ESET Endpoint Protection シリーズ
ESET Endpoint Security for Android V2
機能紹介資料

ENDPOINT PROTECTION ADVANCED
イーセット エンドポイント プロテクション アドバンスト

ENDPOINT PROTECTION STANDARD
イーセット エンドポイント プロテクション スタンダード

第9版
作成：2020年1月16日

Canon
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 V2(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 V2.7で取得しております。そのため、バージョンによっては各機能の名称が異なる可能性がございます。

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、ESET Security Management Center（以降ESMC）またはESET Remote Administrator（以降ERA）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。

EESAの動作環境

タッチスクリーン解像度： 480x800 px
OS　　：Android 5.0/5.1/6.0/7.0/7.1/8.0/8.1/9.0
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。
※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。

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。

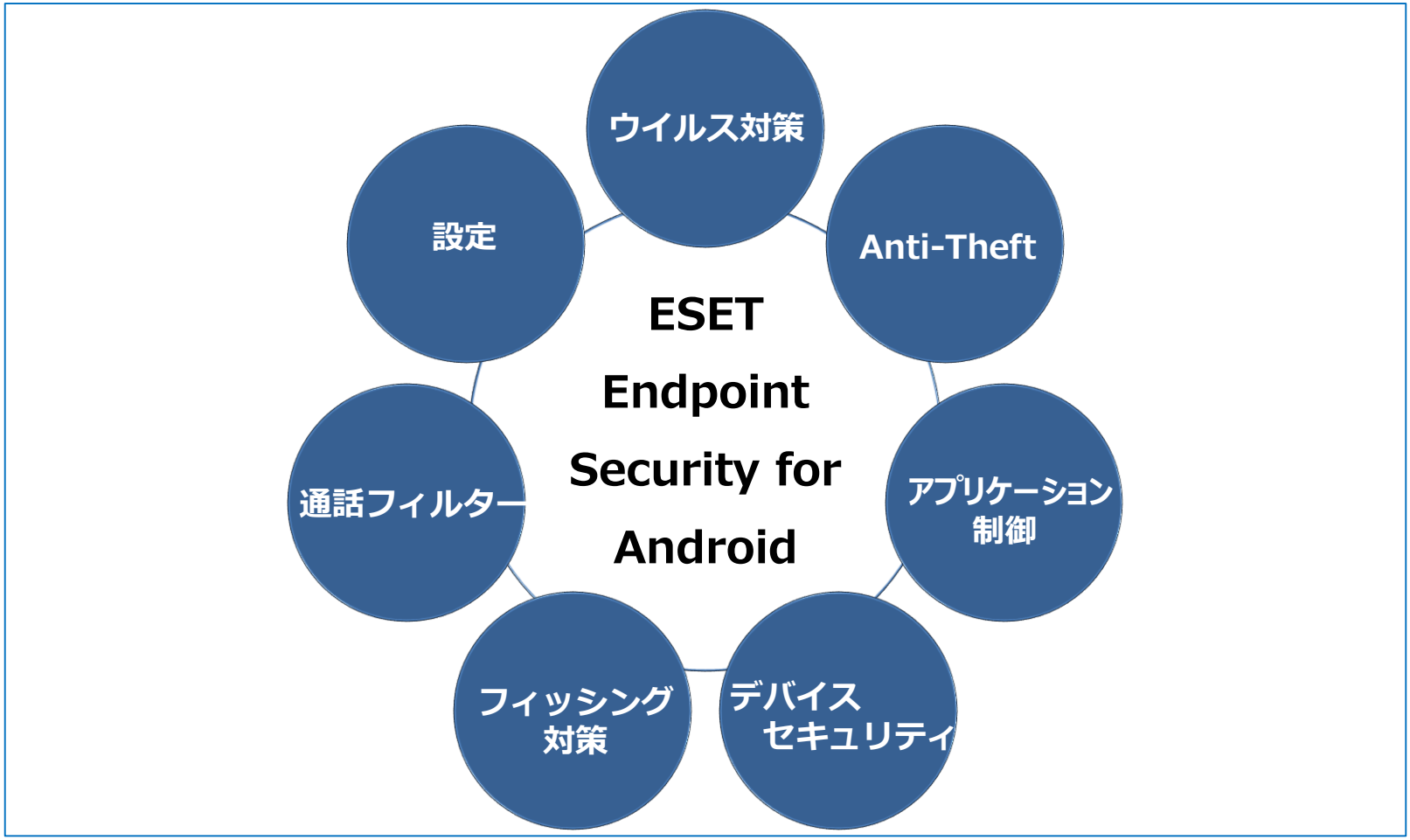
・**ESMCまたはERAから、ほぼリアルタイムでタスクとポリシーを送信できます。**
Firebase Cloud Messagingを利用したプッシュ通知を利用することで、ほぼリアルタイムでのタスクとポリシーの送信を実現しました。

・**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。**
ESMCまたはERAで管理することで、SIMが無いデバイスに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

- 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。

リアルタイム検査

- 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。

自動検査

- 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、 下記[コマンドの送信]機能を使用することで、スマートフォンやタブレットデバイスが盗まれたり紛失したときに、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ESMCまたはERAで管理すればタスク機能を利用して[コマンドの送信]と同等の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。
警報	デバイスがミュートに設定されている場合でも大音量の警報が再生されます。
ロック	対象デバイスのロックが可能です。管理者パスワードもしくは[コマンドの送信]のロック解除から解除可能です。
ロック解除	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。
ワイプ	既定のフォルダに保存されている全ての連絡先、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、動画が完全にデバイスから消去されます。 ESET Endpoint Securityはインストールされたままです。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	デバイスを初期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。

※Android 5.0 / 5.1に対してワイプ機能を実行した際、完了したことが通知されません。

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下記項目を設定する必要があります。特に、ESMCまたはERAを使用せずにデバイス同士で管理する場合は、[管理者連絡先]と[SMSテキストコマンドの着信]を適切な設定に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。 •ここに登録した電話番号からSMSテキストコマンドを送信できます。
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。
SMSテキストコマンドの着信	•管理者連絡先に登録した管理者の番号からSMSテキストコマンドの着信について有効/無効を選択できます。

※SMSを使ってアンチセフトを使用する場合にはSMS発信元のデバイスが、発信先のデバイスのアンチセフト機能において、管理者として登録されている必要があります。

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

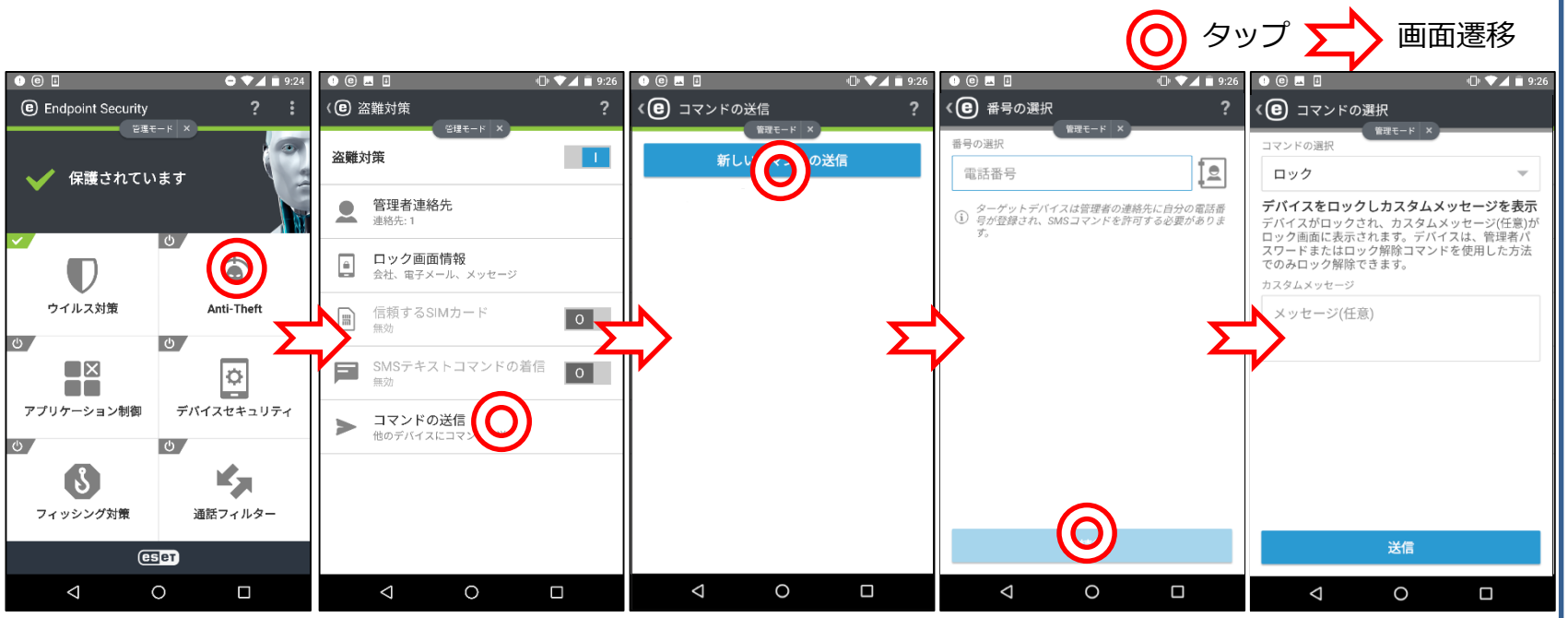
2 EESAの主な機能

2 Anti-Theft

デバイスB(紛失したデバイス)に対して、デバイスA(デバイスBの管理者連絡先)からロック(コマンドの送信)を行う場合。

※SIMカードのないデバイスもESMCまたはERAで管理してタスク機能を使用すれば利用可能です。

デバイスA(デバイスBで管理者番号として登録済)の作業



※デバイスB(紛失したデバイス)へ、SMSを利用してコマンドを送信します。

2 EESAの主な機能

2 Anti-Theft

紛失したデバイスBがデバイスAによってロック(コマンドの送信)された場合。
※SIMカードのないデバイスでもESMCまたはERAで管理すれば利用できます。

デバイスA
(デバイスBで管理者番号として登録済)

※デバイスAのアンチセフトの機能[コマンドを送信]を利用してデバイスB(紛失したデバイス)をロックします。

デバイスB
(紛失したデバイス)

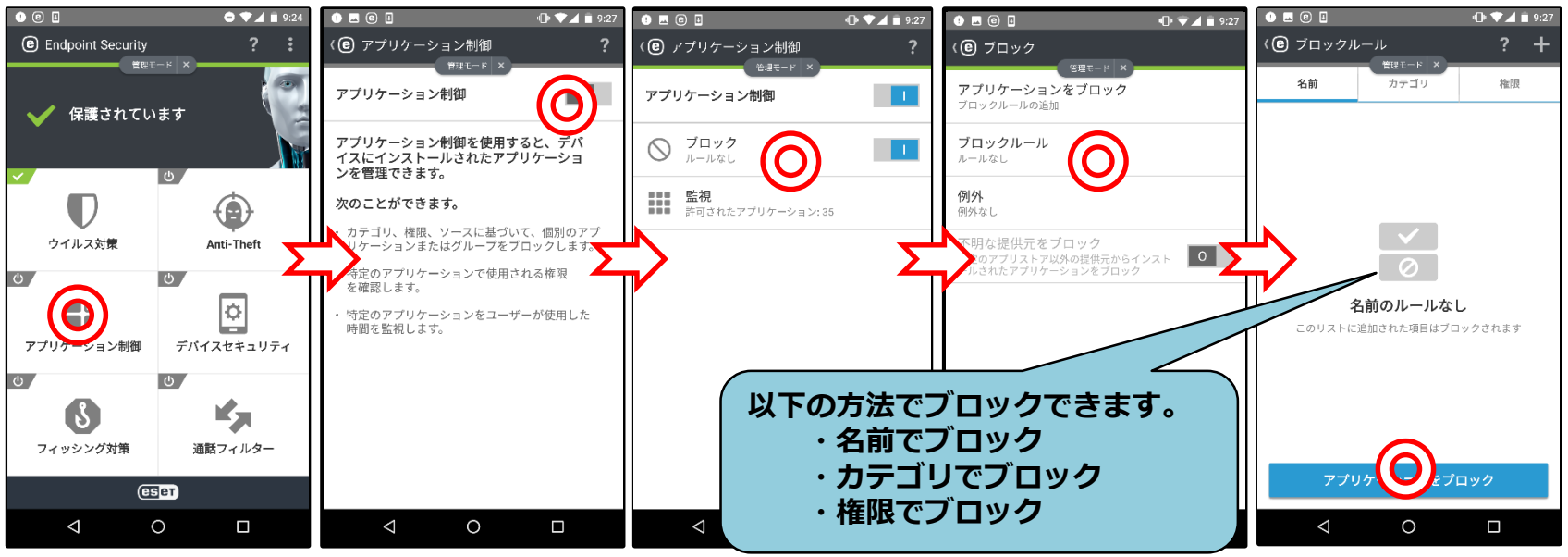
※ロックを実行した場合は、上記画面になり、画面上の操作以外は受け付けなくなります。

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



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[メモ帳]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。

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。
デバックモード	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

デバイスポリシー設定の流れは、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

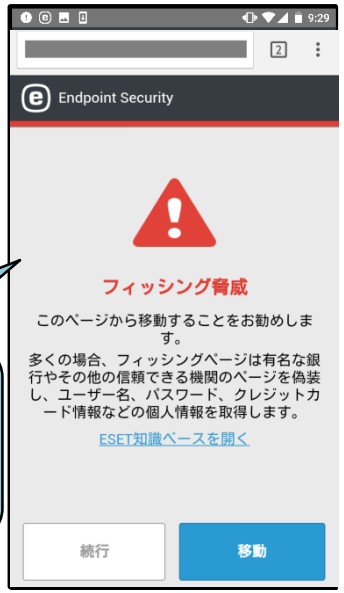
フィッシング対策は、ソーシャルエンジニアリングを用いて個人情報を盗む目的で作成されているサイト、悪意のあるサイトを検出します。フィッシング対策保護を完全に活用するには、サポート対象外のWebブラウザをブロックすることをお勧めします。

※Android7.0以降では、Google ChromeおよびOpera以外のブラウザでは正常に動作しません。

フィッシング対策を有効にする流れ

◎ タップ ⇨ 画面遷移

ブロック時の画面



2 EESAの主な機能

6　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す。また、ユーザールールと管理者ルールを分けて作成できます。

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

6　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

6　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

7　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

言語	国	アップデート
通知表示	使用状況データの送信	設定のインポート/エクスポート
管理者パスワード	Security Management Center	アンインストール

2 EESAの主な機能

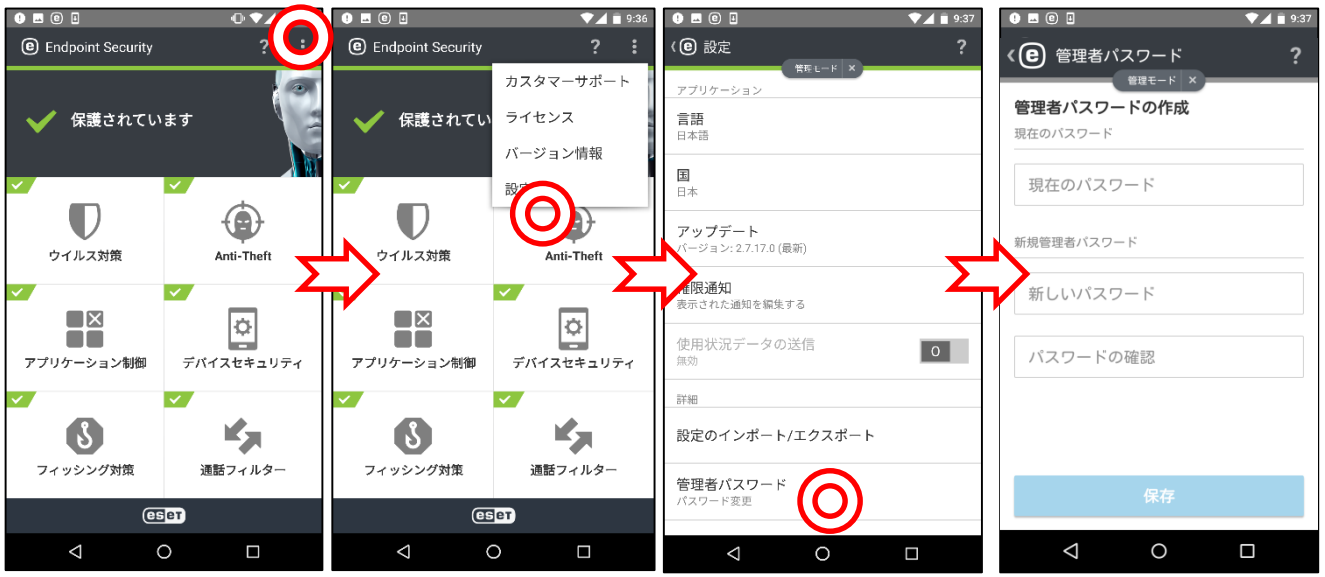
7　設定

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。

※Android 7.0以降で、アプリのメニューから管理者パスワード入力無しでアンインストールできる現象を確認しております。

◎ 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

7　設定

Security Management Centerの設定は、ESMCまたはERAと連携を行うための設定です。ESMCまたはERAからデバイスの操作を実行する為には接続するESMCまたはERAの情報をデバイスに入力しておく必要があります。

※ EESAを管理可能なプログラムは、ESMCまたはERA V6.5です。

◎ タップ ⇨ 画面遷移

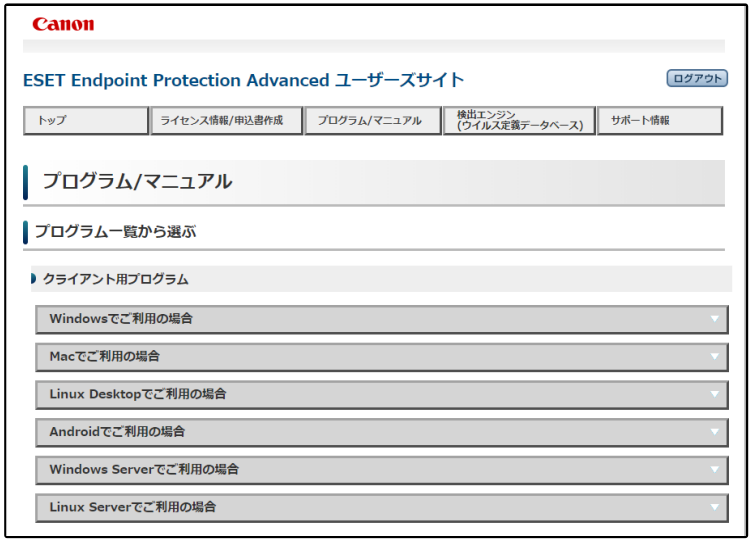
3 EESAの導入について

導入方法

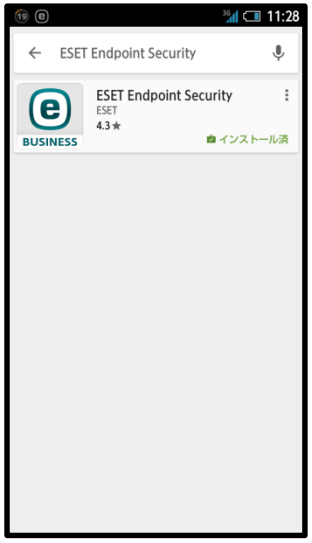
EESAをダウンロードするには下記の方法があります。

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 StoreよりEESAをダウンロードする方法。

ユーザーズサイト利用時



Google Play Store利用時



4 EESAの管理について

ESMC及びERAとの接続構成

EESAをESMCまたはERAで管理する為には、以下の条件確認や作業が必要です。

1. ESMCまたは、ERA V6.5.37以降でEESAの管理が可能です。
   管理する為には、ESMCまたはERAにMobile Device Connector(以後、MDC)の導入が必要です。
   ※MDCとEESAが通信可能な状態(Wi-Fi, VPN経由 等)が必要です。
   ※EESAを導入したデバイスがインターネット接続可能な状態が必要です。

2. 管理するためには、モバイルデバイスを ESMCまたはERA上の[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ESMCまたはERAの管理画面上のQRコードを読み取ります。

3. 受信したメールの登録用リンク、またはQRコードを読み取ると、ESMCまたはERAへ接続が開始され、管理が行われます。

※ESMCやERA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

ESMC及びERAとの連携機能

ESMC及びERA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/ESMC及びERA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

ESMC及びERAから実行できるタスク

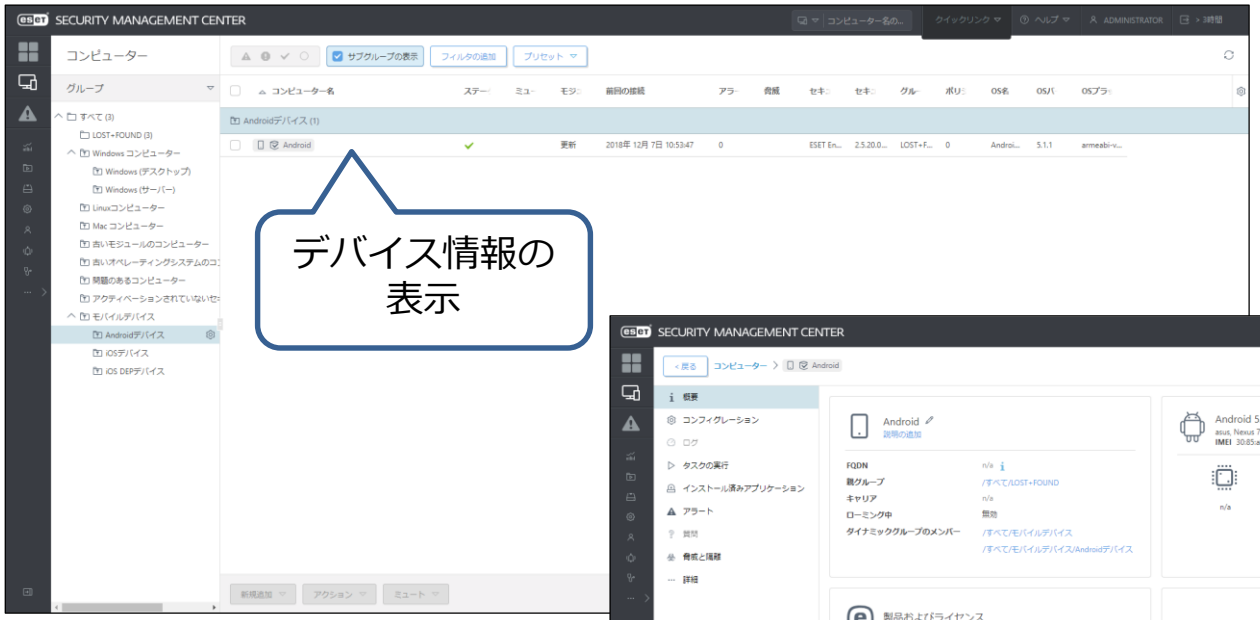
ESMC及びERAからEESAに対して、以下のタスクを実行できます。

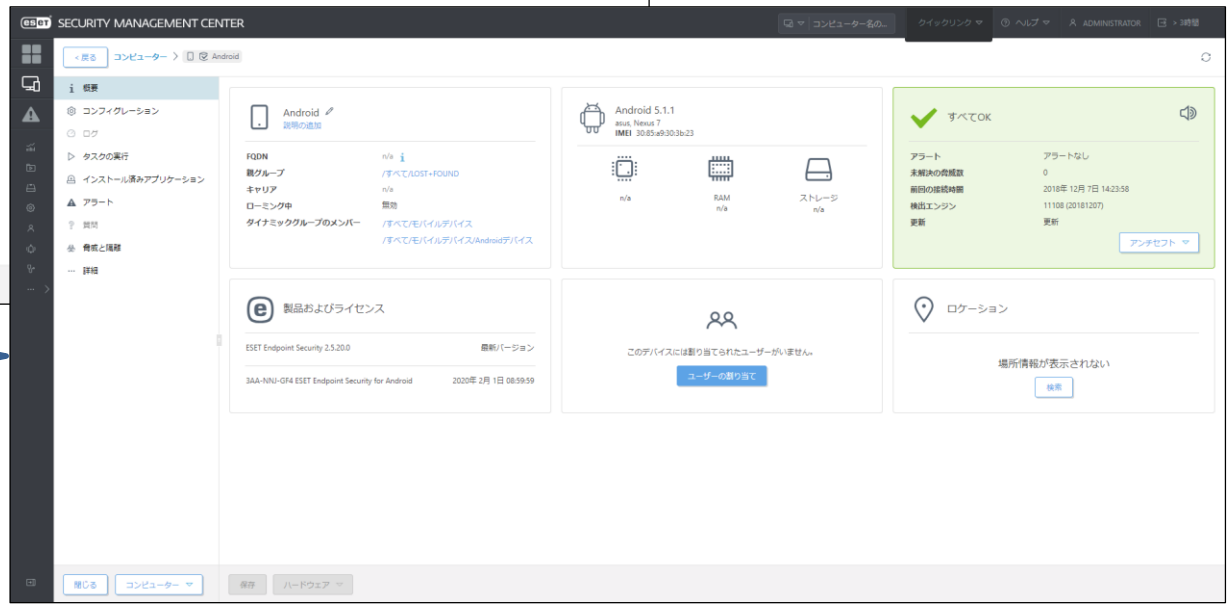
ERAから実行できるタスク

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ESMC及びERAで表示
アンチセフトアクション	以下6種類のアクションを選択 ・検索　・警報　・ロック　・ロック解除　・ワイプ ・拡張初期設定リセット
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

ESMCでの管理イメージ





※画面はESET Security Management Center V7.0のものです。

4 EESAの管理について

ERAでの管理イメージ

※画面はESET Remote Administrator V6.5のものです。