ESET Endpoint Security for Android

ユーザー ガイド

この文書のオンラインバージョンを表示するにはこちらをクリックしてください。

Digital Security
Progress. Protected.

Copyright ©2023 by ESET, spol. s r.o.

ESET Endpoint Security for AndroidはESET, spol. s r.o.によって開発されています

詳細についてはhttps://www.eset.comをご覧ください。

All rights reserved.本ドキュメントのいかなる部分も、作成者の書面による許可がない場合、電子的、機械的、複写、記録、スキャンなど、方法または手段の如何をと遭わず、複製、検索システムへの保存、または転送が禁じられています。

ESET, spol. s r.o.は、事前の通知なしに、説明されたアプリケーションソフトウェアを変更する権利を有します。

テクニカルサポート: https://support.eset.com

改訂: 2023年/12月/4日

1 はじめに 1
1.1 バージョン3の新機能 1
1.2 最低システム要件 1
1.3 変更ログ 2
2 ESET PROTECTおよびESET PROTECT Cloudに接続するユーザー 2
3 リモートインストール 2
4 デバイスでのローカルインストール 3
4.1 ESET Webサイトからダウンロード 4
4.2 起動ウイザード 4
5 アンインストール 6
6 製品のアクティベーション 6
7 リモート管理されたエンドポイントのドキュメント 7
7.1 ESET PROTECTの概要 7
7.2 ESET PROTECT Cloudの概要 9
7.3 ポリシー 9
7.3 ポリシーの適用 10
7.3 フラグ 10
7.3 上書きモードを使用する方法 11
8 ウイルス対策 13
8.1 自動検査 14
8.2 検査ログ 15
8.3 ルールの無視 15
8.4 詳細設定 16
9 Anti-Theft 17
9.1 管理者の連絡先 18
9.1 管理者連絡先の追加方法 18
9.2 ロック画面情報 18
9.3 信頼できるSIMカード 18
9.4 リモートコマンド 19
10 アプリケーションコントロール 19
10.1 ブロックルール 20
10.1 アプリケーション名でブロック 20
10.1 名前でアプリケーションをブロックする方法 21
10.1 アプリケーションカテゴリでブロック 21
10.1 カテゴリに基づいてアプリケーションをブロックする方法 21
10.1 アプリケーション権限でブロック 22
10.1 権限でアプリケーションをブロックする方法 22
10.1 不明なソースをブロック 22
10.2 例外 22
10.2 例外の追加方法 23
10.3 必要なアプリケーション 23
10.3 許可されたアプリケーション 24
10.3 権限 24
10.3 使用状況 25
11 デバイスセキュリティ 26
11.1 画面ロックポリシー 26
11.2 デバイス設定ポリシー 27
12 フィッシング対策 29
13 Webコントロール 31

14 通話フィルター 32
14.1 ルール 34
14.1 新しいルールを追加する方法 34
14.2 履歴 34
15 設定 35
15.1 設定のインポート/エクスポート 35
15.1 設定のエクスポート 36
15.1 設定のインポート 37
15.1 履歴 37
15.2 管理者パスワード 37
15.3 リモート管理 38
15.4 デバイス ID 39
15.5 権限管理 39
16 カスタマーサポート 40
17 カスタマーエクスペリエンス改善プログラム 41
18 エンドユーザーライセンス契約 42
19 プライバシーポリシー 49

はじめに

新しい世代のESET Endpoint Security for Android (EESA)はESET PROTECTおよびESET PROTECT Cloudと動作するように設計されています。これは、新しい管理コンソールであり、すべてのESETセキュリティソリューションをリモート管理できます。

ESET Endpoint Security for Androidバージョン3は次のコンポーネントと互換性があります。

- ESET Security Management Center 7,
- ESET PROTECTおよび ESET PROTECT Cloud

ESET Endpoint Security for Androidは、最新のマルウェア脅威から企業モバイルデバイスを保護し、デバイスが紛失したり盗まれたりした場合でもデータを保護します。また、システム管理者は、デバイスが企業セキュリティポリシーに準拠した状態に保つことができます。

ESET Endpoint Security for Android は、ESET PROTECT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ますIT技術者、システム管理者、または実際のユーザーは、自分のESET Endpoint Security for Android設定を簡単に他の同僚と共有できます。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だった製品のアクティベーションと各製品モジュールの手動設定が完全に必要なくなります。

バージョン3の新機能

追加:

- MS Intune展開のサポート
- オンプレミスからクラウドへ自動移行のサポート

削除済み:

- MS Intuneで登録した場合の冗長デバイスマネジメントに関連する機能
- 削除済み:作業プロファイル下でインストールした場合、フィッシング対策/Webガードが削除されます

最低システム要件

ESET Endpoint Security for Androidをインストールするには Androidデバイスが次の最低システム要件を満たしている必要があります。

- オペレーティングシステム:Android 5 (Lollipop) 以降
- タッチスクリーン解像度:480x800 px
- CPU:ARM とARMv7 命令セットx86 Intel Atom
- 空き記憶領域:20 MB

- インターネット接続

AndroidGoはサポートされていません。

デュアルSIMおよびルート化デバイスはサポートされていません。一部の機能(Anti-Theftや通話フィルターなど)は、通話とメッセージングをサポートしないタブレットでは使用できません。

変更ログ

ESET PROTECTおよびESET PROTECT Cloudに接続するユーザー

ESET PROTECTおよびESET PROTECT Cloudは、1つの中央の場所からネットワーク環境にあるESET製品を管理できるアプリケーションです。ESET PROTECTおよびESET PROTECT Cloudタスク管理システムでは、ESETセキュリティソリューションをリモートコンピューターにインストールし、新たな問題や脅威に迅速に対応することができます。ESET PROTECTは、各クライアントのESETセキュリティソリューションに依存しており、。それ自体では悪意のあるコードに対する保護は提供しません。

ESETセキュリティソリューションは、複数のプラットフォームタイプを含むネットワークをサポートします。ネットワークは現在のMicrosoft、Linuxベース、macOSおよびモバイルデバイス(携帯電話やタブレット)上で実行されるオペレーティングシステムの組み合わせを含めることができます。

ESET PROTECTおよびESET PROTECT Cloudは次世代のリモート管理システムであり、前のバージョンのESET Remote Administratorとは大きく異なります。前のバージョンのESETセキュリティ製品との互換性は次の場所で確認できます。

- ESET PROTECTサポートされている製品
- ESET PROTECT Cloudサポートされている製品

ESET PROTECTとESET PROTECT Cloudの違いについては、ドキュメントをご覧ください。

詳細については、次のドキュメントを参照してください。
- ESET PROTECTオンラインドキュメント
- ESET PROTECT Cloudオンラインドキュメント

リモートインストール

ESET PROTECTからのESET Endpoint Security for Androidのリモートインストールには次のことが必要です。

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

ESET Endpoint Security for Androidインストールシナリオ

- 管理者は、登録リンク、インストールAPKファイル、およびインストール手順をエンドユーザー

に電子メールで送信します。ユーザが登録リンクをタップすると、既定のAndroidインターネットブラウザーにリダイレクトされます。デバイスESET Endpoint Security for Androidが登録されESET PROTECTに接続されます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は、ユーザーがGoogle Playストアにリダイレクトされ、アプリケーションをダウンロードできます。アプリケーションがダウンロードされた後の、標準インストールは次のとおりです。

• 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、およびインストール手順をエンドユーザーに電子メールで送信します。インストール後、ユーザーはアプリケーション設定ファイルを開く必要があります。すべての設定がインポートされ、アプリケーションがアクティベーションされます(ライセンス情報が含まれている場合)。

制限された入力の可能性があるデバイスの登録

ESET Endpoint Security for Androidでは、カメラ、ブラウザー、電子メール(テレビ、スマートディスプレイ、広告表示など)がなくても、デバイスをESET PROTECT Cloudに登録できます。このようなデバイスを登録するにはGoogle PlayまたはAPKファイルを使用してデバイスにESET Endpoint Security for Androidをインストールします。**リモート管理**手順のスタートアップウィザード中に**はい。リモートで管理します**を選択して、**入力が制限されたデバイス**をタップします。

内向き ESET PROTECT Cloud:

1.**コンピューター** > **デバイスの追加** > **Android**または**iOS/iPadOS** > **登録のカスタマイズ**をクリックします。

2.**制限された入力オプションのAndroidデバイス**を選択し、任意の配布方法を選択しますESET PROTECT Cloudコンソールで配布方法の詳細を確認できます。

3.エンドユーザーライセンス契約に同意し、プライバシーポリシーを承諾します。

4.これが新しいデバイスの場合、**追加**をクリックします。すべての必要な情報を入力し、**保存**をクリックします。既存のデバイスを追加している場合は、該当するデバイスを選択します。

5.デバイスの登録リンクを受信します。リンクをクリックし、スタートアップウィザードの**リモート管理**セクションに表示される6桁のセキュリティコードを入力します。

6.**同意**をクリックします。

デバイスはESET PROTECT Cloudに登録されています。

デバイスでのローカルインストール

ESET PROTECTを使用しない場合、管理者はESET Endpoint Security for Android を使用してローカルでEndpointのセットアップと管理ができます。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されているため、常にアプリケーションを完全に管理制御できます。

小規模な企業の管理者がESETPROTECTを使用せずに、企業デバイスを保護し、基本セキュリティポリシーを適用する場合は、デバイスをローカルで管理するためのオプションが2つあります。

1.各企業デバイスへの物理アクセスと設定の手動構成。

2.管理者はAndroidデバイス(ESET Endpoint Security for Android がインストールされている)で任意の設定を準備し、ファイルに設定をエクスポートできます。詳細については、このガイドの「設定のインポート/エクスポート」セクションを参照してください)。管理者はエクスポートされたファイルをエンドユーザーと共有できます(電子メールなど)。ユーザーは、次のものをを実行する任意のデバイスにファイルをインポートできますESET Endpoint Security for Androidユーザーが受信した設定ファイルを開いて許可すると、すべての設定が自動的にインポートされ、アプリケーションがアクティベートされます(ライセンス情報が含まれている場合)。すべての設定は管理者パスワードによって保護されます。

ESET Webサイトからダウンロード

モバイルデバイスのQRスキャンアプリを使用して、以下のQRコードをスキャンし、ESET Endpoint Security for Androidをダウンロードします。

あるいはESET WebサイトからESET Endpoint Security for Android APKインストールファイルをダウンロードできます:

1.インストールファイルをダウンロードします。ESETのWebサイトからダウンロードします。.

2.Android通知領域からファイルを開くか、ファイル参照マネージャアプリケーションを使用して検索します。通常、ファイルはダウンロードフォルダに保存されます。

3.[不明な提供元]からのアプリケーションがデバイスで許可されていることを確認します。このためには、ランチャーアイコン(Androidホーム画面)をタップするか、**ホーム > メニューに移動します。**ユーザーの同意を承認するには、 **設定 > セキュリティ**をタップします。**不明な提供元**オプションを許可する必要があります。

4.ファイルを開いた後、[**インストール]をタップします。**.

ESET WebサイトからダウンロードされたESET Endpoint Security for Androidは、ESET WebサイトのファイルダウンロードによってのみアップグレードできますGoogle Playではアップグレードできません。

起動ウイザード

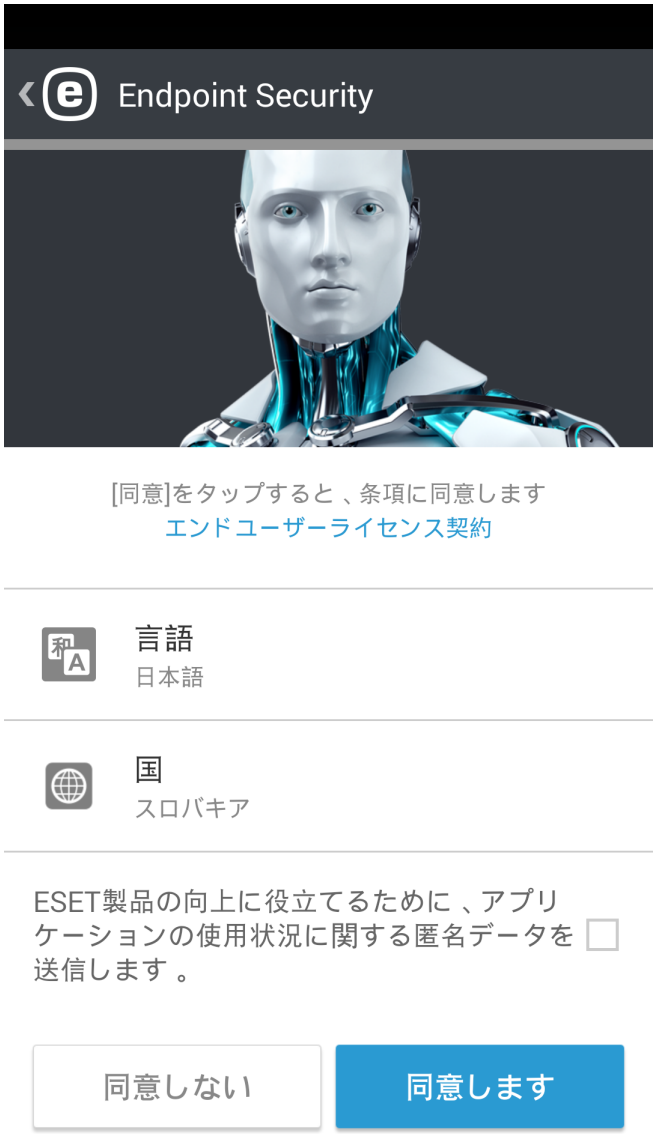
アプリケーションがインストールされたら、**管理者設定** をタップし、スタートアップウィザードのプロンプトに従います。この製品は管理者専用です。

1.ESET Endpoint Security for Androidで使用する**言語**を選択します。

2.右側のナビゲーションペインで**国**（現在の居住国）を選択します。

3.ESET製品の向上に役立てるために、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する場合は、チェックボックスを選択します。

4.**同意**をタップします。**同意**タップすると、エンドユーザー使用許諾契約に同意します。



5.**同意**をタップして、ユーザー同意を承諾します。

6.**はい。リモートで管理します**を選択して、ESET Endpoint Security for AndroidをESET PROTECTに接続するか、**いいえ。保護のみを行います**をタップして手動設定を実行します。

7.手動セットアップでは、電話およびストレージ権限を有効にする必要があります。**続行**をタップしてから、**許可**をタップすると、各権限が有効になります。

8.**続行**をタップすると、他のアプリケーション権限よりも優先させることができます。

9.手動セットアップには製品のアクティベーションが必要です。ESET Endpoint Security for Androidライセンスキーまたは ESET Business Account (EBA)を使用してアクティベーションできます。

10.管理者パスワードを作成します。

11.**アンインストール防止** は権限のないユーザーによるインストールを制限しますESET Endpoint Security for Android.**有効化**をタップし、**デバイス管理者アプリケーション**プロンプトで**アクティベーション**をタップします。

12.適切なアプリケーション機能を有効にするには、使用アクセスを有効にします。**続行**をタップし、**ESET Endpoint Security for Android**をタップして、**使用アクセス**を有効にします。スタートアップウィザードに戻るには、戻る矢印を2回タップします。

13.ESET LiveGrid®フィードバックシステム**への参加を許可**または拒否 するオプションを選択します。ESET LiveGrid®の詳細については、このセクションを参照してください

14.ESET Endpoint Security for Androidで、望ましくない可能性があるアプリケーションの**検出を有効にする**か、**検出を有効にしない**オプションを選択します。こちらのアプリケーションの詳細については、このセクションを参照してください。**次へ**をタップします。

15.**完了**をタップすると、スタートアップウィザードを終了し、最初のデバイス検査を開始します。

アンインストール

次の手順に従い、ESET Endpoint Security for Androidを手動でアンインストールできます。

重要
このガイドは、Androidの標準設定に基づいています。アンインストールプロセスは、デバイスの製造元によって異なる場合があります。

1.Androidデバイスで、**設定 > 生体認証とセキュリティ > その他のセキュリティ設定 > デバイス管理者アプリ**を開きます。**ESET Endpoint Security for Android**の選択を解除して、**[無効にする]**をクリックします。**[ロック解除]**をタップし、管理者パスワードを入力しますESET Endpoint Security for Androidをデバイス管理者に設定していない場合は、この手順を省略します。

2.**設定**に戻り、**アプリ > ESET Endpoint Security for Android > アンインストール > OK**をタップします。

製品のアクティベーション

ESET Endpoint Security for Androidをアクティベートする方法は複数あります。特定のアクティベーション方法が使用できるかどうかは、国および製品の配布方法(ESET Webページなど)によって異なる場合があります。

直接AndroidデバイスでESET Endpoint Security for Android をアクティベーションするには、**メニュー**アイコン (ESET Endpoint Security for Android メイン画面)をタップし、**ライセンスをタップします。**.

次のをアクティベーションするには、次の方法を使用できますESET Endpoint Security for Android:

- **製品認証キー**–形式XXXX-XXXX-XXXX-XXXX-XXXX の一意の文字列であり、ライセンス所有者の特定とライセンスのアクティベーションで使用されます。

- **ESET Business Account** — ESET Business Accountポータルと資格情報(電子メールアドレスとパスワード)。この方法では、1つの場所から複数のライセンスを管理できます。

ESET PROTECTは、管理者が使用可能にしたライセンスを使用してバックグラウンドでクライアントデバイスをアクティベーションできます。

リモート管理されたエンドポイントのドキュメント

ESETビジネス製品およびESET Endpoint Security for Androidは、1つの集中管理された場所から、ネットワーク接続環境におけるクライアントワークステーション、サーバー、およびモバイルデバイスで、リモート管理できます。11台以上のクライアントワークステーションを管理するシステム管理者は、ESETリモート管理ツールの使用を検討してください。ESETリモート管理ツールを使用すると、1つの集中管理された場所からESETソリューションの展開、タスクの管理、セキュリティポリシーの施行、システムステータスの監視、およびリモートコンピューターでの問題や脅威に対する迅速な対応が可能です。

ESETリモート管理ツール

ESET Endpoint Security for Androidは、ESET PROTECTまたはESET PROTECT Cloudでリモート管理できます。

- ESET PROTECTの概要
- ESET PROTECT Cloudの概要

移行ツール
ESET Endpoint Security for Androidバージョン3.5以降は、ESET PROTECTからESET PROTECT Cloudに移行するための移行ツールをサポートしています。

ベストプラクティス

- ESET PROTECTを使用してデバイスを登録する
- 接続されたクライアントコンピューターで管理者パスワードを設定し、不正な修正を防止する
- 推奨されたポリシーを適用して、使用可能なセキュリティ機能を施行する

ガイド

- 上書きモードを使用する方法

Microsoft Intuneで登録されたAndroidデバイス

Android 9以降のデバイスがMicrosoft Intuneで登録されるとESET Endpoint Security for Androidバージョン3.5以降では、対応するポリシーが適用されたときに、次の設定が無視されます。
- デバイスセキュリティ
- アプリケーション制御
- Anti-Theft

ESET PROTECTの概要

ESET PROTECTで、ネットワーク接続環境におけるワークステーション、サーバー、モバイルデバイス上のESET製品を1つの集中管理された場所から管理できます。

ESET PROTECT Webコンソールを使用するとESETソリューションの展開、タスクの管理、セキュリティポリシーの施行、システムステータスの監視、リモートコンピューターでの問題や検出への迅速な対応ができます。ESET PROTECTアーキテクチャおよびインフラストラクチャ要素の概要ESET PROTECT Webコンソールの基本サポートされているデスクトッププロビジョニング環境を参照してください。

ESET PROTECTは次のコンポーネントで構成されています。

- ESET PROTECT サーバー - ESET PROTECTサーバーはWindowsとLinuxにインストールでき、仮想アプライアンスとして付属しています。エージェントとの通信を処理し、アプリケーションデータを収集し、データベースに保存します。

- ESET PROTECT Webコンソール - ESET PROTECT Webコンソールは、環境内のクライアントコンピューターを管理できるメインのインターフェースです。ネットワーク上のクライアントについてステータスの概要を表示し、管理対象外のコンピューターにリモートでESETソリューションを展開できますESET PROTECTサーバーをインストールすればWebブラウザーを使用してWebコンソールにアクセスできますWebサーバーをインターネット上で公開すると、インターネットに接続されているすべての場所とデバイスからESET PROTECTを使用できます。

- ESET Managementエージェント - ESET Managementエージェントは、ESET PROTECTサーバーとクライアントコンピューターの間の通信を容易にします。コンピューターとESET PROTECTサーバーの間の通信を確立するには、エージェントをクライアントコンピューターにインストールする必要があります。そうすれば、クライアントコンピューター上のESET Managementエージェントを使用することになって複数のセキュリティシナリオを保存できるため、新しい検出への対応時間が大幅に短くなりますESET PROTECTWebコンソールを使用するとActive DirectoryまたはESET RD Sensorで特定された管理対象外のコンピューターに、ESET Managementエージェントを展開できます。また、必要に応じて、クライアントコンピューターに、ESET Managementエージェントを手動でインストールできます。

- Rogue Detection Sensor - ESET PROTECT Rogue Detection (RD) Sensorは、ネットワークに存在する管理されていないコンピュータを検出し、その情報をESET PROTECTサーバーに送信します。これにより、新しいクライアントコンピュータを保護されたネットワークに容易に追加できますRD Sensorは検出されたコンピュータを記憶し、同じ情報を2回送信しません。

- Apache HTTP Proxy - ESET PROTECTと組み合わせて使用できるサービスで、

  oクライアントコンピュータにアップデートを配布し、ESET Managementエージェントにインストールパッケージを配布します。

  oESET Managementエージェントから ESET PROTECTサーバーに通信を転送します。

- モバイルデバイスコネクター - ESET PROTECTでモバイルデバイス管理を可能にするコンポーネントであり、モバイルデバイス(AndroidおよびiOS)を管理し、ESET Endpoint Security for Androidを管理できます。

- ESET PROTECT仮想アプライアンス - ESET PROTECT VAは、仮想環境でESET PROTECTを実行したいユーザを対象にしています。。

- ESET PROTECT Virtual Agent Host - ESET PROTECTのコンポーネントであり、エージェントレス仮想マシンの管理ができるように、エージェントエンティティを仮想化します。このソリューションにより、自動化、動的グループの利用、物理コンピューターのESET Managementエージェントと同じレベルのタスク管理が可能になります。仮想エージェントは仮想マシンから情報を収集し、ESET PROTECTサーバーに送信します。

- ミラーツール – ミラーツールは、オフラインモジュールアップデートで必要です。クライアントコンピュータがインターネットに接続しない場合、ミラーツールを使用してESETアップデートサーバー

からアップデートファイルをダウンロードし、ローカルに保存できます。

- ESET Remote Deployment Tool – このツールでは<%PRODUCT%> Webコンソールで作成されたオールインワンパッケージを展開できます。ネットワーク上のコンピュータでESET Managementエージェントと ESET製品を配布するための便利な方法です。

- ESET Business Account - ESETビジネス製品向けの新しいライセンスポータルでは、ライセンスを管理できます。製品をアクティベーションする手順については、このドキュメントの<%EBA%>セクションを参照してください<%EBA%>の使用の詳細については<%EBA%>ユーザーガイドを参照してください。

- ESET Enterprise Inspector – 包括的なエンドポイント検出および応答システムであり、インシデント検出、インシデント管理と応答、データ収集、危険検出の指標、特異性の検出、動作検出、ポリシー違反などの機能があります。

ESET PROTECT Webコンソールを使用してESETソリューションの展開、タスクの管理、セキュリティポリシーの施行、システムステータスの監視、リモートコンピューターでの問題や脅威に対する迅速な対応ができます。

詳細については、ESET PROTECTオンラインユーザーガイドをご覧ください。

ESET PROTECT Cloudの概要

ESET PROTECT CloudではESET PROTECTやESET Security Management Centerなどの物理または仮想サーバーを必要とせずに、ネットワーク環境におけるワークステーションおよびサーバー上のESET製品を、集中管理された1つの場所から管理できますESET PROTECT Cloud Webコンソールを使用すればESETソリューションの展開、タスクの管理、セキュリティポリシーの施行、システムステータスの監視、リモートコンピューターでの問題や脅威への迅速な対応が可能です。

- ESET PROTECT Cloudオンラインユーザーガイドをお読みください

ポリシー

管理者は、ESET PROTECT Webコンソールまたは ESET Security Management Center Webコンソールから、ポリシーを使用して、クライアントデバイスで実行されるESET製品に特定の設定をプッシュすることができます。ポリシーは、直接個別のデバイスやデバイスのグループに適用できます。また、複数のポリシーをデバイスまたはグループに割り当てることができます。

ユーザーが新しいポリシーを作成するには、次の権限が必要です。**読み取り**権限は、ポリシーのリストを読み取ります。**使用**権限は、ポリシーをターゲットコンピュータに割り当てます。**書き込み**権限は、ポリシーを作成、修正、または編集します。

ポリシーは、静的グループの配置順に適用されます。これは、ポリシーが最初に子動的グループに適用される、動的グループには当てはまりません。これにより、より大きい影響度でポリシーをグループツリーの最上位に適用し、より固有のポリシーをサブグループに適用できます。フラグを使用すると、ツリーの上位にあるグループにアクセスできるESET Endpoint Security for Androidユーザーは、下位のグループのポリシーを上書きできます。このアルゴリズムについては、ESET PROTECTオンラインヘルプを参照してください。

デバイスでポリシーを設定すると、ポリシーで制御された設定をローカルで変更するオプションが無効になります。これらの設定は管理者モードでも変更に対してロックされます。上書きモードポリシーを作成すると、一時的な変更を許可できます。

特定のポリシーを設定するには、影響を受けるデバイスでローカルに追加権限をESET Endpoint Security for Androidに付与しなければならない場合があります。

グループツリーの上位にあるグループには、より汎用的なポリシー(アップデートサーバーポリシーなど)を割り当てることをお勧めします。より特定のポリシー(デバイスコントロール設定など)はグループツリーの下位に割り当てられます。通常、マージ時に下位のポリシーが上位の設定を上書きします(ポリシーフラグで定義されている場合を除く)。

ESET Endpoint Security for Androidの既定のポリシー

ポリシー名	ポリシーの説明
全般 – 最大限の保護	ESET Endpoint Security for Androidはすべてのオプションを使用して、デバイスの最大限の保護を確保します。
全般 – バランス重視設定	ESET Endpoint Security for Androidはほとんどの設定で推奨される設定を使用します。
全般 – パフォーマンス優先	ESET Endpoint Security for Androidは、脅威から保護しながら、同時に日常のタスクやデバイスパフォーマンスへの影響を最小限に抑えます。

ポリシーの適用

ESET Endpoint Security for AndroidをESET管理コンソールに接続した後は、推奨ポリシーまたはカスタムポリシーを適用することをお勧めします。

ESET Endpoint Security for Androidには複数の定義済みポリシーがあります。

ポリシー名	ポリシーの説明
全般 – 最大限の保護	ESET Endpoint Security for Androidはすべてのオプションを使用して、デバイスの最大限の保護を確保します。
全般 – バランス重視設定	ESET Endpoint Security for Androidはほとんどの設定に推奨されるセキュリティ設定を使用します。
全般 – パフォーマンス優先	ESET Endpoint Security for Androidは、脅威から保護しながら、同時に日常のタスクやデバイスパフォーマンスへの影響を最小限に抑えます。

ポリシーの詳細については、次のトピックを参照してください。

- ESET PROTECTポリシー
- ESET PROTECT Cloudポリシー
- ESET Security Management Centerを使用してESET Endpoint Security for Androidの推奨または定義済みポリシーを適用する

フラグ

通常、クライアントコンピュータに適用されるポリシーは、1つの最終ポリシーにマージされる複数のポリシーの結果です。ポリシーをマージするときには、適用されるポリシーの順序のため、ポリシーフラグを使用して、最終ポリシーの想定される動作を調整できます。フラグは、ポリシーが特定の設定を処理する方法を定義します。

各設定に対して、次のフラグのいずれかを選択できます。

未適用	このフラグの設定はポリシーによって設定されていません。設定はポリシーによって設定されていないため、後から適用される他のポリシーで変更できます。
適用	**適用**フラグが付いた設定は、クライアントコンピューターに適用されます。ただし、ポリシーをマージするときには、後から適用される他のポリシーによって上書きされることがあります。このフラグが付いた設定を含むクライアントコンピューターにポリシーが送信されるときには、これらの設定により、クライアントコンピューターのローカル設定が変更されます。設定は強制ではないため、後から適用される他のポリシーによって変更されることがあります。
強制	**強制**フラグが付いた設定は優先度があり、(**強制**フラグがある場合でも)後から適用されるどのポリシーによっても上書きされることはありません。これにより、後から適用される他のポリシーがマージ中にこの設定を変更できないことが保証されます。このフラグが付いた設定を含むクライアントコンピューターにポリシーが送信されるときには、これらの設定により、クライアントコンピューターのローカル設定が変更されます。

シナリオ:管理者はユーザー*John*がホームグループのポリシーを作成または編集し、強制フラグが付いたポリシーを含む、管理者が作成したすべてのポリシーを表示できるようにします。管理者は、*John*がすべてのポリシーを表示できるようにしますが、管理者が作成した既存のポリシーの編集は許可しません。*John*は、ホームグループSan Diego内でのみ、ポリシーを作成または編集できます。
ソリューション管理者は次の手順に従います。
カスタム静的グループと権限設定の作成
1. 新しい静的グループの*San Diego*を作成します。
2. 静的グループすべてへのアクセスと**ポリシー**の**読み取り**権限がある新しい権限設定の*Policy - All John*を作成します。
3. 静的グループ*San Diego*へのアクセスと**グループとコンピュータ**と**ポリシー**の**書き込み**権限がある新しい権限設定の*Policy John*を作成します。この権限設定により、*John*は、ホームグループ*San Diego*でポリシーを作成または編集できます。
4. 新しいユーザー*John*を作成し、**権限**設定セクションで、*Policy - All John*と*Policy John*を選択します。
ポリシーの作成
5. 新しいポリシー*All- Enable Firewall*を作成し、**設定**セクションを展開し、**ESET Endpoint for Windows**を選択して、**パーソナル ファイアウォール > 基本**に移動して、強制フラグですべての設定を適用します。**割り当て**セクションを展開し、静的グループ*All*を選択します。
6. 新しいポリシー*John Group- Enable Firewall*を作成し、**設定**セクションを展開し、**ESET Endpoint for Windows**を選択して、**パーソナルファイアウォール > 基本**に移動して、適用フラグですべての設定を適用します。**割り当て**セクションを展開し、静的グループ*San Diego*を選択します。
結果
強制フラグがポリシー設定に適用されたため、管理者が作成したポリシーは最初に適用されます。強制フラグが適用された設定は優先度があり、後から適用される別のポリシーで上書きできません。ユーザー*John*が作成したポリシーは、管理者が作成したポリシーの後に適用されます。最終ポリシー順序を確認するには、**詳細 > グループ > San Diego**に移動します。コンピュータを選択して、**詳細の表**示を選択します。**設定**セクションで、**適用されたポリシー**をクリックします。

上書きモードの使用

ESET Endpoint Security for Android (バージョン2. 1以降)がコンピューターにインストールされているユーザーは上書き機能を使用できます。上書きモードでは、これらの設定に適用されたポリシーがある場合でも、設定された期間の間、クライアントデバイスレベルで、インストールされたESET製品の設定を変更できます。設定した期間が過ぎると、設定はポリシーで設定された設定に戻されます。

既定のポリシー設定では、上書きセッションが終了した後に、ESET Endpoint Security for Androidでデバイ

スが検査されます。**上書きセッション後にデバイスを検査**でこれを変更できます。

- 上書きモード中にデバイスでローカルに設定を変更するにはESET Endpoint Security for Android管理者パスワードを入力する必要があります。
- 上書きモードを1度有効にするとESET Webコンソールから停止できます。上書き期間が終了すると、上書きモードは自動的に無効化されます。
- 上書きモードを使用するユーザーにはESET Endpoint Security for Android管理者パスワードが必要です。そうでないと、ユーザーはESET Endpoint Security for Androidの設定にアクセスできません。各ポリシーの一時管理者上書きパスワードを作成できます。

上書きモードを設定するには

1. **ポリシー > 新しいポリシー**をクリックします。
2. **基本**セクションに、このポリシーの**名前**と**説明**を入力します。
3. **設定**セクションで、**ESET Endpoint Security for Android**を選択します。
4. ポリシーオプションの**設定**をクリックします。
5. **上書きモードの設定**を展開し、上書きモードのルールを設定します。
6. **割り当て**セクションで、該当するデバイスを選択します。
7. **サマリー**セクションで設定を確認し、**完了**をクリックします。

*John*のエンドポイント設定に問題があり、一部の重要な機能またはWebアクセスがデバイスでブロックされる場合、管理者は*John*が既存のエンドポイントポリシーを上書きし、デバイスで手動で設定を調整できるようにすることができます。後から、これらの新しい設定はESET PROTECT Cloudで要求されるため、管理者はそこから新しいポリシーを作成できます。
手順は次のとおりです。
1.**ポリシー > 新しいポリシー**をクリックします。
2.**名前**および**説明**フィールドを入力します。**設定**セクションで、**ESET Endpoint Security for Android**を選択します。
3.ポリシーオプションの**設定**をクリックします。
4.**上書きモード**設定を展開し、1時間上書きモードを有効にします。
5.上書き資格情報で**設定**をクリックし、Johnの一時管理者パスワードを作成します。パスワード(12345など)を2回入力し、**OK**をクリックします。
6.*John*のスマートフォンにポリシーを割り当て、**完了**をクリックしてポリシーを保存します。
7.*John*は管理者パスワードを入力してESET Endpoint Security for Androidで**上書きモード**を有効にし、デバイスで手動で設定を変更する必要があります。
8.ESET PROTECT Cloud Webコンソールで、**コンピューター**に移動し、 *John*のスマートフォンをクリックして、**詳細を表示**をクリックします。
9.**設定**セクションで**設定の要求**をクリックして、クライアントタスクをスケジュールして、クライアントから設定を取得します。
10.新しい設定が表示されます。該当する製品を選択し、**設定を開く**をクリックします。
11.設定を確認し、**ポリシーに変換**をクリックします。
12.**名前**および**説明**フィールドを入力します。
13.**設定**セクションで、必要に応じて設定を変更します。
14.**割り当て**セクションで、このポリシーを*John*のスマートフォン(またはその他)に割り当てます。
15.**完了**をクリックします。必ず、必要がなくなった時点で、上書きポリシーを削除してください。

パスワードの無効化

このオプションでは、一時管理者パスワードを作成し、実際の管理者パスワードにアクセスせずに、ユーザーがクライアントデバイスの設定を変更できます。ポリシーの横の**設定**をクリックして、上書きパスワードを挿入します。

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デバイスを保護します。



デバイスを検査

デバイスの検査は、デバイスへの侵入があるかどうかを確認するために使用できます。

既定では、定義済みの特定のファイル形式が検査されます。完全デバイス検査はメモリ、実行中のプロセス、および依存動的リンクライブラリ、内蔵またはリムーバブルストレージにあるファイルを検査します。検査の概要は、[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。

実行中の検査を中断する場合は、アイコンをタップします。

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DEXファイル(Android OS用の実行ファイル)SOファイル(ライブラリ)、3つのネストされたアーカイブの最大検査深さのZIPファ

イル、およびSDカードの内容を検査します。

• **詳細** – 拡張子に関係なくすべてのファイルタイプが内蔵メモリとSDカードの両方で検査されます。

自動検査

オンデマンドデバイス検査の他に、ESET Endpoint Security for Androidには自動検査もあります。充電中に検査およびスケジュールされた検査の使用方法については、このセクションをお読みください

検査ログ

[検査ログ]セクションには、ログファイルの形式で、完了した検査に関する包括的なデータがあります。詳細については、本マニュアルの「ウイルス対策検査ログ」を参照してください。

検出モジュールのアップデート

既定ではESET Endpoint Security for Androidにはアップデートタスクがあり、プログラムが定期的に更新されることが保証されます。アップデートを手動で実行するには、**検出モジュールのアップデート**をタップします。

> 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、必要に応じてアップデートが発行されます。アップデートは有効なライセンスがあれば無償ですが、モバイルサービスプロバイダによってデータ転送料金が課金される場合があります。

ウイルス対策詳細設定の詳細については、本マニュアルの「詳細設定」セクションを参照してください。

自動検査

検査レベル

2つの検査レベルから選択できます。この設定は、充電中に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DEXファイル(Android OS用の実行ファイル)SOファイル(ライブラリ)、3つのネストされたアーカイブの最大検査深さのZIPファイル、およびSDカードの内容を検査します。

• **詳細** – 拡張子に関係なくすべてのファイルタイプが内蔵メモリとSDカードの両方で検査されます。

充電中に検査

これが選択されている場合、デバイスがアイドル状態のときに検査が自動的に開始します(完全に充電され、充電器に接続している場合)。

スケジュール検査

スケジュールされた検査では、定義した時刻に自動的にデバイス検査を実行できます。検査をスケジュールするには、**[スケジュールされた検査]**の横のをタップし、検査を実行する日時を指定します。既定では、月曜日の午前4時に選択されます。

検査ログ

各スケジュール検査または手動でトリガーされたデバイス検査の後に、検査ログが作成されます。

各ログには次の情報が含まれます。

- 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



ルールの無視

ESET PROTECTからリモートでESET Endpoint Security for Androidを管理する場合は、悪意として報告されないファイルを定義することができます。[**ルールを無視**]に追加されたルールは今後の検査で無視されます。ルールを作成するには、次の点を指定する必要があります。

- 正しい apk 拡張子のファイル名
- アプリケーションパッケージ名(例: uk.co.extorian.EICARAntiVirusTest)
- ウイルス対策プログラムで検出された脅威名(例: Android/MobileTX.A) (このフィールドは必須です)

この機能はESET Endpoint Security for Androidアプリでは使用できません。

詳細設定

リアルタイムファイルシステム保護

このオプションを使用すると、リアルタイムスキャナーを有効または無効にできます。このスキャナーは、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® レピュテーションシステム

ESET LiveGrid®は、デバイスのセキュリティを強化するために設計された予防システムです。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。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。この機能を有効にすることをお勧めします。この機能を有効にすることをお勧めします。

ESET LiveGrid® フィードバックシステム

このフィードバックシステムではESETが不審なオブジェクトに関する匿名の統計情報、クラッシュレポート、診断データを収集することを許可します。これによりESETは自動的にクラウドシステムで検出メカニズムを構築できます。

不審な可能性があるアプリケーションを検出

望ましくないアプリケーションは、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。状況によっては、望ましくないアプリケーションの利点がリスクを上回ると考えられる場合があります。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、低いリスクのカテゴリが割り当てられています。

安全でない可能性があるアプリケーションの検出

ネットワークに接続されたデバイスの管理を容易にするように設計された適正なアプリケーションはたくさんあります。ただし、否定的な点では、悪意のある目的で悪用される可能性があります。安全ではない可能性があるアプリケーションを検出するオプションを使用すると、これらのアプリケーションをを監視し、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、キーロガーなどが含まれます。

未解決の脅威をブロック

この設定によって、検査が完了して脅威が見つかった後に実行されるアクションが決まります。このオプションを有効にすると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。

リムーバブルメディア

デバイスにリムーバブルメディアが挿入された後のアクションを選択できます。

- **常に検査** - リムーバブルメディアは常に検査されます。
- **検査しない** - リムーバブルメディアは検査されません。
- **オプションを表示する** - メディアを挿入すると、リムーバブルメディアを検査するオプションが表示されます。

検出モジュールデータベースのアップデート

このオプションでは、脅威データベースアップデートが自動的にダウンロードされる頻度の間隔を設定できます。これらのアップデートは、新しい脅威がデータベースに追加されるときに、必要に応じて発行されます。これを既定値(毎日)のままに設定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、脅威データベースアップデート間の時間を定義します。この時間の後に、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

このオプションを使用すると、**プレリリースサーバー**からデバイスをアップデートできます。リリース前アップデートは社内テスト済みで、まもなく一般に公開される予定です。テストモードを有効にすることで、最新の保護機能や修正プログラムを利用することができます。ただし、リリース前アップデートは常に十分に安全であるとは限りません。現在のモジュールのリストについては、[**バージョン情報**]セクションを参照してください。ESET Endpoint Security for Androidメイン画面でメニューアイコンをタップして、[**バージョン情報**] > **ESET Endpoint Security for Android**をタップします。基本ユーザーは、[**公開サーバー**]を既定で選択されたままにすることをお勧めします。

ESET Endpoint Security for Androidでは、ネットワーク内の他のデバイスをアップデートするために使用できるアップデートファイルのコピーを作成することができます。**ローカルミラー**の使用 - LAN環境でアップデートファイルのコピーを作成すると、ベンダのアップデートサーバーからモバイルデバイスごとに繰り返しアップデートファイルをダウンロードしなくて済むので便利です。Windows版のESET Endpoint製品を使用してミラーサーバーを構成する詳細な方法については、このドキュメントを参照してください。

Anti-Theft

Anti-Theft機能は、モバイルデバイスを不正アクセスから保護します。

デバイスを紛失した場合、または誰かにデバイスを盗まれて、その人物がSIMカードを新しい(信頼されていない)SIMカードに交換した場合、デバイスはESET Endpoint Security for Androidによって自動的にブロックされ、ユーザーが定義した電話番号に警告SMSが送信されます。このメッセージには、現在挿入されているSIMの電話番号、ユーザー固有の番号であるIMSI (International Mobile Subscriber Identity)番号、および電話固有の番号であるIMEI (International Mobile Equipment Identity)番号が含まれています。このメッセージはデバイスのメッセージングスレッドから自動的に削除されるため、不正なユーザーは、メッセージが送信されたことに気付きません。また、紛失したデバイスのGPS座標を要求し、デバイスに保存されたすべてのデータをリモートで消去できます。

信頼できるSIMカード機能は、Android 10以降のデバイスでは使用できません。

Anti-Theft機能を使用すると、管理者は紛失したデバイスを保護して検索できます。ESET PROTECTからア

クションをトリガーできます。

ESET PROTECTからコマンドを実行すると、管理者はESET PROTECTで確認を受信します。

位置情報を受信する(**検索**コマンド)ときにはGPS座標としての位置情報がESET PROTECTを使用している管理者に送信されます。

すべてのAnti-Theftコマンドは ESETPROTECTからも実行できます。新しいモバイルデバイス管理機能によって、管理者は数回クリックするだけでアンチセフトコマンドを実行できますESET PROTECTインフラストラクチャに統合された新しいプッシュコマンド処理コンポーネント(Mobile Device Connector)によって、タスクはただちに送信され、実行されます

管理者の連絡先

これは、管理者パスワードで保護された管理者の電話番号のリストですAnti-Theftコマンドは信頼できる電話番号からしか送信できません。これらの番号は、Anti-Theftのアクションに関連した通知でも使用されます。

管理者連絡先の追加方法

管理者の名前と電話番号は、Anti-Theftスタートアップウィザード中に入力できます。複数の電話番号が連絡先に含まれる場合は、すべての関連する番号が考慮されます。

管理者の連絡先は、**[Anti-Theft]** > [**管理者連絡先**]セクションで追加または変更できます。

ロック画面情報

管理者はカスタム情報(会社名、電子メールアドレス、メッセージ)を定義できます。この情報は、デバイスがロックされているときに、定義済みの管理者の連絡先のいずれかに電話するオプションとともに表示されます。

この情報には次の内容が含まれます。

- 会社名(オプション)
- 電子メールアドレス(任意)
- カスタムメッセージ

信頼するSIMカード

[**信頼できるSIM**]セクションにはESET Endpoint Security for Androidによって許可される信頼できるSIMカードが一覧表示されます。このリストで定義されていないSIMカードを挿入すると、画面がロックされ、アラートSMSが管理者に送信されます。

新しいSIMカードを追加するには、➕アイコンをタップしますSIMカードの**名前**(HomeWorkなど)とIMSI (International Mobile Subscriber Identity)番号を入力します。一般的に、SIMカードに記載されているIMSIは15桁の番号です。一部の場合、これよりも短いことがあります。

リストからSIMカードを削除するには、エントリをロングタップして、アイコンをタップします。

信頼できるSIMカード機能は、Android 10以降のデバイスでは使用できません。

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。

リモートコマンド

リモートコマンドはESET PROTECTコンソールから直接トリガーできます。

デバイスの検索

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を受信します。より正確な位置情報が10分後に使用可能になった場合は、デバイスは新しいSMSを送信します。

デバイスをロック

これにより、デバイスがロックされます。管理者パスワードまたはロック解除リモートコマンドを使用すると、ロック解除できます。

ロックされたデバイスのロック解除

デバイスのロックが解除され、現在デバイスに挿入されているSIMカードが信頼できるSIMとして保存されます。

警報/紛失モードサウンド

デバイスはロックされ、5分間(またはロック解除されるまで)大音量が鳴ります。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。

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。すべてのアクセス可能なデータが消去されます。ファイルヘッダーは削除されます。これには数分かかる場合があります

アプリケーションコントロール

アプリケーションコントロール機能を使用すると、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。管理者は、次のアプリケーションの複数のフィルタリング方法から選択できます。

- 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）

ブロックルール

[アプリケーションコントロール] > [ブロック] > [ブロックルール]セクションでは、次の条件に基づいて、アプリケーションブロックルールを作成できます。

- アプリケーション名またはパッケージ名
- 分類
- 権限



アプリケーションをブロック

アプリケーション名でブロック

ESET Endpoint Security for Androidでは、管理者が名前またはパッケージ名に応じてアプリケーションをブロックできます。**[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された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。

名前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の名前との完全一致を検索しますESET Endpoint Security for Android 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ります。

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、パッケージ名でこのようなアプリケーションをブロックすることをお勧めします。これは、実行時に変更したり、別のアプリケーションで再利用したりできない一意のアプリケーションIDです。

ローカル管理者の場合、ユーザーは**アプリケーションコントロール > 監視 > 許可されたアプリケーション**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した後に、**詳細**画面にはアプリケーションパッケージ名が表示されます。アプリケーションをブロックするには、次のステップに従いますを

名前でアプリケーションをブロックする方法

1.**[アプリケーションコントロール] > [ブロック] > [アプリケーションのブロック] > [名前でブロック]**をタップします。

2.アプリケーション名またはパッケージ名に応じてアプリケーションをブロックするかどうかを決定します。

3.アプリケーションがブロックされる条件になる単語を入力します。複数の単語を区切るには、カンマ(、)を区切り文字として使用します。

例えば、単語「*poker*」が**[アプリケーション名]**フィールドにある場合、名前に「*poker*」を含むすべてのアプリケーションがブロックされます。「*com.poker.game*」を**[パッケージ名]**フィールドに入力するとESET Endpoint Security for Androidは1つのアプリケーションだけをブロックします。

アプリケーションカテゴリでブロック

ESET Endpoint Security for Androidでは、管理者が定義済みのアプリケーションカテゴリに応じてアプリケーションをブロックできます。**[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されたアプリケーションの一覧が表示されます。

既存のルールを変更する場合は、ルールをロングタップして、**[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]**をタップします。

カテゴリに基づいてアプリケーションをブロックする方法

1.**[アプリケーションコントロール] > [ブロック] > [アプリケーションのブロック] > [カテゴリでブロック]**をタップします。

2.チェックボックスを使用して定義済みのカテゴリを選択し、**[ブロック]**をタップします。

アプリケーション権限でブロック

ESET Endpoint Security for Androidでは、管理者が権限に応じてアプリケーションをブロックできます。**[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されたアプリケーションの一覧が表示されます。

既存のルールを変更する場合は、ルールをロングタップして、**[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]**をタップします。

権限でアプリケーションをブロックする方法

1.**[アプリケーションコントロール]** > **[ブロック]** > **[アプリケーションのブロック]** > **[権限でブロック]**をタップします。

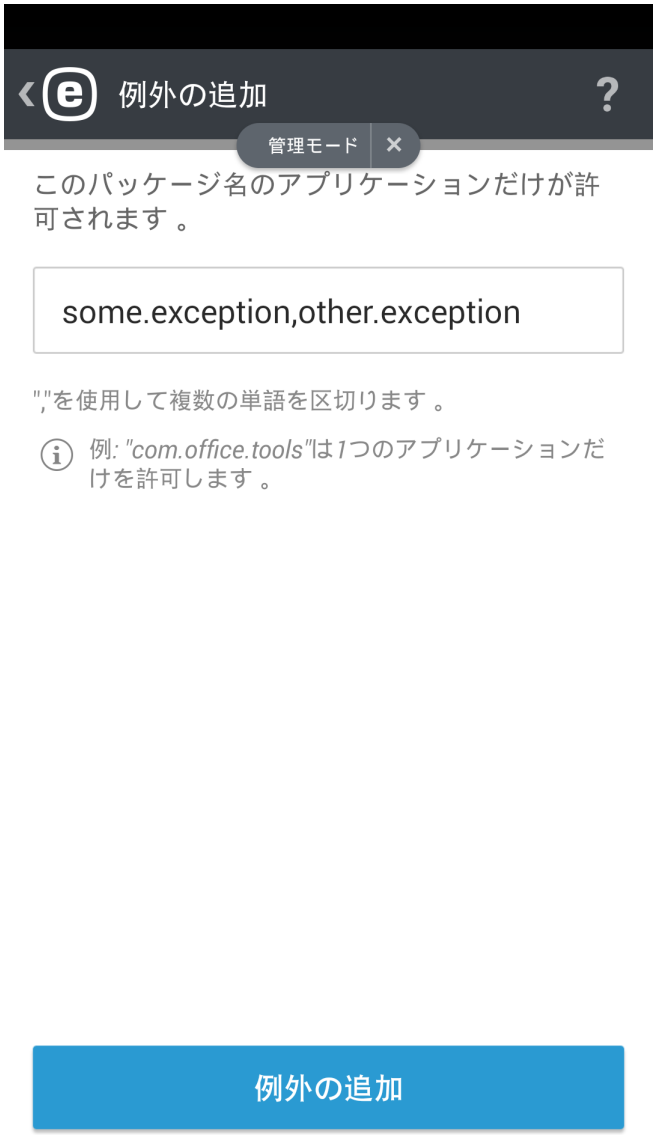
2.チェックボックスを使用して権限を選択し、**[ブロック]**をタップします。

不明なソースをブロック

既定ではESET Endpoint Security for Androidは、インターネットまたはGoogle Play Store以外のソースから取得された他のアプリケーションをブロックしません。**[ブロックされたアプリケーション]**にはブロックされたアプリケーションの概要が表示されます(パッケージ名、適用されたルール)。また、アプリケーションをアンインストールしたり、ホワイトリスト(**[セクション]**セクション)に追加するオプションもあります。

例外

アプリケーションコントロール > **ブロック** > **例外** > **例外の追加**をタップします。例外を作成して、ブロックされたアプリケーションのリストから特定のアプリケーションを除外できますESET Endpoint Security for Androidをリモートで管理する管理者はこの新しい機能を使用して、特定のデバイスがインストール済みアプリケーションに関する企業ポリシーに準拠しているかどうかを判断できます。



例外の追加方法

新しい例外を追加(アプリケーションパッケージ名を入力)する他に、**ブロックされたアプリケーション**のリストから除外すると、アプリケーションをホワイトリストに登録することもできます。

1. ESET Endpoint Security for Androidアプリケーションで**アプリケーションコントロール**をタップします。
2. **ブロック**>**ブロックされたアプリケーション**をタップします。
3. ホワイトリストに追加するアプリケーションを選択します。
4. 右上の3点アイコンをタップし、**例外の追加**をタップします。
5. 管理者パスワードを入力し、**Enter**をタップします。

必要なアプリケーション

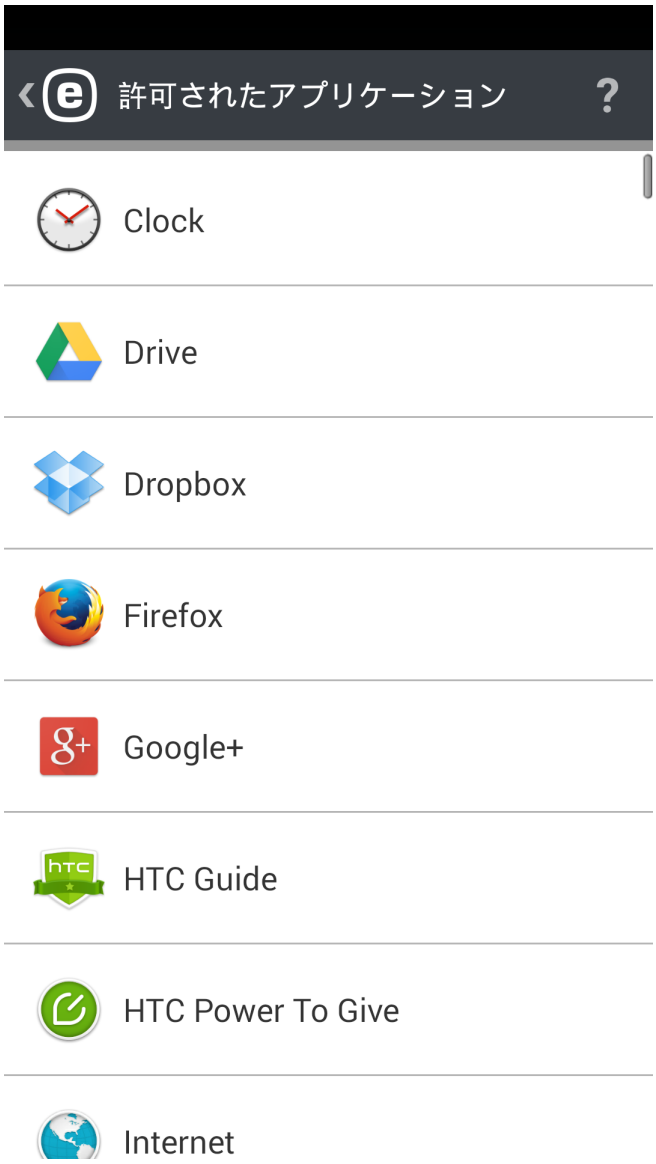
ESET PROTECTからリモートでESET Endpoint Security for Androidを管理する場合は、対象デバイスにインストールする必要があるアプリケーションを定義できます。次の情報が必須です。

- 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。

この機能はESET Endpoint Security for Androidアプリでは使用できません。

許可されたアプリケーション

このセクションには、ブロックルールでブロックされている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。



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の動作を追跡します。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。

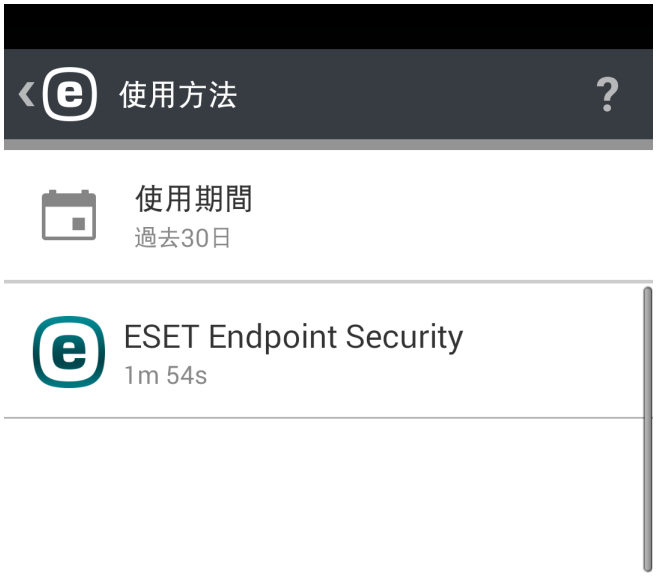
デバイスにインストールされた一部のアプリケーションは、有料のサービスにアクセスしたり、位置情報を追跡したり、個人情報、連絡先、またはテキストメッセージを読み取ったりする場合があります。ESET Endpoint Security for Androidはこのようなアプリケーションを監査します。

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し、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。



使用状況

このセクションでは、管理者は、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。



デバイスセキュリティ

デバイスセキュリティでは、管理者が次の処理を実行できます。

- モバイル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
- 必要な画面ロック強度を指定
- 内蔵のカメラの使用を制限

画面ロックポリシー



このセクションでは、管理者が次のことができます。

- システム画面ロックコードの最低セキュリティレベル(パターン、PIN、パスワード)を設定し、コードの複雑さ(最低コード長など)を定義
- ロック解除の試行を失敗した最大回数を設定(これを超えるとデバイスが初期設定にリセットされます)
- 最大画面ロックコード経過時間を設定
- ロック画面タイマーを設定

現在のデバイス設定が企業セキュリティポリシーに準拠している場合、ESET Endpoint Security for Android は自動的にユーザーと管理者に通知します。デバイスが準拠しない場合、アプリケーションは、自動的に、ユーザーに対してもう一度準拠状態にするために変更する項目を提案します。

デバイス設定ポリシー

デバイスセキュリティには、システム管理者が定義済みデバイスを監視して推奨状態を判断するための**デバイスセキュリティポリシー**(以前の**セキュリティ監査**機能の一部)もあります。

デバイス設定の内容:

- Wi-Fi
- GPS衛星
- 位置情報サービス
- メモリ
- データローミング
- 通話ローミング
- 不明なソース
- デバッグモード
- NFC
- 記憶領域の暗号化
- ルート化されたデバイス


通知センター
管理モード
処理されていない脅威: 1
脅威を確認して解決
画面ロックコードが準拠していません
コードの変更
ブロックされたアプリケーション: 42
ブロックされたアプリケーションを確認してアンインストール
記憶領域が暗号化されていません
記憶装置の暗号化
GPS無効
GPSを有効にしてアンチセフトによる位置情報決定を許可
不明なソースが許可されました
不明なソースからのインストールを無効にします 。
USBのデバッグモードが有効です
セキュリティ強化のためUSBデバッグモードを無効にする
NFC有効

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（機密情報を得るためユーザーを操作する）を使った犯罪行為です。フィッシングは、銀行口座番号、クレジットカード番号⍰PIN番号、ユーザー名、パスワードなどの機密情報を取得するために使用されることがあります。

フィッシング対策は有効にしたままにすることをお勧めします⍰ESET Endpoint Security for AndroidがURLアドレスを検査する - ESETマルウェアデータベースにリストされているWebサイトまたはドメインからの、フィッシングと考えられる攻撃はすべてブロックされ、攻撃があったことを知らせる警告通知が表示されます。

重要: フィッシング対策機能はAndroidOSで使用できる最も一般的なWebブラウザーと統合されています。一般的に、フィッシング対策保護はChrome⍰Firefox⍰Opera⍰Opera Mini⍰Dolphin⍰SamsungおよびAndroidデバイスにプレインストールされているブラウザーで使用できます。その他のブラウザーは保護されていないブラウザに設定されています。 トグルを使用すると、このようなブラウザーへのアクセスをブロックできます。

ESETフィッシング対策が正しく動作するには⍰Androidシステム設定で**アクセシビリティ**を有効にする必要があります。

Android 13の. APKファイルからインストールされたESET Endpoint

Security for Androidでアクセシビリティ権限を許可

備考
セキュリティの理由からAndroid 13は、.apkファイルからインストールされたアプリへのアクセシビリティ権限の使用を制限し。このような権限への不正アクセスを防止します。

ESET Endpoint Security for Androidでのこの権限の使用方法
ESETは、お客様がアクセスしたWebサイトのURLにアクセスするために、この権限を使用します。フィッシング、マルウェア、その他の危険なアクティビティなどWebサイトに悪意があるかどうか分析します。
スレッドが検出されると、ユーザーと機密情報を保護するためにWebサイトがブロックされます。アクセシビリティ権限でアクセスされるデータは第三者と共有されません。

アクセシビリティの問題を解決するには

1. **設定 > アクセシビリティ > ダウンロードされたアプリ**を開きますESET Endpoint Security for Androidが灰色で表示されます。

2. ESET Endpoint Security for Androidアプリをタップすると、**制限された設定**ダイアログが開きます。

3. **[OK]**をタップします。

4. **設定 > アプリ** > ESET Endpoint Security for Androidに移動し、**アプリ情報**を開きます。

5. 右上の3点メニューアイコンをタップし、**制限された設定を許可**します。

アクセシビリティ権限が許可され、アプリケーションの使用を開始できます。

Webコントロール

Webコントロール設定を使用して、法的責任のリスクから会社を保護します。たとえばWebコントロールは、知的財産権に抵触するWebサイトへのアクセスを規制できます。この機能の目的も、作業生産性に悪影響を与える不適切または有害なコンテンツやページに従業員がアクセスしないようにすることにあります。

企業やシステム管理者は、事前に定義された27以上のカテゴリと140以上のサブカテゴリへのアクセスを禁止し、このようなアクセスをログに記録できます。

Webコントロールは管理された機能です。すべての設定はESET PROTECT Cloudで管理されます。

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 Cloudに登録。

保護されたブラウザ

- Chrome
- Chrome Beta
- Firefox

- Firefox Beta
- Opera
- Opera Beta
- Opera Mini
- Opera Mini Beta
- Opera TVブラウザー
- Samsung Internet
- Mint
- Yandexブラウザー
- DuckDuckGo
- Kiwiブラウザー
- エッジ
- AmazonデバイスのSilk
- Miブラウザー
- Xiaomi Miブラウザー
- Android TVのVewd
- Webビューで保護されたブラウザーコンポーネントを使用するアプリも保護されます。

通話フィルター

通話フィルターはユーザー定義のルールに基づいて、受信/送信通話をブロックします。

着信がブロックされているときには、通知は表示されません。これは、迷惑な未承諾情報がないという利点がありますが、通話が誤ってブロックされた可能性がある場合には、常に通話ログを確認できます。

通話フィルターは、通話をサポートしないタブレットでは動作しません。

最後の発信者からの通話をブロックするには、**最後の発信者をブロック**をタップします。これで新しいルールが作成されます。

ワイルドカードを使用して電話番号をブロック

以下の表のワイルドカードを使用して、さまざまな番号をブロックできます。

ワイルドカード	説明
*	は複数の文字を表します。
?	は1文字を表します。

例

特定の国から通話を受信しないようにする場合は、国コードと*ワイルドカード文字を**携帯電話番号**フィールドに入力します。この番号パターンで始まる国からのすべての着信通話はブロックされます。その国からの一部の電話番号を除外するには、**許可**アクションを使用して、新しいルールを追加します。次の図は、スロバキアからのすべての通話をブロックする方法を示します。



ルール

ユーザーとして、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ます。

新しいルールの作成に関する詳細については、このセクションを参照してください。

[**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、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。

新しいルールを追加する方法

新しいルールを追加するには、**ルールの追加**をタップするか、**ルール**画面の右上にあるアイコンをタップします。

個人または電話番号のグループを指定しますESET Endpoint Security for Androidは連絡先に保存された連絡先グループを認識します(家族、友達、同僚など)。**すべての不明な番号**には、連絡先リストに保存されていない電話番号が含まれます。このオプションを使用して、望ましくない電話(勧誘電話など)をブロックしたり、従業員が不明な番号に発信するのを防止できます。**すべての既知の番号**オプションは、連絡先リストに保存されたすべての電話番号を参照します。**番号非通知**は、Calling Line Identification Restriction (CLIR)経由で意図的に非表示になっている電話番号を持つ発信元に適用されます。

ブロックまたは許可される番号を指定します。

- 発信通話
- 着信通話

指定した期間の間だけルールを適用するには、[**常に**]>[**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。この機能は、会議、出張、夜間、または週末中に邪魔されたくない場合に便利です。

注意:海外にいる場合は、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(+1610100100など)。

履歴

[**履歴**]セクションには、通話フィルター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。

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、ルールをタップしてリストのエントリを選択し、アイコンタップします。

リストからエントリを削除するには、エントリを選択して、アイコンをタップします。その他の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、アイコンをタップします。

設定

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。アプリケーションのユーザーインターフェー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。

のアップデート – 最大限の保護のために、最新バージョンのESET Endpoint Security for Androidを使用することが重要です。[アップデート]をタップして、新しいバージョンをESET Webサイトからダウンロードできるかどうかを確認してください。

デバイス ID – デバイスが盗まれたり紛失したりした場合は、管理者のデバイス識別名を設定または変更できます。

リモート管理 – あなたのデバイスをESET PROTECT.に接続してください

詳細設定

詳細設定をクリックして、詳細設定セクションを開きます。

権限通知 - 権限管理セクションを参照してください。

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製品の向上を図ることができます。機密情報は送信されません。インストールセットアップウィザードでこのオプションを有効にしていない場合は、設定 > 詳細設定セクションで有効にできます。

管理者パスワード – このオプションでは、新しい管理者パスワードを設定するか、既存のパスワードを変更できます。詳細については、このマニュアルの「管理者パスワード 」セクションを参照してください。

設定のインポート/エクスポート - ESET Endpointアプリケーションとの間で設定をインポートまたはエクスポートします。

設定のインポート/エクスポート

デバイスがESET PROTECTによって管理されていない場合に1つのモバイルデバイスから設定を簡単に共有するためにESET Endpoint Security for Androidには、プログラム設定をインポートおよびエクスポートするオプションがあります。管理者は手動でデバイス設定をファイルにエクスポートできます。このファイルは共有(電子メール経由など)し、クライアントアプリケーションを実行する任意の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許可すると、すべての設定が自動的に定義され、アプリケーションがアクティベーションされます(ライセンス情報が含まれている場合)。すべての設定は管理者パスワードによって保護されます。



設定のエクスポート

現在のESET Endpoint Security for Androidの設定をエクスポートするには、設定ファイル名を指定します。現在の日時が自動的に入力されます。また、エクスポートされたファイルにライセンス情報(ライセンスキーまたはセキュリティ管理者アカウントの電子メールアドレスとパスワード)も指定できますが、この情報は暗号化されないため、悪用される可能性があります。

次の手順では、ファイルを共有する方法を選択します。

- Wi-Fiネットワーク
- Bluetooth
- メール
- Gmail
- ファイル参照アプリケーション(ASTRO File ManagerやES File Explorerなど)

設定のインポート

デバイスにあるファイルから設定をインポートするには、ファイル参照アプリケーションを使用して、設定ファイルを見つけ□ESET Endpoint Security for Androidを選択します。

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。

履歴

履歴 セクションには、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。

管理者パスワード

指定**管理者パスワード** は、デバイスのロックを解除し、Anti-Theftコマンドを送信し、パスワード保護機能にアクセスし、ESET Endpoint Security for Androidをアンインストールするために必要です。

管理者パスワードを作成すると、ユーザーが設定を変更したり□ESET Endpoint Security for Androidをアンインストールしたりできなくなります。

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。

ロックされた画面を使用してデバイスで管理者パスワードをリセットするには：

1. ユーザーの同意を承認するには、 **パスワードを忘れた場合 > 続行 > 確認コードの要求**をタップします。デバイスが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** リンクをタップし、ESETテクニカルサポートに連絡してください。



2. 確認コードとデバイスIDが記載された電子メールが、ESETライセンスに関連付けられた電子メールアドレスに送信されます。確認コードは7日間有効です。デバイスのロック画面で確認コードと新しいパスワードを入力します。

リモート管理

ESET PROTECT では、1つの中央ロケーションからネットワーク環境のESET Endpoint Security for Android を管理できます。

コマンドとESET PROTECTによってセキュリティレベルが向上するだけでなく、クライアントワークステーションとモバイルデバイスにインストールされたESET 製品の管理が容易になります。デバイスにESET Endpoint Security for Android があると、次のいずれかのインターネット接続でESET PROTECT に接続できますWiFi, LAN, WLANセルラーネットワーク(3G, 4G LTE, HSDPA, GPRS)など。ただし、標準インターネット接続(プロキシまたはファイアウォールがない)で、エンドポイントが両方正しく設定されている場合にかぎります。

セルラーネットワークでESET PROTECT に接続した場合、接続が成功するかどうかはモバイルネットワークプロバイダによって異なり、完全に機能するインターネット接続が必要です。

デバイスをESET PROTECT接続するには、デバイスをコンピューター リスト(ESET PROTECT Webコンソール)に追加し、**デバイス登録**タスクを使用してデバイスを登録し、**MDCサーバーアドレスを入力します。**.

ESET PROTECTでは、登録リンク(MDCサーバーアドレス)は`https://MDCserver:port/token`という標準形式を使用します。このリンクには次の値があります。

- **MDCserver** - Mobile Device Connector (MDC)を実行するサーバーの完全DNS名または公開IPアドレス。ホスト名は、内部Wi-Fi ネットワーク経由で接続している場合にのみ使用できます。
- **ポート** - Mobile Device Connectorに接続するために使用されるポート番号

- **トークン** - ESET PROTECT Webコンソールで管理者が生成した文字列。

ESET PROTECTを使用したネットワーク管理の詳細については、次のオンラインヘルプトピックを参照してください。

- ポリシーの管理方法
- クライアントタスクの作成方法
- レポートの詳細

デバイス ID

デバイスが紛失または盗難に遭った場合に、管理者はデバイスIDによってデバイスを特定できます。

権限管理

Android 6 (Marshmallow)では Googleは新しい権限管理システムを導入しました ESET Endpoint Security for Android はそれに対応します Android 6.0用アプリは使用を開始するときに権限を確認します。インストール中にアプリケーションアクセスを付与する代わりに、最初にアプリが特定のデバイス機能にアクセスするときに確認が表示されます。

ESET Endpoint Security for Android は次の機能へのアクセスが必要です。

- **アクセシビリティ** - ESETフィッシング対策の適切な機能に必要
- **連絡先** - Anti-Theftと通話フィルタリング機能に必要
- **ロケーション** - Anti-Theft
- **電話** -Anti-Theftと通話フィルター
- **SMS** -Anti-Theftと通話フィルター
- **ストレージ** – ウイルス対策とAnti-Theft

管理者は次の場所でこれらの権限の監視を無効にできます。**設定** > **権限通知**.



カスタマーサポート

ESETカスタマーサポートスペシャリストが、ESET Endpoint Security for Androidまたはその他のESET製品に関連する管理支援または技術サポートを提供します。

直接デバイスからサポート要求を送信するにはESET Endpoint Security for Androidメイン画面でメニューアイコンをタップし、**カスタマーサポート** > **カスタマーサポート**をタップして、すべての必須フィールドを入力します。



ESET Endpoint Security for Androidには詳細ロギング機能があり、潜在的な技術上の問題を診断できます。詳細アプリケーションログをESETに提供するには、**アプリケーションログの送信**が選択されていること(既定)を確認してください。**送信**をタップしてリクエストを送信しますESETカスタマーサポートスペシャリストが、指定した電子メールアドレスにご連絡いたします。

カスタマーエクスペリエンス改善プログラム

カスタマーエクスペリエンス改善プログラムに参加することで、製品の使用に関連する匿名情報をESETに提供します。データ処理の詳細については、プライバシーポリシーを参照してください。

同意

プログラムへの参加は任意であり、お客様の同意に基づいています。参加した後は、一切のアクションは不要であり、自動的に処理されます。いつでも、製品設定を変更することで、同意を取り消すことができます。匿名データが処理されます。

収集される情報の種類

製品の操作に関するデータ

この情報は、製品の使用方法に関する詳細情報をESETに提供します。これによりESETは、頻繁に使用される機能、ユーザーが修正する設定、または製品の使用に費やされた時間などを把握することができます。

デバイスに関連するデータ

ESETは、製品が使用されている場所やデバイスについて理解するためにこの情報を収集します。一般的には、デバイスモデル、国、バージョン、オペレーティングシステム名などが収集されます。

エラー診断データ

エラーおよびクラッシュ状況に関するデータも収集されます。たとえば、発生したエラーと原因が何かなどです。

なぜこの情報が収集されるのですか。

この匿名情報により、お客様のために製品を改善できます。この情報は、できるかぎり、関連性が高く、使いやすく、エラーのない製品を開発するうえで役立ちます。

誰がこの情報を管理するのですか。

ESET, spol. s r.o.はプログラムで収集されるデータの単独の管理者です。この情報は第三者と共有されません。

エンドユーザーライセンス契約

発効日：2021年10月19日

重要:ダウンロード、インストール、コピー、または使用の前に、製品利用に関する下記契約条件を注意してお読みください。**本製品をダウンロード、インストール、コピー、または使用することにより、お客様はこれらの条件に対する同意を表明し、**プライバシーポリシー**に同意したことになります。**

エンドユーザー使用許諾契約

本エンドユーザーライセンス契約（「本契約」）は、Einsteinova 24, 85101 Bratislava, Slovak Republicに所在し、ブラチスラバ第1地方裁判所の有限会社部門District Court Bratislava I. Section Sroにおいて掲載番号3586/B, 31333532として商業登記されているESET, spol. s r. o.（ESETまたは「供給者」）と、自然人または法人であるお客様（「お客様」または「エンドユーザー」）との間で締結され、お客様に本契約の第1条で定義する本ソフトウェアを使用する権利を付与するものです。本契約の第1条で定義する本ソフトウェアは、データ記憶媒体への格納、電子メールでの送付、インターネットからのダウンロード、供給者のサーバーからのダウンロード、または後述の条件および状況下におけるその他の供給者からの取得が行えます。

本契約は購入に関する契約ではなく、エンドユーザーの権利に関する合意事項を定めるものです。供給者は、本ソフトウェアのコピー、これが商業包装にて供給される物理的媒体、および本契約に基づきエンドユーザーが権利を付与される本ソフトウェアのすべてのコピーの、所有者であり続けます。

本ソフトウェアのインストール時、ダウンロード時、コピー時または使用時に、[同意します]オプションをクリックすることにより、本契約の条件に明示的に同意し、プライバシーポリシーを承諾するものとします。本契約の規定またはプライバシーポリシーに同意しない場合は、直ちに[同意しない]オプションをクリックし、インストールまたはダウンロードを取り消すか、本ソフトウェア、インストールメディ

ア、付属ドキュメント、および購入時の領収書を破棄するかESETまたは本ソフトウェアの供給者にそれを返却してください。

お客様は、本ソフトウェアを使用することにより、お客様が本契約を読了かつ理解し、本契約条項による拘束に同意したことになります。

1.**ソフトウェア。**(i) 本契約およびすべてのコンポーネントに付属するコンピュータープログラム(ii)データ媒体、電子メール、またはインターネット経由でのダウンロードで提供される本ソフトウェアのオブジェクトコードの形式を含む、本契約で提供されるディスクCD-ROMDVD電子メール、添付ファイル、その他の媒体のすべての内容(iii)本ソフトウェアに関連する書面の説明資料、その他の文書、特に本ソフトウェア、その仕様のすべての説明、 本ソフトウェアの属性または動作の説明、本ソフトウェアが使用される動作環境の説明、本ソフトウェアの使用またはインストール手順、本ソフトウェアの使用方法の説明(「ドキュメント)(iv)本契約の第3条に従い供給者からお客様にライセンス供与された本ソフトウェアのコピー、本ソフトウェアに不具合があった場合のパッチ、本ソフトウェアへの追加機能、本ソフトウェアの拡張機能、本ソフトウェアの修正バージョン、ソフトウェアコンポーネントのアップデート(該当する場合)を意味します。本ソフトウェアは実行可能なオブジェクトコードの形態でのみ提供されるものとします。

2.**インストール、コンピューター、およびライセンスキー**。データキャリアで供給、電子メールで送信、インターネットからダウンロード、供給者のサーバーからダウンロード、または他のソースから取得されたソフトウェアにはインストールが必要です。お客様は、本ソフトウェアを正しく設定されたコンピューターにインストールし、少なくともドキュメントで規定された要件に準拠する必要があります。インストール方法はドキュメントで説明されています。本ソフトウェアをインストールするコンピューターに、本ソフトウェアに悪影響を及ぼす可能性があるコンピュータープログラムやハードウェアをインストールすることはできません。コンピューターとは、本ソフトウェアがインストールまたは使用される、パーソナルコンピューター、ノートブック、ワークステーション、パームトップコンピューター、スマートフォン、ハンドヘルド電子機器、または本ソフトウェアの対象として設計されている他の電子機器を含む(ただしこれらに限定されない)を意味します。ライセンスキーとは、本契約に準拠して、本ソフトウェア、特定のバージョン、またはライセンス条項の拡張の法的な使用を許可するために、エンドユーザーに提供される一意の連続する記号、文字、数字、または特殊記号を意味します。

3.**ライセンス**。お客様が本契約に同意しており、ライセンス料を支払い期日までに支払い、本契約に定められているすべての契約条項に従うことを前提として、供給者はお客様に対し、以下の権利を付与します（以下「ライセンス」とします）。

a) **インストールおよび使用。**お客様には、コンピューターのハードディスクまたはその他のデータ永久記憶媒体にデータを格納するために本ソフトウェアをインストールし、コンピューターシステムのメモリへ本ソフトウェアをインストールおよび格納し、コンピューターシステム上で本ソフトウェアを実装、格納および表示する、非独占的かつ譲渡禁止の権利が付与されます。

b) **ライセンス数の規定。**本ソフトウェアを使用する権利は、エンドユーザー数によって制限されます。1人のエンドユーザーとは(i) 本ソフトウェアがインストールされている1台のコンピューターを意味しますii)ライセンス数がメールボックスを単位として決定される場合、エンドユーザーはメールユーザーエージェント（以下MUAとします）を介して電子メールを受信する1人のコンピューターユーザーを意味します。電子メールがMUAで受信後、複数のユーザーに自動的に配信される場合、エンドユーザーの数は、その電子メールが配信されるユーザーの実際の数によって決まります。メールサーバがメールゲートの役割を果たす場合、エンドユーザーの数は、そのゲートがサービスを提供するメールサーバユーザーの数と同じになります。(エイリアスなどを使用して)1人のユーザーに不特定多数の電子メールアドレスが送信され、それらが受け付けられる場合、クライアント側で多数のユーザーにそのメールが自動的に配信されるのでなければ、ライセンスは1台のコンピューターに必要です。同じライセンスは、同時に複数のコンピューターで使用できません。エンドユーザーは、供給者によって付与されたライセンス数に基づく制限に従い、本ソフトウェアを使用する権限が与えられている範囲においてのみ、本ソフトウェアのライセンスキーを入力する資格があります。このライセンスキーは機密情報であると見なされます。本契約または供給者によって許可されている場合を除き、お客様はライセンスを第三者と共有すること、または第三者がライセンスを使用することを許可することが禁止されています。ライセン

スキーが危険にさらされた場合は、速やかに供給者に通知してください。

c) **Home/Business Edition**本ソフトウェアのHome Editionバージョンは、家庭および家族での利用に限定された個人または非商業環境でのみ使用されるものとします。本ソフトウェアを商業環境、またはメールサーバー、メール中継、メールゲートウェイ、インターネットゲートウェイで使用する場合は、本ソフトウェアのBusiness Editionバージョンを入手する必要があります。

d) **ライセンス契約の期間。**お客様は、本ソフトウェアを期限付きで使用する権利があります。

e) **OEMソフトウェア。**OEMに分類されたソフトウェアの使用は、それがプリインストールされていたコンピューターに制限されます。別のコンピューターにインストールすることはできません。

f) **NFRまたは試用ソフトウェア。**再販不可品NFRまたは試用版に分類されるソフトウェアは、対価を求めて譲渡することはできず、ソフトウェア機能のデモまたはテスト目的のみで使用されるものとします。

g) **ライセンスの契約解除。**ライセンス契約は，その期間の満了により契約が自動的に解除されます。供給者は、お客様が本契約のいずれかの条項に違反したときは、供給者が持つ他の権利および法的救済手段に影響を与えることなく、本契約を解約することができます。本ライセンスを取り消す場合、お客様は、本ソフトウェアおよびバックアップコピーを直ちにすべて削除、破棄するか、自費でESETまたはソフトウェアの入手元にそれを返却する必要があります。ライセンスの終了時には、供給者は、エンドユーザーが、供給者のサーバーまたはサードパーティのサーバーに接続する必要がある本ソフトウェアの機能を使用する権利を取り消す権利があるものとします。

4.**データ収集機能およびインターネット接続要件。**本ソフトウェアの正常な動作には、インターネット接続が必要であり、プライバシーポリシーに従い、定期的に供給者のサーバーまたは第三者のサーバーおよび該当するデータ収集に定期的に接続する必要があります。インターネットへの接続およびデータ収集は、次のソフトウェア機能で必要です。

a) **ソフトウェアのアップデート。**供給者には、本ソフトウェアのアップデートまたはアップグレード(「アップデート」)を適時発行する権利がありますが、アップデートを提供する義務はありません。この機能は、ソフトウェアの標準の設定から有効にできます。エンドユーザーがアップデートの自動インストールを無効にしていないかぎり、アップデートは自動的にインストールされます。アップデートを提供するために、プライバシーポリシーに準拠し、本ソフトウェアがインストールされているコンピューターまたはプラットフォームに関する情報を含む、ライセンスの正当性を検証する必要があります。

アップデートの提供には、サービス終了ポリシ(EOLポリシー」)が適用される場合があります。https://go.eset.com/eol_businessをご覧ください。本ソフトウェアまたは本ソフトウェアの機能がEOLポリシーで定義されているサービス終了日に達した後は、アップデートが提供されません。

b) **供給者への侵入物および情報の転送**。本ソフトウェアには、コンピューターウイルスおよびその他の悪意のあるプログラム、ファイルURLIPパケット、イーサネットフレームなどの不審、問題、潜在的に望ましくない、または潜在的に危険なオブジェクト(「侵入」)のサンプルを収集する機能が含まれ、インストール処理、コンピューター、ソフトウェアがインストールされているプラットフォームの情報、本ソフトウェアの操作および機能の情報(「情報」)を含む(ただしこれらに限定されない)、これらのオブジェクトを供給者に送信します。情報および侵入には、エンドユーザーまたは本ソフトウェアがインストールされているコンピューターの他のユーザーのデータ(ランダムまたは誤って取得された個人データを含む)、関連付けられたメタデータによる侵入の影響を受けるファイルが含まれる場合があります。

情報および侵入は次のソフトウェア機能によって収集される場合があります。

i.LiveGridレピュテーションシステム機能には、侵入に関する単方向ハッシュの収集と供給者への送信が含まれます。この機能は、ソフトウェアの標準設定で有効です。

ii.LiveGridフィードバックシステム機能には、侵入を収集し、関連付けられたメタデータおよび情報とと

もに供給者に送信する機能が含まれます。この機能は、本ソフトウェアのインストール処理中に、エンドユーザーがアクティブ化することができます。

供給者は、侵入の分析と研究、ソフトウェアの改良、およびライセンスの正当性の検証の目的でのみ、受け取った情報および侵入を使用するものとし、適切な対策を講じて、受け取った侵入および情報が安全であることを保証するものとします。本機能をアクティブ化することで、プライバシーポリシーの規定に従い、関連する法規制に準拠して、侵入および情報は供給者によって収集および処理される場合があります。この機能はいつでも無効にすることができます。

本契約の目的のために、プライバシーポリシーに従い、供給者がお客様を特定できるようにするデータを収集、処理、および保存する必要があります。お客様は、供給者が独自の手段によって、お客様が本契約の規定に従って本ソフトウェアを使用しているかどうかを確認することに同意します。お客様は、本契約の目的でのみ、本ソフトウェアと供給者のコンピューターシステムまたは供給者の販売およびサポートネットワークの一部としての供給者のビジネスパートナーのコンピューターシステムとの間の通信中に、お客様のデータを転送し、本ソフトウェアの機能および本ソフトウェアの使用許可を保証し、供給者の権利を守る必要があることを承諾します。

本契約の締結後、供給者および供給者の販売およびサポートネットワークの一部としての供給者のビジネスパートナーは、請求目的、本契約の履行、およびお客様のコンピューターでの通知の送信のために、お客様を特定できる基本データを転送、処理、および保管する権利を有するものとします。

データ主体としてのプライバシー、個人データ保護、およびお客様の権利の詳細については、供給者のWebサイトまたはインストール処理で直接アクセスできるプライバシーポリシーを参照してください。お客様は、ソフトウェアのヘルプセクションからアクセスすることもできます。

5.**エンドユーザの権利行使**。お客様は、エンドユーザーの権利を、直接またはお客様の従業員を通じて行使する必要があります。お客様は、自らの活動を確実なものとするためにのみ、およびお客様がライセンスを取得したコンピューターシステムを保護するためにのみ、本ソフトウェアを使用できます。

6.**権利の制限。**お客様は本ソフトウェアのコピー、配布、部品の分離、または派生バージョンの作成を行ってはなりません。本ソフトウェアの使用時には、下記の制限事項に従う必要があります。

a) お客様は、データの永久記憶用媒体上に本ソフトウェアのコピーを1つ、バックアップコピーとして作成できます。ただし、この保管用のバックアップコピーは、他のいかなるコンピュータにもインストールしたり、または使用したりすることができません。これ以外に本ソフトウェアのコピーを作成することは、本契約に対する違反となります。

b) 本契約に規定されている以外のいかなる態様でも、本ソフトウェアまたは本ソフトウェアのコピーの使用、改変、複製、または使用権の譲渡を行ってはなりません。

c) 本ソフトウェアの売却、サブライセンス付与、他人への賃貸もしくは他人からの賃借、借用、または商業サービスの提供目的での本ソフトウェアの使用は禁じられています。

d) 本ソフトウェアのリバースエンジニアリング、逆コンパイル、またはソフトウェアの逆アセンブルを行ったり、ソースコードを取得しようとしたりしてはなりません。ただし、そのような制限を設けることが法律によって明示的に禁止されている範囲内においては、この限りではありません。

e) お客様は、著作権法およびその他の知的財産権から生じる、適用可能な制限など、本ソフトウェアを使用する際の法律におけるすべての適用可能な法的規制に従う態様においてのみ、本ソフトウェアを使用できます。

f) お客様は、本ソフトウェアおよびその機能を、他のエンドユーザーがそれらのサービスにアクセスする可能性を制限しない方法でのみ使用することに同意するものとします。供給者は、可能な限り多くのエンドユーザーがサービスを利用できるようにするために、個別のエンドユーザーに提供されるサービスの範囲を制限する権利を留保します。サービスの範囲を制限することにより、本ソフトウェアのすべての機能を使用することもできなくなり、本ソフトウェアの特定の機能に関連する供給者のサーバー上

またはサードパーティのサーバー上のデータおよび情報も削除されることとします。

g) お客様は、本契約の条項に反して、ライセンスキーの使用に関する活動、または何らかの形式での使用済みまたは未使用のライセンスキーの譲渡、不正複製、複製または生成されたライセンスキーの配布、あるいは供給者以外から入手したライセンスキーを使用したソフトウェアの利用など、本ソフトウェアの使用の資格がない個人にライセンスキーを提供する行為を実施しないことに同意します。

7.**著作権**。本ソフトウェア、および所有権や知的所有権を含む一切の権利は、ESETおよび / またはESETのライセンス供給者の財産です。これらは、国際条約の規定と本ソフトウェアが使用される国のその他のすべての準拠法によって保護されます。本ソフトウェアの構造、編成、およびコードは、ESETおよび / またはESETのライセンス供給者の重要な企業秘密であり機密情報です。お客様は、第6条(a)に当てはまる場合を除いて、本ソフトウェアをコピーすることはできません。本契約に基づき、お客様が作成するコピーはすべて、本ソフトウェア上に示されるものと同じ著作権表示および所有権表示を含んでいなければなりません。お客様がリバースエンジニアリング、逆コンパイル、逆アセンブルを行ったり、本契約の規定に違反する方法でソースコードを取得しようとした場合、それによって得られたいかなる情報も、それが発生した瞬間からすべて、本契約の違反に関連する供給者の権利にかかわらず、自動的にかつ取り消しできない形で供給者に譲渡され、供給者の所有であるとみなされます。

8.**権利の留保**。本ソフトウェアに対する権利は、本契約において本ソフトウェアのエンドユーザーとしてお客様に明示的に与えられた権利を除き、すべて供給者自身が留保します。

9.**複数言語対応バージョン、デュアルメディアソフトウェア、複数コピー**。本ソフトウェアが複数のプラットフォームまたは言語をサポートしているか、お客様が本ソフトウェアのコピーを複数入手した場合、お客様はライセンスを取得したバージョンのコンピューターシステム数でのみ本ソフトウェアを使用できます。使用していない本ソフトウェアのバージョンやコピーを、他者に売却、賃貸、賃借、サブライセンス付与、貸与、または譲渡することはできません。

10.**本契約の開始と解除。**本契約は、お客様が本契約に同意した日から有効となります。本契約は、お客様が本契約に同意した日から有効となります。お客様は、供給者またはそのビジネスパートナーから入手した本ソフトウェア、すべてのバックアップコピー、および関連するすべての資料を、永久的に削除、破棄、または自費で返却することにより、本契約を解除することができます。本ソフトウェアおよび本ソフトウェアの機能を使用するお客様の権利にはEOLポリシーが適用される場合があります。本ソフトウェアまたは本ソフトウェアの機能がEOLポリシーで定義されているサービス終了日に達した後は、本ソフトウェアを使用するお客様の権利が失効します。本契約の終了の態様に関係なく、第7条、第8条、第11条、第13条、第19条、および第21条の規定は、無期限に有効であり続けるものとします。

11.**エンドユーザーの表明**。お客様はエンドユーザーとして、明示または暗黙のいかなる種類の保証も伴わず、該当の法律によって許可される範囲において、本ソフトウェアが「現状有姿」のまま提供されていることを認めるものとします。供給者、そのライセンス供給者、関係者、および著作権保有者のいずれも、本ソフトウェアの特定の目的に対する商品性または適合性、および第三者の特許、著作権、商標、またはその他の権利に対する侵害の不存在について、明示または黙示を問わず、一切の表明または保証を行いません。供給者もその他の関係者も、本ソフトウェアに含まれている機能がお客様の要求に沿うこと、または本ソフトウェアが円滑で問題なく動作するということの保証を行いません。お客様は、意図する結果に到達するための本ソフトウェアの選択、および本ソフトウェアのインストール、使用、および本ソフトウェアで達成される結果について、完全に責任とリスクを負います。

12.**さらなる義務の否定**。本契約で具体的に列挙される義務以外に、本契約が供給者およびそのライセンサーに対して課す義務はありません。

13.**責任の制限**。準拠法によって許可される最大限の範囲において、いかなる場合も、供給者、その被雇用者、ライセンス供給者は、どのような態様で発生したものであろうと、契約、違法行為、怠慢、または責任の発生を定めるその他の事実のいずれに起因するものであるかを問わず、本ソフトウェアのインストール、本ソフトウェアの使用、または本ソフトウェアが使用できないことにより発生した、利益、収益、または売上の損失、データの喪失、補用品またはサービスの購入にかかった費用、物的損害、人的損害、事業の中断、企業情報の喪失、特別損害、直接損害、間接損害、偶発的損害、経済的損害、補

填損害、懲罰的損害、特別または派生的損害に対し、一切責任を負わないものとします。これは、たとえ供給者、そのライセンス供給者、または関係者がそのような損害の可能性について通知を受けていた場合であっても同様です。一部の国および法律では、免責を認めず、しかし限定された範囲の責任を負うことは許可しています。その場合、供給者、その被雇用者、ライセンス供給者、または関係者の責任は、お客様がライセンスの対価として支払った金額を限度とします。

14. 本契約に含まれるものは何も、それに反する場合であっても、消費者として取引するすべての当事者の法的権利を損なうものではありません。

15.**テクニカルサポート**。テクニカルサポートは、ESETまたはESETの依頼を受けた第三者の独自の判断により提供され、いかなる種類の保証も表明も伴わないものとします。本ソフトウェアまたは本ソフトウェアの機能がEOLポリシーで定義されているサービス終了日に達した後は、テクニカルサポートが提供されません。エンドユーザーは、テクニカルサポートの提供の前に、存在するすべてのデータ、ソフトウェア、プログラム機能をバックアップする必要があります。ESETおよび / またはESETの依頼を受けた第三者は、テクニカルサポートの提供によりお客様に生じたデータ、資産、ソフトウェアまたはハードウェアの損害または損失、もしくは利益の喪失について、いかなる責任も負いません。ESETおよび / またはESETの依頼を受けた第三者は、問題をテクニカルサポートで解決できないと判断する権利があります。ESETは、独自の判断により、テクニカルサポートの提供を拒否、中断、終了する権利があります。ライセンス情報、情報、およびプライバシーポリシーに準拠した他のデータは、技術サポートを提供するために必要になる場合があります。

16.**ライセンスの譲渡**。本契約の条件に違反しないかぎり、あるコンピューターにインストールされていた本ソフトウェアを別のコンピューターシステムにインストールすることができます。エンドユーザーは、本契約の条件に違反しない場合のみ、供給者の同意の元、本契約から派生するライセンスおよびすべての権利を、別のエンドユーザーに永久に譲渡する権利があります。その場合、(i) 元のエンドユーザーは、ソフトウェアのコピーを保持しておらず、(ii) 元のエンドユーザーから新しいエンドユーザーへ直接権利が譲渡され、(iii) 新しいエンドユーザーが元のエンドユーザーに課せられた本契約に基づくすべての権利および義務を負い、(iv) 元のエンドユーザーが新しいエンドユーザーに、第17条で規定するソフトウェアが正規のものであることを証明するドキュメントを提供するものとします。

17.**正規ソフトウェアの証明。**エンドユーザーのソフトウェアの使用資格は、次のいずれかの方法で証明できます。(i)供給者または供給者が指定した第三者が発行するライセンス証明書、(ii)締結されている場合、書面によるライセンス契約、(iii) アップデートを有効にするライセンスの詳細（ユーザ名およびパスワード）が記載された供給者に送信された電子メールの提出。ライセンス情報およびプライバシーポリシーに準拠したエンドユーザー識別データは、ソフトウェアの純正を検証するために必要になる場合があります。

18.**公共団体および米国政府に対するライセンス**。米国政府を含む公共団体に対する本ソフトウェアのライセンスは、本契約に明記しているライセンス権利および制限に基づいて提供されます。

19.**輸出管理規制**

a)お客様は、直接的または間接的に、ESETまたはESETの持ち株会社、ESETの子会社、持ち株会社の子会社、持ち株会社が管理する事業体による次のような輸出貿易管理法の違反または輸出貿易管理法の下で否定的な結果につながる一切の個人に対して本ソフトウェアを輸出、再輸出、移転、または提供せず、そのような方法でソフトウェアを使用せず、そのような行為に関与したりしないものとします。

i. 米国、シンガポール、英国、欧州連合またはその加盟国、本契約の義務が履行される国、あるいはESETまたはその関連会社が登録または事業を行う国の政府、州、規制当局が発行または採用した、商品、ソフトウェア、技術、サービスの輸出、再輸出、または移転を統制、制限、またはライセンス要件を課すすべての法律。

ii. 米国、シンガポール、英国、欧州連合またはその加盟国、本契約の義務が履行される国、あるいはESETまたはその関連会社が登録または事業を行う国の政府、州、規制当局が課した経済、金融、貿易、制裁、制限、禁止、輸出入禁止、資金または資産の移転の禁止、サービス提供の禁止、あるいは同等の

対策。

（上記第i項および第ii項で参照される法律、ならびに「貿易管理法」）。

b) ESETは、次の場合において、本契約の義務を即時停止または解除する権利を有するものとします。

i.ESETが、合理的な意見において、ユーザーが本契約の第19 a)条の条項に違反したか違反する可能性が高いと判断した

ii. エンドユーザーまたは本ソフトウェアに輸出貿易管理法が適用され、その結果として□ESETが、合理的な意見において、本契約の義務の継続的な履行によって□ESETまたはその関連会社が輸出貿易管理法に違反するか、輸出貿易管理法の下で否定的な影響を受ける可能性があると判断した

c) いずれの当事者も、適用される輸出貿易管理法に準拠しないか、輸出貿易管理法の下で罰則を受けるか、禁止される行為または不作為（あるいは行為または不作為に同意すること）を勧誘または義務付けられるように、本契約のいずれの条項も意図せず、何もそのように解釈または理解されない

20.**通知**。すべての通知、ならびに本ソフトウェアおよびドキュメントの返却は、本契約の第22条に従い、本契約、プライバシーポリシ□□EOLポリシー、ドキュメントの変更をお客様に通知するESETの権利を損なうことなく□ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic宛てに送付する必要があります□ESETは、電子メールや、本ソフトウェア経由でのアプリ内通知を送信したり□Webサイトにコミュニケーションを投稿したりする場合があります。お客様は、規約、特別な規約、プライバシーポリシーの変更、契約の提案/承諾、またはキャンペーンへの招待、通知または他の法的な通知に関するコミュニケーションを含め、電子的な形式でESETから法的な通知を受信することに同意します。適用される法律で特に別のコミュニケーションの形態が義務付けられている場合を除き、かかる電子的なコミュニケーションは書面を受け取った場合と同義に見なされるものとします。

21.**準拠法**。本契約は、スロバキア共和国の法律に準拠し、これに従って解釈されるものとします。エンドユーザーおよび供給者は、準拠法および国際物品売買契約に関する国際連合条約の矛盾する規定については、適用されないことに同意するものとします。お客様は、本契約に関するいかなるクレームもしくは供給者との紛争、または本ソフトウェアをお客様が使用することによるいかなる紛争またはクレームも、ブラチスラバ第1地方裁判所で解決し、さらに、ブラチスラバ第1地方裁判所での管轄権の行使に同意し、明示的にこれを承諾するものとします。

22.**一般条項**。本契約の条項のいずれかが無効または履行不能である場合、これが本契約のその他の条項の有効性に影響を及ぼすことはないものとします。これらその他の条項は、本契約に定める条件に基づき、引き続き有効かつ履行可能であるものとします。本契約は英語で締結されました。便宜上またはその他の目的で、本契約書の翻訳が用意されている場合、または本契約の翻訳版の間で不一致がある場合には、英語版が優先されるものとします。

ESETは、(i) 本ソフトウェアまたはESETの事業の方法に関する変更を反映する□(ii) 法律、規制、セキュリティの理由から□(iii) 悪用または被害を防止するため、関連するドキュメントを更新することで、いつでも、本ソフトウェアを変更し、本契約、付録、補遺、プライバシーポリシ□□EOLポリシー、ドキュメントまたはその一部を改訂する権利を留保します。これらの条項の改訂は、電子メール、アプリ内通知、または他の電子的な手段で通知されます。お客様が本契約の変更の提案に同意しない場合は、変更の通知を受領してから30日以内にアカウントまたは影響を受ける購入済みのサービスを解約できます。この期限内に本契約を解約しない場合は、提案された変更が承認されたと見なされ、変更の通知を受け取った日時点でお客様側で変更が有効になります。

本契約は、本ソフトウェアに関するお客様および供給者間の合意事項をすべて網羅しており、本ソフトウェアに関する従前のいかなる表明、議論、約束、情報交換、または広告にも取って代わります。

EULAID: EULA-PRODUCT-LG; 3537.0

プライバシーポリシー

データ管理者としてのESET, spol. s r. o. (登録事業所所在地: Einsteinova 24, 851 01 Bratislava, Slovak Republic 商業登記: ブラチスラバ第1地方裁判所、有限会社部門、登録番号3586/B 事業登記番号:ブラチスラバ第1地方裁判所、有限会社部門、登録番号3586/B 事業登記番号:31333532) (ESET または「当社」)は、お客様の個人データとプライバシーの処理に関して透明でありたいと考えています。この目標を達成するために、当社は、お客様(「エンドユーザー」または「お客様」)に次の事項を通知する目的でのみ、本プライバシーポリシーを発行しています。

- 個人データの処理、
- データの機密保持、
- データの主体の権利。

個人データの処理

製品に実装されたESETが提供するサービスは、エンドユーザーライセンス契約(EULA)の条項に従って提供されますが、項目によっては特定の注意が必要になる場合があります ESETは、サービスの提供に関連するデータ収集の詳細について、お客様に説明します ESETは、アップデート/アップグレードサービス ESET LiveGrid® データの悪用に対する保護、サポートなど、エンドユーザーライセンス契約および製品資料に記載されているさまざまなサービスを提供します。すべてを機能させるために ESETは次の情報を収集する必要があります。

- 製品がインストールされているプラットフォームを含むインストール処理とコンピューターに関する情報、およびオペレーティングシステム、ハードウェア情報、インストールID ライセンスID IPアドレス MACアドレス、製品の構成設定といった製品の動作と機能に関する情報を含むアップデートおよび統計情報。
- ESET LiveGrid®レピュテーションシステムの一部として侵入に関連する単方向ハッシュ。これは、検査済みファイルをクラウドのホワイトリストおよびブラックリスト項目のデータベースと比較し、ESETマルウェア対策ソリューションの効率化を図ります。
- ESET LiveGrid®フィードバックシステムの一部として世界から収集した不審なサンプルおよびメタデータ。これにより ESETは、エンドユーザーのニーズに迅速に対応し、最新の脅威に反応し続けることができます ESETはお客様がESETに送信する次の情報を必要としています
  - oウイルスおよび他の悪意のあるプログラム、ならびにお客様によって迷惑メールとして報告されたか、製品によって警告された実行ファイル、電子メールメッセージなどの不審であるか、問題があるか、望ましくない可能性があるか、危険の可能性があるオブジェクトの潜在的なサンプルといった侵入情報
  - oデバイスの種類、ベンダー、モデル、名前などのローカルネットワークのデバイスに関する情報
  - oIPアドレスおよび地理情報 IPパケット URLおよびイーサネットフレームなどのインターネットの使用に関する情報
  - o含まれるクラッシュダンプファイルと情報

当社は、この範囲外でデータを収集する意志はありませんが、場合によってはそれが防止できないことがあります。誤って収集されたデータは、マルウェア自体に含まれる場合があります。当社は、本プライバシーポリシーで規定された目的において、そのようなデータを当社のシステムまたはプロセスに取り込む意図はありません。

- ライセンスIDなどのライセンス情報、および名前、姓、住所、電子メールアドレスなどの個人データは、課金、ライセンスの真正の検証、サービスの提供のために必要です。

• サポート要求に含まれる連絡先情報およびデータは、サポートのサービスで必要になる場合があります。選択した連絡方法に基づき、当社は、電子メールアドレス、電話番号、ライセンス情報、製品詳細、およびサポートケースの説明を収集する場合があります。サポートのサービスを進めるために、他の情報の提供を求められる場合があります。

データの機密保持

ESETは、販売、サービス、サポートネットワークの一部として、関連会社またはパートナー経由で、世界中で事業を展開している会社です。ESETによって処理された情報は、サービスの提供、サポート、または請求などのEULAの履行のため、関連会社またはパートナー企業との間で転送される場合があります。選択した位置情報およびサービスに基づき、欧州委員会の適切な決定権がない国にお客様のデータを転送する必要がある場合があります。この場合でも、情報を転送するたびに、データ保護法の規制が適用され、必要な場合にのみ実行されます。標準契約条項、拘束的企業準則、または他の適切な安全保護対策を例外なく確立する必要があります。

ESETは、エンドユーザーライセンス契約に従って、サービスを提供している間、必要最低限の期間にのみデータが保存されるように最善の努力を講じます。ESETの保持期間は、お客様が簡単かつスムーズな更新が行える時間的余裕を用意するために、ライセンスの有効期間よりも少し長くなる場合があります。ESET LiveGrid®からの最小化および仮名化された統計情報および他のデータが統計目的で処理される場合があります。

ESETは、適切な技術的および組織的な対策を導入し、潜在的なリスクに適したレベルのセキュリティを保証します。当社は最善を尽くし、処理システムおよびサービスに関する、継続中の機密性、完全性、可用性、および障害回復力を保証します。ただし、お客様の権利と自由を脅かす結果になるデータ違反の場合には、すぐに監督当局とデータ主体に通知します。データ主体として、お客様は、監督当局に苦情を申し立てる権利を有します。

データの主体の権利

ESETはスロバキア法の規制に準拠し、欧州連合の一部としてデータ保護法によって拘束されます。適用されるデータ保護法で規定された条件が適用されます。お客様は、データ主体として、次の権利を有しています。

- ESETに対してお客様の個人データへのアクセスを要求する権利、
- 不正確な個人データを修正する権利(不完全な個人データを完全にする権利もあります)
- 個人データの消去を要求する権利、
- 個人データの処理の制限を要求する権利
- 処理に異議を申し立てる権利
- 苦情を申し立てる権利および
- データ移植性の権利。

データ主体として権利を行使する場合、またはご質問や懸念をお持ちの場合は、以下の宛先までご連絡ください。

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk