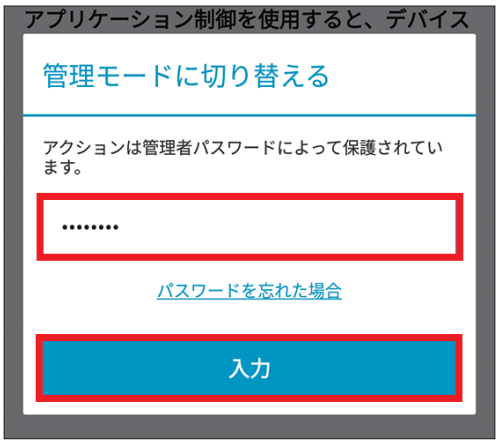
**操作手順**

1. メインメニューの［アプリケーション制御］をタップします。

2 [アプリケーション制御] の O をタップします。




3 「管理モードに切り替える」画面が表示されたら、管理者パスワードを入力し、[入力] をタップします。




4 アプリケーション制御が有効に設定され、各種設定を行えます。

## 5.2 ブロックルール

アプリケーション制御では、ブロックするアプリケーションを登録したブロックルールを作成する必要があります。ブロックルールの作成は、［ブロックルール］セクションで行います。［アプリケーション制御］>［ブロック］>［ブロックルール］とタップすることで［ブロックルール］セクションを表示できます。ここでは、ブロックルールについて説明します。ブロックルールは、次の条件を用いて作成できます。

- アプリケーション名またはパッケージ名
- 分類
- 権限

### 5.2.1 アプリケーション名でブロック

ESET Endpoint Security for Android では、管理者がアプリケーション名またはパッケージ名を利用してアプリケーションをブロックできます。アプリケーション名でアプリケーションをブロックすると、ESET Endpoint Security for Android は、起動されたアプリケーション名との完全一致を検索します。ESET Endpoint Security for Android の GUI を別の言語に変更する場合は、その言語でアプリケーション名を再入力し、ブロックし続ける必要があるので注意してください。日本語版、英語版などさまざまな言語で展開されているアプリケーションを登録するときは、ローカライズされたアプリケーション名の問題を回避するために、パッケージ名を利用してアプリケーションをブロックすることをお勧めします。ローカル管理者の場合、［アプリケーション制御］>［監視］>［許可されたアプリケーション］とタップすることで、アプリケーションパッケージを検索できます。アプリケーションをタップすると、詳細画面にアプリケーションパッケージ名が表示されます。

#### 5.2.1.1 アプリケーション名でアプリケーションをブロックする方法

アプリケーション名を利用してアプリケーションをブロックルールに追加するには、以下の手順で行います。

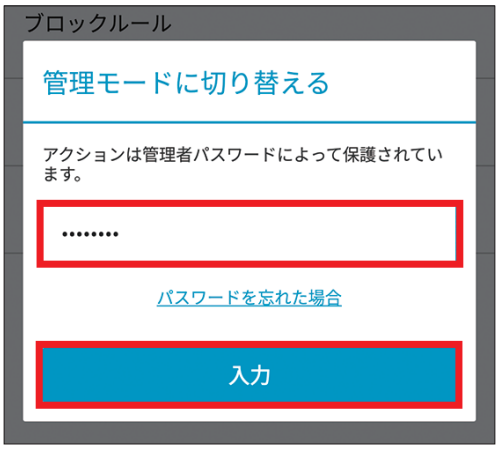
**操作手順**

1. メインメニューで［アプリケーション制御］をタップし、［ブロック］をタップします。


続く

2 ［アプリケーションをブロック］をタップします。


3 「管理モードに切り替える」画面が表示されたら、管理者パスワードを入力し、［入力］をタップします。




4 ブロックの方法を選択します。［名前でブロック］をタップします。


続く

5 ［アプリケーション名でブロック］をタップします。


**ワンポイント**

ここでは、アプリケーション名でブロックルールを作成していますが、［パッケージ名でブロック］をタップすると、パッケージ名を利用してブロックルールを作成できます。

6 アプリケーション名を入力し、［拒否］をタップします。複数のアプリケーション名を指定するときは、「,（カンマ）」で区切ってアプリケーション名を入力します。


**ワンポイント**

アプリケーション名を指定する場合、入力したアプリケーション名（単語）を含むすべてのアプリケーションがブロックされるので注意してください。たとえば、単語「example」を入力した場合、名前に「example」を含んだすべてのアプリケーションがブロックされます。

続く

7 ［ブロックルール］セクションにブロックルールが登録されます。


**ワンポイント**

［ブロックルール］セクションには、作成されたルールの概要とブロックするアプリケーションの一覧が表示されます。既存のルールを修正するには、ルールをロングタップし、［編集］をタップします。リストから一部のルールエントリを削除するには、エントリのいずれかをロングタップして、削除するものを選択し、［削除］をタップします。リスト全体を消去するには、［すべて選択］をタップし、［削除］をタップします。

### 5.2.2 アプリケーションカテゴリでブロック

ESET Endpoint Security for Android では、定義済みのアプリケーションカテゴリからブロックルールを選択できます。アプリケーションカテゴリから選択すると、選択したカテゴリに属するアプリケーションをブロックできます。

#### 5.2.2.1 アプリケーションカテゴリからアプリケーションをブロックする方法

アプリケーションカテゴリを利用してアプリケーションをブロックルールに追加するには、以下の手順で行います。

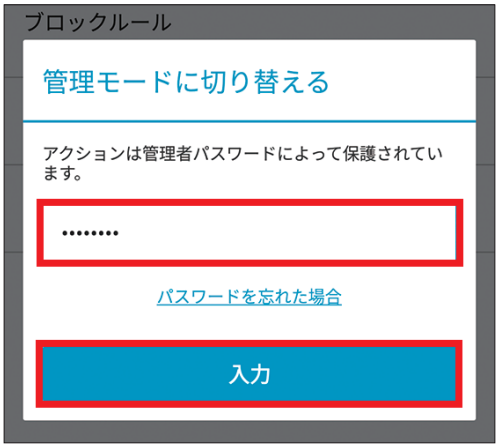
**操作手順**

1. メインメニューで［アプリケーション制御］をタップし、［ブロック］をタップします。


2. ［アプリケーションをブロック］をタップします。


続く

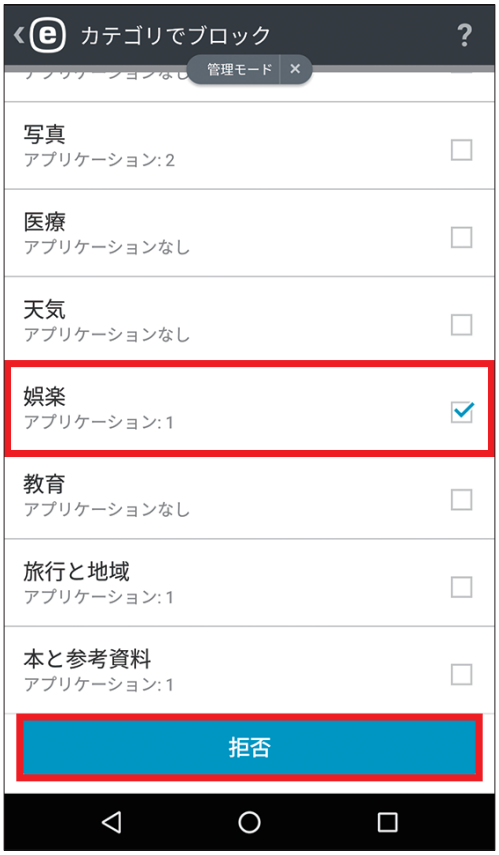
3 「管理モードに切り替える」画面が表示されたら、管理者パスワードを入力し、[入力] をタップします。




4 ブロックの方法を選択します。[カテゴリでブロック] をタップします。


続く

5 ブロックしたいカテゴリをタップしてチェックをオンにし、［拒否］をタップします。




6 ［ブロックルール］セクションにブロックルールが登録されます。


**ワンポイント**

［ブロックルール］セクションには、作成されたルールの概要とブロックするアプリケーションの一覧が表示されます。既存のルールを修正するには、ルールをタッチアンドホールドし、［編集］をタップします。リストから一部のルールエントリを削除するには、エントリのいずれかをロングタップして、削除するものを選択し、［削除］をタップします。リスト全体を消去するには、［すべて選択］をタップし、［削除］をタップします。

### 5.2.3 アプリケーション権限でブロック

ESET Endpoint Security for Android では、管理者が権限を利用してアプリケーションをブロックできます。この機能を利用すると、個人データの読み取りを行うアプリケーションや連絡先にアクセスするアプリケーションといった権限を利用したブロックを行えます。

#### 5.2.3.1 権限でアプリケーションをブロックする方法

アプリケーションの権限を利用してアプリケーションをブロックルールに追加するには、以下の手順で行います。

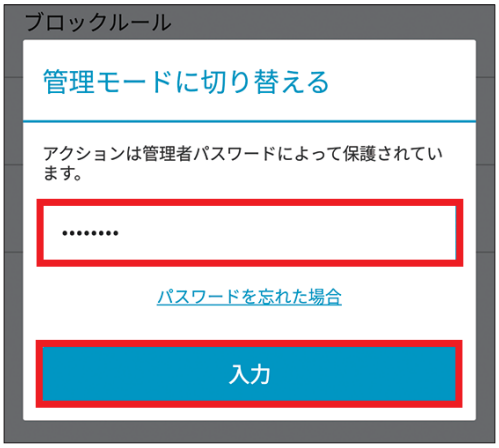
**操作手順**

1. メインメニューで［アプリケーション制御］をタップし、［ブロック］をタップします。


2. ［アプリケーションをブロック］をタップします。


続く

3 「管理モードに切り替える」画面が表示されたら、管理者パスワードを入力し、[入力] をタップします。




4 ブロックの方法を選択します。[権限でブロック] をタップします。


続く

5 ブロックしたい権限をタップしてチェックをオンにし、［拒否］をタップします。


6 ［ブロックルール］セクションにブロックルールが登録されます。


**ワンポイント**

［ブロックルール］セクションには、作成されたルールの概要とブロックするアプリケーションの一覧が表示されます。既存のルールを修正するには、ルールをタッチアンドホールドし、［編集］をタップします。リストから一部のルールエントリを削除するには、エントリのいずれかをロングタップして、削除するものを選択し、［削除］をタップします。リスト全体を消去するには、［すべて選択］をタップし、［削除］をタップします。

### 5.2.4 不明なソースをブロック

ESET Endpoint Security for Android は、Google Play Store 以外のソースから取得されたアプリケーションをブロックしません。Google Play Store 以外のソースから取得されたアプリケーションをブロックしたいときは、メインメニューから［アプリケーション制御］＞［ブロック］とタップし、［不明な提供元をブロック］を有効に設定します。

## 5.3 例外

例外を作成すると、ブロックルールから特定のアプリケーションを除外できます。ブロックルールを作成し、ブロックする必要がないアプリケーションまでブロックしてしまったときは、例外を作成することでそのアプリケーションのブロックを行わないようにできます。

### 5.3.1 例外の追加方法

例外を追加するには、以下の手順で行います。

**操作手順**

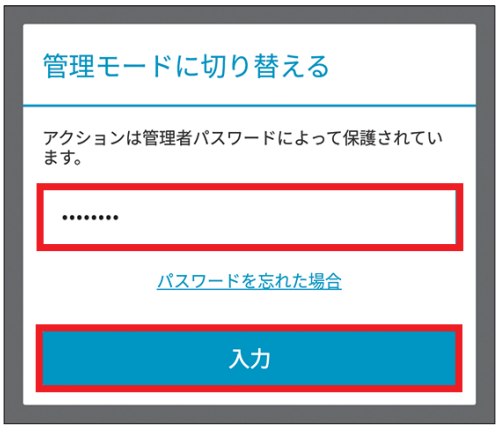
1. メインメニューで［アプリケーション制御］をタップし、［ブロック］をタップします。


2. ［例外］をタップします。


続く

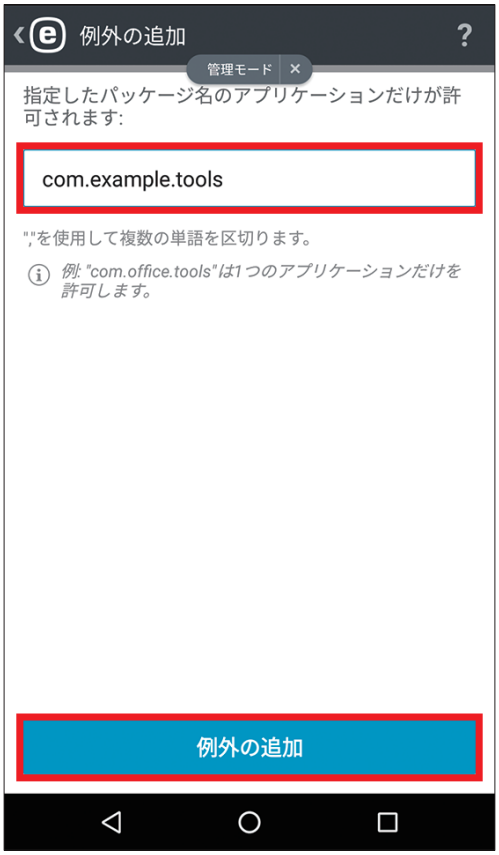
3 ［例外の追加］をタップします。


4 「管理モードに切り替える」画面が表示されたら、管理者パスワードを入入力し、［入力］をタップします。

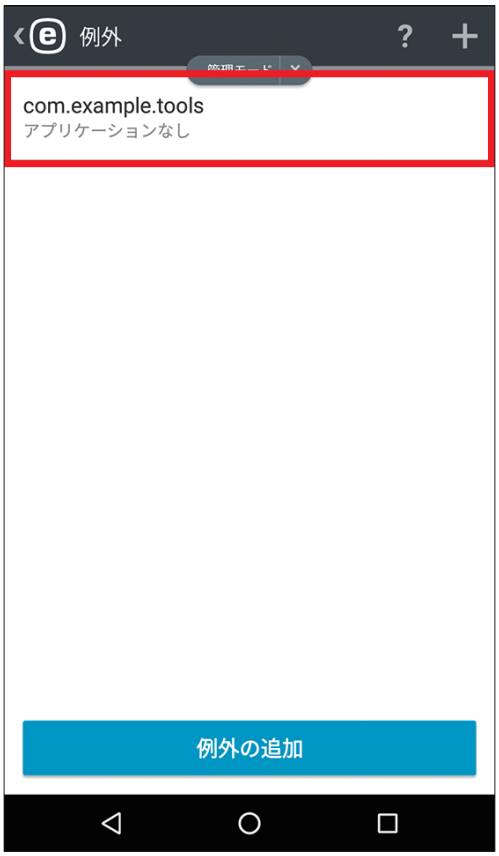



続く

5 除外するアプリケーションのパッケージ名を入力し、［例外の追加］をタップします。




6 除外ルールが登録されます。



## 5.4 必要なアプリケーション

ESET Remote Administrator からリモートで ESET Endpoint Security for Android を管理する場合は、対象 Android デバイスにインストールする必要があるアプリケーションを定義できます。アプリケーションの定義には、次の情報が必須です。

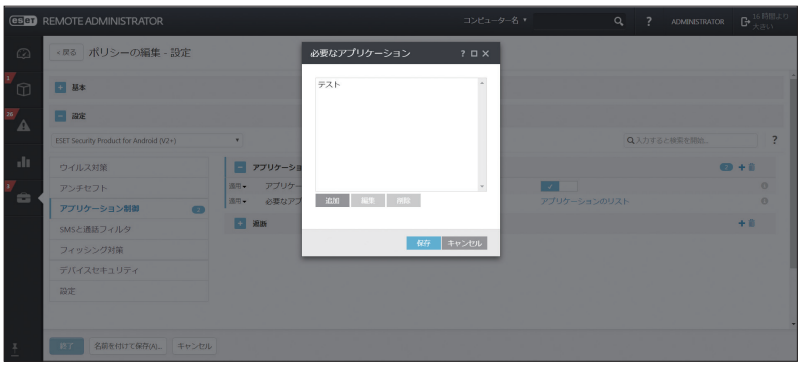
- ユーザーに表示されるアプリケーション名
- 一意のアプリケーションパッケージ名（例 : com.eset.ems2.gp）
- ダウンロードリンクの URL。Google Play リンク（例 : https://play.google.com/store/apps/details?id=com.eset.ems2.gp）も使用できます。

**! 重 要**

この機能は、ESET Endpoint Security for Android アプリ単体では使用できません。使用するには、ESET Remote Administrator が必要です。

**操作手順**

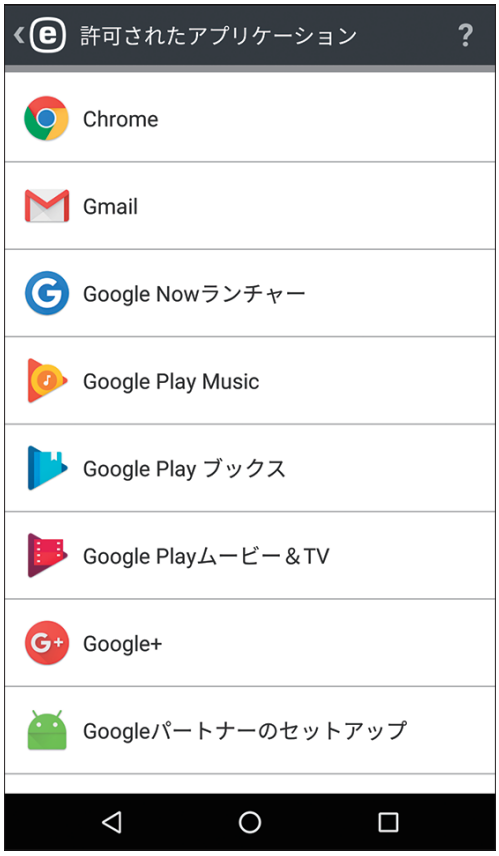
1. ESET Remote Administrator のポリシーの作成で［ESET Endpoint Security for Android（2+）］を選択し、［アプリケーション制御］の中の設定項目の［アプリケーションコントロールを有効にする］を有効にします。その後、［必要なアプリケーションのリスト］にユーザーにインストールすることを通知したアプリケーションを追加し、適用します。




必要なアプリケーションのポリシーを適用された ESET Endpoint Security for Android に、該当のアプリケーションがインストールされていない場合は通知されます。

## 5.5 許可されたアプリケーション

「許可されたアプリケーション」では、ブロックルールでブロックされていないインストール済みアプリケーションの概要が表示されます。「許可されたアプリケーション」は、[アプリケーション制御] > [監視] > [許可されたアプリケーション] とタップすることで表示できます。

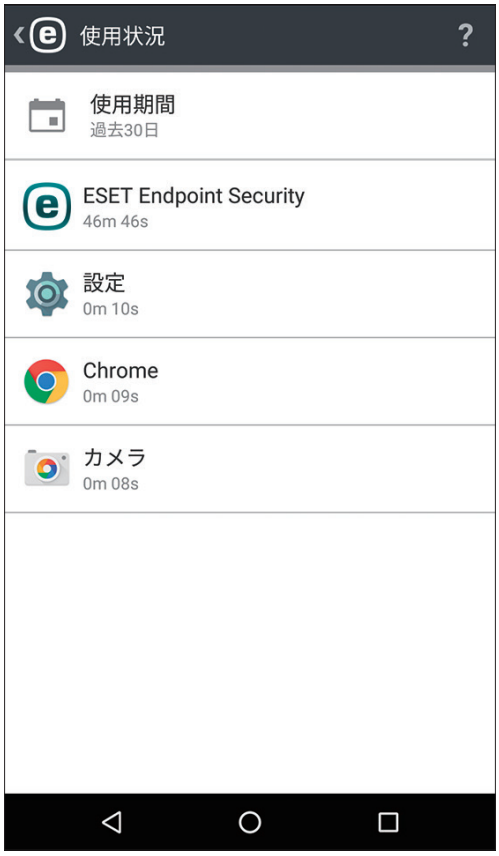


## 5.6 権限

この機能は、個人データまたは企業データにアクセスできるアプリケーションを確認できます。これによって、管理者は、定義済みの権限カテゴリに基づいて、アプリケーションアクセスを監視できます。デバイスにインストールされた一部のアプリケーションは、有料のサービスにアクセスしたり、位置情報を追跡したり、個人情報、連絡先、またはテキストメッセージを読み取ったりする場合があります。ESET Endpoint Security for Android はこのようなアプリケーションを監査します。このセクションには、カテゴリ別に並べ替えられたアプリケーションのリストが表示されます。各カテゴリをタップすると、詳細説明を表示します。各アプリケーションの権限詳細は、特定のアプリケーションをタップすると表示されます。「権限」は、［アプリケーション制御］＞［監視］＞［権限］とタップすることで表示できます。

## 5.7 使用状況

「使用状況」では、ユーザーが特定のアプリケーションを使用した時間を監視できます。使用期間で概要をフィルタリングするには、［間隔］オプションを使用します。「使用状況」は、［アプリケーション制御］＞［監視］＞［使用状況］とタップすることで表示できます。



# Chapter 6 デバイスセキュリティ

デバイスセキュリティでは、Android デバイスの設定を監視および制御できます。デバイスセキュリティでは、管理者が次の処理を実行できます。

- パスワードや PIN のセキュリティ強度など画面ロック強度の強さを定義できます。
- 内蔵カメラの使用を制限します。
- Android デバイス全体で基本セキュリティポリシーを実行し、重要なデバイス設定のポリシーを定義できます。

## 6.1 デバイスセキュリティを有効にする

デバイスセキュリティを利用するには、デバイスセキュリティを有効に設定し、各種設定を行う必要があります。デバイスセキュリティは、次の手順で有効にできます。

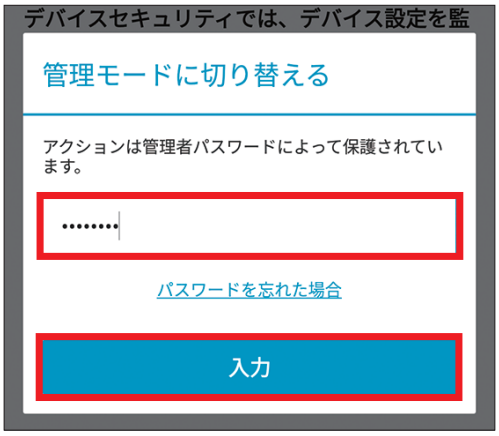
**操作手順**

1. メインメニューの［デバイスセキュリティ］をタップします。


続く

2 ［デバイスセキュリティ］の 0 をタップします。


3 「管理モードに切り替える」画面が表示されたら、管理者パスワードを入力し、［入力］をタップします。




4 デバイスセキュリティが有効に設定され、デバイスセキュリティの各機能の有効／無効を切り替えられます。

## 6.2 画面ロックポリシー

画面ロックポリシーを有効に設定すると、ロック画面に関するセキュリティを設定できます。画面ロックポリシーでは、次の設定が行えます。


| 項目名 | 内容 |
|---|---|
| **セキュリティレベル** | システム画面ロックコードの最低セキュリティレベルを低（少なくともパターン）、中（少なくとも PIN）、高（パスワード）の中から設定できます。 |
| **コードの長さ** | セキュリティレベルを低または中に設定した場合、パスワードや PIN の最低文字数を 4 ～ 16 文字の中から設定できます。セキュリティレベルを高に設定すると最低文字数を 6 ～ 16 文字の中から設定できます。 |
| **データ保護** | この機能を有効にすると、指定した回数ロック解除に失敗した場合、Android デバイスが初期状態に自動的にリセットされます。リセットするまでの回数は、10、15、20 回の中から選択できます。 |
| **コード有効期限** | この機能を有効にすると、パターンや PIN、パスワードなどのロックコードの有効期限を 1 ～ 12 ヶ月の間の中から設定できます。 |
| **デバイス自動ロック** | この機能を有効にすると、ロック画面に移行するまでの時間を設定できます。 |

## 6.3 デバイス設定ポリシー

デバイス設定ポリシーを有効に設定すると、定義済みデバイスを監視して、推奨値から設定が変更されると警告メッセージを表示できます。デバイス設定ポリシーでは、次のデバイスの監視設定が行えます。


| 項目名 | 内容 |
|---|---|
| **Wi-Fi** | パスワードが設定されていないオープンネットワークに接続したら警告を表示 |
| **GPS** | 無効に設定されたら警告を表示 |
| **位置情報サービス** | 無効に設定されたら警告を表示 |
| **メモリ** | メモリ低下時に警告を表示 |
| **データローミング** | データローミングを検出したら警告を表示 |
| **通話ローミング** | ローミングネットワークに接続したら警告を表示 |
| **不明な提供元** | 不明な提供元からのアプリケーションのインストールが許可されたら警告を表示 |
| **デバッグモード** | 有効に設定されたら警告を表示 |
| **NFC** | 有効に設定されたら警告を表示 |
| **記憶領域の暗号化** | 記憶領域が暗号化されていない場合に警告を表示 |
| **ルート化されたデバイス** | ルート化時に警告を表示 |

## 6.4 内蔵カメラの使用を制限

カメラの使用を制限を有効に設定すると、内蔵カメラの使用を制限できます。

# Chapter 7 フィッシング対策

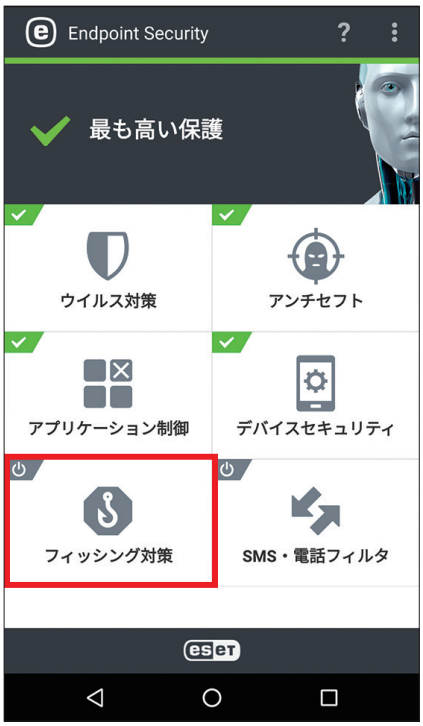
フィッシングとは、ソーシャルエンジニアリング ( 機密情報を入手するために、ユーザーを操ること ) を用いる犯罪行為を指します。フィッシングは、銀行の口座番号、クレジットカード番号、暗証番号、パスワードなどの機密データを入手するためによく使用されます。ESET Endpoint Security for Android は、フィッシング対策機能を搭載しています。フィッシング対策を有効にすると、ESET マルウェアデータベースに登録された Web サイトまたはドメインから実行されるすべての潜在的なフィッシング詐欺攻撃がブロックされ、攻撃を知らせる警告通知が表示されます。

## 7.1 フィッシング対策機能を有効にする

フィッシング対策は、次の手順で有効にできます。

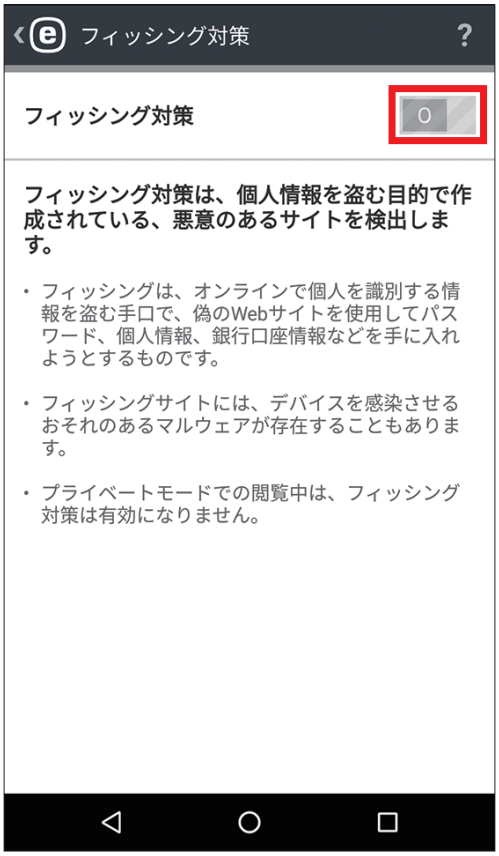
**操作手順**

1. メインメニューの［フィッシング対策］をタップします。

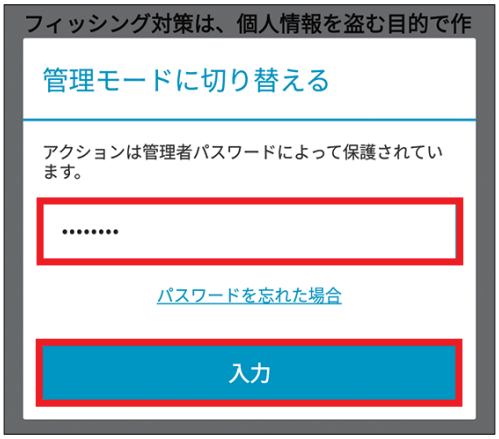



続く

2 [フィッシング対策] の 0 をタップします。




3 「管理モードに切り替える」画面が表示されたら、管理者パスワードを入力し、[入力] をタップします。




続く

4 フィッシング対策が有効に設定されます。


**ワンポイント**

［保護されていないブラウザをブロック］を有効にすると、保護されていないブラウザの利用をブロックできます。

# Chapter 8 SMS・電話フィルタ

SMS・電話フィルタは、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、SMS と電話フィルタの設定について説明します。

**!重 要**

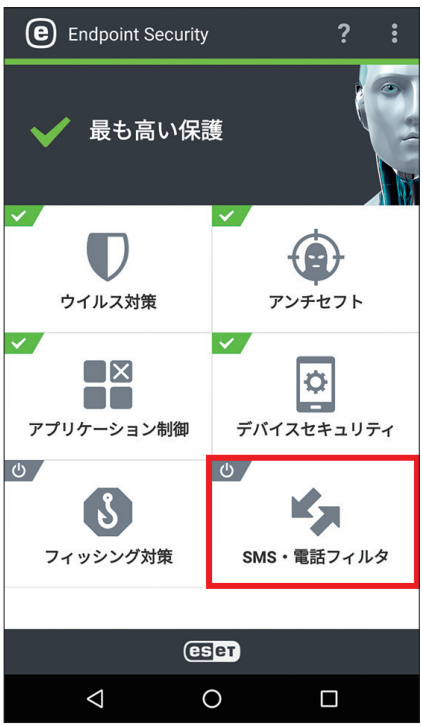
SMS・電話フィルタは、通話およびメッセージングをサポートしないタブレットでは動作しません。SMS や MMS のフィルタリングは Android 4.4（KitKat）以降のデバイスでは使用できません。また、Google ハンドアウトが SMS の主要アプリケーションとして設定されているデバイスではこの機能は無効となります。

## 8.1 SMS・電話フィルタを有効にする

SMS・電話フィルタを利用するには、SMS・電話フィルタを有効に設定し、ルールの作成を行う必要があります。SMS と電話フィルタは、次の手順で有効にできます。

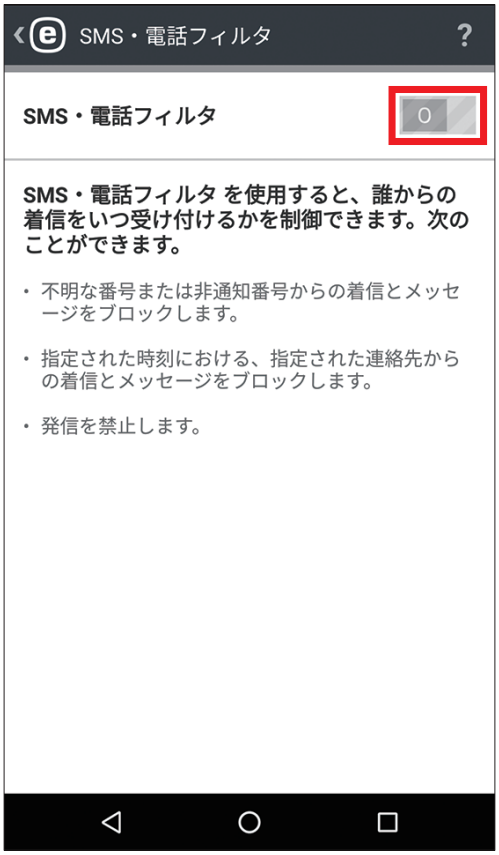
**操作手順**

1 メインメニューの［SMS・電話フィルタ］をタップします。

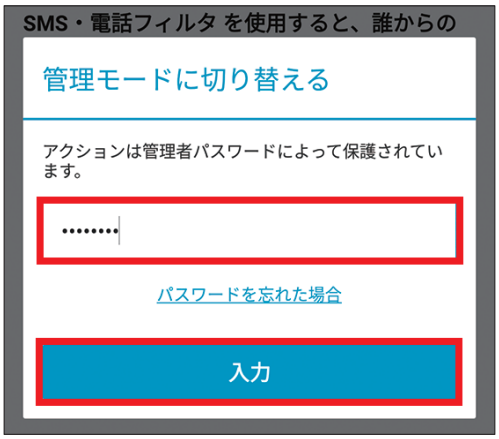



続く

2 [SMS・電話フィルタ]の 0 をタップします。

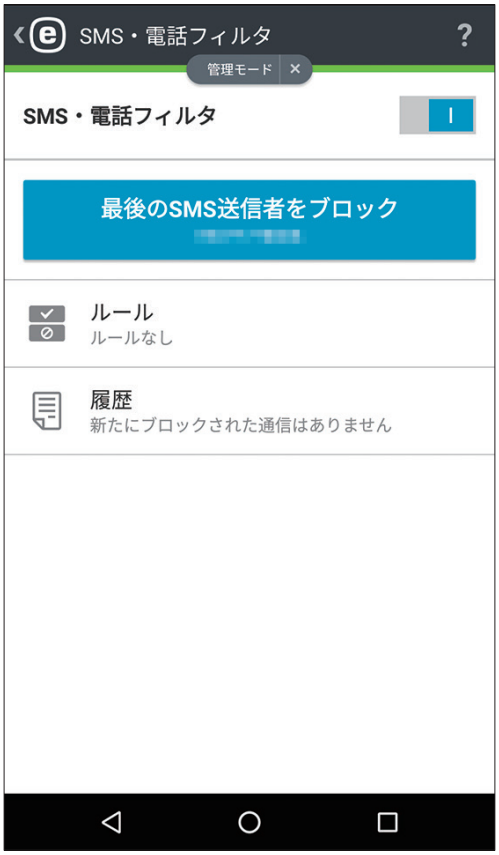



3 「管理モードに切り替える」画面が表示されたら、管理者パスワードを入力し、[入力]をタップします。




続く

4 SMS・電話フィルタが有効に設定されます。



## 8.2　ルールを追加する

SMS・電話フィルタで利用するルールには、ユーザールールと管理者ルールがあります。ユーザーは、管理者パスワードを入力せずにユーザールールを作成できます。管理者ルールは、管理者モードでのみ作成できます。管理者ルールはすべてのユーザールールを上書きし、優先的に適用されます。ルールの作成は、次の手順で行います。

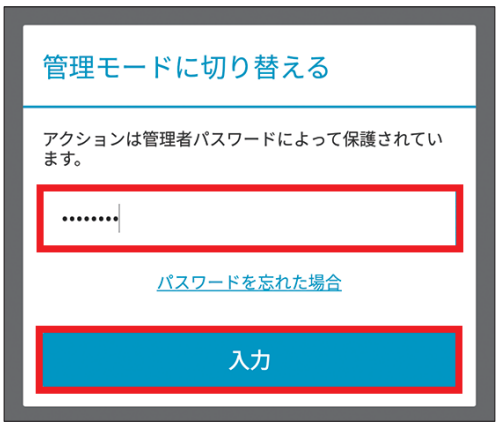
**操作手順**

1 メインメニューで［SMS・電話フィルタ］をタップし、［ルール］をタップします。


続く

2 [ユーザールール] または [管理者ルール] をタップします。ここでは、[管理者ルール] をタップし、[ルールの追加] または ＋ をタップします。


3 「管理モードに切り替える」画面が表示されたら、管理者パスワードを入力し、[入力] をタップします。




続く

4 作製するルールの内容を設定し、［保存］をタップします。ルールの内容は、以下の項目について設定できます。


| 項目名 | 内容 | |
|---|---|---|
| **アクション** | 実行する処理を［拒否］または［許可］の中から選択します。 | |
| **相手** | 対象とする相手を選択します。対象とする相手は、[個人］［グループ］［電話帳未登録の番号］［電話帳登録済みの番号］［すべての番号］［番号非通知］の中から選択できます。「個人」を選択した場合は、相手の名前（任意）や電話番号を設定できます。また、グループを選択した場合は、連絡先に保存された連絡先グループを選択できます。 | |
| **対象** | 処理の対象を次の中から選択します。 | |
| | 発信通話 | |
| | 着信通話 | |
| | 受信 SMS | |
| | 受信 MMS | |
| **時間帯** | ルールを適用する時間帯の設定を行います。指定した期間の間だけルールを適用するには、［常時］>［カスタム］をタップし、ルールを適用する曜日または期間を選択します。既定では、土曜日と日曜日が選択されています。 | |

**! 重　要**

海外からの SMS・通話を設定するときは、リストに入力されたすべての電話番号に国際ダイヤルコードを付け、その後に実際の番号を入力する必要があります。

続く

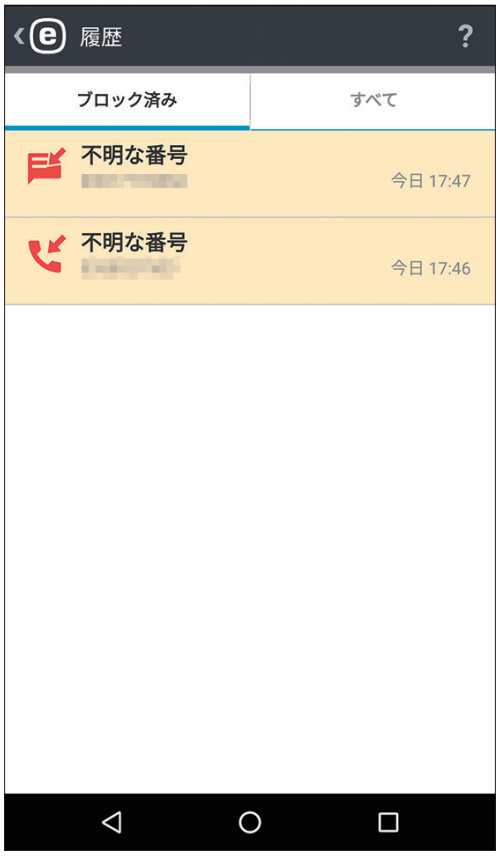
5 ルールが作成されます。


**ワンポイント**

［ルール］リストから既存のルールエントリを削除する場合は、削除したいエントリをロングタップしてから、［削除］アイコンをタップします。

## 8.3 履歴

［履歴］をタップすると、SMS・電話フィルタによってブロックまたは許可された通話とメッセージが表示されます。各ログにはイベント名、対応する電話番号、イベントの日時が含まれます。SMS および MMS メッセージログにはメッセージ本文も含まれます。ブロックされた電話番号と連絡先に関連するルールを変更する場合は、［履歴］をタップして編集したい履歴をタップし、［ルールの表示］をタップします。履歴を削除するには、削除したい履歴をタップして、［削除］をタップします。



# Chapter 9 設定

設定では、次の項目について EST Endpoint Security for Android の設定を行えます。設定を表示するには、メインメニューの ⋮ をタップして［設定］をタップします。

| 項目名 | 内容 |
|---|---|
| **言語** | 既定では、ESET Endpoint Security for Android はシステムロケール（Android OS 言語とキーボード設定）としてデバイスで設定されている言語でインストールされます。アプリケーションユーザーインターフェイスの言語を変更するには、［言語］をタップして、任意の言語を選択します。 |
| **国** | 勤務または居住している国を選択します。 |
| **アップデート** | ［アップデート］をタップすると、新しいバージョンの ESET Endpoint Security for Android を ESET Web サイトからダウンロードできるかどうかを確認します。なお、この機能は、Google Play Store を利用して ESET Endpoint Security for Android をインストールした場合には適用されません。Google Play Store からインストールした場合は、Google Play Store からアップデートが配信されます。 |
| **通知表示** | この機能を有効に設定すると、ESET Endpoint Security for Android のステータスを通知領域に常に表示します。 |
| **使用状況データの送信** | このオプションを使用すると、アプリケーションの使用状況に関する匿名データを送信し、ESET 製品の向上を支援します。機密情報は送信されません。 |
| **設定のインポート / エクスポート** | ［設定のインポート / エクスポート］をタップすると、利用中の Android デバイスの ESET Endpoint Security for Android の設定を設定ファイルにエクスポートしたり、設定ファイルのインポートを行えます。詳細については、「9.1 設定のインポート / エクスポート」をご参照ください。 |
| **管理者パスワード** | ［管理者パスワード］をタップすると、新しい管理者パスワードの登録や既存のパスワードを変更できます。詳細については、「9.2 管理者パスワード」をご参照ください。 |
| **Remote Administrator** | この機能をオンにすると、ESET Remote Administrator に利用中の Android デバイスを接続できます。詳細については、「9.3 ESET Remote Administrator」をご参照ください。 |
| **アンインストール** | ［アンインストール］をタップすると、アンインストールウィザードが実行され、ESET Endpoint Security for Android が完全にデバイスから削除されます。管理者パスワードを入力する必要があります。 |

# 9.1　設定のインポート / エクスポート

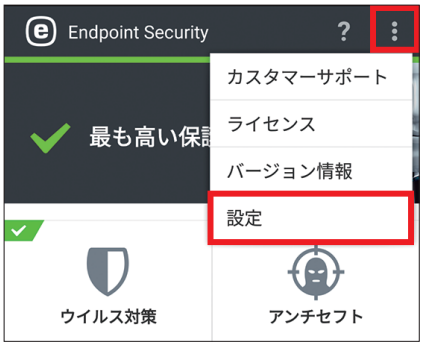
ESET Endpoint Security for Android は、設定ファイルのインポート / エクスポート機能を搭載しています。この機能を利用すると、Android デバイス同士で ESET Endpoint Security for Android の設定を共有できます。Android デバイスが ESET Remote Administrator によって管理されていない場合は、設定のインポート / エクスポート機能を利用することですべてのユーザーが同じ設定の Android デバイスを利用できます。また、エクポートした設定ファイルにライセンス情報を含めた場合、設定ファイルをインポートすることでアクティベーションも行えます。
※設定ファイルには、ESET Remote Administrator への接続情報は含まれません。

## 9.1.1　設定のエクスポート

ESET Endpoint Security for Android の現在の設定をエクスポートするには、次の手順で行います。また、エクスポートする設定には、ライセンス情報（製品認証キー）も指定できますが、この情報は暗号化されていません。ライセンス情報を含めるときは、注意してください。

**操作手順**

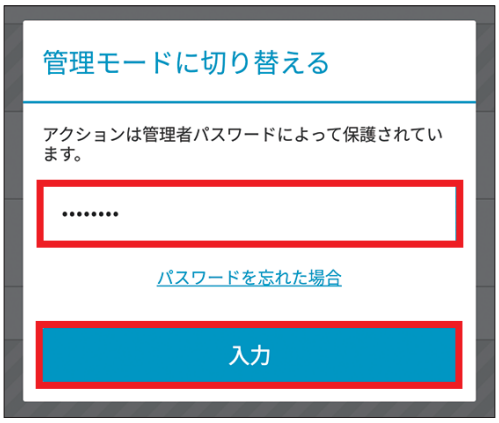
1. メインメニューのの⋮をタップし、［設定］をタップします。



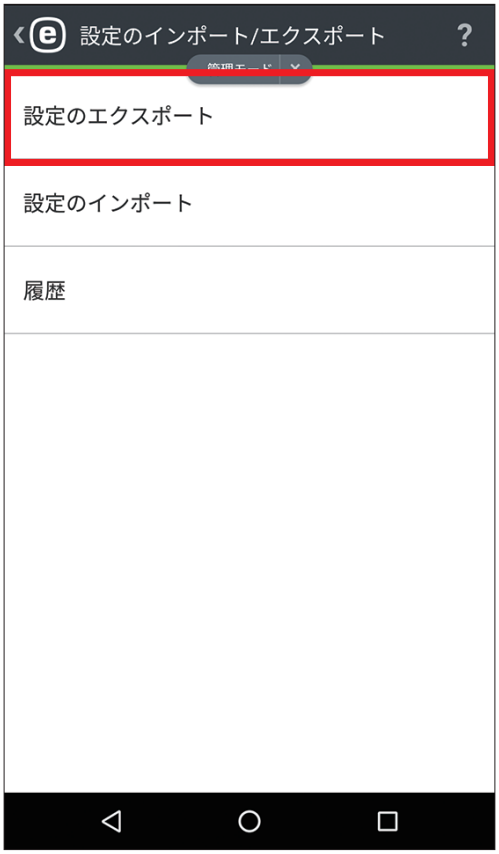

2. ［設定のインポート／エクスポート］をタップします。


続く

3 「管理モードに切り替える」画面が表示されたときは管理者のパスワードを入力し、[入力] ボタンをタップします。

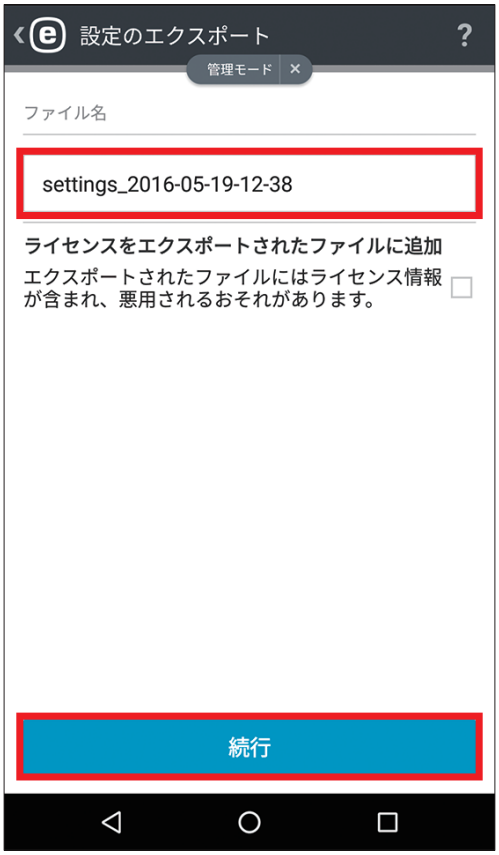



4 [設定のエクスポート] をタップします。




続く

5 ファイル名を必要に応じて変更し、［続行］ボタンをタップします。




**ワンポイント**

［ライセンスをエクスポートされたファイルに追加］をタップしてオンにすると、エクスポートする設定ファイル内にライセンス情報を含めることができます。

6 設定ファイルの共有方法をタップし、画面の指示に従って設定ファイルを保存します。


**ワンポイント**

［NFC サービス］をタップすると、NFC を利用して別の Android デバイスに設定ファイルを送信できます。［ドライブ］をタップすると、Google ドライブに設定ファイルを保存できます。［Gmail］をタップすると、設定ファイルを電子メールに添付して送信できます。

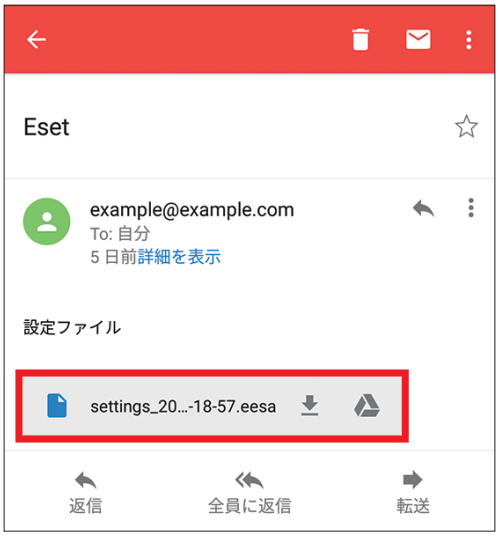
## 9.1.2 設定のインポート

設定ファイルをインポートするには、設定ファイルをタップします。また、［履歴］セクションのファイルを選択して設定をインポートすることもできます。

**操作手順**

ここでは、電子メールで設定ファイルをエクスポートした場合を例に設定ファイルのインポート手順を説明します。

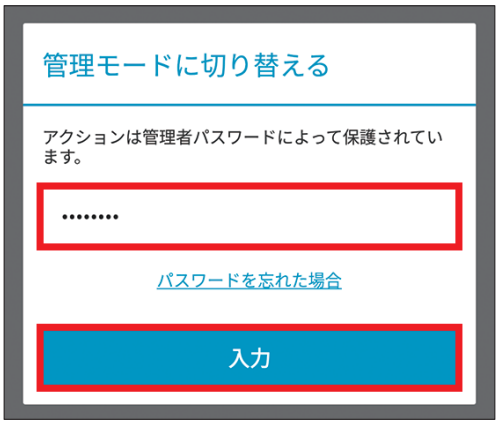
1 設定ファイルが添付された電子メールを開き、設定ファイルをタップします。



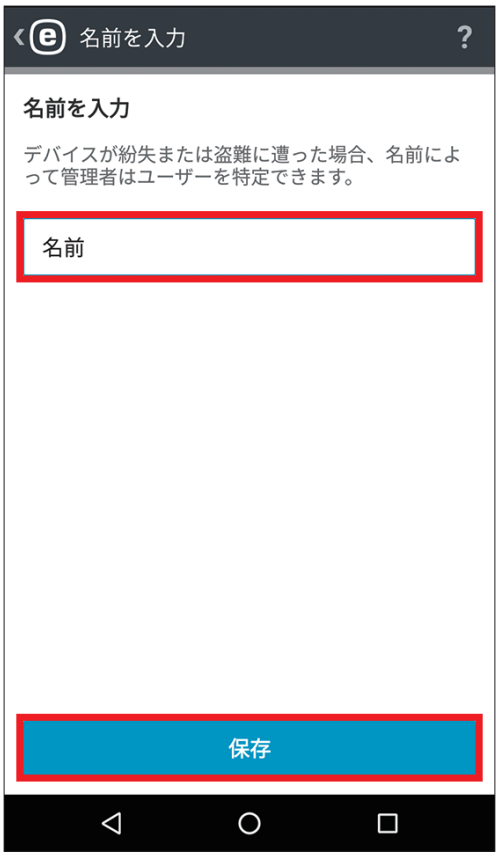

2 「インポート」をタップします。


続く

3 「管理モードに切り替える」画面が表示されたときは管理者のパスワードを入力し、[入力] ボタンをタップします。




4 必要に応じて名前を変更し、「保存」をタップします。




続く

5 「設定が正常に完了しました」を表示されたら設定のインポートは完了です。「OK」をタップします。


### 9.1.3 履歴

［履歴］には、インポートされた設定ファイルのリストが表示され、これらのファイルを共有、インポート、削除できます。［履歴］は、［設定のインポート / エクスポート］＞［履歴］で表示できます。

## 9.2 管理者パスワード

管理者パスワードは、Android デバイスのロックを解除したり、アンチセフトコマンドを送信したり、パスワード保護機能にアクセスして ESET Endpoint Security for Android をアンインストールしたりするために必要です。

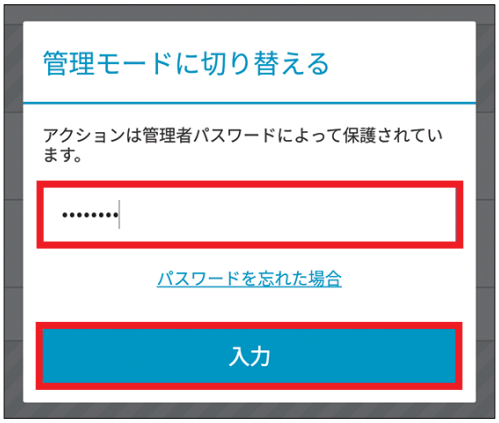
### 9.2.1 管理者パスワードを変更する

管理者パスワードの変更は、次の手順で行います。

**操作手順**

1 設定を開き、［管理者パスワード］をタップします。


2 「管理モードに切り替える」画面が表示されたら、管理者パスワードを入力し、［入力］をタップします。




続く

3 現在のパスワードを入力し、新しく設定したいパスワードを 2 回入力して、［保存］をタップします。


**! 重　要**

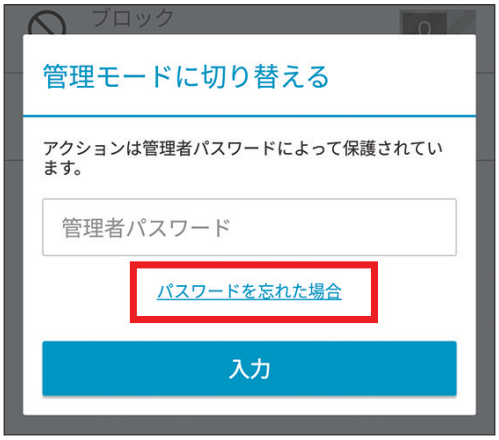
パスワードは注意して選択してください。セキュリティを強化し、他人が推測できにくいパスワードにするには、小文字、大文字、および数字を組み合わせて使用します。

## 9.2.2 パスワードをリセットする

管理者パスワードを忘れてしまった場合など、管理者パスワードのリセットを行いたいときは、パスワードのリセット申請を行います。パスワードのリセット申請を行うと ESET ライセンスに関連付けられた電子メールアドレスに確認コードとデバイス ID が記載された電子メールが送信されます。パスワードのリセットは、電子メールで送付された確認コードを利用して行います。パスワードリセットは次の手順で行います。

**操作手順**

1 管理者パスワードの入力画面で、［パスワードを忘れた場合］をタップします。

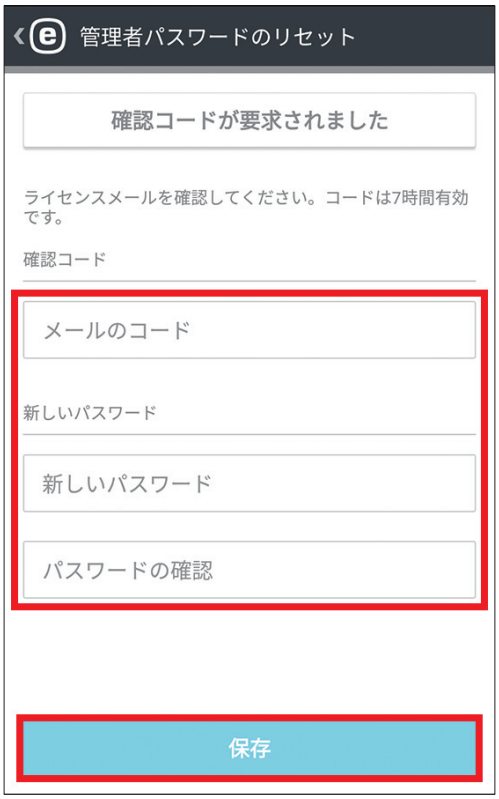



2 ［続行］をタップします。


続く

3 インターネットに接続している場合は、［確認コードの要求］をタップします。インターネットに接続していない場合は、［オフラインリセットを選択してください］をタップし、カスタマーサポートに連絡します。


4 電子メールで送付された確認コードを入力し、新しいパスワードを 2 回入力して、［保存］をタップします。



## 9.3 ESET Remote Administrator

ESET Remote Administrator を利用すると、ESET Endpoint Security for Android の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できます。また、Android デバイスを盗難または紛失したときには、アンチセフト機能を利用した盗難対策処理を行えます。ESET Remote Administrator で ESET Endpoint Security for Android をインストールした Android デバイスの管理を行うには、以下の要件を満たしている必要があります。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、ESET Endpoint Security for Android を ESET Remote Administrator を利用してリモートインストールすると、自動的に ESET Remote Administrator での管理設定が行われます。

- Mobile Device Connector のインストール
- モバイルデバイス登録

### 9.3.1 リモート管理の設定

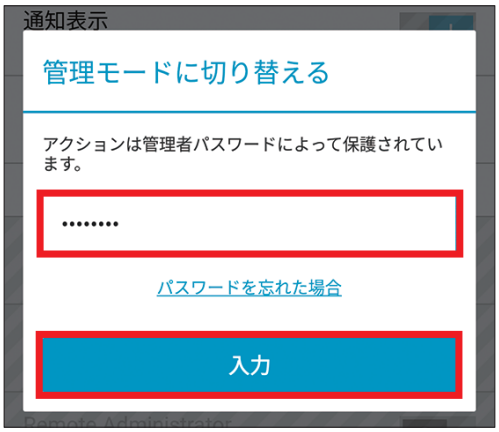
すでに利用中の ESET Endpoint Security for Android をインストールした Android デバイスを ESET Remote Administrator でリモート管理を行うには、ESET Remote Administrator への接続設定を行う必要があります。ESET Remote Administrator への接続設定は、以下の手順で行います。

**操作手順**

1 設定を開き、［Remote Administrator］をタップします。


続く

2 「管理モードに切り替える」画面が表示されたときは管理者のパスワードを入力し、[入力] ボタンをタップします。




3 Mobile Device Connector を実行しているサーバーの完全 DNS 名または公開 IP アドレスとポート番号を入力し、[接続] をタップします。

**! 重 要**

ESET Remote Administrator 6.5 以降と接続する場合は、ESET Remote Administrator で管理者が生成したトークン（一意の文字列）をポート番号の後に入力してください。
（https://MDCserver:port/ トークン）


続く

4 接続成功と表示されたら、設定は完了です。［終了］をタップします。

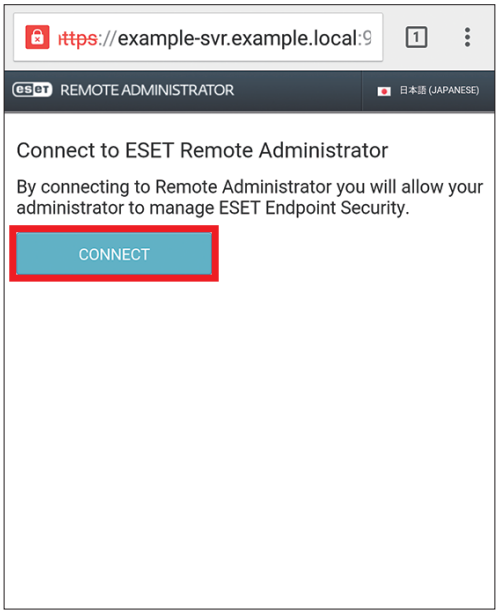
## 9.3.2 リモートインストール

ESET Endpoint Security for Android を ESET Remote Administrator を利用してリモートインストールすると、自動的に ESET Remote Administrator での管理設定が行われます。ここでは、リモートインストールの手順を説明します。

**操作手順**

1. メールアプリで登録リンクが記載されたメールを開き、リンクをタップします。


2. [CONNECT] ボタンをタップします。



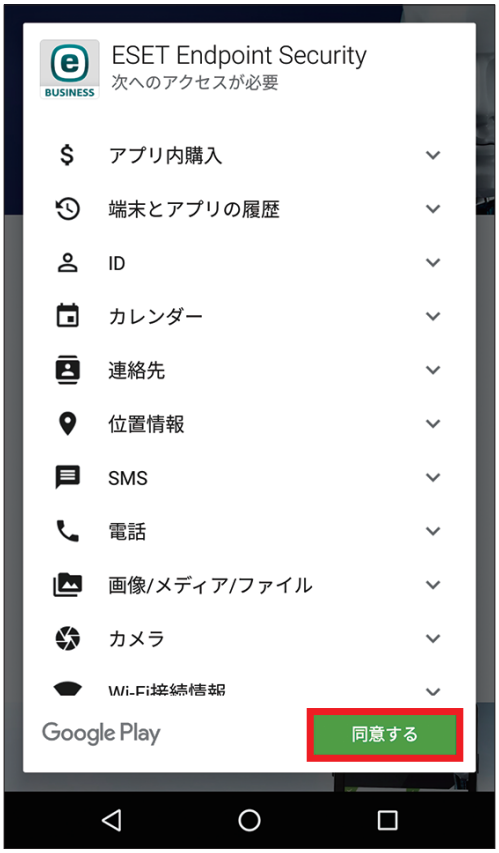

**ワンポイント**

セキュリティの警告画面が表示されたときは、[詳細設定] をタップして、[...（ドメイン名）にアクセスする] をタップします。

続く

3 Google Play Store に移動し［インストール］ボタンをタップします。


4 ［同意する］ボタンをタップすると、インストールが開始されます。




続く

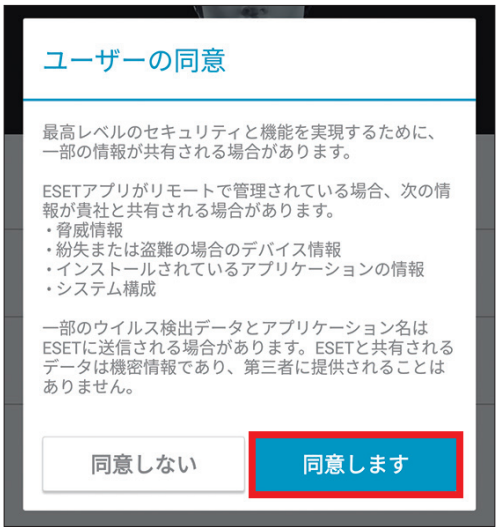
5 インストールが完了したら、［開く］ボタンをタップします。


6 ［管理者設定］ボタンをタップします。


続く

7 [同意します] ボタンをタップします。

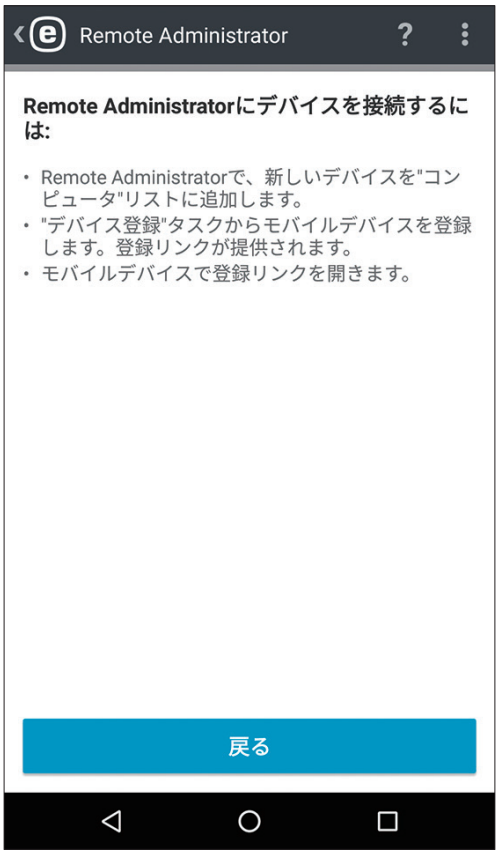

8 [同意します] ボタンをタップします。



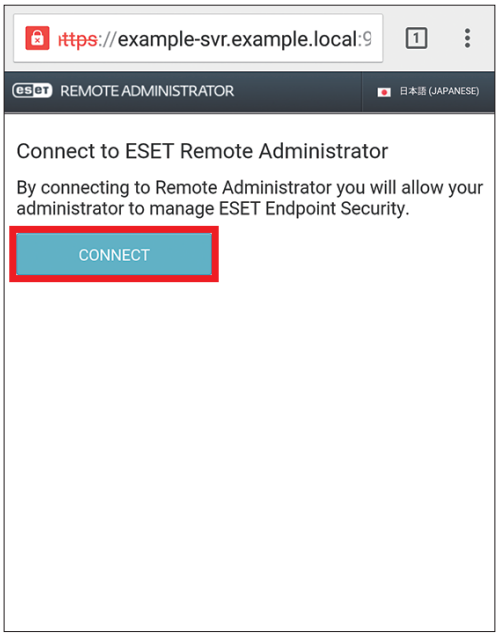

9 [はい、Remote Administrator に接続します] ボタンをタップします。


続く

10 Remote Administrator に接続するための情報が表示されます。ホームボタンをタップして、再度、メールアプリで登録リンクが記載されたメールを開き、リンクをタップします。




11 [CONNECT] ボタンをタップします。



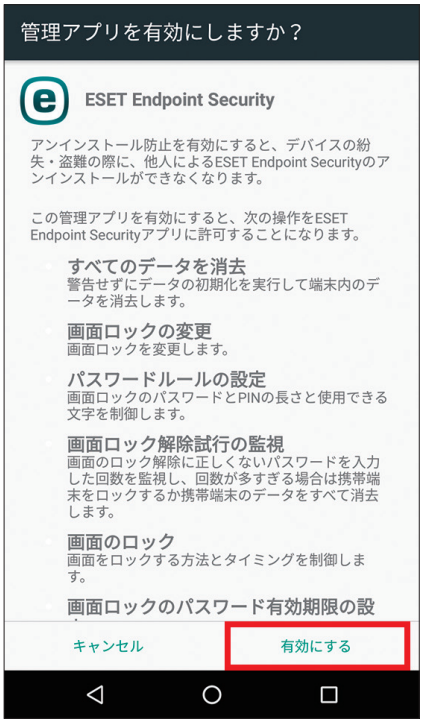

続く

12 名前の入力画面が表示されます。必要に応じて名前の修正を行い、［保存］ボタンをタップします。

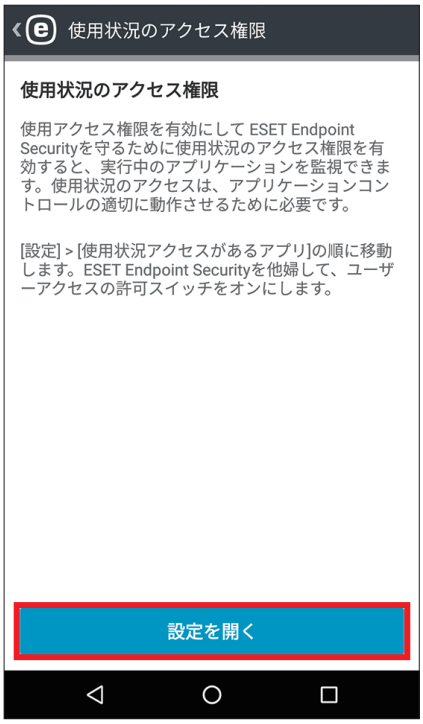

13 ［有効］ボタンをタップします。


続く

14 ［有効にする］をタップします。



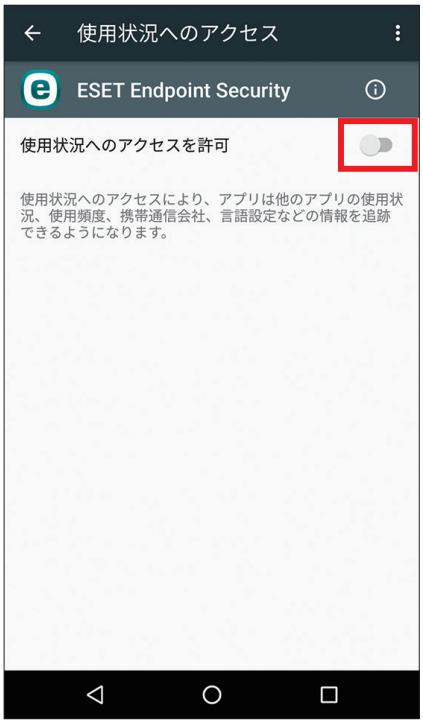

15 ［設定を開く］ボタンをタップします。




続く

16 ［ESET Endpoint Security］をタップします。


17 「使用状況へのアクセスを許可」の右側にあるスライドバーをタップします。




続く

18 「セットアップが完了しました」と表示されます。［閉じる］ボタンをクリックします。ESET Endpoint Security for Android のインストールはこれで完了ですが、この時点では、まだアクティベーションや管理パスワードの設定は行われていません。アクティベーションや管理パスワードの設定は、ERA サーバーから行えます。
アクティベーションの詳細については、「ESET Remote Administrator ユーザーズマニュアル」を参照してください。
管理パスワードの設定は、ポリシーで行うことができます。詳細については、「ESET Remote Administrator ユーザーズマニュアル」を参照してください。

# Chapter 10 サポート

ESET Endpoint Security for Android には、お客様への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。

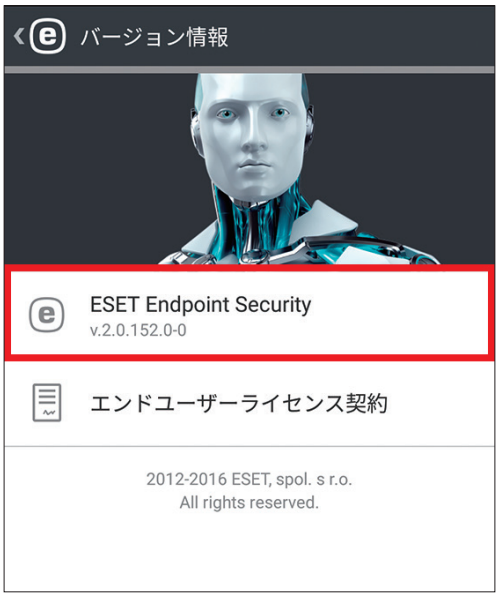
## 10.1　バージョン情報の確認

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。

**操作手順**

1. メインメニューの⋮をタップし、［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。

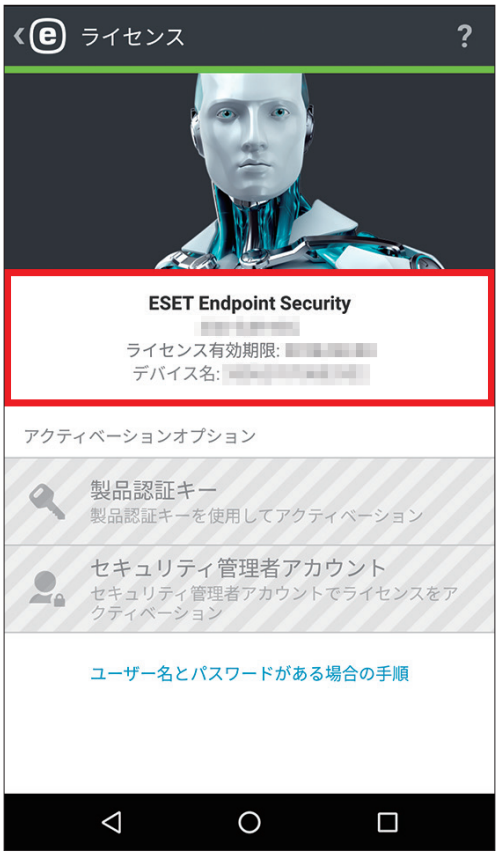


## 10.2　ライセンス情報を確認する

**操作手順**

1 メインメニューの⋮をタップし、［ライセンス］をタップします。


2 ライセンス情報が表示されます。



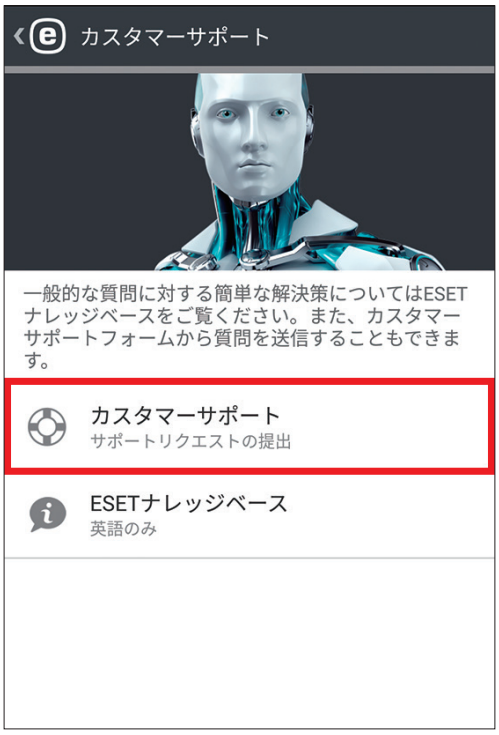
## 10.3　カスタマーサポート

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。

**操作手順**

1 メインメニューの⋮をタップし、［カスタマーサポート］をタップします。


2 ［カスタマーサポート］をタップします。



3 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、「アプリケーションログの送信」のチェックがオンになっていることを確認して、［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。