ESET PROTECTソリューション
ESET Endpoint Security for Android V3
機能紹介資料

第9版

2024年3月29日

キヤノンマーケティングジャパン株式会社

はじめに

- 本資料は、Android向け総合セキュリティ製品であるESET Endpoint Security for Android V3.x (以降EESA)の動作環境や主な機能について説明した資料です。
- 本資料の画面ショットは、ESET Endpoint Security for Android V3.6.6.0 で取得しております。そのため、バージョンによっては表示画面が一部異なる場合がございます。

もくじ

1. EESAの概要と動作環境

EESAの概要

基本的なウイルス/フィッシング対策の他、紛失/盗難時のリモート制御などが可能なアンチセフト、クラウド型セキュリティ管理ツール（ESET PROTECT）による管理に対応したAndroid向け総合セキュリティプログラムです。
※ESET PROTECT（以降EP）

EESAの動作環境

タッチスクリーン解像度：480x800 px
OS　　：Android 6.0/7.0/7.1/8.0/8.1/9.0/10.0/11.0/12.0/13.0
CPU　　：600MHz以上
　　ARMとARMv7命令セット、x86 Intel Atom
内部ストレージ　　：20MB以上の空き
インターネット接続　　：必須

※インターネット接続環境が必要です。
※Android Goはサポート対象外となります。
※microSDカード等の外部ストレージへのインストールには、対応しておりません。
※デュアルSIM、ルート化されたデバイス及びマルチユーザー環境下での動作については、サポートしておりません。
※アンチセフトや通話フィルターは通話とメッセージングをサポートしていないタブレットでは使用できません。
※Android6.0以降では、ワイプ機能を実行すると、拡張初期設定リセット機能の動作をします。
※ご利用時の注意事項の詳細は下記サポートサイトをご確認ください
▼Android向けクライアント用プログラムのご利用の際の注意事項について
https://eset-support.canon-its.jp/faq/show/8636?site_domain=business

1. EESAの概要と動作環境

EESAの特徴

・**スケジュール検査ができます。**
オンデマンド検査、リアルタイムでの検査に加えて、検査を実施する曜日と時間を設定して、
ユーザーへの負荷が少ない時間帯を指定した検査ができます。

・**アプリケーションの制御ができます。**
ユーザーに業務と関係ない不要なアプリケーションの使用を禁止できます。

・**フィッシング対策ができます。**
個人情報を盗んだり、悪意のあるサイトへの接続を防止することができます。

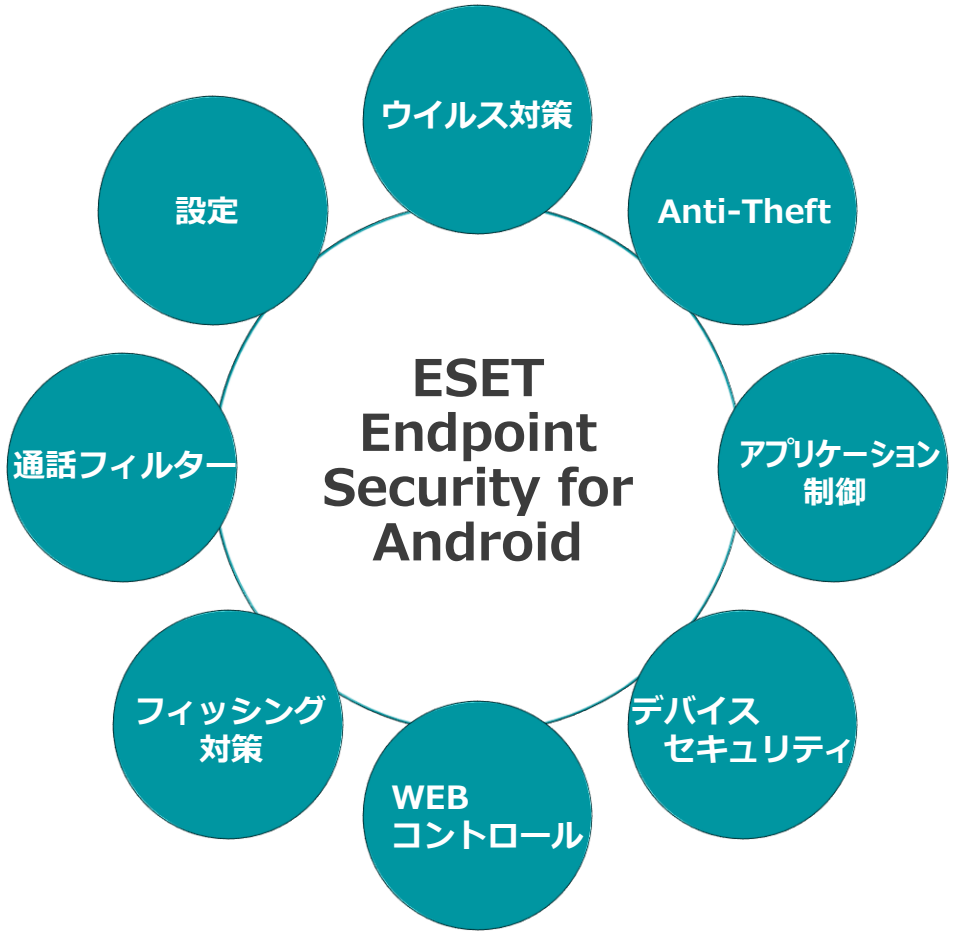
・**セキュリティ管理ツール(EP)からほぼリアルタイムでタスクとポリシーを送信できます。**
Firebase Cloud Messagingを利用したプッシュ通知を利用することで、ほぼリアルタイムでの
タスクとポリシーの送信を実現しました。

・**SIMが無いデバイスにもアンチセフト機能を使用できます。**
セキュリティ管理ツール(EP)で管理することで、SIMが無いデバイスでもアンチセフト機能を使用できます。

・**Google Playよりインストールが可能になりました。**
弊社ユーザーズサイト、またはGoogle Playよりインストールできます。

2. EESAの主な機能

- EESAは主に以下の機能で構成されております



2. EESAの主な機能

1. ウイルス対策

- ウイルス対策機能は、任意のタイミングで実行可能なオンデマンド検査と、ユーザーが操作するファイルに対して検査が行われるリアルタイム検査とあらかじめ定義した条件で検査が行われる自動検査の3種類の検査があります。

オンデマンド検査	リアルタイム検査	自動検査
・検査レベルが2つあります ・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ファイルとSOファイルの内容を検査します ・詳細検査は、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	・ユーザーが操作するファイルをリアルタイムに検査します ・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。	・充電中に検査が有効な場合はデバイスがアイドル状態の時に検査が自動的に開始します(完全に充電され、充電器に接続されている場合) ・スケジュールを設定することで、事前に定義した時刻に自動的に検査が実行されます

※オンデマンド検査は、バックグラウンドで検査する事が可能です。検査中に「ホーム」ボタンを押した場合や別画面に移動しても検査は継続されます。

2. EESAの主な機能

1. ウイルス対策

- デバイス検査は以下の流れで行うことができます

◎ タップ ⇨ 画面遷移

※検査中に「ホーム」ボタンを押した場合や別画面に移動しても検査は継続されます。

2. EESAの主な機能

1. ウイルス対策

- スケジュール検査は以下の流れで設定ができます

◎ タップ ⇨ 画面遷移

2. EESAの主な機能

2. Anti-Theft

- アンチセフトは、モバイルデバイスを不正アクセスから保護します。
  セキュリティ管理ツール(EP) を使用することで、スマートフォンやタブレットデバイスの盗難や紛失時に、他人が勝手にSIMカードを交換して利用することや情報流出を防止します。
  ※SIMカードのない機器でもタスク機能を利用することで機能が使用できます。

機能名	機能の説明
検索	Googleマップ上で対象デバイスのGPS情報を含んだリンクをテキストメッセージで受信できます。 より正確な位置情報が利用可能な場合は、10分後に新しいGPS座標がもう一度デバイスから送信されます。
警報/紛失モードサウンド	対象デバイスはロックされ、しばらくの間、またはロック解除されるまで大音量が鳴ります。
ロック	デバイスのロックが可能です。管理者パスワードの入力またはセキュリティ管理ツールからロック解除コマンドを送信した場合にのみデバイスのロック解除が可能です。
ロック解除	対象デバイスのロックが解除され、デバイスに挿入されているSIMカードが信頼できるSIMカードとして登録されます。
初期設定リセット	デバイスを初期設定(既定の出荷時の設定)にリセットします。全てのアクセス可能なデータが削除されます。 これには数分かかる場合があります。

2. EESAの主な機能

2. Anti-Theft

- アンチセフト機能を使用するためには以下の項目を設定する必要があります。

管理者連絡先	•管理者の電話番号を登録することが出来ます
ロック画面情報	•デバイスがロックされている時に表示する情報の編集ができます •会社(任意)、電子メールアドレス(任意)、カスタムメッセージ(任意)が編集対象です
信頼するSIMカード	•EESAによって許可される信頼できるSIMカードを確認、追加することができます •許可されていないSIMカードが挿入されると、画面がロックされ管理者にアラートが送信されます

※Android 10.0 以降で EESAをご利用の場合、Googleの仕様変更によりアンチセフトのメニューに「信頼するSIMカード」の設定が表示されません。

2. EESAの主な機能

2. Anti-Theft

- ロック画面情報で管理者は会社名、電子メールアドレス、メッセージを定義することができます。また、ここで定義した情報は、デバイスがロックされているときに、管理者の連絡先と一緒に表示されます。

◎ タップ ⇨ 画面遷移

ロック画面情報の設定の流れ

デバイスロック時の画面

2. EESAの主な機能

3. アプリケーション制御

- アプリケーション制御を利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ます。ブロックルールに定義されたアプリケーションへのアクセスをブロックします。また、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。

ブロックルール作成の流れ

タップ　画面遷移

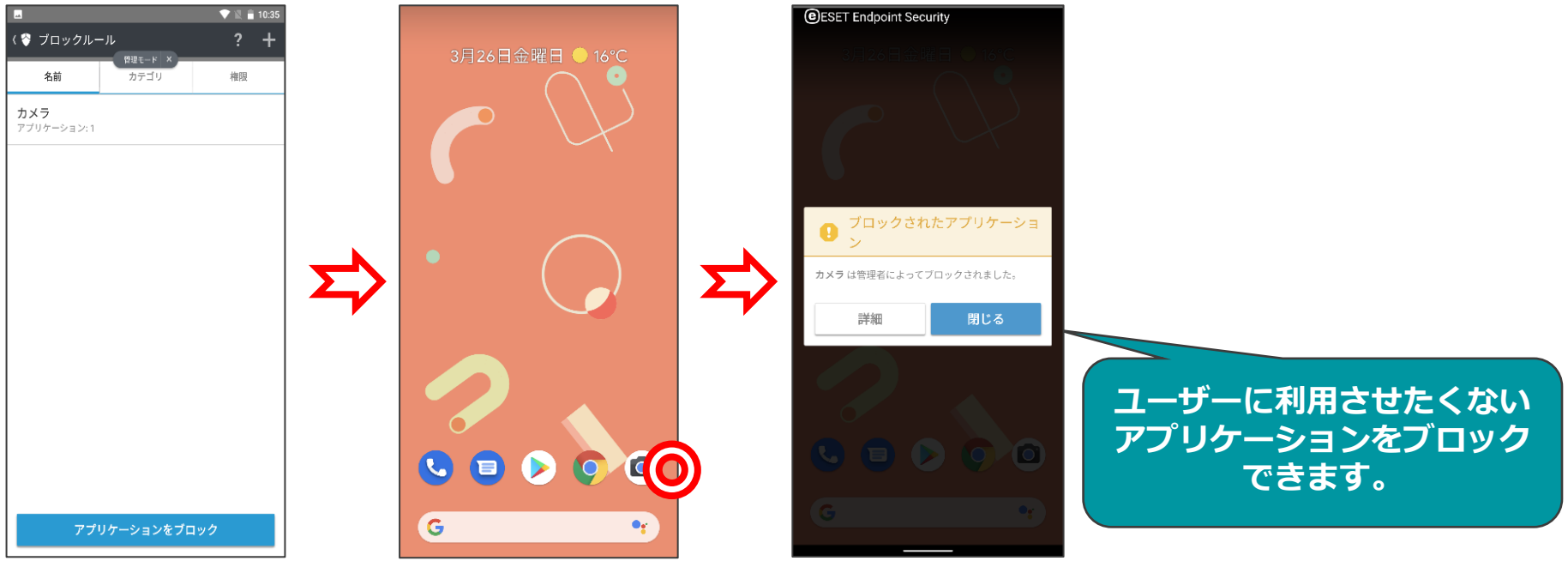
2. EESAの主な機能

3. アプリケーション制御

- 実際に画面をブロックすると、以下の画面が表示されます。
  ここでは例として[カメラ]をブロックしています。

アプリケーションをブロックした画面

タップ　画面遷移

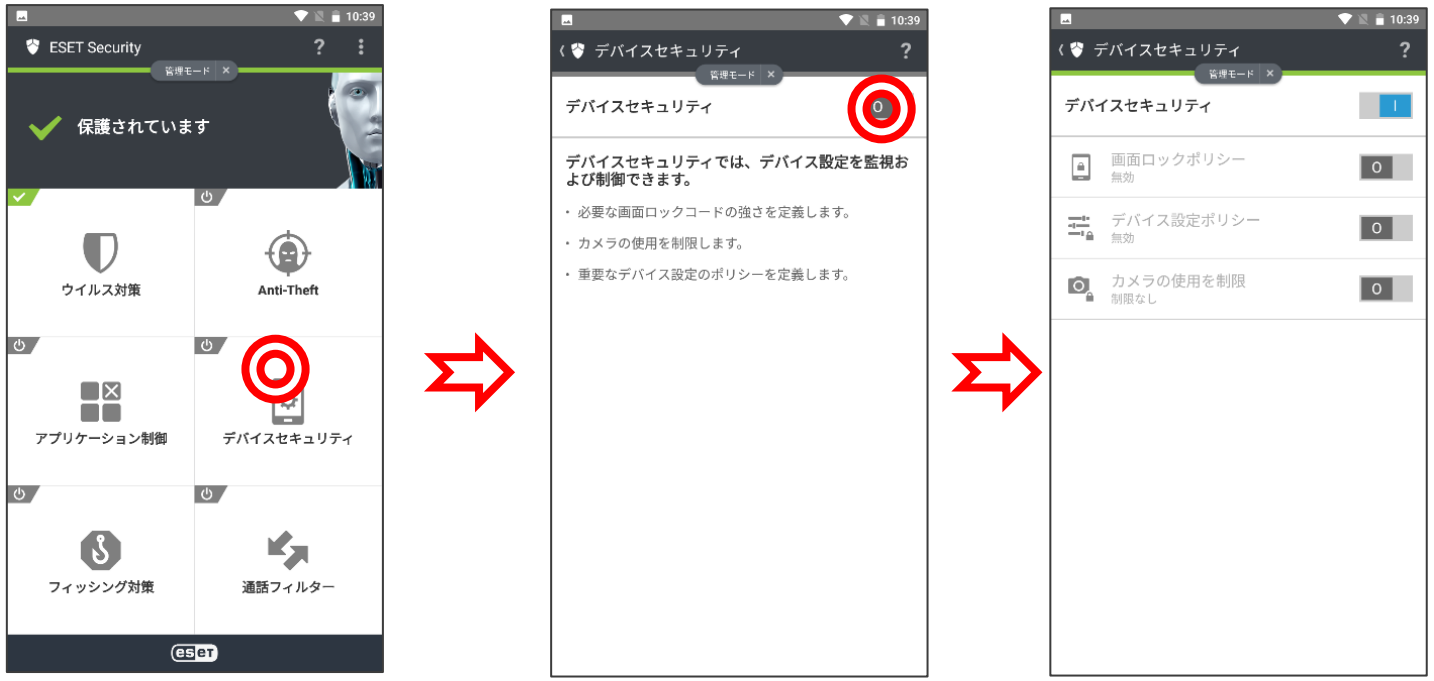


2. EESAの主な機能

4. デバイスセキュリティ

- デバイスセキュリティは、画面ロック時のセキュリティレベルを変更できる[画面ロックポリシー]、デバイス設定が推奨設定になっているか監視する[デバイス設定ポリシー]、カメラの使用制限ができる[カメラの使用を制限]で構成されています。

タップ　画面遷移



※ Android10以降の場合、「カメラの使用を制限」はデバイス所有者モードでのみ使用可能です。

2. EESAの主な機能

4. デバイスセキュリティ

- デバイスセキュリティには、デバイスが下記の推奨状態を外れた場合にアラートを表示する[デバイス設定ポリシー]を設定できます

機能名	機能の説明
Wi-Fi	オープンネットワークに接続したらアラートが表示されます。
GPS	無効になっていたらアラートが表示されます。
位置情報サービス	無効になっていたらアラートが表示されます。
メモリ	メモリ低下時にアラートが表示されます。
データローミング	データローミングが検出されたらアラートが表示されます。
通話ローミング	ローミングネットワークに接続したらアラートが表示されます。
不明な提供元	不明な提供元からのインストールが許可されたらアラートが表示されます。
デバッグモード	デバックモードが有効時にアラートが表示されます。
NFC	NFCが有効時にアラートが表示されます。
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アラートが表示されます。
ルート化されたデバイス	ルート化時にアラートが表示されます。

2. EESAの主な機能

4. デバイスセキュリティ

- デバイス設定ポリシーの設定の流れは、以下になります

◎ タップ ⇨ 画面遷移

2. EESAの主な機能

5. フィッシング対策

- フィッシング対策は、ソーシャルエンジニアリングを用いて個人情報を盗む目的で作成されているサイト、悪意のあるサイトを検出します。フィッシング対策保護を完全に活用するには、サポート対象外のWebブラウザをブロックすることをお勧めします。

フィッシング対策を有効にする流れ

ブロック時の画面

◎ タップ ⇨ 画面遷移

2. EESAの主な機能

6. WEBコントロール

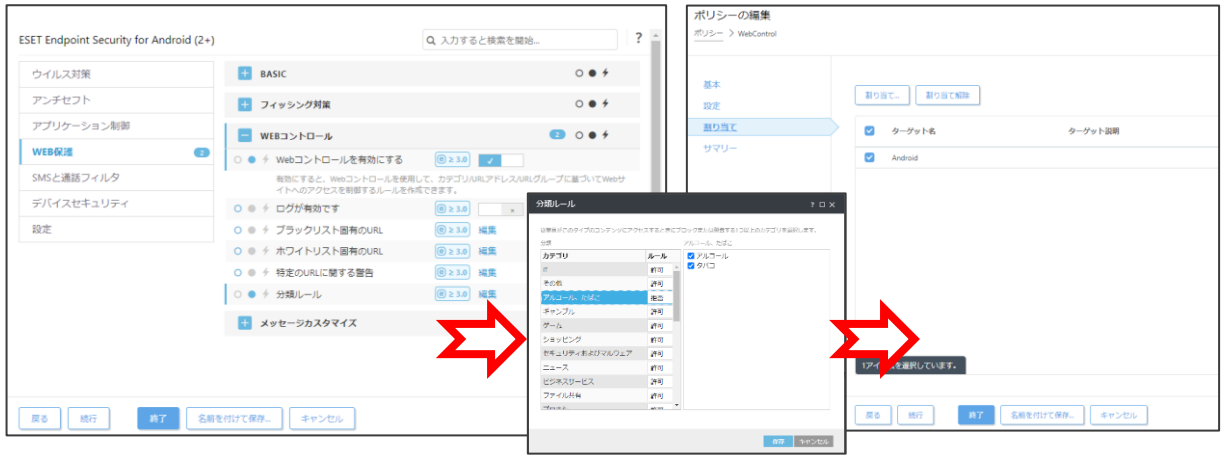
- Webコントロール機能によって、WebサイトをURLやカテゴリごとに接続の許可や拒否の設定を行うことが可能です。これにより、ユーザーの生産性を低下させたり、悪影響を与えたりする可能性のある不適切または有害なコンテンツやページにアクセスすることを防ぐことが可能です。

※Webコントロールが機能するには、管理されたデバイスが次の要件を満たしている必要があります。

- ESET Endpoint Security for Androidバージョン3以降
- Androidバージョン8以降
- デバイス管理者権限でESET PROTECTに登録

WEBコントロールを有効にする流れ

※セキュリティ管理ツールでのみ設定可能です。



ブロック時の画面

2. EESAの主な機能

7. 通話フィルター

- 通話フィルターは、電話の発信/着信やその相手などを定義したルールに基づいて許可/拒否のアクションを行います。電話番号を入力、または電話帳から指定し、個別にルール作成を行うことが可能でユーザールールと管理者ルールを分けて作成できます。また、ルール作成時にはワイルドカードを利用できます。

※Google Playよりプログラムをインストールした場合は本機能を利用できません。
※ルール作成時のワイルドカードの利用はV3.5以降より対応しております。

アクション	•許可 •拒否
相手	•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
名前	•名前　電話番号
対象	•発信 •着信
時間帯	•常時 •カスタム

2. EESAの主な機能

7. 通話フィルター

- ルール作成は以下の流れとなります

◎ タップ ⇨ 画面遷移

2. EESAの主な機能

7. 通話フィルター

- 実際にデバイスAで着信ブロックを実施すると、ブロックした対象のデバイスBから着信があった場合は、デバイスAでは不在着信となります。またブロックされたデバイスBでは「話し中」（デバイスにより動作が異なる場合があります）となり、デバイスAからブロックされていることはわかりません。

ブロックした場合のデバイスAの画面

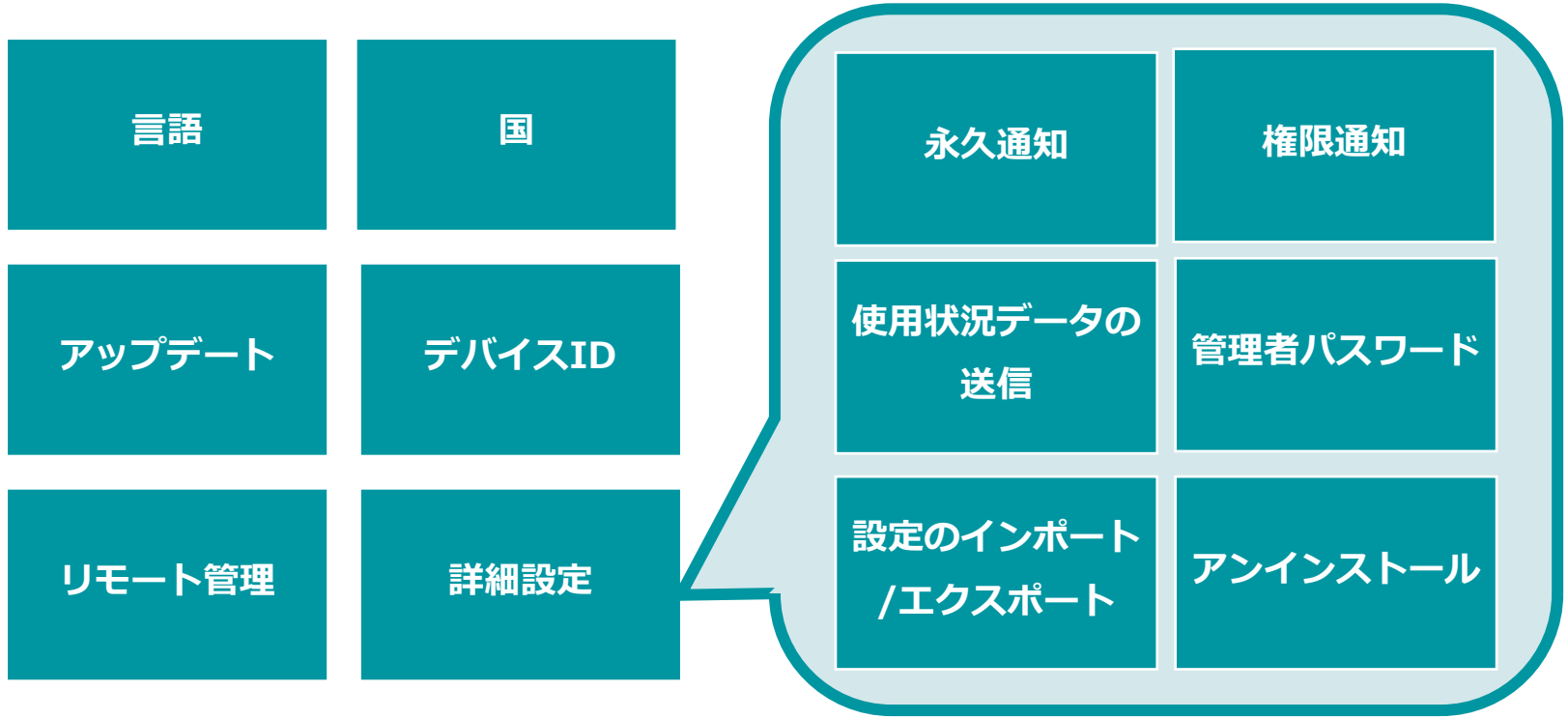
◎ タップ ⇨ 画面遷移

2. EESAの主な機能

8. 設定

- 設定ではEESAの各種設定の変更と確認ができます

設定の項目



2. EESAの主な機能

8. 設定

- 管理者パスワードは、他者による不正利用の防止を実現します。また、パスワード保護を設定することで、各種機能の設定変更やアンインストールを防止します。EESAインストール時に設定できます。
  また、管理者パスワードは[設定]より変更できます。

◎ タップ ⇨ 画面遷移

※初回設定時

※管理者パスワード変更画面

2. EESAの主な機能

8. 設定

- リモート管理の設定は、セキュリティ管理ツール (EP)と連携を行うための設定です。
  セキュリティ管理ツールからデバイスの操作を実行する為には、接続するセキュリティ管理ツールの情報をデバイスに入力しておく必要があります。

◎ タップ ⇨ 画面遷移

3. EESAの導入について

導入方法

- EESAをダウンロードするには下記の方法があります。

  1. 弊社ユーザーズサイトにログインしていただき、[プログラム/マニュアル]よりEESAをダウンロードをする方法

  2. Google PlayよりEESAをダウンロードする方法
     ※ただしGoogle Play版を利用する場合は事前に下記サポートサイトをご確認ください
     ▼Google Playからダウンロードしたプログラムの利用について
     https://eset-support.canon-its.jp/faq/show/21263?site_domain=business

ユーザーズサイト

Google Play

4. EESAの管理について

セキュリティ管理ツールとの接続構成

- EESAをセキュリティ管理ツールで管理する為には以下の条件確認や作業が必要です。

1. 管理するためには、モバイルデバイスをセキュリティ管理ツールの[コンピュータ]へ登録する必要があります。登録には以下の2つの方法があります。

   -**電子メール**…登録用リンクがモバイルデバイスに送信されます
   -**QRコード**…モバイルデバイスでセキュリティ管理ツールの画面上のQRコードを読み取ります

   -**セキュリティコード**…制限されたデバイスをご利用の場合、モバイルデバイスにインストールしたEESAでセキュリティコードを表示させます (※EESA V3.3以降で利用可能)

2. 受信したメールの登録用リンク / QRコードの読み取り、またはセキュリティコードの入力を実施することでセキュリティ管理ツールへの接続が開始され、管理が行われます。

※セキュリティ管理ツールで管理をしない場合でも、EESAのほとんどの主要機能は利用可能です。

4. EESAの管理について

セキュリティ管理ツールとの連携機能

- セキュリティ管理ツールで収集可能な項目は以下の通りです

概要	•名前/MACアドレス/製品名/製品バージョン/検出エンジンのバージョン/ セキュリティ管理ツールへの最後の接続/前回の検査時刻/Androidバージョン 等
コンフィグレーション	•ESET製品の設定の詳細 / 適用されたポリシー
タスクの実行	•タスク名、タスクタイプ、ステータス
アラート	•問題、ステータス、重要度
脅威と隔離	•全ての脅威タイプ、ウイルス名、解決された脅威、発生日時　等
詳細	•デバイスID、OS情報、最後のロケーション / ハードウェア情報 / 製品およびライセンス情報 等

4. EESAの管理について

セキュリティ管理ツールから実行できるタスク

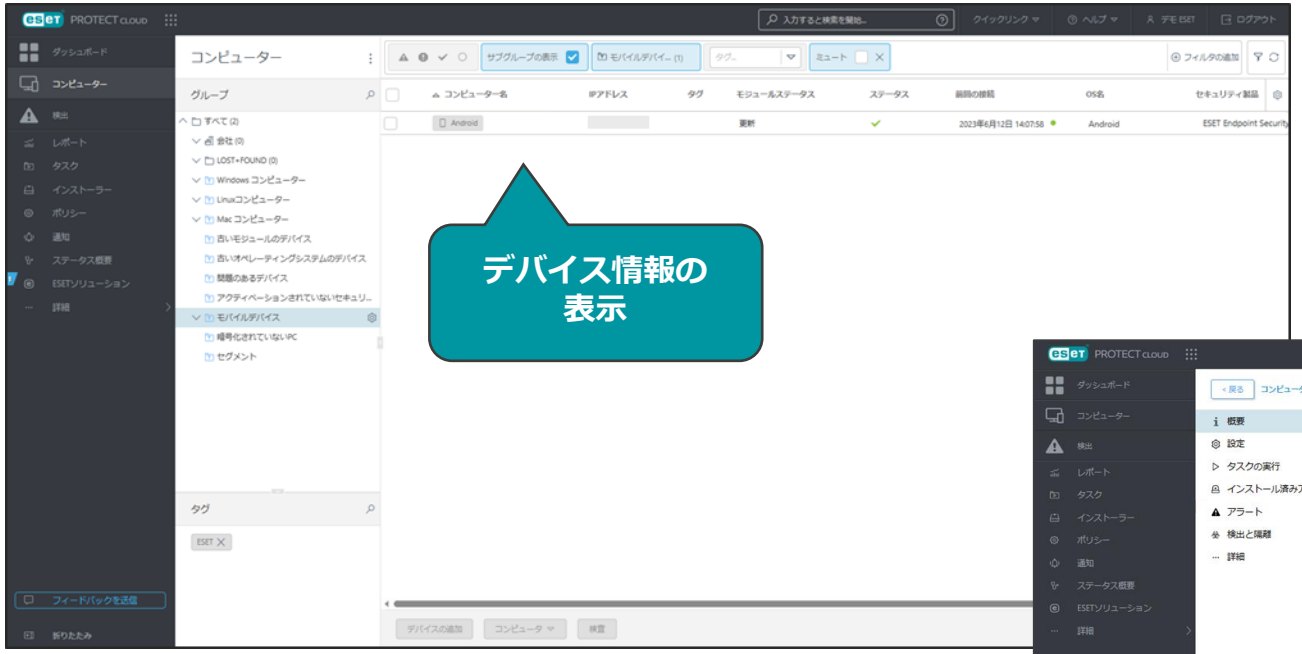
- セキュリティ管理ツールからEESAに対して、以下のタスクを実行できます

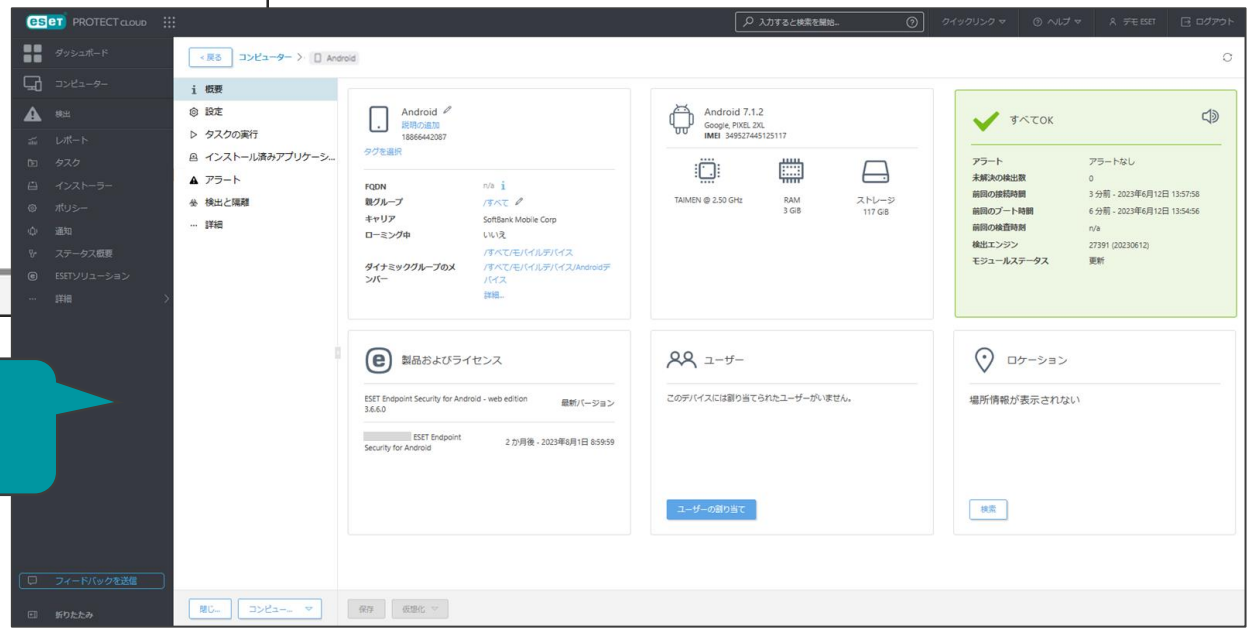
セキュリティ管理ツールから実行できるタスク

タスク名	説明
ESET製品の設定エクスポート	設定情報をEESAからエクスポートしてセキュリティ管理ツールで表示
アンチセフトアクション	以下5種類のアクションを選択 ・検索　・警報/紛失モードサウンド　・ロック　・ロック解除 ・初期設定リセット
オンデマンド検査	オンデマンド検査
ソフトウェアインストール	Androidデバイスにソフトウェアをインストール
メッセージの表示	Androidデバイスにメッセージを表示
モジュールアップデート	モジュール（検出エンジン）の更新
管理の停止	管理対象から削除
製品のアクティベーション	アクティベーションを実施

4. EESAの管理について

EPでの管理イメージ





※画面はESET PROTECT V4.4のものです。