

ESET Mobile Security

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。](#)

Copyright ©2024 by ESET, spol. s r.o.

ESET Mobile Security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問わず、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: 2024年/4月/25日

1 はじめに	1
1.1 新機能	1
1.2 最低システム要件	2
2 インストール	2
3 起動ウィザード	3
4 無料サブスクリプション機能とプレミアムサブスクリプション機能	5
5 アクティベーション	6
6 アンインストール	7
7 ESET HOMEに接続する	8
8 ウイルス対策	9
8.1 検査ログ	12
8.2 詳細設定	12
8.3 Adware Detector	14
9 セキュリティレポート	14
10 アクティビティログ	16
11 Anti-Theft	16
11.1 Anti-Theft設定	18
11.2 最適化	19
11.3 Webポータル	20
11.4 ESET HOME パスワード	20
12 フィッシング対策	21
12.1 SMSおよび通知保護	23
13 アプリのロック	24
13.1 アプリのロックのPINコードを忘れた場合	25
14 決済保護	25
15 通話フィルター	26
15.1 新規ルールの追加	28
16 ネットワーク検査	29
17 セキュリティ監査	30
17.1 デバイス監査	30
17.2 アプリケーション監査	31
18 設定	31
19 カスタマーサポート	32
20 エンドユーザーライセンス契約	33
21 プライバシーポリシー	40

はじめに

ESET Mobile Securityは包括的なセキュリティソリューションで、出現する脅威とフィッシングページからデバイスを保護し、紛失や盗難の場合にリモートでデバイスを制御できます。

主要な機能

- [ウイルス対策](#)
- [Anti-Theft](#)
- [フィッシング対策](#)
- [ESET HOMEポータルとの統合](#)
- [通話フィルター](#)
- [セキュリティ監査](#)
- [セキュリティレポート](#)
- [ネットワーク検査\(Android 12以前のみ\)](#)
- [アプリのロック](#)
- [決済保護](#)

新機能の紹介

ESET Mobile Securityバージョン9の新機能:

追加

- Android 14サポート
- サブスクリプションの提供
- [スミッシング対策\(SMS保護と通知保護\)](#)
- [通話フィルターでのワイルドカードの使用](#)

改良

- 新しい起動ウィザード
- 新しいホーム画面設計
- 新しいメインメニュー設計

最低システム要件

ESET Mobile Security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 6 (Marshmallow) 以降
- タッチスクリーン解像度: 最低240x320 px
- CPU: 500 MHz以上 ARM7以上
- RAM: 512 MB以上
- インターネット接続

サポート除外

- ルート化されたデバイスはサポートされません。Anti-Theftと通話フィルター機能は、通話や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。デュアルSIMデバイスを使用している場合、SIMガードは両方のSIMカードで正しく機能しない可能性があります。
- ! - AndroidGoはサポートされていません。
- ESET Mobile Securityは、Google Playサービスが正常に動作するために必要です。ESET Mobile Securityは、一部のHuaweiデバイスなどのGoogle Playサービスがないデバイスではサポートされません。
- Anti-Theftの信頼できるSIMカード機能は、CDMAデバイスでは使用できません。
- 一部の機能はOSバージョンによって異なります。

インストール

ESET Mobile SecurityはESET Webサイトからダウンロードできます。



あるいは、リンクに従うか、モバイルデバイスと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ます。



[「段階的なインストールガイド」](#)をご覧ください(この記事はすべての言語で提供されています)。

ESET Webサイトからダウンロードされた.APKファイルを使用してデバイスにESET Mobile Securityをインストールするには、不明な発行元を有効にする必要があります。手順については、[ナレッジベース記事](#)を参照してください(一部の言語では、この記事は提供されていません)。


ESET Mobile Security .APKファイルをダウンロードした後、ダウンロードしたファイルをタップし、インストールを選択しますESET Mobile Securityアプリケーションがインストールされ、[スタートアップウィザード](#)が起動します。

個人情報とAndroidデバイスのリソースを保護するにはESET Mobile Securityはデバイスの機能にアクセスし、場合によってはそれらを制御する必要があります。各権限タイプと使用方法の詳細については、[このナレッジベース記事](#)の表を参照してください(この記事が提供されていない言語もあります)。

起動ウィザード


インストール後、スタートアップウィザードの画面のプロンプトに従います。

ESET Mobile Securityの権限を有効にする

-  このガイドは、Androidの標準設定に基づいています。権限の有効化プロセスは、デバイスの製造元によって異なる場合があります。

1. **すべてに同意して続行**をタップすると、[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](#)を確認します。

2. 環境設定をカスタマイズするには、**カスタマイズ**をタップし、次のオプションのうち適用可能なものを選択して、**続行**をタップします。

- **ESET LiveGrid®を許可** — ESET LiveGrid® フィードバックシステムの詳細については、[詳細設定セクションを参照してください](#)

- **アナリティクスによる製品改善を許可**—ESET Mobile Securityでは、匿名のアプリケーション情報(パフォーマンス、動作統計情報)を送信し、アプリケーションとサービスを改善できます。収集する情報の詳細については、[プライバシーポリシーの章](#)を参照してください。

- **マーケティング目的でのデータ使用を許可**

3. お住まいの国が自動的に検出されなかった場合は、国を選択して**続行**をタップします。

4. 1つのモバイルデバイス用のサブスクリプションを購入するか、別のシステム用のマルチデバイスサブスクリプションを選択するプランを選択します。サブスクリプションをお持ちの場合は、**既にサブスクリプションをお持ちの場合**を選択し、以下の手順6に従います。

5. [ESET HOMEアカウント](#)から電子メールアドレス宛てに送信されたダウンロードリンクを使用してESET Mobile Securityをインストールした場合は、アクティベーション詳細を確認します。**続行**をタップし、[ESET HOMEアカウントでESET Mobile Securityをアクティベーションするための手順に従います](#)。同意しない場合は、**拒否**をタップし、以下の手順に従います。

6. ESET HOMEアカウントにログインし、モバイルデバイスをアカウントに接続してESET Mobile Securityをアクティベーションします。

 [Googleで続行](#)

- a.Googleアカウントを選択します。
- b.Googleアカウントで既存のESET HOMEアカウントに初めて接続する場合は、ESET HOMEパスワードを入力する必要があります。パスワードの**確認**をタップします。

✓ Appleで続行

- a.Apple IDとパスワードを入力します。
- b.**ログイン**をタップします。
- c.Appleデバイスに送信されたコードを入力します。
- d.**続行**をタップします。
- e.Webブラウザを信頼する場合は、**信頼**をクリックします。
- f.**続行**をタップし、Apple IDでESET HOMEにアクセスします。
- g.左上の**X**アイコンをタップしてESET Mobile Securityに戻ります。

✓ 電子メール

ESET HOMEへのログイン

- a.電子メールアドレスとパスワードを入力します。
 - b.**ログイン**をタップします。
- ESET HOMEアカウントにログインした後は、デバイスのニックネームを作成する必要があります。これによりESET HOMEアカウントでこのデバイスを特定できます。ニックネームを入力し、**次へ**をタップします。

ESET HOMEアカウントを作成します

- a.電子メールアドレスとパスワードを入力します。




パスワード要件

パスワードは10文字以上で、1つ以上の大文字と1つの数字を使用する必要があります。

- b.**アカウントの作成**をタップすると、電子メールで確認リンクを受信します。
- c.デバイスのニックネームを作成し、**次へ**をタップします。
- d.ESET Mobile Securityが正しく動作するには、**続行**をタップして、すべてのファイルアクセス権を許可します。
- e.**初回検査の開始**をタップします。
- f.登録を完了するには、確認電子メールでリンクをタップします。

✓ QRコードのスキャン

このオプションではESET HOMEアプリがインストールされた別のデバイスが必要です。

- a.別のデバイスでESET HOMEアプリを開きます。
- b.メニューボタン  > **QRコードをスキャン**をタップします。
- c.**QRコードのスキャン**をタップしますESET HOMEでの写真の撮影と動画の記録を許可するように指示される場合があります。アプリの使用**中または今回のみをタップします**。
- d.カメラを使用してQRコードをスキャンします。
- e.**デバイスの接続**をタップします。
- f.ESET Mobile Securityで**完了**をタップします。

7. スタートアップウィザードの最後の手順は、デバイスのAndroidバージョンによって異なります。

✓ Android 6-10

- a.デバイス検査を有効化するにはESET Mobile Securityで複数の権限が必要です。**アクセスの許可**画面で、ESET Mobile Securityの権限を確認し、**続行**をタップします。
- b.**許可**をタップしてESET Mobile Securityに権限を付与します。**スキップ**をタップすると、これらのアクセス権が許可されるまでESET Mobile Securityはデバイスの脅威を検査できず、セキュリティリスク通知が表示されます。

✓ Android 11以降

- a. **続行**をタップします。
- b. ESET Mobile Security **選択**
- c. ESET Mobile Securityの横のトグルをオンにします。
- d. スタートアップウィザードは完了しました。**初回検査の開始**をタップします。

バッテリー保護



多くのデバイスメーカーは、Android 6以降のデバイスでバッテリー保護またはバッテリー節約オプションを導入しました。この機能をオンにするとESET Mobile Securityのフィッシング対策機能がオフになります。この機能が搭載されているデバイスでは、例外を作成し、バッテリー節約機能がオンの間でも、ESET Mobile Securityフィッシング対策機能の動作を許可する必要があります。例外を作成するには、デバイスメーカーのマニュアルをご確認ください。


無料サブスクリプション機能とプレミアムサブスクリプション機能

ESET Mobile Securityには3つのバージョンがあります。

- **無料** - 有効期限がなく、基本機能を無料で使用できます
- **体験版** - 一定期間(既定は30日)プレミアム機能が有効です。無料体験版は、ESET Mobile Securityを初めてインストールするときにGoogle Playアカウントごとに自動的にアクティベーションされます。
- **プレミアム** - サブスクリプションの有効期間の間プレミアム機能が有効です

次の表は、無料、試用、および製品版で使用可能な機能を示します。

	無料	試用およびプレミアム
ウイルス対策	✓	✓
ウイルス対策 - 自動検査		✓
検出エンジンの自動アップデート		✓
アプリのロック		✓
Anti-Theft - SMSコマンド		✓
アンチセフト - Webポータル		✓
アンチセフト - SIMガード		✓
ネットワーク検査(Android 12以前)		✓
フィッシング対策		✓
通話フィルター		✓
決済保護		✓
セキュリティ監査		✓
セキュリティレポート	✓	✓

Androidデバイスで直接ESET Mobile SecurityをアクティベートするにはESET Mobile Securityメイン画面の[メニュー]  をタップ(またはデバイスの[メニュー]ボタンを押下)して、[サブスクリプション]をタップします。


ESET Mobile Securityをアクティベートする方法は複数あります。

- **プレミアムにアップグレード**-サブスクリプションをまだお持ちでなく、購入する予定の場合は、このオプションを選択してください。
- **製品認証キーの入力**-製品認証キーをすでにお持ちの場合は、このオプションを選択します。製品認証キーは次の形式の一意の文字列です (形式: XXXX-XXXX-XXXX-XXXX-XXXX))これは、サブスクリプション所有者の特定で使用されますESETから受信した電子メールに記載されているか、箱に同梱されているサブスクリプションカードに記載されています。

アクティベーション

ESET Mobile Securityでプレミアム機能のロックを解除するには、製品認証キーを使用してESET Mobile Securityをアクティベーションする必要があります。

サブスクリプションがない場合


1. メニューボタンをタップして、メインメニューを開きます。
2. サブスクリプションオプションをタップし、**プレミアムにアップグレード**を選択します。
3. ESET Webサイトにリダイレクトされます。
4. ESETオンラインストアでニーズに適したサブスクリプションを購入します。
5. ESETサブスクリプションの購入中に指定した電子メールアドレスに製品認証キーが送信されます。サブスクリプションを受け取ったら、以下のセクションに進んでください。

既にサブスクリプションがある場合

デバイスをESET HOMEに接続し、ESET HOMEに関連付けられたサブスクリプションでESET Mobile Securityをアクティベーションします。

デバイスをESET HOMEに接続してESET Mobile Securityをアクティベーションするには、[ESET HOMEへの接続](#)のトピックを参照してください。

ESET HOMEを使用せずにESET Mobile Securityをアクティベーションする


1. メニューボタンをタップして、メインメニューを開きます。
2. サブスクリプションオプションをタップします。
3. **製品認証キーを使用する**をタップします。
4. 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。
5. サブスクリプションの確認が完了すると、**アクティベーションに成功しました**と表示されます。**[終了]**をタップしてウィンドウを閉じます。

アンインストール

ESET Mobile SecurityをアンインストールするにはESET Mobile Securityのメインメニューのアンインストールウィザードを使用します。

備考

- i** ESET Mobile Security製品をアンインストールすると、サブスクリプションから1シート解放されます。


1. メニュー  をタップします
2. 設定をタップします。
3. [アンインストール]をタップします。
4. Anti-Theftが有効な場合は、ESET Mobile SecurityセキュリティPIN/パターンまたは指紋を入力します。
5. [アンインストール]をタップします。

あるいは、次の手順に従い、製品を手動でアンインストールします。


Android 7以降:

1. [設定]に戻り、[アプリの管理] > **ESET Mobile Security** > [アンインストール]をタップします。Anti-Theftが有効になっている場合は、アンインストールする前に、ESET Mobile Securityのデバイス管理者を無効にするように指示される場合があります。

または

1. ESET Mobile Securityでメインメニューボタン  をタップして、メインメニューを開きます。
2. [設定]を選択します。
3. [アンインストール]をタップします。
4. [アンインストール]を再度タップして、アンインストールを確定します。

Android 6:

1. Androidホーム画面のランチャーアイコン  をタップ(または[ホーム] > [メニュー]に移動)して、[設定] > [セキュリティ] > [デバイス管理者]をタップします。**ESET Mobile Security**を選択して、[無効にする]をクリックします。**ロック解除**をタップし、セキュリティPIN/パターンを入力します。アプリケーションがデバイス管理者として定義されていない場合は、この手順を省略できます。
2. [設定]に戻り、[アプリの管理] > **ESET Mobile Security** > [アンインストール]をタップします。

ESET HOMEに接続する


この機能を使用するにはESET Mobile Securityバージョン6.3以降にアップグレードします。

ESET HOME経由でESET Mobile Securityをアクティベーション



ESET HOMEを使用して1台のデバイスを2回目にアクティベーションする場合(ESET Mobile Securityの再インストールの後など)はESET HOMEでサブスクリプションからデバイスを手動で削除してから、続行する必要があります。削除しない場合ESET HOME経由でこのデバイスをアクティベーションできません。

デバイスを既存のESET HOMEアカウントに接続

1. メニューボタンをタップします。
2. ESET HOMEをタップします。

✓ [Googleで続行](#)

- a.Googleアカウントを選択します。
- b.Googleアカウントで既存のESET HOMEアカウントに初めて接続する場合は、ESET HOMEパスワードを入力する必要があります。パスワードの**確認**をタップします。

✓ [電子メールアドレスで続行](#)

ESET HOMEへのログイン

- a.電子メールアドレスとパスワードを入力します。
 - b.ログインをタップします。
- ESET HOMEアカウントにログインした後は、デバイスのニックネームを作成する必要があります。これによりESET HOMEアカウントでこのデバイスを特定できます。ニックネームを入力し、**次へ**をタップします。

ESET HOMEアカウントを作成します

- a.電子メールアドレスとパスワードを入力します。



パスワード要件

パスワードは10文字以上で、1つ以上の大文字と1つの数字を使用する必要があります。

- b.アカウントの作成をタップすると、電子メールで確認リンクを受信します。
- c.デバイスのニックネームを作成し、**次へ**をタップします。
- d.ESET Mobile Securityが正しく動作するには、**続行**をタップして、すべてのファイルアクセス権を許可します。
- e.初回検査の開始をタップします。
- f.登録を完了するには、確認電子メールでリンクをタップします。


✓ [Appleで続行](#)

- a.Apple IDとパスワードを入力します。
- b.ログインをタップします。
- c.Appleデバイスに送信されたコードを入力します。
- d.続行をタップします。
- e.Webブラウザを信頼する場合は、**信頼**をクリックします。
- f.続行をタップし、Apple IDでESET HOMEにアクセスします。
- g.左上のXアイコンをタップしてESET Mobile Securityに戻ります。

✓ [QRコードのスキャン](#)

このオプションではESET HOMEアプリがインストールされた別のデバイスが必要です。

a.別のデバイスでESET HOMEアプリを開きます。

b.メニューボタン > QRコードをスキャンをタップします。

c.QRコードのスキャンをタップしますESET HOMEでの写真の撮影と動画の記録を許可するように指示される場合があります。アプリの使用**中または今回のみをタップします**

d.カメラを使用してQRコードをスキャンします。

e.デバイスの**接続**をタップします。

f.ESET Mobile Securityで**完了**をタップします。

3. このデバイスで初めてESET HOMEアカウントにログインする場合は、デバイスのニックネームを作成し、ESET HOMEでデバイスを特定できるようにします。**次へ**をタップします。

4. 無料体験版を使用し、ESET HOMEに使用可能なサブスクリプションがある場合は、ESET Mobile Securityをアクティベーションするように指示されます。

a.該当するサブスクリプションを選択します。

b.[**アクティベーション**]をタップする。

5. **終了**をタップします。

ESET HOMEからデバイスを切断する

1. メニューボタン をタップします。

2. **ESET HOMEアカウント**をタップします。

3. **デバイスの切断**をタップします。デバイスがESET HOMEに接続されていない場合にはこのオプションを使用できません。

4. 指紋認証を行うか**PIN**を入力します。

5. **切断**をタップします。

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。



さまざまなレベルの検査で、脅威を検出し、排除します。

🔍 デバイスを検査

自動検査



充電中に検査
有効



スケジュール検査
無効




アップデート





検出エンジンのアップデート
バージョン: 27121 (最新)

リアルタイムファイルシステム保護



リアルタイムファイルシステム保護は、ファイルを開いたり、作成したり、実行したりしたときに、ダウンロードフォルダーのすべてのファイルを悪意のあるコードから保護します。

既定では、リアルタイムファイルシステム保護はシステムのスタートアップ中に起動し、検査を中断なく実行します。ウイルス対策セクションの[リアルタイムファイルシステム保護を有効にする]は有効にしておくことをお勧めします。リアルタイムファイルシステム保護設定に移動する場合は、ウイルス対策セクションで3点メニューをタップし、**詳細設定>リアルタイムファイルシステム保護**を選択します。

デバイスを検査

ウイルス対策セクションの**デバイスの検査**ボタンをタップすると、いつでもオンデマンド検査を実行できます。既定の検査レベルはスマート検査に設定されています。検査レベルは、ウイルス対策の**詳細設定**で変更できます。3点メニュー>**詳細設定>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)ISO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SDカードの内容を検査します。
- **詳細** – 詳細検査では、ファイル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。

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、**キャンセル**をタップします。検査中には、**ウイルス対策**設定パネルに、検査結果と統計情報が表示されます。



メモリカード検査

ESET Mobile SecurityはAndroid 6以降のデバイスでのメモリカード検査をサポートしません。

処理されていない脅威

ESET Mobile Securityが脅威を検出した後、脅威への対応を選択するまで、このオプションを使用できます。選択できる対応は、脅威を駆除するか、無視するかのみです。

脅威を無視

脅威を無視する選択をすると**脅威を無視**オプションが表示されます。このオプションを使用すると、無視された脅威を後から削除できます。

充電中に検査

このオプション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するようにスケジュールで

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]の横のスイッチをタップし、検査を実行する日時を指定します。

検出エンジンのアップデート

既定ではESET Mobile Securityには、検出エンジンが確実に定期的に更新されるようにするためのタスクが含まれています。プレミアムユーザーの場合、これは、更新プログラムと更新プログラムの検出エンジンを自動的にチェックすることを意味します。無料ユーザーの場合、これは更新を確認し、手動で更新する必要がある古いモジュールについて通知することを意味します。このアップデートは、プレミアムユーザーと無料ユーザーの両方が独自の裁量で手動で実行できます。アップデートを手動で実行するには、**検出エンジンのアップデート**をタップします。詳細については、[ナレッジベースの記事](#)をご覧ください。

データ転送の課金



不要な帯域幅の使用を避けるため、アップデートは必要に応じて発行されます。アップデートは無料ですが、モバイルサービスプロバイダーによってはデータ転送料金が課金される場合があります。

ツールの詳細については、次のリンクを参照してください。

- [検査ログ](#)
- [詳細設定](#)



検査ログ

[検査ログ]セクションには、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に関する包括的なデータが含まれます。

各ログには次の情報が含まれます。

- 検査の日時
- 検査レベル(スマート検査と詳細検査)
- 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
- 検出された脅威数と検出された脅威の一覧

詳細設定

ESET Mobile Securityアプリケーションを開き、メニューアイコン  > ウイルス対策 > 右上隅にある3点  > 詳細設定をタップします。

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のDEXファイル(Android OS用の実行ファイル)の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SDカードの内容を検査します。
- **詳細** – 詳細検査では、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。

リアルタイムファイルシステム保護

リアルタイムスキャナーは、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。自動的に、ダウンロードフォルダーとインストールまたはアップデートされたアプリケーションを検査します。

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。

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。

リムーバブルメディア

ESET Mobile Securityは、USBフラッシュドライブ、外部ハードドライブなどのデバイスに接続されたすべてのリムーバブルメディアを検査します。


望ましくない可能性があるアプリケーションを検出

望ましくない可能性があるアプリケーションは、アドウェアを含んだり、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。場合によっては、リスクよりも望ましくない可能性があるアプリケーションを使用する利点があると考えることがあります。このため、ESETは、このカテゴリのアプリケーションには、悪意のあるソフトウェアと比較して、低いリスクを割り当てています。

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。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。[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が、悪意のある目的で悪用される可能性があります。[安全でない可能性があるアプリケーションの検出]オプションを使用すると、このようなカテゴリ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。


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**からデバイスへのアップデートを許可できます。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。最新の検出方法や修正プログラムを早い段階で利用することができるという利点があります。ただし、リリース前アップデートは常に完全に安全であるとは限りません。現在のプログラムモジュールのバージョンを確認するにはESET Mobile Securityメイン画面で3点メニューをタップして、**バージョン情報 > ESET Mobile Security**をタップします。基本ユーザーの場合は、既定で選択されている**公開サーバー**オプションをオンにしておくことをお勧めします。

Adware Detector

Adware DetectorはESETのアドウェアアプリケーション対策です。アドウェアアプリは、合法的なアプリケーションや、合法的に見せようとするアプリケーション(電卓や懐中電灯など)の可能性があります。これらのアプリは、アプリケーションが閉じていても全画面広告を表示します。このため、ユーザーは、これらの画面広告を表示するアプリケーションを検出できません。

Adware Detectorは、これらのアドウェアアプリケーションを特定するのに役立ちます。使用するには、画面広告が表示された後に次の手順を実行します。

1. ESET Mobile Securityを開きます。
2. メインESET Mobile Security画面で**ウイルス対策**をタップします。
3. 右上のをタップすると、メニューが表示されます。
4. メニューの**Adware Detector**をタップします。
5. Adware Detectorでアドウェアアプリケーションを検出するガイドが表示された後、**続行**をタップします。

Adware Detectorは過去5分間に開いたアプリケーションを表示します。不審なアプリケーションを特定し、**削除**をタップして、デバイスからそのアプリケーションを削除します。通常、不審なアプリケーションは、開くことが想定されていないアプリケーションか、現在使用していないアプリケーションです。

セキュリティレポート

セキュリティレポートには、各プログラムモジュールとそのステータスおよび統計の包括的な概要が表示されます。\\[**セキュリティレポート**]画面から現在有効ではないモジュールを有効にできます。各プログラムモジュールセクションには次の情報が含まれます。

一部の情報が存在しない場合は、発生がゼロであることを意味します。

ウイルス対策

- アプリ検査
- 見つかった脅威
- データベースアップデート

- 検出されました
- 検査されたファイル
- アップデートされたアプリ

アプリのロック

- 保護されたアプリケーション数
- アプリケーションロック解除の成功回数
- ロック解除の試みに失敗した回数

フィッシング対策

- 検査されたWebサイト
- 検査された通知
- 検出された脅威

通話フィルター

- 発信通話
- 受信した通話
- ブロックされた通話

決済保護

- 保護されたアプリケーション数
- 保護されたアプリケーションの検査数
- 見つかった問題の数
- セーフランチャーからオンラインバンキングまたは決済アプリを起動した回数

セキュリティ監査

- ローミングアラートは、ローミングネットワークに接続されていることを警告された回数を表示します。
- WIFI警告を開く

ネットワーク検査(Android 12以前のデバイスでのみ)

- ネットワーク検査
- 検出されたデバイス

- 脆弱性が見つかりました


ESET Mobile Securityでは、毎月Android通知バーに簡潔な月次レポートメッセージが表示されます。これらの通知を受信しない場合は、**月次レポート通知を表示しない**オプションをオンにします。

アクティビティログ

アクティビティログにはESET Mobile Securityアプリのメイン画面での毎日のアクティビティが表示されます。アクティビティログにはESET Mobile Securityによって検査されたWebサイトESET Mobile Securityアップデート、アプリのアップデート、インストールされたアプリESET Mobile Security検査などに関する情報が含まれています。

完全なアクティビティログ履歴を表示するには、アクティビティログの横の>アイコンをタップします。アクティビティログの詳細レポートでは、**フィルター**を使用して、ステータスまたはESET Mobile Securityの機能別にアクティビティを確認できます（例：警告、リスクAnti-Theftサブスクリプション）。発生日の昇順または降順でアクティビティをフィルタリングすることもできます。

アクティビティログ履歴を消去するには

- 1.ESET Mobile Securityを開きます。
- 2.ホーム画面を下にスワイプします。
- 3.アクティビティログの横の>アイコンをタップします。
- 4.右上の3点メニューアイコンをタップします。
- 5.[すべてクリア]をタップします。

アクティビティログ履歴から個々のレコードを削除するには、次の手順を実行します。

- 1.ESET Mobile Securityを開きます。
- 2.ホーム画面を下にスワイプします。
- 3.アクティビティログの横の>アイコンをタップします。
- 4.該当するレコードを左にスワイプします。
- 5.削除をタップします。

Anti-Theft

ESET 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、他者による操作を監視できるようにして、デバイスの位置を追跡します。また、デバイスを紛失した場合、見つけた人にメッセージを表示することができます。


ESET Anti-Theftでは次の権限が必要です。

- 侵入者の写真を撮影するためのカメラへのアクセス権。
- 機密データをリモートで削除するためのファイルの編集アクセス権。
- デバイスが見つからない場合にデバイスを追跡するための位置情報データへのアクセス権。
- デバイスが移動したときを認識するための物理アクティビティアクセス権。
- デバイスが見つからない場合や、ESET Mobile Securityが閉じていたり、使用されていなかったりするときにもデバイスを追跡するためのバックグラウンド位置情報アクセス権。この権限を付与するときに、**常に許可**を選択して、完全な保護を保証します。
- デバイスがロックされた場合にデバイスで通話を受信できるようにするための使用アクセス。
- 許可されていないESET Mobile Securityのアンインストールを防止するためのデバイス管理者アクセス権。デバイス管理者をアクティベーションした後はESET Mobile SecurityでPINを作成し、重要な設定を保護するように指示されます。
- SIMカードの取り外しを検出するためにデバイス情報を読み取ります。SIMカードが取り外されると、デバイスがロックされます。

ESET Mobile SecurityでAnti-Theft保護を設定するには、[ESET Mobile Security for AndroidでAnti-Theftを設定する」ナレッジベース記事](#)をご覧ください(ナレッジベース記事は一部の言語では提供されていません)。

デバイスの自動ロック

ESET HOMEポータルからデバイスをロックするほかに、次のアクションのいずれかが実行された場合に自動的にデバイスをロックするようにESET Mobile Securityをセットアップします。

- **SIMカードが取り外された** – 信頼できるSIMカードがデバイスから取り外された場合にデバイスをロックします。信頼できるSIMカードを取り外してチェックするには、**[信頼できるSIMカードを管理]**を選択し、取り外すSIMカードを選択して、ごみ箱アイコンをタップします。信頼できるSIMカードを追加するには、そのSIMカードを挿入します。自動ロックが有効になっている場合は、デバイスをロック解除する必要があります。ESET Mobile Securityにより、新しく追加したSIMカードを信頼するように求められます。

SIMカード取り外し時の自動ロックのサポート

- ⚠️ • SIMカード取り外し時の自動ロック機能は、CDMA、WCDMAおよびWi-Fi専用デバイスでは使用できません。

- **ロック解除が[X]回施行された後** – 有効にすると、ロック解除の試行失敗回数を設定している場合に、実際にその回数だけ失敗すると、デバイスがロックされます。この回数はAnti-Theftの設定で設定できます。誤って試行に失敗した場合は30秒以内であれば訂正でき、失敗した試行としてカウントされなくなります。訂正できる時間はAnti-Theftの**訂正猶予時間**オプションの設定で変更できます。訂正猶予時間を無効にすれば、設定した回数失敗した場合に、デバイスはただちにロックされます。

デバイスをロックした場合、デバイス所有者の連絡先情報を表示できます。デバイスのロックを解除しようとしている人物の写真を取得するために両方のカメラで写真を撮ったりすることもできます。

デバイスのロック後

デバイスがロックされた後に次の問題が発生する場合があります。

- **連絡先詳細の表示**オプションは、正しくない画面ロックコードが入力されたときに**所有者に連絡**オプションを表示します。**連絡先詳細の編集**をタップし、デバイスを紛失した際に表示する連絡先詳細を入力します。ESET HOMEの電子メールアドレスが既定で入力されます。

- **写真を撮る**オプションは、ロック解除の試行に失敗したりSIMカードが取り外されたりした場合に、背面および正面カメラの写真をデバイスギャラリーとAnti-Theftポータルに保存します。

モバイルデバイスのロックを解除する方法

ESET Anti-TheftポータルまたはESET Mobile Security for Android経由でモバイルデバイスをロックした場合またはモバイルデバイスをロックした場合は、ESET HOMEパスワードにアクセスする必要があります。

別のユーザーが管理するデバイスのロックを解除

! ESET Mobile Security for Androidが別のユーザーのESET HOMEアカウントで管理されている場合は、そのアカウントのパスワードを入力して、デバイスのロックを解除します。

モバイルデバイスのロック解除に関する視覚的な手順については、次の[ESETナレッジベース記事](#) (英語および他の複数の言語で提供されています)をお読みください。

Anti-Theft設定

試行の失敗後にロックする

ロック解除を何回試行するとデバイスがロックされるか、その回数を選択します。ロック解除の試行回数を設定するには、**Anti-Theft画面の** **設定** **試行の失敗後にロックする** を順にタップし、必要な試行失敗回数を選択します。

訂正猶予時間

[試行の失敗後にロックする]を有効にした場合、選択した試行失敗回数に達すると、デバイスがロックされます。。失敗した試行回数に達したときにデバイスをただちにロックする場合は、[訂正猶予時間]を無効にします。あるいは、選択した試行失敗回数に達してからデバイスがロックされるまでにデバイスをロック解除できるようにする場合は、その間の時間の長さを設定します。

例

i [試行の失敗後にロックする]が有効で、試行失敗回数が3に設定されているとします。
また、[訂正猶予時間]は15秒に設定されています。
誤ったロック解除パターンを3回入力した場合、15秒以内に正しいロック解除パターンを入力すれば、デバイスはESET Mobile Securityによってロックされないで済みます。

連絡先の詳細を編集

ESET Anti-Theftでデバイスを紛失したとマーキングした場合、または選択したロック解除失敗回数に達した場合、デバイスのロック画面に**連絡先詳細**が表示され、見つけた人が連絡できるようになります。

次の情報が表示される場合があります。

- 表示されるメッセージ(任意)
- お名前(任意)

- 自分以外の電話番号
- 電子メールアドレス

信頼できるSIMカードを管理

このオプションを使用すると、挿入されているSIMカードを削除したり、名前変更したりできます。信頼できる新しいSIMカードを追加するには、デバイスにSIMカードを挿入します。すると、デバイスがロックされるためセキュリティコードを使用してデバイスのロックを解除します。新しく挿入したSIMカードを信頼できるSIMカードの一覧に追加するように求められます。このSIMカードを一覧に追加しない場合にはSIMガードは無効のままになります。

ロックタイプの変更

ESET Anti-Theftのロックを解除する方法を選択します。Anti-Theftのセットアップ中に既定のオプションとして設定されるのはPINコードです。パターンロック解除のオプションに変更できます。

指紋を使用する

有効にすると、デバイスに保存されている指紋を使用してAnti-Theftオプションのロックを解除できます。

最適化

ESET Anti-Theftの最適化はデバイスのセキュリティ状態に関する測定可能な技術評価です。Anti-Theft保護では、次の問題に関してシステムが検証されます。

各セキュリティの問題に対して、**[設定の変更]**をタップし、特定の問題を解決できる画面に移動します。ESET Mobile Securityで問題を報告しない場合は、**この問題を無視**をタップします。

- **位置情報サービスがオフです** – オンにするには[Android設定] > [位置情報サービス]に移動し、[モバイルネットワークを使用]を選択します。
- **GPS衛星が使用されていません** - Android設定 > 位置情報 > モード > 高精度でこの設定にアクセスします。
- **画面ロックで保護されていません** – 画面ロックコード、パスワードPIN またはパターンでデバイスを保護するには[Android設定] > [画面のロック]; [画面ロック]に移動し、使用可能なオプションのいずれかを選択します。ほとんどのAndroidデバイスは、スワイプ、モーション、顔ロック解除、顔と音声、パターンPINまたはパスワード機能を搭載しています。誰かが間違ったコードを使用してデバイスのロックを解除しようとした場合ESET Anti-TheftはESET HOMEポータルで不審なアクティビティを通知します。
- **モバイルデータが有効ではありません** - [Android設定] > [ワイヤレスネットワーク] > [モバイルネットワーク] > [データ]でこの設定にアクセスします。
- **Google Playサービスが存在しません** – ESET Anti-TheftはGoogle Playサービスを使用して、リアルタイムでコマンドをデバイスに配信し、プッシュ通知を表示します。これらのサービスがデバイスで無効になっているか、存在しない場合ESET Anti-Theftで管理されるESET HOMEの機能は制限されます。

Webポータル

ESET Mobile Securityは新しい[ESET HOMEポータル](#)経由で完全にESET Anti-Theft保護と統合されます。ESET Anti-Theft Webポータルでは、デバイスアクティビティの監視、デバイスのロック、デバイス発見人へのカスタムメッセージの送信が可能です。また、リモートで大音量の警報を鳴らしたり、リモートでデバイスデータをワイプしたりもできます。

ESET HOMEアカウントを作成するには、[新しいアカウントの作成]をタップし、登録フォームを入力します。アカウント確認メールが届くので、リンクをクリックしてアカウントを有効化します。アカウントのアクティベーションの後、ESET HOMEポータルで、接続されたデバイスのESET Anti-Theftセキュリティ機能をリモートで管理できます。ESET HOMEアカウントがある場合は、[サインイン]をタップし、電子メールアドレスとパスワードを入力します。これらの手順が完了すると、デバイスをESET HOMEアカウントに関連付けることができます。

ESET Anti-Theft機能を使用する詳細な手順については、[Anti-Theftユーザーガイド](#)を参照するかESET HOMEポータルの右上端にあるヘルプアイコンをタップします。

ESET HOME パスワード

忘れたパスワードを変更する:

1. <https://login.eset.com/LostPassword>をご覧ください。
2. ESET HOMEでの登録で使った電子メールアドレスを入力し、**送信をクリックします**。
3. 電子メールアカウントにログインし、**アカウントパスワードリセット - ESET HOME**電子メールを開き、電子メールのリンクをクリックします。
4. 新しいパスワードを入力して確認し、**変更の確認**をクリックします。
5. デバイスに新しいパスワードを入力し、**ロック解除**をタップしてデバイスのロックを解除します。

ESET HOMEパスワードの変更:

1. [ESET HOME](#) Webサイトに移動します。
2. 電子メールアドレスと現在のパスワードを使用してサインインします。
3. 右上にある下向き矢印の横の電子メールアドレスをクリックします。
4. **[パスワードの変更]**をクリックします。
5. 現在のパスワードを入力します。
6. 新しいパスワードを入力して確認します。
7. **変更の保存**をクリックします。


フィッシング対策

フィッシングとは、ユーザーを操って本物のように見えて偽物であるWebサイトで機密情報を入力させる犯罪活動を意味します。このような種類のユーザー心理の操作はソーシャルエンジニアリングとして知られています。多くの場合、フィッシングは、銀行口座番号、決済カード番号、PIN、ユーザー名、パスワードなどの機密情報を取得する目的で使用されます。


ESET Mobile Securityのフィッシング対策は、悪意や危険があると見なされたWebサイトからユーザーを保護します。

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。有効な場合、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、攻撃の試みがあったことを知らせる警告通知が表示されます。

フィッシング対策はAndroid OS (ChromeおよびAndroidデバイスにプレインストール済みの既定のインターネットまたはブラウザ) で使用可能な最も一般的なWebブラウザおよびソーシャルネットワークアプリと統合されています。他のブラウザはフィッシング対策のための適切な統合がないため、保護対象にならない場合があります。フィッシング対策機能を完全に活用するには、サポート対象のWebブラウザを使用することをお勧めします。

 フィッシング対策がWebブラウザと正常に統合されるようにAndroid 6 (Marshmallow)以降を使用することをお勧めします。

機能の改善 – フィッシング対策機能でAndroid OSから追加の権限を付与する必要がある場合ESET Mobile Securityからの警告を表示します。許可をタップすると、システムのアクセシビリティ設定を開き、使用可能なオプションを検討して、その他のブラウザのサポートを提供し、プライベート (incognito) モードで閲覧するときに保護を有効にします。この問題が問題として報告されないようにするには、[この問題を無視 (非推奨)] をタップします。


フィッシング対策を無効化するには、フィッシング対策セクションの3点メニュー  をタップし、無効にするをタップします。

Android 13の .APKファイルからインストールされたESET Mobile Security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 Mobile Security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。
- 脅威が検出されると、機密データを保護するために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

アクセシビリティ権限を許可

手順の図については、[ナレッジベース記事](#) (英語版) をお読みください。


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 Mobile Securityは使用できま

せん。

2. ESET Mobile Security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 Mobile Security**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  > **制限された設定を許可**をタップします。

制限された設定は許可されます。[安全にアプリケーションの使用を開始](#)できます。

Samsung DeXでのフィッシング対策

 Samsung DeXステーションに接続されたデバイスでは、フィッシング対策がサポートされていません。

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
- Samsung Internet
- Mint
- Yandexブラウザ
- DuckDuckGo (ESET Mobile Securityバージョン6.1以降)
- Kiwiブラウザ
- エッジ
- AmazonデバイスのSilk
- Miブラウザ
- Xiaomi Miブラウザ

- Android TVのVewd

保護されたソーシャルネットワークアプリ

- Facebook
- Facebook Lite
- Messenger
- Messenger Lite
- Instagram
- 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ソーシャルネットワークアプリも保護されます。

SMSおよび通知保護

SMSと通知保護はスミッシングから保護します。

スミッシングは、フィッシングとSMS (ショートメッセージサービス) を組み合わせて作成されました。このためSMSフィッシングと呼ばれることもあります。ユーザーは電子メールよりもメッセージを信頼する傾向があるため、攻撃者はSMSメッセージを使用します。

SMS保護は、SMSメッセージで拡散されるスミッシングからユーザーを守ります。ただし、この脅威はすべてのメッセージングプラットフォームからも拡散されます。ここで、通知保護が実行されます。SMSまたは通知を受信する(Whatsappからのメッセージの受信後など)とESET Mobile Securityによってリンクが分析されます。分析に基づいて、次の3つの結果があります。

- 脅威は見つかりませんでした。
- 望ましくない可能性のあるコンテンツが見つかりました。メッセージまたは通知の内容が直接的なリスクにならない可能性があります。この目的は、ウイルスやトロイの木馬などの他のタイプのマルウェアほど、明確な悪意があるではありません。ただし、追加の不審なソフトウェアをインストールし、デジタルデバイスの動作デジタルを変更し、ユーザーによって承認または想定されていないアクティビティを実行する可能性があります。
- 危険なコンテンツが見つかりました。このメッセージまたは通知には、危険なリンクまたはフィッシングリンクが含まれています。内容を開かずに、メッセージまたは通知を削除することをお勧めします。

メッセージと通知を削除する

- ❗ セキュリティの理由からESET Mobile Securityはメッセージと通知を削除できません。危険なコンテンツは手動で削除する必要があります。

スミッシングの仕組み

1. 攻撃者がWebサイトへのリンクを含むメッセージを送信します。
2. 通常、このリンクはフィッシングWebサイトに誘導し、個人情報を入力するようにユーザーを騙す可能性があります。これらは、金銭を盗んだり、さらに詐欺行為を行ったりする目的などで使用され

る場合があります。リンクは、マルウェアを含む悪意のあるWebサイトや、騙してダウンロードさせようとするWebサイトに誘導する可能性があります。

スミッシングの兆候

- 外国の電話番号や標準の長さではない電話番号といった不審な電話番号。
- メッセージに不明なファイルまたはリンクが含まれている。
- 通常、スミッシングメッセージでは緊急であることが強調されています。
- 多くの場合、スミッシングメッセージは、懸賞などで当選したことを知らせています。

アプリのロック

アプリロックではPINコードまたは指紋を使用して、選択したアプリケーション(電子メール、メッセージ、カレンダーなど)へのアクセスを保護できます。アプリのロックにより、デバイスがロック解除されている場合でも、選択したアプリケーションへの不正アクセスが防止されます。


推奨設定

- ✓ 機能向上のためESET Mobile Securityのオーバーレイ(上部に表示されるアプリ)権限をオンにします。

デバイスでアプリのロックを設定するには

1. ESET Mobile Securityメイン画面で[アプリのロック]をタップします。
2. 有効にするをタップします。
3. 使用アクセス権限を許可し、**続行**をクリックします。
4. PINを入力すると、アプリケーションのロックが解除されます。
5. もう一度入力してPINを確認します。
6. ロックまたはロック解除するアプリケーションをタップします。

アプリロック設定の構成


アプリのロック設定にアクセスするには、右上の  メニューを開き、**設定**をクリックします。

- **新しいアプリのロック** - アプリのロックを有効にすると、デバイスでの新しいアプリケーションのインストール後に、新しいアプリケーションをロックするかどうかを確認されます。
- **アプリの再ロック** - アプリロックを設定すると、閉じた直後か、画面がオフになるか、1分間経過した後に、アプリケーションをロックできます。
- **ロックのタイプ** - PINコードまたはパターンを使用してアプリケーションをロックできます。
- **指紋でロックを解除** - このオプションは、認証済みの指紋がデバイスに保存されているときのみ使用できます。有効にすると、デバイスに保存されている指紋を使用して、アプリケーションをロック解除できます。その場合も引き続き、PINでもアプリケーションをロック解除できます。このために

は、ロックされたアプリケーションを開くときに、**[PINを使用]**をタップします。

• **侵入者アラート** — ロック解除の試みが連続して失敗するとESET Mobile Securityは侵入者の写真を撮影します。。この写真は、次にアプリケーションのロック解除が成功したときに表示されます。

アプリロックを無効にする

1. ESET Mobile Securityでアプリのロック機能に移動します。
2. アプリのロックPINを入力します。
3. 右上にある  メニューをタップします。
4. **無効**をタップします。



夜間モードを有効にする

[アプリのロック]画面で夜間モードをオンにすると、目に優しい画面にすることができます。右上端の[夜間モード]をタップします。

アプリのロックのPINコードを忘れた場合

アプリのロックのPINを忘れ、デバイスに指紋が保存されていない場合Anti-Theft設定に従い、ロックされたアプリケーションを解除するための2つのオプションがあります。

- ESET Mobile SecurityでAnti-Theft機能を有効にした場合

- 1.ESET Mobile Securityを開きます。
- 2.アプリのロック機能に移動します。
- 3.PINを入力します。画面中央の**PINを忘れた場合**をタップします。
- 4.Anti-Theft機能が有効な場合は、ESET HOMEパスワードを入力する必要があります。パスワードフィールドにパスワードを入力し、**入力**をタップします。
- 5.新しいPINを入力し、をタップして確認します。
- 6.同じPINを再入力して確認します。完了したらをタップします。

- Anti-Theft機能をアクティベーションしていない場合は、[ESET Mobile Security](#)をアンインストールしてから、もう一度インストールします。

決済保護



決済保護は保護の層を強化し、高度なフィッシング詐欺やその他の脅威に対してAndroidデバイスで金融データを保護するために設計されています。決済保護は、保護されたアプリケーションの起動を他のアプリケーションに通知せず、他のアプリケーションが保護されたアプリケーションでの情報の置換や画面情報を読み取れないように防止します。決済保護は保護されたアプリケーションのリストにあるすべてのアプリケーションを検査します。決済保護をアクティベーションした後は、一部のオンラインバ

ンキングおよび決済アプリケーションが自動的に保護されたアプリケーションのリストに追加されます。

保護されたアプリケーションのリストに新しいアプリケーションを追加する

1. [アプリ]メニューまたはESET Mobile Securityで決済保護を開きます。
2. 管理をタップします。
3. 決済保護で保護するアプリケーションを選択します。
4. [OK] をタップして選択内容を確定します。

決済保護を使用して銀行および決済アプリケーションを開く

オンラインバンキングおよび決済アプリケーションの最高の保護を保証するには、セーフランチャーからこれらのアプリケーションを開きます。セーフランチャーは、セーフランチャーの外でアプリケーションを起動するときに、決済保護機能の標準の保護と比較して、保護を強化します。

セーフランチャーは、決済保護が有効なときに自動的に作成されます。セーフランチャーには、決済保護で保護されているすべてのアプリケーションが含まれています。目的の支払いアプリケーションを選択すると、迅速な決済保護検査が開始され、検査の結果が記載された通知が届きます。

セーフランチャーとは何ですか。どのようにして使用することができますか。

セーフランチャーは、アプリケーションリスト  または ESET Mobile Security > 決済保護にあります。



セーフランチャーの起動

- i** オンラインバンキングや決済アプリケーションを簡単にすばやく起動するために、セーフランチャーをホーム画面に追加することができます。セーフランチャーをホーム画面に追加するには、セーフランチャーアイコンを長押しし、ホーム画面までドラッグします。

通話フィルター

通話フィルターは、設定したルールに基づいて、発着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、電話通知は表示されません。誤ってブロックされた可能性がある通話を確認するには、**通話ログ**を表示してください。

最後の発信者をブロック - タップすると、最後に受信した電話番号から受信通話をブロックします。これで新しいルールが作成されます。

ルール

新しいルールを作成するには、+アイコンをタップします。詳細については、[次の章](#)を参照してください。

既存のルールを修正するには、ルールを選択し、編集をタップします。ルール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、**削除**をタップします。

通話ログ

通話セクションには、通話フィルターによってブロックされたすべての通話とメッセージのログが表示されます。各ログには、発信者の名前、対応する電話番号、イベントの日時が記録されます。



SIMカードがないデバイス

通話フィルターは、通話およびメッセージングをサポートしないデバイスでは動作しません。

発信通話



Google PlayからダウンロードしたESET Mobile Securityの通話フィルタでは、発信通話はブロックされません。



Androidサポート

通話フィルターは、Android 6以降のデバイスでのみ使用できます。

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。

対象

拒否

相手

個人

名前

名前(任意)

電話番号

+421*

時間帯

常時

保存

新規ルールの追加

新しいルールを作成するには、+アイコンをタップします。

1. **[対象]** セクションで、**拒否** または **許可** を選択し、通話とメッセージのルールタイプを指定します。ブロックする通話方向を選択します(既定では受信が選択されています)
2. **[相手]** セクションで、ルールが影響する電話番号を指定するオプションを選択します。
 - **個人** – 連絡先リストから人を選択するか、手動で名前と番号を手動で追加します。その他の電話番号を1つの名前に割り当てるには、**電話番号** セクションで+ボタンをクリックします。
 - **グループ** – ESET Mobile Security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)。
 - **電話帳未登録の番号** 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します。
 - **電話帳登録済みの番号** 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。

- **すべての番号**はすべての着信通話をブロックします。
- **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。

3.[**時間帯**]セクションで[**常に**]または[**カスタム**]を選択し、ルールが有効になる間隔と曜日を指定します。既定では、土曜日と日曜日が選択されています。


図の手順については、[このナレッジベース記事](#)をご覧ください。

通話フィルター(海外)

- i** 海外にいる場合は、リストにの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します(+1610100100など)。

ネットワーク検査



ネットワーク検査では、ネットワークのルーターに接続されたデバイスを検査し、脆弱性を確認します。ネットワーク検査は2つのステップでネットワークを検査します。

まず、ネットワーク検査は、ネットワークの接続されたデバイスを検査します。新しいデバイスが検出された場合は、通知が表示され、デバイスに星マークが表示されます。手動でネットワークのデバイスを検索するには、**ネットワークの検査**をタップします。自動的にデバイスを検出することもできます。このオプションを使用するには、メニューアイコン  > **詳細設定**をタップし、**自動的にデバイスを検出**オプションをタップします。

2番目の検査ステップでは、ネットワーク検査は、接続されたデバイスに接続し、開いているポート、弱いルーターユーザー名/パスワード、ルーターファームウェアの問題といった脆弱性を確認することで、デバイスの脆弱性をテストします。これらの脆弱性は、ルーターやルーターに接続されている他のデバイスを乗っ取るために、攻撃者によって利用される可能性があります。攻撃者によって制御されるルーターとデバイスは、ユーザーの情報を収集したり、分散サービス拒否攻撃(DDoS)などを実行したりするために使用される可能性があります。

ネットワーク検査は、ネットワークに接続されているデバイスの包括的な一覧を提供するため、ネットワークに接続しているユーザーに関する情報を常に把握することができます。この情報に基づき、ルーターの**Web**インターフェイスからネットワークに対するこれらのデバイスのアクセス権を管理または拒否することができます。。ネットワーク検査から直接、ルーターの**Web**インターフェイスにアクセスには、ルーターを選択し、**Webインターフェイスを開く**オプションをタップします。

接続されたデバイスは一覧として確認するか、視覚的に確認することができます。

-  **リストビュー** – 接続されたデバイスは、標準のリストビューで表示されます。ルーターが最上位に表示され、その後にオンラインのデバイスが表示され、最後に以前に接続されたデバイスの履歴が表示されます。
-  **ソナービュー** – デバイスは、ルーターを中心に、半円で視覚的に表示されます。中央から2番目の層には、その時点でオンラインのデバイスが表示されます。3番目の層には、以前に接続されたデバイスの履歴が表示されます。デバイス間を移動するには、矢印ボタンをタップするか、円の方向にスクロールします。

簡単なデバイス管理のため、カテゴリをデバイスに割り当て(スマートフォン、テレビ、ゲームコンソー


ル、コンピューターなど)、標準のメーカー名またはIPアドレスからよりわかりやすい名前にデバイス名を変更します(例: SM-G955Fからサムの電話、192.168.1.52からジェーンのコンピューターなど)。

ネットワーク検査でデバイス名を変更するには、ネットワーク検査のデバイスアイコンをタイプし、右上の鉛筆アイコンをタップして、デバイスカテゴリを選択し、デバイスの名前を入力してから、**OK**をタップします。

! ネットワーク検査は、Android 12以前のデバイスでのみ動作します。

セキュリティ監査

セキュリティ監査では、重要なデバイス設定の監視および変更を行うことができます。デバイスにインストールされている各アプリケーションの権限を確認して、セキュリティリスクを防止できます。



セキュリティ監査と特定のコンポーネントを有効または無効にするには、メニューボタン  をタップし、**デバイス監視を無効にする**または**アプリケーション監査を無効にする**をタップします。

- [デバイス監査](#)
- [アプリケーション監査](#)

デバイス監査

セキュリティ監査の**デバイス監視**セクションではESET Mobile Securityによって監視されるデバイスコンポーネントを定義します。

各コンポーネントの監視を無効にすることができます。

1. 無効にするコンポーネントをタップします。
2. メニューアイコン  をタップします。
3. 無効にするをタップします

Wi-Fi

データは盗聴者によって簡単に傍受される可能性があります。適切なアプリ暗号化なしで、機密ビジネス情報または個人情報にアクセスしたり、このような情報を送信したりするときには注意してください。**Wi-Fi**コンポーネントは、安全でない可能性のあるネットワークにアクセスしようとしたときに問題があることを示します。

メモリ

ストレージメモリ容量が少ないと、新しいアプリケーションをインストールするときに問題が発生し、既存のアプリケーションの速度が低下する可能性があります。**メモリ**機能は、内部ストレージが95%以上使用されている場合に問題を示します。

データローミング

普段使用しているネットワークのサービス地域外に移動するときに、高額なデータサービス料の発生を

防ぐためにデータローミングをオフにします。ローミング機能は、デバイスがローミングネットワークをアクティブに使用している間の問題のみを示します。

通話ローミング

サービス料金はローミング時に高くなる場合があります。ローミング機能は、デバイスがローミングネットワークをアクティブに使用している間の問題のみを示します。

デバッグモード

USBデバッグモードは開発目的専用です。USBデバッグモードでは、USB経由でコンピュータに接続されているときに、デバイスが感染に対して脆弱になる可能性があります。

ルート化されたデバイス

ルート化されたデバイスは他社製のソフトウェアに対してオペレーティングシステムへの無制限のアクセスを許可し、重要なデータへのアクセスを許可する場合があります。この機能は、デバイスがルート化されている(スーパーユーザーアクセスが許可されている)場合に問題があることを示します。

アプリケーション監査

アプリケーション監査では、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。デバイスにインストールされたアプリケーションを監査します。ESET Mobile Securityはこのようなアプリケーションのカテゴリ別リストを提供します。各カテゴリをタップし、詳細説明を表示します。アプリケーションをタップし、権限詳細を表示します。

設定

プログラムの設定にアクセスするには、ESET Mobile Securityメイン画面でメニューアイコン  をタップ(またはデバイスの[メニュー]ボタンを押下)し、[設定]をタップします。

バックアップと復元

ESET Mobile Securityでは、ESET Mobile Security設定を含むバックアップファイルを作成できます。このファイルを外部デバイスにダウンロードしてESET Mobile Security設定を復元するために使用することができます。

言語

既定では、ESET Mobile Securityは、デバイスのシステム既定値(Android OS言語とキーボード設定)として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。

永久通知

(このオプションはAndroid 7以降でのみ使用できます)

ESET Mobile SecurityはAndroid通知バーの下部に通知を表示します。通知を表示しない場合は、[永久通知]を選択解除し、[オフにする]をタップします。

ユーザーの同意

- ESET LiveGrid®を許可 — ESET LiveGrid® フィードバックシステムの詳細については、[詳細設定セクションを参照してください](#)。
- アナリティクスによる製品改善を許可—ESET Mobile Securityでは、匿名のアプリケーション情報(パフォーマンス、動作統計情報)を送信し、アプリケーションとサービスを改善できます。収集する情報の詳細については、[プライバシーポリシーの章](#)を参照してください。
- マーケティング目的でのデータ使用を許可

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 Mobile Security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。このオプションは、Google PlayからESET Mobile Securityをダウンロードした場合には使用できません。この場合、製品はGoogle Playからアップデートされます。

アンインストール

アンインストールウィザードを実行すると、デバイスからESET Mobile Securityが完全に削除されます。Anti-Theftが有効な場合は、ESET Mobile SecurityセキュリティPIN/パターンまたは指紋を入力します。製品を手動でアンインストールするには、[このセクションの手順](#)に従います。

i アンインストール防止

アンインストール保護は、Androidバージョン7.0以降ではアクティブではありません。

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 Mobile Security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。

[ESETカスタマーサポートに連絡](#)

デバイスから直接サポート要求を送信する

1. ESET Mobile Securityメイン画面でメニューアイコン  をタップ(またはデバイスの[メニュー]ボタンを押下)します。
2. カスタマーサポートをタップします。
3. カスタマーサポートをタップして、テクニカルサポートのリクエストを作成します。
4. すべての必須フィールドを入力します。ESET Mobile Securityには、詳細ログ機能があり、技術的な問題の可能性を診断できます。
5. 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。
6. **送信**をタップしてリクエストを送信します。
7. 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。

トラブルシューティングの一環としてESET Mobile Securityをアンインストールして再インストールした場合、診断ログは削除されます。問題をもう一度複製し、その後にログを送信することをお勧めします。

アプリケーションが開いていないか、応答していません

! ESET Mobile Securityが応答していないか、開けない場合にESETにサポート要求を送信するには、設定 > アプリケーション > ESET Mobile Security > ストレージ > ストレージの管理に移動します。カスタマーサポートをクリックして、すべての必須フィールドを入力します。

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、掲載番号31333532として商業登記されているESET, spol. s r. o.またはESETグループ内の別企業（以下ESETまたは「供給者」とします）と、自然人または法人であるお客様（以下「お客様」または「エンドユーザー」とします）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的説明（「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④(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④(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④MUA④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。メールサーバー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ー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 Edition④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④NFR④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

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ー(「EOLポリシー」)が適用される場合があります。<https://go.eset.com/eolhome>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URL、IP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、質借、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、たとえば供給者、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な場合があります。

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(ii) 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(ii) 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ー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ー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。

契約書の補遺

ネットワーク接続デバイスセキュリティ評価。 ネットワーク接続デバイスセキュリティ評価には、次のように追加の条項が適用されます。

本ソフトウェアには、ネットワーク接続デバイスセキュリティ評価の一部としてライセンス情報に関連する、ローカルネットワークのデバイスの存在、タイプ、名前IPアドレス、およびMACアドレスなど、ローカルネットワークのデバイスに関する情報とローカルネットワーク名が必要な、エンドユーザーのセキュリティとローカルネットワークのデバイスのセキュリティを確認する機能があります。これらの情報には、ルーターデバイスのワイヤレスセキュリティタイプとワイヤレス暗号化タイプも含まれます。この機能は、ローカルネットワークのデバイスを保護するためのセキュリティソフトウェアソリューションの利用状況に関する情報も提供する場合があります。

データの悪用に対するAnti-Theftの保護。 データの悪用に備える保護対策には、次のように追加の条項が適用されます。

本ソフトウェアには、コンピューターの窃盗と直接関連して、重要なデータの損失または悪用を防止する機能が含まれています。この機能は、本ソフトウェアの既定の設定でオフにされています。アクティベーションするにはESET HOMEアカウントを作成する必要があります。これによって、コンピューターの窃盗の際に、データ収集が有効になります。本ソフトウェアのこの機能を有効にする場合は、盗まれたコンピューターに関するデータが収集され、供給者に送信されます。これには、コンピューターのネットワーク位置情報データ、コンピューター画面に表示された内容のデータ、コンピューターの構成のデータ、およびコンピューターに接続されたカメラによって記録されたデータ(「データ」)が含まれることがあります。エンドユーザーは、コンピューターの窃盗が原因の問題を修正する目的でのみ、この機能

で取得されESET HOMEアカウントに送信されたデータを使用する資格があります。この機能の目的に限り、供給者は、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、データを処理します。供給者は、データが取得された目的を達成するために必要な期間の間、エンドユーザーがデータにアクセスすることを許可するものとします。ただし、この期間は、プライバシーポリシーで規定された保持期間を超えないものとします。データの悪用に対する保護は、エンドユーザーが合法的にアクセスできるコンピューターおよびアカウントでのみ使用されるものとします。不法使用は管轄当局に報告されます。供給者は関連する法律を遵守し、悪用の場合には法執行機関を支援します。お客様は、自身がESET HOMEアカウントにアクセスするためのパスワードを保護する責任を有することを認め、パスワードをいかなる第三者にも開示しないことに同意します。エンドユーザーは、許可の有無を問わず、データの悪用保護機能ESET HOME アカウントを使用したすべての活動に責任を負いますESET HOMEアカウントが危険にさらされた場合は、ただちに供給者に通知してください。

コード。コードには、次のように追加の条項が適用されます。

ESETは独自の裁量で販売促進またはマーケティング目的(「コード」)の照会コードまたは他のコードを作成および提供できます。お客様はコードを利用して、本契約に従ってライセンス期間を延長できますESETは本契約に準拠しない方法でコードが取得または使用されたとき、あるいは瑕疵、詐欺、または不法行為があると合理的に見なされる場合には、コードをいつでも無効にする権利を留保します。お客様は次の制限に従う必要があります。

- i.お客様はコードを複数回使用できません。
- ii.コードの販売、賃貸借、または商業サービスの提供目的でのコードの使用はできません。
- iii.お客様は、ESETがESETに対する一切の義務なくいつでもコードの提供または使用を無効にできることに同意します。
- iv.お客様は、コードが現金または他の補償として有効ではないことに同意します。
- v. お客様は、コードおよびコードの使用には特定の照会、販売促進、またはマーケティングキャンペーンのためにESETで提供される特殊な条件が適用されることに同意します。

EULAID: EULA-PRODUCT-LG-EMS; 3537.0

プライバシーポリシー

個人データの保護は、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事業登記番号: 31333532)(ESETまたは「当社」)にとって特に重要ですESETは、EU一般データ保護規制(GDPR)の下で法的に規定された透明性要件に準拠します。この目標を達成するためにESETは、データ主体としてのお客様(「エンドユーザー」または「お客様」)に次の個人データ保護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。

- 個人データの処理の法的根拠
- データ共有と機密保持
- データセキュリティ
- データ主体としての権利
- 個人データの処理
- 連絡先情報。

個人データの処理の法的根拠

ESETが個人データの保護に関連する該当する法的フレームワークに従って使用するデータ処理には、ほとんど法的根拠がありませんESETにおける個人データの処理は、主に、エンドユーザーとの [エンドユー](#)

ザイ使用許諾契約 (EULA) の履行(GDPR第6 (1) (b)条)に必要です。これは、明示的な記載がないかぎりESETの製品またはサービスの提供に適用されます。例:

- 正当な利益という法的根拠(GDPR第6 (1) (f)条)。これにより、お客様がサービスを使用する方法、ならびにESETが提供できる最高の保護、サポート、およびエクスペリエンスに対するお客様の満足度に関するデータを処理できます。適用される法律では、マーケティングも正当な利益と認識されているため、通常はお客様とのコミュニケーションで使用されるCookieについては、この概念を適用します。
- 同意(GDPR第6 (1) (a)条)ESETがこの法的根拠を最も適切な根拠であると見なすとき、または法律で義務付けられている場合には、特定の状況においてESETがお客様の同意を求める場合があります。
- 電子通信、請求または課金文書の保持に関する要件の規定など、法的義務の遵守(GDPR第6 (1) (c)条)。

データ共有と機密保持

ESETがお客様のデータを第三者と共有することはありません。ただしESETは、販売、サービス、および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を通して、世界中で事業を展開する企業ですESETが処理するライセンス、請求、テクニカルサポート情報は、サービスやサポートの提供といったエンドユーザーライセンス契約の履行の目的で、関連会社またはパートナーとの間で転送される場合があります。

基本的に、ESETは、欧州連合(EU)でデータを処理します。ただし、お客様の居住国(EU外での製品またはサービスの利用)またはお客様が選択するサービスによってはEU外の国にお客様データを転送しなければならない場合があります。たとえばESETは、クラウドコンピューティングに関連してサードパーティサービスを使用しています。このような場合ESETはサービスプロバイダーを厳選し、契約、技術、組織的な対策を導入して、適切なレベルのデータ保護を保証します。原則としてESETは、EUの標準契約条項と補足契約規制(必要な場合)に同意します。

英国やスイスなどのEU外の一部の国についてはEUが既に同等のデータ保護を決定しています。同等のデータ保護が規定されているため、このような国へのデータ転送には特別な認可または同意が必要ありません。

データセキュリティ

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、すぐに該当する監督当局とデータ主体として影響を受けるエンドユーザーに通知します。

データの主体の権利

すべてのエンドユーザーの権利は重要ですESETは、すべてのエンドユーザー(EU加盟国およびEU非加盟国)が次の権利について保証されていることを通知します。データ主体の権利を行使するには、サポートフォームまたは電子メール(dpo@eset.sk)でお問い合わせください。本人確認目的で、次の情報をご提示ください。お名前、電子メールアドレス、製品認証キー(該当する場合)、お客様番号、会社名。生年月日などの他の個人データは送信しないでください。またESETは、お客様の依頼を処理し、本人確認を行うために、お客様の個人データを処理します。

同意を取り消す権利。同意のみに基づく処理の場合、同意を取り消す権利が適用されますESETがお客様の同意に基づいてお客様の個人データを処理する場合、お客様は、理由を提供せずに、いつでも同意を取り消す権利があります。同意の取り消しは将来に対してのみ有効であり、取り消し前に処理されたデータの合法性には影響しません。

異議を申し立てる権利。同意のみに基づく処理の場合、同意を取り消す権利が適用されます。ESETが合法的な利益を保護するために、お客様の個人データを処理する場合、データ主体としてのお客様は、いつでもESETが指名した合法的な利益および個人データの処理に対して異議を申し立てる権利があります。異議申し立ては将来に対してのみ有効であり、異議申し立て前に処理されたデータの合法性には影響しません。ESETがダイレクトマーケティング目的で個人データを処理している場合、お客様の異議申し立ての理由を提出する必要はありません。これは、このようなダイレクトマーケティングに関連しているかぎり、プロファイリングにも該当します。他のすべての場合において、お客様は、ESETが個人データを処理する正当な利益に対する苦情について簡潔に通知することが求められます。

場合によっては、お客様が同意を取り消したにもかかわらずESETは、契約の履行など、別の法的根拠に基づいて個人データを引き続き処理する資格があります。

アクセスの権利。お客様は、データ主体として、いつでも無料で、ESETによって保存されたデータに関する情報を取得する権利があります。

修正する権利。ESETがお客様に関する誤った個人データを間違えて処理した場合、お客様はこれを修正する権利があります。

消去する権利および処理を制限する権利。データ主体として、お客様は、個人データの削除または制限を要求する権利があります。お客様の同意を得た場合などESETがお客様の個人データを処理し、お客様がその同意を取り消し、それ以上の法的根拠(契約など)が存在しない場合ESETはただちにお客様の個人データを削除します。お客様の個人データは、保持期間の終了に指定された目的で必要とされなくなった時点ですみやかに削除されます。

ESETが直接マーケティングの目的でのみお客様の個人データを使用し、お客様が同意を取り消したか、根拠となるESETの合法的な利益に対して異議を申し立てた場合ESETは、未承諾の連絡を回避する目的でお客様の連絡先データを社内ブラックリストに追加する範囲で、お客様の個人データの処理を制限します。そうでない場合、お客様の個人データは削除されます。

ESETは、立法当局または監督当局によって発行された保持義務および期間が終了するまで、お客様のデータを保存することが義務付けられている場合があります。保持義務と期間は、スロバキア法律によっても生じ得る場合があります。その後、該当するデータは日常的に削除されます。

データ移植性の権利。ESETは、データ主体としてのお客様に対してESETが処理する個人データをxls形式で提供いたします。

苦情を申し立てる権利。データ主体として、お客様は、いつでも監督当局に苦情を申し立てる権利を有します。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。該当するデータ監督当局は、スロバキア共和国個人データ保護局(Hraničná 12, 82007 Bratislava 27, Slovak Republic)です。

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](#)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、エンドユーザーライセンス契約および製品[ドキュメント](#)をご覧ください。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。

ライセンスおよび請求データ。名前、電子メールアドレス、製品認証キー、(該当する場合)住所、会社名、決済データは、適用法またはお客様の同意に従って、ライセンスのアクティベーション、製品認証キーの提供、有効期限のリマインダー、サポート依頼、ライセンスが本物であることの検証、サービスの提供、および他の通知(マーケティングメッセージを含む)を支援する目的で、ESETによって収集および処理されます。ESETは、10年間請求情報を保持する法的義務を負っています。ただし、ライセンス情

報は、遅くともライセンスの有効期限から12か月間経過した後に匿名化されます。

アップデートおよび他の統計情報。処理される情報には、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が含まれます。これらの情報は、アップデートおよびアップグレードサービスの提供、ならびにESETバックエンドインフラストラクチャのメンテナンス、セキュリティ、改善の目的で処理されます。

この情報はエンドユーザーを特定する必要がないため、ライセンスおよび請求目的に必要な個人を識別する情報とは別に保持されます。保持期間は最大4年間です。

ESET LiveGrid®レピュテーションシステム。侵入に関連する単方向ハッシュは、検査されたファイルを、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することで、マルウェア対策ソリューションを効率化するESET LiveGrid®レピュテーションシステムの目的で処理されます。この処理中にエンドユーザーが特定されることはありません。

ESET LiveGrid®フィードバックシステム。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

- 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
- IP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
- 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。

ESET LiveGrid®フィードバックシステム経由で取得および処理されるすべての情報は、エンドユーザーを特定せずに使用されます。

ネットワーク接続デバイスセキュリティ評価。セキュリティ評価機能を提供するためにESETは、ライセンス情報に関連する、ローカルネットワークのデバイスの存在、タイプ、名前、IPアドレス、およびMACアドレスなど、ローカルネットワークのデバイスに関する情報とローカルネットワーク名を処理します。これらの情報には、ルーターデバイスのワイヤレスセキュリティタイプとワイヤレス暗号化タイプも含まれます。エンドユーザーを識別するライセンス情報は、ライセンスの有効期限から最大12か月間匿名化されます。

テクニカルサポート。サポート要求に含まれる連絡先・ライセンス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。テクニカルサポートで処理されたデータは4年間保管されます。

データの悪用に対するAnti-Theftの保護 <https://home.eset.com>でESET HOMEアカウントを作成し、Anti-Theftでデバイスを紛失に設定した場合、次の情報が収集、処理されます。位置情報、スクリーンショット、コンピューターの設定に関するデータ、コンピューターのカメラで記録されたデータ。収集されたデータは、ESETまたはESETのサービスプロバイダーのサーバーに保存され、保存期間は3ヶ月です。

使用状況とクラッシュ分析。お客様のオプトインの同意に基づきESET製品の使用に関連するデータを収集、分析してESET製品の性能をテストし、お客様のために製品を改善します。収集されるデータには、製品で発生するさまざまなユーザーアクションとイベント(アプリの起動、アプリアップデート、セッション期間、アプリ内購入など)、使用されているデバイス、プラットフォームやオペレーティングシステムに関する情報、年齢、性別、位置情報、関心に関連するデータ(インストールIDなど)が含まれます。さらにESETは、アプリケーションクラッシュに関連する技術データ(デバイス情報、インストール識別子、クラッシュトレース、クラッシュミニダンプなど)を収集および処理して、クラッシュを調査し、クラッシュの原因を解明し、アプリケーションが完全に動作することを保証する場合があります。これらのデータを収集して分析するためにESETは、カスタマーエクスペリエンス改善プログラム(匿名のテレメトリデータだけが処理される)とGoogleサービスを使用して、より詳細な分析情報を取得しますGoogleによるデータの処理の詳細については、関連する[Googleプライバシーポリシー](#)をご覧ください。

マーケティング目的での処理。マーケティング目的に関する同意をESETに付与する場合ESETおよびマーケティングパートナーは、お客様の製品の使用状況に関するデータを使用して、オンラインマーケティングアクティビティのパフォーマンスを評価し、お客様の関心をより良く理解し、お客様に関連性が高いオンライン広告を表示します。収集されるデータには、製品で発生するさまざまなユーザーアクションとイベント(アプリの起動、アプリアップデート、セッション期間、アプリ内購入など)、使用されているデバイス、プラットフォームやオペレーティングシステムに関する情報、年齢、性別、位置情報、関心に関連するデータ(インストールID、モバイル広告ID)が含まれますESETはGoogleを使用して、これらのデータを収集および分析しますGoogleによるデータの処理の詳細については、関連する[Googleプライバシーポリシー](#)をご覧ください。

ESETの製品およびサービスを使用する個人が製品またはサービスを購入したエンドユーザーではなくESETとエンドユーザーライセンス契約を締結していない場合(例: エンドユーザーの従業員、家族、エンドユーザーライセンス契約に従ってエンドユーザーから製品またはサービスの使用を許可された人)GDPR第6(1)f)条の解釈に従い、ESETの合法的な利益において、データの処理が実行され、エンドユーザーが許可したユーザーはエンドユーザーライセンス契約に従ってESETが提供する製品およびサービスを使用できるものとします。

連絡先情報

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