kaspersky

Kaspersky Security for Mobile

目次

Kaspersky Security for Mobile ヘルプ

Kaspersky Security for Mobile は、企業用モバイルデバイス、従業員が社用で使用する個人用モバイルデバイスの保護と管理を目的として設計されています。

Kaspersky Security for Mobile のコンポーネントと機能は、 モバイルデバイスの管理と保護に使用する Kaspersky Security Center コンソールによって異なります。

Kaspersky Security Center コンソールに応じて、必要なヘルプのセクションを選択してください。

- マイクロソフト管理コンソールベースの管理コンソール
- Kaspersky Security Center Web コンソールまたは Kaspersky Security Center Cloud コンソール

個別のヘルプセクションで、Kaspersky Endpoint Security for Android アプリと Kaspersky Security for iOS アプリでユーザーが使用可能な機能と動作について説明します。

主な変更点

Kaspersky Security for iOS Technical Release 1

新しい Kaspersky Security for iOS アプリは、企業の iOS、iPadOS の保護と管理を目的として設計されています。本アプリの主要な機能は次の通りです：

- オンラインの脅威からの保護
- ジェイルブレイクの検知
- Kaspersky Security Center Web コンソールまたは Cloud コンソールでの企業のモバイルデバイス管理

Kaspersky Endpoint Security for Android Technical Release 42

- Kaspersky Endpoint Security for Android のユーザーインターフェイスを改善しました。
- Bluetooth の使用を管理者が制限するために、Android 12 以降の［付近の Bluetooth デバイス］権限を必要とするようになりました。
- 一部の問題を修正し、改善しました。

Kaspersky Endpoint Security for Android Technical Release 41

- Kaspersky Endpoint Security for Android のユーザーインターフェイスを改善しました。
- Kaspersky Security Center Web コンソールと Cloud コンソール向けの Kaspersky Security for Mobile (Policies) プラグインのポリシー設定のユーザーインターフェイスを改善しました。
- 一部の問題を修正し、改善しました。

Kaspersky Endpoint Security for Android Technical Release 40

- 一部の問題を修正し、改善しました。

Kaspersky Endpoint Security for Android Technical Release 39

- Android 12L をサポートするようになりました。
- 次の契約書、声明が更新されました：
  - 使用許諾契約書
  - Kaspersky Security Network に関する声明
  - マーケティング目的に沿ったデータ処理に関する声明

管理者は、管理コンソールで契約書と声明の諸条項に同意できます。これにより、Kaspersky Endpoint Security for Android のユーザーがデバイス上で同意する手順をスキップできます。

- 一部の問題を修正し、改善しました。

Kaspersky Endpoint Security for Android Technical Release 33

- サードパーティ製の EMM システムを使用した Kaspersky Endpoint Security for Android の管理時に、1 つのコマンドを使用して複数の使用許諾契約書に同意できるようになりました。
- Samsung KNOX のアクティベーションにライセンスが必要なくなりました。
- Kaspersky Security for Mobile コンポーネントのバージョンが変更され、リリース番号を含むようになりました。

Kaspersky Endpoint Security for Android Technical Release 32

- Kaspersky Endpoint Security for Android は、Android の更新された要件をサポートするように変更されました。

Kaspersky Endpoint Security for Android Technical Release 31

- Kaspersky Security Center が組織に導入されていない場合、またはモバイルデバイスからアクセスできない場合、ユーザーは Kaspersky Endpoint Security for Android をデバイス上で手動でアクティベートできます。
- Kaspersky Security for Mobile が、Google Chrome のカスタムタブ機能をサポートするようになりました。

Kaspersky Endpoint Security for Android Technical Release 30

- Kaspersky Security for Mobile が、 Kaspersky Security Center Cloud コンソールでモバイルデバイスを保護、管理できるようになりました。
- Kaspersky Endpoint Security for Android が iOS 15 と iPadOS 15 をサポートしました。

Kaspersky Endpoint Security for Android Technical Release 29

- Kaspersky Endpoint Security for Android が Android 12 をサポートしました。

Kaspersky Endpoint Security for Android Technical Release 27

- Kaspersky Security for Mobile が、 Kaspersky Security Center Web コンソールでモバイルデバイスを保護、管理できるようになりました。

Kaspersky Endpoint Security for Android Technical Release 26

- Kaspersky Endpoint Security のライセンスと定額制サービスの自動更新がサポートされました。

Kaspersky Endpoint Security for Android Technical Release 22

- Kaspersky Endpoint Security が Kaspersky Private Security Network をサポートしました。このソリューションにより、企業ネットワークの外部へデータを送信することなく、Kaspersky Security Network の評価データベースへのアクセスが可能となります。
- Android バージョン 4.2 ～ 4.4.4 のデバイスへのインストールが、サポート対象外になりました。

Kaspersky Endpoint Security for Android Technical Release 20

- 法的な声明を管理者がグローバルに同意することを選択した場合、ユーザーには同意が要求されません。
- アプリのパフォーマンスが最適化されました。

Kaspersky Endpoint Security for Android Technical Release 19

- Kaspersky Security Center を使用して、Kaspersky Security Network やその他の声明に管理者がエンドユーザーの代わりに同意できるようになりました。
- いくつかのエラーが修正され、動作の安定性が向上しました。

Kaspersky Endpoint Security for Android Technical Release 18

- Kaspersky Security for Mobile がファーウェイモバイルサービスをサポートするようになりました。
- Kaspersky Endpoint Security for Android を、Huawei AppGallery からインストールできるようになりました。

Kaspersky Endpoint Security for Android Technical Release 17

- Kaspersky Endpoint Security は、API レベル 29 以降をターゲットとしています。Android 10 以降のデバイス上でのアプリ動作が、一部変更されます。
- 必要な複雑性を持つパスワードを設定する際の、パスワード強度設定が新しくなりました。
- 指紋での画面ロック解除の設定は、仕事用プロファイルでのみ使用可能になりました。
- いくつかのエラーが修正され、動作の安定性が向上しました。

Kaspersky Endpoint Security for Android Technical Release 16

- Kaspersky Endpoint Security for Android が Android 11 をサポートしました。
- 位置情報とカメラに対する新しいアクセス権の要求オプション（Android 11 より追加）に対応しました。カメラと位置情報へのアクセス権に関する新しいルールについては、ここに詳細を記載しています。

- サードパーティの EMM コンソールで、ユーザーの企業メールアドレスを指定できるようになりました。新規パラメータ KscCorporateEmail が設定されている場合、Kaspersky Security Center にこれらのメールアドレスが表示されます。

Kaspersky Endpoint Security for Android Technical Release 14

- 本アプリのデバイス管理者の権限をユーザーが許可したり取り消したりすると、管理コンソールにイベントが必ず送信されるようになりました。

- サードパーティの EMM コンソールで、「KscGroup」パラメータを指定できるようになりました。Kaspersky Security Center へデバイスを接続すると、［未割り当てデバイス］フォルダーのサブフォルダーにそのデバイスが自動的に追加されます。サブフォルダーの名前は、EMM コンソールで設定したグループ名と同一です。

Kaspersky Endpoint Security for Android Technical Release 13

- Kaspersky Endpoint Security for Android のユーザーインターフェイスのデザインが新しくなりました。

- すべてのヘルプセクションがオンラインになりました。

- 管理対象デバイスの IP アドレスが Kaspersky Security Center に送信され、デバイス情報セクションで表示できるようになりました。

Kaspersky Endpoint Security for Android Technical Release 12

- Kaspersky Security Center 12.1 にある使用許諾契約書（EULA）への同意がリモートで可能になりました。使用許諾契約書の条項とプライバシーポリシーに管理コンソール上で管理者が同意すると、Kaspersky Endpoint Security for Android のインストール中に同意のステップがスキップされます。

- VMware AirWatch を使用するユーザーのデバイス名を Kaspersky Security Center で編集する機能が追加されました。本アプリの設定に使用する設定ファイルに新しい設定項目を追加しました。デバイスのシリアル番号など、デバイス名にさらに情報を追加できます。これにより、Kaspersky Security Center でのデバイスの検索と並べ替えが容易になります。

Kaspersky Endpoint Security for Android Technical Release 11

いくつかのエラーが修正され、動作の安定性が向上しました。

Kaspersky Endpoint Security for Android Technical Release 10

- Kaspersky Security for Mobile は、Kaspersky Security Center 12 をサポートするようになりました。

- Kaspersky Safe Browser は、Kaspersky Security Center 12 ではサポート対象外となりました。Kaspersky Security Center 11 以前を使用している場合、Kaspersky Safe Browser の機能を使用できます。

- いくつかのエラーが修正され、動作の安定性が向上しました。

Kaspersky Endpoint Security for Android Service Pack 4 Maintenance Release 3

- Kaspersky Endpoint Security for Android が Microsoft Intune（エンタープライズ・モビリティ・マネジメント製品（EMM））をサポートすることを確認しました。カスペルスキーは、AppConfig Community に加入しており、本アプリがサードパーティ製の EMM 製品と併用できるようにしています。

- 本アプリがバックグラウンドモードで実行されている時は、通知とポップアップメッセージを無効にする機能を追加しました。バックグラウンドモードでのこれらの機能の実行は安全ではないことにご注意ください。バックグラウンドモードで通知とポップアップメッセージを無効にすると、本アプリは脅威に関する警告をユーザーにリアルタイムで通知しなくなります。モバイルデバイスのユーザーが端末の保護ステータスを知るのは、本アプリを開いた時のみとなります。

- VMware AirWatch 内で、使用許諾契約書（EULA）とプライバシーポリシーに同意できるようになりました。AirWatch コンソール内で使用許諾契約書とプライバシーポリシーに同意した場合、Kaspersky Endpoint Security for Android は初期設定ウィザードで発生する同意のステップをスキップします。

- 危険サイトブロックの使用を目的としたデータ処理に関する声明（「危険サイトブロックに関する声明」）を追加しました。危険サイトブロックを使用するには、この声明に同意する必要があります。Kaspersky Endpoint Security for Android は、Kaspersky Security Network（KSN）を Web サイトのスキャンに使用します。危険サイトブロックに関する声明は、KSN とのデータ交換に関する諸条項を含んでいます。危険サイトブロックに関する声明は、ポリシー内で同意することも、端末のユーザー宛てに同意の要求を送信することも可能です。

- いくつかのエラーが修正され、動作の安定性が向上しました。

管理ツールごとのアプリケーション機能の比較

次の管理ツールを使用して、Kaspersky Security Center でモバイルデバイスを管理できます：

- Kaspersky Security Centerの Microsoft 管理コンソールベースの（以降、「MMC ベースの」と表記）管理コンソール
- Kaspersky Security Center Web コンソール
- Kaspersky Security Center Cloud コンソール

下の表に、これらのツールで使用可能な機能の比較を記載しています：

管理ツールごとに使用可能な機能

	MMC ベースのコンソール	Web コンソール	Cloud コンソール
全般			
Android デバイスの管理	使用可能	使用可能	使用可能
iOS デバイスの管理	使用可能（APNs 証明書を使用）	使用可能（Kaspersky Security for iOS アプリを使用）	使用可能（Kaspersky Security for iOS アプリを使用）
モバイルデバイス管理			
Google Play リンクを使用してデバイスを追加	使用可能	使用可能	使用可能
App Store リンクを使用してデバイスを追加	使用不可	使用可能	使用可能
iOS MDM プロファイルを使用して iOS デバイスを追加	使用可能	使用不可	使用不可
インストールパッケージを使用してデバイスを追加	使用可能	使用不可	使用不可
モバイルデバイスへのコマンドの送信	使用可能	使用可能（遠隔撮影のコマンドを除く）	使用可能（遠隔撮影のコマンドを除く）
Kaspersky Security Center からモバイルデバイスを削除	使用可能	使用可能（デバイスのリストからの削除のみ可能。アプリは、デバイスから手動で削除する必要があります。）	使用可能（デバイスのリストからの削除のみ可能。アプリは、デバイスから手動で削除する必要があります。）
証明書の管理			

メール証明書の発行	使用可能	使用不可	使用不可
VPN 証明書の発行	使用可能	使用不可	使用不可
モバイル証明書の発行	使用可能	使用可能	使用可能
管理サーバーツールを使用してモバイル証明書を発行する	使用可能	使用可能	使用可能
証明書ファイルの指定	使用可能	使用不可	使用不可
公開鍵基盤との統合	使用可能	使用不可	使用不可
ポリシーの管理			
グループポリシーの設定へのロールベースのアクセス	使用可能	使用不可	使用不可
Kaspersky Security Centerとモバイルデバイスの同期の設定	使用可能	使用可能	使用可能
モバイルデバイスのウイルススキャンの設定	使用可能	使用可能	使用可能
モバイルデバイスの保護の設定	使用可能	使用可能	使用可能
定義データベースのアップデートの設定	使用可能	使用可能	使用可能
盗難時または紛失時のデバイスデータの保護の設定	使用可能	使用可能	使用可能
Web サイトへのユーザーアクセスの設定	使用可能	使用可能	使用可能
アプリ管理の設定	使用可能	使用可能	使用可能
コンプライアンスコントロールの設定	使用可能	使用可能	使用可能
Android 仕事用プロファイルの設定	使用可能	使用不可	使用不可
Wi-Fi ネットワークへの接続の設定	使用可能	使用不可	使用不可
Samsung KNOX	使用可能	使用不可	使用不可
その他の機能			

Kaspersky Security Center での EULA へのグローバルな同意	使用可能	使用不可	使用不可
Kaspersky Private Security Network の設定	使用可能	使用不可	使用不可

配布キット

Kaspersky Security for Mobile 配布キットには、様々なコンポーネントが含まれており、その内容は選択した製品バージョンによって異なります。

Kaspersky Security Center Web コンソールでのモバイルデバイス管理

- `on_prem_ksm_devices_xx.x.x.x.zip`
  Kaspersky Security for Mobile (Devices) プラグインのインストールに必要なファイルを含むアーカイブ：
  - `plugin.zip`
    Kaspersky Security for Mobile (Devices) プラグインを含むアーカイブ。
  - `signature.txt`
    Kaspersky Security for Mobile (Devices) プラグインの署名を含むファイル。
- `on_prem_ksm_policies_xx.x.x.x.zip`
  Kaspersky Security for Mobile (Policies) プラグインのインストールに必要なファイルを含むアーカイブ：
  - `plugin.zip`
    Kaspersky Security for Mobile (Policies) プラグインを含むアーカイブ。
  - `signature.txt`
    Kaspersky Security for Mobile (Policies) プラグインの署名を含むファイル。

Kaspersky Security Center Cloud コンソールでのモバイルデバイス管理

Kaspersky Security Center Cloud コンソールでの管理には、配布パッケージのダウンロードは不要です。Kaspersky Security Center Cloud コンソールでのアカウントの作成のみが必要です。アカウントの作成の詳細は、*Kaspersky Security Center Cloud コンソールのヘルプ*を参照してください。

MMC ベースの管理コンソールでのモバイルデバイス管理

- `Klcfginst_en.exe`
  Kaspersky Security Center のリモート管理システムから本アプリを管理するための Kaspersky Endpoint Security for Android 管理プラグインのインストーラー。
- `Klmdminst.exe`
  Kaspersky Security Center のリモート管理システムを使用して本アプリを管理するための Kaspersky Device Management for iOS の管理プラグインのインストーラー。

Kaspersky Endpoint Security for Android アプリのファイル

`KES10_xx_xx_xxx.apk` — Kaspersky Endpoint Security for Android アプリの Android パッケージファイル。

補助的なファイル

- `sc_package_xx.exe`

  インストールパッケージの作成による、Kaspersky Endpoint Security for Android アプリ のインストールに必要なファイルを含む自己解凍アーカイブ。

  - `adb.exe`、`AdbWinApi.dll`、`AdbWinUsbApi.dll`

    インストールパッケージの作成に必要なファイル。

  - `installer.ini`

    管理サーバー接続設定を含む設定ファイル。

  - `KES10_xx_xx_xxx.apk`

    Kaspersky Endpoint Security for Android アプリの Android パッケージファイル。

  - `kmlisten.exe`

    管理者のコンピューターを使用してインストールパッケージを配信するツール。

  - `kmlisten.ini`

    ツール `kmlisten.exe`の設定を含む設定情報ファイル。

  - `kmlisten.kpd`

    製品記述ファイル。

- `SigningUtility.zip`

  Kaspersky Endpoint Security for Android アプリの配布パッケージと iOS デバイス用のコンテナーの配布パッケージへの署名に使用するツールが同梱されたアーカイブ。

ガイド

- Kaspersky Security for Mobile のヘルプ。

Kaspersky Security Center Web コンソールおよび Kaspersky Security Center Cloud コンソールの操作

このヘルプセクションでは、Kaspersky Security Center Web コンソール（以降、「Web コンソール」と表記）、または Kaspersky Security Center Cloud コンソール（以降、「Cloud コンソール」と表記）を使用したモバイルデバイスの保護と管理について説明します。

Kaspersky Security Center Web コンソールまたは Cloud コンソールでのモバイルデバイス管理の概要

次のコンポーネントを使用して、Kaspersky Security Center Web コンソールと Cloud コンソールでモバイルデバイスを管理できます：

- **Kaspersky Endpoint Security for Android アプリ**

  Kaspersky Endpoint Security for Android アプリは、Web の脅威や、脅威となるその他のウイルスやプログラムからモバイルデバイスを保護します。

- **Kaspersky Security for iOS アプリ**

  Kaspersky Security for iOS アプリは、フィッシングおよびマルウェアからモバイルデバイスを保護します。

- **Kaspersky Security for Mobile (Devices) プラグイン**

  Kaspersky Security for Mobile (Devices) プラグインを使用すると、Kaspersky Security Center Web コンソールと Cloud コンソールを使用して、モバイルデバイスとそのデバイスにインストールされたモバイルアプリを管理するインターフェイスが使用できます。

- **Kaspersky Security for Mobile (Policies) プラグイン**

  Kaspersky Security for Mobile (Policies) プラグインを使用すると、Kaspersky Security Center に接続されたデバイスの設定を、グループポリシーを使用して編集できます。

プラグインは、*Kaspersky Security Center リモート管理システム*に統合されます。Kaspersky Security Center Web コンソールまたは Cloud コンソールを使用して、クライアントコンピューターや仮想システム同様に、モバイルデバイスを管理できます。モバイルデバイスが管理サーバーに接続すると、そのデバイスは管理対象となります。管理対象デバイスを遠隔で監視できます。

Kaspersky Security Center Web コンソールまたは Cloud コンソールでのモバイルデバイス管理の主な機能

Kaspersky Security for Mobile には、次の機能があります：

- Google Play から Kaspersky Endpoint Security for Android アプリをダウンロードするリンクを使用して Android モバイルデバイスを Kaspersky Security Center に接続するためのメールメッセージを配信します。

- App Store から Kaspersky Security for iOS をダウンロードするためのリンクを使用して iOS モバイルデバイスを Kaspersky Security Center に接続するためのメールメッセージを配信します。

- モバイルデバイスを Kaspersky Security Center、またはその他のサードパーティ製の EMM システム（VMware AirWatch、MobileIron、IBM Maas360、SOTI MobiControl など）に遠隔操作で接続します。

- モバイルアプリ、モバイルデバイスのサービス、アプリ、機能の設定をリモートで編集。
- 企業のセキュリティ要件に従ったモバイルデバイスの遠隔操作で設定します。
- 紛失時または盗難時にモバイルデバイスに保存された企業情報の流出を防止します（盗難対策）。Android デバイスでのみサポートされています。
- 企業のセキュリティ要件に基づいたコンプライアンスを管理します（コンプライアンスコントロール）。Android デバイスでのみサポートされています。
- モバイルデバイスでのオンラインの脅威からの保護機能およびインターネット使用を管理します（危険サイトブロック）。
- Kaspersky Endpoint Security for Android および Kaspersky Security for iOS のユーザーに表示される通知を設定します。
- Kaspersky Endpoint Security for Android および Kaspersky Security for iOS のステータスとイベントに関する管理者からの通知を、Kaspersky Security Center またはメール経由で配信します。
- ポリシー設定の変更を管理します（リビジョンの履歴）。

Kaspersky Security for Mobile には、次の保護および管理コンポーネントが含まれます：

- アンチウイルス（Android デバイス）
- 盗難対策（Android デバイス）
- 危険サイトブロック（Android および iOS デバイス）
- アプリケーションコントロール（Android デバイス）
- コンプライアンスコントロール（Android デバイス）
- Android デバイスの root 化および iOS デバイスのジェイルブレイクの検知

Kaspersky Endpoint Security for Android の概要

Kaspersky Endpoint Security for Android アプリは、Web の脅威や、脅威となるその他のウイルスやプログラムからモバイルデバイスを保護します。

Kaspersky Endpoint Security for Android アプリには、次のコンポーネントが含まれます：

- **アンチウイルス**：定義データベースと Kaspersky Security Network クラウドサービスを使用して、デバイス上の脅威を検知し、処理します。アンチウイルスには次のコンポーネントがあります：
  - **プロテクション**：開かれるファイル内の脅威を検知し、新しいアプリをスキャンして、リアルタイムでデバイスの感染を防止します。
  - **スキャン**：要求に応じて、ファイルシステム全体、インストールされたアプリ、または選択したファイルまたはフォルダーに対して開始されます。
  - **アップデート**：新しい定義データベースをダウンロードできます。

- **盗難対策**：デバイスの紛失時または盗難時に、デバイス内の情報を不正なアクセスから保護します。この機能を使用して、デバイスへ次のコマンドを送信することができます：
  - **GPS 追跡**：デバイスの位置情報を取得します。
  - **遠隔アラーム**：デバイスのアラームを大音量で作動させます。
  - **データ消去**：企業の機密情報を保護するためデータを消去します。
- **危険サイトブロック**：悪意のあるコードを拡散するように設計された悪意のある Web サイトをブロックします。また、ユーザーの機密情報（オンラインバンキングや電子マネーシステムのパスワード）を盗んだり、ユーザーの金融情報にアクセスしたりするように設計された偽装 Web サイト（フィッシングサイト）もブロックします。危険サイトブロックは、Web サイトを開く前に、Kaspersky Security Network クラウドサービスを使用して、その Web サイトをスキャンします。スキャンが完了すると、信頼できる Web サイトが読み込まれ、悪意のある Web サイトはブロックされます。また、Kaspersky Security Network クラウドサービスで定義されたカテゴリを使用して Web サイトをフィルタリングすることもできます。これにより管理者は、Web サイトの特定のカテゴリ（例：「ギャンブル、宝くじ、懸賞」や「インターネットコミュニケーション」などのカテゴリに該当する Web サイト）へのユーザーのアクセスを制限できます。
- **アプリ管理：**この機能では、配布パッケージへの直リンクまたは Google Play へのリンクから、推奨アプリと必須アプリをデバイスにインストールできます。アプリ管理では、企業のセキュリティ要件に違反してブロックされているアプリを削除できます。
- **コンプライアンスコントロール：**管理対象デバイスが企業のセキュリティ要件に従っているかチェックし、従っていないデバイスの特定の機能を制限できます。

グループポリシーの設定を指定することにより、 Kaspersky Security Center Web コンソールと Cloud コンソールで、Kaspersky Endpoint Security for Android のコンポーネントを設定できます。

Kaspersky Security for iOS の概要

Kaspersky Security for iOS アプリは、フィッシングおよびマルウェアからモバイルデバイスを保護します。

Kaspersky Security for iOS アプリで提供する主な機能は、次の通りです：

- **危険サイトブロック**：悪意のあるコードを拡散するように設計された悪意のある Web サイトをブロックします。また、ユーザーの機密情報（オンラインバンキングや電子マネーシステムのパスワード）を盗んだり、ユーザーの金融情報にアクセスしたりするように設計された偽装 Web サイト（フィッシングサイト）もブロックします。危険サイトブロックは、Web サイトを開く前に、Kaspersky Security Network クラウドサービスを使用して、その Web サイトをスキャンします。スキャンが完了すると、信頼できる Web サイトが読み込まれ、悪意のある Web サイトはブロックされます。グループポリシーの設定を指定することにより、Kaspersky Security Center Web コンソールでこのコンポーネントを設定できます。
- **ジェイルブレイクの検知**：Kaspersky Security for iOS がジェイルブレイクを検知すると、重大な問題であることを示すメッセージが表示され、この問題が通知されます。

Kaspersky Security for Mobile (Devices) プラグインの概要

Kaspersky Security for Mobile (Devices) プラグインを使用すると、Kaspersky Security Center Web コンソールと Cloud コンソールを使用して、モバイルデバイスとそのデバイスにインストールされたモバイルアプリを管理するインターフェイスが使用できます。Kaspersky Security for Mobile (Devices) プラグインを使用すると次が実行可能になります：

- モバイルデバイスと Kaspersky Security Center の接続。
- モバイルデバイスの証明書の管理。
- Firebase Cloud Messaging の設定（Android デバイスのみ）。
- モバイルデバイスへのコマンドの送信（Android デバイスのみ）。

Kaspersky Security for Mobile (Devices) プラグインは、Kaspersky Security Center Web コンソールの設定時にインストール可能です。Kaspersky Security Center Cloud コンソールを使用中の場合は、このプラグインのインストールは不要です。異なる種別のコンソールでの導入シナリオの詳細は、「導入シナリオ」セクションを参照してください。

Kaspersky Security for Mobile (Policies) プラグインの概要

Kaspersky Security for Mobile (Policies) プラグインを使用すると、Kaspersky Security Center に接続されたデバイスの設定を、グループポリシーを使用して編集できます。Kaspersky Security for Mobile (Policies) プラグインを使用すると次が実行可能になります：

- モバイルデバイスのためのグループセキュリティポリシーを作成する。
- ユーザーのモバイルデバイスのモバイルアプリの動作を遠隔で設定する。
- ユーザーのモバイルデバイスのモバイルアプリの動作に関するレポートと統計情報を受信する。

Kaspersky Security for Mobile (Policies) プラグインは、Kaspersky Security Center Web コンソールの設定時にインストール可能です。Kaspersky Security Center Cloud コンソールを使用中の場合は、このプラグインのインストールは不要です。異なる種別のコンソールでの導入シナリオの詳細は、「導入シナリオ」セクションを参照してください。

システム要件

このセクションには、Kaspersky Security Center Web コンソールと Cloud コンソールでの Kaspersky Security for Mobile (Devices) プラグインと Kaspersky Security for Mobile (Policies) プラグインのインストールに必要な管理者用コンピューターのシステム要件と、モバイルアプリのシステム要件を一覧として記載しています。

管理者用コンピューターのシステム要件

Kaspersky Security for Mobile (Devices) プラグインと Kaspersky Security for Mobile (Policies) プラグインをインストールするには、管理者用コンピューターが Kaspersky Security Center のハードウェア要件を満たしている必要があります。Kaspersky Security Center のシステム要件の詳細情報：

- Kaspersky Security Center Web コンソールを使用している場合、*Kaspersky Security Center のヘルプ*を参照してください。
- Kaspersky Security Center Cloud コンソールを使用している場合、*Kaspersky Security Center Cloud コンソールのヘルプ*を参照してください。

Kaspersky Security for Mobile (Devices) プラグインと Kaspersky Security for Mobile (Policies) プラグインを Kaspersky Security Center Web コンソールで使用するには、管理者のコンピューターに Kaspersky Security Center Web コンソールがインストールされている必要があります。

Kaspersky Security for Mobile (Devices) プラグインと Kaspersky Security for Mobile (Policies) プラグインを Kaspersky Security Center Cloud コンソールで使用するには、Kaspersky Security Center Cloud コンソールのアカウントを作成する必要があります。アカウントの作成の詳細は、*Kaspersky Security Center Cloud コンソールのヘルプ*を参照してください。

Kaspersky Endpoint Security for Android モバイルアプリは、次のサードパーティ製 EMM システムの中で使用できます：

- VMware AirWatch 9.3 以降
- MobileIron バージョン 10.0 以降
- IBM MaaS360 バージョン 10.68 以降
- Microsoft Intune 1908 以降
- SOTI MobiControl 14.1.4（1693）以降

Kaspersky Endpoint Security for Android のインストールに必要な、モバイルデバイスのシステム要件

Kaspersky Endpoint Security for Android のシステム要件は次の通りです：

- 画面解像度が 320 x 480 ピクセル以上のスマートフォンまたはタブレット
- デバイスのメインメモリの空き容量：65 MB
- Android 5.0〜12（Go Edition 以外の Android 12L を含む）
- x86、x86-64、Arm5、Arm6、Arm7、Arm8 プロセッサアーキテクチャ

本アプリは、デバイスのメインメモリにのみインストールされます。

Kaspersky Security for iOS のインストールに必要な、モバイルデバイスのシステム要件

Kaspersky Security for iOS アプリのハードウェア要件は次の通りです：

- iPhone 6S 以降
- iPad Air 2 以降

Kaspersky Security for iOS アプリのソフトウェア要件は次の通りです：

- iOS 14.1 以降
- iPadOS 14.1 以降

Kaspersky Security for iOS アプリは、アクティブな VPN 接続がある VPN クライアントが同一デバイスで実行されていると、正しく動作しません。

既知の問題と注意点

Kaspersky Endpoint Security for Android と Kaspersky Security for iOS には既知の問題がありますが、アプリの動作には重大な影響を与えません。

Kaspersky Security for iOS の既知の問題

- Kaspersky Security for iOS アプリは、アクティブな VPN 接続がある VPN クライアントが同一デバイスで実行されていると、正しく動作しません。

Kaspersky Endpoint Security for Android の既知の問題

Kaspersky Security Center Web コンソールでモバイルデバイスの管理を開始する場合の既知の問題

- Kaspersky Security Center の MMC ベースの管理コンソールの初期設定時（クイックスタートウィザードの実行中）か、後で管理コンソールで［モバイルデバイス管理］フォルダーを表示することで、モバイルデバイス管理を開始できます。

アプリのインストールに関する既知の問題

- Kaspersky Endpoint Security for Android は、デバイスの内部ストレージにのみインストール可能です。
- Android バージョン 7.0 以降のデバイスでは、Kaspersky Endpoint Security for Android の管理者権限をデバイスの設定で無効にしようとするとエラーが発生する場合があります。これは、Kaspersky Endpoint Security for Android による他のウィンドウ上のオーバーレイが禁止されている場合に発生します。この問題は、Android 7 の既知の問題によるものです。
- Android バージョン 7.0 以降のデバイスの Kaspersky Endpoint Security for Android は、マルチウィンドウに対応していません。
- Kaspersky Endpoint Security for Android は、Chrome オペレーティングシステムの Chromebook では動作しません。
- Kaspersky Endpoint Security for Android は、Android Go エディションのデバイスでは動作しません。
- Kaspersky Endpoint Security for Android アプリをサードパーティの EMM システム（VMware AirWatch など）で使用する場合は、アンチウイルスと危険サイトブロックのみが使用可能です。管理者は、EMM システムのコンソールで、アンチウイルスと危険サイトブロックを設定できます。この場合、アプリの動作に関する通知は、Kaspersky Endpoint Security for Android アプリにのみ表示されます（レポート）。

本アプリのアップグレードに関する既知の問題

- Kaspersky Endpoint Security for Android は、現在より新しいバージョンにのみアップグレード可能です。旧バージョンへのダウングレードはできません。

アンチウイルスの動作に関する既知の問題

- 技術的な制限により、Kaspersky Endpoint Security for Android はサイズが 2 GB 以上のファイルをスキャンできません。スキャン中、そのようなファイルがスキップされたことを通知せずに、ファイルはスキップされます。

- 定義データベースに情報が追加されていない新しい脅威がデバイスに存在するかどうかを分析する場合は、Kaspersky Security Network の使用を有効にする必要があります。*Kaspersky Security Network（KSN）*は、ファイル、Web リソース、ソフトウェアの評価に関する情報を含むカスペルスキーのオンラインナレッジベースへのアクセスを提供する、クラウドサービスの基盤です。KSN を使用するには、モバイルデバイスがインターネットに接続している必要があります。

- 管理サーバーからモバイルデバイスへの定義データベースのアップデートが失敗する場合があります。その場合、定義データベースのアップデートタスクを管理サーバーで実行してください。

- 一部のデバイスでは、USB OTG で接続されたデバイスを Kaspersky Endpoint Security for Android が検出しません。検出されないデバイスに対しては、ウイルススキャンができません。

- Android 11.0 以降のデバイスでは、ユーザーは「すべてのファイルへのアクセス」権限を付与する必要があります。

- Android バージョン 7.0 以降のデバイスでは、ウイルススキャンのスケジュールを設定する画面が正しく表示されない場合があります（管理に関する項目が非表示になります）。この問題は、Android 7 の既知の問題によるものです。

- Android 7.0 のデバイスで、拡張モードのリアルタイム保護によって外付け SD カード上に保存されたファイル内の脅威が検知されません。

- Android バージョン 6.0 のデバイスでは、悪意のあるファイルがデバイスのストレージにコピーされた場合、Kaspersky Endpoint Security for Android は検知しません。アンチウイルスが悪意のあるファイルを検知する可能性があるのは、悪意のあるファイルの実行中、デバイスのウイルススキャンの実行中です。この問題は、Android 6.0 の既知の問題によるものです。デバイスのセキュリティを確保するために、ウイルススキャンのスケジュールを設定しておくことを推奨します。

危険サイトブロックに関する既知の問題

- 危険サイトブロックは、Google Chrome（カスタムタブ機能を含む）、Huawei Browser、Samsung Internet Browser でのみ動作します。

- 危険サイトブロックを使用するには、Kaspersky Security Network の使用を有効にする必要があります。危険サイトブロックは、サイトの評価およびカテゴリに関する KSN のデータに基づいてサイトをブロックします。

- Android バージョン 6.0 以上で Google Chrome バージョン 51 以前がインストールされているデバイスでは、ブロック対象のサイトが危険サイトブロックでブロックされない場合があります。これは、サイトが次の方法で開かれている場合に発生します（この問題は Google Chrome の既知の問題によるものです）：

  - 検索結果から開いた場合
  - ブックマークリストから開いた場合
  - 検索履歴から開いた場合
  - URL をオートコンプリートで入力した場合
  - Google Chrome の新しいタブで Web サイトを開いた場合

- Google Chrome バージョン 50 以前がインストールされているデバイスでは、ブロック対象のサイトが危険サイトブロックでブロックされない場合があります。これは、サイトが**タブとアプリの統合**機能をブラウザーの設定で有効にし、Google の検索履歴からサイトを開くと発生します。この問題は、Google Chrome の既知の問題によるものです。

- ブロック対象カテゴリのサイトが Google Chrome でブロックされない場合があります。これは、サイトをサードパーティ製のアプリ（メッセンジャークライアントのアプリなど）から開くと発生します。この問題は、ユーザー補助機能サービスの Chrome カスタムタブ機能に対する動作に関係しています。

- ブロック対象のサイトが Samsung Internet Browser でブロックされない場合があります。これは、コンテキストメニューまたはサードパーティ製アプリ（メッセンジャークライアントのアプリなど）からバックグラウンドモードでサイトを開くと発生します。

- 危険サイトブロックを正常に動作させるには、Kaspersky Endpoint Security for Android をユーザー補助機能として設定しておく必要があります。

- 危険サイトブロックの［**リストの Web サイトのみを許可する**］を有効にして指定したサイトが、Samsung Internet Browser でページを更新すると、ブロックされる場合があります。正規表現が詳細な表現を含む場合（`^https?:\/\/example\.com\/pictures\/` など）、サイトがブロックされます。詳細な表現を含まない、`^https?:\/\/example\.com` などの正規表現の使用を推奨します。

盗難対策の動作に関する既知の問題

- Android デバイスへのタイムリーなコマンド送信を目的として、本アプリは Firebase Cloud Messaging（FCM）サービスを使用します。FCM を設定していない場合、ポリシーで設定したスケジュール（24 時間ごとなど）に基づいて Kaspersky Security Center とデバイスが同期される時のみにコマンドが送信されます。

- デバイスをロックするには、Kaspersky Endpoint Security for Android をデバイス管理者として設定しておく必要があります。

- Android 7.0 以降のデバイスをロックするには、Kaspersky Endpoint Security for Android をユーザー補助機能として設定しておく必要があります。

- 一部のデバイスでは、盗難対策コマンドの実行に失敗する場合があります。これは、デバイスの省電力モードを有効にしていると発生します。この問題は、Alcatel 5080X での発生が確認されています。

- Android 10.0 以降のデバイスの位置情報を特定するには、位置情報へのアクセス権を常に許可するように設定する必要があります。

アプリ管理の動作に関する既知の問題

- アプリ管理を正常に動作させるには、Kaspersky Endpoint Security for Android をユーザー補助機能として設定しておく必要があります。

- アプリ管理（アプリのカテゴリ）を使用するには、Kaspersky Security Network の使用を有効にする必要があります。アプリ管理が使用するアプリのカテゴリは、KSN で使用可能なデータに基づいて決定します。KSN を使用するには、モバイルデバイスがインターネットに接続している必要があります。アプリ管理では、個別のアプリを許可またはブロックする対象のリストに追加できます。この場合、KSN の使用は不要です。

- アプリ管理の設定時には、［**システムアプリをブロックする**］をオフにすることを推奨します。システムアプリをブロックすると、デバイスの動作に問題が生じる可能性があります。

デバイスのロック解除パスワードの長さに関する既知の問題

- Android 10.0 以降のデバイスでは、パスワードの強度要件（中程度または高強度）がシステムの値として実装されます。

  1～4 文字のパスワード長が必要な場合、中程度の強度のパスワードを設定するようユーザーに要求します。重複したり順番（例：1234）に並んでいたりしない数字（PIN）か、英字と数字の組み合わせである必要があります。PIN またはパスワードは、4 文字以上である必要があります。

  5 文字以上のパスワード長が必要な場合、高強度のパスワードを設定するようユーザーに要求します。重複したり順番に並んでいたりしない数字（PIN）か、英字と数字の組み合わせ（パスワード）である必要があります。PIN は 8 文字以上の数字で、パスワードは 6 文字以上である必要があります。

- Android バージョン 7.1.1 のデバイスでは、ロック解除パスワードが企業のセキュリティ要件（コンプライアンスコントロール）を満たさない場合、そのパスワードを Kaspersky Endpoint Security for Android で変更しようとすると、Settings アプリ（システムアプリ）が正しく動作しない場合があります。この問題は、Android 7.1.1 の既知の問題によるものです。この場合、ロック解除パスワードを変更するには、Settings アプリ（システムアプリ）を使用するしか方法がありません。

- 一部の Android バージョン 6.0 以降のデバイスでは、画面のロックを解除するパスワードを入力するとエラーが発生する場合があります。これは、デバイスのデータを暗号化していると発生します。この問題は、MIUI ファームウェア端末のユーザー補助サービスの特定の機能に関係しています。

アプリを削除から保護する際の既知の問題

- Kaspersky Endpoint Security for Android をデバイス管理者に設定しておく必要があります。

- Android 7.0 以降のデバイスでアプリが削除されないように保護するには、Kaspersky Endpoint Security for Android をユーザー補助機能として設定しておく必要があります。

- 一部の Xiaomi または Huawei デバイスでは、Kaspersky Endpoint Security for Android を削除から保護できません。この問題は、Xiaomi の MIUI 7 / 8 ファームウェアおよび Huawei の EMUI ファームウェアの特定の機能によるものです。

デバイスの制限の設定に関する既知の問題

- Android 10.0 以降のデバイスでは、Wi-Fi ネットワークの使用の禁止はサポートされていません。

- Android 10 以降のデバイスの場合、カメラの使用を完全には禁止できません。

- Android バージョン 11 以降のデバイスでは、Kaspersky Endpoint Security for Android をユーザー補助機能として設定しておく必要があります。初期設定ウィザードで Kaspersky Endpoint Security for Android をユーザー補助機能として設定するよう要求されます。このステップはスキップできます。また、後からデバイスの設定でサービスを無効にすることもできます。この場合、カメラの使用を制限することはできません。

モバイルデバイスにコマンドを送信する際の既知の問題

- Android 12 以降を実行しているデバイスでは、ユーザーが［おおよその位置情報］の権限を付与していても、 Kaspersky Endpoint Security for Android は最初に正確な位置情報を取得しようとします。これが成功しなかった場合、コマンドが 30 分以内に送信された場合のみ、おおよその位置情報が返されます。そうでない場合は **GPS 追跡**は失敗します。

特定のデバイスで発生する既知の問題

- 一部のデバイス（Huawei、Meizu、Xiaomi など）では、Kaspersky Endpoint Security for Android に自動起動の権限を許可するか、オペレーティングシステム起動時に開始するアプリのリストに Kaspersky Endpoint Security for Android を手動で追加する必要があります。本アプリがリストに追加されていない場合、Kaspersky Endpoint Security for Android はモバイルデバイスの再起動後に全機能の実行を停止します。また、デバイスがロックされると、デバイスのロック解除コマンドを使用できません。デバイスのロックを解除するには、ロック解除用のワンタイムパスワードを使用するしか方法はありません。

- Android バージョン 6.0 以降の一部の Android デバイス（Meiz や Asus など）では、データを暗号化し、Android デバイスを再起動した後、デバイスのロックを解除するには、数字のパスワードの入力が必要です。パターンパスワードをデバイスのロック解除に使用している場合、ロック方法を数字のパスワードに変更する必要があります。パターンパスワードを数値のパスワードへ変換する方法の詳細は、モバイルデバイス製造元のテクニカルサポートサイトを参照してください。この問題は、ユーザー補助機能サービスの動作に関係しています。

- Android バージョン 5.X の Huawei デバイスでは、Kaspersky Endpoint Security for Android にユーザー補助機能を設定すると、十分な権限が不足しているという誤ったメッセージが表示されます。このメッセージを非表示にするには、デバイスの設定で、本アプリを保護されたアプリに設定する必要があります。

- Android バージョン 5.X または 6.X の Huawei デバイスでは、省電力モードを Kaspersky Endpoint Security for Android に対して有効にすると、本アプリを手動で終了できます。終了すると、ユーザーのデバイスは保護されなくなります。この問題は、Huawei 製ソフトウェアの一部の機能に由来します。デバイスの保護を再度有効にするには、Kaspersky Endpoint Security for Android を手動で起動してください。デバイスの設定で、本アプリのバッテリーセーバーモードを無効にすることを推奨します。

- EMUI ファームウェアを搭載した Android バージョン 7.0 の Huawei デバイスでは、Kaspersky Endpoint Security for Android による保護機能に関する通知を非表示にできます。この問題は、Huawei 製ソフトウェアの一部の機能に由来します。

- 一部の Xiaomi デバイスでは、ポリシーでパスワードの長さを 5 文字以上に設定すると、ロック解除用パスワードを PIN コードの代わりに変更するように要求する通知が表示されます。5 文字を超える PIN コードは設定できません。この問題は、Xiaomi ソフトウェアの一部の機能に由来します。

- MIUI ファームウェアを搭載した Android バージョン 6.0 の Xiaomi デバイスでは、Kaspersky Endpoint Security for Android のアイコンがステータスバー上で非表示になる場合があります。この問題は、Xiaomi ソフトウェアの一部の機能に由来します。通知の設定でアイコン表示を許可することを推奨します。

- Android バージョン 6.0.1 の Nexus デバイスでは、Kaspersky Endpoint Security for Android のクイックスタートウィザード中に、正しい動作に必要な権限が許可されません。この問題は、Google 提供の Android 用セキュリティパッチの既知の問題によるものです。正常に動作させるには、デバイスの設定で必要な権限を手動で設定する必要があります。

- 一部の Android バージョン 7.0 以降の Samsung デバイスでは、デバイスがサポートしていないロック解除方法（パターンパスワードなど）を設定しようとするとデバイスがロックされる場合があります。発生条件は次の通りです：Kaspersky Endpoint Security for Android の削除からの保護が有効で、ロック解除のパスワードの強度要件を設定している場合。デバイスのロックを解除するには、特別なコマンドをデバイスに送信する必要があります。

- 一部の Samsung デバイスでは、画面のロック解除に指紋認証を使用することをブロックできません。

- 一部の Samsung デバイスでは、危険サイトブロックを有効にできません。これは、デバイスが 3G/4G ネットワークに接続し、省電力モードを有効にしており、バックグラウンドデータをブロックしていると発生します。バッテリーセーバーの設定で、バックグラウンドデータをブロックする設定を無効にすることを推奨します。

- 一部の Samsung デバイスでは、ロック解除用パスワードが企業のセキュリティ要件に準拠していない場合、Kaspersky Endpoint Security for Android は画面のロック解除での指紋認証の使用をブロックしません。

- 一部の Honor デバイスと Huawei デバイスで、Bluetooth の使用を制限できません。本アプリが Bluetooth の使用の制限を試行すると、オペレーティングシステムが通知を表示します。通知には、この制限を拒否するか許可するか選択するオプションが含まれています。ユーザーはこの制限を拒否して Bluetooth の使用を継続できます。

- Blackview デバイスでは、ユーザーは Kaspersky Endpoint Security for Android のメモリを消去できます。その結果、デバイスの保護と管理は無効になり、すべての定義された設定も無効になり、Kaspersky Endpoint Security for Android はユーザー補助機能から削除されます。これはこの製造元の端末が、カスタマイズされた最近の画面のアプリに強い権限を付与しているためです。このアプリは Kaspersky Endpoint Security for Android の設定より優先され、また Android のオペレーティングシステムの一部であるため、置き換えることはできません。

- Android 11 の一部のデバイスで、Kaspersky Endpoint Security for Android が起動直後にクラッシュします。この問題は、既知の Android 11 の問題 によるものです。

Kaspersky Security Center Web コンソールまたは Cloud コンソールでのモバイルデバイス管理ソリューションの導入

Kaspersky Security Center Web コンソールまたは Cloud コンソールを使用してモバイルデバイスを管理するには、モバイルデバイス管理ソリューションを導入する必要があります。

導入シナリオ

Kaspersky Security Center Web コンソールでの導入

Kaspersky Security Center Web コンソールでのモバイルデバイス管理ソリューションの導入のステップは次の通りです：

1. **Kaspersky Security Center Web コンソールの導入準備**
2. **管理プラグインの導入**
3. **モバイルアプリの導入**
4. **（任意、Android のみ）Firebase Cloud Messaging との情報交換の設定**

   このステップを実行し、モバイルデバイスへのコマンドのタイムリーな配信と、ポリシー設定の変更時の強制的な同期がされるように設定することを推奨します。

Kaspersky Security Center Cloud コンソールでの導入

Kaspersky Security Center Cloud コンソールでのモバイルデバイス管理ソリューションの導入のステップは次の通りです：

1. **Kaspersky Security Center Cloud コンソールの導入準備**
2. **モバイルアプリの導入**

❸ （任意、Android のみ）Firebase Cloud Messaging との情報交換の設定

このステップを実行し、モバイルデバイスへのコマンドのタイムリーな配信と、ポリシー設定の変更時の強制的な同期がされるように設定することを推奨します。

Kaspersky Security Center Web コンソールと Cloud コンソールの導入準備

このセクションでは、Kaspersky Security Center Web コンソールと Cloud コンソールの導入準備について説明します。

モバイルデバイスを接続するための管理サーバーの設定

モバイルデバイスが管理サーバーへ接続できるようにするには、Kaspersky Endpoint Security for Android または Kaspersky Security for iOS をモバイルデバイスにインストールする前に、モバイルデバイスの接続設定を管理サーバーのプロパティで指定する必要があります。

モバイルデバイスの接続のために管理サーバーの設定を指定するには：

1. 管理サーバーでモバイルデバイス管理を開始します。

   Kaspersky Security Center の MMC ベースの管理コンソールの初期設定時（クイックスタートウィザードの実行中）か、後で管理コンソールで［モバイルデバイス管理］フォルダーを表示することで、モバイルデバイス管理を開始できます。

2. Kaspersky Security Center Web コンソールまたは Cloud コンソールのメインウィンドウで、**設定**（）をクリックします。

   管理サーバーのプロパティウィンドウが表示されます。

3. モバイルデバイスが使用する管理サーバーのポートを設定します：

   a. ［**追加のポート**］セクションを選択します。

   b. ［**モバイルデバイス用ポートを開く**］切り替えスイッチをオンにします。

   c. ［**モバイルデバイスとの同期用のポート**］フィールドで、モバイルデバイスが管理サーバーへの接続に使用するポートを指定します。

      既定ではポート 13292 が使用されます。

      ［**モバイルデバイス用ポートを開く**］がオフの場合や、接続ポートの指定が正しくない場合、モバイルデバイスは管理サーバーに接続できません。

   d. ［**モバイルデバイスのアクティベーション用のポート**］で、モバイルアプリのアクティベート時に、モバイルデバイスが管理サーバーへの接続に使用するポートを指定します。

      既定ではポート 17100 が使用されます。

      指定した接続ポートが正しくない場合、モバイルデバイスのユーザーは、管理サーバーを使用して モバイルアプリをアクティベートすることができません。

4. 必要に応じて、管理サーバーへの接続にモバイルデバイスが使用する証明書を編集します。

既定では、管理サーバーは、管理サーバーのインストール中に作成された証明書を使用します。必要に応じて、管理サーバーが発行した証明書を別の証明書に置換するか、管理サーバーが発行した証明書を再発行します。

証明書を編集するには：

a. ［**証明書**］セクションを選択します。

b. 必要な設定を指定します。

証明書に関する詳細情報は、*Kaspersky Security Center のヘルプ*を参照してください。

5. ［**保存**］をクリックして設定の変更を保存し、管理サーバーのプロパティウィンドウを終了します。

モバイルデバイスの接続設定の編集後、Kaspersky Endpoint Security for Android または Kaspersky Security for iOS をモバイルデバイスにインストールし、指定した設定を使用して管理サーバーへ接続することができます。

管理グループの作成

グループポリシーは、ユーザーのモバイルデバイスにインストールされている Kaspersky Endpoint Security for Android と Kaspersky Security for iOS の一元的な設定を実行する目的で使用されます。

デバイスグループにポリシーを適用するために、ユーザーのデバイスにモバイルアプリをインストールする前に、**管理対象デバイス**にこれらのデバイス用の独立したグループを作成しておくことを推奨します。

管理グループの作成後、アプリをインストールするデバイスをこのグループに自動的に割り当てるオプションを設定することを推奨します。グループポリシーを使用して、全デバイスに共通の設定を編集します。

管理グループを作成するには：

1. Kaspersky Security Center Web コンソールまたは Cloud コンソールのメインウィンドウで、［**デバイス**］→［**グループ階層構造**］の順に選択します。

2. 管理グループ構造で、新しい管理グループを含める管理グループを選択します。

3. ［**追加**］をクリックします。

4. **表示される**［**新しい管理グループ**の名前］ウィンドウで、グループの名前を入力し、［**追加**］をクリックします。

指定した名前の新しい管理グループが、管理グループの階層に表示されます。

デバイスを管理グループに自動的に割り当てるためのルールの作成

Kaspersky Endpoint Security for Android と Kaspersky Security for iOS アプリがモバイルデバイスにインストールされると、Kaspersky Security Center Web コンソールまたは Cloud コンソールの［**検出と製品の導入**］→［**未割り当てデバイス**］ページに表示されます。新しく接続されたデバイスを管理するには、管理グループへ手動で移動するか、管理グループへ自動的に割り当てるルールを作成します。

管理グループへのモバイルデバイスの自動的な割り当てルールを作成するには：

1. Kaspersky Security Center Web コンソールまたは Cloud コンソールのメインウィンドウで、［**検出と製品の導入**］→［**導入と割り当て**］→［**移動ルール**］の順に選択します。

2. ［**新規ルール**］ウィンドウが開いたら、［**追加**］をクリックします。

3. ［**ルール名**］フィールドで、ルール名を指定します。

4. アプリをモバイルデバイスにインストールした後に、そのデバイスを割り当てる管理グループを、［**管理グループ**］フィールドで選択します。

5. ［**ルールの適用**］セクションで、［**各デバイスにつき 1 回**］を選択します。

6. ［**どの管理グループにも属していないデバイスのみ移動する**］をオンにすると、ルールを適用する時に、他の管理グループに割り当て済みのモバイルデバイスは、選択したグループに割り当てられません。

7. ［**ルールを有効にする**］をオンにして、ルールの作成後にすぐに適用します。
   ［**移動ルール**］ページの切り替えスイッチを使用して、任意のタイミングでルールを有効化できます。

8. ［**ルールの条件**］→［**アプリケーション**］の順に選択し、次を実行します：

   a. ［**OS のバージョン**］切り替えスイッチをオンにします。

   b. 表示される OS のリストで、［**Android**］または［**iOS**］を選択します。

   対応するデバイスにルールが適用されます。少なくとも 1 つの条件を指定してルールを作成する必要があります。

9. ［**保存**］をクリックしてルールを作成します。

［**移動ルール**］ページに、新規作成したルールが表示されます。ルールに従い、Kaspersky Security Center は新しく接続されたデバイスを、選択した管理グループへ割り当てます。

管理グループの管理、未割り当てデバイスへの処理の詳細：

- Kaspersky Security Center Web コンソールを使用している場合、*Kaspersky Security Center のヘルプ*を参照してください。
- Kaspersky Security Center Cloud コンソールを使用している場合、*Kaspersky Security Center Cloud コンソールのヘルプ*を参照してください。

管理プラグインの導入

Kaspersky Security Center Web コンソールでモバイルデバイスを管理するには、次の管理プラグインをインストールする必要があります：

- Kaspersky Security for Mobile (Devices) プラグイン
- Kaspersky Security for Mobile (Policies) プラグイン

> Kaspersky Security Center Cloud コンソールを使用中の場合は、管理プラグインのインストールは不要です。Kaspersky Security Center Cloud コンソールでのアカウントの作成のみが必要です。アカウントの作成の詳細は、*Kaspersky Security Center Cloud コンソールのヘルプ*を参照してください。

管理プラグインのインストールに使用可能な方法は次の通りです：

- Kaspersky Security Center Web コンソールのクイックスタートウィザードを使用する。

  管理サーバーのインストール後、管理サーバーへの初回接続時に、クイックスタートウィザードの実行が自動的に要求されます。クイックスタートウィザードは、いつでも手動で開始できます。

  Kaspersky Security Center のクイックスタートウィザードの詳細は、*Kaspersky Security Center のヘルプ*を参照してください。

- Kaspersky Security Center Web コンソールで使用可能な配布パッケージのリストを使用する。

  使用可能な配布パッケージのリストは、新しいバージョンのカスペルスキー製品の公開後に自動的にアップデートされます。

- 配布パッケージを外部のソースからダウンロードし、管理プラグインを Kaspersky Security Center Web コンソールに追加します。

  たとえば、カスペルスキーの Web サイトから管理プラグインの配布パッケージをダウンロードできます。

使用可能な配布パッケージのリストからの管理プラグインのインストール

管理プラグインをインストールするには：

1. Kaspersky Security Center Web コンソールのメインウィンドウで、［**コンソールの設定**］→［**WEB プラグイン**］の順に選択します。
2. ［**追加**］をクリックします。

   最新バージョンのカスペルスキー製品を含むリストが表示されます。
3. 管理プラグインをインストールします：
   a. 使用可能なアプリケーションのリストで、［**モバイルデバイス**］セクションを選択し展開します。
   b. ［**Kaspersky Security for Mobile (Devices)**］を選択し、［**プラグインのインストール**］をクリックします。
   c. ［**Kaspersky Security for Mobile (Policies)**］を選択し、［**プラグインのインストール**］をクリックします。

配布パッケージがダウンロードされ、プラグインがインストールされます。各プラグインが Kaspersky Security Center Web コンソールへインストール、追加されると、確認のウィンドウが表示されます。

配布パッケージからの管理プラグインのインストール

配布パッケージはカスペルスキーの Web サイトでダウンロード可能です。

Kaspersky Security for Mobile (Devices) プラグインを配布パッケージからインストールするには：

1. 配布パッケージの圧縮ファイル `on_prem_ksm_devices_xx.x.x.x.zip` から `plugin.zip` と `signature.txt` を管理者のワークステーションにコピーします。
2. Kaspersky Security Center Web コンソールのメインウィンドウで、［**コンソールの設定**］→［**WEB プラグイン**］の順に選択します。

3. ［**ファイルから追加**］をクリックします。

4. 表示される［**ファイルから追加**］ウィンドウで、［**ZIP ファイルのアップロード**］をクリックし、`plugin.zip` を参照し指定します。

5. ［**署名のアップロード**］をクリックし、`signature.txt` を参照し指定します。

6. ［**追加**］をクリックします。

Kaspersky Security for Mobile (Devices) プラグインが Kaspersky Security Center Web コンソールにインストール、追加されます。

Kaspersky Security for Mobile (Policies) プラグインを配布パッケージからインストールするには：

1. 配布パッケージの圧縮ファイル `on_prem_ksm_policies_xx.x.x.x.zip` から `plugin.zip` と `signature.txt` を管理者のワークステーションにコピーします。

2. Kaspersky Security Center Web コンソールのメインウィンドウで、［**コンソールの設定**］→［**WEB プラグイン**］の順に選択します。

3. ［**ファイルから追加**］をクリックします。

4. 表示される［**ファイルから追加**］ウィンドウで、［**ZIP ファイルのアップロード**］をクリックし、`plugin.zip` を参照し指定します。

5. ［**署名のアップロード**］をクリックし、`signature.txt` を参照し指定します。

6. ［**追加**］をクリックします。

Kaspersky Security for Mobile (Policies) プラグインが Kaspersky Security Center Web コンソールにインストール、追加されます。

［**コンソールの設定**］→［**WEB プラグイン**］ページに表示されるインストール済みプラグインのリストで、管理プラグインがインストールされたことを確認できます。

モバイルアプリの導入

Kaspersky Security Center Web コンソールまたは Cloud コンソールでモバイルデバイスを管理するには、Kaspersky Endpoint Security for Android または Kaspersky Security for iOS をモバイルデバイスに導入する必要があります。Kaspersky Security Center Web コンソールまたは Cloud コンソールを使用して、アプリをモバイルデバイスに導入できます。

Kaspersky Security Center Web コンソールまたは Cloud コンソールを使用したモバイルアプリの導入

モバイルアプリは、ユーザーアカウントが Kaspersky Security Center に追加されているユーザーのモバイルデバイスにインストールされます。Kaspersky Security Center のユーザーアカウントの詳細は、次を参照してください：

- Kaspersky Security Center Web コンソールを使用している場合、*Kaspersky Security Center のヘルプ* を参照してください。

- Kaspersky Security Center Cloud コンソールを使用している場合、*Kaspersky Security Center Cloud コンソールのヘルプ*を参照してください。

Kaspersky Security for Mobile (Devices) プラグインを使用して、モバイルデバイスにリンクを送信することにより、Kaspersky Security Center Web コンソールおよび Cloud コンソールからアプリをインストールできます。

- Android デバイスの場合、ユーザーは、Kaspersky Endpoint Security for Android アプリをダウンロードするための Google Play リンクを受信します。アプリは、次に示す Android プラットフォームの標準的なインストール方法でインストールできます。アプリのインストール後、ユーザーは必要な権限を許可する必要があります。

  Huawei および Honor の一部のデバイスは、Google サービスが使用できないので、Google Play のアプリへアクセスできません。Huawei および Honor の一部の端末のユーザーが Google Play からアプリをインストールできない場合は、Huawei AppGallery からインストールする必要があります。

- iOS デバイスの場合、ユーザーは、Kaspersky Security for iOS アプリをダウンロードするための App Store リンクを受信します。アプリは、次に示す iOS プラットフォームの標準的なインストール方法でインストールできます。

  接続のセキュリティを強化するために、iOS デバイスを接続する前に、Kaspersky Security Center のアドレスをデバイスユーザーに送信します。アプリのインストール中にこのアドレスがユーザーに表示されます。表示されるアドレスと受信したアドレスが一致しない場合は、接続をキャンセルできます。

リンクには次のデータが含まれています：

- Kaspersky Security Center の同期設定
- 証明書

モバイルデバイスにアプリを導入するには：

1. モバイルデバイス接続ウィザードを開始します：

   - Kaspersky Security Center Web コンソールまたは Cloud コンソールのメインウィンドウで、［**デバイス**］→［**モバイル**］→［**デバイス**］の順に選択し、［**追加**］をクリックします。
   - Kaspersky Security Center Web コンソールまたは Cloud コンソールのメインウィンドウで、［**ユーザーとロール**］→［**ユーザー**］の順に選択します。モバイルデバイスを接続するためのリンクを送信するユーザーまたはユーザーグループの名前をクリックし、［**デバイス**］**を選択します。**［**モバイルデバイスを追加**］をクリックします。この場合は、ステップ 3 をスキップします。

   ［**次へ**］を使用して、ウィザードを続行します。

2. 追加するデバイスのオペレーティングシステムを選択します：

   - **Android**
   - **iOS / iPadOS**

3. モバイルデバイスを接続するためのリンクを送信するユーザーまたはユーザーグループを選択します。

4. リンクの送信先のメールアドレスを選択します：

- **すべてのメールアドレス**
- **メインのメールアドレス**
- **予備のメールアドレス**
- **別のメールアドレス**
  このオプションを選択する場合は、下のメールアドレスを指定してください。

5. リンクの概要が表示されます。
   リンクのすべてのパラメータが正しいことを確認し、［**送信**］をクリックします。
6. モバイルデバイスを追加するためのリンクが送信されたことを確認するウィンドウが開きます。
   ［**OK**］をクリックしてウィザードを終了します。

Kaspersky Endpoint Security for Android または Kaspersky Security for iOS アプリをユーザーがインストールすると、Web コンソールまたは Cloud コンソールの［**デバイス**］→［**モバイル**］→［**デバイス**］タブに、ユーザーデバイスが表示されます。アプリをユーザーのモバイルデバイスにインストールした後、グループポリシーを使用してデバイスとアプリを設定できます。また、デバイスの紛失や盗難時には、データ保護のためにモバイルデバイスにコマンドを送信することもできます（Android のみ）。

モバイルアプリのアクティベート

Kaspersky Security Center では、ライセンスによってその適用対象の機能が異なります。Kaspersky Endpoint Security for Android と Kaspersky Security for iOS を完全に機能させるには、組織が購入した Kaspersky Security Center ライセンスを**モバイルデバイス管理**機能のために使用する必要があります。**モバイルデバイス管理**機能は、モバイルデバイスを Kaspersky Security Center に接続し、接続されたデバイスを管理することを目的としています。

Kaspersky Security Center のライセンスとライセンスオプションの詳細は、次を参照してください：

- Kaspersky Security Center Web コンソールを使用している場合、*Kaspersky Security Center のヘルプ*を参照してください。
- Kaspersky Security Center Cloud コンソールを使用している場合、*Kaspersky Security Center Cloud コンソールのヘルプ*を参照してください。

モバイルデバイスでの Kaspersky Endpoint Security for Android と Kaspersky Security for iOS のアクティベートは、有効なライセンス情報を本アプリに追加することで完了します。ライセンス情報は、Kaspersky Security Center とモバイルデバイスの同期時に、ポリシーと一緒にデバイスに送信されます。

デバイスにインストールされた時点から 30 日以内にモバイルアプリのアクティベーションが完了しなかった場合、アプリは自動的に機能制限モードに切り替わります。このモードでは、ほとんどのアプリ機能は機能しません。機能制限モードに切り替わると、本アプリは Kaspersky Security Center との自動同期を停止します。そのため、何らかの理由で本アプリのアクティベーションがインストール後 30 日以内に完了しなかった場合、ユーザーは手動でデバイスを Kaspersky Security Center と同期させる必要があります。

Kaspersky Security Center が組織に導入されていない場合、またはモバイルデバイスからアクセスできない場合、ユーザーはモバイルアプリをデバイス上で手動でアクティベートできます。

モバイルアプリをアクティベートするには：

1. ポリシーのプロパティウィンドウを開きます：

- Kaspersky Security Center Web コンソールまたは Cloud コンソールのメインウィンドウで、［**デバイス**］→［**ポリシーとプロファイル**］の順に選択します。開いたグループポリシーのリストで、設定するポリシーの名前をクリックします。

- Kaspersky Security Center Web コンソールまたは Cloud コンソールのメインウィンドウで、［**デバイス**］→［**モバイル**］→［**デバイス**］の順に選択します。設定するポリシーの適用対象であるモバイルデバイスをクリックし、［**アクティブなポリシーとポリシーのプロファイル**］タブでポリシーを選択します。

2. ポリシーのプロパティページで、［**アプリケーション設定**］→［**ライセンス**］の順に選択します。

3. ドロップダウンリストを使用して、管理サーバーのライセンス保管領域から必要なライセンスを選択します。

   ライセンスの詳細は、下のフィールドに表示されます。

   上記のドロップダウンリストで選択したものと異なる場合は、モバイルデバイスの既存のアクティベーション用ライセンスを置換できます。置換するには、［**デバイスのライセンスが異なる場合は、このライセンスと置き換える**をオンにします。

4. ［**保存**］をクリックして、ポリシーに加えた変更を保存し、ポリシーのプロパティウィンドウを終了します。

モバイルデバイスと Kaspersky Security Center との次回の同期時に、デバイスに設定が適用されます。

Kaspersky Endpoint Security for Android アプリへの必要な権限の許可

Kaspersky Endpoint Security for Android アプリの一部の機能には、権限が必要です。Kaspersky Endpoint Security for Android は、インストール中、インストール後、アプリの各機能の使用前に、必須の権限を要求します。必須権限を提供せずに Kaspersky Endpoint Security for Android をインストールすることはできません。

一部のデバイス（Huawei、Meizu、Xiaomi など）では、デバイスの設定で、オペレーティングシステム起動時に開始するアプリのリストに Kaspersky Endpoint Security for Android を手動で追加する必要があります。本アプリがリストに追加されていない場合、Kaspersky Endpoint Security for Android はモバイルデバイスの再起動後に全機能の実行を停止します。

Android 11.0 以降のデバイスでは、システム設定［**アプリが使用されていない場合に権限を削除**］を無効にする必要があります。無効にしないと、本アプリが数か月使用されなかった場合、ユーザーが本アプリに付与した権限がシステムによって自動的にリセットされます。

Kaspersky Endpoint Security for Android により要求される権限

権限	アプリの機能
電話（Android 5.0～9.X でのみ必要）	Kaspersky Security Center への接続（デバイス ID）
ストレージ（必須）	アンチウイルス

すべてのファイルへのアクセス	危険サイトブロック（Android 11 以降のみ）
付近の Bluetooth デバイス（Android 12 以降）	Bluetooth の使用制限
デバイス管理者（必須）	盗難対策 ー デバイスのロック（Android 5.0～6.X のみ）
	盗難対策 - フロントカメラによる遠隔撮影 Kaspersky Security Center Web コンソールと Cloud コンソールでは遠隔撮影はサポートされていませんが、Kaspersky Endpoint Security for Android アプリは、すべての Kaspersky Security Center コンソールでこの機能を管理可能にするために、この権限を必要とします。
	盗難対策 - アラーム音
	盗難対策 - 完全リセット
	パスワードによる保護
	アプリ削除に対する保護
	セキュリティ証明書のインストール
	アプリ管理
	カメラ、Bluetooth、Wi-Fi の使用制限
カメラ	盗難対策 - フロントカメラによる遠隔撮影 Kaspersky Security Center Web コンソールと Cloud コンソールでは遠隔撮影はサポートされていませんが、Kaspersky Endpoint Security for Android アプリは、すべての Kaspersky Security Center コンソールでこの機能を管理可能にするために、この権限を必要とします。 Android 11.0 以降のデバイスでは、デバイスに要求された際に、アクセス権をアプリの使用中のみ許可するように設定する必要があります。
位置情報	盗難対策 - デバイスの GPS 追跡 Android 10.0 以降のデバイスでは、デバイスに要求された際に、アクセス権を常に許可するように設定する必要があります。
ユーザー補助	盗難対策 - デバイスのロック（Android 7.0 以降のみ）
	危険サイトブロック
	アプリ管理
	アプリ削除に対する保護（Android 7.0 以降のみ）

	Kaspersky Endpoint Security for Android による警告の表示（Android 10.0 以降のみ）
	カメラの使用の制限（Android 11 以降のみ）

証明書の管理

モバイル証明書は、管理サーバー上のモバイルデバイスのユーザーを識別する目的で使用されます。

Kaspersky Security Center Web コンソールおよび Cloud コンソールを使用すると、ユーザーのモバイル証明書を使用して次の操作が可能です：

- 証明書とそのステータスを表示します。
- 新しい証明書を作成します。
- 有効期限が切れる証明書を更新します。
- 証明書を削除します。

Kaspersky Security Center 証明書の詳細は、次を参照してください：

- Kaspersky Security Center Web コンソールを使用している場合、*Kaspersky Security Center のヘルプ*を参照してください。
- Kaspersky Security Center Cloud コンソールを使用している場合、*Kaspersky Security Center Cloud コンソールのヘルプ*を参照してください。

証明書リストの表示

Kaspersky Security Center Web コンソールと Cloud コンソールを使用すると、適用されたユーザーモバイル証明書、それらのステータス、およびプロパティを表示できます。

適用されたユーザーモバイル証明書のリストを表示するには：

1. Kaspersky Security Center Web コンソールまたは Cloud コンソールのメインウィンドウで、［**デバイス**］→［**モバイル**］→［**デバイス**］の順に選択します。
2. ［**証明書の管理**］を選択します。

［**モバイル証明書**］ページが開き、適用されたユーザーモバイル証明書の情報が表示されます。［**ユーザー名**］列で証明書をクリックすると、証明書の詳細を表示できます。

証明書の設定の指定

Kaspersky Security Center Web コンソールまたは Cloud コンソールを使用して、モバイル証明書の有効期間、自動更新、パスワードによる保護を設定できます。

モバイル証明書の設定を指定するには：

1. Kaspersky Security Center Web コンソールまたは Cloud コンソールのメインウィンドウで、［**デバイス**］→［**モバイル**］→［**デバイス**］の順に選択します。

2. ［**証明書の管理**］を選択します。

3. ［**証明書の設定**］を選択します。

4. 表示される［**モバイル証明書を生成**］ウィンドウで、次の項目を設定できます：

   - **パスワードの有効期間（日）**

     証明書の有効期間（日）。既定の証明書の有効期間は 365 日です。この期間を経過すると、モバイルデバイスが管理サーバーへ接続できなくなります。

   - **証明書の有効期間が次の日数になったら再発行する（日）**

     現在の証明書の有効期限までの残り日数。指定した日数以内に、管理サーバーが新しい証明書を発行する必要があります。たとえば、このフィールドの値が「4」の場合、 管理サーバーは新しい証明書を現在の証明書の有効期限が切れる 4 日前に発行します。既定値は 1 です。

   - **可能な場合、証明書を自動的に再発行する**

     可能な場合、証明書を自動的に再発行します。このオプションをオフにすると、有効期限が切れた証明書を手動で再発行する必要があります。既定では、このオプションはオフです。

   - **証明書のインストール中にパスワードを要求する**

     証明書がモバイルデバイスへインストールされると、パスワードの入力がユーザーへ要求されます。このパスワードは、モバイルデバイスへの証明書のインストール中に 1 回のみ使用されます。管理サーバーがこのパスワードを自動的に生成し、ユーザーへメールで送信します。［**パスワードの長さ**］フィールドで、パスワードの長さを指定できます。

5. ［**保存**］をクリックして変更を適用し、ウィンドウを閉じます。

指定した設定は、Kaspersky Security Center でのモバイル証明書の作成、アップデート、保護に使用されます。

証明書の作成

Kaspersky Security Center Web コンソールまたは Cloud コンソールで、モバイルデバイスのユーザーを識別する目的でモバイル証明書を作成できます。

モバイル証明書を作成するには：

1. Kaspersky Security Center Web コンソールまたは Cloud コンソールのメインウィンドウで、［**デバイス**］→［**モバイル**］→［**デバイス**］の順に選択します。

2. ［**証明書の管理**］を選択します。

3. 表示される［**モバイル証明書**］ウィンドウで［**追加**］をクリックし、**モバイル証明書作成ウィザード**を開始します。［**次へ**］を使用して、ウィザードを続行します。

4. 新しい証明書を使用して管理するモバイルデバイスのユーザーまたはユーザーグループを選択します。

5. **公開パラメータ**を指定します：

   - 新しい証明書についてユーザーに通知する場合は、［**新しい証明書をユーザーに通知**］をオンにします。

- 1つの証明書を同一のデバイスで複数回使用することを許可するには、［**1つの証明書を同一のデバイスで複数回使用することを許可（Kaspersky Endpoint Security for Android がインストールされたデバイスのみ）**］をオンにします。

6. **認証の種別**を選択します：

   - 証明書へのアクセスにユーザーの資格情報を使用させる場合は、［**資格情報（ドメインログインまたはユーザー名）**］を選択します。

   - 証明書へのアクセスにワンタイムパスワードを使用させる場合は、［**ワンタイムパスワード**］を選択します。

     ［**1つの証明書を同一のデバイスで複数回使用することを許可（Kaspersky Endpoint Security for Android がインストールされたデバイスのみ）**］を前のステップでオンにしていない場合のみ、このオプションは使用可能です。

   - 証明書へのアクセスにパスワードを使用させる場合は、［**パスワード**］を選択します。

     ［**1つの証明書を同一のデバイスで複数回使用することを許可（Kaspersky Endpoint Security for Android がインストールされたデバイスのみ）**］を前のステップでオンにした場合のみ、このオプションは使用可能です。

7. 証明書の配信方法を、［**証明書の配信**］フィールドで選択します。

   - ［**ワンタイムパスワード**］を前のステップで選択した場合、次のオプションのうち1つを選択します：

     - パスワードをメールで送信する場合、［**ユーザーにメールで通知**］を選択します。

       次に、使用するメードアドレスを選択するか、［**別のメールアドレス**］を選択して別のメールアドレスを指定します。

     - 別の方法でパスワードをユーザーに通知する場合は、［**ウィザードの終了後にパスワードを表示**］を選択します。

   - ［**資格情報（ドメインログインまたはユーザー名）**］を前のステップで選択した場合は、使用するメールアドレスを選択するか、［**別のメールアドレス**］を選択して別のメールアドレスを指定します。

8. 証明書の概要が表示されます。

   すべてのパラメータが正しいことを確認し、［**作成**］をクリックします。

これにより、**モバイル証明書作成ウィザード**によってユーザーがモバイルデバイスにインストールできる証明書が作成されます。証明書は、モバイルデバイスと Kaspersky Security Center の次回の同期後に使用可能になります。

証明書の作成と、証明書発行のためのルールの設定に関する詳細：

- Kaspersky Security Center Web コンソールを使用している場合、*Kaspersky Security Center のヘルプ*を参照してください。
- Kaspersky Security Center Cloud コンソールを使用している場合、*Kaspersky Security Center Cloud コンソールのヘルプ*を参照してください。

証明書の更新

適用されたモバイル証明書のいずれかの有効期限がまもなく切れる場合は、Kaspersky Security Center Web コンソールまたは Cloud コンソールを使用して更新できます。

モバイル証明書を更新するには：

1. Kaspersky Security Center Web コンソールまたは Cloud コンソールのメインウィンドウで、［**デバイス**］→［**モバイル**］→［**デバイス**］の順に選択します。
2. ［**証明書の管理**］を選択します。
3. 更新する証明書を選択し、［**再発行**］をクリックします。

   証明書のステータスが、「**証明書が再発行されました**」に変更されます。

証明書の削除

Kaspersky Security Center Web コンソールまたは Cloud コンソールを使用して、モバイル証明書を削除できます。

モバイル証明書を削除すると、デバイスは管理サーバーと同期できなくなり、Kaspersky Security Center を使用して管理できなくなります。モバイルデバイスの管理を開始するには、Kaspersky Endpoint Security for Android アプリを再インストールする必要があります。

モバイル証明書を削除するには：

1. Kaspersky Security Center Web コンソールまたは Cloud コンソールのメインウィンドウで、［**デバイス**］→［**モバイル**］→［**デバイス**］の順に選択します。
2. ［**証明書の管理**］を選択します。
3. 削除する証明書を選択し、［**削除**］をクリックします。

   証明書が削除され、証明書リストから削除されます。

Firebase Cloud Messaging との情報交換

Kaspersky Endpoint Security for Android は、Firebase Cloud Messaging（FCM）サービスを使用して、ポリシーの設定が変更された時にコマンドや強制同期をタイムリーに実行します。

Firebase Cloud Messaging サービスを使用するには、Kaspersky Security Center Web コンソールまたは Cloud コンソールでこのサービスを設定する必要があります。

Kaspersky Security Center Web コンソールまたは Cloud コンソールで Firebase Cloud Messaging を有効にするには：

1. Kaspersky Security Center Web コンソールまたは Cloud コンソールのメインウィンドウで、［**デバイス**］→［**モバイル**］→［**Android デバイスの同期**］の順に選択します。

   ［**Android デバイスの同期**］ウィンドウが開きます。
2. ［**送信者 ID** ］フィールドと［**サーバー鍵**フィールドで、Firebase Cloud Messaging の設定である SENDER_ID と API キーを指定します。

Firebase Cloud Messaging が有効になります。

送信者 ID とサーバー鍵を取得するには：

1. Google ポータルに登録します。
2. Google Cloud Platformへ移動します。
3. プロジェクトを新規作成します。
   プロジェクトが作成されるのを待ちます。
4. 関連するプロジェクトの SENDER_ID を検索します。
5. Google Firebase Cloud Messaging for Android を有効にします。
6. 画面上の指示に従い、資格情報を作成します。
7. 新しく作成された資格情報のプロパティから API キーを取得します。

Google Cloud Platform での動作の詳細は、Google Cloud のドキュメントを参照してください。

これで、Firebase Cloud Messaging 設定を編集する**送信者 ID** と、**サーバー鍵**ができました。

Firebase Cloud Messaging が設定されていない場合、モバイルデバイスのコマンドは、ポリシーで設定されたスケジュールに従ってデバイス と Kaspersky Security Center が同期される時に実行されます（たとえば 24 時間ごと）。つまり、コマンドやポリシーの設定は、すぐには反映されません。

本アプリの主要な機能をサポートする目的で、本アプリのインストールの一意な識別子（インスタンス ID）と次のデータを Firebase Cloud Messaging サービスに自動的に提供することにお客様は同意するものとします：

- インストールされた本ソフトウェアに関する情報：アプリのバージョン、アプリの識別子、アプリのビルドバージョン、アプリのパッケージ名。
- 本ソフトウェアがインストールされた端末に関する情報：OS バージョン、デバイスの識別子、Google サービスのバージョン。
- FCM に関する情報：FCM 内のアプリの識別子、FCM のユーザーの識別子、プロトコルのバージョン。

データはセキュアな通信で Firebase サービスへ転送されます。情報へのアクセスと保護は、Firebase サービスの関連する利用規約によって規制されています：Firebase データ処理とセキュリティ規約、 Firebaseのプライバシーとセキュリティ。

Firebase Cloud Messaging サービスとの情報交換を停止するには：

1. Kaspersky Security Center Web コンソールまたは Cloud コンソールのメインウィンドウで、［**デバイス**］→［**モバイル**］→［**Android デバイスの同期**］の順に選択します。
   ［**Android デバイスの同期**］ウィンドウが開きます。
2. ［**リセット**］をクリックします。
3. 開いたウィンドウで、［**OK**］をクリックしてリセットを確認します。

Firebase Cloud Messaging の設定がクリアされます。

Kaspersky Security Center Web コンソールまたは Cloud コンソールでのモバイルデバイス管理

グループポリシーの使用およびモバイルデバイスへのコマンドの送信により、Kaspersky Security Center Web コンソールと Cloud コンソールでモバイルデバイスを管理できます（Android のみ）。

Kaspersky Security Center Web コンソールでモバイルデバイスを管理するには、管理プラグインをインストールする必要があります。

モバイルデバイスと Kaspersky Security Center の接続

Kaspersky Security Center Web コンソールまたは Cloud コンソールを使用してモバイルデバイスを管理するには、デバイスが Kaspersky Security Center へ接続されている必要があります。Kaspersky Security Center に接続されたデバイスのリストは、Web コンソールまたは Cloud コンソールの［**デバイス**］→［**モバイル**］→［**デバイス**］タブに表示されます。

接続のセキュリティを強化するために、iOS デバイスを接続する前に、Kaspersky Security Center のアドレスをデバイスユーザーに送信します。アプリのインストール中にこのアドレスがユーザーに表示されます。表示されるアドレスと受信したアドレスが一致しない場合は、接続をキャンセルできます。

デバイスと Kaspersky Security Center を接続するには：

1. モバイルデバイス接続ウィザードを開始します：

   - Kaspersky Security Center Web コンソールまたは Cloud コンソールのメインウィンドウで、［**デバイス**］→［**モバイル**］→［**デバイス**］の順に選択し、［**追加**］をクリックします。
   - Kaspersky Security Center Web コンソールまたは Cloud コンソールのメインウィンドウで、［**ユーザーとロール**］→［**ユーザー**］の順に選択します。モバイルデバイスを接続するためのリンクを送信するユーザーまたはユーザーグループの名前をクリックし、［**デバイス**］**を選択します。**［**モバイルデバイスを追加**］をクリックします。この場合は、ステップ 3 をスキップします。

   ［**次へ**］を使用して、ウィザードを続行します。

2. 追加するデバイスのオペレーティングシステムを選択します：

   - **Android**
   - **iOS / iPadOS**

3. モバイルデバイスを接続するためのリンクを送信するユーザーまたはユーザーグループを選択します。

4. リンクの送信先のメールアドレスを選択します：

   - **すべてのメールアドレス**
   - **メインのメールアドレス**

- **予備のメールアドレス**
- **別のメールアドレス**
  このオプションを選択する場合は、下のメールアドレスを指定してください。

5. リンクの概要が表示されます。
   リンクのすべてのパラメータが正しいことを確認し、［**送信**］をクリックします。

6. モバイルデバイスを追加するためのリンクが送信されたことを確認するウィンドウが開きます。
   ［OK］をクリックしてウィザードを終了します。

Kaspersky Endpoint Security for Android または Kaspersky Security for iOS アプリをユーザーがインストールすると、Web コンソールまたは Cloud コンソールの［**デバイス**］→［**モバイル**］→［**デバイス**］タブに、ユーザーデバイスが表示されます。

未割り当てのモバイルデバイスの管理グループへの移動

Kaspersky Endpoint Security for Android と Kaspersky Security for iOS アプリがモバイルデバイスにインストールされると、Kaspersky Security Center Web コンソールまたは Cloud コンソールの［**検出と製品の導入**］→［**未割り当てデバイス**］ページに表示されます。新しく接続されたデバイスを管理するには、管理グループへ自動的に割り当てするルールを作成するか、手動で管理グループへ移動する必要があります。

未割り当てのモバイルデバイスを管理グループへ移動するには：

1. Kaspersky Security Center Web コンソールまたは Cloud コンソールのメインウィンドウで、［**検出と製品の導入**］→［**未割り当てデバイス**］の順に選択します。

2. 管理グループへ移動するデバイスを選択し、［**グループへ移動**］をクリックします。

3. 表示される管理グループのツリーで、デバイスの移動先となるグループを選択します。
   既存のグループを選択し［**子グループを追加**］をクリックすると、管理グループを新規作成できます。

4. ［**移動**］をクリックします。

指定した管理グループへデバイスが移動され、グループポリシーが適用されます。

モバイルデバイスへのコマンドの送信

Android モバイルデバイスへコマンドを送信し、デバイスの紛失または盗難時にデータを保護したり、Kaspersky Security Center とデバイスとの強制同期を実行したりできます。

iOS デバイスにコマンドを送信することはできません。

以下のコマンドがサポートされています：

- **デバイスのロック**
  モバイルデバイスがロックされます。

- **デバイスのロック解除**

モバイルデバイスのロックが解除されます。Android 5.0 - 6.X のモバイルデバイスでロックを解除すると、画面ロックの解除パスワード（PIN コード）は「1234」にリセットされます。Android 7.0 以降のデバイスでは、ロックの解除後も画面ロックの解除パスワードは変更されません。

- **出荷時の設定にリセットする**

  すべてのデータがモバイルデバイスから削除され、設定が既定値にロールバックされます。

- **企業データを消去する**

  コンテナー化されたデータと企業メールアカウントは、モバイルデバイスから消去されます。

- **GPS 追跡**

  デバイスの位置が追跡され、Google Maps に表示されます。インターネットアクセス料金がモバイルサービスプロバイダーより請求される場合があります。

  Android 12 以降を実行しているデバイスでは、ユーザーが［おおよその位置情報］の権限を付与していても、 Kaspersky Endpoint Security for Android は最初に正確な位置情報を取得しようとします。これが成功しなかった場合、コマンドが 30 分以内に送信された場合のみ、おおよその位置情報が返されます。そうでない場合は **GPS 追跡**は失敗します。

- **音声アラーム**

  モバイルデバイスのアラームが作動します。アラームは 5 分間鳴動します（デバイスのバッテリーが少ない場合は 1 分）。

- **デバイスを同期**

  モバイルデバイスが、Kaspersky Security Center と同期されます。

Kaspersky Endpoint Security for Android には、コマンドを実行するための特定の権限が必要です。初期設定ウィザードの実行時に、必要な権限を Kaspersky Endpoint Security for Android に付与するよう要求されます。このステップはスキップできます。また、後からデバイスの設定で権限を無効にすることもできます。その場合、コマンドを実行することはできません。

Android 10.0 以降のデバイスの場合、位置情報へのアクセス権を常に許可するように設定する必要があります。Android 11.0 以降のデバイスの場合、カメラへのアクセス権をアプリの使用時のみ許可するように設定する必要があります。設定しない場合、盗難対策コマンドが動作しません。制限に関する通知が表示され、必要なレベルのアクセス権を許可するように再度要求されます。カメラへのアクセス権を今回のみ許可するオプションをユーザーが選択すると、本アプリはアクセス権が許可されたと判断します。カメラへのアクセス権が再度要求される場合は、ユーザーに直接確認することを推奨します。

モバイルデバイスへコマンドを送信するには：

1. Kaspersky Security Center Web コンソールまたは Cloud コンソールのメインウィンドウで、［**デバイス**］→［**モバイル**］→［**デバイス**］の順に選択します。
2. コマンドの送信先のデバイスを選択し、［**コントロール**］または［**管理**］をクリックします。
3. 必要なコマンドを**使用可能なコマンド**のリストから選択し、［OK］をクリックします。
4. 操作の確定を要求された場合、［OK］をクリックします。

指定したコマンドがモバイルデバイスへ送信され、確認のウィンドウが表示されます。

Kaspersky Security Center からモバイルデバイスを削除

モバイルデバイスの管理が不要となった場合、Web コンソールまたは Cloud コンソールを使用して、Kaspersky Security Center からデバイスを削除できます。

Kaspersky Security Center からモバイルデバイスを削除するには：

1. デバイスからモバイルアプリを削除するか、ユーザーが当該デバイスからアプリを削除したことを確認します。
2. Kaspersky Security Center Web コンソールまたは Cloud コンソールのメインウィンドウで、［**デバイス**］→［**モバイル**］→［**デバイス**］の順に選択します。
3. 削除するモバイルデバイスを選択し、［**削除**］をクリックします。
4. ［OK］をクリックし、操作を確定します。

デバイスが Kaspersky Security Center から削除されます。

グループポリシーの管理

このセクションでは、Kaspersky Security Center Web コンソールまたは Cloud コンソールでグループポリシーを管理する方法について説明します。

モバイルデバイスを管理するためのグループポリシー

*グループポリシー*とは、管理グループに属するモバイルデバイスと、これらのデバイスにインストールされているモバイルアプリを管理するための設定のパッケージです。

ポリシーを使用して、個々のデバイスとデバイスのグループの両方の設定が行えます。デバイスのグループの場合、管理設定はグループポリシープロパティのウィンドウで設定できます。

ポリシーで表される各パラメータは「ロック」属性を持っています。これは、ネストされた階層レベル（ネストされたグループとセカンダリー管理サーバー）のポリシーの設定をローカルアプリ設定で変更できるかどうかを示します。

ポリシーで設定された値およびローカルアプリ設定の値は管理サーバーに保存された後、同期中にモバイルデバイスに送信され、現在の設定としてデバイスに保存されます。ロックされていない設定にユーザーが別の値を指定した場合、デバイスと管理サーバーの次回の同期中に、設定の新しい値が管理サーバーに送信され、管理者により以前に指定された値の代わりにアプリのローカル設定に保存されます。

Android モバイルデバイスに対する企業のセキュリティを最新に保つために、ユーザーのデバイスが企業のセキュリティ要件に準拠しているかを監視できます。

Kaspersky Security Center Web コンソールまたは Cloud コンソールでのポリシーと管理グループの管理に関する詳細：

- Kaspersky Security Center Web コンソールを使用している場合、*Kaspersky Security Center のヘルプ*を参照してください。

- Kaspersky Security Center Cloud コンソールを使用している場合、 *Kaspersky Security Center Cloud コンソールのヘルプ*を参照してください。

グループポリシーのリストの表示

Kaspersky Security Center Web コンソールまたは Cloud コンソールを使用すると、グループポリシーとそのステータスやプロパティを表示できます。

グループポリシーのリストを表示するには：

Kaspersky Security Center Web コンソールまたは Cloud コンソールのメインウィンドウで、［**デバイス**］→［**ポリシーとプロファイル**］の順に選択します。

概要が記載されたグループポリシーのリストが開きます。このページで、グループポリシーの作成、変更、コピー、移動、削除が可能です。

ポリシー導入の結果の表示

Kaspersky Security Center Web コンソールまたは Cloud コンソールを使用すると、グループポリシーとそのポリシーを適用される全デバイスの情報の分布図を表示できます。

グループポリシーの導入結果を表示するには：

1. Kaspersky Security Center Web コンソールまたは Cloud コンソールのメインウィンドウで、［**デバイス**］→［**ポリシーとプロファイル**］の順に選択します。
2. 表示されたグループポリシーのリストで、導入結果を表示したいポリシーの名前に隣接するチェックボックスをオンにして、［**導入**］をクリックします。

   ポリシーの導入結果のページが開きます。このページには、ポリシーの概要、ポリシーの分布図、このポリシーが適用される全デバイスの情報を表示するテーブルが含まれています。ポリシーのプロパティウィンドウは、［**ポリシーの設定**］をクリックすると開きます。

グループポリシーの作成

Kaspersky Security Center Web コンソールまたは Cloud コンソールで、モバイルデバイスを管理する目的でグループポリシーを作成できます。

グループポリシーを作成するには：

1. Kaspersky Security Center Web コンソールまたは Cloud コンソールのメインウィンドウで、［**デバイス**］→［**ポリシーとプロファイル**］の順に選択します。
2. 表示される Kaspersky Security Center グループポリシーで、［**現在のパス**］をクリックし、ポリシーを作成する管理グループを選択します。

   既定では、新しいグループポリシーは［**管理対象デバイス**］グループに適用されます。
3. ［**追加**］をクリックしてポリシー作成ウィザードを開始します。［**次へ**］を使用して、ウィザードを続行します。

4. プラットフォームに応じてアプリを選択します：

   - **Kaspersky Endpoint Security for Android**
   - **Kaspersky Security for iOS**

5. ［**名前**］に新しいポリシーの名前を入力します。既存のポリシーの名前を指定すると、その名前の末尾に「(1)」が自動的に付加されます。

6. ポリシーのステータスを選択します：

   - **アクティブ**

     作成したポリシーを管理サーバーに保存します。モバイルデバイスと管理サーバーが次に同期した時に、このポリシーがアクティブポリシーとしてデバイスで使用されます。

   - **非アクティブ**

     作成したポリシーをバックアップポリシーとして管理サーバーに保存します。このポリシーは、将来、特定のイベントが発生した後に有効になります。必要に応じて、非アクティブポリシーをアクティブステータスに切り替えることができます。

     > グループで1つのアプリについて複数のポリシーを作成できますが、一度に有効にできるポリシーは1つのみです。アクティブポリシーを新しく作成すると、それまでのアクティブポリシーは自動的にアクティブでなくなります。

7. ［**親ポリシーから設定を継承する**］または［**設定を子ポリシーへ強制的に継承させる**］の 2 つの継承オプションを有効または無効に設定できます。

   - ［**親ポリシーから設定を継承する**］を子の管理グループに対して有効にし、親ポリシーの一部の設定をロックすると、これらの設定は子グループで変更できなくなります。親ポリシーでロックされていない設定は変更可能です。
   - ［**親ポリシーから設定を継承する**］を子の管理グループに対して無効にすると、親ポリシーの一部の設定がロックされていても、子グループの設定をすべて変更できるようになります。
   - ［**設定を子ポリシーへ強制的に継承させる**］を親の管理グループで有効にすると、［**親ポリシーから設定を継承する**］がそれぞれの子ポリシーに対して有効になります。この場合、このオプションはどの子ポリシーに対しても無効にできません。親ポリシーでロックされた設定はすべて子グループに強制的に継承され、これらの設定は子グループで変更できません。
   - ［**管理対象デバイス**］グループのポリシーでは、［**親ポリシーから設定を継承する**］は設定に影響しません。［**管理対象デバイス**］グループにはそれより上位のグループが存在せず、ポリシーが継承されることがないためです。

   既定では、［**親ポリシーから設定を継承する**］は有効になっており、［**設定を子ポリシーへ強制的に継承させる**］は無効になっています。

8. 必要に応じて、新規作成したポリシーの設定を定義できます。設定するには、［**アプリケーション設定**］タブを開き、「ポリシー設定の定義」セクションの記載に従ってポリシー設定を定義します。

   または、後で設定することも可能です。

9. ［**保存**］をクリックし、ポリシーを作成します。

モバイルデバイスを管理する新しいグループポリシーが作成されます。

グループポリシーの変更

Kaspersky Security Center Web コンソールまたは Cloud コンソールで、グループポリシーの設定を編集できます。

グループポリシーを変更するには：

1. ポリシーのプロパティウィンドウを開きます：

   - Kaspersky Security Center Web コンソールまたは Cloud コンソールのメインウィンドウで、［**デバイス**］→［**ポリシーとプロファイル**］の順に選択します。開いたグループポリシーのリストで、設定するポリシーの名前をクリックします。

   - Kaspersky Security Center Web コンソールまたは Cloud コンソールのメインウィンドウで、［**デバイス**］→［**モバイル**］→［**デバイス**］の順に選択します。設定するポリシーの適用対象であるモバイルデバイスをクリックし、［**アクティブなポリシーとポリシーのプロファイル**］タブでポリシーを選択します。

2. ポリシーのプロパティウィンドウで［**アプリケーション設定**］を開き、「ポリシー設定の定義」セクションの記載に従ってポリシー設定を定義します。

   全般的な設定、設定の継承、イベントの記録と通知、ポリシープロファイルを編集したり、リビジョンの履歴を表示したりすることができます。詳細は、*Kaspersky Security Center のヘルプ*を参照してください。

3. ［**保存**］をクリックして、ポリシーに加えた変更を保存し、ポリシーのプロパティウィンドウを終了します。

モバイルデバイスと Kaspersky Security Center との次回の同期時に、デバイスに設定が適用されます。

グループポリシーのコピー

Kaspersky Security Center Web コンソールまたは Cloud コンソールで、グループポリシーのコピーを作成できます。

グループポリシーのコピーを作成するには：

1. Kaspersky Security Center Web コンソールまたは Cloud コンソールのメインウィンドウで、［**デバイス**］→［**ポリシーとプロファイル**］の順に選択します。

2. 表示されるグループポリシーのリストで、コピーを作成するポリシーの名前に隣接するチェックボックスをオンにして、［**コピー**］をクリックします。

3. 表示される管理グループツリーで、ポリシーのコピーを作成するグループを選択します。

   既存のグループを選択し［**子グループを追加**］をクリックすると、管理グループを新規作成できます。

4. ［**コピー**］をクリックします。

5. ［OK］をクリックし、操作を確定します。

ポリシーのコピーが、選択したグループの下に同名で作成されます。選択したグループへコピーまたは移動された各ポリシーのステータスは**非アクティブ**になります。ステータスは、いつでも**アクティブ**に変更できます。

新規作成、または移動されたポリシーと同名のポリシーが選択したグループに既に存在する場合、新規作成、または移動されたポリシーの名前に「(<次の連番>)」のインデックスが追加されます。例：(1)。

ポリシーを別の管理グループへ移動

Kaspersky Security Center Web コンソールまたは Cloud コンソールで、ポリシーを別の管理グループへ移動できます。

ポリシーを別の管理グループへ移動するには：

1. Kaspersky Security Center Web コンソールまたは Cloud コンソールのメインウィンドウで、［**デバイス**］→［**ポリシーとプロファイル**］の順に選択します。
2. 表示されるグループポリシーのリストで、別の管理グループへ移動するポリシーの名前に隣接するチェックボックスをオンにして、［**移動**］をクリックします。
3. 表示される管理グループのツリーで、ポリシーの移動先となるグループを選択します。
   既存のグループを選択し［**子グループを追加**］をクリックすると、管理グループを新規作成できます。
4. ［**移動**］をクリックします。
5. ［OK］をクリックし、操作を確定します。

ポリシーの継承プロパティによって結果が異なります。

- ポリシーが元のグループから継承されない場合、移動先のグループへ移動されます。
- ポリシーが元のグループから継承される場合、移動されません。代わりに、ポリシーのコピーが移動先のグループに作成されます。

選択したグループへコピーまたは移動された各ポリシーのステータスは**非アクティブ**になります。ステータスは、いつでも**アクティブ**に変更できます。

新規作成、または移動されたポリシーと同名のポリシーが選択したグループに既に存在する場合、新規作成、または移動されたポリシーの名前に「(<次の連番>)」のインデックスが追加されます。例：(1)。

グループポリシーの削除

Kaspersky Security Center Web コンソールまたは Cloud コンソールで、グループポリシーを削除できます。

現在の管理グループに継承されていないポリシーのみ削除できます。ポリシーが継承されている場合、継承元のポリシーが作成された上位のグループでのみ削除可能です。

グループポリシーを削除するには：

1. Kaspersky Security Center Web コンソールまたは Cloud コンソールのメインウィンドウで、［**デバイス**］→［**ポリシーとプロファイル**］の順に選択します。
2. 表示されるグループポリシーのリストで、削除するポリシーの名前に隣接するチェックボックスをオンにして、［**削除**］をクリックします。
3. ［OK］をクリックし、操作を確定します。

グループポリシーが削除されます。

ポリシー設定の定義

このセクションでは、モバイルデバイスを管理するためのKaspersky Security Center ポリシーの設定を定義する方法について説明します。

ポリシーの作成または変更時に、ポリシー設定を指定できます。

アンチウイルスによる保護の設定

これらのポリシー設定は、Android デバイスでのみ定義できます。

脅威、ウイルス、その他の悪意のあるアプリケーションを迅速に検知するため、リアルタイム保護とウイルススキャンの自動実行を設定する必要があります。

Kaspersky Endpoint Security for Android が検知するオブジェクトには、次の種別が含まれます：

- ウイルス、ワーム、トロイの木馬、悪意のあるツール
- アドウェア
- デバイスや個人情報に損害を与える目的で悪用される可能性のあるアプリ

技術的な制限により、Kaspersky Endpoint Security for Android はサイズが 2 GB 以上のファイルをスキャンできません。スキャン中、そのようなファイルはスキップされ、ファイルがスキップされたことは通知されません。

リアルタイム保護の設定

これらのポリシー設定は、Android デバイスでのみ定義できます。

リアルタイム保護を設定するには：

1. ポリシーのプロパティウィンドウを開きます：

- Kaspersky Security Center Web コンソールまたは Cloud コンソールのメインウィンドウで、［**デバイス**］→［**ポリシーとプロファイル**］の順に選択します。開いたグループポリシーのリストで、設定するポリシーの名前をクリックします。

- Kaspersky Security Center Web コンソールまたは Cloud コンソールのメインウィンドウで、［**デバイス**］→［**モバイル**］→［**デバイス**］の順に選択します。設定するポリシーの適用対象であるモバイルデバイスをクリックし、［**アクティブなポリシーとポリシーのプロファイル**］タブでポリシーを選択します。

2. ポリシーのプロパティウィンドウで、［**アプリケーション設定**］→［**脅威対策**］の順に選択します。

3. ［**アンチウイルス**］セクションで、モバイルデバイスのファイルシステムの保護を設定します：

   - 脅威に対するモバイルデバイスのリアルタイム保護を有効にするには、［**アンチウイルスによるリアルタイム保護を有効にする**］をオンにします。

   - 保護レベルを指定します：

     - Kaspersky Endpoint Security for Android でダウンロードフォルダーの新しいアプリとファイルのみをスキャンする場合は、［**新しいアプリのみをスキャン**］を選択します。

     - 脅威からのモバイルデバイスの拡張保護を有効にするには、［**すべてのアプリをスキャンし、ファイルの動作を監視**］を選択します。

       新たにインストールされたモバイルアプリに加え、デバイス上でユーザーが開くファイル、変更するファイル、移動するファイル、コピーするファイル、起動するファイル、保存するファイルがすべてスキャンされます。

       > Android バージョン 8.0 以降のデバイスでは、Kaspersky Endpoint Security for Android はユーザーが編集、移動、インストール、保存、コピーしたファイルをスキャンします。Kaspersky Endpoint Security for Android は、開かれた状態のファイル、またはコピー元のファイルをスキャンしません。

   - 新しくデバイスにインストールしたアプリの初回起動前に、Kaspersky Security Network サービスを使用して追加のスキャンを実行できるようにするには、［**Kaspersky Security Network による追加の保護**］をオンにします。

   - アドウェアや、デバイスやユーザーのデータに損害を与える目的で悪用される可能性があるアプリをブロックするには、［**アドウェア、オートダイヤラー、ユーザーに損害を与える目的でサイバー犯罪者に悪用される可能性があるアプリの検知**］をオンにします。

4. ［**アンチウイルス設定**］セクションで、脅威の検知時に実行する動作を選択します：

   - **削除し、ファイルのバックアップコピーを隔離に保存**

     検知したオブジェクトを自動的に削除します。ユーザー側での処理は必要ありません。オブジェクトを削除する前に、Kaspersky Endpoint Security for Android はファイルのバックアップコピーを作成し、隔離に保存します。

   - **削除**

     検知したオブジェクトを自動的に削除します。ユーザー側での処理は必要ありません。オブジェクトの削除前に、オブジェクトの削除に関する通知が一時的に表示されます。

   - **スキップ**

オブジェクトがスキップされると、Kaspersky Endpoint Security for Android はデバイス保護の問題についてユーザーに警告します。スキップされた脅威に関する情報は、アプリの［**状態**］セクションに表示されます。スキップされた各脅威について、脅威を除去するためにユーザーが実行できる処理が示されます。スキップされたオブジェクトのリストは、悪意のあるファイルが削除または移動された時などに変わることがあります。最新の脅威のリストを取得するには、完全スキャンを実行します。信頼性が高いレベルでデータを保護するには、検知されたすべての脅威を取り除きます。

5. ［**保存**］をクリックして、ポリシーに加えた変更を保存し、ポリシーのプロパティウィンドウを終了します。

モバイルデバイスと Kaspersky Security Center との次回の同期時に、デバイスに設定が適用されます。

モバイルデバイスでのウイルススキャンの自動実行の設定

これらのポリシー設定は、Android デバイスでのみ定義できます。

モバイルデバイスでのウイルススキャンの自動実行を設定するには：

1. ポリシーのプロパティウィンドウを開きます：

   - Kaspersky Security Center Web コンソールまたは Cloud コンソールのメインウィンドウで、［**デバイス**］→［**ポリシーとプロファイル**］の順に選択します。開いたグループポリシーのリストで、設定するポリシーの名前をクリックします。

   - Kaspersky Security Center Web コンソールまたは Cloud コンソールのメインウィンドウで、［**デバイス**］→［**モバイル**］→［**デバイス**］の順に選択します。設定するポリシーの適用対象であるモバイルデバイスをクリックし、［**アクティブなポリシーとポリシーのプロファイル**］タブでポリシーを選択します。

2. ポリシーのプロパティウィンドウで、［**アプリケーション設定**］→［**脅威対策**］の順に選択します。

3. アドウェアや、デバイスやユーザーのデータに損害を与える目的で悪用される可能性があるアプリをブロックするには、［**アドウェア、オートダイヤラー、ユーザーに損害を与える目的でサイバー犯罪者に悪用される可能性があるアプリの検知**］を［**デバイスのスキャン**］セクションでオンにします。

4. ［**脅威の検知時の処理**］リストで、次のオプションから1つ選択します：

   - **削除し、ファイルのバックアップコピーを隔離に保存**

     検知したオブジェクトを自動的に削除します。ユーザー側での処理は必要ありません。オブジェクトを削除する前に、Kaspersky Endpoint Security for Android はファイルのバックアップコピーを作成し、隔離に保存します。

   - **削除**

     検知したオブジェクトを自動的に削除します。ユーザー側での処理は必要ありません。オブジェクトの削除前に、オブジェクトの削除に関する通知が一時的に表示されます。

   - **スキップ**

オブジェクトがスキップされると、Kaspersky Endpoint Security for Android はデバイス保護の問題についてユーザーに警告します。スキップされた脅威に関する情報は、アプリの［**状態**］セクションに表示されます。スキップされた各脅威について、脅威を除去するためにユーザーが実行できる処理が示されます。スキップされたオブジェクトのリストは、悪意のあるファイルが削除または移動された時などに変わることがあります。最新の脅威のリストを取得するには、完全スキャンを実行します。信頼性が高いレベルでデータを保護するには、検知されたすべての脅威を取り除きます。

- **手動選択**

  Kaspersky Endpoint Security for Android アプリが、検知したオブジェクトに対して実行する処理を次から選択するよう要求する通知を表示します：**スキップ**、**削除**。

  複数のオブジェクトが検知された場合、［**手動選択**］が設定されている状態で、［**すべての脅威に適用**］をオンにすることにより、選択した同じ処理を各ファイルに適用できます。

Android 10.0 以降のモバイルデバイスで通知を表示させるには、Kaspersky Endpoint Security for Android をユーザー補助機能としておく必要があります。初期設定ウィザードで Kaspersky Endpoint Security for Android をユーザー補助機能として設定するよう要求されます。このステップはスキップできます。また、後からデバイスの設定でサービスを無効にすることもできます。この場合、Android のシステムウィンドウが表示され、検知したオブジェクトに対して実行する次の処理の選択を要求します：スキップ、削除。複数のオブジェクトに対して 1 つの処理を適用するには、Kaspersky Endpoint Security を開く必要があります。

5. ［**定期スキャン**］セクションでは、デバイスファイルシステムの自動完全スキャンを設定できます。

   次のいずれかのオプションを選択します：

   - **無効**

     デバイスファイルシステムのスキャンは自動的には開始されません。

   - **定義データベースのアップデート後**

     デバイスファイルシステムは、定義データベースがアップデートされるたびに自動的にスキャンされます。

   - **毎日**

     デバイスファイルシステムは毎日自動的にスキャンされます。

     このオプションを選択すると、［**開始時刻**］フィールドでスキャンの時刻を指定することもできます。

   - **毎週**

     デバイスファイルシステムは、週に 1 回自動的にスキャンされます。

     このオプションを選択すると、ドロップダウンリストを使用してスキャンを実行する曜日を選択し、［**開始時刻**］フィールドでスキャンの時刻を指定することもできます。

Android 12 以降のデバイスでは、バッテリー節約モードの場合、タスクの実行が指定よりも遅れる場合があります。

6. ［**保存**］をクリックして、ポリシーに加えた変更を保存し、ポリシーのプロパティウィンドウを終了します。

モバイルデバイスと Kaspersky Security Center との次回の同期時に、デバイスに設定が適用されます。

定義データベースのアップデートの設定

これらのポリシー設定は、Android デバイスでのみ定義できます。

定義データベースのアップデートを設定するには：

1. ポリシーのプロパティウィンドウを開きます：

   - Kaspersky Security Center Web コンソールまたは Cloud コンソールのメインウィンドウで、［**デバイス**］→［**ポリシーとプロファイル**］の順に選択します。開いたグループポリシーのリストで、設定するポリシーの名前をクリックします。

   - Kaspersky Security Center Web コンソールまたは Cloud コンソールのメインウィンドウで、［**デバイス**］→［**モバイル**］→［**デバイス**］の順に選択します。設定するポリシーの適用対象であるモバイルデバイスをクリックし、［**アクティブなポリシーとポリシーのプロファイル**］タブでポリシーを選択します。

2. ポリシーのプロパティウィンドウで、［**アプリケーション設定**］→［**定義データベースのアップデート**］の順に選択します。

3. ［**定義データベースのアップデート**］セクションで、ユーザーデバイスでの定義データベースの自動アップデートを設定します。

   次のいずれかのオプションを選択します：

   - **無効**

     定義データベースの自動アップデートが無効になります。

   - **毎日**

     定義データベースが毎日アップデートされます。

     このオプションを選択すると、［**アップデート時間**］フィールドでアップデート時間を指定することもできます。

   - **毎週**

     定義データベースが週に 1 回アップデートされます。

     このオプションを選択すると、［**アップデート時間**］フィールドでアップデート時刻を指定し、［**曜日**］ドロップダウンリストでアップデートを実行する曜日を指定することもできます。

   Android 12 以降のデバイスでは、バッテリー節約モードの場合、タスクの実行が指定よりも遅れる場合があります。

4. ［**定義データベースのアップデート元**］セクションで、定義データベースのアップデートを取得し、インストールする時の入手元を指定します：

   - **カスペルスキーのサーバー**

     定義データベースをユーザーデバイスにダウンロードするためのアップデート元として、カスペルスキーのアップデートサーバーを使用します。

   - **管理サーバー**

Kaspersky Security Center Web コンソールを使用する場合のみ使用可能です。

定義データベースをユーザーデバイスにダウンロードするためのアップデート元として、Kaspersky Security Center 管理サーバーのリポジトリを使用します。

- **その他のソース**

  定義データベースをユーザーデバイスにダウンロードするためのアップデート元として、サードパーティのサーバーを使用します。

  このオプションを選択する場合は、［**定義データベースのアップデート元に別のサーバーを使用する**］フィールドで HTTP サーバーのアドレスを指定する必要があります。

5. デバイスのローミング時に定義データベースのアップデートをスケジュールに従って実行するには、［**ローミング中の定義データベースのアップデート**］セクションで［**ローミング中の定義データベースのアップデートを許可する**］をオンにします。

6. ［**保存**］をクリックして、ポリシーに加えた変更を保存し、ポリシーのプロパティウィンドウを終了します。

モバイルデバイスと Kaspersky Security Center との次回の同期時に、デバイスに設定が適用されます。

デバイスのロック解除設定の指定

これらのポリシー設定は、Android デバイスでのみ定義できます。

Android デバイスをセキュアな状態にするには、デバイスのスリープモードの解除時に入力するパスワードの使用を設定する必要があります。

ロック解除用パスワードが弱い場合、デバイスでのユーザーの操作に制限をかけることができます（デバイスのロックなど）。コンプライアンスコントロールを使用して、制限を設定できます。

一部の Android バージョン 7.0 以降の Samsung デバイスでは、デバイスがサポートしていないロック解除方法（パターンパスワードなど）を設定しようとするとデバイスがロックされる場合があります。発生条件は次の通りです：Kaspersky Endpoint Security for Android の削除からの保護が有効で、ロック解除のパスワードの強度要件を設定している場合。デバイスのロックを解除するには、特別なコマンドをデバイスに送信する必要があります。

デバイスのロック解除用パスワードの強度を設定するには：

1. ポリシーのプロパティウィンドウを開きます：

   - Kaspersky Security Center Web コンソールまたは Cloud コンソールのメインウィンドウで、［**デバイス**］→［**ポリシーとプロファイル**］の順に選択します。開いたグループポリシーのリストで、設定するポリシーの名前をクリックします。

   - Kaspersky Security Center Web コンソールまたは Cloud コンソールのメインウィンドウで、［**デバイス**］→［**モバイル**］→［**デバイス**］の順に選択します。設定するポリシーの適用対象であるモバイルデバイスをクリックし、［**アクティブなポリシーとポリシーのプロファイル**］タブでポリシーを選択します。

2. ポリシーのプロパティウィンドウで、［**アプリケーション設定**］→［**脅威対策**］の順に選択します。

3. ロック解除用パスワードが設定されているかどうかをアプリで確認する場合は、［パスワードによる保護］セクションで［**画面のロック解除用パスワードの設定を要求する**］をオンにします。

   デバイスにシステムパスワードが設定されていない場合は、ユーザーが設定する必要があります。パスワードは管理者により定義されたパラメータに従って設定します。

4. パスワードを構成する文字数の最小値を指定します。

   指定可能な値：4 ～ 16 の文字。

   既定の最小文字数は 4 です。

   > Android 10.0 以降のデバイスでは、パスワードの強度要件（中程度または高強度）がシステムの値として実装されます。

   Android 10.0 以降のデバイスでは、値は次のルールに従って決定されます：

   - 1 ～ 4 文字のパスワード長が必要な場合、中程度の強度のパスワードを設定するようユーザーに要求します。重複したり順番（例：1234）に並んでいたりしない数字（PIN）か、英字と数字の組み合わせである必要があります。PIN またはパスワードは、4 文字以上である必要があります。

   - 5 文字以上のパスワード長が必要な場合、高強度のパスワードを設定するようユーザーに要求します。重複したり順番に並んでいたりしない数字（PIN）か、英字と数字の組み合わせ（パスワード）である必要があります。PIN は 8 文字以上の数字で、パスワードは 6 文字以上である必要があります。

5. ユーザーが指紋を使用して画面のロックを解除できるようにする場合は、［**指紋認証の使用を許可する（Android 9 以降のデバイスでのみ有効）**］をオンにします（Android 10 以降のデバイスでは、作業プロファイルでのみ有効）。ロック解除のパスワードが企業のセキュリティ要件に適合していない場合、画面のロック解除に指紋認証スキャナーを使用することはできません。

   > Android 10.0 以降を実行しているデバイスでは、指紋認証を使用した画面のロック解除はサポートされていません。

   > Kaspersky Endpoint Security for Android は、アプリへのサインイン時または購入の確認時の指紋認証スキャナーの使用は制限しません。

   > 一部の Samsung デバイスでは、画面のロック解除に指紋認証を使用することをブロックできません。

   > 一部の Samsung デバイスでは、ロック解除用パスワードが企業のセキュリティ要件に準拠していない場合、Kaspersky Endpoint Security for Android は画面のロック解除での指紋認証の使用をブロックしません。

   デバイス設定に指紋認証を追加した後、ユーザーは次の方法で画面のロックを解除できます：

   - 指紋認証スキャナーに指を押し当てる（メインの方法）。

   - ロック解除用パスワードを入力する（予備の方法）。

6. ［**保存**］をクリックして、ポリシーに加えた変更を保存し、ポリシーのプロパティウィンドウを終了します。

モバイルデバイスと Kaspersky Security Center との次回の同期時に、デバイスに設定が適用されます。

盗難時または紛失時のデバイスデータの保護の設定

これらのポリシー設定は、Android デバイスでのみ定義できます。

モバイルデバイスの紛失または盗難の発生時に企業データを保護するには、不正アクセスからの保護を設定する必要があります。

盗難または紛失したデバイスのデータを確実に保護するには、Kaspersky Endpoint Security for Android をユーザー補助機能として設定する必要があります。初期設定ウィザードで Kaspersky Endpoint Security for Android をユーザー補助機能として設定するよう要求されます。このステップはスキップできます。また、後からデバイスの設定でサービスを無効にすることもできます。

盗難または紛失時のデバイスデータの保護を設定するには：

1. ポリシーのプロパティウィンドウを開きます：

   - Kaspersky Security Center Web コンソールまたは Cloud コンソールのメインウィンドウで、［**デバイス**］→［**ポリシーとプロファイル**］の順に選択します。開いたグループポリシーのリストで、設定するポリシーの名前をクリックします。
   - Kaspersky Security Center Web コンソールまたは Cloud コンソールのメインウィンドウで、［**デバイス**］→［**モバイル**］→［**デバイス**］の順に選択します。設定するポリシーの適用対象であるモバイルデバイスをクリックし、［**アクティブなポリシーとポリシーのプロファイル**］タブでポリシーを選択します。

2. ポリシーのプロパティウィンドウで、［**アプリケーション設定**］→［**脅威対策**］の順に選択します。
3. ［**盗難対策**］セクションで、デバイスのロックを設定します：

   - ロック解除コードの文字数を指定します。
   - デバイスのロック時に表示されるテキストを指定します。

4. ［**保存**］をクリックして、ポリシーに加えた変更を保存し、ポリシーのプロパティウィンドウを終了します。

モバイルデバイスと Kaspersky Security Center との次回の同期時に、デバイスに設定が適用されます。

アプリ管理の設定

これらのポリシー設定は、Android デバイスでのみ定義できます。

*アプリ管理*は、モバイルデバイスにインストールされているアプリが企業のセキュリティ要件に準拠しているか確認します。Kaspersky Security Center では、管理者が企業のセキュリティ要件に従い、許可するアプリ、ブロックするアプリ、必須アプリ、および推奨アプリのリストを作成します。アプリ管理の結果に応じて、Kaspersky Endpoint Security は必須アプリおよび推奨アプリをインストールし、ブロック対象アプリを削除するよう要求します。モバイルデバイスでブロック対象アプリを起動することはできません。

Kaspersky Security Center Web コンソールおよび Cloud コンソールでは、事前定義されたルールを適用することにより、ユーザーのデバイス上のアプリを管理できます。［**アプリ管理**］で設定可能なルールは 2 種類です：アプリケーションルール、カテゴリルール。

アプリケーションルールは特定のアプリに適用され、**カテゴリルール**は事前定義されたカテゴリに属するすべてのアプリに適用されます。アプリのカテゴリは、カスペルスキーのエキスパートによって指定されています。

***アプリ管理**を設定するには：*

1. ポリシーのプロパティウィンドウを開きます：

   - Kaspersky Security Center Web コンソールまたは Cloud コンソールのメインウィンドウで、［**デバイス**］→［**ポリシーとプロファイル**］の順に選択します。開いたグループポリシーのリストで、設定するポリシーの名前をクリックします。

   - Kaspersky Security Center Web コンソールまたは Cloud コンソールのメインウィンドウで、［**デバイス**］→［**モバイル**］→［**デバイス**］の順に選択します。設定するポリシーの適用対象であるモバイルデバイスをクリックし、［**アクティブなポリシーとポリシーのプロファイル**］タブでポリシーを選択します。

2. ポリシーのプロパティページで、［**アプリケーション設定**］→［**セキュリティコントロール**］の順に選択します。

3. ［**アプリ管理**］セクションの下の表に、管理対象のアプリを定義するルールを追加します。

   - 特定のアプリのルールを追加するには：

     a. 表で、［**アプリケーションルール**］をクリックします。

     b. 開いた［**アプリケーションルール**］ウィンドウで、作成したルールの対象となるアプリで実行する動作を選択します。

     c. **インストールパッケージのリンク（例：https://play.google.com/store/apps/details?id=com.kaspersky.kes）**、**パッケージ名（例：katana.facebook.com）**、**アプリの名前**を入力し、ルールの対象となるアプリを指定します。

     d. ［**保存**］をクリックします。

     アプリ管理ルールのリストに、ルールが追加されます。

   - アプリのカテゴリにルールを追加するには：

     a. ［**アプリ管理**］セクションの下の表で、［**カテゴリルール**］をクリックします。

     b. 開いた［**カテゴリルール**］ウィンドウで、ドロップダウンリストからアプリのカテゴリを選択します。

     選択したカテゴリ内のアプリに、作成したルールが適用されます。

     c. ［**動作モード**］セクションで、選択したカテゴリ内のアプリが起動を試行した時に実行される処理（［**ブロック対象アプリ**］または［**許可するアプリ**］）を選択します。

d. **指定のカテゴリに該当するアプリの検出時にユーザーデバイスに追加で表示するコメント**を、必要に応じて入力します。

e. ［**保存**］をクリックします。

アプリ管理ルールのリストに、ルールが追加されます。

4. ［**ブロック対象アプリに対する処理**］セクションで、ブロック対象アプリに対して実行される処理を選択します：

- ユーザーのモバイルデバイスでのブロック対象アプリの起動をブロックする場合は、［**アプリの起動をブロック**］を選択します。
- Kaspersky Endpoint Security for Android がブロック対象アプリのデータをイベントログに記録し、ブロックはしないようにするには、［**ブロックせずレポートのみ行う**］をオンにします。

5. ［**動作モード**セクションで、追加するルールで許可するアプリとブロック対象アプリのどちらを定義するかを選択します。

- 許可するアプリをルールで定義する場合は、［**ブロック対象アプリ**選択します。

  ［**ブロック対象アプリ**］モードのモバイルデバイスでシステムアプリ（カレンダー、カメラ、設定など）の起動をブロックする場合は、［**システムアプリをブロックする**］をオンにします。

  > システムアプリをブロックすると、デバイスの動作に支障が出ることがあるので、カスペルスキーではシステムアプリをブロックしないことを推奨しています。

- ブロック対象アプリをルールで定義する場合は、［**許可するアプリ**選択します。

6. モバイルデバイスにインストールされているすべてのアプリに関する情報を受信するには、［**アプリケーションレポート**］セクションで、［**モバイルデバイスにインストールされたアプリのリストを送信**］をオンにします。

   Kaspersky Endpoint Security for Android は、デバイスへのインストールやデバイスからのアンインストールが発生するたびに、イベントログにデータを送信します。

7. ［**保存**］をクリックして、ポリシーに加えた変更を保存し、ポリシーのプロパティウィンドウを終了します。

モバイルデバイスと Kaspersky Security Center との次回の同期時に、デバイスに設定が適用されます。

企業のセキュリティ要件に基づいたモバイルデバイスのコンプライアンスコントロールの設定

> これらのポリシー設定は、Android デバイスでのみ定義できます。

コンプライアンスコントロールにより、Androidデバイスを監視して企業のセキュリティ要件に準拠しているかどうかを監視し、準拠していない場合に処理を実行できます。企業のセキュリティ要件には、ユーザーがデバイスをどのように使用できるかが規定されています。たとえば、デバイスでリアルタイム保護を必ず有効にすること、定義データベースを必ずアップデートすること、デバイスのパスワードが十分な強度であることなどです。コンプライアンスコントロールは、ルールのリストに基づきます。コンプライアンスルールには、次の項目が含まれます：

- デバイスのルール違反の基準。
- 設定された期間内にルール違反を是正しない場合にデバイスで実行される処理。
- ルール違反を修正するまでユーザーに与えられる期間（例：24 時間）。
  指定した期間の終了後、選択された処理がユーザーデバイスで実行されます。

  Android 12 以降のデバイスでは、バッテリー節約モードの場合、タスクの実行が指定よりも遅れる場合があります。

コンプライアンスコントロールを設定するには、次を実行します：

- 既存のコンプライアンスルールを有効または無効にします。
- 既存のコンプライアンスルールを編集します。
- 新しいルールを追加します。
- ルールを削除します。

コンプライアンスルールの有効化と無効化

これらのポリシー設定は、Android デバイスでのみ定義できます。

企業のセキュリティ要件を満たす必要があるモバイルデバイスに適用するコンプライアンスコントロールの既存のルールを、有効または無効にするには：

1. ポリシーのプロパティウィンドウを開きます：
   - Kaspersky Security Center Web コンソールまたは Cloud コンソールのメインウィンドウで、［**デバイス**］→［**ポリシーとプロファイル**］の順に選択します。開いたグループポリシーのリストで、設定するポリシーの名前をクリックします。
   - Kaspersky Security Center Web コンソールまたは Cloud コンソールのメインウィンドウで、［**デバイス**］→［**モバイル**］→［**デバイス**］の順に選択します。設定するポリシーの適用対象であるモバイルデバイスをクリックし、［**アクティブなポリシーとポリシーのプロファイル**］タブでポリシーを選択します。
2. ポリシーのプロパティページで、［**アプリケーション設定**］→［**セキュリティコントロール**］の順に選択します。
3. ［**コンプライアンスコントロール**］セクションで、［**ステータス**］列の切り替えスイッチを使用して、既存のコンプライアンスルールを有効または無効にします。
4. ［**保存**］をクリックして、ポリシーに加えた変更を保存し、ポリシーのプロパティウィンドウを終了します。

モバイルデバイスと Kaspersky Security Center との次回の同期時に、デバイスに設定が適用されます。

コンプライアンスルールの編集

これらのポリシー設定は、Android デバイスでのみ定義できます。

企業のセキュリティ要件にモバイルデバイスが準拠するよう管理するルールを編集するには：

1. ポリシーのプロパティウィンドウを開きます：

   - Kaspersky Security Center Web コンソールまたは Cloud コンソールのメインウィンドウで、［**デバイス**］→［**ポリシーとプロファイル**］の順に選択します。開いたグループポリシーのリストで、設定するポリシーの名前をクリックします。

   - Kaspersky Security Center Web コンソールまたは Cloud コンソールのメインウィンドウで、［**デバイス**］→［**モバイル**］→［**デバイス**］の順に選択します。設定するポリシーの適用対象であるモバイルデバイスをクリックし、［**アクティブなポリシーとポリシーのプロファイル**］タブでポリシーを選択します。

2. ポリシーのプロパティページで、［**アプリケーション設定**］→［**セキュリティコントロール**］の順に選択します。

3. ［**コンプライアンスコントロール**］セクションで、編集するルールを選択し、［**編集**］をクリックします。

4. 開いた［**ルール**］ウィンドウで、次のようにルールを編集します：

   a. ［**処理**］列で、新しい処理を追加するか、既存の処理を編集するか、または削除することにより、ルール違反の場合の処理のリストを設定します。

   b. 必要に応じて、各アクションの［**違反の是正までの時間**］列を使用して、ユーザーがルール違反を是正可能な期間を指定します。

   c. ［**保存**］をクリックして、ルールを保存します。

5. ［**保存**］をクリックして、ポリシーに加えた変更を保存し、ポリシーのプロパティウィンドウを終了します。

モバイルデバイスと Kaspersky Security Center との次回の同期時に、デバイスに設定が適用されます。

コンプライアンスルールの追加

これらのポリシー設定は、Android デバイスでのみ定義できます。

企業のセキュリティ要件にモバイルデバイスが準拠するよう管理するルールを追加するには：

1. ポリシーのプロパティウィンドウを開きます：

   - Kaspersky Security Center Web コンソールまたは Cloud コンソールのメインウィンドウで、［**デバイス**］→［**ポリシーとプロファイル**］の順に選択します。開いたグループポリシーのリストで、設定する

ポリシーの名前をクリックします。

- Kaspersky Security Center Web コンソールまたは Cloud コンソールのメインウィンドウで、［**デバイス**］→［**モバイル**］→［**デバイス**］の順に選択します。設定するポリシーの適用対象であるモバイルデバイスをクリックし、［**アクティブなポリシーとポリシーのプロファイル**］タブでポリシーを選択します。

2. ポリシーのプロパティページで、［**アプリケーション設定**］→［**セキュリティコントロール**］の順に選択します。
3. ［**コンプライアンスコントロール**］セクションで、［**ルール**］をクリックします。
4. 開いた［**ルール**］ウィンドウで、次のようにルールを定義します：
   a. ルール違反の基準を選択します。
   b. ［**追加**］をクリックし、［**処理**］列からルール違反の場合の処理を選択します。
      複数の処理を追加できます。
   c. 各処理の「**違反の是正までの時間**」列を使用して、ユーザーがルール違反を是正可能な期間を指定します。
   d. ［**保存**］をクリックして、ルールを保存します。
5. ［**保存**］をクリックして、ポリシーに加えた変更を保存し、ポリシーのプロパティウィンドウを終了します。

モバイルデバイスと Kaspersky Security Center との次回の同期時に、デバイスに設定が適用されます。

コンプライアンスルールの削除

これらのポリシー設定は、Android デバイスでのみ定義できます。

企業のセキュリティ要件にモバイルデバイスが準拠するよう管理するルールを削除するには：

1. ポリシーのプロパティウィンドウを開きます：
   - Kaspersky Security Center Web コンソールまたは Cloud コンソールのメインウィンドウで、［**デバイス**］→［**ポリシーとプロファイル**］の順に選択します。開いたグループポリシーのリストで、設定するポリシーの名前をクリックします。
   - Kaspersky Security Center Web コンソールまたは Cloud コンソールのメインウィンドウで、［**デバイス**］→［**モバイル**］→［**デバイス**］の順に選択します。設定するポリシーの適用対象であるモバイルデバイスをクリックし、［**アクティブなポリシーとポリシーのプロファイル**］タブでポリシーを選択します。
2. ポリシーのプロパティページで、［**アプリケーション設定**］→［**セキュリティコントロール**］の順に選択します。
3. ［**コンプライアンスコントロール**］セクションで、削除するルールを選択し、［**削除**］をクリックします。

4. ［**保存**］をクリックして、ポリシーに加えた変更を保存し、ポリシーのプロパティウィンドウを終了します。

モバイルデバイスと Kaspersky Security Center との次回の同期時に、デバイスに設定が適用されます。

ルール違反の基準のリスト

これらのポリシー設定は、Android デバイスでのみ定義できます。

Android デバイスが企業のセキュリティ要件に準拠していることを確認するために、Kaspersky Endpoint Security for Androidはデバイスを次の基準に照らしてチェックします：

- **リアルタイム保護が無効です。**

  リアルタイム保護を有効にする必要があります。

  リアルタイム保護の設定の詳細は、「リアルタイム保護の設定」を参照してください。

- **定義データベースがアップデートされていません。**

  Kaspersky Endpoint Security for Android の定義データベースを、定期的にアップデートする必要があります。

  定義データベースのアップデート設定の詳細は、「アンチウイルスによる保護の設定」を参照してください。

- **ブロック対象アプリがインストールされています。**

  起動をブロックするように［**アプリ管理**］セクションで指定されたアプリケーションは、モバイルデバイスにインストールされていない必要があります。

  アプリケーションのルール作成の詳細は、「アプリ管理の設定」を参照してください。

- **ブロック対象カテゴリに該当するアプリがインストールされています。**

  起動をブロックするカテゴリに［**アプリ管理**］セクションで指定されたアプリケーションは、モバイルデバイスにインストールされていない必要があります。

  アプリケーションカテゴリのルールの作成の詳細は、「アプリ管理の設定」を参照してください。

- **一部の必須アプリがインストールされていません。**

  インストールを強制するように［**アプリ管理**］セクションで指定されたアプリケーションは、モバイルデバイスにインストールされている必要があります。

  アプリケーションのルール作成の詳細は、「アプリ管理の設定」を参照してください。

- **OS のバージョンがアップデートされていません。**

  デバイスには、許可されたバージョンのオペレーティングシステムが必要です。

  このルール違反の基準を使用するには、［**OS の最も古いバージョン**］および［**OS の最も新しいバージョン**］ドロップダウンリストで、許可するオペレーティングシステムバージョンの範囲を指定する必要があります。

- **デバイスが長期間同期されていません。**

  デバイスと管理サーバーを定期的に同期する必要があります。

  このルール違反の基準を使用するには、［**同期間隔**］ドロップダウンリストでデバイスの同期の最大時間間隔を指定する必要があります。

- **デバイスが root 化されています。**
  デバイスを root 化しないでください。
  詳細は、「デバイスハッキング（root）の検知」を参照してください。

- **ロック解除用パスワードがセキュリティ要件に適合していません。**
  デバイスは、ロック解除用パスワードの強度要件に準拠するロック解除用パスワードで保護する必要があります。

ルール違反の場合の処理のリスト

これらのポリシー設定は、Android デバイスでのみ定義できます。

ユーザーが指定された期間内にルール違反を是正しない場合、次の処理が実行可能です：

- **システムアプリ以外のすべてのアプリをブロックする**：
  ユーザーのモバイルデバイス上の、システムアプリ以外のすべてのアプリの起動がブロックされます。

- **デバイスのロック**：
  モバイルデバイスがロックされます。データにアクセスするには、デバイスのロックを解除する必要があります。デバイスのロックを解除した後、デバイスロックの理由が解決していない場合、指定した時間の経過後にデバイスは再度ロックされます。

- **企業データを消去する**：
  コンテナ化されたデータ、企業のメールアカウント、企業の Wi-Fi ネットワークと VPN に接続するための設定、アクセスポイント名（APN）を消去します。

- **デバイスを完全リセットして出荷時の設定にする**：
  すべてのデータがモバイルデバイスから削除され、設定が工場出荷時の値にロールバックされます。

Web サイトへのユーザーアクセスの設定

これらのポリシー設定は、Android と iOS デバイスで定義できます。

インターネットブラウジング中にモバイルデバイスに保存される個人データおよび企業データを保護するには、危険サイトブロックを使用して Web サイトへのユーザーアクセスを設定します。危険サイトブロックは、ユーザーが Web サイトを開く前にスキャンし、悪意のあるコードを配布する Web サイトや、機密データを盗んで金融口座にアクセスするように設計されたフィッシングサイトをブロックします。

Android デバイスの場合は、Kaspersky Security Network クラウドサービスで定義されたカテゴリを使用して Web サイトをフィルタリングすることもできます。フィルタリングにより、特定の Web サイトまたは Web サイトの特定のカテゴリ（「**ギャンブル、宝くじ、懸賞**」や「**インターネットコミュニケーション**」など）へのアクセスを制限できます。

Android デバイスの場合、危険サイトブロックは、Google Chrome、Huawei Browser、Samsung Internet Browser でのみ動作します。

危険サイトブロックが適切に動作するようにするには、Kaspersky Endpoint Security for Android をユーザー補助機能として設定する必要があります。初期設定ウィザードで Kaspersky Endpoint Security for Android をユーザー補助機能として設定するよう要求されます。このステップはスキップできます。また、後からデバイスの設定でサービスを無効にすることもできます。

iOS デバイスで危険サイトブロックを使用するには、ユーザーが Kaspersky Security for iOS で VPN 設定の追加を許可する必要があります。

Web サイトへのユーザーアクセスを設定するには：

1. ポリシーのプロパティウィンドウを開きます：

   - Kaspersky Security Center Web コンソールまたは Cloud コンソールのメインウィンドウで、［**デバイス**］→［**ポリシーとプロファイル**］の順に選択します。開いたグループポリシーのリストで、設定するポリシーの名前をクリックします。

   - Kaspersky Security Center Web コンソールまたは Cloud コンソールのメインウィンドウで、［**デバイス**］→［**モバイル**］→［**デバイス**］の順に選択します。設定するポリシーの適用対象であるモバイルデバイスをクリックし、［**アクティブなポリシーとポリシーのプロファイル**］タブでポリシーを選択します。

2. ポリシーのプロパティページで、［**アプリケーション設定**］→［**セキュリティコントロール**］の順に選択します。

3. ［**危険サイトブロック**］セクションで、［**危険サイトブロックを有効にする**］をオンにして機能を有効にします。

4. Android デバイスの場合は、次のいずれかのオプションを選択できます：

   - コンテンツに基づいて Web サイトへのユーザーアクセスを制限するには：

     a. ［**指定したカテゴリの Web サイトをブロック**］を選択します。

     b. Kaspersky Endpoint Security for Android がアクセスをブロックする Web サイトのカテゴリに隣接するチェックボックスをオンにします。

     危険サイトブロックを有効にすると、**フィッシング**および**マルウェアサイト**のカテゴリに属する Web サイトへのアクセスがブロックされます。

   - 許可する Web サイトのリストを指定するには：

     a. ［**指定した Web サイトのみ許可**］を選択します。

     b. アクセスをブロックしない Web サイトのアドレスを追加して、Web サイトのリストを作成します。Kaspersky Endpoint Security for Android は正規表現のみをサポートします。アクセスを許可する Web サイトのアドレスを入力する時は、次のルールを使用してください：

        - `http:\/\/www\.example\.com.*` – 指定した Web サイトのすべての子ページを許可する（例：`http://www.example.com/about`）。

        - `https:\/\/.*example\.com` – 指定した Web サイトのすべてのサブドメインページを許可する（例：`https://pictures.example.com`）。

c. HTTP プロトコルと HTTPS プロトコルを選択するために、`https?` という表現も使用できます。正規表現の詳細については、Oracle のテクニカルサポートサイトを参照してください。

- すべての Web サイトへのユーザーアクセスをブロックするには、［**すべての Web サイトをブロック**］を選択します。

5. ［**保存**］をクリックして、ポリシーに加えた変更を保存し、ポリシーのプロパティウィンドウを終了します。

モバイルデバイスと Kaspersky Security Center との次回の同期時に、デバイスに設定が適用されます。

機能制限の設定

これらのポリシー設定は、Android デバイスでのみ定義できます。

Kaspersky Security Center Web コンソールを使用すると、モバイルデバイスの次の機能へのユーザーアクセスを設定できます：

- Wi-Fi
- カメラ
- Bluetooth

既定では、デバイスでの Wi-Fi、カメラ、Bluetooth の使用に制限はありません。

デバイスでの Wi-Fi、カメラ、Bluetooth の使用制限を設定するには：

1. ポリシーのプロパティウィンドウを開きます：
   - Kaspersky Security Center Web コンソールまたは Cloud コンソールのメインウィンドウで、［**デバイス**］→［**ポリシーとプロファイル**］の順に選択します。開いたグループポリシーのリストで、設定するポリシーの名前をクリックします。
   - Kaspersky Security Center Web コンソールまたは Cloud コンソールのメインウィンドウで、［**デバイス**］→［**モバイル**］→［**デバイス**］の順に選択します。設定するポリシーの適用対象であるモバイルデバイスをクリックし、［**アクティブなポリシーとポリシーのプロファイル**］タブでポリシーを選択します。
2. ポリシーのプロパティページで、［**アプリケーション設定**］→［**セキュリティコントロール**］の順に選択します。
3. ［**デバイス機能の管理**］セクションで、Wi-Fi、カメラ、Bluetooth の使用を設定します：
   - ユーザーのモバイルデバイスの Wi-Fi モジュールを無効にするには、［**Wi-Fi の使用を禁止する**］をオンにします。

     Android 10.0 以降のデバイスでは、Wi-Fi ネットワークの使用の禁止はサポートされていません。

- ユーザーのモバイルデバイスのカメラを無効にするには、［**カメラの使用を禁止する**］をオンにします。

  Android 10 以降のデバイスの場合、カメラの使用を完全には禁止できません。

  Android バージョン 11 以降のデバイスでは、Kaspersky Endpoint Security for Android をユーザー補助機能として設定しておく必要があります。初期設定ウィザードで Kaspersky Endpoint Security for Android をユーザー補助機能として設定するよう要求されます。このステップはスキップできます。また、後からデバイスの設定でサービスを無効にすることもできます。この場合、カメラの使用を制限することはできません。

- ユーザーのモバイルデバイスの Bluetooth を無効にするには、［**Bluetooth の使用を禁止する**］をオンにします。

  Android 12 以降では、デバイスユーザーが［**付近の Bluetooth デバイス**］権限を付与している場合に限り、Bluetooth の使用を無効にできます。ユーザーは、初期設定ウィザードの実行中、または後からこの権限を付与できます。

4. ［**保存**］をクリックして、ポリシーに加えた変更を保存し、ポリシーのプロパティウィンドウを終了します。

モバイルデバイスと Kaspersky Security Center との次回の同期時に、デバイスに設定が適用されます。

Kaspersky Endpoint Security for Android の削除に対する保護

モバイルデバイス保護と企業のセキュリティ要件準拠のため、Kaspersky Endpoint Security for Android の削除からの保護を有効にできます。この場合、ユーザーは Kaspersky Endpoint Security for Android のインターフェイスを使用して本アプリを削除することはできません。Android オペレーティングシステムのツールを使用してアプリを削除する場合、Kaspersky Endpoint Security for Android の管理者権限を無効にするよう要求されます。権限を無効にすると、モバイルデバイスはロックされます。

Kaspersky Endpoint Security for Android の削除からの保護を有効にするには：

1. ポリシーのプロパティウィンドウを開きます：

   - Kaspersky Security Center Web コンソールまたは Cloud コンソールのメインウィンドウで、［**デバイス**］→［**ポリシーとプロファイル**］の順に選択します。開いたグループポリシーのリストで、設定するポリシーの名前をクリックします。

   - Kaspersky Security Center Web コンソールまたは Cloud コンソールのメインウィンドウで、［**デバイス**］→［**モバイル**］→［**デバイス**］の順に選択します。設定するポリシーの適用対象であるモバイルデバイスをクリックし、［**アクティブなポリシーとポリシーのプロファイル**］タブでポリシーを選択します。

2. ポリシーのプロパティページで、［**アプリケーション設定**］→［**セキュリティコントロール**］の順に選択します。

3. ［**モバイルデバイスのアプリを管理**］セクションで、［**デバイスからの Kaspersky Endpoint Security for Android の削除を許可**］をオフにします。

Android 7.0 以降のデバイスでアプリが削除されないように保護するには、Kaspersky Endpoint Security for Android をユーザー補助機能として設定しておく必要があります。初期設定ウィザードの実行時に、必要な権限を Kaspersky Endpoint Security for Android に付与するよう要求されます。このステップはスキップできます。また、後からデバイスの設定で権限を無効にすることもできます。その場合、手動による削除はブロックできません。

4. ［**保存**］をクリックして、ポリシーに加えた変更を保存し、ポリシーのプロパティウィンドウを終了します。

モバイルデバイスと Kaspersky Security Center との次回の同期時に、デバイスに設定が適用されます。

本アプリを削除しようとすると、モバイルデバイスはロックされます。

Kaspersky Security Center とモバイルデバイスの同期の設定

これらのポリシー設定は、Android と iOS デバイスで定義できます。

モバイルデバイスを管理し、ユーザーのモバイルデバイスからレポートや統計情報を受信するには、同期を設定する必要があります。Kaspersky Security Center とモバイルデバイスの同期は、次のように実行されます：

- **スケジュール**：スケジュールに基づく同期は、HTTP プロトコルを使用して実行されます。同期スケジュールは、ポリシーのプロパティで指定できます。グループポリシーの設定変更、コマンド、タスクは、スケジュールに基づいてデバイスが Kaspersky Security Center と同期すると実行されます（同期するまで、実行が遅延します）。既定では、モバイルデバイスと Kaspersky Security Center との同期は 6 時間ごとに自動的に実行されます。

  Android 12 以降のデバイスでは、バッテリー節約モードの場合、タスクの実行が指定よりも遅れる場合があります。

- **強制**（Android デバイス）：強制的な同期は、FCM サービス（Firebase Cloud Messaging）のプッシュ通知を使用して実行されます。強制的な同期は、モバイルデバイスへのコマンドのタイムリーな配信を主な目的としています。強制的な同期を使用する場合は、FCM が Kaspersky Security Center で設定されていることを確認してください。

Kaspersky Security Center とのモバイルデバイスの同期を設定するには：

1. ポリシーのプロパティウィンドウを開きます：

   - Kaspersky Security Center Web コンソールまたは Cloud コンソールのメインウィンドウで、［**デバイス**］→［**ポリシーとプロファイル**］の順に選択します。開いたグループポリシーのリストで、設定するポリシーの名前をクリックします。

   - Kaspersky Security Center Web コンソールまたは Cloud コンソールのメインウィンドウで、［**デバイス**］→［**モバイル**］→［**デバイス**］の順に選択します。設定するポリシーの適用対象であるモバイルデバイスをクリックし、［**アクティブなポリシーとポリシーのプロファイル**］タブでポリシーを選択します。

2. ポリシーのプロパティページで、［**アプリケーション設定**］→［**同期**］の順に選択します。

3. ［**管理サーバーとの同期**］セクションで、［**同期間隔**］ドロップダウンリストを使用して、同期間隔を選択します。

既定では、同期は 6 時間ごとに実行されます。

4. Android デバイスの場合は、デバイスのローミング中の同期を無効にできます。無効にするには、［**ローミング中は同期しない**をオンにします。

   既定では、ローミング中の同期が有効になっています。

5. ［**保存**］をクリックして、ポリシーに加えた変更を保存し、ポリシーのプロパティウィンドウを終了します。

モバイルデバイスと Kaspersky Security Center との次回の同期時に、デバイスに設定が適用されます。

Kaspersky Security Network

モバイルデバイスをより効果的に保護するために、Kaspersky Endpoint Security for Android と Kaspersky Security for iOS は、世界中のユーザーから取得されたデータを使用しています。*Kaspersky Security Network* は、そのような集められたデータの処理を目的としています。

*Kaspersky Security Network（KSN）*は、ファイル、Web リソース、ソフトウェアの評価に関する情報を含むカスペルスキーのオンラインナレッジベースへのアクセスを提供する、クラウドサービスの基盤です。Kaspersky Security Network のデータを使用することにより、脅威に対するカスペルスキー製品の対応が迅速化され、保護コンポーネントのパフォーマンスが向上し、誤検知の可能性も低減されます。

Kaspersky Security Network に参加していただくことで、カスペルスキーでは新たな脅威の種別とソースに関する情報をリアルタイムで取得し、新しい脅威を駆除する方法を開発することができます。また、誤検知の件数も低減できます。また、Kaspersky Security Network に参加するユーザーは、アプリケーションと Web サイトのレピュテーション統計情報を利用することもできます。

Kaspersky Security Network に参加すると、モバイルアプリの実行中に一定の統計が収集され、カスペルスキーに自動的に送信されます。この情報によって、リアルタイムでの脅威の追跡が可能になっています。コンピューターまたはユーザーのコンテンツに損害を与える目的で侵入者に悪用される可能性があるファイルやその一部が、追加の調査を目的としてカスペルスキーに送信される場合もあります。

以下のアプリのコンポーネントは、Kaspersky Security Network クラウドサービスを使用します：

- Kaspersky Endpoint Security for Android の アンチウイルス、危険サイトブロック、およびアプリ管理コンポーネント
- Kaspersky Security for iOS の危険サイトブロックコンポーネント

KSN の使用を開始するには、使用許諾契約書の条項に同意する必要があります。KSN へのデータ送信の詳細は、「Kaspersky Security Network との情報交換」を参照してください。

KSN への参加を拒否すると、デバイスの保護レベルが下がり、デバイスの感染やデータの消失の原因となる可能性があります。

本モバイルアプリのパフォーマンス改善を目的として、Kaspersky Security Network に統計情報を提供することもできます。

Kaspersky Security Network への情報の提供は任意です。

Kaspersky Security Network との情報交換

Kaspersky Endpoint Security for Android での情報交換

リアルタイム保護を改善するため、Kaspersky Endpoint Security for Android は次のコンポーネントの動作で Kaspersky Security Network クラウドサービスを使用します：

- **アンチウイルス**：本アプリはカスペルスキーのオンラインナレッジベースへアクセスし、ファイルやアプリに関する評価の情報を取得します。定義データベースには追加されていないが、KSN では確認できる情報を持つ脅威に対して、このスキャンが実行されます。Kaspersky Security Network クラウドサービスにより、アンチウイルスの機能が制限なく発揮され、また誤検知の可能性も低減されます。

- **危険サイトブロック**：KSN から取得したデータを使用して、Web サイトが開かれる前にそのサイトをスキャンします。また、Web サイトのカテゴリを判別し、許可するカテゴリとブロックするカテゴリのリストに基づいてユーザーのインターネットアクセスを制御します（たとえば、「インターネットコミュニケーション」カテゴリなど）。

- **アプリ管理**：アプリのカテゴリを判別し、許可するカテゴリとブロックするカテゴリのリストに基づいて、企業のセキュリティ要件を満たさないアプリの開始を制限します（たとえば「ゲーム」カテゴリなど）。

アンチウイルスおよびアプリ管理の動作中、KSN を使用している時にカスペルスキーに送信されるデータの種別に関する情報は、使用許諾契約書に記載されています。使用許諾契約書の諸条項に同意すると、この情報の送信に同意したことになります。

危険サイトブロックの動作中、KSN を使用している時にカスペルスキーに送信されるデータの種別に関する情報は、データ処理に関する声明に記載されています。声明の諸条項に同意すると、この情報の送信に同意したことになります。

KSN へのデータ提供の詳細は、「Kaspersky Endpoint Security for Android でのデータ提供」を参照してください。

KSN へのデータの提供は任意です。必要に応じて、KSN とのデータ交換を無効にすることができます。

Kaspersky Security for iOS での情報交換

リアルタイム保護を改善するため、Kaspersky Security for iOS は**危険サイトブロック**コンポーネントの動作で Kaspersky Security Network クラウドサービスを使用します。KSN から取得したデータを使用して、Web リソースが開かれる前にそのリソースをスキャンします。

危険サイトブロックの動作中、KSN を使用している時にカスペルスキーに送信されるデータの種別に関する情報は、使用許諾契約書に記載されています。使用許諾契約書の諸条項に同意すると、この情報の送信に同意したことになります。

KSN へのデータ提供の詳細は、「Kaspersky Security for iOS でのデータ提供」を参照してください。

KSN へのデータの提供は任意です。必要に応じて、KSN とのデータ交換を無効にすることができます。

Android および iOS アプリから KSN への統計情報の送信

本アプリのパフォーマンスの向上を目的として、KSN とデータを交換するには、次の条件を満たす必要があります：

- Kaspersky Security Network に関する声明にデバイスユーザーが同意する必要があります。

- グループポリシーの設定で、KSN への統計情報の送信を許可するように設定する必要があります。

Kaspersky Security Network への統計情報の送信はいつでも停止できます。モバイルアプリの動作中、KSN の使用時にカスペルスキーに送信されるデータの種別に関する情報は、使用許諾契約書に記載されています。

Kaspersky Security Network の有効化と無効化

既定では、Kaspersky Security Network の使用が有効になっています。

Kaspersky Security Network の使用が無効になると、Kaspersky Security Network の危険サイトブロック、アプリ管理、追加の保護も自動的に無効になり、それらの設定が使用できなくなります。

Kaspersky Security Network の使用を有効または無効にするには：

1. ポリシーのプロパティウィンドウを開きます：

   - Kaspersky Security Center Web コンソールまたは Cloud コンソールのメインウィンドウで、［**デバイス**］→［**ポリシーとプロファイル**］の順に選択します。開いたグループポリシーのリストで、設定するポリシーの名前をクリックします。

   - Kaspersky Security Center Web コンソールまたは Cloud コンソールのメインウィンドウで、［**デバイス**］→［**モバイル**］→［**デバイス**］の順に選択します。設定するポリシーの適用対象であるモバイルデバイスをクリックし、［**アクティブなポリシーとポリシーのプロファイル**］タブでポリシーを選択します。

2. ポリシーのプロパティページで、［**アプリケーション設定**］→［**KSN と統計情報**］の順に選択します。

3. Kaspersky Security Network の使用を有効または無効にするには、［**Kaspersky Security Network を使用する**をオンまたはオフにします。

4. Kaspersky Security Network の使用が有効になっていて、カスペルスキーへのデータ送信に同意する場合は、［**Kaspersky Security Network への統計情報の送信を許可**］をオンにします。このデータにより、モバイルアプリによる脅威への対応がより早くなり、保護コンポーネントのパフォーマンスが向上し、誤検知の可能性も低減されます。

5. ［**保存**］をクリックして、ポリシーに加えた変更を保存し、ポリシーのプロパティウィンドウを終了します。

モバイルデバイスと Kaspersky Security Center との次回の同期時に、デバイスに設定が適用されます。

Firebase 向け Google アナリティクス、SafetyNet Attestation、Firebase Performance Monitoring、Crashlytics との情報交換

これらのポリシー設定は、Android デバイスでのみ定義できます。

Kaspersky Endpoint Security for Android は、ユーザーエクスペリエンス、機能、ステータス、使用中のデバイス設定を分析することで、カスペルスキー製品、製品、サービス、インフラストラクチャの品質、外観、パフォーマンスを向上させることを目的として、Firebase 向け Google アナリティクスサービス、SafetyNet Attestation、Firebase Performance Monitoring、Crashlytics サービスとデータを交換します。

Firebase 向け Google アナリティクス、SafetyNet Attestation、Firebase Performance Monitoring、Crashlytics との情報交換は、既定では無効になっています。

情報交換を有効にするには：

1. ポリシーのプロパティウィンドウを開きます：

   - Kaspersky Security Center Web コンソールまたは Cloud コンソールのメインウィンドウで、［**デバイス**］→［**ポリシーとプロファイル**］の順に選択します。開いたグループポリシーのリストで、設定するポリシーの名前をクリックします。

   - Kaspersky Security Center Web コンソールまたは Cloud コンソールのメインウィンドウで、［**デバイス**］→［**モバイル**］→［**デバイス**］の順に選択します。設定するポリシーの適用対象であるモバイルデバイスをクリックし、［**アクティブなポリシーとポリシーのプロファイル**］タブでポリシーを選択します。

2. ポリシーのプロパティページで、［**アプリケーション設定**］→［**KSN と統計情報**］の順に選択します。

3. ［**統計情報の送信**］セクションで、［**データ転送を許可し、本アプリの品質、デザイン、パフォーマンスの改善に協力する**］をオンにします。

4. ［**保存**］をクリックして、ポリシーに加えた変更を保存し、ポリシーのプロパティウィンドウを終了します。

モバイルデバイスと Kaspersky Security Center との次回の同期時に、デバイスに設定が適用されます。

モバイルデバイスでの通知の設定

これらのポリシー設定は、Android デバイスでのみ定義できます。

Kaspersky Endpoint Security for Android の通知をモバイルデバイスに表示したくない場合は、特定の通知を無効にできます。

Kaspersky Endpoint Security は次のツールを使用して、デバイスの保護ステータスを表示します：

- **保護ステータスの通知**：この通知は通知バーにピン留めされています。保護ステータスの通知は削除できません。通知には、デバイスの保護ステータス（例：）と、問題がある場合は問題の数が表示されます。デバイスの保護ステータスをタップして、問題を一覧表示させることができます。

- **アプリの通知**：デバイスユーザーに本アプリの情報を通知します（例：脅威の検知）。

- **ポップアップメッセージ**：ポップアップメッセージは、デバイスのユーザーによる操作が必要な場合に表示されます（例：脅威の検知時に実行する処理）。

既定では、Kaspersky Endpoint Security for Android の通知はすべて有効になっています。

Android デバイスのユーザーは、通知バーの設定で、Kaspersky Endpoint Security for Android からの通知をすべて無効にできます。通知を無効にすると、本アプリの動作が監視されないので、重要な通知を見逃してしまう場合もあります（Kaspersky Security Center とデバイスの同期が失敗した場合の情報など）。この場合、動作の状態を確認するには、Kaspersky Endpoint Security for Android を開く必要があります。

Kaspersky Endpoint Security for Android の動作に関するモバイルデバイス上の通知の表示を設定するには：

1. ポリシーのプロパティウィンドウを開きます：

   - Kaspersky Security Center Web コンソールまたは Cloud コンソールのメインウィンドウで、［**デバイス**］→［**ポリシーとプロファイル**］の順に選択します。開いたグループポリシーのリストで、設定するポリシーの名前をクリックします。

   - Kaspersky Security Center Web コンソールまたは Cloud コンソールのメインウィンドウで、［**デバイス**］→［**モバイル**］→［**デバイス**］の順に選択します。設定するポリシーの適用対象であるモバイルデバイスをクリックし、［**アクティブなポリシーとポリシーのプロファイル**］タブでポリシーを選択します。

2. ポリシーのプロパティページで、［**アプリケーション設定**］→［**通知とレポート**］の順に選択します。

3. ［**通知**］セクションで、通知の表示を設定します：

   - すべての通知とポップアップメッセージを非表示にするには、［**Kaspersky Endpoint Security をバックグラウンドで実行している場合も通知を表示する**］を切り替えスイッチでオフにします。

     保護ステータスに関する通知のみが表示されるようになります。通知には、デバイスの保護ステータス（例：）と、問題の数が表示されます。また、ユーザーによるアプリの操作時（例：定義データベースを手動でアップデート）に通知を表示します。

     カスペルスキーのエキスパートは、通知とポップアップメッセージの有効化を推奨しています。バックグラウンドモードで通知とポップアップメッセージを無効にすると、本アプリは脅威に関する警告をユーザーにリアルタイムで通知しなくなります。モバイルデバイスのユーザーがデバイスの保護ステータスを知るのは、本アプリを開いた時のみとなります。

   - ［**ユーザーデバイスに表示するセキュリティ上の問題のリスト**］で、ユーザーのモバイルデバイスに表示する Kaspersky Endpoint Security for Android の問題を選択します。

4. ［**保存**］をクリックして、ポリシーに加えた変更を保存し、ポリシーのプロパティウィンドウを終了します。

モバイルデバイスと Kaspersky Security Center との次回の同期時に、デバイスに設定が適用されます。

デバイスハッキングの検知

Kaspersky Security Center Web コンソールでは、Android デバイスでのデバイスハッキング（root）および iOS デバイスでのジェイルブレイクを検知できます。ハッキングされたデバイスでは、システムファイルの保護が解除され、その結果、編集可能になってしまいます。さらに、提供元が不明なサードパーティのアプリをハッキングされたデバイスにインストールすることもできてしまいます。ハッキング試行を検知した場合、ただちにデバイスの正常動作を復元してください。

Kaspersky Endpoint Security for Android は次のサービスを使用して、ユーザーによるルート権限の取得を検知します：

- *Kaspersky Endpoint Security for Android の組み込みサービス*。カスペルスキーのサービス（Kaspersky Mobile Security SDK）。モバイルデバイスユーザーが root 権限を取得したかどうかを確認します。

- *SafetyNet Attestation*Google のサービス。オペレーティングシステムの整合性を確認し、デバイスのハードウェアおよびソフトウェアを分析し、その他のセキュリティ上の問題を特定します。SafetyNet

Attestation の詳細は、Android のテクニカルサポートサイトを参照してください。

Kaspersky Security for iOS は、次のサービスを使用してジェイルブレイクを検知します：

- *Kaspersky Security for iOS の組み込みサービス*。モバイルデバイスがジェイルブレイクされているかを確認するカスペルスキーのサービス（Kaspersky Mobile Security SDK）。

デバイスがハッキングされた場合は、通知を受信します。ハッキング通知は、Kaspersky Security Center Web コンソールの［**監視とレポート**］→［**ダッシュボード**］タブで確認できます。また、イベント通知設定でハッキングについての通知を無効にすることもできます。

Android デバイスでは、デバイスがハッキングされた場合、デバイスでのユーザー操作を制限できます（デバイスのロックなど）。コンプライアンスコントロールを使用して、制限を設定できます。設定するには、［**デバイスが root 化されています**］の基準を使用してコンプライアンスルールを作成します。

ライセンス設定の指定

これらのポリシー設定は、Android と iOS デバイスで定義できます。

Kaspersky Security Center Web コンソールまたは Cloud コンソールでモバイルデバイスを管理するには、モバイルデバイスでモバイルアプリをアクティベートする必要があります。モバイルデバイスでの Kaspersky Endpoint Security for Android と Kaspersky Security for iOS のアクティベートは、有効なライセンス情報を本アプリに追加することで完了します。ライセンス情報は、Kaspersky Security Center とモバイルデバイスの同期時に、ポリシーと一緒にデバイスに送信されます。

デバイスにインストールされた時点から 30 日以内にモバイルアプリのアクティベーションが完了しなかった場合、アプリは自動的に機能制限モードに切り替わります。このモードでは、ほとんどのアプリ機能は機能しません。機能制限モードに切り替わると、本アプリは Kaspersky Security Center との自動同期を停止します。そのため、何らかの理由で本アプリのアクティベーションがインストール後 30 日以内に完了しなかった場合、ユーザーは手動でデバイスを Kaspersky Security Center と同期させる必要があります。

グループポリシーのライセンス設定を指定するには：

1. ポリシーのプロパティウィンドウを開きます：

   - Kaspersky Security Center Web コンソールまたは Cloud コンソールのメインウィンドウで、［**デバイス**］→［**ポリシーとプロファイル**］の順に選択します。開いたグループポリシーのリストで、設定するポリシーの名前をクリックします。

   - Kaspersky Security Center Web コンソールまたは Cloud コンソールのメインウィンドウで、［**デバイス**］→［**モバイル**］→［**デバイス**］の順に選択します。設定するポリシーの適用対象であるモバイルデバイスをクリックし、［**アクティブなポリシーとポリシーのプロファイル**］タブでポリシーを選択します。

2. ポリシーのプロパティページで、［**アプリケーション設定**］→［**ライセンス**］の順に選択します。

3. ドロップダウンリストを使用して、管理サーバーのライセンス保管領域から必要なライセンスを選択します。

   ライセンスの詳細は、下のフィールドに表示されます。

上記のドロップダウンリストで選択したものと異なる場合は、モバイルデバイスの既存のアクティベーション用ライセンスを置換できます。置換するには、［**デバイスのライセンスが異なる場合は、このライセンスと置き換える**をオンにします。

4. ［**保存**］をクリックして、ポリシーに加えた変更を保存し、ポリシーのプロパティウィンドウを終了します。

モバイルデバイスと Kaspersky Security Center との次回の同期時に、デバイスに設定が適用されます。

イベントの設定

これらのポリシー設定は、Android と iOS デバイスで定義できます。

ユーザーデバイスで発生し、Kaspersky Security Center へ送信されるイベントの保存と通知に関する設定を指定できます。

ポリシーの編集時にのみ、イベントの設定を指定できます。

イベントは、重要度に応じて次のタブに割り当てられます：

- **緊急**
  緊急イベントは、データの損失、誤動作、致命的なエラーを発生させる可能性がある問題を示します。
- **機能エラー**
  機能エラーは、本アプリの動作中に発生した深刻な問題、エラー、誤動作などを示します。
- **警告**
  警告は、必ずしも深刻ではないが、将来問題になる可能性があるイベントを示します。
- **情報**
  情報イベントは、本アプリの動作や手順、正常な機能の完了を通知します。

各セクションに、イベント種別とイベントの既定の保管期間（日）がリスト表示されます。

イベントリストで可能な操作は次の通りです：

- Kaspersky Security Center へ送信されるイベント種別のリストへイベント種別を追加したり、またはリストから削除したりします。
- 各イベント種別の保管、通知の設定を指定します。例：イベント種別の管理サーバーデータベースでの保管期間、イベントをメールで通知するかどうか、など。

Kaspersky Security Center Web コンソール、Cloud コンソールでおのイベントの設定の詳細：

- Kaspersky Security Center Web コンソールを使用している場合、*Kaspersky Security Center のヘルプ*を参照してください。

- Kaspersky Security Center Cloud コンソールを使用している場合、*Kaspersky Security Center Cloud コンソールのヘルプ*を参照してください。

ユーザーデバイスのアプリのインストール、アップデート、削除に関するイベントの設定

これらのポリシー設定は、Android と iOS デバイスで定義できます。

Kaspersky Security Center Cloud コンソールを使用する場合、ユーザーデバイスで発生するイベントと、Kaspersky Security Center へ送信されるイベントの種別のリストには、デバイスのアプリのインストール、アップデート、削除は含まれません。これらのイベントの発生頻度は非常に高く、イベントの最大数に達すると、Kaspersky Security Center データベースの他の重要なイベントを見落としてしまう可能性が高くなる場合があるためです。また、これらのイベントは管理サーバーまたは DBMS のパフォーマンス、Kaspersky Security Center Cloud コンソールとのインターネット接続の帯域に影響する可能性もあります。

それでもこれらの種別のイベントを保管し、通知させる場合は、このセクションに記載された手順を実行します。

ユーザーデバイスのアプリのインストール、アップデート、削除に関するイベントの設定を指定するには：

1. ポリシー設定の［**イベントの設定**］タブで、［**インストールまたは削除されたアプリ（インストール済みアプリのリスト）**］の情報イベント種別を、管理サーバーのデータベースへ保管するイベントのリストに追加します。

   イベントの設定の詳細は、*Kaspersky Security Center Cloud コンソールのヘルプ*を参照してください。

2. ［**モバイルデバイスにインストールされたアプリのリストを送信**］をオンにします。

ユーザーデバイスのアプリのインストール、アップデート、削除に関するイベントが Kaspersky Security Center データベースに、保管されるようになります。これらのイベントが通知されるようになります。

ネットワーク負荷

このセクションは、モバイルデバイスと Kaspersky Security Center の間で発生するネットワーク通信の量に関する情報を記載しています。

通信量

タスク	送信トラフィック	受信トラフィック	通信の総量
アプリの初回導入（MB 単位）	0.08	17.76	17.84
定義データベースの初回アップデート（通信量は定義データベースのサイズに応じて異なる場合があります）（MB 単位）	0.04	2.21	2.25
モバイルデバイスと Kaspersky Security Center の同期（MB 単位）	0.03	0.02	0.05
通常の定義データベースのアップデート（通信量は定義データベースのサイズに応じて異なる場合があります）（MB 単位）	0.08	3.06	3.14
盗難対策コマンドの実行デバイスの GPS 追跡（通信量は搭載されたカメラの性能および写真の画質に応じて異なる場合があります）（MB 単位）	0.09	0.8	0.17

盗難対策コマンドの実行遠隔撮影（MB 単位）	1.0	0.02	1.02
盗難対策コマンドの実行デバイスロック（MB 単位）	0.06	0.05	0.11
1 日あたりの平均量（MB 単位）	0.22	6.96	7.18

MMC ベースの管理コンソールの操作

このヘルプセクションでは、MMC ベースの Kaspersky Security Center 管理コンソールを使用したモバイルデバイスの保護と管理について説明します。

主要なユースケース

インストール

Kaspersky Endpoint Security for Android を遠隔でインストールするには？

ユーザーによる Kaspersky Endpoint Security for Android の削除をブロックするには？

Kaspersky Endpoint Security for Android をアクティベートするには？

プロテクション

紛失または盗難にあったデバイスをロックするには？

インターネットの脅威から自分自身を保護するには？

空のパスワードの使用を禁止するには？

サードパーティ製品の使用

Android Enterprise（ブリーフケースのアイコンが表示されたアプリケーション、Android 仕事用プロファイルの設定）

VMware AirWatch、MobileIron、IBM Maas360、SOTI MobiControl

制御

デバイスでユーザーがゲームをしないようにブロックするには？

デバイスでの Web サイトへのアクセスを設定するには？

Root を検知するには？

管理

デバイスでメールボックスを設定するには？

モバイルデバイスを Wi-Fi に接続するには？

企業アプリをインストールするには？

Kaspersky Security for Mobile について

*Kaspersky Security for Mobile*は組織のモバイルデバイス、および業務目的で使用される社員個人のモバイルデバイスを保護、管理するための統合ソリューションです。

Kaspersky Security for Mobile には、次のコンポーネントが含まれます：

- Kaspersky Endpoint Security for Android モバイルアプリ

  Kaspersky Endpoint Security for Android アプリは、Web の脅威や、脅威となるその他のウイルスやプログラムからモバイルデバイスを保護します。

- Kaspersky Endpoint Security for Android 管理プラグイン

Kaspersky Endpoint Security for Android の管理プラグインは、Kaspersky Security Center の管理コンソールからモバイルデバイスおよびデバイスにインストールされているモバイルアプリを管理するためのインターフェイスを提供します。

- Kaspersky Device Management for iOS 管理プラグイン

  Kaspersky Device Management iOS 管理プラグインにより、iOS MDM プロトコルで Kaspersky Security Center に接続されているデバイス（以降、「iOS MDM デバイス」と表記）および Exchange ActiveSync プロトコルで Kaspersky Security Center に接続されているデバイス（以降、「EAS デバイス」と表記）の設定を定義できます。iPhone Configuration Utility または Exchange Management Console を使用する必要はありません。

管理プラグインは、*Kaspersky Security Center リモート管理システム*に統合されます。管理者は、Kaspersky Security Center の 1 つの管理コンソールを使用して、会社のネットワーク上のすべてのモバイルデバイスならびにクライアントコンピューターと仮想システムを管理できます。モバイルデバイスが管理サーバーに接続すると、そのデバイスは管理対象となります。管理者は管理対象デバイスを遠隔で監視できます。

Kaspersky Endpoint Security for Android モバイルアプリは、*Kaspersky Endpoint Security Cloud リモート管理システム*の一部としても動作させることができます。Kaspersky Endpoint Security Cloud によるアプリの使用方法の詳細については、*Kaspersky Endpoint Security Cloud オンラインヘルプ*を参照してください。

Kaspersky Endpoint Security for Android モバイルアプリは、AppConfig Community の参加者による EMM ソリューションの一部としても使用できます。

MMC ベースの管理コンソールでのモバイルデバイス管理の主な機能

Kaspersky Security for Mobile には、次の機能があります：

- Android デバイスを Kaspersky Security Center へ接続するためのメールメッセージを Google Play のリンクを使用して配信します。
- モバイルデバイスを Kaspersky Security Center、またはその他のサードパーティ製の EMM システム（VMware AirWatch、MobileIron、IBM Maas360、SOTI MobiControl など）に遠隔操作で接続します。
- Kaspersky Endpoint Security for Android と、Android デバイスのサービス、アプリ、機能を遠隔操作で設定します。
- 企業のセキュリティ要件に従ったモバイルデバイスの遠隔操作で設定します。
- 紛失時または盗難時にモバイルデバイスに保存された企業情報の流出を防止します（盗難対策）。
- 企業のセキュリティ要件に基づいたコンプライアンスを管理します（コンプライアンスコントロール）。
- モバイルデバイスでのインターネット使用を管理します。
- モバイルデバイスの企業メール（Microsoft Exchange メールサーバーが社内に配備された組織など）をセットアップします（iOS、Samsung デバイスのみ）。
- 企業ネットワーク（Wi-Fi、VPN）を設定し、VPN の使用をモバイルデバイスに許可します。VPN は、iOS と Samsung デバイスでのみ設定可能です。
- ポリシーのルール違反時に、Kaspersky Security Center に表示するモバイルデバイスのステータス表示を次から選択します：緊急、警告、または OK。
- Kaspersky Endpoint Security for Android のユーザーに表示される通知を設定します。

- Samsung KNOX 2.6 以降をサポートするデバイスを設定します。
- Android 仕事用プロファイルをサポートするデバイスの設定を編集します。
- Samsung KNOX Mobile Enrollment コンソールを使用して Kaspersky Endpoint Security for Android を導入します。Samsung KNOX Mobile Enrollment は、承認済みリセラーから購入した新しい Samsung デバイスへのアプリのインストールと初期設定を一括で処理する目的で使用されます。
- Kaspersky Security Center のポリシーを使用して、Kaspersky Endpoint Security for Android を特定のバージョンにアップグレードできるようになりました。
- Kaspersky Endpoint Security for Android のステータスとイベントに関する管理者からの通知を、Kaspersky Security Center またはメール経由で配信します。
- ポリシー設定の変更を管理します（リビジョンの履歴）。

Kaspersky Security for Mobile には、次の保護および管理コンポーネントが含まれます：

- アンチウイルス（Android デバイス）
- 盗難対策（Android デバイス）
- 危険サイトブロック（Android および iOS デバイス）
- アプリケーションコントロール（Android デバイス）
- コンプライアンスコントロール（Android デバイス）
- デバイスのルート権限の検出（Android デバイス）

Kaspersky Endpoint Security for Android アプリについて

Kaspersky Endpoint Security for Android アプリは、Web の脅威や、脅威となるその他のウイルスやプログラムからモバイルデバイスを保護します。

Kaspersky Endpoint Security for Android アプリには、次のコンポーネントが含まれます：

- **アンチウイルス**：定義データベースと Kaspersky Security Network クラウドサービスを使用して、デバイス上の脅威を検知し、処理します。アンチウイルスには次のコンポーネントがあります：
  - プロテクション：開かれるファイル内の脅威を検知し、新しいアプリをスキャンして、リアルタイムでデバイスの感染を防止します。
  - スキャン：要求に応じて、ファイルシステム全体、インストールされたアプリ、または選択したファイルまたはフォルダーに対して開始されます。
  - アップデート：新しい定義データベースをダウンロードできます。
- **盗難対策：**デバイスの紛失時または盗難時に、デバイス内の情報を不正なアクセスから保護します。この機能を使用して、デバイスへ次のコマンドを送信することができます：
  - **GPS 追跡**：デバイスの位置情報を取得します。
  - **遠隔アラーム**：デバイスのアラームを大音量で作動させます。

- **遠隔撮影**：デバイスのロックを誰かが解除しようとすると、デバイスのフロントカメラで写真が遠隔撮影されます。

- **企業データ消去**：企業の機密情報を保護するためデータを消去します。

- **危険サイトブロック：**悪意のあるコードを拡散するように設計された悪意のある Web サイトをブロックします。また、ユーザーの機密情報（オンラインバンキングや電子マネーシステムのパスワード）を盗んだり、ユーザーの金融情報にアクセスしたりするように設計された偽装 Web サイト（フィッシングサイト）もブロックします。危険サイトブロックは、Web サイトを開く前に、Kaspersky Security Network クラウドサービスを使用して、その Web サイトをスキャンします。スキャンが完了すると、信頼できる Web サイトが読み込まれ、悪意のある Web サイトはブロックされます。また、Kaspersky Security Network クラウドサービスで定義されたカテゴリを使用して Web サイトをフィルタリングすることもできます。これにより管理者は、Web サイトの特定のカテゴリ（例：「ギャンブル、宝くじ、懸賞」や「インターネットコミュニケーション」などのカテゴリに該当する Web サイト）へのユーザーのアクセスを制限できます。

- **アプリ管理：**この機能では、配布パッケージへの直リンクまたは Google Play へのリンクから、推奨アプリと必須アプリをデバイスにインストールできます。アプリ管理では、企業のセキュリティ要件に違反してブロックされているアプリを削除できます。

- **コンプライアンスコントロール：**管理対象デバイスが企業のセキュリティ要件に従っているかチェックし、従っていないデバイスの特定の機能を制限できます。

Kaspersky Device Management for iOS について

Kaspersky Device Management for iOS は、Kaspersky Security Center に接続するモバイルデバイスを保護および制御し、次のようなデバイス管理機能を提供します：

- **パスワードによる保護**：ユーザーが企業のパスワードポリシーに準拠した複雑なパスワードを使用するように、パスワードの複雑さの要件を定義します。

- **ネットワーク管理**：承認された VPN および Wi-Fi ネットワークを追加したり、その他へのアクセスを制限したりします。

- **企業データを消去する**：デバイスの紛失時や盗難時に、企業の機密情報を保護するため、消去コマンドを送信できます。

- **危険サイトブロック**：悪意のあるコードを拡散するように設計された悪意のある Web サイトをブロックします。また、ユーザーの個人情報（オンラインバンキングや電子マネーシステムのパスワード）を盗んだり、ユーザーの金融情報にアクセスしたりするように設計された偽の Web サイト（フィッシングサイト）もブロックします。危険サイトブロックは、Web サイトを開く前に、Kaspersky Security Network クラウドサービスを使用して、その Web サイトをスキャンします。スキャンが完了すると、信頼できる Web サイトが読み込まれ、悪意のある Web サイトはブロックされます。また、Kaspersky Security Network クラウドサービスで定義されたカテゴリを使用して Web サイトをフィルタリングすることもできます。これにより管理者は、Web サイトの特定のカテゴリ（例：「ギャンブル、宝くじ、懸賞」や「インターネットコミュニケーション」などのカテゴリに該当する Web サイト）へのユーザーのアクセスを制限できます。

- **アプリケーションの制限：**iTunes、Safari または Game Center などのネイティブアプリを監視対象デバイスで使用できるかどうかを制御します。

- **機能の制限：**管理対象デバイスが企業のセキュリティ要件に従っているかチェックし、従っていないデバイスの特定の機能を制限できます。

Exchange メールボックスについて

*Exchange メールボックス*は、Exchange ActiveSync サービスのクライアントアプリです。企業のユーザーのメール、カレンダー、連絡先、タスクを使った業務の支援を目的としています。Exchange メールボックスにより、モバイルデバイスを Microsoft Exchange サーバーに接続できます。Exchange ActiveSync サービスの詳細については、*Microsoft のテクニカルサポートサイト*を参照してください。

Exchange ActiveSync プロトコルを使用してモバイルデバイスを管理するには、Exchange サーバーが Microsoft Exchange サーバーにインストールされている必要があります。Exchange Server のインストールについて詳しくは、*Kaspersky Security Center のオンラインヘルプ*を参照してください。モバイルデバイスでの追加設定は必要ありません。

Exchange メールボックスを使用して、グループポリシーにより EAS デバイスを遠隔操作で設定すること、およびデータ消去コマンドを送信することができます。次のオペレーティングシステムが Exchange ActiveSync プロトコルをサポートしています：

- Windows Mobile
- Windows CE
- Windows Phone
- Android
- Bada
- BlackBerry 10
- iOS
- Symbian

Exchange ActiveSync デバイスの管理設定のセットの内容は、モバイルデバイスが実行しているオペレーティングシステムによって異なります。特定のオペレーティングシステムに対する Exchange ActiveSync プロトコルのサポート機能の詳細については、個々のオペレーティングシステムのガイドをご参照ください。

Kaspersky Endpoint Security for Android 管理プラグインについて

Kaspersky Endpoint Security for Android の管理プラグインは、Kaspersky Security Center の管理コンソールからモバイルデバイスおよびデバイスにインストールされているモバイルアプリを管理するためのインターフェイスを提供します。Kaspersky Endpoint Security for Android 管理プラグインは次の目的で使用できます：

- モバイルデバイスのためのグループセキュリティポリシーを作成する。
- ユーザーのモバイルデバイスの Kaspersky Endpoint Security for Android の動作を遠隔で設定する。
- ユーザーのデバイスの Kaspersky Endpoint Security for Android の動作に関するレポートと統計情報を受信する。

Kaspersky Security Center の導入時に、Kaspersky Endpoint Security Android 管理プラグインは既定でインストールされます。プラグインを個別にインストールする必要はありません。

Kaspersky Device Management for iOS 管理プラグインについて

Kaspersky Device Management for iOS の管理プラグインは、Kaspersky Security Center の管理コンソールから、iOS MDM および Exchange ActiveSync プロトコルを使用して接続されたモバイルデバイスを管理するためのインターフェイスを提供します。Kaspersky Device Management for iOS 管理プラグインは次の目的で使用できます：

- モバイルデバイスのためのグループセキュリティポリシーを作成する。
- Exchange ActiveSync プロトコルで接続されたデバイス（以後「EAS デバイス」と表記）を遠隔操作で設定する。
- iOS MDM プロトコルで接続されたデバイス（以後「iOS MDM デバイス」と表記）を遠隔操作で設定する。
- ユーザーのモバイルデバイスの動作に関するレポートと統計情報を受信する。

iOS MDM プロトコルおよび Exchange ActiveSync プロトコルでモバイルデバイスを Kaspersky Security Center へ接続する方法の詳細については、*Kaspersky Security Center のヘルプ*を参照してください。

Kaspersky Device Management iOS 管理プラグインは、Kaspersky Security Center の導入時に既定でインストールされます。プラグインを個別にインストールする必要はありません。

システム要件

このセクションでは、モバイルデバイスに本アプリを導入する際に使用する管理者用コンピューターのシステム要件と、Kaspersky Security for Mobile でサポートするモバイルデバイスのオペレーティングシステムについて説明します。

管理者用コンピューターのシステム要件

包括的なソリューションである Kaspersky Security for Mobile を導入するには、管理者のコンピューターが Kaspersky Security Center のハードウェア要件を満たしている必要があります。Kaspersky Security Center のハードウェア要件の詳細については、*Kaspersky Security Center のヘルプ*をご参照ください。

Kaspersky Endpoint Security の管理プラグインを使用するには、バージョン 12 以降の Kaspersky Security Center 管理コンソールを管理者のコンピューターにインストールしておく必要があります。

Kaspersky Device Management for iOS 管理プラグインを一緒に使用するには、管理者のコンピューターが次のソフトウェア要件を満たしている必要があります：

- Kaspersky Security Center 12 以降の管理コンソール
- Exchange サーバーのコンポーネント
- iOS MDM サーバーのコンポーネント
- SSE2 以降のバージョンの命令セット

管理サーバーから Kaspersky Endpoint Security for Android を導入するには、管理者のコンピューターが次のソフトウェア要件を満たしている必要があります：

- Kaspersky Security Center 12 以降
- Kaspersky Endpoint Security for Android 管理プラグイン

Kaspersky Endpoint Security for Android モバイルアプリを関連するオンラインストアから導入する場合、管理者のコンピューターに必要なソフトウェア要件はありません。

Kaspersky Endpoint Security for Android モバイルアプリは、Kaspersky Endpoint Security Cloud リモート管理システムの一部としても使用できます（バージョン 6.0 以降）。Kaspersky Endpoint Security Cloud によるアプリの使用方法の詳細については、*Kaspersky Endpoint Security Cloud のヘルプ*をご参照ください。

Kaspersky Endpoint Security for Android モバイルアプリは、サードパーティ製 EMM システムの中で使用できます。

- VMware AirWatch 9.3 以降
- MobileIron バージョン 10.0 以降
- IBM MaaS360 バージョン 10.68 以降
- Microsoft Intune 1908 以降
- SOTI MobiControl 14.1.4（1693）以降

Kaspersky Endpoint Security for Android のインストールに必要な、モバイルデバイスのシステム要件

Kaspersky Endpoint Security for Android のシステム要件は次の通りです：

- 画面解像度が 320 x 480 ピクセル以上のスマートフォンまたはタブレット
- デバイスのメインメモリの空き容量：65 MB
- Android 5.0〜12（Go Edition 以外の Android 12L を含む）
- x86、x86-64、Arm5、Arm6、Arm7、Arm8 プロセッサアーキテクチャ

本アプリは、デバイスのメインメモリにのみインストールされます。

iOS MDM プロファイルのハードウェアとソフトウェアの要件

iOS MDM プロファイル向けに、デバイスは次のハードウェアとソフトウェアの要件を満たしている必要があります：

- iOS 10.0〜15.0 または iPadOS 13〜15
- インターネット接続

既知の問題と注意点

Kaspersky Endpoint Security for Android には制限事項がありますが、アプリの動作には重大な影響を与えません。

アプリのインストールに関する既知の問題

- Kaspersky Endpoint Security for Android は、デバイスの内部ストレージにのみインストール可能です。
- Android バージョン 7.0 以降のデバイスでは、Kaspersky Endpoint Security for Android の管理者権限をデバイスの設定で無効にしようとするとエラーが発生する場合があります。これは、Kaspersky Endpoint Security for Android による他のウィンドウ上のオーバーレイが禁止されている場合に発生します。この問題は、Android 7 の既知の問題 によるものです。
- Android バージョン 7.0 以降のデバイスの Kaspersky Endpoint Security for Android は、マルチウィンドウに対応していません。
- Kaspersky Endpoint Security for Android は、Chrome オペレーティングシステムの Chromebook では動作しません。
- Kaspersky Endpoint Security for Android は、Android Go エディションのデバイスでは動作しません。
- Kaspersky Endpoint Security for Android アプリをサードパーティの EMM システム（VMware AirWatch など）で使用する場合は、アンチウイルスと危険サイトブロックのみが使用可能です。管理者は、EMM システムのコンソールで、アンチウイルスと危険サイトブロックを設定できます。この場合、アプリの動作に関する通知は、Kaspersky Endpoint Security for Android アプリにのみ表示されます（レポート）。

本アプリのアップグレードに関する既知の問題

- Kaspersky Endpoint Security for Android は、現在より新しいバージョンにのみアップグレード可能です。旧バージョンへのダウングレードはできません。
- スタンドアロンインストールパッケージを使用して Kaspersky Endpoint Security for Android をアップグレードするには、ユーザーのモバイルデバイスで提供元不明のアプリのインストールを許可しておく必要があります。
- Kaspersky Endpoint Security for Android が Google Play からインストールされた場合、Google Play からアップデートできます。他の方法を使用してインストールされた場合、Google Play からアップデートすることはできません。
- Kaspersky Endpoint Security for Android が Kaspersky Security Center からインストールされた場合、Kaspersky Security Center からアップデートできます。Google Play からインストールされた場合、Kaspersky Security Center からアップデートすることはできません。
- 管理プラグインの Technical Release 33 へのアップグレード後、 Kaspersky Endpoint Security for Android も Technical Release 33 へアップグレードする必要があります。アップグレードしない場合、一部のユーザーデバイスで Samsung KNOX をアクティベートできません。

アンチウイルスの動作に関する既知の問題

- 技術的な制限により、Kaspersky Endpoint Security for Android はサイズが 2 GB 以上のファイルをスキャンできません。スキャン中、そのようなファイルがスキップされたことを通知せずに、ファイルはスキップされます。

- 定義データベースに情報が追加されていない新しい脅威がデバイスに存在するかどうかを分析する場合は、Kaspersky Security Network の使用を有効にする必要があります。*Kaspersky Security Network（KSN）*は、ファイル、Web リソース、ソフトウェアの評価に関する情報を含むカスペルスキーのオンラインナレッジベースへのアクセスを提供する、クラウドサービスの基盤です。KSN を使用するには、モバイルデバイスがインターネットに接続している必要があります。

- 管理サーバーからモバイルデバイスへの定義データベースのアップデートが失敗する場合があります。その場合、定義データベースのアップデートタスクを管理サーバーで実行してください。

- 一部のデバイスでは、USB OTG で接続されたデバイスを Kaspersky Endpoint Security for Android が検出しません。検出されないデバイスに対しては、ウイルススキャンができません。

- Android 11.0 以降のデバイスでは、ユーザーは「すべてのファイルへのアクセス」権限を付与する必要があります。

- Android バージョン 7.0 以降のデバイスでは、ウイルススキャンのスケジュールを設定する画面が正しく表示されない場合があります（管理に関する項目が非表示になります）。この問題は、Android 7 の既知の問題によるものです。

- Android 7.0 のデバイスで、拡張モードのリアルタイム保護によって外付け SD カード上に保存されたファイル内の脅威が検知されません。

- Android バージョン 6.0 のデバイスでは、悪意のあるファイルがデバイスのストレージにコピーされた場合、Kaspersky Endpoint Security for Android は検知しません。アンチウイルスが悪意のあるファイルを検知する可能性があるのは、悪意のあるファイルの実行中、デバイスのウイルススキャンの実行中です。この問題は、Android 6.0 の既知の問題によるものです。デバイスのセキュリティを確保するために、ウイルススキャンのスケジュールを設定しておくことを推奨します。

危険サイトブロックに関する既知の問題

- 危険サイトブロックは、Google Chrome（カスタムタブ機能を含む）、Huawei Browser、Samsung Internet Browser でのみ動作します。仕事用プロファイルを使用しており、危険サイトブロックが仕事用プロファイルでのみ有効となるよう設定されている場合は、Samsung Internet Browser 用の危険サイトブロックはモバイルデバイス上でサイトをブロックしません。

- 仕事用プロファイルで使用する Kaspersky Endpoint Security は、HTTPS トラフィックを使用する Web サイトのドメインのみをスキャンします。悪意のある Web サイトまたはフィッシングサイトは、本アプリが仕事用プロファイルにインストールされている場合、ブロックされない可能性があります。ドメインが信頼済みである場合、危険サイトブロックは脅威をスキップします（例：`https://trusted.domain.com/phishing/`）。ドメインが信頼されていない場合、危険サイトブロックは悪意のある Web サイトおよびフィッシングサイトをブロックします。

- 危険サイトブロックを使用するには、Kaspersky Security Network の使用を有効にする必要があります。危険サイトブロックは、サイトの評価およびカテゴリに関する KSN のデータに基づいてサイトをブロックします。

- Android バージョン 6.0 以上で Google Chrome バージョン 51 以前がインストールされているデバイスでは、ブロック対象のサイトが危険サイトブロックでブロックされない場合があります。これは、サイトが次の方法で開かれている場合に発生します（この問題は Google Chrome の既知の問題によるものです）：

  - 検索結果から開いた場合
  - ブックマークリストから開いた場合
  - 検索履歴から開いた場合

- URL をオートコンプリートで入力した場合
- Google Chrome の新しいタブで Web サイトを開いた場合

- Google Chrome バージョン 50 以前がインストールされているデバイスでは、ブロック対象のサイトが危険サイトブロックでブロックされない場合があります。これは、サイトが**タブとアプリの統合**機能をブラウザーの設定で有効にし、Google の検索履歴からサイトを開くと発生します。この問題は、Google Chrome の既知の問題によるものです。
- ブロック対象カテゴリのサイトが Google Chrome でブロックされない場合があります。これは、サイトをサードパーティ製のアプリ（メッセンジャークライアントのアプリなど）から開くと発生します。この問題は、ユーザー補助機能サービスの Chrome カスタムタブ機能に対する動作に関係しています。
- ブロック対象のサイトが Samsung Internet Browser でブロックされない場合があります。これは、コンテキストメニューまたはサードパーティ製アプリ（メッセンジャークライアントのアプリなど）からバックグラウンドモードでサイトを開くと発生します。
- 危険サイトブロックを正常に動作させるには、Kaspersky Endpoint Security for Android をユーザー補助機能として設定しておく必要があります。
- 危険サイトブロックの設定に URL を入力する時は、次のルールに従ってください：
  - Android デバイスでは、`http:\/\/www\.example\.com.*` のように正規表現で URL を指定してください。
  - iOS MDM デバイスでは、`http://www.example.com` のように HTTP または HTTPS データ転送プロトコルに即した形式で URL を指定してください。
- 危険サイトブロックの［**リストの Web サイトのみを許可する**］を有効にして指定したサイトが、Samsung Internet Browser でページを更新すると、ブロックされる場合があります。正規表現が詳細な表現を含む場合（`^https?:\/\/example\.com\/pictures\/` など）、サイトがブロックされます。詳細な表現を含まない、`^https?:\/\/example\.com` などの正規表現の使用を推奨します。

盗難対策の動作に関する既知の問題

- Android デバイスへのタイムリーなコマンド送信を目的として、本アプリは Firebase Cloud Messaging（FCM）サービスを使用します。FCM を設定していない場合、ポリシーで設定したスケジュール（24 時間ごとなど）に基づいて Kaspersky Security Center とデバイスが同期される時のみにコマンドが送信されます。
- デバイスをロックするには、Kaspersky Endpoint Security for Android をデバイス管理者として設定しておく必要があります。
- Android 7.0 以降のデバイスをロックするには、Kaspersky Endpoint Security for Android をユーザー補助機能として設定しておく必要があります。
- 一部のデバイスでは、盗難対策コマンドの実行に失敗する場合があります。これは、デバイスの省電力モードを有効にしていると発生します。この問題は、Alcatel 5080X での発生が確認されています。
- Android 10.0 以降のデバイスの位置情報を特定するには、位置情報へのアクセス権を常に許可するように設定する必要があります。
- Android 11.0 以降のデバイスで遠隔撮影を実行するには、カメラへのアクセス権をアプリの使用時のみ許可するように設定する必要があります。

アプリ管理の動作に関する既知の問題

- アプリ管理を正常に動作させるには、Kaspersky Endpoint Security for Android をユーザー補助機能として設定しておく必要があります。
- アプリ管理（アプリのカテゴリ）を使用するには、Kaspersky Security Network の使用を有効にする必要があります。アプリ管理が使用するアプリのカテゴリは、KSN で使用可能なデータに基づいて決定します。KSN を使用するには、モバイルデバイスがインターネットに接続している必要があります。アプリ管理では、個別のアプリを許可またはブロックする対象のリストに追加できます。この場合、KSN の使用は不要です。
- アプリ管理の設定時には、［**システムアプリをブロックする**］をオフにすることを推奨します。システムアプリをブロックすると、デバイスの動作に問題が生じる可能性があります。

メール設定に関する既知の問題

- メールボックスを遠隔で設定可能なのは、以下のデバイスのみです：
  - iOS MDM デバイス
  - Samsung デバイス（Exchange ActiveSync）
  - TouchDown メールクライアントをインストールした Android デバイス

    以前のバージョンの Kaspersky Endpoint Security for Android では、Kaspersky Security Center を使用して、ユーザーのデバイスの TouchDown のプロファイルをリモートで設定できます。TouchDown のサポートは、Kaspersky Endpoint Security for Android Service Pack 4 以降では提供されません。詳細は、*Symantec のテクニカルサポートサイト*を参照してください。

    Kaspersky Endpoint Security for Android 管理プラグインのアップデート後、ポリシー内の TouchDown の設定は非表示になりますが、保存はされます。新しいデバイスが接続されると、TouchDown の設定はポリシーの適用後に変更されます。

    ポリシーが変更されたり保存されたりすると、TouchDown の設定は削除されます。ユーザーのデバイス上の TouchDown 設定は、ポリシーが適用されるとクリアされます。

デバイスのロック解除パスワードの長さに関する既知の問題

- Android 10.0 以降のデバイスでは、パスワードの強度要件（中程度または高強度）がシステムの値として実装されます。

  1～4 文字のパスワード長が必要な場合、中程度の強度のパスワードを設定するようユーザーに要求します。重複したり順番（例：1234）に並んでいたりしない数字（PIN）か、英字と数字の組み合わせである必要があります。PIN またはパスワードは、4 文字以上である必要があります。

  5 文字以上のパスワード長が必要な場合、高強度のパスワードを設定するようユーザーに要求します。重複したり順番に並んでいたりしない数字（PIN）か、英字と数字の組み合わせ（パスワード）である必要があります。PIN は 8 文字以上の数字で、パスワードは 6 文字以上である必要があります。
- Android 10.0 以降のデバイスでは、指紋での画面ロック解除の使用は仕事用プロファイルでのみ管理可能です。

- Android バージョン 7.1.1 のデバイスでは、ロック解除パスワードが企業のセキュリティ要件（コンプライアンスコントロール）を満たさない場合、そのパスワードを Kaspersky Endpoint Security for Android で変更しようとすると、Settings アプリ（システムアプリ）が正しく動作しない場合があります。この問題は、Android 7.1.1 の既知の問題によるものです。この場合、ロック解除パスワードを変更するには、Settings アプリ（システムアプリ）を使用するしか方法がありません。

- 一部の Android バージョン 6.0 以降のデバイスでは、画面のロックを解除するパスワードを入力するとエラーが発生する場合があります。これは、デバイスのデータを暗号化していると発生します。この問題は、MIUI ファームウェア端末のユーザー補助サービスの特定の機能に関係しています。

Wi-Fi 設定の既知の問題

- Android バージョン 8.0 以降のデバイスでは、Wi-Fi 用のプロキシサーバーの設定をポリシーで再定義できません。Wi-Fi 用のプロキシサーバーの設定を、モバイルデバイス上で手動で設定することは可能です。

APN 設定の既知の問題

- 遠隔での APN のリモート設定は、iOS MDM デバイスまたは Samsung デバイスでのみ可能です。

- iOS MDM デバイス向けの APN を［**セルラー通信**］セクションで設定します。［**APN**］セクションは使用されなくなりました。APN を設定する前に、［**端末に設定を適用する**］が［**APN**］セクションでオフになっていることを確認してください。

ファイアウォールの既知の問題

- ファイアウォールは、Samusung デバイスでのみ使用可能です。

VPN 設定の既知の問題

- VPN のリモート設定は、次のデバイスでのみ可能です：
  - iOS MDM デバイス
  - Samsung デバイス

コンテナーの仕様に関する既知の問題

- Kaspersky Security for Android Service Pack 3 Maintenance Release 2 では、コンテナーの作成をサポートしません。旧バージョンの製品で作成したコンテナーを Android デバイスに追加することは可能です。

- コンテナーアプリをインストールするには、ユーザーのモバイルデバイスで提供元不明のアプリのインストールを許可しておく必要があります。Google Play ストアを経由せずにアプリをインストールする方法の詳細は、*Android ヘルプ*を参照してください。

- 65 536 以上のメソッドを含むアプリに対して、Android デバイスではアプリコンテナー機能はサポートされません（Multidex 設定）。

アプリを削除から保護する際の既知の問題

- Kaspersky Endpoint Security for Android をデバイス管理者に設定しておく必要があります。
- Android 7.0 以降のデバイスでアプリが削除されないように保護するには、Kaspersky Endpoint Security for Android をユーザー補助機能として設定しておく必要があります。
- 一部の Xiaomi または Huawei デバイスでは、Kaspersky Endpoint Security for Android を削除から保護できません。この問題は、Xiaomi の MIUI 7 / 8 ファームウェアおよび Huawei の EMUI ファームウェアの特定の機能によるものです。

デバイスの制限の設定に関する既知の問題

- Android 10.0 以降のデバイスでは、Wi-Fi ネットワークの使用の禁止はサポートされていません。
- Android 10 以降のデバイスの場合、カメラの使用を完全には禁止できません。
- Android バージョン 11 以降のデバイスでは、Kaspersky Endpoint Security for Android をユーザー補助機能として設定しておく必要があります。初期設定ウィザードで Kaspersky Endpoint Security for Android をユーザー補助機能として設定するよう要求されます。このステップはスキップできます。また、後からデバイスの設定でサービスを無効にすることもできます。この場合、カメラの使用を制限することはできません。

モバイルデバイスにコマンドを送信する際の既知の問題

- Android 12 以降を実行しているデバイスでは、ユーザーが［おおよその位置情報］の権限を付与していても、 Kaspersky Endpoint Security for Android は最初に正確な位置情報を取得しようとします。これが成功しなかった場合、コマンドが 30 分以内に送信された場合のみ、おおよその位置情報が返されます。そうでない場合は **GPS 追跡**は失敗します。

Android 仕事用プロファイルの既知の問題

- ポリシーを使用して Android 仕事用プロファイルを作成する場合、Android 11 以降のデバイスにインストールされており、その作業プロファイルに関連する Kaspersky Endpoint Security for Android に、「すべてのファイルへのアクセス」権限をユーザーが付与する必要があります。

特定のデバイスで発生する既知の問題

- 一部のデバイス（Huawei、Meizu、Xiaomi など）では、Kaspersky Endpoint Security for Android に自動起動の権限を許可するか、オペレーティングシステム起動時に開始するアプリのリストに Kaspersky Endpoint Security for Android を手動で追加する必要があります。本アプリがリストに追加されていない場合、Kaspersky Endpoint Security for Android はモバイルデバイスの再起動後に全機能の実行を停止します。また、デバイスがロックされると、デバイスのロック解除コマンドを使用できません。デバイスのロックを解除するには、ロック解除用のワンタイムパスワードを使用するしか方法はありません。
- Android バージョン 6.0 以降の一部の Android デバイス（Meiz や Asus など）では、データを暗号化し、Android デバイスを再起動した後、デバイスのロックを解除するには、数字のパスワードの入力が必要です。パターンパスワードをデバイスのロック解除に使用している場合、ロック方法を数字のパスワードに変更する必要があります。パターンパスワードを数値のパスワードへ変換する方法の詳細については、モバイルデバイス製造元のテクニカルサポートサイトを参照してください。この問題は、ユーザー補助機能サービスの動作に関係しています。
- Android バージョン 5.X の Huawei デバイスでは、Kaspersky Endpoint Security for Android にユーザー補助機能を設定すると、十分な権限が不足しているという誤ったメッセージが表示されます。このメッセージを

非表示にするには、デバイスの設定で、本アプリを保護されたアプリに設定する必要があります。

- Android バージョン 5.X または 6.X の Huawei デバイスでは、省電力モードを Kaspersky Endpoint Security for Android に対して有効にすると、本アプリを手動で終了できます。終了すると、ユーザーのデバイスは保護されなくなります。この問題は、Huawei 製ソフトウェアの一部の機能に由来します。デバイスの保護を再度有効にするには、Kaspersky Endpoint Security for Android を手動で起動してください。デバイスの設定で、本アプリのバッテリーセーバーモードを無効にすることを推奨します。

- EMUI ファームウェアを搭載した Android バージョン 7.0 の Huawei デバイスでは、Kaspersky Endpoint Security for Android による保護機能に関する通知を非表示にできます。この問題は、Huawei 製ソフトウェアの一部の機能に由来します。

- 一部の Xiaomi デバイスでは、ポリシーでパスワードの長さを 5 文字以上に設定すると、ロック解除用パスワードを PIN コードの代わりに変更するように要求する通知が表示されます。5 文字を超える PIN コードは設定できません。この問題は、Xiaomi ソフトウェアの一部の機能に由来します。

- MIUI ファームウェアを搭載した Android バージョン 6.0 の Xiaomi デバイスでは、Kaspersky Endpoint Security for Android のアイコンがステータスバー上で非表示になる場合があります。この問題は、Xiaomi ソフトウェアの一部の機能に由来します。通知の設定でアイコン表示を許可することを推奨します。

- Android バージョン 6.0.1 の Nexus デバイスでは、Kaspersky Endpoint Security for Android のクイックスタートウィザード中に、正しい動作に必要な権限が許可されません。この問題は、Google 提供の Android 用セキュリティパッチの既知の問題によるものです。正常に動作させるには、デバイスの設定で必要な権限を手動で設定する必要があります。

- 一部の Android バージョン 7.0 以降の Samsung デバイスでは、デバイスがサポートしていないロック解除方法（パターンパスワードなど）を設定しようとするとデバイスがロックされる場合があります。発生条件は次の通りです：Kaspersky Endpoint Security for Android の削除からの保護が有効で、ロック解除のパスワードの強度要件を設定している場合。デバイスのロックを解除するには、特別なコマンドをデバイスに送信する必要があります。

- 一部の Samsung デバイスでは、画面のロック解除に指紋認証を使用することをブロックできません。

- 一部の Samsung デバイスでは、危険サイトブロックを有効にできません。これは、デバイスが 3G/4G ネットワークに接続し、省電力モードを有効にしており、バックグラウンドデータをブロックしていると発生します。バッテリーセーバーの設定で、バックグラウンドデータをブロックする設定を無効にすることを推奨します。

- 一部の Samsung デバイスでは、ロック解除用パスワードが企業のセキュリティ要件に準拠していない場合、Kaspersky Endpoint Security for Android は画面のロック解除での指紋認証の使用をブロックしません。

- 盗難対策コマンド（GPS 追跡、デバイスのロック、ロック解除、遠隔撮影など）の実行後、証明書と VPN 証明書が一部の Samsung デバイスで削除される場合があります。続行するには、証明書を再度インストールする必要があります。この問題は、MDFPP（Mobile Device Fundamentals Protection Profile）のセキュリティ基準に由来します。

- 一部の Honor デバイスと Huawei デバイスで、Bluetooth の使用を制限できません。本アプリが Bluetooth の使用の制限を試行すると、オペレーティングシステムが通知を表示します。通知には、この制限を拒否するか許可するか選択するオプションが含まれています。ユーザーはこの制限を拒否して Bluetooth の使用を継続できます。

- 一部の Samsung デバイスで、インストールパッケージからの Kaspersky Endpoint Security のインストールまたはアップデート後に、KNOX MDM プロファイルを有効化できません。

- Blackview デバイスでは、ユーザーは Kaspersky Endpoint Security for Android のメモリを消去できます。その結果、デバイスの保護と管理は無効になり、すべての定義された設定も無効になり、Kaspersky Endpoint Security for Android はユーザー補助機能から削除されます。これはこの製造元の端末が、カスタマイズされた最近の画面のアプリに強い権限を付与しているためです。このアプリは Kaspersky Endpoint Security

for Android の設定より優先され、また Android のオペレーティングシステムの一部であるため、置き換えることはできません。

- Android 11 の一部のデバイスで、Kaspersky Endpoint Security for Android が起動直後にクラッシュします。この問題は、既知の Android 11 の問題 によるものです。

導入

このヘルプセクションは、Kaspersky Security for Mobile をインストールする担当者、ならびに Kaspersky Security for Mobile を使用する組織にテクニカルサポートを提供する担当者を対象としています。

製品の構成

Kaspersky Security for Mobile には、次のコンポーネントが含まれます：

- Kaspersky Endpoint Security for Android モバイルアプリ

  Kaspersky Endpoint Security for Android アプリは、Web の脅威や、脅威となるその他のウイルスやプログラムからモバイルデバイスを保護します。Firebase Cloud Messaging を使用して、モバイルデバイスと Kaspersky Security Center 管理サーバー間の通信をサポートします。

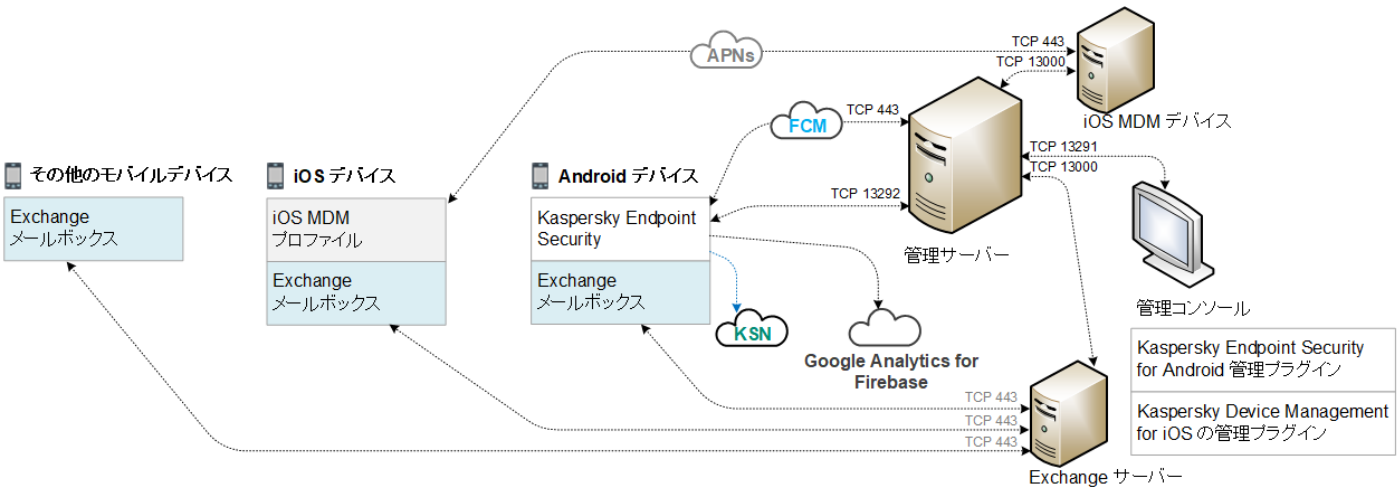
- Kaspersky Endpoint Security for Android 管理プラグイン

  Kaspersky Endpoint Security for Android の管理プラグインは、Kaspersky Security Center の管理コンソールからモバイルデバイスおよびデバイスにインストールされているモバイルアプリを管理するためのインターフェイスを提供します。

- Kaspersky Device Management for iOS 管理プラグイン

  Kaspersky Device Management for iOS の管理プラグインは、Kaspersky Security Center の管理コンソールから、iOS MDM および Exchange ActiveSync プロトコルを使用して接続されたモバイルデバイスを管理するためのインターフェイスを提供します。

Kaspersky Security for Mobile 統合ソリューションのアーキテクチャを下の図に示します。



Kaspersky Security for Mobile のアーキテクチャ

管理コンソール、管理サーバー、Exchange サーバー、iOS MDM サーバーの詳細は、*Kaspersky Security Center のヘルプ* を参照してください。

統合ソリューションの一般的な導入シナリオ

このセクションでは、Kaspersky Security for Mobile 統合ソリューションの一般的な導入シナリオについて説明します。

Android デバイスと iOS デバイスの統合ソリューションは、別の導入シナリオを使用して導入することもできます。組織で使用しているモバイルデバイスのオペレーションシステムが複数ある場合、各オペレーティングシステムに最適な導入シナリオに従って製品をインストールする必要があります。

Kaspersky Endpoint Security for Android の導入シナリオ

会社のネットワーク内で Kaspersky Endpoint Security for Android をモバイルデバイスに導入するには、いくつかの方法があります。自分の組織に最も適したシナリオを選択したり、複数の導入シナリオを組み合わせたりすることができます。

Kaspersky Endpoint Security Cloud で Kaspersky Endpoint Security for Android を導入する方法の詳細については、*Kaspersky Endpoint Security Cloud のヘルプ* を参照してください。

Kaspersky Security Center からの Kaspersky Endpoint Security for Android の導入

次の方法を使用して、Kaspersky Security Center から Kaspersky Endpoint Security for Android を導入できます：

- Google Play へのリンクが記載されたメッセージを配信する（推奨）
- スタンドアロンアプリパッケージへのリンクが記載されたメッセージを配信する

Google Play を使用して Kaspersky Endpoint Security for Android を導入するには、管理コンソールからデバイスのユーザーに Google Play へのリンクが記載されたメッセージを送信します。

スタンドアロンパッケージの配信により Kaspersky Endpoint Security for Android を導入するには、管理者は次のステップを実行します：

1. アプリのインストールパッケージを作成する。
2. インストールパッケージの設定を編集する。
3. スタンドアロンインストールパッケージを作成する。
4. スタンドアロンインストールパッケージのダウンロードリンクが含まれたメッセージを、Android デバイスのユーザーに送信する。一斉送信を使用できます。

ユーザーは、Kaspersky Security Center Web サーバーから Google Play へのリンクまたはインストールパッケージをダウンロードするためのリンクが記載されたメッセージを受信した後、モバイルデバイスに Kaspersky Endpoint Security for Android をインストールします。製品の使用を開始するために、他に必要な準備は一切ありません。

Google Play からの Kaspersky Endpoint Security for Android の導入

リモートインストールが可能でない場合は、Google Play からの導入シナリオを推奨します。

Kaspersky Endpoint Security for Android は、デバイスのユーザーによって Google Play から個別にインストールされます。ユーザーは Google Play からモバイルアプリ配布パッケージをダウンロードし、デバイスにアプリをインストールします。製品をデバイスにインストールした後、さらに管理サーバーへの接続を設定し証明書をインストールします。その後、製品の使用を開始できます。

KNOX Mobile Enrollment からの Kaspersky Endpoint Security for Android の導入

Kaspersky Endpoint Security for Android の導入にも、KNOX MDM プロファイルのモバイルデバイスへの追加が含まれます。KNOX MDM プロファイルには、Kaspersky Security Center の Web サーバー、または別のサーバーに導入されたアプリへのリンクが含まれています。本アプリのインストール後に、証明書もインストールする必要があります。

Samsung KNOX セクションで KNOX Mobile Enrollment を使用したインストールに関する情報を参照してください。

iOS MDM プロファイルの導入シナリオ

*iOS MDM プロファイル*は、iOS モバイルデバイスを Kaspersky Security Center に接続するための設定が含まれたプロファイルです。iOS MDM プロファイルをインストールし、Kaspersky Security Center と同期すると、そのデバイスは管理対象デバイスとなります。モバイルデバイスは、Apple Push Notification サービス（APNs）により管理されます。iOS MDM プロファイルのインストール方法と APNs 使用方法の詳細は、*Kaspersky Security Center のヘルプ*を参照してください。

iOS MDM プロファイルを使用して、次のことができます：

- グループポリシーを使用して iOS MDM デバイスを遠隔操作で設定する。
- デバイスロックコマンドとデータ消去コマンドを送信する。
- カスペルスキー製品とサードパーティのアプリを遠隔操作でインストールする。

会社のネットワーク内で iOS MDM プロファイルをモバイルデバイスに導入するには、いくつかの方法があります。自分の組織に最も適したシナリオを選択したり、複数の導入シナリオを組み合わせたりすることができます。

iOS MDM プロファイルを導入する前に、管理者は次の作業をしておく必要があります：

1. iOS MDM サーバーをインストールする。
2. Apple Push Notification サービス証明書（APNs 証明書）を取得する。
3. iOS MDM サーバーに APNs 証明書をインストールする。

iOS MDM サーバーのインストール方法と APNs 証明書の使用方法の詳細は、*Kaspersky Security Center のヘルプ*を参照してください。

Kaspersky Endpoint Security Cloud で iOS MDM プロファイルを導入する方法の詳細は、*Kaspersky Endpoint Security Cloud のヘルプ*を参照してください。

Kaspersky Security Center からの iOS MDM プロファイルの導入

Kaspersky Security Center からの iOS MDM プロファイルは、iOS MDM プロファイルをダウンロードするリンクが記載されたメッセージを送信して導入できます。一斉送信を使用できます。

ユーザーは、Kaspersky Security Center Web サーバーへのリンクが記載されたメッセージを受信した後、モバイルデバイスに iOS MDM プロファイルをインストールします。iOS MDM プロファイルのために、他に必要な準備は一切ありません。

iOS MDM プロファイルの作成に関する詳細は、*Kaspersky Security Center のオンラインヘルプ*を参照してください。

統合ソリューションを導入するための管理コンソールの準備

このセクションでは、統合ソリューションを導入するための管理コンソールの準備方法について説明します。

モバイルデバイスを接続するための管理サーバーの設定

モバイルデバイスを管理サーバーに接続するには、Kaspersky Endpoint Security モバイルアプリをインストールする前に、管理サーバーのプロパティでモバイルデバイスの接続を設定します。

モバイルデバイスを接続するために管理サーバーを設定するには：

1. 管理サーバーのコンテキストメニューから［**プロパティ**］を選択します。

   管理サーバーの設定ウィンドウが表示されます。

2. ［**管理サーバー接続設定**］-［**追加のポート**］の順に選択します。

3. ［**モバイルデバイス用ポートを開く**］をオンにします。

4. ［**モバイルデバイス用ポート**］で、モバイルデバイスが管理サーバーに接続するためのポートを指定します。

   既定ではポート 13292 が使用されます。［**モバイルデバイス用ポートを開く**］がオフの場合や、接続ポートの指定が正しくない場合、モバイルデバイスは管理サーバーに接続できません。

5. ［**モバイルクライアントを起動するポート**］で、Kaspersky Endpoint Security for Android のアクティベート時に、モバイルデバイスが管理サーバーへの接続に使用するポートを指定します。既定ではポート 17100 が使用されます。

6. ［**OK**］をクリックします。

管理コンソールでのモバイルデバイス管理フォルダーの表示

管理コンソールで［**モバイルデバイス管理**］フォルダーを表示することにより、管理サーバーにより管理されているモバイルデバイスのリストを表示したり、モバイルデバイスの管理設定を行ったり、ユーザーのモバイルデバイスに証明書をインストールしたりできます。

*管理コンソールでの［**モバイルデバイス管理**］フォルダーの表示を有効にするには：*

1. ［管理サーバー］フォルダーのコンテキストメニューから、［**表示**］-［**インターフェイスの設定**］の順に選択します。

2. 表示されるウィンドウで、［**モバイルデバイス管理の表示**］をオンにします。

3. ［**OK**］をクリックします。

管理コンソールを再起動すると、［**モバイルデバイス管理**］フォルダーが管理コンソールツリーに表示されます。

管理グループの作成

ユーザーのモバイルデバイスにインストールされた Kaspersky Endpoint Security for Android の設定を一元的に行うには、グループポリシーをデバイスに適用する必要があります。

デバイスのグループにポリシーを適用するには、ユーザーのデバイスにモバイルアプリをインストールする前に、［**管理対象デバイス**］にこれらのデバイス用の独立したグループを作成しておきます。

管理グループの作成後、アプリをインストールするデバイスをこのグループに自動的に割り当てるオプションを設定することを推奨しますグループポリシーを使用して、すべてのデバイスに共通の設定を行います。

管理グループを作成するには、次の操作を行います：

1. コンソールツリーで、［**管理対象デバイス**］フォルダーを開きます。

2. ［**管理対象デバイス**］フォルダーの作業領域またはサブフォルダーの作業領域で、［**デバイス**］タブを選択します。

3. ［**新規グループ**］をクリックします。
ウィンドウが開き、新しいグループを作成できます。

4. ［**グループ名**］ウィンドウでグループ名を入力し、［**OK**］をクリックします。

指定した名前の新しい管理グループフォルダーがコンソールツリーに表示されます。管理グループの使用方法の詳細については、*Kaspersky Security Center のヘルプ*を参照してください。

デバイスを管理グループに自動的に割り当てるためのルールの作成

ユーザーのモバイルデバイスにインストールされた Kaspersky Endpoint Security for Android アプリの設定を一元的に管理するには、事前に作成した管理グループにデバイスを追加し、その管理グループにはグループポリシーを設定しておく必要があります。

ネットワークで検出されたモバイルデバイスを管理グループに自動的に割り当てるルールが設定されていない場合、デバイスは管理サーバーとの初回同期時に、管理コンソールの［**詳細**］→［**ネットワークポーリング**］→［**ドメイン**］→［**KES10**］フォルダーに自動的に送信されます。グループポリシーはこのデバイスには適用されません。

モバイルデバイスを管理グループに自動的に割り当てるルールを作成するには、次の操作を行います：

1. コンソールツリーで、［**未割り当てデバイス**］フォルダーを開きます。

2. ［**未割り当てデバイス**］フォルダーのコンテキストメニューから［**プロパティ**］を選択します。
未割り当てデバイスのプロパティウィンドウが表示されます。

3. ［**デバイスの移動**］セクションの［**追加**］をクリックすると、管理グループにデバイスを自動的に割り当てるルールの作成が開始されます。

   ［**新規ルール**］ウィンドウが表示されます。

4. ルール名を入力します。

5. Kaspersky Endpoint Security for Android をモバイルデバイスにインストールした後に、そのデバイスを割り当てる管理グループを指定します。そのためには、［**デバイスの移動先グループ**］の右側にある［**参照**］をクリックし、表示されるウィンドウからグループを選択します。

6. ［**ルールの適用**］セクションで、［**各デバイスにつき 1 回**］を選択します。

7. ［**どの管理グループにも属していないデバイスのみ移動する**］をオンにすると、ルールを適用する時に、他の管理グループに割り当て済みであるモバイルデバイスは、選択したグループに割り当てられません。

8. ［**ルールを有効にする**］をオンにすると、新しく検出されるデバイスにルールを適用できます。

9. ［**アプリケーション**］セクションを開き、次の操作を行います：

   a. ［**OS のバージョン**］をオンにします。

   b. 指定したグループに割り当てるデバイスのオペレーティングシステムの種別を選択します：Android または iOS。

10. ［**OK**］をクリックします。

    ルールが作成されると、［**未割り当てデバイス**］フォルダーのプロパティウィンドウの［**デバイスの移動**］セクションのデバイス割り当てルールのリストに表示されます。

ルールに従って、Kaspersky Security Center は指定した要件を満たしているすべてのデバイスを［**未割り当てデバイス**］フォルダーから選択されたグループに割り当てます。また、［**未割り当てデバイス**］フォルダーにそれまでに割り当てられていたモバイルデバイスを［**管理対象デバイス**］フォルダーの必要な管理グループに手動で割り当てることもできます。管理グループの管理と未配信デバイスでの処理の詳細については、*Kaspersky Security Center のヘルプ*を参照してください。

証明書の作成

モバイルデバイスのユーザーを識別するために、管理コンソールで証明書を作成する必要があります。

証明書を作成するには：

1. コンソールツリーで、［**モバイルデバイス管理**］→［**証明書**］の順に選択します。

2. ［**証明書**］フォルダーの作業領域で、［**証明書の追加**］をクリックして、証明書インストールウィザードを開始します。

3. ウィザードの［**証明書の種別**］ウィンドウで、［**一般証明書**］を選択します。

4. ウィザードの［**ユーザーの選択**］ウィンドウで、証明書作成の対象となるユーザーを指定します。

5. ウィザードの［**証明書ソース**］ウィンドウで、証明書を作成する方法を選択します。

   - 管理サーバーツールを使用して自動的に証明書を作成するには、［**管理サーバーツール経由で証明書を指定する**］を選択します。

- あらかじめ作成されている証明書をユーザーに割り当てるには、［**証明書ファイルを指定する**］を選択します。［**指定**］をクリックして［**証明書**］ウィンドウを開き、証明書ファイルを指定します。

  モバイルデバイスの種別と、証明書の作成を通知する方法を指定しない場合は、［**証明書の発行**］をオフにします。

6. ウィザードの［**ユーザー通知方法**］ウィンドウで、テキストメッセージまたはメールを使って証明書の作成をユーザーに通知するモバイルデバイスの設定を行います。

7. ウィザードの［**証明書の生成中**］ウィンドウで［**完了**］をクリックして、証明書インストールウィザードを終了します。

これにより、ユーザーがモバイルデバイスにインストールできる証明書が作成されます。証明書を取得するために、モバイルデバイスと管理サーバーとの同期を開始します。証明書の作成および証明書の発行ルールの設定に関する詳細は、*Kaspersky Security Center のヘルプ*を参照してください。

Kaspersky Endpoint Security for Android のインストール

このセクションでは、会社のネットワークに Kaspersky Endpoint Security for Android を導入する方法について説明します。

権限

アプリのすべての機能について、Kaspersky Endpoint Security for Android は権限をユーザーに要求します。必須権限が要求されるのは、セットアップウィザードの完了時、およびインストール後にアプリの個々の機能を使用する前です。必須権限を提供せずに Kaspersky Endpoint Security for Android をインストールすることはできません。

一部のデバイス（Huawei、Meizu、Xiaomi など）では、デバイスの設定で、オペレーティングシステム起動時に開始するアプリのリストに Kaspersky Endpoint Security for Android を手動で追加する必要があります。本アプリがリストに追加されていない場合、Kaspersky Endpoint Security for Android はモバイルデバイスの再起動後に全機能の実行を停止します。

Android 11.0 以降のデバイスでは、システム設定［**アプリが使用されていない場合に権限を削除**］を無効にする必要があります。無効にしないと、本アプリが数か月使用されなかった場合、ユーザーが本アプリに付与した権限がシステムによって自動的にリセットされます。

着信拒否の機能は、Kaspersky Endpoint Security for Android Service Pack 4 Update 4（ビルド 10.8.0.103）ではサポートされません。この場合、Kaspersky Endpoint Security for Android は SMS の権限についてユーザーに通知しません。着信拒否および SIM 監視の機能を動作させるには、旧バージョンの Kaspersky Endpoint Security for Android を使用する必要があります。

Kaspersky Endpoint Security for Android により要求される権限

権限	アプリの機能
電話（Android 5.0～9.X でのみ必要）	Kaspersky Security Center への接続（デバイス ID）
ストレージ（必須）	アンチウイルス

すべてのファイルへのアクセス	危険サイトブロック（Android 11 以降のみ）
付近の Bluetooth デバイス（Android 12 以降）	Bluetooth の使用制限
デバイス管理者（必須）	盗難対策 ― デバイスのロック（Android 5.0～6.X のみ）
	盗難対策 - フロントカメラによる遠隔撮影
	盗難対策 - アラーム音
	盗難対策 - 完全リセット
	パスワードによる保護
	アプリ削除に対する保護
	セキュリティ証明書のインストール
	アプリ管理
	KNOX の管理（Samsung デバイスのみ）
	Wi-Fi の設定
	Exchange ActiveSync の設定
	カメラ、Bluetooth、Wi-Fi の使用制限
カメラ	盗難対策 - フロントカメラによる遠隔撮影 Android 11.0 以降のデバイスでは、デバイスに要求された際に、アクセス権をアプリの使用中のみ許可するように設定する必要があります。
位置情報	盗難対策 - デバイスの GPS 追跡 Android 10.0 以降のデバイスでは、デバイスに要求された際に、アクセス権を常に許可するように設定する必要があります。
ユーザー補助	盗難対策 - デバイスのロック（Android 7.0 以降のみ）
	危険サイトブロック
	アプリ管理
	アプリ削除に対する保護（Android 7.0 以降のみ）
	Kaspersky Endpoint Security for Android による警告の表示（Android 10.0 以降のみ）
	カメラの使用の制限（Android 11 以降のみ）

Google Play のリンクを使用した Kaspersky Endpoint Security for Android のインストール

Kaspersky Endpoint Security for Android は、ユーザーアカウントが Kaspersky Security Center に追加されているユーザーのモバイルデバイスにインストールされます。Kaspersky Security Center のユーザーアカウントの詳細は、Kaspersky Security Center のヘルプを参照してください。

Kaspersky Security for Mobile を使用すると、Google Play リンクを使用して Kaspersky Security Center からアプリをインストールできます（推奨する方法）。

ユーザーは Google Play へのリンクを受信します。アプリは、次に示す Android プラットフォームの標準的なインストール方法でインストールできます。インストール後に Kaspersky Endpoint Security for Android を追加設定する必要はありません。

Huawei および Honor の一部のデバイスは、Google サービスが使用できないので、Google Play のアプリへアクセスできません。Huawei および Honor の一部の端末のユーザーが Google Play からアプリをインストールできない場合は、Huawei AppGallery からインストールする必要があります。

リンクには次のデータが含まれています：

- Kaspersky Security Center の同期設定。
- 証明書。
- Kaspersky Endpoint Security for Android の使用許諾契約書および追加声明の条項への同意を示すフラグ。使用許諾契約書および追加声明の条項に管理コンソール上で管理者が同意すると、Kaspersky Endpoint Security for Android のインストール中に同意のステップがスキップされます。

Google Play リンクを使用して Kaspersky Security Center から Kaspersky Endpoint Security for Android をインストールするには：

1. コンソールツリーで、［**モバイルデバイス管理**］→［**モバイルデバイス**］の順に選択します。
2. ［**モバイルデバイス**］フォルダーの作業領域で［**モバイルデバイスの追加**］をクリックします。
   新規モバイルデバイス接続ウィザードが開始されます。ウィザードの指示に従います。
3. ウィザードの［**オペレーティングシステム**］ウィンドウで［**Android**］を選択します。
   Kaspersky Security Center が、管理プラグインのアップデートをチェックします。アップデートが検出された場合、新しいバージョンの管理プラグインをインストールできます。管理プラグインのアップデート時に、Kaspersky Endpoint Security for Android の使用許諾契約書（EULA）および追加声明の条項に同意できます。使用許諾契約書および追加声明の条項に管理コンソール上で管理者が同意すると、Kaspersky Endpoint Security for Android のインストール中に同意のステップがスキップされます。この機能は、Kaspersky Security Center バージョン 12 でのみ使用可能です。
4. ［**Kaspersky Endpoint Security for Android のインストール方法**］で、［**Google Play のリンクを使用**］をアプリをインストールする方法として選択します。
5. ウィザードの［**ユーザーを選択してください**］ウィンドウで、モバイルデバイスに Kaspersky Endpoint Security for Android をインストールするユーザーを 1 人または複数選択します。
   ユーザーがリストにない場合、新規モバイルデバイス接続ウィザードを終了せずに、新しいユーザーアカウントを追加できます。
6. ウィザードの［**証明書ソース**］ウィンドウで、Kaspersky Endpoint Security for Android と Kaspersky Security Center 間のデータ転送を保護するための証明書のソースを選択します：
   - **管理サーバーツールから証明書を発行する：**この場合、証明書は自動的に作成されます。

- **証明書ファイルを指定する**：この場合、独自の証明書を事前に準備しておき、それをウィザードのウィンドウで選択する必要があります。このオプションは、複数のモバイルデバイスに Kaspersky Endpoint Security for Android をインストールする場合には使用できません。ユーザーごとに個別の証明書を作成する必要があります。

7. ウィザードの［**ユーザー通知方法**］ウィンドウで、アプリのインストールリンクを転送するために使用するチャネルを選択します：

   - メールでリンクを送信するには、［**Kaspersky Endpoint Security にリンクを送信**］を選択し、［**メール**］セクションで設定を行います。ユーザーアカウントの設定でメールアドレスが指定されていることを確認してください。

   - SMS メッセージでリンクを送信するには、［**Kaspersky Endpoint Security にリンクを送信**］を選択し、［**SMS 経由**］セクションで設定を行います。ユーザーアカウントの設定で電話番号が指定されていることを確認してください。

   - QR コードを使用して Kaspersky Endpoint Security for Android をインストールするには、［**インストールパッケージへのリンクを表示**］を選択し、モバイルデバイスのカメラを使用して QR コードをスキャンします。

   - リストされたどの方法も適切ではない場合、［**インストールパッケージへのリンクを表示**］→［**コピー**］の順に選択して、Kaspersky Endpoint Security for Android をインストールするためのリンクをクリップボードにコピーします。使用可能ないずれかの方法で、アプリのインストールリンクを配信します。Kaspersky Endpoint Security for Android をインストールする別の方法も使用できます。

8. ［**終了**］をクリックして新規モバイルデバイス接続ウィザードを終了します。

Kaspersky Endpoint Security for Android をユーザーのモバイルデバイスにインストールした後、グループポリシーを使用してデバイスとアプリを設定できます。また、デバイスの紛失時や盗難時には、データ保護のためにモバイルデバイスにコマンドを送信することもできます。

Kaspersky Endpoint Security for Android をインストールする他の方法

Kaspersky Endpoint Security for Android を、自社の Web サーバーへのリンクを使用するか、手動でのインストール方法をユーザーに指示することでインストールできます。

Google Play または Huawei AppGallery からの手動インストール

ユーザーは、Kaspersky Endpoint Security for Android を Google Play または Huawei AppGallery から手動でインストールできます。アプリは、次に示す Android プラットフォームの標準的なインストール方法でインストールできます。本アプリをインストールするには、ユーザー自身の Google アカウントを使用します。

Google Play から Kaspersky Endpoint Security for Android をインストールする手順の詳細については、Google のテクニカルサポートサイトを確認してください。

Huawei AppGallery から Kaspersky Endpoint Security for Android をインストールする手順の詳細については、Huawei のサポートサイトを確認してください。

Huawei および Honor の一部のデバイスは、Google サービスが使用できないので、Google Play のアプリへアクセスできません。Huawei および Honor の一部の端末のユーザーが Google Play からアプリをインストールできない場合は、Huawei AppGallery からインストールする必要があります。

Google Play または Huawei AppGallery から Kaspersky Endpoint Security for Android をインストールした後は、アプリを使用するための準備が必要です。アプリを使用するための準備として、次のステップを実行します：

1. 管理者は、モバイルデバイスと管理サーバー（サーバーのアドレスとポート番号）の同期設定を、利用可能な任意の方法（メール送信など）で送信します。

2. ユーザーは、初期設定ウィザードの動作中または Kaspersky Endpoint Security for Android の設定で、モバイルデバイスと管理サーバーの同期を設定できます。

3. 管理者は、モバイルデバイスユーザーに対して証明書を作成します。

4. ユーザーは、証明書をインストールするかどうかの通知を自動で受信します。確定すると、証明書がモバイルデバイスにインストールされます。

管理サーバーと同期するには、モバイルデバイスのインターネットアクセスを有効にしておく必要があります。

モバイルデバイスと管理サーバーの同期の設定方法および証明書の取得方法については、『Kaspersky Security Center ヘルプ』を参照してください。

モバイルデバイスと管理サーバーの次回の同期中に、Kaspersky Endpoint Security for Android がインストールされたユーザーのモバイルデバイスは、［**詳細**］→［**ネットワークポーリング**］→［**ドメイン**］フォルダーの、アプリのインストール時に指定した管理グループに移動します（既定のグループは **KES10**）。手動で、または自動割り当てルールを使用して、［管理対象デバイス］フォルダーで作成した管理グループにモバイルデバイスを移動できます。

このインストール方法は、特定のバージョンの Kaspersky Endpoint Security for Android をインストールする場合に便利です。

自社の Web サーバーへのリンクを使用して Kaspersky Endpoint Security for Android をインストールするには：

1. インストールパッケージを作成し、設定します。

   *インストールパッケージ*は、Kaspersky Security Center を使用してアプリを遠隔操作でインストールする目的で作成されたファイルのセットです。

2. スタンドアロンインストールパッケージを作成します。

   *スタンドアロンインストールパッケージ*は、アプリと管理サーバーを接続するための設定を含むモバイルアプリのインストールファイルです。Kaspersky Endpoint Security for Android の使用許諾契約書（EULA）の条項への同意を示すフラグも含まれています。Kaspersky Endpoint Security for Android インストールパッケージをベースに作成されます。スタンドアロンパッケージは、特殊なインストールパッケージです。

ユーザーは、Kaspersky Endpoint Security for Android のスタンドアロンインストールパッケージが配置されている Web サーバーへのリンクを受信します。アプリをインストールするには、ユーザーは APK ファイルを実行する必要があります。インストール後に Kaspersky Endpoint Security for Android を追加設定する必要はありません。

自社の Web サーバーへのリンクを使用して Kaspersky Endpoint Security for Android をアップグレードするには、ユーザーのモバイルデバイスで提供元不明のアプリのインストールを許可しておく必要があります。

インストールパッケージの作成と設定

Kaspersky Endpoint Security の Android インストールパッケージは、自己解凍圧縮ファイル `sc_package.exe` です。パッケージには、デバイスにモバイルアプリをインストールするために必要なファイルが含まれています。

- `adb.exe`、`AdbWinApi.dll`、`AdbWinUsbApi.dll` - Kaspersky Endpoint Security for Android をインストールするために必要なファイルのセット。
- `installer.ini` - 管理サーバー接続設定が入った設定ファイル。
- `kesandroid10.x.x.xx_ja_Prod_Release.apk` - Kaspersky Endpoint Security for Android のセットアップファイル。
- `kmlisten.exe` - ワークステーションから製品のインストールパッケージを配布するためのツール。
- `kmlisten.ini` - インストールパッケージ配布ツール用の設定が入った設定ファイル。
- `kmlisten.kpd` - 製品記述ファイル。

Kaspersky Endpoint Security for Android インストールパッケージを作成するには：

1. コンソールツリーで、［**詳細**］→［**リモートインストール**］→［**インストールパッケージ**］フォルダーの順に選択します。
2. ［**インストールパッケージ**］フォルダーの作業領域で［**インストールパッケージの作成**］をクリックします。

   インストールパッケージ作成ウィザードが起動します。ウィザードの指示に従います。
3. ［**インストールパッケージの種別の選択**］ウィンドウで、［**カスペルスキー製品のインストールパッケージを作成する**］をクリックします。
4. ウィザードの［**インストールパッケージ名の定義**］ウィンドウで、インストールパッケージの名前を入力します。この名前は、作業領域の［**インストールパッケージ**］フォルダーに表示されます。
5. ウィザードの［**インストールする配布パッケージの選択**］ウィンドウで、配布キットに含まれる自己解凍圧縮ファイル `sc_package.exe` を選択します。

   圧縮ファイルを解凍済みの場合は、製品記述ファイル `kmlisten.kpd` を選択します。アプリケーション名とバージョン番号が入力フィールドに表示されます。
6. ウィザードの［**使用許諾契約書の条項に同意**］ウィンドウで、使用許諾契約書の内容を確認し、理解した上で条項に同意します。

   インストールパッケージを作成するには、使用許諾契約書の条項に同意する必要があります。使用許諾契約書の条項に管理コンソール上で同意すると、Kaspersky Endpoint Security for Android のインストール中に同意のステップがスキップされます。

   モバイルデバイスの保護を停止する場合は、Kaspersky Endpoint Security for Android アプリをアンインストールして、使用許諾契約書（EULA）を取り消すことができます。使用許諾契約の取り消しについて詳しくは、*Kaspersky Security Center のヘルプ*を参照してください。

ウィザード終了後、作成されたインストールパッケージが［**インストールパッケージ**］フォルダーの作業領域に表示されます。このインストールパッケージは、管理サーバーのパブリック共有フォルダーの［Packages］フォルダーに保管されます。

インストールパッケージの設定を行うには：

1. コンソールツリーで、［**詳細**］→［**リモートインストール**］→［**インストールパッケージ**］フォルダーの順に選択します。

2. Kaspersky Endpoint Security for Android インストールパッケージのコンテキストメニューで、［**プロパティ**］を選択します。

3. ［**設定**］タブで、モバイルデバイスの管理サーバー接続設定と、モバイルデバイスが管理サーバーとの初回同期後に自動的に追加される管理グループの名前を指定します。次の手順に従ってください：

   - ［**管理サーバーへの接続**］セクションの［**サーバーのアドレス**］に、モバイルデバイス用の管理サーバーの名前を入力します。この名前は、管理サーバーの導入時に**モバイルデバイスサポート**をインストールするために使用した形式で入力します。

     モバイルデバイスサポートの管理サーバー名の形式に応じて、管理サーバーの DNS 名または IP アドレスを指定します。［**SSL ポート番号**］に、モバイルデバイスを接続するために管理サーバーで開いているポートの番号を指定します。既定ではポート 13292 が使用されます。

   - ［**グループへのコンピューターの割り当て**］セクションの［**グループ名**］に、管理サーバーとの初回同期後のモバイルデバイスを追加するグループの名前を入力します（既定では **KES10** が使用されます）。

     指定したグループが［**詳細**］→［**ネットワークポーリング**］→［**ドメイン**］フォルダーに自動的に作成されます。

   - 本アプリの初回起動時に、会社のメールアドレスをユーザーに要求するように設定するには、［**インストール中の処理**］で、［**メールアドレスの要求**］をオンにします。

     このメールアドレスは、モバイルデバイスを管理グループに追加する時、そのデバイスの名前に使用されます。

4. 指定した設定を適用するには、［**適用**］をクリックします。

スタンドアロンインストールパッケージの作成

スタンドアロンインストールパッケージを作成するには、次の操作を行います：

1. コンソールツリーで、［**詳細**］→［**リモートインストール**］→［**インストールパッケージ**］フォルダーの順に選択します。

2. Kaspersky Endpoint Security for Android のインストールパッケージを選択します。

3. インストールパッケージのコンテキストメニューから［**スタンドアロンインストールパッケージの作成**］を選択します。

   スタンドアロンインストールパッケージを作成するウィザードが起動します。ウィザードの指示に従います。

4. スタンドアロンインストールパッケージの配信方法を設定します：

   - 作成したスタンドアロンインストールパッケージへのパスをメールでユーザーに配信するには、［**次の処理**］セクションで［**スタンドアロンインストールパッケージのリンクをメールで送信**］をクリックします。

     メッセージを編集するウィンドウが開きます。ウィンドウのテキストに、スタンドアロンインストールパッケージが配置されている共有フォルダーへのパスが含まれています。

- 作成したスタンドアロンインストールパッケージへのリンクを会社の Web サイトに掲載するには、［**Web サイト公開リンク用サンプル HTML**］をクリックします。

  HTML_RJL リンクが含まれた tmp ファイルが開きます。

5. 作成したスタンドアロンインストールパッケージを Kaspersky Security Center Web サーバーで公開し、選択したインストールパッケージのスタンドアロンパッケージの全リストを表示するには、［**スタンドアロンインストールパッケージ作成ウィザードが完了しました**］ウィンドウで［**スタンドアロンパッケージのリストを開く**］をオンにします。

ウィザードが閉じた後、［**インストールパッケージ「<インストールパッケージ名>」のスタンドアロンパッケージのリスト**］ウィンドウが開きます。

［**インストールパッケージ「<インストールパッケージ名>」のスタンドアロンパッケージのリスト**］ウィンドウには、次の情報が含まれます：

- スタンドアロンインストールパッケージのリスト
- 共有フォルダーへのネットワークパス（［**パス**］に表示）
- Kaspersky Security Center Web サーバーでのスタンドアロンパッケージのアドレス（［**URL**］に表示）

メール通知を送信する場合、ユーザーがアプリのセットアップファイルをダウンロードできるリソースとして、［**URL**］にアドレスを指定するか、［**パス**］にパスを指定できます。ユーザーにテキストメッセージ通知を送信する場合、［**URL**］に表示されているダウンロードリンクを指定する必要があります。

作成したスタンドアロンパッケージのアドレスをクリップボードにコピーして、必要なインストールパッケージへのリンクをユーザーへのメール通知またはテキストメッセージ通知に貼り付けてください。

同期の設定

モバイルデバイスを管理し、ユーザーのモバイルデバイスからレポートや統計情報を受信するには、同期を設定する必要があります。Kaspersky Security Center とモバイルデバイスの同期は、次のように実行されます：

- **スケジュール**：スケジュールに基づく同期は、HTTP プロトコルを使用して実行されます。同期スケジュールは、グループポリシーの設定で指定できます。グループポリシーの設定変更、コマンド、タスクは、スケジュールに基づいてデバイスが Kaspersky Security Center と同期すると実行されます（同期するまで、実行が遅延します）。既定では、モバイルデバイスと Kaspersky Security Center との同期は 6 時間ごとに自動的に実行されます。

  Android 12 以降のデバイスでは、バッテリー節約モードの場合、タスクの実行が指定よりも遅れる場合があります。

- **強制**：強制的な同期は、FCM サービス（Firebase Cloud Messaging）のプッシュ通知を使用して実行されます。強制的な同期は、モバイルデバイスへのコマンドのタイムリーな配信を主な目的としています。強制的な同期を使用する場合は、GSM が Kaspersky Security Center で設定されていることを確認してください。詳細については、Kaspersky Security Center のヘルプを参照してください。

モバイルデバイスと Kaspersky Security Center との同期を設定するには：

1. コンソールツリーの［**管理対象デバイス**］フォルダーで、デバイスが属する管理グループを選択します。

2. 選択したグループの作業領域で、［**ポリシー**］タブを選択します。

3. 任意の列をダブルクリックして、ポリシーのプロパティウィンドウを開きます。

4. ポリシーの**プロパティ**ウィンドウで、［**同期**］セクションを選択します。

5. ［**同期**］ドロップダウンリストから同期の頻度を選択します。

6. デバイスがローミング中の場合に Kaspersky Security Center との同期を無効にするには、［**ローミング中は同期しない**］をオンにします。

   デバイスユーザーは同期を手動で実行するようにアプリを設定できます（→［**設定**］→［**同期**］→［**同期**］）。

7. アプリの設定で同期設定（サーバーアドレス、ポート、管理グループ）をユーザーに対して非表示にするには、［**デバイスの同期の設定を表示する**］をオフにします。非表示の設定を変更することはできません。

8. ［**適用**］をクリックして、変更を保存します。

モバイルデバイスと Kaspersky Security Center との次回の同期時に、デバイスに設定が適用されます。モバイルデバイスの同期は、専用のコマンドを使用して手動で実行することでもできます。モバイルデバイスのコマンドの使用については、*Kaspersky Security Center のヘルプ*を参照してください。

Kaspersky Endpoint Security for Android アプリのアクティベーション

Kaspersky Security Center では、ライセンスによってその適用対象の機能が異なります。Kaspersky Security for Mobile を完全に機能させるには、組織が購入した Kaspersky Security Center ライセンスを**モバイルデバイス管理**機能のために使用する必要があります。**モバイルデバイス管理**機能は、モバイルデバイスを Kaspersky Security Center に接続し、接続されたデバイスを管理することを目的としています。

Kaspersky Security Center のライセンス管理とライセンスオプションの詳細は、*Kaspersky Security Center のヘルプ*を参照してください。

モバイルアプリの Kaspersky Endpoint Security for Android のアクティベートは、有効なライセンス情報を本アプリに追加することで完了します。ライセンス情報は、Kaspersky Security Center とモバイルデバイスの同期時に、ポリシーと一緒にデバイスに送信されます。

デバイスにインストールされた時点から 30 日以内に本アプリのアクティベーションが完了しなかった場合、アプリは自動的に機能制限モードに切り替わります。このモードでは、ほとんどのアプリ機能は機能しません。機能制限モードに切り替わると、本アプリは Kaspersky Security Center との自動同期を停止します。そのため、何らかの理由で本アプリのアクティベーションがインストール後 30 日以内に完了しなかった場合、ユーザーは手動でデバイスを Kaspersky Security Center と同期させる必要があります。

Kaspersky Security Center が組織に導入されていない場合、またはモバイルデバイスからアクセスできない場合、ユーザーは Kaspersky Endpoint Security for Android をデバイス上で手動でアクティベートできます。

Kaspersky Endpoint Security for Android アプリをアクティベートするには：

1. コンソールツリーの［**管理対象デバイス**］フォルダーで、デバイスが属する管理グループを選択します。

2. 選択したグループの作業領域で、［**ポリシー**］タブを選択します。

3. 任意の列をダブルクリックして、ポリシーのプロパティウィンドウを開きます。

4. ポリシーの**プロパティ**ウィンドウで、［**ライセンス**］セクションを選択します。

5. ［**ライセンス**］セクションで、［**キー**］ドロップダウンリストを表示し、Kaspersky Security Center 管理サーバーのライセンス保管領域からアプリのアクティベーションに必要なライセンスを選択します。

   ライセンスを購入済みのアプリの詳細が、下のフィールドに表示されます。

6. ［**Kaspersky Security Center の保管領域からのライセンス情報でアクティベート**］をオンにします。

   Kaspersky Security Center の保管領域に保存されているライセンス情報を使用せずにアプリがアクティベートされていた場合、Kaspersky Security for Mobile はこのライセンス情報を［**キー**］ドロップダウンリストで選択されたライセンス情報に置き換えます。

7. モバイルデバイスでアクティベーションを実行するため、設定の変更をブロックします。

8. ［**適用**］をクリックして、変更を保存します。

   モバイルデバイスと Kaspersky Security Center との次回の同期時に、デバイスに設定が適用されます。

iOS MDM プロファイルのインストール

このセクションでは、会社のネットワークに iOS MDM プロファイルを導入する方法について説明します。

iOS MDM プロファイルを導入する前に、管理者は次の作業をしておく必要があります：

1. iOS MDM サーバーをインストールする。

2. Apple Push Notification サービス証明書（APNs 証明書）を取得する。

3. iOS MDM サーバーに APNs 証明書をインストールする。

iOS MDM サーバーのインストール方法と APNs 証明書の使用方法の詳細は、*Kaspersky Security Center のヘルプ*を参照してください。

Kaspersky Endpoint Security Cloud で iOS MDM プロファイルを導入する方法の詳細は、*Kaspersky Endpoint Security Cloud のヘルプ*を参照してください。

iOS デバイス管理モードについて

iOS デバイス管理システムを導入するには、方法がいくつかあります。管理モードは、モバイルデバイスの所有者（個人または会社）と企業のセキュリティ要件によって決まります。会社に最も適した管理モードを選択することができ、同時に複数のモードを使用できます。

監視対象外のデバイス

*監視対象外の iOS デバイス*とは、Kaspersky Security Center に接続されている社員個人のデバイスです。このモードでは、ユーザーは個人の Apple ID を使用すること、好きなアプリを使用すること、個人情報をデバイスに保存することが許可されています。Kaspersky Device Management for iOS グループポリシーを使用して、企業リソースへのアクセス設定、セキュリティ設定、およびその他の設定を行えます。既定では、すべての iOS デバイスは監視対象外です。

監視対象のデバイス

*監視対象の iOS デバイス*とは、Kaspersky Security Center に接続されている会社のデバイスです。モバイルデバイスの初期設定は、Apple Configurator で行われます。*Apple Configurator* は、iOS デバイスの準備と設定を行うことを目的としたアプリケーションです。Apple Configurator は、OS X が稼働するコンピューターにインストールされます。Apple Configurator の使用方法の詳細については、Apple のテクニカルサポートサイトを参照してください。Kaspersky Device Management for iOS グループポリシーを使用して、さらに設定を行えます。監視対象のデバイスでは、拡張設定にアクセスできます。たとえば、Global HTTP Proxy や追加制限（iMessage や Game Center の使用をブロックするなど）を設定したり、ユーザーアカウントの変更をブロックしたりできます。

監視対象および監視対象外の iOS デバイスを使用するには、iOS MDM モバイルデバイスサーバーに APNs 証明書がインストールされており、iOS MDM プロファイルがユーザーのモバイルデバイスにインストールされている必要があります。

Kaspersky Security Center からのインストール

IOS MDM プロファイルは、ユーザーアカウントが Kaspersky Security Center に追加されているユーザーのモバイルデバイスにインストールされます。Kaspersky Security Center のユーザーアカウントの詳細は、*Kaspersky Security Center のヘルプを参照してください*。

IOS MDM プロファイルをインストールするには：

1. コンソールツリーで、［**モバイルデバイス管理**］→［**モバイルデバイス**］の順に選択します。
2. ［**モバイルデバイス**］フォルダーの作業領域で［**モバイルデバイスの追加**］をクリックします。

   新規モバイルデバイス接続ウィザードが開始されます。ウィザードの指示に従います。
3. ウィザードの［**オペレーティングシステム**］ウィンドウで［**iOS**］を選択します。
4. ウィザードの［**iOS MDM デバイスの保護方法**］ウィンドウで、［**iOS MDM サーバーの iOS MDM プロファイルを使用**］を選択し、リストから iOS MDM プロファイルを指定します。
5. ウィザードの［**ユーザーの選択**］ウィンドウで、モバイルデバイスに iOS MDM プロファイルをインストールするユーザーを 1 人または複数選択します。

   ユーザーがリストにない場合、新規モバイルデバイス接続ウィザードを終了せずに、新しいユーザーアカウントを追加できます。
6. ウィザードの［**証明書ソース**］ウィンドウで、モバイルデバイスと Kaspersky Security Center 間のデータ転送を保護するための証明書のソースを選択します：

   - **管理サーバーツールから証明書を発行する**：この場合、証明書は自動的に作成されます。
   - **証明書ファイルを指定する**：この場合、独自の証明書を事前に準備しておき、それをウィザードのウィンドウで選択する必要があります。このオプションは、複数のモバイルデバイスに iOS MDM プロファイルをインストールする場合には使用できません。ユーザーごとに個別の証明書を作成する必要があります。
7. ウィザードの［**ユーザー通知方法**］ウィンドウで、アプリのインストールリンクを転送するために使用するチャネルを選択します：

   - メールでリンクを送信するには、［**iOS MDM プロファイルにリンクを送信**］を選択し、［**メール**］セクションで設定を行います。ユーザーアカウントの設定でメールアドレスが指定されていることを確認してください。

- SMS メッセージでリンクを送信するには、［**iOS MDM プロファイルにリンクを送信**］を選択し、［**SMS 経由**］セクションで設定を行います。ユーザーアカウントの設定で電話番号が指定されていることを確認してください。

- QR コードを使用して iOS MDM プロファイルをインストールするには、［**インストールパッケージへのリンクを表示**］を選択し、モバイルデバイスのカメラを使用して QR コードをスキャンします。

- リストされたどの方法も適切ではない場合、［**インストールパッケージへのリンクを表示**］→［**コピー**］の順に選択して、iOS MDM プロファイルをインストールするためのリンクをクリップボードにコピーします。使用可能ないずれかの方法で、アプリのインストールリンクを配信します。

8. 新規モバイルデバイス接続ウィザードを終了します。

IOS MDM プロファイルをユーザーのモバイルデバイスにインストールした後、グループポリシーを使用してアプリを設定できます。また、デバイスの紛失時や盗難時には、データ保護のためにモバイルデバイスにコマンドを送信することもできます。

IOS 12.1 以降のモバイルデバイスでは、デバイスへの iOS MDM プロファイルのインストールを手動で確認する必要があります。また、デバイスのリモート管理の権限も許可する必要があります。

管理プラグインのインストール

モバイルデバイスを管理するには、次の管理プラグインを管理者のワークステーションにインストールする必要があります：

- Kaspersky Endpoint Security for Android の管理プラグインは、Kaspersky Security Center の管理コンソールからモバイルデバイスおよびデバイスにインストールされているモバイルアプリを管理するためのインターフェイスを提供します。

- Kaspersky Device Management for iOS の管理プラグインは、Kaspersky Security Center の管理コンソールから、iOS MDM および Exchange ActiveSync プロトコルを使用して接続されたモバイルデバイスを管理するためのインターフェイスを提供します。

管理プラグインは次の方法を使用してインストールできます：

- Kaspersky Security Center のクイックスタートウィザードを使用して管理プラグインをインストールします。

  管理サーバーのインストール後、管理サーバーへの初回接続時に、クイックスタートウィザードの実行が自動的に促されます。クイックスタートウィザードは、いつでも手動で開始できます。

  クイックスタートウィザードを使用すると、Kaspersky Endpoint Security for the Android アプリの使用許諾契約書（EULA）の条項に管理コンソール上で同意できます。使用許諾契約書の条項に管理コンソール上で管理者が同意すると、Kaspersky Endpoint Security for Android のインストール中に同意のステップがスキップされます。Kaspersky Security Center のクイックスタートウィザードの詳細は、*Kaspersky Security Center のヘルプ*を参照してください。

- Kaspersky Security Center 管理コンソールの使用可能な配布パッケージを使用して管理プラグインをインストールします。

  使用可能な配布パッケージのリストは、新しいバージョンのカスペルスキー製品の公開後に自動的にアップデートされます。

- 外部ソースから配布パッケージをダウンロードし、EXE ファイルを使用して管理プラグインをインストールします。

  たとえば、カスペルスキーの Web サイトから管理プラグインの配布パッケージをダウンロードできます。

管理コンソールのリストから管理コンソールをインストール

管理プラグインをインストールするには：

1. コンソールツリーで、［**詳細**］→［**リモートインストール**］→［**インストールパッケージ**］の順に選択します。
2. 作業領域で、［**その他の操作**］→［**カスペルスキー製品の現在のバージョンの表示**］の順に選択します。

   最新バージョンのカスペルスキー製品を含むリストが表示されます。
3. ［**モバイルデバイス**］セクションで、**Kaspersky Endpoint Security for Android** または **Kaspersky Device Management for iOS** のプラグインを選択します。
4. ［**配布パッケージをダウンロード**］をクリックします。

   プラグインがコンピューターにダウンロードされます（EXE ファイル）。
5. インストールウィザードの指示に従って EXE ファイルを実行します。

配布パッケージからの管理プラグインのインストール

Kaspersky Endpoint Security for Android 管理プラグインをインストールするには：

プラグインのインストールファイル `klcfinst.exe` を製品の配布パッケージからコピーし、管理者のワークステーションで実行します。

インストールはウィザードによって行われるため、設定を行う必要はありません。

Kaspersky Device Management for iOS 管理プラグインをインストールするには：

プラグインのインストールファイル `klmdminst.exe` を製品の配布パッケージからコピーし、管理者のワークステーションで実行します。

インストールはウィザードによって行われるため、設定を行う必要はありません。

管理プラグインがインストールされているかどうかを確認するには、管理サーバーのプロパティウィンドウの［**詳細**］→［**インストール済みアプリケーション管理プラグインの情報**］セクションで、インストール済みのアプリケーション管理プラグインのリストを表示します。

旧バージョンのアプリのアップデート

アップグレードは、次の要件を満たしている必要があります：

- Kaspersky Endpoint Security 管理プラグインのバージョンと Kaspersky Endpoint Security for Android モバイルアプリのバージョンが一致している必要があります。

管理プラグインとモバイルアプリのバージョンのビルド番号は、Kaspersky Security for Mobile のリリースノートで確認できます。

- Kaspersky Security Center が Kaspersky Security for Mobile のソフトウェア要件を満たしていることを確認します。
- Kaspersky Endpoint Security 10.0 Service Pack 2（ビルド 10.6.0.1801）と Kaspersky Device Management for iOS10.0 Service Pack 2（ビルド 10.6.0.1767）、および以降のバージョンは、自動的に最新のバージョンにアップグレードできます。旧バージョンの管理プラグインのアップグレードはサポートしていません。

  旧バージョンの管理プラグインをアップグレードするには、インストール済みの管理プラグインとそれらを使用して作成されたグループポリシーを削除する必要があります。その後、新しいバージョンの管理プラグインをインストールします。管理プラグインの削除の詳細については、*カスペルスキーのテクニカルサポートサイト*をご参照ください。
- 組織のすべてのモバイルデバイスで同じバージョンの Kaspersky Endpoint Security for Android を使用してください。

Kaspersky Security for Mobile の各バージョンのテクニカルサポート条件については、*カスペルスキーのテクニカルサポートサイト*を参照してください。

管理プラグインのバージョンとビルド番号を確認するには：

1. コンソールツリーで、管理サーバーのコンテキストメニューから［**プロパティ**］を選択します。
2. 管理サーバーのプロパティウィンドウで、［**詳細**］→［**インストール済みのアプリケーション管理プラグインの詳細**］を選択します。

   作業領域に、インストール済み管理プラグインについての情報が <プラグイン名> <バージョン> <ビルド> の形式で表示されます。

Kaspersky Endpoint Security for Android アプリのバージョンとビルド番号は、次の方法を使用して確認できます：

- Kaspersky Endpoint Security for Android をスタンドアロンインストールパッケージを使用してインストールした場合、パッケージのプロパティでアプリのバージョンとビルド番号を確認できます。
- Kaspersky Endpoint Security for Android を Google Play からインストールした場合、アプリ設定でビルド番号を確認できます（→［**製品情報**］）。

旧バージョンの Kaspersky Endpoint Security for Android のアップグレード

Kaspersky Endpoint Security for Android は次の方法でアップデートできます：

- Google Play を使用する。Google Play から製品の新しいバージョンをダウンロードし、デバイスにインストールします。
- Kaspersky Security Center を使用する。Kaspersky Security Center のリモート管理システムで、デバイスに入っている製品のバージョンを遠隔操作でアップデートできます。

組織に最も適したアプリのアップデート方法を選択できます。1つのアップデート方法のみを使用できます。

Google Play からの本アプリのアップデート

Android プラットフォームの標準的なアップデート方法で、Google Play から本アプリをアップデートします。製品をアップデートするには、次の条件を満たす必要があります：

- デバイスのユーザーが Google アカウントを所持している。
- デバイスが Google アカウントに紐づけられている。
- デバイスがインターネットに接続している必要があります。

Google Play からの本アプリのダウンロード後、Kaspersky Endpoint Security for Android が使用許諾契約書（EULA）の条項をチェックします。使用許諾契約書の条項が更新されている場合、本アプリが Kaspersky Security Center へリクエストを送信します。使用許諾契約書の条項に管理コンソール上で管理者が同意すると、Kaspersky Endpoint Security for Android のインストール中に同意のステップがスキップされます。最新ではないバージョンの管理プラグインを管理者が使用している場合、Kaspersky Security Center は管理プラグインのアップデートを促す通知を表示します。管理プラグインのアップデート時に、管理者はKaspersky Endpoint Security for Android の EULA の条項に管理コンソールで同意できます。

Kaspersky Endpoint Security for Android が Google Play からインストールされた場合、Google Play から本アプリをアップデートできます。他の方法を使用してインストールされた場合、Google Play から本アプリをアップデートすることはできません。

Kaspersky Security Center を使用した本アプリのアップデート

グループポリシーの適用後、Kaspersky Security Center を使用して Kaspersky Endpoint Security for Android をアップグレードできます。グループポリシー設定で、企業のセキュリティ要件を満たすバージョンの Kaspersky Endpoint Security for Android スタンドアロンインストールパッケージを選択できます。

Kaspersky Endpoint Security for Android が Kaspersky Security Center からインストールされた場合、Kaspersky Security Center からアップデートできます。Google Play からインストールされた場合、Kaspersky Security Center からアップデートすることはできません。

スタンドアロンインストールパッケージを使用して Kaspersky Endpoint Security for Android をアップグレードするには、ユーザーのモバイルデバイスで提供元不明のアプリのインストールを許可しておく必要があります。Google Play ストアを経由せずにアプリをインストールする方法の詳細は、*Android ヘルプ* を参照してください。

製品のバージョンをアップデートするには：

1. コンソールツリーの［**管理対象デバイス**］フォルダーで、デバイスが属する管理グループを選択します。
2. 選択したグループの作業領域で、［**ポリシー**］タブを選択します。
3. 任意の列をダブルクリックして、ポリシーのプロパティウィンドウを開きます。
4. ポリシーの**プロパティ**ウィンドウで、［**詳細**］セクションを選択します。
5. ［**Kaspersky Endpoint Security for Android のアップグレード**］セクションで、［**選択**］をクリックします。

［**Kaspersky Endpoint Security for Android のアップグレード**］ウィンドウが開きます。

6. Kaspersky Endpoint Security のスタンドアロンインストールパッケージのリストで、企業のセキュリティ要件を満たすバージョンのパッケージを選択します。

   Kaspersky Endpoint Security は、現在のバージョンよりも新しいバージョンにしかアップグレードできません。現在のバージョンよりも古いバージョンへの更新はできません。

7. ［**選択**］をクリックします。

   選択したスタンドアロンインストールパッケージの説明が［**Kaspersky Endpoint Security for Android のアップグレード**］セクションに表示されます。

8. ［**適用**］をクリックして、変更を保存します。

モバイルデバイスと Kaspersky Security Center との次回の同期時に、デバイスに設定が適用されます。新しいバージョンのインストールを要求されます。ユーザーが同意すると、新しいバージョンがモバイルデバイスにインストールされます。

旧バージョンの Kaspersky Endpoint Security for Android のインストール

本アプリが自動的にアップデートされないようにして、特定のバージョンを使用するには、本アプリの自動アップデートを Google Play の設定で無効にしてください。詳細は、Google のテクニカルサポートサイトをご参照ください。

Kaspersky Endpoint Security for Android の自動アップデートは、本アプリが Google Play ストア経由または Google Play ストアへのリンクを使用して Kaspersky Security Center 経由でインストールされている場合のみ可能です。本アプリがお客様の環境にある Web サーバーへのリンク（スタンドアロンインストールパッケージを使用）を使用して Kaspersky Security Center 経由でインストールされている場合は、自動アップデートは使用できません。この場合、グループポリシーを使用して、Kaspersky Endpoint Security for Android を手動でアップデートできます。

旧バージョンの Kaspersky Endpoint Security for Android をインストールするには：

1. ユーザーのモバイルデバイスから Kaspersky Endpoint Security for Android を削除します。
2. お客様の環境にある Web サーバーへのリンクを使用して、Kaspersky Security Center 経由で Kaspersky Endpoint Security for Android をインストールします。インストールするには、特定のバージョンのインストールパッケージが必要です。Kaspersky Endpoint Security for Android の旧バージョンの配布パッケージは、カスペルスキーのテクニカルサポートサイトからダウンロードできます。

旧バージョンの Kaspersky Endpoint Security for Android の詳細は、*対応するバージョンのヘルプ*をご参照ください。

旧バージョンの管理プラグインのアップグレード

管理プラグインは次の方法を使用してアップグレードできます：

- Kaspersky Security Center 管理コンソールの使用可能な配布パッケージのリストから新しいバージョンの管理プラグインをインストールする。

  使用可能な配布パッケージのリストは、新しいバージョンのカスペルスキー製品の公開後に自動的にアップデートされます。

- 外部ソースから配布パッケージをダウンロードし、新しいバージョンの管理プラグインを EXE ファイルを使用してインストールする。

  Kaspersky Endpoint Security 管理プラグインと Kaspersky Device Management for iOS 管理プラグインをアップグレードするには、最新バージョンのアプリケーションを Kaspersky Security for Mobile の Web サイト からダウンロードして、2 つのプラグインのそれぞれでセットアップウィザードを実行する必要があります。旧バージョンのプラグインは、インストールウィザードの動作中に自動で削除されます。

カスペルスキーでは、アプリと管理プラグインで同一のバージョンを使用することを推奨しています。本アプリを Google Play からアップグレードする場合、Kaspersky Security Center は管理プラグインのアップグレードを要求する通知を表示します。

管理プラグインがアップデートされると、［**管理対象デバイス**］フォルダー内の既存の管理グループと、［**未割り当てデバイス**］フォルダーからこれらのグループにデバイスを自動的に割り当てるルールが保存されます。モバイルデバイスの既存のグループポリシーも保存されます。Kaspersky Security for Mobile 統合ソリューションの新しい機能を実装する新しいポリシー設定は、既存のポリシーに追加され、既定値が使用されます。

設定が追加されたり、既定値が新しいバージョンの管理プラグインで変更されたりした場合は、それらの変更はグループポリシーが開かれた後にのみ適用されます。プラグインのバージョンがアップデートされても、管理者がグループポリシーを開くまでは、旧バージョンのプラグインの設定がモバイルデバイスに適用されます。

管理コンソールのリストからのアップグレード

管理プラグインをアップグレードするには：

1. コンソールツリーで、［**詳細**］→［**リモートインストール**］→［**インストールパッケージ**］の順に選択します。
2. 作業領域で、［**その他の操作**］→［**カスペルスキー製品の現在のバージョンの表示**］の順に選択します。

   最新バージョンのカスペルスキー製品を含むリストが表示されます。
3. ［**モバイルデバイス**］セクションで、**Kaspersky Endpoint Security for Android** または **Kaspersky Device Management for iOS** のプラグインを選択します。
4. ［**配布パッケージをダウンロード**］をクリックします。

   プラグインがコンピューターにダウンロードされます（EXE ファイル）。EXE ファイルを実行します。ウィザードの指示に従います。

配布パッケージからのアップグレード

Kaspersky Endpoint Security for Android 管理プラグインをアップグレードするには：

プラグインのインストールファイル `klcfinst.exe` を製品の配布パッケージからコピーし、管理者のワークステーションで実行します。

インストールはウィザードによって行われるため、設定を行う必要はありません。

Kaspersky Device Management for iOS 管理プラグインをアップグレードするには：

プラグインのインストールファイル `klmdminst.exe` を製品の配布パッケージからコピーし、管理者のワークステーションで実行します。

プラグインのインストールはウィザードによって行われるため、設定を行う必要はありません。

管理プラグインがアップグレードされているかどうかを確認するには、管理サーバーのプロパティウィンドウの［**詳細**］→［**インストール済みアプリケーション管理プラグインの情報**］セクションで、インストール済みのアプリケーション管理プラグインのリストを表示します。

Kaspersky Endpoint Security for Android の削除

Kaspersky Endpoint Security for Android は次の方法で削除できます：

1. ユーザーによるアプリの削除

   アプリのインターフェイスを使用して、ユーザーが手動で Kaspersky Endpoint Security for Android を削除します。ユーザーによるアプリの削除を有効にするには、デバイスに適用されているポリシーでアプリの削除が許可されている必要があります。

2. 管理者によるアプリの削除

   Kaspersky Security Center の管理コンソールを使用して、管理者が遠隔操作でアプリを削除します。アプリは、デバイスごとに削除することも、一度に複数のデバイスから削除することもできます。

遠隔操作によるアプリの削除

ユーザーのモバイルデバイスから Kaspersky Endpoint Security for Android を遠隔操作で削除するには、次の方法を実行します：

- グループポリシーを作成する。一度に複数のデバイスからアプリを削除する場合に有効です。
- ローカルのアプリ設定を変更する。デバイスごとにアプリを削除する場合に有効です。

グループポリシーを適用してアプリを削除するには：

1. コンソールツリーの［**管理対象デバイス**］フォルダーで、デバイスが属する管理グループを選択します。
2. 選択したグループの作業領域で、［**ポリシー**］タブを選択します。
3. 任意の列をダブルクリックして、ポリシーのプロパティウィンドウを開きます。
4. ポリシーの**プロパティ**ウィンドウで、［**詳細**］セクションを選択します。
5. ［**Kaspersky Endpoint Security for Android のアンインストール**］セクションで、［**デバイスから Kaspersky Endpoint Security for Android を削除**］をオンにします。
6. ［**適用**］をクリックして、変更を保存します。

   これにより、管理サーバーとの同期後に Kaspersky Endpoint Security for Android がモバイルデバイスから削除されます。モバイルデバイスのユーザーは、アプリが削除されたことを知らせる通知を受信します。

ローカルの設定を変更してアプリを削除するには：

1. コンソールツリーで、［**モバイルデバイス管理**］→［**モバイルデバイス**］の順に選択します。
2. デバイスのリストから、アプリを削除するデバイスを選択します。
3. ダブルクリックでデバイスのプロパティウィンドウを開きます。
4. ［**アプリケーション**］→［**Kaspersky Endpoint Security for Android**］の順に選択します。
5. ダブルクリックで Kaspersky Endpoint Security のプロパティウィンドウを開きます。
6. ［**詳細**］セクションを選択します。
7. ［**Kaspersky Endpoint Security for Android の削除**］セクションで、［**デバイスから Kaspersky Endpoint Security for Android を削除**］をオンにします。
8. ［**適用**］をクリックして、変更を保存します。

これにより、管理サーバーとの同期後に Kaspersky Endpoint Security for Android がモバイルデバイスから削除されます。モバイルデバイスのユーザーは、アプリが削除されたことを知らせる通知を受信します。

ユーザーによるアプリの削除の許可

Android 7.0 以降のデバイスでアプリが削除されないように保護するには、Kaspersky Endpoint Security for Android をユーザー補助機能として設定しておく必要があります。初期設定ウィザードの実行時に、必要な権限を Kaspersky Endpoint Security for Android に付与するよう要求されます。このステップはスキップできます。また、後からデバイスの設定で権限を無効にすることもできます。その場合、手動による削除はブロックできません。

ユーザーによるモバイルデバイスからの Kaspersky Endpoint Security for Android の削除を許可するには、次の方法があります：

- グループポリシーを作成する。一度に複数のデバイスからのアプリの削除を許可する場合に有効です。
- ローカルのアプリ設定を使用する。各デバイスのユーザーごとに対してアプリの削除を許可する場合に有効です。

グループポリシーでアプリの削除を許可するには：

1. コンソールツリーの［**管理対象デバイス**］フォルダーで、デバイスが属する管理グループを選択します。
2. 選択したグループの作業領域で、［**ポリシー**］タブを選択します。
3. 任意の列をダブルクリックして、ポリシーのプロパティウィンドウを開きます。
4. ポリシーの**プロパティ**ウィンドウで、［**詳細**］セクションを選択します。
5. ［**Kaspersky Endpoint Security for Android の削除**］セクションで、［**Kaspersky Endpoint Security for Android の削除を許可**］をオンにします。
6. ［**適用**］をクリックして、変更を保存します。

これにより、管理サーバーとの同期後に、ユーザーによるモバイルデバイスでのアプリの削除が許可されます。Kaspersky Endpoint Security の Android 設定で、アプリの削除ボタンが使用可能になります。

ローカルのアプリ設定でアプリの削除を許可するには：

1. コンソールツリーで、［**詳細**］→［**モバイルデバイス管理**］→［**モバイルデバイス**］の順に選択します。
2. デバイスのリストから、アプリの削除を許可するデバイスを選択します。
3. ダブルクリックでデバイスのプロパティウィンドウを開きます。
4. ［**アプリケーション**］→［**Kaspersky Endpoint Security for Mobile**］の順に選択します。
5. ダブルクリックで Kaspersky Endpoint Security のプロパティウィンドウを開きます。
6. ［**詳細**］セクションを選択します。
7. ［**Kaspersky Endpoint Security for Android の削除**］セクションで、［**Kaspersky Endpoint Security for Android の削除を許可**］をオンにします。
8. ［**適用**］をクリックして、変更を保存します。

これにより、管理サーバーとの同期後に、ユーザーによるモバイルデバイスでのアプリの削除が許可されます。Kaspersky Endpoint Security の Android 設定で、アプリの削除ボタンが使用可能になります。

ユーザーによるアプリの削除

Kaspersky Endpoint Security for Android をモバイルデバイスから個別に削除するには、ユーザーは次の操作を行う必要があります：

1. Kaspersky Endpoint Security for Android のメインウィンドウで、☰ →［**アプリをアンインストール**］の順にタップします。

   削除を確認するメッセージが画面に表示されます。

   ［**アプリをアンインストール**］ボタンがない場合は、Kaspersky Endpoint Security for Android が削除されないようにする保護を管理者が有効にしていることを意味します。
2. Kaspersky Endpoint Security for Android の削除を確認します。

Kaspersky Endpoint Security for Android アプリはユーザーのモバイルデバイスから削除されます。

設定と管理

このヘルプセクションは、Kaspersky Security for Mobile の管理担当者、ならびに Kaspersky Security for Mobile を使用する組織にテクニカルサポートを提供する担当者を対象としています。

開始時の操作

このセクションでは、Kaspersky Security for Mobile の開始時に実行を推奨する操作について説明します。

製品の起動と終了

Kaspersky Endpoint Security と Kaspersky Device Management for iOS の各管理プラグインを、Kaspersky Security Center が自動的に開始または停止します。

Kaspersky Endpoint Security for Android は、オペレーティングシステムが起動すると立ち上がり、セッション全体を通してモバイルデバイスを保護します。ユーザーは、すべての Kaspersky Endpoint Security for Android コンポーネントを無効にすることで、アプリを停止できます。グループポリシーを使用して、アプリのコンポーネントを管理するためのユーザー権限を設定できます。

一部のデバイス（Huawei、Meizu、Xiaomi など）では、オペレーティングシステム起動時に開始するアプリのリストに Kaspersky Endpoint Security for Android を手動で追加する必要があります（［**セキュリティ**］→［**権限**］→［**自動実行**］）。本アプリがリストに追加されていない場合、Kaspersky Endpoint Security for Android はモバイルデバイスの再起動後に全機能の実行を停止します。

また、Kaspersky Endpoint Security for Android の省電力モードも無効にする必要があります。これは、定期スキャンの実行やデバイスと Kaspersky Security Center との同期など、バックグラウンドで実行するアプリのために必要です。この問題は、これらのデバイスに組み込まれたソフトウェアの特定機能に起因しています。

管理グループの作成

ユーザーのモバイルデバイスにインストールされた Kaspersky Endpoint Security for Android の設定を一元的に行うには、グループポリシーをデバイスに適用する必要があります。

デバイスのグループにポリシーを適用するには、ユーザーのデバイスにモバイルアプリをインストールする前に、［**管理対象デバイス**］にこれらのデバイス用の独立したグループを作成しておきます。

管理グループの作成後、アプリをインストールするデバイスをこのグループに自動的に割り当てるオプションを設定することを推奨しますグループポリシーを使用して、すべてのデバイスに共通の設定を行います。

管理グループを作成するには、次の操作を行います：

1. コンソールツリーで、［**管理対象デバイス**］フォルダーを開きます。
2. ［**管理対象デバイス**］フォルダーの作業領域またはサブフォルダーの作業領域で、［**デバイス**］タブを選択します。
3. ［**新規グループ**］をクリックします。
   ウィンドウが開き、新しいグループを作成できます。
4. ［**グループ名**］ウィンドウでグループ名を入力し、［**OK**］をクリックします。

指定した名前の新しい管理グループフォルダーがコンソールツリーに表示されます。管理グループの使用方法の詳細については、*Kaspersky Security Center のヘルプ*を参照してください。

モバイルデバイスを管理するためのグループポリシー

*グループポリシー*とは、管理グループに属するモバイルデバイスと、これらのデバイスにインストールされているモバイルアプリを管理するための設定のパッケージです。グループポリシーは、ポリシーウィザードを使用して作成できます。

ポリシーを使用して、個々のデバイスとデバイスのグループの両方の設定が行えます。デバイスのグループの場合、管理設定はグループポリシープロパティのウィンドウで設定できます。個々のデバイスの場合、ローカルアプリ設定のウィンドウで設定できます。あるデバイスに対して指定する個別の管理設定は、このデバイスが属するグループ用のポリシーで指定された設定値と異なっている場合があります。

ポリシーで表される各パラメータは「ロック」属性を持っています。これは、ネストされた階層レベル（ネストされたグループとセカンダリー管理サーバー）のポリシーの設定をローカルアプリ設定で変更できるかどうかを示します。

ポリシーで設定された値およびローカルアプリ設定の値は管理サーバーに保存された後、同期中にモバイルデバイスに送信され、現在の設定としてデバイスに保存されます。ロックされていない設定にユーザーが別の値を指定した場合、デバイスと管理サーバーの次回の同期中に、設定の新しい値が管理サーバーに送信され、管理者により以前に指定された値の代わりにアプリのローカル設定に保存されます。

モバイルデバイスに対する企業のセキュリティを最新に保つために、ユーザーのデバイスがグループ管理ポリシーに準拠しているかを監視できます。

セキュリティレベルのインジケーターはグループポリシーのウィンドウの上部に表示されます。このインジケーターは、デバイスの保護レベルをポリシーで高く設定するのに役立ちます。保護レベルのインジケーターの状態は、ポリシーの設定に応じて変更されます：

- **高レベルの保護** – デバイスの保護レベルが適切な状態です。すべての保護機能が、カスペルスキーが推奨する設定に従って動作しています。
- **中レベルの保護** – 推奨よりも低い保護レベルです。一部の重要な保護機能が無効です（例：危険サイトブロック）。重大な問題は、● アイコンでマークされます。
- **低レベルの保護** – デバイスの感染や、データの消失の原因となる可能性がある問題があります。一部の重要な保護機能が無効です（例：デバイスのリアルタイム保護が無効）。緊急の問題は、● アイコンでマークされます。

Kaspersky Security Center の管理コンソールでのポリシーと管理グループの管理の詳細については、*Kaspersky Security Center のヘルプ*を参照してください。

グループポリシーの作成

このセクションでは、Kaspersky Endpoint Security for Android がインストールされているデバイスのグループポリシーの作成方法と、EAS デバイスおよび iOS MDM デバイスのポリシーの作成方法について説明します。

管理グループ用に作成したポリシーは、Kaspersky Security Center 管理コンソールのグループの作業領域の［**ポリシー**］タブに表示されます。ポリシーのステータス（アクティブまたは非アクティブ）を示すアイコンがポリシー名の前に表示されます。1つのグループで、異なるアプリケーションに対して複数のポリシーを作成することができます。各アプリケーションに対してアクティブにできるポリシーは、1つのみです。アクティブポリシーを新しく作成すると、それまでのアクティブポリシーは非アクティブになります。

ポリシーは、作成した後でも変更できます。

モバイルデバイスを管理するためのポリシーを作成するには：

1. コンソールツリーから、ポリシーを作成する管理グループを選択します。
2. 選択したグループの作業領域で、［**ポリシー**］タブを選択します。
3. ［**ポリシーの作成**］をクリックして、ポリシーウィザードを開始します。

これにより、新規ポリシーウィザードが起動します。

ステップ1：グループポリシー作成対象のアプリの選択

このステップでは、グループポリシーを作成するアプリケーションをアプリケーションのリストから選択します：

- **Kaspersky Endpoint Security for Android** - Kaspersky Endpoint Security for Android モバイルアプリを使用するデバイスの場合。

Google play を持たない Huawei と Honor のデバイスには個別のポリシーを作成してください。そうすることで、これらのデバイスのユーザーには Huawei AppGallery へのリンクを送信することができます。

- **Kaspersky Device Management for iOS** - EAS デバイスおよび iOS MDM デバイスの場合。

モバイルデバイスのポリシーは、Kaspersky Endpoint Security Android 管理プラグインおよび Kaspersky Device Management for iOS 管理プラグインが管理者のデスクトップにインストールされている場合に作成できます。プラグインがインストールされていない場合、該当するアプリケーションの名前がリストに表示されません。

ポリシーウィザードの次のステップに進みます。

ステップ2：グループポリシー名の入力

このステップでは、［**名前**］に新しいポリシーの名前を入力します。既存のポリシーの名前を指定すると、その名前の末尾に「(1)」が自動的に付加されます。

ポリシーウィザードの次のステップに進みます。

ステップ3：アプリケーションのグループポリシーの定義

このステップでは、ポリシーのステータスを選択します：

- **アクティブポリシー**：作成したポリシーを管理サーバーに保存します。モバイルデバイスと管理サーバーが次に同期した時に、このポリシーがアクティブポリシーとしてデバイスで使用されます。
- **非アクティブポリシー：**作成したポリシーをバックアップポリシーとして管理サーバーに保存します。このポリシーは、将来、特定のイベントが発生した後に有効になります。必要に応じて、非アクティブポリシーをアクティブステータスに切り替えることができます。

  グループで1つのアプリについて複数のポリシーを作成できますが、一度に有効にできるポリシーは1つのみです。アクティブポリシーを新しく作成すると、それまでのアクティブポリシーは自動的にアクティブでなくなります。

ウィザードを終了します。

同期の設定

モバイルデバイスを管理し、ユーザーのモバイルデバイスからレポートや統計情報を受信するには、同期を設定する必要があります。Kaspersky Security Center とモバイルデバイスの同期は、次のように実行されます：

- **スケジュール**：スケジュールに基づく同期は、HTTP プロトコルを使用して実行されます。同期スケジュールは、グループポリシーの設定で指定できます。グループポリシーの設定変更、コマンド、タスクは、スケジュールに基づいてデバイスが Kaspersky Security Center と同期すると実行されます（同期するまで、実行が遅延します）。既定では、モバイルデバイスと Kaspersky Security Center との同期は 6 時間ごとに自動的に実行されます。

  Android 12 以降のデバイスでは、バッテリー節約モードの場合、タスクの実行が指定よりも遅れる場合があります。

- **強制**：強制的な同期は、FCM サービス（Firebase Cloud Messaging）のプッシュ通知を使用して実行されます。強制的な同期は、モバイルデバイスへのコマンドのタイムリーな配信を主な目的としています。強制的な同期を使用する場合は、GSM が Kaspersky Security Center で設定されていることを確認してください。詳細については、Kaspersky Security Center のヘルプを参照してください。

モバイルデバイスと Kaspersky Security Center との同期を設定するには：

1. コンソールツリーの［**管理対象デバイス**］フォルダーで、デバイスが属する管理グループを選択します。
2. 選択したグループの作業領域で、［**ポリシー**］タブを選択します。
3. 任意の列をダブルクリックして、ポリシーのプロパティウィンドウを開きます。
4. ポリシーの**プロパティ**ウィンドウで、［**同期**］セクションを選択します。
5. ［**同期**］ドロップダウンリストから同期の頻度を選択します。
6. デバイスがローミング中の場合に Kaspersky Security Center との同期を無効にするには、［**ローミング中は同期しない**］をオンにします。

   デバイスユーザーは同期を手動で実行するようにアプリを設定できます（→［**設定**］→［**同期**］→［**同期**］）。
7. アプリの設定で同期設定（サーバーアドレス、ポート、管理グループ）をユーザーに対して非表示にするには、［**デバイスの同期の設定を表示する**］をオフにします。非表示の設定を変更することはできません。
8. ［**適用**］をクリックして、変更を保存します。

モバイルデバイスと Kaspersky Security Center との次回の同期時に、デバイスに設定が適用されます。モバイルデバイスの同期は、専用のコマンドを使用して手動で実行することでもできます。モバイルデバイスのコマンドの使用については、*Kaspersky Security Center のヘルプ*を参照してください。

グループポリシーリビジョンの管理

Kaspersky Security Center によってグループポリシーの変更を追跡できます。グループポリシーに対する変更を保存するたびに、*リビジョン*が作成されます。各リビジョンには番号が振られています。

Kaspersky Endpoint Security for Android ポリシーについてのみリビジョンを管理できます。Kaspersky Device Management for iOS ポリシーのリビジョンは管理できません。

グループポリシーリビジョンで次の処理を実行できます：

- 選択したリビジョンを現在のリビジョンと比較する。

- 選択したリビジョン同士を比較する。
- ポリシーを別のポリシーの選択したリビジョンと比較する。
- 選択したリビジョンを表示する。
- ポリシーの変更を選択したリビジョンにロールバックする。
- リビジョンを TXT ファイルとして保存する。

グループポリシーやユーザーアカウントなどその他のオブジェクトのリビジョンの管理については、*Kaspersky Security Center のヘルプ*を参照してください。

グループポリシーのリビジョンの履歴を確認するには：

1. コンソールツリーの［**管理対象デバイス**］フォルダーで、デバイスが属する管理グループを選択します。
2. 選択したグループの作業領域で、［**ポリシー**］タブを選択します。
3. 任意の列をダブルクリックして、ポリシーのプロパティウィンドウを開きます。
4. ポリシーの**プロパティ**ウィンドウで、［**変更履歴**］セクションを選択します。
   ポリシーリビジョンのリストが表示されます。次の情報が含まれています：
   - ポリシーリビジョン番号
   - ポリシーが変更された日時
   - ポリシーを変更したユーザーの名前
   - ポリシーで実行された処理
   - ポリシー設定に対して行われたリビジョンの説明

グループポリシーの削除

グループポリシーを削除するには：

1. コンソールツリーから、ポリシーを削除する管理グループを選択します。
2. ［**ポリシー**］タブの管理グループの作業領域で、削除するポリシーを選択します。
3. ポリシーのコンテキストメニューから、［**削除**］を選択します。

   これにより、ポリシーが削除されます。新しいポリシーが適用されるまで、管理グループに属するモバイルデバイスは、削除されたポリシーに指定されている設定で動作します。

グループポリシーを設定する権限の制限

Kaspersky Security Center の管理者は、本アプリの様々な機能に対して、管理コンソールユーザーのアクセス権限をユーザーの職務に応じて設定できます。

管理コンソールのインターフェイスで、管理サーバーのプロパティウィンドウの［**セキュリティ**］および［**ユーザーロール**］タブでアクセス権を設定できます。［**ユーザーロール**］タブでは、一連の事前定義された権限を持つ標準のユーザーロールを追加できます。［**セキュリティ**］セクションでは、1人のユーザーまたはユーザーのグループに対して権限を設定したり、1人のユーザーまたはユーザーのグループに対してロールを割り当てたりすることができます。各アプリケーションのユーザー権限は、*機能の範囲*に従って設定されます。

各機能分野固有のユーザー権限も設定することができます。機能分野とポリシータブの対応関係については、付録で説明しています。

各機能分野に対して、管理者は以下の権限を割り当てられます：

- **編集を許可する**：管理コンソールのユーザーは、プロパティウィンドウでポリシー設定を変更することができます。
- **編集をブロックする**：管理コンソールのユーザーは、プロパティウィンドウでポリシー設定を変更することができません。この権限が割り当てられている機能の範囲に属するポリシータブは、インターフェイスには表示されません。

Kaspersky Security Center の管理コンソールでのユーザー権限とロールの管理の詳細は、*Kaspersky Security Center のヘルプ*を参照してください。

プロテクション

このセクションでは、Kaspersky Security Center の管理コンソールでモバイルデバイスの保護を遠隔管理する方法について説明します。

Android デバイスでの保護の設定

脅威、ウイルス、およびその他の悪意のあるアプリケーションを迅速に検知するため、リアルタイム保護とウイルススキャンの自動実行を設定する必要があります。

Kaspersky Endpoint Security for Android が検知するオブジェクトには、次の種別が含まれます：

- ウイルス、ワーム、トロイの木馬、悪意のあるツール
- アドウェア
- デバイスや個人情報に損害を与える目的で悪用される可能性のあるアプリ

アンチウイルスには制限事項があります：

- アンチウイルスの実行中、デバイスの外部ストレージ（SD カードなど）で検知された脅威は、仕事用プロファイルでは自動的に処理されません（ブリーフケースのアイコンが表示されたアプリケーション、Android 仕事用プロファイルの設定）。Kaspersky Endpoint Security for Android は、仕事用プロファイルでは外部ストレージにアクセスできません。検知したオブジェクトの情報は、本アプリの［**状態**］セクションに表示されます。外部ストレージで検知されたオブジェクトを処理するには、手動でオブジェクトを削除し、デバイスのスキャンを再開する必要があります。
- 技術的な制限により、Kaspersky Endpoint Security for Android はサイズが 2 GB 以上のファイルをスキャンできません。スキャン中、そのようなファイルがスキップされたことを通知せずに、ファイルはスキップされます。

モバイルデバイスのリアルタイム保護を設定するには：

1. コンソールツリーの［**管理対象デバイス**］フォルダーで、デバイスが属する管理グループを選択します。
2. 選択したグループの作業領域で、［**ポリシー**］タブを選択します。
3. 任意の列をダブルクリックして、ポリシーのプロパティウィンドウを開きます。
4. ポリシーの**プロパティ**ウィンドウで、［**プロテクション**］セクションを選択します。
5. ［**プロテクション**］セクションで、モバイルデバイスのファイルシステムのプロテクションを設定します：
   - 脅威に対するモバイルデバイスのリアルタイム保護を有効にするには、［**プロテクションを有効にする**］をオンにします。
     新しいアプリとダウンロードフォルダーにあるファイルのみをスキャンします。
   - 脅威に対するモバイルデバイスの拡張保護を有効にするには、［**拡張保護モード**］をオンにします。
     新たにインストールされたモバイルアプリに加え、デバイス上でユーザーが開くファイル、変更するファイル、移動するファイル、コピーするファイル、起動するファイル、保存するファイルがすべてスキャンされます。

     > Android バージョン 8.0 以降のデバイスでは、Kaspersky Endpoint Security for Android はユーザーが編集、移動、インストール、保存、およびコピーしたファイルをスキャンします。Kaspersky Endpoint Security for Android は、開かれた状態のファイル、またはコピー元のファイルをスキャンしません。

   - デバイスに新しくインストールしたアプリを最初に起動する前に、Kaspersky Security Network クラウドサービスを使用してスキャンするには、［**クラウドプロテクション（KSN）**］をオンにします。
   - アドウェアや、デバイスやユーザーのデータに損害を与える目的で悪用される可能性があるアプリをブロックするには、［**アドウェア、オートダイヤラー、リスクウェアの検知**］をオンにします。
6. ［**脅威の検知時の処理**］リストで、次のオプションから1つ選択します：
   - **削除**
     検知したオブジェクトを自動的に削除します。ユーザー側での処理は必要ありません。オブジェクトの削除前に、オブジェクトの削除に関する通知が一時的に表示されます。
   - **スキップ**

     > オブジェクトがスキップされると、Kaspersky Endpoint Security for Android はデバイス保護の問題についてユーザーに警告します。スキップされた脅威に関する情報は、アプリの［**状態**］セクションに表示されます。スキップされた各脅威について、脅威を除去するためにユーザーが実行できる処理が示されます。スキップされたオブジェクトのリストは、悪意のあるファイルが削除または移動された時などに変わることがあります。最新の脅威のリストを取得するには、完全スキャンを実行します。信頼性が高いレベルでデータを保護するには、検知されたすべての脅威を取り除きます。

   - **隔離**
7. ［**適用**］をクリックして、変更を保存します。

モバイルデバイスと Kaspersky Security Center との次回の同期時に、デバイスに設定が適用されます。

モバイルデバイスでのウイルススキャンの自動実行を設定するには：

1. コンソールツリーの［**管理対象デバイス**］フォルダーで、デバイスが属する管理グループを選択します。
2. 選択したグループの作業領域で、［**ポリシー**］タブを選択します。
3. 任意の列をダブルクリックして、ポリシーのプロパティウィンドウを開きます。
4. ポリシーの**プロパティ**ウィンドウで、［**スキャン**］セクションを選択します。
5. アドウェアや、デバイスやユーザーのデータに損害を与える目的で悪用される可能性があるアプリをブロックするには、［**アドウェア、オートダイヤラー、リスクウェアの検知**］をオンにします。
6. ［**脅威の検知時の処理**］リストで、次のオプションから1つ選択します：

   - **削除**

     検知したオブジェクトを自動的に削除します。ユーザー側での処理は必要ありません。オブジェクトの削除前に、オブジェクトの削除に関する通知が一時的に表示されます。

   - **スキップ**

     > オブジェクトがスキップされると、Kaspersky Endpoint Security for Android はデバイス保護の問題についてユーザーに警告します。スキップされた脅威に関する情報は、アプリの［**状態**］セクションに表示されます。スキップされた各脅威について、脅威を除去するためにユーザーが実行できる処理が示されます。スキップされたオブジェクトのリストは、悪意のあるファイルが削除または移動された時などに変わることがあります。最新の脅威のリストを取得するには、完全スキャンを実行します。信頼性が高いレベルでデータを保護するには、検知されたすべての脅威を取り除きます。

   - **隔離**

   - **手動選択**

     Kaspersky Endpoint Security for Android アプリが、検知したオブジェクトに対して実行する処理を次から選択するよう要求する通知を表示します：**スキップ**、**削除**。

     複数のオブジェクトが検知された場合、［**手動選択**］が設定されている状態で、［**すべての脅威に適用**］をオンにすることにより、選択した同じ処理を各ファイルに適用できます。

     > Android 10.0 以降のモバイルデバイスで通知を表示させるには、Kaspersky Endpoint Security for Android をユーザー補助機能としておく必要があります。初期設定ウィザードで Kaspersky Endpoint Security for Android をユーザー補助機能として設定するよう要求されます。このステップはスキップできます。また、後からデバイスの設定でサービスを無効にすることもできます。この場合、Android のシステムウィンドウが表示され、検知したオブジェクトに対して実行する次の処理の選択を要求します：スキップ、削除。複数のオブジェクトに対して1つの処理を適用するには、Kaspersky Endpoint Security を開く必要があります。

7. ［**定期スキャン**］セクションでは、デバイスのファイルシステムの完全スキャンを自動的に開始させる設定を行います。この設定を行うには、［**スケジュール**］をクリックし、［**スケジュール**］ウィンドウで完全スキャンの頻度と開始時刻を指定します。

   > Android 12 以降のデバイスでは、バッテリー節約モードの場合、タスクの実行が指定よりも遅れる場合があります。

8. ［**適用**］をクリックして、変更を保存します。

モバイルデバイスと Kaspersky Security Center との次回の同期時に、デバイスに設定が適用されます。Kaspersky Endpoint Security for Android はすべてのファイルをスキャンし、圧縮ファイルの内容もスキャン対象に含まれます。

モバイルデバイスの保護を最新の状態に保つには、定義データベースのアップデート設定を行ってください。

既定では、デバイスのローミング時の定義データベースのアップデートは無効になっています。定義データベースの定期アップデートは行われません。

定義データベースのアップデート設定を行うには：

1. コンソールツリーの［**管理対象デバイス**］フォルダーで、デバイスが属する管理グループを選択します。
2. 選択したグループの作業領域で、［**ポリシー**］タブを選択します。
3. 任意の列をダブルクリックして、ポリシーのプロパティウィンドウを開きます。
4. ポリシーの**プロパティ**ウィンドウで、［**定義データベースのアップデート**］セクションを選択します。
5. デバイスのローミング時に定義データベースのアップデートをスケジュールに従って実行するには、［**ローミング時のアップデート**］セクションで［**ローミング中の定義データベースのアップデートを許可する**］をオンにします。

   このチェックボックスがオフの場合でも、デバイスのローミング時に定義データベースのアップデートを手動で開始できます。
6. ［**定義データベースのアップデート元**］セクションで、定義データベースのアップデートを取得し、インストールする時の入手元を指定します：

   - **カスペルスキーのサーバー**

     Kaspersky Endpoint Security for Android の定義データベースをユーザーのモバイルデバイスにダウンロードするために、カスペルスキーのアップデートサーバーをアップデート元として使用します。カスペルスキーのサーバーから定義データベースをアップデートする目的で、Kaspersky Endpoint Security for Android はカスペルスキーにデータを転送します（例：アップデートタスクの実行 ID）。定義データベースのアップデート中に転送されるデータのリストは、使用許諾契約書に記載されています。

   - **管理サーバー**

     Kaspersky Endpoint Security for Android の定義データベースをユーザーのモバイルデバイスにダウンロードするために、Kaspersky Security Center の管理サーバーのリポジトリをアップデート元として使用します。

   - **その他のソース**

     Kaspersky Endpoint Security for Android の定義データベースをユーザーのモバイルデバイスにダウンロードするために、サードパーティのサーバーをアップデート元として使用します。アップデートを開始するには、次のフィールドに HTTP サーバーのアドレス（http://domain.com/ など）を入力する必要があります。
7. ［**定義データベースの定期アップデート**］セクションで、ユーザーのデバイスでの定義データベースの自動アップデートを設定します。そのためには、［**スケジュール**］をクリックし、［**スケジュール**］ウィンドウで定義データベースのアップデートの頻度と時刻を指定します。

Android 12 以降のデバイスでは、バッテリー節約モードの場合、タスクの実行が指定よりも遅れる場合があります。

8. ［**適用**］をクリックして、変更を保存します。

モバイルデバイスと Kaspersky Security Center との次回の同期時に、デバイスに設定が適用されます。

インターネット上での Android デバイスの保護

インターネット上でモバイルデバイスユーザーの個人情報を保護するには、危険サイトブロックを有効にします。危険サイトブロックは、悪意のあるコードを配信する Web サイトや、個人情報を盗んで金融機関のアカウントにアクセスする目的で設計されたフィッシングサイトをブロックします。危険サイトブロックは、Web サイトを開く前に、Kaspersky Security Network クラウドサービスを使用して、その Web サイトをスキャンします。また、危険サイトブロックは、あらかじめ定義された許可する Web サイトとブロックする Web サイトのリストに基づいて、Web サイトへのアクセスを設定できます。

Kaspersky Endpoint Security for Android をユーザー補助機能に設定しておく必要があります。初期設定ウィザードで Kaspersky Endpoint Security for Android をユーザー補助機能として設定するよう要求されます。このステップはスキップできます。また、後からデバイスの設定でサービスを無効にすることもできます。

危険サイトブロックは、Google Chrome（カスタムタブ機能を含む）、Huawei Browser、Samsung Internet Browser でのみ動作します。仕事用プロファイルを使用しており、危険サイトブロックが仕事用プロファイルでのみ有効となるよう設定されている場合は、Samsung Internet Browser 用の危険サイトブロックはモバイルデバイス上でサイトをブロックしません。

危険サイトブロックを Google Chrome、Huawei Browser、Samsung Internet Browser で有効にするには：

1. コンソールツリーの［**管理対象デバイス**］フォルダーで、デバイスが属する管理グループを選択します。
2. 選択したグループの作業領域で、［**ポリシー**］タブを選択します。
3. 任意の列をダブルクリックして、ポリシーのプロパティウィンドウを開きます。
4. ポリシーの**プロパティ**ウィンドウで、［**危険サイトブロック**］セクションを選択します。
5. 危険サイトブロックを使用するには、危険サイトブロックの使用を目的としたデータ処理に関する声明（「危険サイトブロックに関する声明」）への管理者または端末のユーザーによる同意が必要です。

   a. ［**危険サイトブロックに関する声明**］をクリックします。

   ［**危険サイトブロックの使用を目的としたデータ処理に関する声明**］ウィンドウが開きます。危険サイトブロックに関する声明に同意するには、プライバシーポリシーを読んで同意する必要があります。

   b. ［プライバシーポリシー］をクリックします。プライバシーポリシーを読んで同意します。

   この方法でプライバシーポリシーに同意しない場合、モバイルデバイスのユーザーは初期設定ウィザードの途中か、または本アプリの設定で同意できます（☰ → ［**製品情報**］→［**契約書、ポリシー、声明**］→［**プライバシーポリシー**］）。

   c. 危険サイトブロックに関する声明への同意方法を選択します：

   - **危険サイトブロックに関する声明を確認し、同意する**
   - **危険サイトブロックに関する声明への同意を端末のユーザーに要求する**

- **危険サイトブロックに関する声明に同意しない**

6. ［**危険サイトブロックに関する声明に同意しない**］を選択すると、危険サイトブロックはサイトをブロックしなくなります。また、モバイルデバイスユーザーが危険サイトブロックを有効にすることもできません。

7. ［**危険サイトブロックを有効にする**］をオンにします。

8. ［**適用**］をクリックして、変更を保存します。

モバイルデバイスと Kaspersky Security Center との次回の同期時に、デバイスに設定が適用されます。

盗難または紛失時のデバイスデータの保護

このセクションでは、モバイルデバイスの紛失時または盗難時に、デバイスのデータを不正なアクセスから保護する設定について説明します。

モバイルデバイスへのコマンドの送信

紛失したデバイスや盗難にあったデバイスのデータを保護するため、特別なコマンドを送信できます（下の表を参照）。

紛失したデバイスや盗難にあったデバイスのデータを保護するためのコマンド

Kaspersky Security Center に接続する方法	コマンド	コマンドの実行結果
Kaspersky Endpoint Security for Android	ロック	モバイルデバイスがロックされます。
	ロック解除	Android 5.0 - 6.X のモバイルデバイスでロックを解除すると、画面ロックの解除パスワード（PIN コード）は「1234」にリセットされます。Android 7.0 以降のデバイスでは、ロックの解除後も画面ロックの解除パスワードは変更されません。
	デバイスの GPS 追跡	デバイスの位置が追跡され、Google Maps に表示されます。SMS の送信およびインターネットアクセスにかかる費用は有料です。 Android 12 以降を実行しているデバイスでは、ユーザーが［おおよその位置情報］の権限を付与していても、 Kaspersky Endpoint Security for Android は最初に正確な位置情報を取得しようとします。これが成功しなかった場合、コマンドが 30 分以内に送信された場合のみ、おおよその位置情報が返されます。そうでない場合は **GPS 追跡**は失敗します。
	遠隔撮影	モバイルデバイスがロックされます。デバイスのロックを誰かが解除しようとすると、デバイスのフロントカメラで写真が遠隔撮影されます。SMS の送信およびインターネットアクセスにかかる費用は有料です。 デバイスのロック解除を試行すると、ユーザーは遠隔撮影に自動的に同意したことになります。

		カメラを使用する権限が無効になっていると、権限を与えるよう促す通知が表示されます。Android 12 以降を実行しているモバイルデバイスでは、クイック設定でカメラを使用する権限が無効になっていると通知は表示されませんが撮影された写真は黒い画面になります。
	遠隔アラーム	モバイルデバイスのアラームが作動します。アラームは 5 分間作動します（デバイスのバッテリーが少ない場合は 1 分）。
	企業データを消去する	コンテナーデータ、会社のメールアカウント、会社の Wi-Fi ネットワークと VPN への接続設定、アクセスポイント名（APN）、Android 仕事用プロファイル、KNOX のコンテナー、KNOX License Manager ライセンスを消去します。
	出荷時の設定にリセットする	すべてのデータがモバイルデバイスから削除され、設定が工場出荷時の値にロールバックされます。このコマンドの実行後、デバイスはそれ以降のコマンドを受信または実行できなくなります。
iOS MDM プロファイル	ロック	モバイルデバイスがロックされます。
	ロック解除	PIN コードによるモバイルデバイスのロックは無効です。以前に指定された PIN コードはリセットされました。
	企業データを消去する	インストール済みの設定プロファイル、プロビジョニングプロファイル、iOS MDM プロファイル、［**iOS MDM プロファイルと一緒に削除する**］がオンのアプリ、これらはすべてデバイスから削除されます。
	出荷時の設定にリセットする	すべてのデータがモバイルデバイスから削除され、設定が工場出荷時の値にロールバックされます。このコマンドの実行後、デバイスはそれ以降のコマンドを受信または実行できなくなります。
Exchange メールボックス	出荷時の設定にリセットする	すべてのデータがモバイルデバイスから削除され、設定が工場出荷時の値にロールバックされます。このコマンドの実行後、デバイスはそれ以降のコマンドを受信または実行できなくなります。

Kaspersky Endpoint Security for Android のコマンドの実行には、特別な権限が必要です。初期設定ウィザードの実行時に、必要なすべての権限を Kaspersky Endpoint Security for Android に付与するよう要求されます。このステップはスキップできます。また、後からデバイスの設定で権限を無効にすることもできます。その場合、コマンドを実行することはできません。

Android 10.0 以降のデバイスの場合、位置情報へのアクセス権を常に許可するように設定する必要があります。Android 11.0 以降のデバイスの場合、カメラへのアクセス権をアプリの使用時のみ許可するように設定する必要があります。設定しない場合、盗難対策コマンドが動作しません。動作の制限に関する通知が表示され、必要なレベルのアクセス権を許可するように再度要求されます。カメラへのアクセス権を今回のみ許可するオプションをユーザーが選択すると、本アプリはアクセス権が許可されたと判断します。カメラへのアクセス権が再度要求される場合は、ユーザーに直接確認することを推奨します。

管理コンソールのモバイルデバイスリストからコマンドを送信する方法については、*Kaspersky Security Center のヘルプ*を参照してください。

モバイルデバイスのロック解除

次の方法でモバイルデバイスのロックを解除できます：

- モバイルデバイスロック解除用コマンドを送信する。
- モバイルデバイスでロック解除用のワンタイムパスワードを入力する（Android デバイスのみ）。

一部のデバイス（Huawei、Meizu、Xiaomi など）では、オペレーティングシステム起動時に開始するアプリのリストに Kaspersky Endpoint Security for Android を手動で追加する必要があります。アプリがリストに追加されていない場合、デバイスのロックを解除するには、ロック解除用のワンタイムパスワードを使用するしか方法はありません。デバイスのロックを解除するコマンドは使用できません。

管理コンソールのモバイルデバイスリストからコマンドを送信する方法については、*Kaspersky Security Center のヘルプ*を参照してください。

*ロック解除用のワンタイムパスワード*は、モバイルデバイスのロック解除に使用する秘密のアプリケーションコードです。ワンタイムパスワードは本アプリによって生成され、モバイルデバイスごとに異なります。グループポリシー設定の［**盗難対策**］セクションでワンタイムパスワードの長さ（4 桁、8 桁、16 桁）を変更できます。

ワンタイムパスワードを使用してモバイルデバイスのロックを解除するには：

1. コンソールツリーで、［**モバイルデバイス管理**］→［**モバイルデバイス**］の順に選択します。
2. ロック解除用のワンタイムパスワードを取得するモバイルデバイスを選択します。
3. ダブルクリックでモバイルデバイスのプロパティウィンドウを開きます。
4. ［**アプリケーション**］→［**Kaspersky Endpoint Security for Android**］の順に選択します。
5. ダブルクリックで Kaspersky Endpoint Security のプロパティウィンドウを開きます。
6. ［**盗難対策**］セクションを選択します。
7. ［**デバイスロック解除用ワンタイムパスワード**］セクションの［**ワンタイムパスワード**］に、選択した端末用の一意のワンタイムパスワードが表示されます。
8. 任意の方法（メールなど）で、ロックされたデバイスのユーザーにワンタイムパスワードを連絡します。
9. Kaspersky Endpoint Security for Android によってロックされたデバイスの画面に、ユーザーがワンタイムパスワードを入力します。

モバイルデバイスのロックが解除されます。Android 5.0 - 6.X のモバイルデバイスでロックを解除すると、画面ロックの解除パスワード（PIN コード）は「1234」にリセットされます。Android 7.0 以降のデバイスでは、ロックの解除後も画面ロックの解除パスワードは変更されません。

データ暗号化

不正なアクセスからデータを保護するには、デバイス上のすべてのデータの暗号化を有効にする必要があります（ユーザーアカウント、外部デバイス、アプリからのデータ、メールメッセージ、SMS メッセージ、連絡先、写真、その他のファイルなど）。暗号化されたデータにアクセスするには、特別なキー、すなわちデバイスロック解除用パスワードを指定する必要があります。データが暗号化されている場合、デバイスロックが解除されている場合のみ、データにアクセスすることができます。

パスワードでロックされた iOS デバイスでは、既定でデータ暗号化が有効です（［**設定**］→［**Touch ID / Face ID とパスコード**］→［**パスワードをオンにする**］）。

Android デバイス上のすべてのデータを暗号化するには：

1. Android デバイスで画面ロックを有効にします（［**設定**］→［**セキュリティ**］→［**画面ロック**］）。
2. 企業のセキュリティ要件に準拠したデバイスロック解除用パスワードを設定します。

   デバイスのロック解除にパターンロックは使用しないでください。Android バージョン 6.0 以降の一部の Android デバイスでは、データを暗号化し、Android デバイスを再起動した後、デバイスのロックを解除するには、パターンロックではなく数値のパスワードの入力が必要です。この問題は、ユーザー補助機能サービスの動作に関係しています。この場合、デバイス画面のロックを解除するには、パターンロックを数値のパスワードに変換してください。パターンロックを数値のパスワードへ変換する方法の詳細については、モバイルデバイス製造元のテクニカルサポートサイトを参照してください。

3. デバイスですべてのデータの暗号化を有効にします（［**設定**］→［**セキュリティ**］→［**データの暗号化**］）。

デバイスロック解除用パスワードの強度の設定

ユーザーのモバイルデバイスに対するアクセスを保護するには、デバイスロック解除用パスワードを設定する必要があります。

このセクションでは、Android デバイスおよび iOS デバイスにおいて、パスワード保護を設定する方法について説明します。

Android デバイスでのロック解除用パスワードの強度の設定

Android デバイスの安全性を保つには、デバイスのスリープモードを解除する時に入力するパスワードの使用を設定する必要があります。

ロック解除用パスワードが弱い場合、デバイスでのユーザーの操作に制限をかけることができます（デバイスのロックなど）。制限はコンプライアンスコントロールコンポーネントを使用して設定できます。そのためには、スキャンルール設定で［**ロック解除のパスワードがセキュリティ要件に適合していません**］基準を選択する必要があります。

一部の Android バージョン 7.0 以降の Samsung デバイスでは、デバイスがサポートしていないロック解除方法（パターンパスワードなど）を設定しようとするとデバイスがロックされる場合があります。発生条件は次の通りです：Kaspersky Endpoint Security for Android の削除からの保護が有効で、ロック解除のパスワードの強度要件を設定している場合。デバイスのロックを解除するには、特別なコマンドをデバイスに送信する必要があります。

ロックを解除するパスワードの使用を設定するには：

1. コンソールツリーの［**管理対象デバイス**］フォルダーで、デバイスが属する管理グループを選択します。
2. 選択したグループの作業領域で、［**ポリシー**］タブを選択します。
3. 任意の列をダブルクリックして、ポリシーのプロパティウィンドウを開きます。
4. ポリシーの**プロパティ**ウィンドウで、［**デバイス管理**］セクションを選択します。
5. ロック解除用パスワードが設定されているかどうかをアプリで確認する場合は、［**画面ロック**］セクションの［**画面のロック解除用パスワードの設定を要求する**］をオンにします。

   デバイスにシステムパスワードが設定されていない場合は、ユーザーが設定する必要があります。パスワードは管理者により定義されたパラメータに従って設定します。
6. 最小文字数を指定します。

   パスワードを構成する文字数の最小値。指定可能な値：4 ～ 16 の文字。

   既定の最小文字数は 4 です。

   Android 10.0 以降のデバイスでは、パスワードの強度要件（中程度または高強度）がシステムの値として実装されます。

   Android 10.0 以降のデバイスでは、値は次のルールに従って決定されます：

   - 1 ～ 4 文字のパスワード長が必要な場合、中程度の強度のパスワードを設定するようユーザーに要求します。重複したり順番（例：1234）に並んでいたりしない数字（PIN）か、英字と数字の組み合わせである必要があります。PIN またはパスワードは、4 文字以上である必要があります。
   - 5 文字以上のパスワード長が必要な場合、高強度のパスワードを設定するようユーザーに要求します。重複したり順番に並んでいたりしない数字（PIN）か、英字と数字の組み合わせ（パスワード）である必要があります。PIN は 8 文字以上の数字で、パスワードは 6 文字以上である必要があります。
7. 画面のロック解除に指紋認証を使用することをユーザーに認める場合は、［**指紋認証の使用を許可する**］をオンにします。ロック解除のパスワードが企業のセキュリティ要件に適合していない場合、画面のロック解除に指紋認証スキャナーを使用することはできません。

   Android 10.0 以降のデバイスでは、画面ロック解除は仕事用プロファイルでのみ管理可能です。

   Kaspersky Endpoint Security for Android は、アプリへのログイン時または購入の確認時の指紋認証スキャナーの使用は制限しません。

一部の Samsung デバイスでは、画面のロック解除に指紋認証を使用することをブロックできません。
一部の Samsung デバイスでは、ロック解除用パスワードが企業のセキュリティ要件に準拠していない場合、Kaspersky Endpoint Security for Android は画面のロック解除での指紋認証の使用をブロックしません。

デバイス設定に指紋認証を追加した後、ユーザーは次の方法で画面のロックを解除できます：

- 指紋認証スキャナーに指を押し当てる（メインの方法）。
- ロック解除用パスワードを入力する（予備の方法）。

8. ［**適用**］をクリックして、変更を保存します。

モバイルデバイスと Kaspersky Security Center との次回の同期時に、デバイスに設定が適用されます。

iOS MDM デバイスでのロック解除用パスワードの強度の設定

iOS MDM デバイスのデータを保護するために、ロック解除用パスワードの強度を設定します。

既定では、簡単なパスワードを使用できます。「*簡単なパスワード*」とは、「abcd」や「2222」のような連続する文字や反復する文字で構成されたパスワードです。特殊文字を含む英数字のパスワードを入力する必要はありません。既定では、パスワードの有効期間およびパスワードの試行回数に制限はありません。

iOS MDM デバイスのロック解除用パスワードの強度を設定するには：

1. コンソールツリーの［**管理対象デバイス**］フォルダーで、iOS MDM デバイスが属する管理グループを選択します。
2. 選択したグループの作業領域で、［**ポリシー**］タブを選択します。
3. ダブルクリックでポリシーのプロパティウィンドウを開きます。
4. ポリシーの**プロパティ**ウィンドウで、［**パスワード**］セクションを選択します。
5. ［**パスワードの設定**］セクションで、［**デバイスに設定を適用する**］をオンにします。
6. ロック解除用パスワードの強度の設定：
   - 簡単なパスワードを使用できるようにするには、［**簡単なパスワードを許可する**］をオンにします。
   - 英字と数字の両方をパスワードに使用することを要求する場合は、［**英数字の値を要求する**］をオンにします。
   - ［**パスワードの長さの最小値**］で、パスワードの文字数の最小値を選択します。
   - ［**特殊文字の最小数**］で、パスワードに使用する特殊文字（「$」「&」「!」など）の最小文字数を選択します。
   - ［**パスワードの最長有効期間**］で、パスワードの有効期間を日数で指定します。この期間を過ぎると、Kaspersky Device Management for iOS はユーザーにパスワードの変更を要求します。
   - ［**自動ロックを有効にする**］で、iOS MDM デバイスの自動ロックを有効にする時間を選択します。

- ［**パスワードの履歴**］に、パスワードを変更する時に、Kaspersky Device Management が新しいパスワードと比較するためにパスワードの数（現在のパスワードも含む）を指定します。パスワードが一致した場合、新しいパスワードは拒否されます。

- ［**パスワードなしでロック解除する最長時間**］で、パスワードを入力せずに iOS MDM デバイスのロックを解除できる時間を設定します。

- ［**アクセスの最大試行回数**］で、iOS MDM デバイスのロック解除用パスワードを入力できる試行回数を選択します。

7. ［**適用**］をクリックして、変更を保存します。

これにより、ポリシーが適用された後、Kaspersky Device Management for iOS はモバイルデバイスに設定されているパスワードの強度を確認します。デバイスのロック解除用パスワードの強度がポリシーに準拠していない場合、ユーザーはパスワードを変更するように要求されます。

EAS デバイスでのロック解除用パスワードの強度の設定

EAS デバイスのデータを保護するために、強力なロック解除用パスワードを設定します。

既定では、モバイルデバイスが起動された時に、Kaspersky Device Management for iOS はロック解除用パスワードを入力または設定するようにユーザーに要求しません。

EAS デバイスのロック解除用パスワードの強度を設定するには：

1. コンソールツリーの［**管理対象デバイス**］フォルダーで、EAS デバイスが属する管理グループを選択します。

2. 選択したグループの作業領域で、［**ポリシー**］タブを選択します。

3. ダブルクリックでポリシーのプロパティウィンドウを開きます。

4. ポリシーのプロパティウィンドウで、［**パスワード**］セクションを選択します。

5. ［**パスワードの設定**］セクションで、［**パスワードを要求する**］をオンにします。

6. ロック解除用パスワードの強度の設定：

   - 英字と数字の両方をパスワードに使用することを要求する場合は、［**英数字の値を要求する**］をオンにします。［**文字セットの最小数**］に、英数字のパスワードの強度レベルを指定します。指定可能な値：1 ～ 4。値「1」は、最も低いレベルの強度です。

   - パスワードの復旧機能の使用を許可する場合は、［**パスワードの復旧を有効にする**］をオンにします。

   - デバイスのメモリ内でファイルを暗号化する場合は、［**デバイス上で暗号化が必要**］をオンにします。

   - メモリカード上でファイルを暗号化する場合は、［**メモリカード上で暗号化が必要**］をオンにします。

   - 数字のみの簡単なパスワードの使用を許可する場合は、［**簡単なパスワードを許可する**］をオンにします。

   - デバイスにアクセスするためのパスワード入力の試行回数を制限するには、［**アクセスの最大試行回数**］をオンにします。チェックボックスの右側にあるフィールドに、デバイスのロックを解除するためのパスワード入力の試行回数を指定します。指定された試行回数内に正しいパスワードが入力されない場合、Kaspersky Device Management for iOS はすべてのデバイスデータを消去します。

- パスワードの最も少ない文字数を指定するには、［**パスワードの長さの最小値**］をオンにします。チェックボックスの右側にあるフィールドに、パスワードの文字数の最小値を指定します。指定可能な値：4 ～ 16 の文字。

- ある一定時間、デバイスがアイドル状態になった時、ユーザーにパスワードの入力を要求する場合は、［**パスワードの新規入力までのアイドル時間（分）**］をオンにします。チェックボックスの右側にあるフィールドに、アイドル時間を分単位で指定します。この時間が経過すると、ユーザーはパスワードの入力を要求されます。

- パスワードの有効期間を制限するには、［**パスワードの有効期間（日）**］をオンにします。チェックボックスの右側にあるフィールドに、パスワードの有効期間を指定します。この期間が経過すると、ユーザーはパスワードの変更を要求されます。

- ［**パスワードの履歴**］に、再利用できない以前のパスワードの数を指定できます。

7. ［**適用**］をクリックして、変更を保存します。

モバイルデバイスと Kaspersky Security Center との次回の同期時に、デバイスに設定が適用されます。ポリシーが適用された後、Kaspersky Device Management for iOS はモバイルデバイスに設定されているパスワードの強度をチェックします。ロック解除用パスワードがデバイスに設定されていない場合、ユーザーはパスワードを設定するように要求されます。パスワードは、ポリシーの設定内容を考慮して設定する必要があります。デバイスのロック解除用パスワードが設定されていても、ポリシーに準拠していない場合、ユーザーはパスワードを変更するように要求されます。

仮想プライベートネットワーク（VPN）の設定

このセクションでは、Wi-Fi ネットワークへの安全な接続のための仮想プライベートネットワーク（VPN）の設定について説明します。

Android デバイスでの VPN の設定（Samsung のみ）

Android デバイスを Wi-Fi ネットワークに安全に接続し、データ転送を保護するには、VPN（仮想プライベートネットワーク）を設定する必要があります。

VPN の設定は、Samsung デバイスでのみ編集可能です。

仮想プライベートネットワークを使用する時に考慮すべき要件は次の通りです：

- VPN 接続を使用するアプリは、ファイアウォール設定で許可しておく必要があります。

- ポリシーで指定された仮想プライベートネットワークの設定は、システムアプリケーションに適用することはできません。システムアプリケーションの VPN 接続は手動で設定する必要があります。

- VPN 接続を使用する一部のアプリケーションは、初回起動時に詳細設定を行う必要があります。設定を行うには、アプリケーション設定で VPN 接続を許可する必要があります。

ユーザーのモバイルデバイスで VPN を設定するには：

1. コンソールツリーの［**管理対象デバイス**］フォルダーで、デバイスが属する管理グループを選択します。

2. 選択したグループの作業領域で、［**ポリシー**］タブを選択します。

3. 任意の列をダブルクリックして、ポリシーのプロパティウィンドウを開きます。

4. ポリシーの**プロパティ**ウィンドウで、［**Samsung KNOX の管理**］→［**Samsung デバイスの管理**］セクションを順に選択します。

5. ［**VPN**］セクションで、［**設定**］をクリックします。
［**VPN ネットワーク**］ウィンドウが開きます。

6. ［**接続種別**］ドロップダウンリストで、VPN 接続の種別を選択します。

7. ［**ネットワーク名**］に、VPN トンネルの名前を入力します。

8. ［**サーバーのアドレス**］に、VPN サーバーのネットワーク名または IP アドレスを入力します。

9. ［**DNS 検索ドメイン**］に、DNS サーバー名に自動的に追加する DNS 検索ドメインを入力します。
DNS 検索ドメインは、空白で区切って複数指定できます。

10. ［**DNS サーバー**］に、VPN サーバーの完全ドメイン名または IP アドレスを入力します。
複数の DNS サーバーを空白で区切って指定できます。

11. ［**ルーティング**］に、VPN 接続を介してデータ交換を行うネットワークの IP アドレスの範囲を入力します。

> IP アドレスの範囲を［**ルーティング**］に指定しない場合は、すべてのインターネットトラフィックが VPN 接続を通過することになります。

12. さらに、**IPSec Xauth PSK** と **L2TP IPSec PSK** のネットワークタイプに対して次の設定を行います：

    a. ［**IPSec 共有鍵**］に、プリセットされた IPSec 暗号鍵を入力します。

    b. ［**IPSec ID**］に、モバイルデバイスのユーザーの名前を入力します。

13. **L2TP IPSec PSK** ネットワークについては、［**L2TP 暗号鍵**］に L2TP 暗号鍵のパスワードを指定することもできます。

14. **PPTP** ネットワークの場合は、［**SSL 接続を使用する**］を選択すると、アプリはモバイルデバイスが VPN サーバーに接続する時に、データ暗号化として MPPE（Microsoft Point-to-Point 暗号化）方式を使用してデータ転送を保護します。

15. ［**適用**］をクリックして、変更を保存します。

モバイルデバイスと Kaspersky Security Center との次回の同期時に、デバイスに設定が適用されます。

iOS MDM デバイスでの VPN の設定

iOS MDM デバイスを仮想プライベートネットワーク（VPN）に接続し、VPN への接続中にデータを保護するため、VPN 接続を設定します。

iOS MDM デバイスで VPN 接続を設定するには：

1. コンソールツリーの［**管理対象デバイス**］フォルダーで、iOS MDM デバイスが属する管理グループを選択します。

2. 選択したグループの作業領域で、［**ポリシー**］タブを選択します。

3. ダブルクリックでポリシーのプロパティウィンドウを開きます。

4. ポリシーの**プロパティ**ウィンドウで、［**VPN**］セクションを選択します。

5. ［**VPN ネットワーク**］セクションで、［**追加**］をクリックします。
［**VPN ネットワーク**］ウィンドウが開きます。

6. ［**ネットワーク名**］に、VPN トンネルの名前を入力します。

7. ［**接続種別**］ドロップダウンリストで、VPN 接続の種別を選択します：

   - **L2TP**（Layer 2 Tunneling Protocol）：この接続は、MS-CHAP v2 パスワード、2 要素認証、および公開鍵による自動認証を使用する iOS MDM モバイルデバイスユーザーの認証をサポートします。

   - **PPTP**（Point-to-Point Tunneling Protocol）：この接続は、MS-CHAP v2 パスワード、および 2 要素認証を使用する iOS MDM モバイルデバイスユーザーの認証をサポートします。

   - **IPSec (Cisco)**：この接続は、パスワードベースのユーザー認証、2 要素認証、および公開鍵と証明書を使用する自動認証をサポートします。

   - **Cisco AnyConnect**：この接続は、Cisco Adaptive Security Appliance（ASA）ファイアウォールのバージョン 8.0(3).1 以降をサポートします。VPN 接続を設定するには、iOS MDM モバイルデバイスに App Store から Cisco AnyConnect アプリをインストールします。

   - **Juniper SSL**：この接続は、Juniper Networks IVE パッケージのバージョン 7 以降が搭載された、Juniper Networks SSL VPN gateway Series SA バージョン 6.4 以降をサポートします。VPN 接続を設定するには、App Store から JUNOS アプリを iOS MDM モバイルデバイスにインストールします。

   - **F5 SSL**：この接続は、F5 BIG-IP Edge Gateway、Access Policy Manager、および Fire SSL VPN ソリューションをサポートします。VPN 接続を設定するには、iOS MDM モバイルデバイスに App Store から F5 BIG-IP Edge Client アプリをインストールします。

   - **SonicWALL Mobile Connect**：この接続は、SonicWALL Aventail E-Class Secure Remote Access バージョン 10.5.4 以降、SonicWALL SRA バージョン 5.5 以降、ならびに SonicOS バージョン 5.8.1.0 以降が搭載された TZ、NSA、E-Class NSA を含む SonicWALL Next-Generation Firewall をサポートします。VPN 接続を設定するには、iOS MDM モバイルデバイスに App Store から SonicWALL Mobile Connect アプリをインストールします。

   - **Aruba VIA**：この接続は、Aruba Networks mobile access controllers をサポートします。この接続を設定するには、iOS MDM モバイルデバイスに App Store から Aruba Networks VIA アプリをインストールします。

   - **カスタム SSL**：この接続は、パスワードと証明書を使用する iOS MDM モバイルデバイスユーザーの認証、および 2 要素認証をサポートします。

8. ［**サーバーのアドレス**］に、VPN サーバーのネットワーク名または IP アドレスを入力します。

9. ［**アカウント名**］に、VPN サーバーで認証を行うアカウント名を入力します。［**使用できるマクロ**］ドロップダウンリストからマクロを使用できます。

10. 選択した仮想プライベートネットワークの種別に従って、VPN 接続のセキュリティ設定を行います。

11. 必要に応じて、プロキシサーバーを使用した VPN 接続の設定を行います：

    a. ［**プロキシサーバーの設定**］タブを選択します。

b. プロキシサーバーの設定モードを選択し、接続設定を指定します。

c. ［**OK**］をクリックします。

これにより、プロキシサーバーを使用した VPN への接続設定が、iOS MDM デバイスに適用されます。

12. ［**OK**］をクリックします。
新しい VPN がリストに表示されます。

13. ［**適用**］をクリックして、変更を保存します。

これにより、ポリシーが適用された後、VPN 接続が iOS MDM デバイスに設定されます。

Android デバイスでのファイアウォールの設定（Samsung のみ）

モバイルデバイスでのネットワーク接続を監視するために、ファイアウォール設定を行います。

モバイルデバイスでファイアウォールを設定するには：

1. コンソールツリーの［**管理対象デバイス**］フォルダーで、デバイスが属する管理グループを選択します。
2. 選択したグループの作業領域で、［**ポリシー**］タブを選択します。
3. 任意の列をダブルクリックして、ポリシーのプロパティウィンドウを開きます。
4. ポリシーの**プロパティ**ウィンドウで、［**Samsung KNOX の管理**］→［**Samsung デバイスの管理**］セクションを順に選択します。
5. ［**ファイアウォール**］ウィンドウで、［**設定**］をクリックします。
［**ファイアウォール**］ウィンドウが表示されます。
6. ファイアウォールのモードを選択します：
   - すべてのインバウンド接続とアウトバウンド接続を許可するには、スライダーを［**すべて許可**］まで移動します。
   - 除外リストのアプリを除くすべてのネットワーク活動をブロックするように設定する場合は、スライダーを［**すべてブロック（例外あり）**］まで移動させます。
7. ファイアウォールモードを［**すべてブロック（例外あり）**］に設定した場合は、除外リストを作成します：
   a. ［**追加**］をクリックします。
   ［**ファイアウォールで信頼するオブジェクト**］ウィンドウが開きます。
   b. ［**アプリの名前**］に、モバイルアプリの名前を入力します。
   c. ［**パッケージ名**］にモバイルアプリのパッケージのシステム名を入力します（例：`com.mobileapp.example`）。
   d. ［**OK**］をクリックします。
8. ［**適用**］をクリックして、変更を保存します。

モバイルデバイスと Kaspersky Security Center との次回の同期時に、デバイスに設定が適用されます。

Kaspersky Endpoint Security for Android の削除に対する保護

モバイルデバイス保護と企業のセキュリティ要件準拠のため、Kaspersky Endpoint Security for Android の削除に対する保護を有効にできます。この場合、ユーザーは Kaspersky Endpoint Security for Android のインターフェイスを使用して本アプリを削除することはできません。Android オペレーティングシステムのツールを使用してアプリを削除する場合、Kaspersky Endpoint Security for Android の管理者権限を無効にするよう要求されます。権限を無効にすると、モバイルデバイスはロックされます。

一部の Android バージョン 7.0 以降の Samsung デバイスでは、デバイスがサポートしていないロック解除方法（パターンパスワードなど）を設定しようとするとデバイスがロックされる場合があります。発生条件は次の通りです：Kaspersky Endpoint Security for Android の削除からの保護が有効で、ロック解除のパスワードの強度要件を設定している場合。デバイスのロックを解除するには、特別なコマンドをデバイスに送信する必要があります。

Kaspersky Endpoint Security for Android の削除に対する保護を有効にするには：

1. コンソールツリーの［**管理対象デバイス**］フォルダーで、デバイスが属する管理グループを選択します。
2. 選択したグループの作業領域で、［**ポリシー**］タブを選択します。
3. 任意の列をダブルクリックして、ポリシーのプロパティウィンドウを開きます。
4. ポリシーの**プロパティ**ウィンドウで、［**詳細**］セクションを選択します。
5. ［**Kaspersky Endpoint Security for Android の削除**］セクションで、［**Kaspersky Endpoint Security for Android の削除を許可**］をオフにします。

   Android 7.0 以降のデバイスでアプリが削除されないように保護するには、Kaspersky Endpoint Security for Android をユーザー補助機能として設定しておく必要があります。初期設定ウィザードの実行時に、必要な権限を Kaspersky Endpoint Security for Android に付与するよう要求されます。このステップはスキップできます。また、後からデバイスの設定で権限を無効にすることもできます。その場合、手動による削除はブロックできません。
6. ［**適用**］をクリックして、変更を保存します。

モバイルデバイスと Kaspersky Security Center との次回の同期時に、デバイスに設定が適用されます。本アプリを削除しようとすると、モバイルデバイスはロックされます。

デバイスハッキング（root）の検知

Kaspersky Security for Mobile では、デバイスハッキング（root）を検知できます。ハッキングされたデバイスでは、システムファイルの保護が解除され、その結果、編集可能になってしまいます。さらに、提供元が不明なサードパーティのアプリをハッキングされたデバイスにインストールすることもできてしまいます。ハッキング試行を検知した場合、ただちにデバイスの正常動作を復元してください。

ユーザーによるルート権限の取得を検知する時、次のサービスが使用されます：

- *Embedded Kaspersky Endpoint Security for Android* は、カスペルスキーのサービスです（Kaspersky Mobile Security SDK）。モバイルデバイスユーザーがルート権限を取得したかどうかを確認します。

- *SafetyNet Attestation* は Google のサービスです。オペレーティングシステムの整合性を確認し、デバイスのハードウェアおよびソフトウェアを分析し、その他のセキュリティ上の問題を特定します。SafetyNet Attestation の詳細は、Android のテクニカルサポートサイトを参照してください。

デバイスがハッキングされた場合は、通知を受信します。ハッキング通知は、管理サーバーの作業領域の［**監視**］タブで確認できます。また、イベント通知設定でハッキングについての通知を無効にすることもできます。

Android デバイスでは、デバイスがハッキングされた場合、デバイスでのユーザーの操作に制限をかけることができます（デバイスのロックなど）。制限はコンプライアンスコントロールコンポーネントを使用して設定できます（下の図を参照）。それには、スキャンルール設定で［**デバイスに管理者権限があります**］基準を選択します。

iOS MDM デバイスでのグローバル HTTP プロキシの設定

インターネットのトラフィックを保護するために、 iOS MDM デバイスがプロキシサーバーを使用してインターネットへ接続するように設定します。

プロキシサーバーを使用してインターネットに自動的に接続できるのは、管理対象のデバイスのみです。

iOS MDM デバイスでグローバル HTTP プロキシを設定するには：

1. コンソールツリーの［**管理対象デバイス**］フォルダーで、iOS MDM デバイスが属する管理グループを選択します。
2. 選択したグループの作業領域で、［**ポリシー**］タブを選択します。
3. ダブルクリックでポリシーのプロパティウィンドウを開きます。
4. ポリシーの**プロパティ**ウィンドウで、［**グローバル HTTP プロキシ**］セクションを選択します。
5. ［**グローバル HTTP プロキシの設定**］セクションで、［**デバイスに設定を適用する**］をオンにします。
6. グローバル HTTP プロキシ設定の種別を選択します。

   既定では、グローバル HTTP プロキシの種別として「手動」が選択され、ユーザーはプロキシサーバーに接続せずにキャプティブネットワークに接続することはできません。*キャプティブネットワーク*とは、プロキシサーバーへの接続なしでモバイルデバイス上での事前認証を必要とする無線ネットワークです。

   - プロキシサーバーの接続設定を手動で指定するには：
     a. ［**プロキシ設定の種別**］ドロップダウンリストで、［**手動**］を選択します。
     b. **プロキシサーバーのアドレスとポート**のフィールドに、プロキシサーバーのホスト名または IP アドレスと、プロキシサーバーのポート番号を入力します。
     c. ［**ユーザー名**］に、プロキシサーバーの認証に必要なユーザーアカウント名を設定します。［**使用できるマクロ**］ドロップダウンリストからマクロを使用できます。
     d. ［**パスワード**］に、プロキシサーバーの認証に必要なユーザーアカウントパスワードを設定します。

e. ユーザーがキャプティブネットワークにアクセスできるようにするには、［**プロキシに接続せずにキャプティブネットワークへのアクセスを許可する**］をオンにします。

- 定義済みの PAC（プロキシ自動設定）ファイルを使用して、プロキシサーバーの接続を設定するには：

  a. ［**プロキシ設定の種別**］ドロップダウンリストで、［**自動**］を選択します。

  b. ［**PAC ファイルの URL**］に、PAC ファイルの URL（http://www.example.com/filename.pac など）を入力します。

  c. PAC ファイルにアクセスできない時に、プロキシサーバーを使用せずにモバイルデバイスを無線ネットワークに接続できるようにするには、［**PAC ファイルにアクセスできない場合は直接接続を許可する**］をオンにします。

  d. ユーザーがキャプティブネットワークにアクセスできるようにするには、［**プロキシに接続せずにキャプティブネットワークへのアクセスを許可する**］をオンにします。

7. ［**適用**］をクリックして、変更を保存します。

これにより、ポリシーの適用後、モバイルデバイスユーザーはプロキシサーバーを使用してインターネットに接続されます。

iOS MDM デバイスへのセキュリティ証明書の追加

ユーザー認証を簡素化してデータのセキュリティを確保するために、ユーザーの iOS MDM デバイスに証明書を追加します。証明書によって署名されたデータは、ネットワークを介してデータをやりとりしている間に改竄されないように保護されます。証明書を使用したデータ暗号化は、データのセキュリティレベルを高めます。証明書は、ユーザー識別の検証にも使用されます。

Kaspersky Device Management for iOS は、次の証明書の企画をサポートしています：

- **PKCS#1** - RSA アルゴリズムに基づく公開鍵による暗号化。
- **PKCS#12** - 証明書および秘密鍵の格納と送信。

iOS MDM デバイスにセキュリティ証明書を追加するには：

1. コンソールツリーの［**管理対象デバイス**］フォルダーで、iOS MDM デバイスが属する管理グループを選択します。
2. 選択したグループの作業領域で、［**ポリシー**］タブを選択します。
3. ダブルクリックでポリシーのプロパティウィンドウを開きます。
4. ポリシーの**プロパティ**ウィンドウで、［**証明書**］セクションを選択します。
5. ［**証明書**］セクションで、［**追加**］をクリックします。
   ［**証明書**］ウィンドウが表示されます。
6. ［**ファイル名**］に、証明書ファイルのパスを指定します：

PKCS#1 証明書ファイルの拡張子は、CER、CRT、DER のいずれかです。PKCS#12 証明書ファイルの拡張子は、P12 または PFX のどちらかです。

7. ［**開く**］をクリックします。

   証明書がパスワードで保護されている場合は、パスワードを指定します。新しい証明書がリストに表示されます。

8. ［**適用**］をクリックして、変更を保存します。

これにより、ポリシーが適用された後、ユーザーは作成したリストから証明書をインストールするように要求されます。

iOS MDM デバイスへの SCEP プロファイルの追加

iOS MDM デバイスユーザーがインターネット経由で証明書センターから証明書を自動的に受け取れるようにするには、SCEP プロファイルを追加する必要があります。SCEP プロファイルによって Simple Certificate Enrollment Protocol（SCEP）のサポートが有効になります。

既定では、以下のように設定された SCEP プロファイルが追加されます：

- 証明書の登録に、サブジェクトの別名は使用しない。
- SCEP サーバーへのポーリングは、10 秒間隔で 3 回試行する。証明書に署名するすべての試行が失敗した場合、署名を要求する新しい証明書を生成する必要があります。
- 受け取った証明書を、データの署名または暗号化に使用することはできない。

SCEP プロファイルを追加する時に、特定の設定を編集できます。

SCEP プロファイルを追加するには：

1. コンソールツリーの［**管理対象デバイス**］フォルダーで、iOS MDM デバイスが属する管理グループを選択します。
2. 選択したグループの作業領域で、［**ポリシー**］タブを選択します。
3. ダブルクリックでポリシーのプロパティウィンドウを開きます。
4. ポリシーの**プロパティ**ウィンドウで、［**SCEP**］セクションを選択します。
5. ［**SCEP プロファイル**］セクションで、［**追加**］をクリックします。
   ［**SCEP プロファイル**］ウィンドウが表示されます。
6. ［**サーバーの Web アドレス**］に、証明書センターが導入されている SCEP サーバーの URL を入力します。
   URL には IP アドレスまたは完全ドメイン名（FQDN）を含めることができます。例：
   http://10.10.10.10/certserver/companyscep
7. ［**名前**］に、SCEP サーバーに導入されている証明書センターの名前を入力します。
8. ［**サブジェクト**］に、X.500 証明書に登録されている iOS MDM デバイスユーザーの属性を入力します。
   属性には、国（C）、組織（O）、共通名（CN）の詳細を定義できます。
   例：/C=RU/O=MyCompany/CN=User/RFC 5280 に指定されたその他の属性も使用できます。
9. ［**サブジェクトの別名の種別**］ドロップダウンリストで、SCEP サーバーのサブジェクトの別名の種別を選択します：
   - **なし** - 別名による識別は使用しません。

- **RFC 822 名** - メールアドレスを使用した識別。メールアドレスは RFC 822 に従って指定する必要があります。
- **DNS 名** - ドメイン名を使用した識別。
- **URI** - IP アドレスまたは FQDN 形式のアドレスを使用した識別。

サブジェクトの別名は、iOS MDM モバイルデバイスのユーザーを識別するために使用できます。

10. ［**サブジェクトの別名**］に X.500 証明書の別名を入力します。サブジェクトの別名の値は、サブジェクトの種別（ユーザーのメールアドレス、ドメインまたは Web アドレス）によって異なります。
11. ［**NT サブジェクト名**］に、Windows NT ネットワーク上の iOS MDM モバイルデバイスユーザーの DNS 名を入力します。

    NT サブジェクト名は、SCEP サーバーに送信される証明書要求に含められます。
12. ［**SCEP サーバーのポーリング試行回数**］に、証明書の署名を取得するために行う SCEP サーバーのポーリングの最大試行回数を指定します。
13. ［**試行頻度（秒）**］に、証明書の署名を取得するために行う SCEP サーバーのポーリングの試行間隔を秒単位で指定します。
14. ［**登録要求**］に、事前に公開されている登録鍵を入力します。

    証明書に署名する前に、SCEP サーバーはモバイルデバイスユーザーに暗号鍵の提供を要求します。このフィールドが空の場合、SCEP は暗号鍵を要求しません。
15. ［**暗号鍵のサイズ**］ドロップダウンリストで、1024 ビットまたは 2048 ビットを登録鍵のサイズとして選択します。
16. SCEP サーバーから受け取った証明書を、ユーザーが署名する証明書として使用することを許可する場合は、［**署名に使用**］をオンにします。
17. SCEP サーバーから受け取った証明書を、ユーザーがデータの暗号化に使用することを許可する場合は、［**暗号化に使用**］をオンにします。

    SCEP サーバー証明書を、データ署名証明書とデータ暗号化証明書の両方に同時に使用することは禁止されています。
18. ［**証明書のフィンガープリント**］に、証明書センターからの応答を検証するための一意の証明書のフィンガープリントを入力します。SHA-1 または MD5 ハッシュアルゴリズムによる証明書のフィンガープリントを使用できます。証明書のフィンガープリントを手動でコピーすること、または［**証明書から作成**］で証明書を選択することができます。［**証明書から作成**］でフィンガープリントを作成した場合、フィンガープリントはフィールドに自動的に追加されます。

    証明書のフィンガープリントは、モバイルデバイスと証明書センターとの間のデータ交換が HTTP プロトコル経由で行われる場合は必ず指定する必要があります。
19. ［**OK**］をクリックします。

    新しい SCEP プロファイルがリストに表示されます。
20. ［**適用**］をクリックして、変更を保存します。

これにより、ポリシーの適用後、ユーザーのモバイルデバイスはインターネット経由で証明書センターから証明書を自動的に受け取るように設定されます。

制御

このセクションでは、Kaspersky Security Center の管理コンソールでモバイルデバイスを遠隔監視する方法について説明します。

制限の設定

このセクションでは、モバイルデバイスの機能へのユーザーアクセスを設定する方法について説明します。

Android 10 以降のデバイスに関する特別な注意事項

Android 10 には、API 29 以降を対象とした多くの変更点および制限があります。これらの変更の一部は、本アプリの一部の機能や仕様の可用性にも影響します。この注意事項は、Android 10 以降のデバイスのみを対象としています。

Wi-Fi の有効化、無効化、設定変更

- Wi-Fi ネットワークの追加、削除、設定変更は、Kaspersky Security Center 管理コンソールで実行できます。Wi-Fi ネットワークをポリシーに追加すると、Kaspersky Security Center への初回接続時に、本アプリはネットワーク設定情報を受信します。

- Kaspersky Security Center を使用して設定されたネットワークをデバイスが検出すると、本製品はユーザーにそのネットワークへの接続を促します。ユーザーがそのネットワークへの接続を選択すると、Kaspersky Security Center を使用して指定された設定情報が自動的に適用されます。その後、そのネットワークが使用可能な範囲では、自動的にそのネットワークにデバイスが自動的に接続するようになります。ユーザーへの通知は以降は表示されません。

- ユーザーのデバイスが別の Wi-Fi ネットワークへ接続済みである場合、ネットワークを追加する通知が表示されない場合があります。この場合、ユーザーは手動で Wi-Fi を一度オフにし再度オンにしてから、ネットワークの提案を再受信する必要があります。

- Kaspersky Endpoint Security が Wi-Fi ネットワークへの接続を提案し、ユーザーがそれを拒否した場合、Wi-Fi のステータスを変更する本アプリの権限が取り消されます。これにより、本製品から Wi-Fi ネットワークへの接続が提案されなくなります。接続を提案できるようにするには、［**設定 → アプリと通知 → 特別なアプリアクセス → Wi-Fi の管理 → Kaspersky Endpoint Security**］の順に手動で選択して権限を許可する必要があります。

- オープンネットワークか、WPA2-PSK で暗号化されたネットワークのみがサポートされます。WEP / WPA 暗号化はサポートされません。

- 本アプリが以前に推奨したネットワークのパスワードが変更された場合は、既知のネットワークからそのネットワークをユーザーが手動で削除する必要があります。これにより、デバイスがネットワークの提案を本アプリから受信し、接続できるようになります。

- デバイスの OS が Android 9 以前から Android 10 以降にアップデートされるか、Android 10 以降のデバイスにインストールされた本製品がアップデートされるか、あるいはその両方の場合、Kaspersky Security Center を使用して以前に追加されたネットワークは、Kaspersky Security Center ポリシーを使用して変更

および削除できません。デバイスの設定で、これらの設定をユーザーが手動で変更および削除することは可能です。

- Android 10 以降のデバイスでは、提案されたネットワークが保護されている場合、ユーザーが手動で接続試行するとパスワードの入力が要求されます。自動的に接続する場合は、パスワード入力は不要です。ユーザーのデバイスが別の Wi-Fi ネットワークに接続されている場合、提案されたネットワークへ接続するには、まず接続中のネットワークとの接続を切断する必要があります。

- Android 11 のデバイスでは、本アプリが提案する保護されたネットワークへ、パスワード入力なしで手動で接続することができます。

- 本アプリをデバイスから削除すると、本アプリが提案したネットワークは無視されます。

- Wi-Fi ネットワークの使用の禁止はサポートされません。

カメラへのアクセス

- Android 10 のデバイスの場合、カメラの使用を完全には禁止できません。仕事用プロファイルでのカメラの使用の禁止は可能です。

- サードパーティ製アプリがデバイスカメラへのアクセスを試行すると、そのアプリがブロックされ、そのことがユーザーに通知されます。ただし、バックグラウンドモードで実行されているアプリによるカメラの使用はブロックできません。

- 外部カメラがデバイスから切断されると、カメラが使用不可能であるという通知が表示される場合があります。

画面ロックの解除方法の管理

- パスワードの強度要件（中程度または高強度）を、システムの値として実装しました。

  - 1～4 文字のパスワード長が必要な場合、中程度の強度のパスワードを設定するようユーザーに要求します。重複したり順番（例：1234）に並んでいたりしない数字（PIN）か、英字と数字の組み合わせである必要があります。PIN またはパスワードは、4 文字以上である必要があります。

  - 5 文字以上のパスワード長が必要な場合、高強度のパスワードを設定するようユーザーに要求します。重複したり順番に並んでいたりしない数字（PIN）か、英字と数字の組み合わせ（パスワード）である必要があります。PIN は 8 文字以上の数字で、パスワードは 6 文字以上である必要があります。

- 指紋での画面ロック解除は、仕事用プロファイルでのみ管理可能です。

Android デバイスの制限設定

Android デバイスを安全に保つために、デバイスでの Wi-Fi、カメラ、Bluetooth の使用を設定します。

既定では、デバイスでの Wi-Fi、カメラ、Bluetooth の使用に制限はありません。

デバイスでの Wi-Fi、カメラ、Bluetooth の使用制限を設定するには：

1. コンソールツリーの［**管理対象デバイス**］フォルダーで、デバイスが属する管理グループを選択します。

2. 選択したグループの作業領域で、［**ポリシー**］タブを選択します。

3. 任意の列をダブルクリックして、ポリシーのプロパティウィンドウを開きます。

4. ポリシーの**プロパティ**ウィンドウで、［**デバイス管理**］セクションを選択します。

5. ［**制限**］セクションで、Wi-Fi、カメラ、Bluetooth の使用に関する設定を行います：

   - ユーザーのモバイルデバイスの Wi-Fi モジュールを無効にするには、［**Wi-Fi の使用を禁止する**］をオンにします。

     Android 10.0 以降のデバイスでは、Wi-Fi ネットワークの使用の禁止はサポートされていません。

   - ユーザーのモバイルデバイスのカメラを無効にするには、［**カメラの使用を禁止する**］をオンにします。

     Android 10 以降のデバイスの場合、カメラの使用を完全には禁止できません。

     Android バージョン 11 以降のデバイスでは、Kaspersky Endpoint Security for Android をユーザー補助機能として設定しておく必要があります。初期設定ウィザードで Kaspersky Endpoint Security for Android をユーザー補助機能として設定するよう要求されます。このステップはスキップできます。また、後からデバイスの設定でサービスを無効にすることもできます。この場合、カメラの使用を制限することはできません。

   - ユーザーのモバイルデバイスの Bluetooth を無効にするには、［**Bluetooth の使用を禁止する**］をオンにします。

     Android 12 以降では、デバイスユーザーが［**付近の Bluetooth デバイス**］権限を付与している場合に限り、Bluetooth の使用を無効にできます。ユーザーは、初期設定ウィザードの実行中、または後からこの権限を付与できます。

6. ［**適用**］をクリックして、変更を保存します。

モバイルデバイスと Kaspersky Security Center との次回の同期時に、デバイスに設定が適用されます。

iOS MDM デバイス機能の制限の設定

企業のセキュリティ要件に準拠するために、iOS MDM デバイスの動作についての制限を設定します。

iOS MDM デバイスの機能制限を設定するには：

1. コンソールツリーの［**管理対象デバイス**］フォルダーで、iOS MDM デバイスが属する管理グループを選択します。

2. 選択したグループの作業領域で、［**ポリシー**］タブを選択します。

3. ダブルクリックでポリシーのプロパティウィンドウを開きます。

4. ポリシーの**プロパティ**ウィンドウで、［**機能の制限**］セクションを選択します。

5. ［**機能の制限設定**］セクションで、［**デバイスに設定を適用する**］をオンにします。

6. iOS MDM デバイスの機能制限を設定します。

7. ［**適用**］をクリックして、変更を保存します。

8. ［**アプリケーションの制限**］セクションを選択します。

9. ［**アプリケーションの制限設定**］セクションで、［**デバイスに設定を適用する**］をオンにします。

10. iOS MDM デバイスのアプリについての制限を設定します。

11. ［**適用**］をクリックして、変更を保存します。

12. ［**メディアコンテンツの制限**］セクションを選択します。

13. ［**メディアコンテンツの制限設定**］セクションで、［**デバイスに設定を適用する**］をオンにします。

14. iOS MDM デバイスのメディアコンテンツについての制限を設定します。

15. ［**適用**］をクリックして、変更を保存します。

これにより、ポリシーが適用された後、機能、アプリ、メディアコンテンツについての制限がモバイルデバイスに設定されます。

EAS デバイス機能の制限の設定

EAS デバイスを保護するために、デバイスの機能制限を設定します。

既定では、ユーザーは EAS デバイスの機能を制限なしで使用できます。

EAS デバイスの機能制限を設定するには：

1. コンソールツリーの［**管理対象デバイス**］フォルダーで、EAS デバイスが属する管理グループを選択します。

2. 選択したグループの作業領域で、［**ポリシー**］タブを選択します。

3. ダブルクリックでポリシーのプロパティウィンドウを開きます。

4. ポリシーのプロパティウィンドウで、［**機能の制限**］セクションを選択します。

5. ［**機能の制限設定**］セクションで、EAS デバイス機能の使用を許可またはブロックします：

   - メモリカードなどのリムーバブルドライブをデバイスへ接続できるようにするには、［**リムーバブルドライブを許可する**］をオンにします。
   - カメラの使用を許可するには、［**カメラの使用を許可する**］をオンにします。
   - Wi-Fi 接続を許可するには、［**Wi-Fi の使用を許可する**］をオンにします。
   - 赤外線接続ポートの使用を許可するには、［**赤外線接続を許可する**］をオンにします。
   - Wi-Fi アクセスポイントとしてデバイスを使用し、無線ネットワークを作成できるようにするには、［**デバイスの Wi-Fi アクセスポイントとしての使用を許可する**］をオンにします。

- デバイスからリモートデスクトップへの接続を許可するには、［**リモートデスクトップ接続を許可する**］をオンにします。
- デバイスでのデスクトップの ActiveSync クライアントを使用できるようにするには、［**デスクトップ同期を許可する**］をオンにします。
- ［**Bluetooth の使用**］ドロップダウンリストで、EAS デバイスでの Bluetooth の使用を許可またはブロックします：
  - **許可**：モバイルデバイスでの Bluetooth の使用を許可します。
  - **ハンズフリーの使用時**：無線ヘッドセットがモバイルデバイスに接続されている時に、Bluetooth の使用が許可されます。
  - **拒否**：モバイルデバイスでの Bluetooth の使用をブロックします。

6. ［**適用**］をクリックして、変更を保存します。

モバイルデバイスと Kaspersky Security Center との次回の同期時に、デバイスに設定が適用されます。

Web サイトへのユーザーアクセスの設定

このセクションでは、Android デバイスおよび iOS デバイスにおいて、Web サイトへのアクセスを設定する方法について説明します。

Android デバイスでの Web サイトへのアクセスの設定

Android デバイスユーザーの Web サイトへのアクセスを設定するには、危険サイトブロックを使用できます。危険サイトブロックは、Kaspersky Security Network クラウドサービスで定義されたカテゴリを使用して Web サイトをフィルタリングできます。フィルタリングにより、特定の Web サイトまたは Web サイトの特定のカテゴリ（「ギャンブル、宝くじ、懸賞」や「インターネットコミュニケーション」など）へのユーザーアクセスを制限できます。また、危険サイトブロックは、インターネット上でユーザーの個人情報を保護します。

Kaspersky Endpoint Security for Android をユーザー補助機能に設定しておく必要があります。初期設定ウィザードで Kaspersky Endpoint Security for Android をユーザー補助機能として設定するよう要求されます。このステップはスキップできます。また、後からデバイスの設定でサービスを無効にすることもできます。その場合、危険サイトブロックは実行しません。

危険サイトブロックは、Google Chrome（カスタムタブ機能を含む）、Huawei Browser、Samsung Internet Browser でのみ動作します。仕事用プロファイルを使用しており、危険サイトブロックが仕事用プロファイルでのみ有効となるよう設定されている場合は、Samsung Internet Browser 用の危険サイトブロックはモバイルデバイス上でサイトをブロックしません。

危険サイトブロックは既定で有効になっており、**フィッシング**および**マルウェア**のカテゴリに属する Web サイトへのアクセスがブロックされます。

デバイスユーザーの Web サイトへのアクセスを設定するには：

1. コンソールツリーの［**管理対象デバイス**］フォルダーで、デバイスが属する管理グループを選択します。

2. 選択したグループの作業領域で、［**ポリシー**］タブを選択します。

3. 任意の列をダブルクリックして、ポリシーのプロパティウィンドウを開きます。

4. ポリシーの**プロパティ**ウィンドウで、［**危険サイトブロック**］セクションを選択します。

5. ［**危険サイトブロックを有効にする**］をオンにします。

6. 危険サイトブロックを使用するには、危険サイトブロックの使用を目的としたデータ処理に関する声明（「危険サイトブロックに関する声明」）への管理者または端末のユーザーによる同意が必要です。

   a. ［**危険サイトブロックに関する声明**］をクリックします。

   ［**危険サイトブロックの使用を目的としたデータ処理に関する声明**］ウィンドウが開きます。危険サイトブロックに関する声明に同意するには、プライバシーポリシーを読んで同意する必要があります。

   b. ［プライバシーポリシー］をクリックします。プライバシーポリシーを読んで同意します。

   この方法でプライバシーポリシーに同意しない場合、モバイルデバイスのユーザーは初期設定ウィザードの途中か、または本アプリの設定で同意できます（☰ → ［**製品情報**］→［**契約書、ポリシー、声明**］→［**プライバシーポリシー**］）。

   c. 危険サイトブロックに関する声明への同意方法を選択します：

   - **危険サイトブロックに関する声明を確認し、同意する**
   - **危険サイトブロックに関する声明への同意を端末のユーザーに要求する**
   - **危険サイトブロックに関する声明に同意しない**

［**危険サイトブロックに関する声明に同意しない**］を選択すると、危険サイトブロックはサイトをブロックしなくなります。また、モバイルデバイスユーザーが危険サイトブロックを有効にすることもできません。

7. Web サイトのコンテンツに応じて、ユーザーのアクセスを制限するように設定するには、次の操作を行います：

   a. ［**危険サイトブロック**］セクションで、［**選択したカテゴリの Web サイトをブロックする**］を選択します。

   b. アクセスをブロックする Web サイトのカテゴリの横にあるチェックボックスをオンにして、ブロック対象カテゴリのリストを作成します。

8. 管理者が指定した Web サイトのみへのアクセスを許可する場合は、次の操作を行います：

   a. ［**危険サイトブロック**］セクションで、［**リストの Web サイトのみを許可する**］を選択します。

   b. アクセスをブロックしない Web サイトのアドレスを追加して、Web サイトのリストを作成します。Kaspersky Endpoint Security for Android は正規表現のみをサポートします。アクセスを許可する Web サイトのアドレスを入力する時は、次のルールを使用してください：

   - `http:\/\/www\.example\.com.*` – 指定した Web サイトのすべての子ページを許可する（例：`http://www.example.com/about`）。
   - `https:\/\/.*example\.com` – 指定した Web サイトのすべてのサブドメインページを許可する（例：`https://pictures.example.com`）。

HTTP プロトコルと HTTPS プロトコルを選択するために、`https?` という表現も使用できます。正規表現の詳細については、Oracle のテクニカルサポートサイトを参照してください。

9. すべての Web サイトへのアクセスをブロックする場合は、［**危険サイトブロック**］セクションで［**すべての Web サイトをブロックする**］を選択します。

10. Web サイトへのアクセスについてコンテンツに基づく制限をなくすには、［**危険サイトブロックを有効にする**］をオフにします。

11. ［**適用**］をクリックして、変更を保存します。

モバイルデバイスと Kaspersky Security Center との次回の同期時に、デバイスに設定が適用されます。

iOS MDM デバイスでの Web サイトへのアクセスの設定

危険サイトブロックの設定を指定し、iOS MDM デバイスユーザーによる Web　サイトへのアクセスを管理します。危険サイトブロックでは、許可する Web サイトとブロックする Web サイトのリストに基づいて、ユーザーによる Web サイトへのアクセスを管理します。また、Safari のブックマークに Web サイトのブックマークを追加できます。

既定では、Web サイトへのアクセスは制限されません。

危険サイトブロックは、監視対象のデバイスにのみ設定できます。

iOS MDM デバイスで Web サイトへのアクセスを設定するには：

1. コンソールツリーの［**管理対象デバイス**］フォルダーで、iOS MDM デバイスが属する管理グループを選択します。

2. 選択したグループの作業領域で、［**ポリシー**］タブを選択します。

3. ダブルクリックでポリシーのプロパティウィンドウを開きます。

4. ポリシーの**プロパティ**ウィンドウで、［**危険サイトブロック**］セクションを選択します。

5. ［**危険サイトブロックの設定**］セクションで、［**デバイスに設定を適用する**］をオンにします。

6. ブロックする Web サイトへのアクセスをブロックし、許可する Web サイトへのアクセスを許可するには：

   a. ［**Web フィルターモード**］ドロップダウンリストで、［**アダルトコンテンツを制限する**］を選択します。

   b. ［**許可する Web サイト**］セクションで、許可する Web サイトのリストを作成します。

   Web サイトのアドレスは「`http://`」または「`https://`」で始めます。Kaspersky Device Management for iOS はそのドメイン内のすべての Web サイトへのアクセスを許可します。たとえば、http://www.example.com を許可する Web サイトのリストに追加した場合、http://pictures.example.com および http://example.com/movies へのアクセスが許可されます。許可する Web サイトのリストが空の場合、ブロックする Web サイトのリストに含まれる Web サイト以外のすべての Web サイトへのアクセスを許可します。

   c. ［**ブロック対象の Web サイト**］セクションで、ブロックする Web サイトのリストを作成します。

   Web サイトのアドレスは「`http://`」または「`https://`」で始めます。Kaspersky Device Management for iOS がそのドメイン内のすべての Web サイトへのアクセスをブロックします。

7. タブリストにある許可する Web サイトを除くすべての Web サイトへのアクセスをブロックするには：

   a. ［**Web フィルターモード**］ドロップダウンリストで、［**ブックマークされている Web サイトのみ許可する**］を選択します。

   b. ［**ブックマーク**］セクションで、許可する Web サイトのブックマークのリストを作成します。

      Web サイトのアドレスは「`http://`」または「`https://`」で始めます。Kaspersky Device Management for iOS はそのドメイン内のすべての Web サイトへのアクセスを許可します。ブックマークリストが空の場合、すべての Web サイトへのアクセスを許可します。Kaspersky Device Management for iOS は、モバイルデバイスの Safari のブックマークタブのブックマークのリストから Web サイトを追加します。

8. ［**適用**］をクリックして、変更を保存します。

これにより、ポリシーが適用された後、選択されたモードと作成されたリストに基づいて、モバイルデバイス上で危険サイトブロックが設定されます。

企業のセキュリティ要件に沿った Android デバイスのコンプライアンスコントロール

Android デバイスを企業のセキュリティ要件に準拠するように管理できます。企業のセキュリティ要件には、ユーザーがデバイスをどのように使用できるかが規定されています。たとえば、デバイスで必ずリアルタイム保護を有効にすること、定義データベースを必ずアップデートすること、デバイスのパスワードが十分な強度であることなどです。コンプライアンスコントロールは、ルールのリストに基づきます。コンプライアンスルールには、次の項目が含まれます：

- デバイスチェック基準（例：デバイスでブロックされたアプリがない）。
- ルール違反を修正するまでユーザーに与えられる期間（例：24 時間）。
- 設定された期間内にルール違反を修正しない場合にデバイスで実行される処理（例：デバイスのロック）。

> Android 12 以降のデバイスでは、バッテリー節約モードの場合、タスクの実行が指定よりも遅れる場合があります。

ユーザーが指定された期間内にルール違反を修正しない場合、次の処理が実行可能です：

- **システムアプリ以外のすべてのアプリをブロックする**：ユーザーのモバイルデバイス上の、システムアプリ以外のすべてのアプリの起動がブロックされます。
- **デバイスのロック**：モバイルデバイスがロックされます。データにアクセスするには、デバイスのロックを解除する必要があります。デバイスのロックを解除した後、デバイスロックの理由が解決していない場合、指定した時間の経過後にデバイスは再度ロックされます。
- **企業データを消去する**：コンテナーデータ、会社のメールアカウント、会社の Wi-Fi ネットワークと VPN への接続設定、アクセスポイント名（APN）、Android 仕事用プロファイル、KNOX のコンテナー、KNOX License Manager ライセンスを消去します。
- **完全リセット**：すべてのデータがモバイルデバイスから削除され、設定が工場出荷時の値にロールバックされます。この処理が完了すると、デバイスは管理対象デバイスではなくなります。デバイスを Kaspersky Security Center に接続するには、Kaspersky Endpoint Security for Android を再インストールする必要があります。

デバイスがグループポリシーに準拠しているかチェックするためのスキャンルールを作成するには：

1. コンソールツリーの［**管理対象デバイス**］フォルダーで、デバイスが属する管理グループを選択します。
2. 選択したグループの作業領域で、［**ポリシー**］タブを選択します。
3. 任意の列をダブルクリックして、ポリシーのプロパティウィンドウを開きます。
4. ポリシーの**プロパティ**ウィンドウで、［**コンプライアンスコントロール**］セクションを選択します。
5. ポリシーに準拠していないデバイスに関する通知を受け取るには、［**コンプライアンス違反の通知**］セクションで［**管理者に通知する**］をオンにします。

   デバイスと管理サーバーの同期中に、モバイルデバイスにポリシー違反が検知された場合、Kaspersky Endpoint Security for Android は、**違反の検知と確認した基準の名前**をイベントログに記録します。イベントログは、管理サーバーのプロパティの［**イベント**］タブ、または製品のローカルのプロパティで確認できます。
6. モバイルデバイスがポリシーに準拠していないことをユーザーに通知するには、［**ユーザーに通知する**］セクションで［**ユーザーに通知する**］をオンにします。

   デバイスがポリシーに違反している場合、デバイスと管理サーバーを同期した時に、［**ステータス**］セクションでその旨を表示しユーザーに通知します。
7. ［**コンプライアンスルール**］セクションで、デバイスがポリシーに準拠しているかをチェックするルールのリストを編集します。次の手順に従ってください：

   a. ［**追加**］をクリックします。

      スキャンルールウィザードが起動します。

   b. スキャンルールウィザードの指示に従います。

      ウィザードが終了すると、新しいルールが［**コンプライアンスルール**］セクションのスキャンルールのリストに表示されます。
8. 作成したスキャンルールを一時的に無効にするには、選択したルールのトグルスイッチを使用します。
9. ［**適用**］をクリックして、変更を保存します。

モバイルデバイスと Kaspersky Security Center との次回の同期時に、デバイスに設定が適用されます。ユーザーのモバイルデバイスがポリシーに準拠していない場合、スキャンルールのリストで指定した制限がデバイスに適用されます。

アプリの起動管理

このセクションでは、モバイルデバイス上のアプリに対するユーザーアクセスを設定する方法について説明します。

Android デバイスでのアプリ起動管理

ユーザーのモバイルデバイスを安全に保つには、デバイスでのアプリの起動を設定する必要があります。

ブロックするアプリがインストールされているデバイス、または必須アプリがインストールされていないデバイスに対して、ユーザーの操作に制限をかけることができます（デバイスのロックなど）。制限はコンプライアンスコントロールコンポーネントを使用して設定できます。それには、スキャンルール設定で、［**ブロック対象アプリがインストールされています**］基準、［**ブロック対象カテゴリに該当するアプリがインストールされています**］基準、または［**一部の必須アプリがインストールされていません**］基準を選択する必要があります。

アプリ管理を正常に動作させるには、Kaspersky Endpoint Security for Android をユーザー補助機能として設定しておく必要があります。初期設定ウィザードで Kaspersky Endpoint Security for Android をユーザー補助機能として設定するよう要求されます。このステップはスキップできます。また、後からデバイスの設定でサービスを無効にすることもできます。その場合、アプリ管理は実行しません。

モバイルデバイスでのアプリの起動を設定するには：

1. コンソールツリーの［**管理対象デバイス**］フォルダーで、デバイスが属する管理グループを選択します。
2. 選択したグループの作業領域で、［**ポリシー**］タブを選択します。
3. 任意の列をダブルクリックして、ポリシーのプロパティウィンドウを開きます。
4. ポリシーの**プロパティ**ウィンドウで、［**アプリ管理**］セクションを選択します。
5. ［**操作モード**］セクションで、モバイルデバイスでアプリを起動するモードを選択します：
   - カテゴリとアプリのリストでブロックするアプリとして指定されているアプリを除くすべてのアプリを起動できるようにする場合は、［**ブロック対象アプリ**］モードを選択します。
   - カテゴリとアプリのリストで許可するアプリ、推奨するアプリ、または必須アプリとして指定されているアプリのみを起動できるようにする場合は、［**許可するアプリ**］モードを選択します。
6. Kaspersky Endpoint Security for Android がブロック対象アプリのデータをイベントログに記録し、ブロックはしないようにするには、［**禁止されたアプリをブロックせずイベントログへの記録のみ行う**］をオンにします。

   モバイルデバイスと管理サーバーが次に同期した時に、［**ブロック対象アプリがインストールされました**］とイベントログに記録されます。イベントログは、管理サーバーのプロパティの［**イベント**］タブ、または製品のローカルのプロパティで確認できます。
7. ［**許可するアプリ**］モードのモバイルデバイスでシステムアプリ（カレンダー、カメラ、設定など）の起動をブロックする場合は、［**システムアプリをブロックする**］をオンにします。

   システムアプリをブロックすると、デバイスの動作に支障が出ることがあるので、カスペルスキーではシステムアプリをブロックしないことを推奨しています。
8. カテゴリとアプリのリストを作成して、アプリの起動を設定します。

   アプリのカテゴリの詳細については、「付録」を参照してください。

   各カテゴリに属するアプリのリストについては、カスペルスキーの Web サイトを参照してください。
9. ［**適用**］をクリックして、変更を保存します。

モバイルデバイスと Kaspersky Security Center との次回の同期時に、デバイスに設定が適用されます。

アプリに対する EAS デバイス制限の設定

EAS デバイスを安全に保つために、アプリの動作の制限を設定します（ブラウザー、署名されていないアプリケーション）。

既定では、ユーザーは EAS デバイスのアプリを制限なしで使用できます。

EAS デバイスでのアプリの動作に関する制限を設定するには：

1. コンソールツリーの［**管理対象デバイス**］フォルダーで、EAS デバイスが属する管理グループを選択します。
2. 選択したグループの作業領域で、［**ポリシー**］タブを選択します。
3. ダブルクリックでポリシーのプロパティウィンドウを開きます。
4. ポリシーのプロパティウィンドウで、［**アプリケーションの制限**］セクションを選択します。
5. ［**アプリケーションの制限設定**］セクションで、アプリの動作に関する制限を設定します：
   - ブラウザーの使用を許可するには、［**ブラウザーの使用を許可する**］をオンにします。
   - 個人のメールアカウント（POP3 または IMAP4）を使用できるようにするには、［**個人のメールを許可する**］をオンにします。
   - 認証証明書によって署名されていないアプリを起動できるようにするには、［**署名されていないアプリを許可する**］をオンにします。
   - 認証証明書によって署名されていないアプリインストールできるようにするには、［**署名されていないインストールパッケージを許可する**］をオンにします。
6. ［**適用**］をクリックして、変更を保存します。

モバイルデバイスと Kaspersky Security Center との次回の同期時に、デバイスに設定が適用されます。

Android デバイスのソフトウェアインベントリ

Kaspersky Security Center に接続された Android デバイス上のアプリのインベントリを作成できます。Kaspersky Endpoint Security for Android はモバイルデバイスにインストールされているすべてのアプリに関する情報を受け取ります。インベントリ作成中に取得された情報は、デバイスプロパティの［**イベント**］セクションに表示されます。インストール済みの各アプリについて、バージョンや発行元などの詳細情報を確認できます。

ソフトウェアインベントリを有効にするには：

1. コンソールツリーの［**管理対象デバイス**］フォルダーで、デバイスが属する管理グループを選択します。
2. 選択したグループの作業領域で、［**ポリシー**］タブを選択します。
3. 任意の列をダブルクリックして、ポリシーのプロパティウィンドウを開きます。
4. ポリシーの**プロパティ**ウィンドウで、［**アプリ管理**］セクションを選択します。
5. ［**インストールされているアプリのデータを送信する**］をオンにします。
6. ［**適用**］をクリックして、変更を保存します。

モバイルデバイスと Kaspersky Security Center との次回の同期時に、デバイスに設定が適用されます。Kaspersky Endpoint Security for Android は、デバイスへのインストールやデバイスからのアンインストールが発生するたびに、イベントログにデータを送信します。

Kaspersky Security Center での Android デバイスの表示の設定

モバイルデバイスのリストでの操作を容易にするため、Kaspersky Security Center でのデバイスの表示方法を設定してください。既定では、モバイルデバイスのリストは、コンソールツリーの［**詳細**］→［**モバイルデバイス管理**］→［**モバイルデバイス**］に表示されます。デバイス情報は自動的に更新されます。右上隅の［**アップデート**］をクリックして、モバイルデバイスのリストを手動で更新することもできます。

デバイスを Kaspersky Security Center に接続すると、デバイスは自動的にモバイルデバイスのリストに追加されます。モバイルデバイスのリストには、そのデバイスに関する詳細な情報（モデル、オペレーティングシステム、IP アドレスなど）が含まれている場合があります。

デバイス名の形式の設定や、デバイスのステータスの選択ができます。デバイスのステータスは、Kaspersky Endpoint Security for Android のコンポーネントがユーザーのモバイルデバイスでどのように動作しているかについて情報を提供します。

Kaspersky Endpoint Security for Android のコンポーネントは、次の理由で動作していないことがあります：

- ユーザーがデバイスの設定でコンポーネントを無効にした。
- ユーザーがコンポーネントの動作に必要な権限をアプリに付与しなかった（たとえば、盗難対策コマンドに必要な、デバイス位置の特定権限がない）。

デバイスのステータスを表示するには、管理グループのプロパティで［**製品によって定義済み**］条件を有効にする必要があります（［**プロパティ**］→［**デバイスのステータス**］→［**ステータスを「緊急」にする条件**］および［**ステータスを「警告」にする条件**］）。管理グループのプロパティでは、モバイルデバイスの状態を形成する他の基準も選択できます。

Kaspersky Security Center での Android デバイスの表示を設定するには：

1. コンソールツリーの［**管理対象デバイス**］フォルダーで、デバイスが属する管理グループを選択します。
2. 選択したグループの作業領域で、［**ポリシー**］タブを選択します。
3. 任意の列をダブルクリックして、ポリシーのプロパティウィンドウを開きます。
4. ポリシーの**プロパティ**ウィンドウで、［**デバイスの情報**］セクションを選択します。
5. ［**Kaspersky Security Center でのデバイスの名前**］セクションで、管理コンソールで表示するモバイルデバイスの名前形式を選択します：
   - デバイスのモデル［メール、デバイス ID］
   - デバイスのモデル［メール（ある場合）またはデバイス ID］

   デバイス ID は、Kaspersky Endpoint Security がデバイスから受け取ったデータから生成する一意の ID です。Android 10 以降のモバイルデバイスでは、SSAID（Android ID）または別のデータのチェックサムをデバイスから受け取って使用します。それ以前の Android バージョンでは、IMEI を使用します。
6. 「ロック」アイコンをロック状態（🔒）に設定します。

7. ［**Kaspersky Security Center のデバイスの状態**］セクションで、Kaspersky Endpoint Security for Android のコンポーネントが動作していない場合の適切なデバイスの状態を選択します：（**緊急**）、（**警告**）、または（**OK**） から選択できます。

   モバイルデバイスのリストで、デバイスステータスは選択したステータスに従って変更されます。

8. 「ロック」アイコンをロック状態に設定します。

9. ［**適用**］をクリックして、変更を保存します。

モバイルデバイスと Kaspersky Security Center との次回の同期時に、デバイスに設定が適用されます。

管理

このセクションでは、Kaspersky Security Center の管理コンソールでモバイルデバイスの設定を遠隔管理する方法について説明します。

Wi-Fi ネットワークへの接続の設定

このセクションでは、Android デバイスおよび iOS MDM デバイスで企業の Wi-Fi ネットワークへの自動接続を設定する方法について説明します。

Android デバイスの Wi-Fi ネットワークへの接続

モバイルデバイスを Wi-Fi ネットワークに接続するには：

1. コンソールツリーの［**管理対象デバイス**］フォルダーで、デバイスが属する管理グループを選択します。

2. 選択したグループの作業領域で、［**ポリシー**］タブを選択します。

3. 任意の列をダブルクリックして、ポリシーのプロパティウィンドウを開きます。

4. ポリシーの**プロパティ**ウィンドウで、［**Wi-Fi**］セクションを選択します。

5. ［**Wi-Fi ネットワーク**］セクションで、［**追加**］をクリックします。
   ［**Wi-Fi ネットワーク**］ウィンドウが開きます。

6. ［**サービスセット識別子（SSID）**］に、アクセスポイント（SSID）を含む Wi-Fi ネットワークの名前を入力します。

7. ［**ネットワークプロテクション**］セクションで、Wi-Fi ネットワークのセキュリティの種別（オープンネットワークまたは WEP や WPA/WPA2 PSK プロトコルで保護された安全なネットワーク）を選択します。

8. 前のステップで保護されたネットワークを選択した場合は、ネットワークにアクセスするためのパスワードを［**パスワード**］に設定します。

9. 必要に応じて、［**プロキシサーバーのアドレスとポート**］に、プロキシサーバーの IP アドレスまたは DNS 名、およびポート番号を入力します。

Android バージョン 8.0 以降のデバイスでは、Wi-Fi 用のプロキシサーバーの設定をポリシーで再定義できません。Wi-Fi 用のプロキシサーバーの設定を、モバイルデバイス上で手動で設定することは可能です。

Wi-Fi ネットワークへの接続にプロキシサーバーを使用している場合、ポリシーを使用してネットワークへの接続を設定できます。Android バージョン 8.0 以降のデバイスでは、プロキシサーバーの設定を手動で編集する必要があります。Android バージョン 8.0 以降のデバイスでは、ポリシーを使用して Wi-Fi ネットワーク接続を設定することができません。ネットワークアクセスのパスワードのみ設定できます。

Wi-Fi ネットワークへの接続にプロキシサーバーを使用していない場合、Wi-Fi ネットワーク接続を管理するポリシーの使用が制限されなくなります。

10. ［**次のアドレスにはプロキシを使用しない**］に、プロキシサーバーを使用しないでアクセス可能な URL のリストを作成します。

    たとえば、アドレスを「`example.com`」と入力します。この場合、プロキシサーバーは次のアドレスには使用されません：`pictures.example.com`、`example.com/movies` など。プロトコル部分（`http://` など）は省略できます。

Android バージョン 8.0 以降のデバイスでは、プロキシサーバーの URL による除外が機能しません。

11. ［**OK**］をクリックします。

    追加した Wi-Fi ネットワークが［**Wi-Fi ネットワーク**］のリストに表示されます。

ネットワークのリストにある Wi-Fi ネットワークを変更または削除する場合は、リストの上部にある［**編集**］または［**削除**］を使用してください。

12. ［**適用**］をクリックして、変更を保存します。

モバイルデバイスと Kaspersky Security Center との次回の同期時に、デバイスに設定が適用されます。モバイルデバイスにポリシーが適用されると、ユーザーは追加された Wi-Fi ネットワークに接続できるようになります。ネットワークの設定をユーザー側で指定する必要はありません。

Android 10.0 以降のデバイスでは、提案された Wi-Fi ネットワークへの接続をユーザーが拒否すると、本アプリが Wi-Fi のステータスを変更する権限が取り消されます。ユーザーは手動でこの権限を許可する必要があります。

iOS MDM デバイスの Wi-Fi ネットワークへの接続

iOS MDM デバイスが使用できる Wi-Fi ネットワークに自動的に接続し、接続中のデータを保護できるようにするために、次の接続設定を行ってください。

iOS MDM デバイスの Wi-Fi ネットワークへの接続を設定するには：

1. コンソールツリーの［**管理対象デバイス**］フォルダーで、iOS MDM デバイスが属する管理グループを選択します。

2. 選択したグループの作業領域で、［**ポリシー**］タブを選択します。

3. ダブルクリックでポリシーのプロパティウィンドウを開きます。

4. ポリシーの**プロパティ**ウィンドウで、［**Wi-Fi**］セクションを選択します。

5. ［**Wi-Fi ネットワーク**］セクションで、［**追加**］をクリックします。
［**Wi-Fi ネットワーク**］ウィンドウが開きます。

6. ［**サービスセット識別子（SSID）**］に、アクセスポイント（SSID）を含む Wi-Fi ネットワークの名前を入力します。

7. iOS MDM デバイスを自動的に Wi-Fi ネットワークに接続させる場合は、［**自動接続**］をオンにします。

8. 事前認証を必要とする Wi-Fi ネットワーク（キャプティブネットワーク）に iOS MDM デバイスを接続できないようにするには、［**キャプティブネットワーク検出を無効にする**］をオンにします。
キャプティブネットワークを使用するには、登録し、使用条件に同意して、支払いを行う必要があります。キャプティブネットワークは、カフェやホテルなどに導入されていることがあります。

9. iOS MDM デバイスで使用できるネットワークのリストで Wi-Fi ネットワークを非表示にするには、［**非公開のネットワーク**］をオンにします。
この場合、ネットワークに接続するには、Wi-Fi ルーターに設定されているサービスセット識別子（SSID）を、ユーザーが手動で入力する必要があります。

10. ［**ネットワークプロテクション**］ドロップダウンリストで、Wi-Fi ネットワーク接続のプロテクションの種別を選択します：

- **無効**：ユーザー認証は必要ありません。
- **WEP**：ネットワークは WEP プロトコル（Wireless Encryption Protocol）を使用して保護されます。
- **WPA/WPA2（パーソナル）**：ネットワークは WPA / WPA2 プロトコル（Wi-Fi Protected Access）を使用して保護されます。
- **WPA2（パーソナル）**：ネットワークは WPA2 プロトコル（Wi-Fi Protected Access 2.0）を使用して保護されます。WPA2 による保護は、iOS バージョン 8 以降のモバイルデバイスで使用できます。WPA2 は Apple TV デバイスでは使用できません。
- **すべて（パーソナル）**：ネットワークは、Wi-Fi ルーターの種別に応じて WEP、WPA、または WPA2 暗号化プロトコルを使用して保護されます。各ユーザーに固有の暗号鍵が認証に使用されます。
- **WEP（動的）**：ネットワークは、動的鍵を使用した WEP プロトコルを使用して保護されます。
- **WPA/WPA2（エンタープライズ）**：ネットワークは、802.1X を使用した WPA/WPA2 暗号化プロトコルで保護されています。
- **WPA2 (エンタープライズ)**：ネットワークは、すべてのユーザーに共有される 1 つの暗号鍵（802.1X）を使用した WPA / WPA2 暗号化プロトコルを使用して保護されます。WPA2 による保護は、iOS バージョン 8 以降のモバイルデバイスで使用できます。WPA2 は Apple TV デバイスでは使用できません。
- **すべて（エンタープライズ）**：ネットワークは、Wi-Fi ルーターの種別に応じて WEP プロトコルまたは WPA / WPA2 プロトコルを使用して保護されます。すべてのユーザーにより共有される 1 つの暗号鍵が認証に使用されます。

［**ネットワークプロテクション**］リストで［**WEP（動的）**］、［**WPA/WPA2（エンタープライズ）**］、［**WPA2（エンタープライズ）**］、［**すべて（エンタープライズ）**］のいずれかを選択した場合、Wi-Fi ネットワークでユーザー認証を行うための EAP プロトコル（拡張認証プロトコル）の種別を［**プロトコル**］リストで選択します。

［**信頼済み証明書**］セクションで、信頼されたサーバー上で iOS MDM デバイスのユーザー認証を行うための信頼された証明書のリストを作成することもできます。

11. iOS MDM デバイスが Wi-Fi ネットワークに接続された時に、ユーザー認証を行うためのアカウントを設定します：

    a. ［**認証**］セクションで、［**設定**］をクリックします。
    ［**認証**］ウィンドウが表示されます。

    b. ［**ユーザー名**］に、Wi-Fi ネットワークへの接続時にユーザー認証を行うためのアカウント名を入力します。

    c. Wi-Fi ネットワークへの接続ごとに、手動でユーザーがパスワードを入力するように設定する場合は、［**接続時に毎回パスワードを要求する**］をオンにします。

    d. ［**パスワード**］に、Wi-Fi ネットワーク上で認証を行うためのアカウントのパスワードを入力します。

    e. ［**認証証明書**］ドロップダウンリストで、Wi-Fi ネットワーク上でユーザー認証を行うための証明書を選択します。リストに証明書がない場合、［証明書］セクションで**追加できます**。

    f. ［**ユーザー ID**］に、認証後のデータ送信中に、ユーザーの本名の代わりに表示するユーザー ID を入力します。
    ユーザー ID は認証プロセスをより安全にするように設計されています。ユーザー名が公開されることはなく、暗号化された TLS トンネル経由で送信されます。

    g. ［**OK**］をクリックします。

    これにより、Wi-Fi ネットワークへの接続時にユーザー認証を行うためのアカウント設定が、iOS MDM デバイスに適用されます。

12. 必要に応じて、プロキシサーバーを使用した Wi-Fi ネットワーク接続の設定を行います：

    a. ［**プロキシサーバー**］セクションで、［**設定**］をクリックします。

    b. ［**プロキシサーバー**］ウィンドウが開いたら、プロキシサーバーの設定モードを選択し、接続設定を指定します。

    c. ［**OK**］をクリックします。

    これにより、プロキシサーバーを使用した Wi-Fi ネットワークへの接続設定が、iOS MDM デバイスに適用されます。

13. ［**OK**］をクリックします。
    新しい Wi-Fi ネットワークがリストに表示されます。

14. ［**適用**］をクリックして、変更を保存します。

これにより、ポリシーが適用された後、Wi-Fi ネットワーク接続が iOS MDM デバイスに設定されます。ユーザーのモバイルデバイスは、使用できる Wi-Fi ネットワークに自動的に接続されます。Wi-Fi ネットワークへの接続中のデータのセキュリティは、認証技術によって確保されます。

メールの設定

このセクションでは、モバイルデバイスのメールボックスの設定について説明します。

iOS MDM デバイスでのメールボックスの設定

iOS MDM デバイスユーザーがメールを使用できるようにするには、ユーザーのメールアカウントを iOS MDM デバイスのアカウントのリストに追加します。

既定では、以下のように設定されたメールアカウントが追加されます：

- メールプロトコル - IMAP。
- ユーザーのアカウント間でメッセージを移動させ、アカウントのアドレスを同期させることができます。
- ユーザーは、「メール」以外のすべてのメールクライアントを使用して、メールを利用することができます。
- メッセージの送信中に SSL 接続は使用されません。

アカウントの追加時に、特定の設定を編集することができます。

iOS MDM デバイスユーザーのメールアカウントを追加するには：

1. コンソールツリーの［**管理対象デバイス**］フォルダーで、iOS MDM デバイスが属する管理グループを選択します。
2. 選択したグループの作業領域で、［**ポリシー**］タブを選択します。
3. ダブルクリックでポリシーのプロパティウィンドウを開きます。
4. ポリシーの**プロパティ**ウィンドウで、［**メール**］セクションを選択します。
5. ［**メールアカウント**］セクションで、［**追加**］をクリックします。
   ［**メールアカウント**］ウィンドウが表示されます。
6. ［**説明**］に、ユーザーのメールアカウントの詳細を入力します。
7. 次のどちらかのメールプロトコルを選択します：
   - POP
   - IMAP
8. 必要に応じて、［**IMAP パスの接頭辞**］に、IMAP パスの接頭辞を指定します。
   IMAP パスの接頭辞は、必ず大文字で入力する必要があります（たとえば、Google Mail の場合は GMAIL と入力します）。このフィールドは、IMAP アカウントプロトコルが選択されている場合に有効です。
9. ［**メッセージに表示されるユーザー名**］に、すべての発信メッセージの［**差出人**］に表示するユーザー名を入力します。
10. ［**メールアドレス**］に、iOS MDM デバイスユーザーのメールアドレスを指定します。
11. メールアカウントの詳細設定を行います：
    - ユーザーのアカウント間でメールメッセージを移動できるようにする場合は、［**アカウント間でメッセージの移動を許可する**］をオンにします。

- ユーザーアカウント間でメールアドレスを同期させる場合は、［**最近のアドレスの同期を許可する**］をオンにします。

- 大きなサイズの添付ファイルを送信するための Mail Drop サービスを使用できるようにするには、［**Mail Drop を許可する**］をオンにします。

- ユーザーが使用するメールクライアントを iOS 標準のメールクライアントのみにする場合は、［**メールアプリの使用のみを許可する**］をオンにします。

12. S/MIME プロトコルをメールアプリで使用するように設定します。*S/MIME* は、デジタル署名付きの暗号化されたメッセージを送信するためのプロトコルです。

    - S/MIME プロトコルを使用して送信メールに署名するには、［**署名メッセージ**］をオンにして、署名に使用する証明書を選択します。デジタル署名には、送信者の信頼性を確認し、受信者への送信の過程でメッセージが改竄されていないことを示します。メッセージの署名は、iOS バージョン 10.3 以降のデバイスで利用可能です。

    - S/MIME プロトコルを使用して送信メールを暗号化するには、［**既定でメッセージを暗号化する**］をオンにして、暗号化に使用する証明書（公開鍵）を選択します。メッセージの暗号化は、iOS バージョン 10.3 以降のモバイルデバイスで利用可能です。

    - ユーザーによる個別のメッセージの暗号化を可能にするには、［**暗号化のメッセージにトグルボタンを表示する**］をオンにします。暗号化されたメッセージを送信するには、メールアプリの［**宛先**］フィールドの🔒アイコンをクリックします。

13. ［**受信メールサーバー**］および［**送信メールサーバー**］セクションで、［**設定**］をクリックして、次の接続設定を行います：

    - **サーバーアドレスとポート**：インバウンドメールサーバーおよびアウトバウンドメールサーバーのホスト名または IP アドレスと、サーバーのポート番号。

    - **アカウント名**：インバウンドメールサーバーとアウトバウンドメールサーバーでの認証に必要なユーザーのアカウント名。

    - **認証の種別**：インバウンドメールサーバーおよびアウトバウンドメールサーバーで行うメールアカウントの認証の種別。

    - **パスワード**：インバウンドメールサーバーおよびアウトバウンドメールサーバーで認証を行うためのアカウントパスワード。選択された認証方法によって保護されます。

    - **送受信のメールサーバーに 1 つのパスワードを使用する**：送信メールサーバーと受信メールサーバーでのユーザー認証に 1 つのパスワードを使用します。

    - **SSL 接続を使用する**：暗号化および証明書ベースの認証を使用してデータ転送を保護するために、SSL（Secure Sockets Layer）データ転送プロトコルを使用します。

14. ［**OK**］をクリックします。

    新しいメールアカウントがリストに表示されます。

15. ［**適用**］をクリックして、変更を保存します。

これにより、ポリシーが適用された後、メールアカウントが編集したリストからユーザーのモバイルデバイスに追加されます。

iOS MDM デバイスでの Exchange メールボックスの設定

iOS MDM デバイスユーザーが、会社のメール、カレンダー、連絡先、メモ、タスクを使用できるようにするには、ユーザーの Exchange ActiveSync アカウントを Microsoft Exchange サーバーに追加します。

既定では、以下のように設定されたアカウントが Microsoft Exchange サーバーに追加されます：

- 週に 1 回、メールの同期が実行されます。
- ユーザーのアカウント間でメッセージを移動させ、アカウントアドレスを同期させることができます。
- ユーザーは、「メール」以外のすべてのメールクライアントを使用して、メールを利用することができます。
- メッセージの送信中に SSL 接続は使用されません。

Exchange ActiveSync アカウントを追加する時に、特定の設定を編集できます。

iOS MDM デバイスユーザーの Exchange ActiveSync アカウントを追加するには：

1. コンソールツリーの［**管理対象デバイス**］フォルダーで、iOS MDM デバイスが属する管理グループを選択します。
2. 選択したグループの作業領域で、［**ポリシー**］タブを選択します。
3. ダブルクリックでポリシーのプロパティウィンドウを開きます。
4. ポリシーの**プロパティ**ウィンドウで、［**Exchange ActiveSync**］セクションを選択します。
5. ［**Exchange ActiveSync アカウント**］セクションで、［**追加**］をクリックします。
   ［**Exchange ActiveSync アカウント**］ウィンドウが表示され、［**全般**］タブが開きます。
6. ［**アカウント名**］に、Microsoft Exchange サーバーで認証を行うためのアカウント名を入力します。［**使用できるマクロ**］ドロップダウンリストからマクロを使用できます。
7. ［**サーバーのアドレス**］に、Microsoft Exchange サーバーのネットワーク名または IP アドレスを入力します。
8. SSL（Secure Sockets Layer）データ転送プロトコルを使用し、データを保護して転送する場合は、［**SSL 接続を使用する**］をオンにします。
9. ［**ドメイン**］に、iOS MDM デバイスユーザーのドメイン名を入力します。［**使用できるマクロ**］ドロップダウンリストからマクロを使用できます。
10. ［**アカウントのユーザー名**］に、iOS MDM デバイスユーザーの名前を入力します。
    このフィールドに何も指定しないと、ポリシーを iOS MDM デバイスに適用する時に、ユーザー名を入力するように要求されます。［**使用できるマクロ**］ドロップダウンリストからマクロを使用できます。
11. ［**メールアドレス**］に、iOS MDM デバイスユーザーのメールアドレスを指定します。［**使用できるマクロ**］ドロップダウンリストからマクロを使用できます。
12. ［**パスワード**］に、Microsoft Exchange サーバーで認証を行うための Exchange ActiveSync アカウントのパスワードを入力します。
13. ［**詳細**］タブを選択し、Exchange ActiveSync アカウントの詳細設定を行います：
    - **メールを同期する日数 <期間>**

- **認証の種別**
- **アカウント間でメッセージの移動を許可する**
- **最近のアドレスの同期を許可する**
- **メールアプリの使用のみを許可する**

14. S/MIME プロトコルをメールアプリで使用するように設定します。*S/MIME* は、デジタル署名付きの暗号化されたメッセージを送信するためのプロトコルです。

    - S/MIME プロトコルを使用して送信メールに署名するには、［**署名メッセージ**］をオンにして、署名に使用する証明書を選択します。デジタル署名には、送信者の信頼性を確認し、受信者への送信の過程でメッセージが改竄されていないことを示します。メッセージの署名は、iOS バージョン 10.3 以降のデバイスで利用可能です。
    - S/MIME プロトコルを使用して送信メールを暗号化するには、［**既定でメッセージを暗号化する**］をオンにして、暗号化に使用する証明書（公開鍵）を選択します。メッセージの暗号化は、iOS バージョン 10.3 以降のモバイルデバイスで利用可能です。
    - ユーザーによる個別のメッセージの暗号化を可能にするには、［**暗号化のメッセージにトグルボタンを表示する**］をオンにします。暗号化されたメッセージを送信するには、メールアプリの［**宛先**］フィールドのアイコンをクリックします。

15. ［**OK**］をクリックします。

    新しい Exchange ActiveSync アカウントがリストに表示されます。

16. ［**適用**］をクリックして、変更を保存します。

これにより、ポリシーが適用された後、Exchange ActiveSync アカウントが編集したリストからユーザーのモバイルデバイスに追加されます。

Android デバイスでの Exchange メールボックスの設定（Samsung のみ）

モバイルデバイスで企業のメール、連絡先、カレンダーを使用するには、Exchange メールボックスを設定する必要があります。

Exchange メールボックスの設定は、Samsung デバイスでのみ編集可能です。

モバイルデバイスで Exchange メールボックスを設定するには：

1. コンソールツリーの［**管理対象デバイス**］フォルダーで、デバイスが属する管理グループを選択します。
2. 選択したグループの作業領域で、［**ポリシー**］タブを選択します。
3. 任意の列をダブルクリックして、ポリシーのプロパティウィンドウを開きます。
4. ポリシーの**プロパティ**ウィンドウで、［**Samsung KNOX の管理**］→［**Samsung デバイスの管理**］セクションを順に選択します。
5. ［**Exchange ActiveSync**］ウィンドウで、［**設定**］をクリックします。

   ［**Exchange メールサーバーの設定**］ウィンドウが表示されます。

6. ［**サーバーのアドレス**］に、メールサーバーをホスティングしているサーバーの IP アドレスまたは DNS 名を入力します。

7. ［**ドメイン**］に、会社のネットワークでのモバイルデバイスユーザーのドメイン名を入力します。

8. ［**同期間隔**］ドロップダウンリストで、モバイルデバイスと Microsoft Exchange サーバーとの同期の間隔を選択します。

9. SSL（Secure Sockets Layer）データ転送プロトコルを使用する場合は、［**SSL 接続を使用する**］をオンにします。

10. モバイルデバイスと Microsoft Exchange サーバー間でのデータ転送を保護するためにデジタル証明書を使用する場合は、［**サーバー証明書を確認する**］をオンにします。

11. ［**適用**］をクリックして、変更を保存します。

モバイルデバイスと Kaspersky Security Center との次回の同期時に、デバイスに設定が適用されます。

サードパーティのモバイルアプリの管理

コンテナーを使用して、ユーザーのデバイスで起動したモバイルアプリの動作を監視できます。*コンテナー*は、モバイルアプリ用の特別な入れ物で、コンテナーに入れられたアプリ（コンテナーアプリ）の動作を制御することができるため、デバイス上の個人情報や会社のデータを保護できます。

Kaspersky Security for Android Service Pack 3 Maintenance Release 2 では、コンテナーの作成をサポートしません。旧バージョンの製品で作成したコンテナーを Android デバイスに追加することは可能です。

次のいずれかの方法でユーザーのデバイスにコンテナーアプリをインストールします：

- コンテナーアプリのインストールパッケージへのリンクをメールでユーザーに送信します。
- ポリシーのプロパティウィンドウの［**アプリ管理**］セクションで、コンテナーアプリを必須アプリまたは許可するアプリとして指定します。モバイルデバイスが Kaspersky Security Center と同期されると、コンテナーにあるアプリ配布パッケージが自動的にユーザーのデバイスにコピーされます。

コンテナーアプリをインストールするには、ユーザーのモバイルデバイスで提供元不明のアプリのインストールを許可しておく必要があります。コンテナーアプリをインストールした後、デバイスとデータを保護するために、提供元不明のアプリのインストールを禁止しておいてください。Google Play ストアを経由せずにアプリをインストールする方法の詳細は、*Android ヘルプ*を参照してください。

Kaspersky Endpoint Security for Android の通知設定

Kaspersky Endpoint Security for Android の通知をモバイルデバイスに表示したくない場合は、特定の通知を無効にできます。

Kaspersky Endpoint Security は次のツールを使用して、端末の保護ステータスを表示します：

- **保護ステータスの通知**：この通知は通知バーにピン留めされています。保護ステータスの通知は削除できません。通知には、デバイスの保護ステータス（例：  ）と、問題がある場合は問題の数が表示されます。端末の保護ステータスをタップして、問題を一覧表示させることができます。
- **アプリの通知**：デバイスユーザーに本アプリの情報を通知します（例：脅威の検知）。

- **ポップアップメッセージ**：ポップアップメッセージは、端末のユーザーによる操作が必要な場合に表示されます（例：脅威の検知時に実行する処理）。

既定では、Kaspersky Endpoint Security for Android の通知はすべて有効になっています。

Android デバイスのユーザーは、通知バーの設定で、Kaspersky Endpoint Security for Android からの通知をすべて無効にできます。通知を無効にすると、本アプリの動作が監視されないので、重要な通知を見逃してしまう場合もあります（Kaspersky Security Center とデバイスの同期が失敗した場合の情報など）。この場合、動作の状態を確認するには、Kaspersky Endpoint Security for Android を開く必要があります。

Kaspersky Endpoint Security for Android の動作に関する通知の表示を設定するには：

1. コンソールツリーの［**管理対象デバイス**］フォルダーで、デバイスが属する管理グループを選択します。
2. 選択したグループの作業領域で、［**ポリシー**］タブを選択します。
3. 任意の列をダブルクリックして、ポリシーのプロパティウィンドウを開きます。
4. ポリシーの**プロパティ**ウィンドウで、［**詳細**］セクションを選択します。
5. ［**アプリの通知**］セクションで、［**設定**］をクリックします。
   ［**デバイスの通知設定**］ウィンドウが開きます。
6. ユーザーのモバイルデバイスで非表示にする Kaspersky Endpoint Security for Android の問題を選択し、［OK］をクリックします。
   保護ステータスの通知に表示する問題や、本アプリの**ステータス**セクションに表示される問題が表示されなくなります。保護ステータスに関する通知と、本アプリの通知は表示されます。

   表示が必須である一部の問題の通知は、無効にできません（ライセンスの有効期限切れに関する問題など）。

7. 通知とポップアップメッセージをすべて非表示にするには、［**本アプリをバックグラウンドで実行している時は通知やポップアップを無効にする**］**をオンにします。**
   保護ステータスに関する通知のみが表示されるようになります。通知には、端末の保護ステータス（例：）と、問題の数が表示されます。また、ユーザーが本アプリを操作している場合も、通知が表示されます（例：定義データベースを手動でアップデートするなど）。

   カスペルスキーでは、通知とポップアップメッセージの有効化を推奨しています。バックグラウンドモードで通知とポップアップメッセージを無効にすると、本アプリは脅威に関する警告をユーザーにリアルタイムで通知しなくなります。モバイルデバイスのユーザーがデバイスの保護ステータスを知るのは、本アプリを開いた時のみとなります。

8. ［**適用**］をクリックして、変更を保存します。

モバイルデバイスと Kaspersky Security Center との次回の同期時に、デバイスに設定が適用されます。無効にした Kaspersky Endpoint Security for Android の通知が、ユーザーのモバイルデバイスで表示されなくなります。

iOS MDM デバイスの AirPlay への接続

iOS MDM デバイスから AirPlay デバイスへのミュージック、写真、ビデオのストリーミングができるようにするために、AirPlay デバイスへの接続を設定します。AirPlay 技術を使用できるようにするには、モバイルデバイスと AirPlay デバイスを同じ無線ネットワークに接続する必要があります。AirPlay デバイスには、Apple TV（第 2 世代と第 3 世代）、AirMac Express、AirPlay をサポートするスピーカーやラジオなどがあります。

AirPlay デバイスへの自動接続が使用できるのは、管理対象のデバイスのみです。

iOS MDM デバイスの AirPlay デバイスへの接続を設定するには：

1. コンソールツリーの［**管理対象デバイス**］フォルダーで、iOS MDM デバイスが属する管理グループを選択します。
2. 選択したグループの作業領域で、［**ポリシー**］タブを選択します。
3. ダブルクリックでポリシーのプロパティウィンドウを開きます。
4. ポリシーの**プロパティ**ウィンドウで、［**AirPlay**］セクションを選択します。
5. ［**AirPlay デバイス**］セクションで、［**デバイスに設定を適用する**］をオンにします。
6. ［**パスワード**］セクションで、［**追加**］をクリックします。
   パスワードの表に空の行が追加されます。
7. ［**デバイス名**］列に、無線ネットワーク上の AirPlay デバイスの名前を入力します。
8. ［**パスワード**］列に、AirPlay デバイスのパスワードを入力します。
9. iOS MDM デバイスの AirPlay デバイスへのアクセスを制限するには、［**許可されるデバイス**］セクションで許可するデバイスのリストを作成します。この場合、AirPlay デバイスの MAC アドレスを許可するデバイスのリストに追加します。
   許可されるデバイスのリストにない AirPlay デバイスへのアクセスはブロックされます。許可するデバイスのリストに何も入力されていない場合は、Kaspersky Device Management for iOS はすべての AirPlay デバイスへのアクセスを許可します。
10. ［**適用**］をクリックして、変更を保存します。

これにより、ポリシーが適用された後、モバイルデバイスは自動的に AirPlay デバイスに接続され、メディアコンテンツをストリーム配信できるようになります。

iOS MDM デバイスの AirPrint への接続

AirPrint 技術を使用して無線で iOS MDM デバイスからドキュメントを印刷できるようにするには、AirPrint プリンターへの自動接続を設定します。モバイルデバイスとプリンターは同じ無線ネットワークに接続していなければなりません。AirPrint プリンターですべてのユーザーの共有アクセスを設定する必要があります。

iOS MDM デバイスの AirPrint プリンターへの接続を設定するには：

1. コンソールツリーの［**管理対象デバイス**］フォルダーで、iOS MDM デバイスが属する管理グループを選択します。
2. 選択したグループの作業領域で、［**ポリシー**］タブを選択します。
3. ダブルクリックでポリシーのプロパティウィンドウを開きます。

4. ポリシーの**プロパティ**ウィンドウで、［**AirPrint**］セクションを選択します。

5. ［**AirPrint プリンター**］セクションで、［**追加**］をクリックします。
［**プリンター**］ウィンドウが表示されます。

6. ［**IP アドレス**］に、AirPrint プリンターの IP アドレスを入力します。

7. ［**リソースパス**］に、AirPrint プリンターへのパスを入力します。
プリンターへのパスは、Bonjour プロトコルの rp（リソースパス）キーに対応します。例：

   - printers/Canon_MG5300_series
   - ipp/print
   - Epson_IPP_Printer

8. ［**OK**］をクリックします。
追加された AirPrint プリンターがリストに表示されます。

9. ［**適用**］をクリックして、変更を保存します。

これにより、ポリシーが適用された後、モバイルデバイスのユーザーは AirPrint プリンターでドキュメントを無線で印刷できるようになります。

アクセスポイント名（APN）の設定

モバイルデバイスをモバイルネットワークのデータ転送サービスに接続するには、APN（アクセスポイント名）を設定する必要があります。

Android デバイスでの APN の設定（Samsung のみ）

APN の設定は、Samsung デバイスでのみ編集可能です。

ユーザーのモバイルデバイスでアクセスポイントを使用するには、SIM カードが挿入されている必要があります。アクセスポイントの設定は、通信事業者により提供されます。アクセスポイントの設定が適切でないと、通信事業者により追加料金が請求される可能性があります。

アクセスポイント名（APN）を設定するには：

1. コンソールツリーの［**管理対象デバイス**］フォルダーで、デバイスが属する管理グループを選択します。

2. 選択したグループの作業領域で、［**ポリシー**］タブを選択します。

3. 任意の列をダブルクリックして、ポリシーのプロパティウィンドウを開きます。

4. ポリシーの**プロパティ**ウィンドウで、［**Samsung KNOX の管理**］→［**APN**］セクションを順に選択します。

5. ［**APN**］セクションで、［**設定**］をクリックします。
［**APN 設定**］ウィンドウが開きます。

6. ［**全般**］タブで、以下のアクセスポイント設定を指定します：

   a. ［**APN 種別**］ドロップダウンリストで、アクセスポイントの種別を選択します。

   b. **APN 名**のフィールドに、アクセスポイントの名前を指定します。

   c. ［**MCC**］に、モバイル国コード（MCC）を入力します。

   d. ［**MNC**］に、モバイルネットワークコード（MNC）を入力します。

   e. ［**MMS**］または［**インターネットと MMS**］をアクセスポイントの種別として選択した場合は、次の MMS 設定を指定します：

      - ［**MMS サーバー**］に、MMS のやりとりに使用するモバイル通信事業者の完全ドメイン名を指定します。

      - ［**MMS プロキシサーバー**］に、MMS のやりとりに使用するモバイル通信事業者のサーバーのプロキシサーバーのネットワーク名または IP アドレスとポート番号を指定します。

7. ［**詳細**］タブで、アクセスポイント名（APN）の詳細設定を行います：

   a. ［**認証の種別**］ドロップダウンリストで、ネットワークにアクセスするための、モバイル通信事業者のサーバーでのユーザーの認証の種別を選択します。

   b. ［**サーバーのアドレス**］に、データ送信サービスにアクセスするモバイル通信事業者のサーバーのネットワーク名を指定します。

   c. ［**プロキシサーバーのアドレス**］に、ネットワークにアクセスするための、モバイル通信事業者のプロキシサーバーのネットワーク名または IP アドレスとポート番号を指定します。

   d. **ユーザー名**のフィールドに、モバイルネットワーク上での認証に使用するユーザー名を入力します。

   e. **パスワード**のフィールドに、モバイルネットワーク上での認証に使用するパスワードを入力します。

8. ［**適用**］をクリックして、変更を保存します。

モバイルデバイスと Kaspersky Security Center との次回の同期時に、デバイスに設定が適用されます。

iOS MDM デバイスでの APN の設定

モバイルネットワーク上でのデータ送信サービスをユーザーの iOS MDM デバイスで有効にするには、アクセスポイント名（APN）を設定する必要があります。

［**APN**］セクションは使用されなくなりました。APN 設定を行うには、［**セルラー通信**］セクションを使用してください。セルラー通信設定を編集する前に、［**APN**］セクションの設定がデバイスに適用されていないこと（［**デバイスに設定を適用する**］がオフであること）を確認してください。［**APN**］セクションと［**セルラー通信**］セクションの設定を同時に使用することはできません。

iOS MDM デバイス上でアクセスポイントを設定するには：

1. コンソールツリーの［**管理対象デバイス**］フォルダーで、iOS MDM デバイスが属する管理グループを選択します。

2. 選択したグループの作業領域で、［**ポリシー**］タブを選択します。

3. ダブルクリックでポリシーのプロパティウィンドウを開きます。

4. ポリシーの**プロパティ**ウィンドウで、［**セルラー通信**］セクションを選択します。

5. ［**セルラー通信設定**］セクションで、［**デバイスに設定を適用する**］をオンにします。

6. ［**APN 種別**］リストで、GPRS / 3G / 4G モバイルネットワークでのデータ転送に使用するアクセスポイントの種別を選択します：

   - **組み込み APN** – 組み込み Apple SIM に対応するモバイルネットワークオペレーターを経由したデータ転送のためのセルラー通信設定の編集。組み込み Apple SIM に対応するデバイスの詳細については、Apple のテクニカルサポートサイトを参照してください。

   - **APN** – セルラー通信設定の設定情報。デバイスに挿入した SIM カードのモバイル通信事業者を経由したデータ通信の設定です。

   - **組み込み APN および APN** – セルラー通信設定の設定情報。デバイスに挿入した SIM カードや、組み込まれた Apple 製 SIM のモバイル通信事業者を経由したデータ通信の設定です。組み込み Apple SIM に対応するデバイスおよび SIM カードスロットの詳細については、Apple のテクニカルサポートサイトを参照してください。

7. **APN 名**のフィールドに、アクセスポイントの名前を指定します。

8. **認証の種別**のドロップダウンリストで、デバイスユーザーの認証の種別を選択します。この認証は、モバイル通信事業者のサーバーにログインし、ネットワークアクセス（インターネットまたは MMS）を可能にするために必要です。

9. **ユーザー名**のフィールドに、モバイルネットワーク上での認証に使用するユーザー名を入力します。

10. **パスワード**のフィールドに、モバイルネットワーク上での認証に使用するパスワードを入力します。

11. **プロキシサーバーのアドレスとポート**のフィールドに、プロキシサーバーのホスト名または IP アドレスと、プロキシサーバーのポート番号を入力します。

12. ［**適用**］をクリックして、変更を保存します。

これにより、ポリシーが適用された後、アクセスポイント名（APN）がモバイルデバイスに設定されます。

Android 仕事用プロファイルの設定

このセクションでは、Android 仕事用プロファイルの使用について説明します。

Android 仕事用プロファイルについて

Android Enterprise は企業のモバイルインフラストラクチャを管理するためのプラットフォームです。モバイルデバイスを使用できる職場環境を提供します。Android Enterprise の使用の詳細については、Google のサポートサイトを確認してください。

Android 仕事用プロファイル（以下、「仕事用プロファイル」とも表記）はユーザーのモバイルデバイスで作成できます。*Android 仕事用プロファイル*は、ユーザーのデバイスにある安全な環境で、管理者は、ユーザーによる自身のデータの使用を制限することなくアプリやユーザーアカウントを管理できます。ユーザーのモバイルデバイスに仕事用プロファイルが作成されると、次の企業向けアプリが自動的にインストールされます：Google Play Market、Google Chrome、Downloads、Kaspersky Endpoint Security for Android など。仕事用プロファイルにインストールされた企業用アプリとそれらのアプリの通知は、赤いブリーフケースのアイコンで表示されます。Google Play アプリを使用するには、Google の企業アカウントを別途作成する必要があります。仕事用プロファイルにインストールされたアプリは、アプリの共通リストに表示されます。

仕事用プロファイルの設定

Android 仕事用プロファイルを設定するには：

1. コンソールツリーの［**管理対象デバイス**］フォルダーで、デバイスが属する管理グループを選択します。
2. 選択したグループの作業領域で、［**ポリシー**］タブを選択します。
3. 任意の列をダブルクリックして、ポリシーのプロパティウィンドウを開きます。
4. ポリシーの**プロパティ**ウィンドウで、［**Android 仕事用プロファイル**］を選択します。
5. ［**Android 仕事用プロファイル**］の作業領域で、［**仕事用プロファイルの作成**］をオンにします。
6. 仕事用プロファイルを指定します：

   - Android 仕事用プロファイル内ではアプリ管理を有効にし、個人プロファイル内では無効にする場合は、［**仕事用プロファイル内でのみアプリ管理を有効にする**］をオンにします。

     ［**ユーザー**］セクションで［**アプリ管理**］を選択し、作業領域を使用して、許可対象、ブロック対象、推奨、必須のアプリのリストを作成できます。また、許可またはブロック対象のアプリのカテゴリも作成できます。

   - Google Chrome 用の危険サイトブロックを仕事用プロファイル内で有効にし、個人用プロファイル内では無効にするには、［**Android 仕事用プロファイル**］セクションで［**仕事用プロファイル内でのみ危険サイトブロックを有効にする**］をオンにします。

     Samsung Internet Browser 用の危険サイトブロックは、仕事用プロファイルおよび個人プロファイルでサイトをブロックします。Samsung Internet Browser 用の危険サイトブロックを、仕事用プロファイルでのみ有効にすることはできません。Samsung Internet Browser 用の危険サイトブロックを仕事用プロファイルで有効にするには、［**仕事用プロファイル内でのみ危険サイトブロックを有効にする**］を無効にします。このオプションを有効にすると、Samsung Internet Browser 用の危険サイトブロックは実行されません。既定では、仕事用プロファイルでの危険サイトブロックは無効にされています。

     危険サイトブロックは、Google Chrome および Samsung Internet Browser でのみ動作します。

     Web サイトへのアクセス設定（ブロックする Web サイトのカテゴリのリストや許可する Web サイトのリストの作成）は、［**危険サイトブロック**］セクションで行えます。

   - 仕事用プロファイルアプリから個人用アプリへのクリップボードによるデータのコピーを禁止するには、［**仕事用プロファイルから個人用プロファイルへのデータ転送を禁止する**］をオンにします。

- 仕事用プロファイルのモバイルデバイスで、ユーザーによる USB デバッグモードの使用をブロックするには、［**USB デバッグモードの有効化を禁止する**］をオンにします。

  USB デバッグモードでは、ユーザーはワークステーションなどからアプリをダウンロードできます。

- Android 仕事用プロファイル内で、Google Play ストア以外のあらゆるソースからのアプリのインストールを禁止するには、［**製造元が不明なアプリの仕事用プロファイルへのインストールを禁止する**］をオンにします。

- Android 仕事用プロファイル内のアプリの削除を禁止するには、［**仕事用プロファイルからのアプリの削除を禁止する**］をオンにします。

7. ユーザーのモバイルデバイスで仕事用プロファイルの設定を行うため、設定の変更をブロックします。

8. ［**適用**］をクリックして、変更を保存します。

モバイルデバイスと Kaspersky Security Center との次回の同期時に、デバイスに設定が適用されます。モバイルデバイスの容量は、仕事用プロファイルと個人用プロファイルに分けられます。

LDAP アカウントの追加

iOS MDM デバイスユーザーが、LDAP サーバー上の会社の連絡先にアクセスできるようにするには、LDAP アカウントを追加します。

iOS MDM デバイスユーザーの LDAP アカウントを追加するには：

1. コンソールツリーの［**管理対象デバイス**］フォルダーで、iOS MDM デバイスが属する管理グループを選択します。

2. 選択したグループの作業領域で、［**ポリシー**］タブを選択します。

3. ダブルクリックでポリシーのプロパティウィンドウを開きます。

4. ポリシーの**プロパティ**ウィンドウで、［**LDAP**］セクションを選択します。

5. ［**LDAP アカウント**］セクションで、［**追加**］をクリックします。
   ［**LDAP アカウント**］ウィンドウが表示されます。

6. ［**説明**］に、ユーザーの LDAP アカウントの詳細を入力します。［**使用できるマクロ**］ドロップダウンリストからマクロを使用できます。

7. ［**アカウント名**］に、LDAP サーバーで認証を行うためのアカウント名を入力します。［**使用できるマクロ**］ドロップダウンリストからマクロを使用できます。

8. ［**パスワード**］に、LDAP サーバーで認証を行うための LDAP アカウントのパスワードを入力します。

9. ［**サーバーのアドレス**］に、LDAP サーバーのドメイン名を入力します。［**使用できるマクロ**］ドロップダウンリストからマクロを使用できます。

10. メッセージの送信を保護するために、SSL（Secure Sockets Layer）データ転送プロトコルを使用する場合は、［**SSL 接続を使用する**］をオンにします。

11. iOS MDM モバイルデバイスユーザーが LDAP サーバー上の会社のデータへアクセスするための、検索クエリのリストを編集します：

a. ［**検索設定**］セクションで、［**追加**］をクリックします。
検索クエリの表に、空白行が表示されます。

b. ［**名前**］列に、検索クエリの名前を入力します。

c. ［**検索範囲**］列で、LDAP サーバー上で会社のデータを検索するためのフォルダーのネストレベルを選択します：

- **ベース** - LDAP サーバーのベースフォルダーで検索します。
- **1 レベル** - ベースフォルダーから数えて最初のネストレベルのフォルダーで検索します。
- **サブツリー** - ベースフォルダーから数えてすべてのネストレベルのフォルダーで検索します。

d. ［**検索ベース**］列に、検索を開始する LDAP サーバー上のフォルダーのパスを入力します（例："ou=people"、"o=example corp"）。

e. iOS MDM デバイスに追加するすべての検索クエリについて、ステップ a ～ d を繰り返します。

12. ［**OK**］をクリックします。
新しい LDAP アカウントがリストに表示されます。

13. ［**適用**］をクリックして、変更を保存します。

これにより、ポリシーが適用された後、LDAP アカウントが編集したリストからユーザーのモバイルデバイスに追加されます。ユーザーは iOS 標準アプリ（連絡先、メッセージ、メール）で企業の連絡先にアクセスできます。

カレンダーアカウントの追加

iOS MDM デバイスユーザーが、CalDAV サーバー上のユーザーのカレンダーイベントにアクセスできるようにするには、CalDAV アカウントを追加します。CalDAV サーバーとの同期によって、ユーザーは招待状の作成や受信、イベントの更新の受信、リマインダーアプリとのタスクの同期を実行できるようになります。

iOS MDM デバイスユーザーの CalDAV アカウントを追加するには：

1. コンソールツリーの［**管理対象デバイス**］フォルダーで、iOS MDM デバイスが属する管理グループを選択します。

2. 選択したグループの作業領域で、［**ポリシー**］タブを選択します。

3. ダブルクリックでポリシーのプロパティウィンドウを開きます。

4. ポリシーの**プロパティ**ウィンドウで、［**カレンダー**］セクションを選択します。

5. ［**CalDAV アカウント**］セクションで、［**追加**］をクリックします。
［**CalDAV アカウント**］ウィンドウが表示されます。

6. ［**説明**］に、ユーザーの CalDAV アカウントの詳細を入力します。

7. ［**サーバーアドレスとポート**］に、CalDAV サーバーのホスト名または IP アドレスと、CalDAV サーバーのポート番号を入力します。

8. ［**メイン URL**］に、CalDAV サーバーでの iOS MDM デバイスユーザーの CalDAV アカウントの URL を指定します（例：http://example.com/caldav/users/mycompany/user）。

   URL は「`http://`」または「`https://`」で始めます。

9. ［**アカウント名**］に、CalDAV サーバーで認証を行うためのアカウント名を入力します。

10. ［**パスワード**］に、CalDAV サーバーで認証を行うための CalDAV アカウントパスワードを設定します。

11. CalDAV サーバーとモバイルデバイス間でのイベントデータの送信を保護するために、SSL（Secure Sockets Layer）データ転送プロトコルを使用する場合は、［**SSL 接続を使用する**］をオンにします。

12. ［**OK**］をクリックします。

    新しい CalDAV アカウントがリストに表示されます。

13. ［**適用**］をクリックして、変更を保存します。

    これにより、ポリシーが適用された後、CalDAV アカウントが編集したリストからユーザーのモバイルデバイスに追加されます。

連絡先アカウントの追加

iOS MDM デバイスユーザーが、データを CardDAV サーバーと同期させることができるようにするには、CardDAV アカウントを追加します。CardDAV サーバーとの同期によって、ユーザーは任意のデバイスから連絡先の詳細にアクセスできるようになります。

iOS MDM デバイスユーザーの CardDAV アカウントを追加するには：

1. コンソールツリーの［**管理対象デバイス**］フォルダーで、iOS MDM デバイスが属する管理グループを選択します。

2. 選択したグループの作業領域で、［**ポリシー**］タブを選択します。

3. ダブルクリックでポリシーのプロパティウィンドウを開きます。

4. ポリシーの**プロパティ**ウィンドウで、［**連絡先**］セクションを選択します。

5. ［**CardDAV アカウント**］セクションで、［**追加**］をクリックします。

   ［**CardDAV アカウント**］ウィンドウが表示されます。

6. ［**説明**］に、ユーザーの CardDAV アカウントの詳細を入力します。［**使用できるマクロ**］ドロップダウンリストからマクロを使用できます。

7. ［**サーバーアドレスとポート**］に、CardDAV サーバーのホスト名または IP アドレスと、CardDAV サーバーのポート番号を入力します。

8. ［**メイン URL**］に、CardDAV サーバーでの iOS MDM デバイスユーザーの CardDAV アカウントの URL を指定します（例：http://example.com/carddav/users/mycompany/user）。

   URL は「`http://`」または「`https://`」で始めます。

9. ［**アカウント名**］に、CardDAV サーバーで認証を行うためのアカウント名を入力します。［**使用できるマクロ**］ドロップダウンリストからマクロを使用できます。

10. ［**パスワード**］に、CardDAV サーバーで認証を行うための CardDAV アカウントパスワードを設定します。

11. CardDAV サーバーとモバイルデバイス間での連絡先の送信を保護するために、SSL（Secure Sockets Layer）データ転送プロトコルを使用する場合は、［**SSL 接続を使用する**］をオンにします。

12. ［**OK**］をクリックします。

    新しい CardDAV アカウントがリストに表示されます。

13. ［**適用**］をクリックして、変更を保存します。

これにより、ポリシーが適用された後、CardDAV アカウントが編集したリストからユーザーのモバイルデバイスに追加されます。

購読したカレンダーの設定

iOS MDM デバイスユーザーが、共有カレンダー（会社のカレンダーなど）のイベントをユーザーのカレンダーに追加できるようにするには、このカレンダーに購読を追加します。「*共有カレンダー*」とは、CalDAV アカウントを持つ別のユーザーのカレンダー、iCal カレンダー、その他の公開されているカレンダーのことです。

購読したカレンダーを追加するには：

1. コンソールツリーの［**管理対象デバイス**］フォルダーで、iOS MDM デバイスが属する管理グループを選択します。

2. 選択したグループの作業領域で、［**ポリシー**］タブを選択します。

3. ダブルクリックでポリシーのプロパティウィンドウを開きます。

4. ポリシーの**プロパティ**ウィンドウで、［**購読したカレンダー**］セクションを選択します。

5. ［**購読したカレンダー**］セクションで、［**追加**］をクリックします。

   ［**購読したカレンダー**］ウィンドウが開きます。

6. ［**説明**］に、購読したカレンダーの詳細を入力します。

7. ［**サーバーの Web アドレス**］に、サードパーティのカレンダーの URL を指定します。

   このフィールドでは、購読しているカレンダーの、ユーザーの CalDAV アカウントのメール URL を入力できます。iCal カレンダーの URL や公開されている他のカレンダーの URL も指定できます。

8. ［**ユーザー名**］に、サードパーティのカレンダーのサーバーの認証に使用するユーザーアカウント名を入力します。

9. ［**パスワード**］に、サードパーティのカレンダーのサーバーでの認証に使用する購読したカレンダー用のパスワードを入力します。

10. CalDAV サーバーとモバイルデバイス間でのイベントデータの送信を保護するために、SSL（Secure Sockets Layer）データ転送プロトコルを使用する場合は、［**SSL 接続を使用する**］をオンにします。

11. ［**OK**］をクリックします。

12. 新しい購読したカレンダーがリストに表示されます。

13. ［**適用**］をクリックして、変更を保存します。

これにより、ポリシーが適用された後、リストのイベントが共有カレンダーからユーザーのモバイルデバイスのカレンダーに追加されます。

Web クリップの追加

*Web クリップ*は、モバイルデバイスのホーム画面から Web サイトを開くアプリです。デバイスのホーム画面で Web クリップのアイコンをクリックすることで、Web サイト（会社の Web サイトなど）をすばやく開くことができます。ユーザーのデバイスに Web クリップを追加し、画面に表示される Web クリップのアイコンの外観を設定できます。

既定では、Web クリップには以下の制限が適用されます：

- ユーザーはモバイルデバイスから Web クリップを手動で削除することはできません。
- Web クリップアイコンをクリックして開いた Web サイトは、フルスクリーンモードで表示されません。
- 角の丸み、影、光沢などの視覚効果が、画面上の Web クリップアイコンに適用されます。

iOS MDM デバイスに Web クリップを追加するには：

1. コンソールツリーの［**管理対象デバイス**］フォルダーで、iOS MDM デバイスが属する管理グループを選択します。
2. 選択したグループの作業領域で、［**ポリシー**］タブを選択します。
3. ダブルクリックでポリシーのプロパティウィンドウを開きます。
4. ポリシーの**プロパティ**ウィンドウで、［**Web クリップ**］セクションを選択します。
5. ［**Web クリップ**］セクションで、［**追加**］をクリックします。
   ［**Web クリップ**］ウィンドウが表示されます。
6. ［**名前**］に、iOS MDM デバイスのホーム画面に表示する Web クリップの名前を入力します。
7. ［**URL**］に、Web クリップアイコンをクリックした時に表示される Web サイトの URL を入力します。アドレスは「`http://`」または「`https://`」で始めます。
8. ユーザーが Web クリップを iOS MDM デバイスから削除できるようにするには、［**削除を許可する**］をオンにします。
9. ［**選択**］をクリックし、Web クリップアイコンの画像が入っているファイルを指定します。
   iOS MDM デバイスのホーム画面にアイコンが表示されます。イメージは以下の要件を満たしている必要があります：
   - 画像サイズは 400 x 400 ピクセル以下
   - ファイル形式：GIF、JPEG、PNG
   - ファイルサイズは 1 MB 以下

   Web クリップアイコンは、［**アイコン**］でプレビューできます。Web クリップのイメージが選択されていない場合、アイコンとして空白が表示されます。

   特殊な視覚効果（角の丸み、光沢効果など）を付けずに Web クリップアイコンを表示する場合は、［**Precomposed アイコン**］をオンにします。

10. アイコンをクリックした時に、iOS MDM デバイスで Web サイトをフルスクリーンモードで開く場合は、［**フルスクリーン Web クリップ**］をオンにします。

11. ［**OK**］をクリックします。

    新しい Web クリップがリストに表示されます。

12. ［**適用**］をクリックして、変更を保存します。

これにより、ポリシーが適用された後、作成済みの Web クリップアイコンが、リストからユーザーのモバイルデバイスのホーム画面に追加されます。

フォントの追加

iOS MDM デバイスにフォントを追加するには：

1. コンソールツリーの［**管理対象デバイス**］フォルダーで、iOS MDM デバイスが属する管理グループを選択します。

2. 選択したグループの作業領域で、［**ポリシー**］タブを選択します。

3. ダブルクリックでポリシーのプロパティウィンドウを開きます。

4. ポリシーの**プロパティ**ウィンドウで、［**フォント**］セクションを選択します。

5. ［**フォント**］セクションで、［**追加**］をクリックします。

   ［**フォント名**］ウィンドウが表示されます。

6. ［**ファイル名**］に、フォントファイル（拡張子 TTF または OTF が付いたファイル）のパスを指定します。

   拡張子 TTC または OTC のフォントはサポートしていません。

   フォントは PostScript 名を使用して識別されます。内容が異なっていても、同じ PostScript 名のフォントはインストールしないでください。同じ PostScript 名を持つフォントをインストールすると、不明なエラーが発生します。

7. ［**開く**］をクリックします。

   新しいフォントがリストに表示されます。

8. ［**適用**］をクリックして、変更を保存します。

これにより、ポリシーが適用された後、ユーザーは作成したリストからフォントをインストールするように要求されます。

サードパーティ製の EMM システムを使用したアプリの管理（Android のみ）

カスペルスキーの管理システムがなくとも、Kaspersky Endpoint Security for Android アプリを使用できます。他の EMM（エンタープライズ・モビリティ・マネジメント）サービスプロバイダーの製品を使用して、Kaspersky Endpoint Security for Android アプリを導入し、管理します。カスペルスキーは、AppConfig Community に加入しており、本アプリがサードパーティ製の EMM 製品と併用できるようにしています。

Kaspersky Endpoint Security for Android のサードパーティ製 EMM 製品での管理は、Android デバイスでのみ可能です。

サードパーティ製の EMM 製品を使用して、Kaspersky Endpoint Security for Android アプリのみを導入できます。デバイスを Kaspersky Security Center に接続し、管理コンソールでアプリを管理します。この場合、EMM コンソールでの Kaspersky Endpoint Security for Android アプリの管理は使用できなくなります。

サードパーティの EMM システムを使用して Kaspersky Endpoint Security for Android アプリを導入した場合、Kaspersky Endpoint Security Cloud でアプリを管理することはできません。EMM コンソールで Kaspersky Endpoint Security for Android アプリを管理できます。

Kaspersky Endpoint Security for Android アプリの使用をサポートする EMM 製品は、次の通りです：

- VMware AirWatch
- MobileIron
- IBM Maas360
- Microsoft Intune
- SOTI MobiControl

EMM コンソールでは、以下が可能です：

- 本アプリのユーザーデバイスの Android 仕事用プロファイルへの追加。
- 本アプリのアクティベート。
- アプリの設定：
  - インターネット上の悪意のあるサイトやフィッシングサイトからの保護を有効にする
  - Kaspersky Security Center と端末との接続に関する設定
  - アンチウイルスの設定
  - デバイスのウイルススキャンのスケジュールの設定
  - アドウェアと、デバイスや個人情報に損害を与える目的で悪用される可能性のあるアプリの検知の有効化
  - 定義データベースのアップデートのスケジュールの設定

開始時の操作

本アプリをユーザーのモバイルデバイスに導入するには、Kaspersky Endpoint Security for Android を EMM のアプリストアに追加する必要があります。Google Play へのリンクを使用して EMM アプリストアへ追加できます。EMM コンソールの使用方法の詳細は、*EMM 製品の提供元のテクニカルサポートサイト*をご参照ください。

Kaspersky Endpoint Security for Android アプリが Android 仕事用プロファイルに追加されます。本アプリは、ユーザーの個人データに関与せず、仕事用プロファイルの企業データのみを保護します。本アプリが削除されないよう、EMM コンソールツールで保護しておくことを推奨します。

本アプリのインストール方法

EMM コンソールに応じて、本アプリのデバイスへのインストール方法を次から選択します：サイレントインストール、Google Play 上のアプリへのリンクを含むメールの送信、またはその他の可能な方法。

アプリを動作させるには、次の権限が必要です：

- アンチウイルスの実行中に、ファイルアクセスの目的でメモリを使用する権限（Android 6.0 以降のみ）。
- デバイスを識別する目的で電話する権限（本アプリのアクティベーション時など）。
- オペレーティングシステムの起動時に開始されるアプリのリストへの本アプリの追加要求（Huawei、Meizu、Xiaomi などの一部のデバイスで要求されます）：リクエストが表示されない場合は、スタートアップアプリのリストに手動で追加してください。仕事用プロファイルにセキュリティアプリを追加していない場合は、このリクエストは表示されない場合があります。

Kaspersky Endpoint Security for Android アプリを導入する前に、EMM コンソールで必要な権限を付与できます。EMM コンソールでの権限の付与について詳細は、*EMM 製品の提供元のテクニカルサポートサイト*をご参照ください。デバイス上の Kaspersky Endpoint Security for Android の初期設定ウィザードが完了した後でも権限を付与することができます。

Kaspersky Endpoint Security for Android アプリが、Android 仕事用プロファイルに追加されます。

危険サイトブロックの動作には、Google Chrome の設定でプロキシサーバーを設定することも必要です：

- プロキシサーバーの編集モード：手動
- プロキシサーバーのアドレスとポート：127.0.0.1:3128
- SPDY プロトコルのサポート：無効
- プロキシサーバー使用時のデータ圧縮：無効

本アプリのアクティベート方法

ライセンスに関する情報は、設定情報ファイル内のその他の情報と共に、モバイルデバイスに転送されます。

モバイルデバイスへのインストール後 30 日以内に本アプリがアクティベートされないと、試用版ライセンスの有効期限が切れます。試用版ライセンスの有効期限が切れると、Kaspersky Endpoint Security for Android モバイルアプリのすべての機能が無効になります。

製品版ライセンスの有効期限が切れると、製品は引き続き動作しますが、機能が制限されます（たとえば、Kaspersky Endpoint Security for Android の定義データベースのアップデートは使用できません）。機能の制限がない状態で製品の使用を継続するには、製品版ライセンスを更新する必要があります。

Kaspersky Endpoint Security for Android をアクティベートするには：

1. EMM コンソールで、Kaspersky Endpoint Security for Android アプリの設定を開きます。
2. ［`LicenseActivationCode`］フィールドに、アクティベーションコードを入力します。

   デバイス上の本アプリをアクティベートするには、カスペルスキーのアクティベーションサーバーへのアクセスが必要です。

デバイスを Kaspersky Security Center へ接続する方法

Kaspersky Endpoint Security for Android をモバイルデバイスにインストールした後、デバイスを Kaspersky Security Center へ接続できます。デバイスと Kaspersky Security Center の接続に必要なデータが、設定ファイルに記載されたその他の設定とともにモバイルデバイスに転送されます。デバイスを Kaspersky Security Center と接続した後、グループポリシーを使用して本アプリを一元的に設定できます。本アプリのパフォーマンスに関するレポートや統計情報の受信も可能です。

Kaspersky Security Center をデバイスに接続する前に、次の条件を満たしているかどうかを確認してください：

- 管理者用のワークステーションに、Kaspersky Endpoint Security for Android 管理プラグインがインストールされている。
- 管理サーバーのプロパティで、モバイルデバイスの接続に使用するポートが開放されている。
- 管理コンソールでの［**モバイルデバイス管理**］フォルダーの表示が有効である。
- モバイルデバイスユーザーの識別用の証明書が、Kaspersky Security Center の証明書保管領域で作成されている。

デバイスを Kaspersky Security Center へ接続する前に、次のことを行っておくことを推奨します：

- モバイルデバイスのタスクとポリシーを作成する場合、モバイルデバイス用に個別の管理グループを作成する。
- 個別の管理グループにモバイルデバイスを移動する場合、［**未割り当てデバイス**］フォルダーから、デバイスを自動的に移動するルールを作成します。
- Kaspersky Endpoint Security for Android を一元的に設定できるようにする場合、グループポリシーを作成する。

デバイスと Kaspersky Security Center を接続するには：

1. EMM コンソールで、Kaspersky Endpoint Security for Android アプリの設定を開きます。
2. ［`KscServer`］フィールドに、Kaspersky Security Center 管理サーバーの DNS 名または IP アドレスを入力します。既定のポートは 13292 です。
3. Kaspersky Endpoint Security for Android の通知をモバイルデバイスに表示したくない場合は、アプリの通知を無効にできます。表示を無効にするには、`DisableNotification = True` と設定します。

   接続すると、すべての通知が表示されるようになります。特定のアプリの通知を、ポリシーの設定で無効に設定できます。

Kaspersky Security Center を使用しない場合は、アプリの通知を無効にしないでください。無効にすると、ライセンスの有効期限に関する通知をユーザーが受け取れなくなる可能性があります。ライセンスの有効期間が終了すると、本アプリの機能が実行されなくなります。

接続設定の編集後、Kaspersky Endpoint Security for Android は次の権限および許可を要求する通知を表示します：

- 盗難対策の動作による［カメラ］の使用許可（**遠隔撮影**コマンド）。
- 盗難対策の動作による［位置情報］の使用許可（**GPS 追跡**コマンド）。
- デバイスの管理者権限（Android 仕事用プロファイルの所有者）。次のアプリ機能の動作が管理者権限を必要とします：
  - セキュリティ証明書のインストール。
  - Wi-Fi の設定。
  - Exchange ActiveSync の設定。
  - カメラ、Bluetooth、Wi-Fi の使用制限。

Android 仕事用プロファイルの特定の仕様（補助機能サービスが存在しない）により、アプリ管理と盗難対策の機能が本アプリで使用できません。

ユーザーが必要な権限と許可を付与すると、デバイスが Kaspersky Security Center へ接続されます。管理グループへデバイスを自動的に移動するルールを作成していない場合、デバイスは［**未割り当てデバイス**］フォルダーに追加されます。管理グループへデバイスを自動的に移動するルールを作成していた場合、デバイスは定義済みのグループに追加されます。

Kaspersky Endpoint Security は、次のデバイス名の形式を提供します：

- デバイスのモデル［メール、デバイス ID］
- デバイスのモデル［メール（ある場合）またはデバイス ID］

デバイス ID は、Kaspersky Endpoint Security がデバイスから受け取ったデータから生成する一意の ID です。Android 10 以降のモバイルデバイスでは、SSAID（Android ID）または別のデータのチェックサムをデバイスから受け取って使用します。それ以前の Android バージョンでは、IMEI を使用します。グループポリシーでデバイス名の形式を設定できます。デバイス名にタグを追加することもできます。これにより、Kaspersky Security Center でのデバイスの検索と並べ替えが容易になります。このタグは VMware AirWatch でのみ使用可能です。

デバイス名にタグを追加することもできます：

1. EMM コンソールで、Kaspersky Endpoint Security for Android アプリの設定を開きます。
2. `KscDeviceNameTag` フィールドで値を選択します：
   - `{DeviceSerialNumber}` - デバイスのシリアルナンバー。
   - `{DeviceUid}` - 一意なデバイスの識別子（UDID）。
   - `{DeviceAssetNumber}` - デバイスのアセットナンバー。この番号は組織内で作成されます。

これらの値のみを使用してください。VMware AirWatch では他の値もサポートしていますが、Kaspersky Endpoint Security ではそれらの値が機能することを保証できません。

`{DeviceSerialNumber} {DeviceUid}` など、複数の値を追加できます。タグは Kaspersky Security Center のデバイス名に追加されます。タグとデバイス名はスペースで区切ります。たとえば、デバイス名が `Google Pixel 2 a10c6b75f7b31de9 22:7D:78:9E:C5:1E` の場合、`22:7D:78:9E:C5:1E` が UDID タグです。Kaspersky Security Center と VMware AirWatch を使用している場合、タグを使用すると、両方のコンソールでデバイスを識別できます。デバイスを一致させるには、デバイス名に同じ値を選択します（デバイスのシリアル番号など）。

デバイスが Kaspersky Security Center へ接続された後、本アプリの設定はグループポリシーで設定された内容に変更されます。EMM コンソールで編集された設定ファイルにある本アプリの設定は無視されます。ポリシーのすべてのセクションで設定を編集できますが、次のセクションは編集できません：

- **盗難対策**（デバイスロック）
- **コンテナー**
- **デバイス管理**（スクリーンロック）
- **アプリ管理**（ブロック対象アプリのブロック）
- **Android 仕事用プロファイル**
- **Samsung KNOX の管理**

作業プロファイルの導入に使用する方法により、［**Android 仕事用プロファイル**］セクションからグループポリシーの設定を適用することができません。これらの設定は、Kaspersky Security Center を使用して仕事用プロファイルが作成された場合にのみ設定可能です。

AppConfig ファイル

設定情報ファイルは、EMM コンソール内の本アプリを設定する目的で作成されます。設定情報ファイル内の本アプリの設定は、以下の表に記載されています。

設定情報ファイルの設定

設定項目	説明	種別	値
`LicenseActivationCode`	アプリのアクティベーションコード	文字列	20 文字の英数字の組み合わせで構成されるアプリのアクティベーションコードクティベーションコードを使用して本リをアクティベートするには、カスペキーのアクティベーションサーバーにするためのインターネットアクセスがです。

			このフィールドを空白にすると、試用 イセンスでアクティベートされます。 版ライセンスの有効期間は、30 日です 試用版ライセンスの有効期限が切れる Kaspersky Endpoint Security for Androi バイルアプリのすべての機能が無効に ます。引き続き製品を使用するには、 版ライセンスを購入してください。
`EulaAcceptanceConfirmationV1`	<使用許諾契約書のリンク>	選択肢	この設定は VMware AirWatch でのみ使用可能です。 `Accepted` - この使用許諾契約書の内容すべて確認し、理解した上で条項に同ます。 `Declined` - 使用許諾契約書の条項に同しません。 すべてのモバイルデバイスのために使諾契約書の条項に同意するには、カススキーのサーバーへ接続するためのイーネットアクセスが必要です。 ［`Declined`］を選択した場合、本アはユーザーに使用許諾契約書の条項へ意を要求します。モバイルデバイスのザーは、初期設定の途中で条項に同意ことができます。
`EulaAcceptanceCodeV1`	使用許諾契約書のコード	文字列	これらの設定は、VMware AirWatch のみ使用可能です。 単一の使用許諾契約書（EULA）に同意る場合は、`EulaAcceptanceCodeV1` を用します。複数の使用許諾契約書に同同意する場合は、`EulaAcceptanceCodesV2` を使用しま ［`EulaAcceptanceCodesV2`］フィーには、セミコロンで区切られた使用許約書コードのリストを含む必要がありす：`"<EULAid1>;<EULAid2>;<EULAid3>;..."` 使用許諾契約書のコードは、使用許諾書に含まれています。 *使用許諾契約書のコードを読むには：* 1. 使用許諾契約書のリンク（`EulaAcceptanceConfirmationV` を EMM コンソールからコピーしま 2. コピーしたリンクをブラウザーに貼付けます。 使用許諾契約書が開きます。
`EulaAcceptanceCodesV2`	使用許諾契約書のコード	文字列	

			3. 使用許諾契約書の条項を確認し、使 許諾契約書のコードを探します。 すべてのモバイルデバイスのために 用許諾契約書の条項に同意するには カスペルスキーのサーバーへ接続す ためのインターネットアクセスが必 です。 このフィールドを空白にすると、本ア はユーザーに使用許諾契約書の条項へ 意を要求します。モバイルデバイスの ザーは、初期設定の途中で条項に同意 ことができます。 両方のフィールドに値を指定すると、 らで指定されたすべての使用許諾契約 条項が同意されます。
`KscServer`	Kaspersky Security Center 管理サーバーのアドレスとポート	文字列	Kaspersky Security Center 管理サーバー DNS 名または IP アドレスとポート番号 アドレスを次の形式で入力します：<サ バーのアドレス>:<ポート>.サーバーの ドレスのみ入力してポート番号を指定 いと、既定のポート 13292 が使用され す。
`DisableNotification`	Kaspersky Security Center へ接続されるまで、アプリの通知を無効にします。	True/False	`True` – アプリの通知をすべて非表示に ます。デバイスが Kaspersky Security Center に接続されるまで、通知は非表 のままです。接続すると、すべての通 表示されるようになります。特定のア の通知を、ポリシーの設定で無効に設 きます。 Kaspersky Security Center を使用しな い場合は、アプリの通知を無効にし いでください。無効にすると、ライ ンスの有効期限に関する通知をユー ーが受け取れなくなる可能性があり す。ライセンスの有効期間が終了す と、本アプリの機能が実行されなく ります。 `False` – アプリの通知をすべて表示し す。
`ScanScheduleType`	スキャンの実行方法	選択肢	`AfterUpdate` - 定義データベースのア プデート後にスキャンを開始します。 プデートは、`UpdateScheduleType` で 義したスケジュールに従って実行され す。 `Daily` - 1 日に 1 回スキャンを開始しま す。開始時刻は、`ScanScheduleTime` 設定します。

			`Weekly` - 1週間に1回スキャンを開始し す。スキャンの曜日は、 `ScanScheduleDay` で設定し、時刻は `ScanScheduleTime` で設定します。 `Off` - スキャンの自動開始が無効にな す。 どの値を設定した場合でも、デバイス ザーは手動でもスキャンを開始できま
`ScanScheduleDay`	スキャンを実行する曜日	選択肢	`Monday / Tuesday / Wednesday / Thursday / Friday / Saturday / Sunday` 上記から値を1つ選択して設定します。
`ScanScheduleTime`	スキャンを実行する時刻を指定します	文字列	24時間表記（13:00など）または12時記（10:30 PMなど）で指定できます。
`ScanScheduleLock`	ユーザーによるスキャンの実行方法の設定をブロックします	True/False	`True` - 本アプリの設定でユーザーがウルススキャンの方法を設定できなくなす。 `False` - 本アプリの設定でユーザーがルススキャンの方法を設定できます（開始を無効にするなど）。
`ScanOnlyExecutableFiles`	スキャン対象のファイル種別（ウイルススキャン）	選択肢	`AllFiles` - すべてのファイルをスキャします。 `OnlyExecutables` - 実行ファイルのみキャンします。実行ファイルとは、拡がAPK（ZIP）、DEX、SOのファイルす。 Kaspersky Endpoint Security for Androi Service Pack 4 Maintenance Release 1 では、実行ファイルのみのスキャンを有できません。
`ScanArchives`	圧縮ファイルを解凍してスキャンする	True/False	`True` - 圧縮ファイルを解凍し、解凍さた内容をスキャンします。 `False` - 圧縮ファイル自体のみをスキします。 拡張子がZIP（APK）の圧縮ファイルのをスキャンします。 Kaspersky Endpoint Security for Androi Service Pack 4 Maintenance Release 1 では、圧縮ファイルの内容のスキャンをにできません。
`ScanActionOnThreatFound`	脅威の検知時の処理（ウイルススキャン）	選択肢	`Quarantine` - 検知したオブジェクトを離に移動します。隔離に移動されたフルは、デバイスに損害を与えないよう縮ファイルとして保管されます。隔離は、隔絶された保管領域に移動されたイルを削除したり、復元したりできま `Delete` - 検知したオブジェクトを削除ます。

			Skip - 検知したオブジェクトをそのまにし、変更しません。オブジェクトがップされると、Kaspersky Endpoint Security for Android はデバイス保護のについてユーザーに警告します。デバ上のオブジェクトへのアクセス試行をすると（オブジェクトをコピーしたりたりしようとする試行など）、アプリアクセスをブロックします。 AskUser - 検知したオブジェクトごと処理（スキップ、隔離、削除）の選択求します。複数のオブジェクトを検知場合は、選択したアクションをすべてブジェクトに適用できます。 検知した脅威に関する情報と、脅威にて実行した処理は、アプリのレポート録されます。
ScanLock	スキャンの設定の編集をブロックします	True/False	True - 本アプリの設定で、次のスキャ設定にアクセスできなくなります：スンするファイル種別、圧縮ファイルのャン、脅威の検知時に実行する処理。 False - スキャンの設定を編集できまたとえば、検知した脅威をスキップすように設定できます。
ScanAndProtectionAdwareRiskware	アドウェアや、ユーザーのデバイスやデータに損害を与える目的で悪用される可能性があるアプリをブロックします。	True/False	True - アドウェアや、ユーザーのデバスやデータに損害を与える目的で悪用る可能性があるアプリを検知します。 False - アドウェアや、ユーザーのデスやデータに損害を与える目的で悪用る可能性があるアプリをスキップしま
ProtectionMode	リアルタイム保護モード	選択肢	Recommended - 新しくインストールさたアプリと、ダウンロードフォルダーるファイルのみをスキャンします。 Extended - デバイス上で開かれたファル、変更されたファイル、コピーされァイル、実行されたファイル、保存さファイルをすべてスキャンします。ま新しくインストールされたアプリと、ンロードフォルダーにあるファイルもャンします・ Disabled – リアルタイム保護を無効ます。
UseKsnMode	Kaspersky Security Network モード	選択肢	Recommended - Kaspersky Security Network（KSN）と本アプリでデータをりとりします。KSN は、脅威から端末リアルタイムで保護したり（クラウドテクション）、インターネット上の危イトをブロックしたりするのに使用さす。

			`Extended` - Kaspersky Security Networ データをやりとりし、本アプリの一部 フォーマンスに関する統計情報をウイ ラボに送信します。この情報によって アルタイムでの脅威の追跡が可能にな います。KSN サービスは、個人情報の 集、処理、保管は行いません。 `Disabled` - Kaspersky Security Networ らのデータを使用しません。危険サイ ロックは使用できません （`EnableWebFilter`）。アンチウイル のクラウドプロテクションの機能は使 きません。
`ProtectScanOnlyExecutableFiles`	スキャン対象のファイル種別（リアルタイム保護）	True/False	`AllFiles` - すべてのファイルをスキャ します。 `OnlyExecutables` - 実行ファイルのみ キャンします。実行ファイルとは、拡 が APK（ZIP）、DEX、SO のファイル す。 Kaspersky Endpoint Security for Androi Service Pack 4 Maintenance Release 1 で は、実行ファイルのみのスキャンを有 できません。
`ProtectionActionOnThreatFound`	脅威の検知時の処理（リアルタイム保護）	選択肢	`Quarantine` - 検知したオブジェクトを 離に移動します。隔離に移動されたフ ルは、デバイスに損害を与えないよう 縮ファイルとして保管されます。隔離 は、隔絶された保管領域に移動された イルを削除したり、復元したりできま `Delete` - 検知したオブジェクトを削除 ます。 `Skip` - 検知したオブジェクトをそのま にし、変更しません。オブジェクトが ップされると、Kaspersky Endpoint Security for Android はデバイス保護の についてユーザーに警告します。デバ 上のオブジェクトへのアクセスが試行 ると（オブジェクトをコピーしたり開 りしようとする試みなど）、オブジェ へのアクセスがブロックされます。 検知した脅威に関する情報と、脅威に て実行した処理は、アプリのレポート 録されます。
`ProtectionLock`	リアルタイム保護の設定の編集をブロックします	True/False	`True` - 本アプリの設定で、次のリアル イム保護設定にアクセスできなくなり す：リアルタイム保護モード、スキャ るファイル種別、脅威の検知時に実行 処理。 `False` - リアルタイム保護の設定を編 きます。たとえば、検知した脅威をス ップするように設定できます。
`UpdateScheduleType`	定義データベースのアップ	選択肢	`Daily` - 1日1回、定義データベースの ップデートを確認し、デバイスにダウ

	デートの実行方法		ードします。アップデートの開始時刻は、UpdateScheduleTime で設定しま す。 Weekly - 1 週間に 1 回、定義データベ- のアップデートを確認し、デバイスに ンロードします。アップデートの曜日 UpdateScheduleDay で選択し、時刻 UpdateScheduleTime で設定します。 Off - 定義データベースの自動アップ トが無効になります。 どの値を設定した場合でも、デバイス ザーは手動でもアップデートを開始で す。
UpdateScheduleDay	定義データベースのアップデートを開始する曜日	選択肢	Monday / Tuesday / Wednesday / Thursday / Friday / Saturday / Sunday 上記から値を 1 つ選択して設定します。
UpdateScheduleTime	定義データベースのアップデートを開始する時刻	文字列	24 時間表記（13:00 など）または 12 時記（10:30 PM など）で指定できます。
UpdateScheduleLock	アップデートの実行方法の設定をブロックします	True/False	True - 本アプリの設定でユーザーがア プデートの方法の設定にアクセスでき なります。 False - 本アプリの設定でユーザーが プデートの方法を設定できます（自動 を無効にするなど）。
AllowUpdateInRoaming	ローミング時に定義データベースをアップデートします	True/False	True - デバイスのローミング中に定義 ータベースをアップデートします。ダ ロードは、UpdateScheduleType で定 したスケジュールに従って実行されま False - デバイスがホームネットワー 接続している場合のみ、定義データベ をアップデートします。
EnableWebFilter	危険サイトブロック	True/False	True - 危険サイトブロックを使用し、 ンターネット上の悪意のある Web サイ やフィッシングサイトをブロックしま 危険サイトブロックは、Google Chrom でのみサポートされています。 悪意のある Web サイトおよびフィッ シングサイトが HTTPS プロトコルを 使用しており、ドメインが信頼済み 場合、それらのサイトはブロックさ ない状態が続きます。ドメインが信 されていない場合、危険サイトブロ クは悪意のある Web サイトおよびフ ィッシングサイトをブロックします False - 危険な Web サイトやフィッシ グサイトからの保護が無効になります

			危険サイトブロックが動作するには、条件を満たす必要があります：
			• プライバシーポリシーおよび危険サトブロックに関する声明に、初期設ウィザードまたは本アプリの設定でバイスのユーザーが同意していること。
			• プロキシサーバーがブラウザーで次ように設定されていること：
			`ProxyMode = "fixed_servers"`
			`ProxyServer = "127.0.0.1:3128`
			`DisableSpdy = true`
			`DataCompressionProxyEnabled = false`
			プロキシサーバーの設定は Google Chrome のバージョンにより異なる合があります。Google Chrome の設の詳細は、Chromium プロジェクトサイトをご参照ください：
			Kaspersky Endpoint Security for Andアプリをモバイルデバイスから削除た後は、プロキシサーバーの設定をセットしてください。
			• KSN の使用を本アプリの設定で有効します（`UseKsnMode = Recommen`または `UseKsnMode = Extended`）
			• Google Chrome を通常使用するブラザーとしてオペレーティングシステで設定しておくことを推奨します。

`EnableWebFilterLock`	危険サイトブロックの設定の編集をブロックします	True/False	`True` - 本アプリの設定でユーザーが危サイトブロックの設定にアクセスできなります。 `False` - 本アプリの設定で危険サイトックの設定を編集できます。たとえば険な Web サイトやフィッシングサイトらの保護を無効にできます。
`UpdateServer`	定義データベースのアップデート元のアドレス	文字列	定義データベースのアップデート元のバーのアドレスを、`http://update.server.com` のよう定します。 このフィールドを空白にすると、Kaspersky Endpoint Security for Androiは、カスペルスキーのアップデートサーを使用します。
`AllowGoogleAnalytics`	Firebase 向け Google アナリティクス、SafetyNet Attestation、Firebase Performance Monitoring、	True/False	`True` - Kaspersky Endpoint Security for Android の動作に関するデータを Fireb向け Google アナリティクス、SafetyNAttestation、Firebase Performance Monitoring、Crashlytics サービスへ自に送信します。このデータは、本アプパフォーマンスの改善およびユーザー度の分析に使用されます。データはセ

	Crashlytics サービスへのデータ送信		アな通信で Firebase 向け Google アナィクス、SafetyNet Attestation、Firebase Performance Monitoring、Crashlytics サビスへ転送されます。データへのアクと保護は、Firebase 向け Google アナリィクス、SafetyNet Attestation、Firebase Performance Monitoring、Crashlytics サビスの使用に対応する条件により規制ます。 `False` - Firebase 向け Google アナリテクス、SafetyNet Attestation、Firebase Performance Monitoring、Crashlytics サビスへのデータの送信が無効になりま
`KscDeviceNameTag`	Kaspersky Security Center のデバイス名のタグ	文字列	この設定は VMware AirWatch でのみ使用可能です。 タグは Kaspersky Security Center のデス名に追加されます。タグとデバイススペースで区切ります。これにより、Kaspersky Security Center でのデバイス検索と並べ替えが容易になります。 • `{DeviceSerialNumber}` - デバイスシリアルナンバー。 • `{DeviceUid}` - 一意なデバイスの識子（UDID）。 • `{DeviceAssetNumber}` - デバイスセットナンバー。この番号は組織内作成されます。 `{DeviceSerialNumber}` `{DeviceUid}` など、複数の値を追加きます。 これらの値のみを使用してください。VMware AirWatch では他の値もサポートしていますが、Kaspersky Endpoint Security ではそれらの値が機能するとを保証できません。
`KscGroup`	デバイスグループ名	文字列	デバイスグループ名を EMM コンソーで指定できます。Kaspersky Security Center へデバイスを接続すると、［未り当てデバイス］フォルダーのサブフダーにそのデバイスが自動的に追加さす。サブフォルダーの名前は、このパータで指定した値と一致します。［未当てデバイス］フォルダーのサブフォーから［管理対象デバイス］フォルダデバイスを自動的に移動するルールをできます。

			このフィールドを空白にすると、デバは［未割り当てデバイス］のルートフダーに自動的に追加されます。
KscCorporateEmail	ユーザーの企業メール	文字列	サードパーティの EMM コンソールで、ーザーの企業メールアドレスを指定です。企業メールアドレスは、Kaspersky Security Center に表示されます。 有効なメールアドレスを指定する必要ります。無効な値は無視されます。

ネットワーク負荷

このセクションは、モバイルデバイスと Kaspersky Security Center の間で発生するネットワーク通信の量に関する情報を記載しています。

通信量

タスク	送信トラフィック	受信トラフィック	通信の総量
アプリの初回導入（MB 単位）	0.08	17.76	17.84
定義データベースの初回アップデート（通信量は定義データベースのサイズに応じて異なる場合があります）（MB 単位）	0.04	2.21	2.25
モバイルデバイスと Kaspersky Security Center の同期（MB 単位）	0.03	0.02	0.05
通常の定義データベースのアップデート（通信量は定義データベースのサイズに応じて異なる場合があります）（MB 単位）	0.08	3.06	3.14
盗難対策コマンドの実行デバイスの GPS 追跡（通信量は搭載されたカメラの性能および写真の画質に応じて異なる場合があります）（MB 単位）	0.09	0.8	0.17
盗難対策コマンドの実行遠隔撮影（MB 単位）	1.0	0.02	1.02
盗難対策コマンドの実行デバイスロック（MB 単位）	0.06	0.05	0.11
1 日あたりの平均量（MB 単位）	0.22	6.96	7.18

Kaspersky Security Network への参加

モバイルデバイスをより効果的に保護するために、Kaspersky Endpoint Security for Android は、世界中のユーザーから取得したデータを使用しています。*Kaspersky Security Network* は、そのような集められたデータの処理を目的としています。

*Kaspersky Security Network（KSN）*は、ファイル、Web リソース、ソフトウェアの評価に関する情報を含むカスペルスキーのオンラインナレッジベースへのアクセスを提供する、クラウドサービスの基盤です。Kaspersky Security Network のデータを使用することにより、脅威に対するカスペルスキー製品の対応が迅速化され、保護コンポーネントのパフォーマンスが向上し、誤検知の可能性も低減されます。

Kaspersky Security Network に参加していただくことで、カスペルスキーでは新たな脅威の種別とソースに関する情報をリアルタイムで取得し、新しい脅威を駆除する方法を開発することができます。また、Kaspersky Endpoint Security for Android による誤検知の件数も低減できます。また、Kaspersky Security Network に参加するユーザーは、アプリケーションと Web サイトのレピュテーション統計情報を利用することもできます。

Kaspersky Security Network に参加すると、Kaspersky Endpoint Security for Android の実行中に一定の統計が集められ、自動でカスペルスキーに送信されます。この情報によって、リアルタイムでの脅威の追跡が可能になっています。コンピューターまたはユーザーのコンテンツに損害を与える目的で侵入者に悪用される可能性があるファイルや、ファイルのそのような部分もカスペルスキーに送られ、追加で調査を行うことがあります。

Kaspersky Security Network の使用は、Kaspersky Endpoint Security for Android の操作に必要です。KSN は次の主要な機能に使用されます：アンチウイルス、危険サイトブロック、アプリ管理。KSN への参加を拒否すると、デバイスの保護レベルが下がり、デバイスの感染やデータの消失の原因となる可能性があります。Kaspersky Security Network の使用を開始するには、本アプリのインストール前に、使用許諾契約書の諸条件に同意する必要があります。使用許諾契約書を読むことで、Kaspersky Endpoint Security for Android が Kaspersky Security Network に転送するデータの種類を知ることができます。

本アプリのパフォーマンス改善を目的として、Kaspersky Security Network に統計情報を提供することもできます。上記の情報の KSN へのご提供は任意です。Kaspersky Security Network を使用するには、専用の規約である *Kaspersky Security Network に関する声明*に同意する必要があります。Kaspersky Security Network への参加を取りやめることは、いつでも可能です。Kaspersky Security Network 声明では、Kaspersky Endpoint Security for Android から Kaspersky Security Network に送信されるデータの種別について説明しています。

Kaspersky Security Network との情報交換

リアルタイム保護を改善するため、Kaspersky Security for Mobile は次のコンポーネントの動作に対して Kaspersky Security Network クラウドサービスを使用します：

- **アンチウイルス：**本アプリはカスペルスキーのオンラインナレッジベースへアクセスし、ファイルやアプリに関する評価の情報を取得します。定義データベースには追加されていないが、KSN では確認できる情報を持つ脅威に対して、このスキャンが実行されます。Kaspersky Security Network クラウドサービスにより、アンチウイルスの機能が制限なく発揮され、また誤検知の可能性も低減されます。

- **危険サイトブロック：**KSN から取得したデータを使用して、Web サイトが開かれる前にそのサイトに対してスキャンを実行します。また、Web サイトのカテゴリを判別し、許可するカテゴリとブロックするカテゴリのリストに基づいてユーザーのインターネットアクセスを制御します（たとえば、「インターネットコミュニケーション」カテゴリなど）。

- **アプリ管理：**アプリのカテゴリを判別し、許可するカテゴリとブロックするカテゴリのリストに基づいて、企業のセキュリティ要件を満たさないアプリの開始を制限します（たとえば「ゲーム」カテゴリなど）。

アンチウイルスおよびアプリ管理の動作中、KSN を使用している時にカスペルスキーに送信されるデータの種別に関する情報は、使用許諾契約書に記載されています。使用許諾契約書の諸条項に同意すると、この情報の送信に同意したことになります。

危険サイトブロックの動作中、KSN を使用している時にカスペルスキーに送信されるデータの種別に関する情報は、データ処理に関する声明に記載されています。声明の諸条項に同意すると、この情報の送信に同意したことになります。

情報セキュリティの脅威、侵入の脅威、検知しにくい脅威の出現を（それぞれの発生源と共に）検知するため、デバイスで保存、処理される情報の保護を向上するため、Kaspersky Security Network に参加し、さらに統計情報を Kaspersky Security Network に送信するように設定できます。

本アプリのパフォーマンスの向上を目的として、KSN とデータを交換するには、次の条件を満たす必要があります：

- Kaspersky Security Network に関する声明に管理者またはデバイスユーザーが同意する必要があります。ユーザーによる声明の同意を必要とする選択をした場合、ユーザーが使用する本アプリのメイン画面に、声

明の条項への同意を要求する通知が表示されます。ユーザーは、本アプリの設定の［**製品情報**］セクションから声明に同意することもできます。

声明にグローバルに同意することを選択した場合、Kaspersky Security Center を使用して同意する声明のバージョンが、ユーザーが同意済みである声明のバージョンと一致する必要があります。一致しない場合、ユーザーにその問題が通知され、管理者がグローバルに同意した声明と同じバージョンの声明への同意が要求されます。Kaspersky Security for Mobile (Devices) プラグインのデバイスステータスも、「*警告*」に変更されます。

- グループポリシーの設定で、KSN への統計情報の送信を許可するように設定する必要があります。

Kaspersky Security Network への統計情報の送信はいつでも停止できます。Kaspersky Endpoint Security for Android モバイルアプリの動作中、KSN の使用時にカスペルスキーに送信されるデータの種別に関する情報は、使用許諾契約書に記載されています。

KSN へのデータ提供の詳細は、「データ提供」セクションを参照してください。

KSN へのデータの提供は任意です。必要に応じて、KSN とのデータ交換を無効にすることができます。

Kaspersky Security Network の使用の有効化と無効化

Kaspersky Security Network を使用する Kaspersky Endpoint Security for Android コンポーネントを動作させる目的で、本アプリはクラウドサービスにリクエストを送信します。リクエストは、「データ提供」セクションに記載されたデータを含んでいます。

Kaspersky Security Network の使用がデバイスで無効になると、クラウドプロテクション、危険サイトブロック、アプリ管理の各コンポーネントも自動で無効になります。

Kaspersky Security Network の使用を有効または無効にするには：

1. Kaspersky Endpoint Security for Android がインストールされているモバイルデバイスの管理ポリシーの設定ウィンドウを開きます。
2. ポリシーの**プロパティ**ウィンドウで、［**詳細**］セクションを選択します。
3. ［**Kaspersky Security Network（KSN）への参加の設定**］セクションで、Kaspersky Security Network の使用に関する設定を指定します：
   - ［**Kaspersky Security Network を使用する**］をオンにして、次のコンポーネントの動作を設定します：アンチウイルス（クラウドプロテクション）、危険サイトブロック、アプリ管理（アプリのカテゴリ）。
   - ［**KSN への統計情報の送信を許可する**］をオンにすると、データがカスペルスキーに送信されます。このデータにより、Kaspersky Endpoint Security for Android による脅威への対応がより早くなり、保護コンポーネントのパフォーマンスが向上し、誤検知の可能性も低減されます。
4. ［**適用**］をクリックして、変更を保存します。

モバイルデバイスと Kaspersky Security Center との次回の同期時に、デバイスに設定が適用されます。ポリシーが適用されると、Kaspersky Security Network を使用するコンポーネントが無効になり、コンポーネントの設定も行えなくなります。

Kaspersky Private Security Network を使用する

Kaspersky Private Security Network（以降「*プライベート KSN*」または「*KPSN*」とも表記）は、Kaspersky Security Network の評価データベースへのアクセスを許可しますが、ユーザーデバイスから Kaspersky Security Network へデータは送信されません。

Kaspersky Private Security Network サーバーにはオブジェクト（ファイルまたは URL）のデータベースが保管されますが、Kaspersky Security Network サーバーには保管されません。KPSN 評価データベースは、企業ネットワーク内に保管され、企業の管理者が管理します。

KPSN を有効にすると、Kaspersky Endpoint Security はユーザーデバイスから KSN へ統計データを送信しません。

Kaspersky Security Center でプライベート KSN の使用を有効にするには：

1. Kaspersky Security Center Web コンソールまたは Cloud コンソールのメインウィンドウで、**設定**（）をクリックします。

   管理サーバーのプロパティウィンドウが表示されます。

2. ［**全般**］タブで、［**KSN プロキシ設定**］セクションを選択します。

3. 切り替えスイッチを［**Kaspersky Private Security Network の使用が［有効］です**］に切り替えます。

4. ［**KSN プロキシの設定ファイルを選択**］をクリックし、拡張子が pkcs7 または pem の設定情報ファイル（カスペルスキーから提供されます）を選択します。

5. ［**開く**］をクリックします。

6. 管理サーバーのプロパティでプロキシサーバーの設定を編集しているがネットワーク構成によりプライベート KSN への直接アクセスが必要な場合は、［**プライベート KSN への接続時に KSC プロキシサーバーの設定を無視する**］をオンにします。有効にしないと、管理対象アプリケーションからのリクエストが プライベート KSN へ到達できません。

7. ［**Save**］をクリックします。

設定のダウンロード後、プロバイダー名と連絡先、ファイルの作成日がプライベート KSN の設定とともにインターフェイスに表示されます。KPSN 設定がモバイルデバイスに適用されます。

プライベート KSN へ切り替えると、グローバル KSN の使用時に使用可能なアプリのカテゴリがアプリ管理でサポートされなくなります。アプリのカテゴリは、KSN へ切り替えると使用可能になります。

サードパーティのサービスへのデータ提供

Kaspersky Endpoint Security for Android は、Google™ のサービスである Firebase Cloud Messaging、Firebase 向け Google Analytics、SafetyNet Attestation、Firebase Performance Monitoring、Crashlytics を使用しています。Kaspersky Endpoint Security for Android は、Firebase Cloud Messaging（FCM）サービスを使用して、ポリシーの設定が変更された時にコマンドや強制同期をタイムリーに実行します。Kaspersky Endpoint Security for Android は、Firebase Cloud Messaging、Firebase 向け Google Analytics、SafetyNet Attestation、Firebase Performance Monitoring、Crashlytics サービスを使用し、本アプリのパフォーマンスを向上させたり、カスペルスキーがより効果的なマーケティング資料を作成できるように協力したりします。

Firebase Cloud Messaging との情報交換

Kaspersky Endpoint Security for Android は、Firebase Cloud Messaging（FCM）サービスを使用して、ポリシーの設定が変更された時にコマンドや強制同期をタイムリーに実行します。また、プッシュ通知も使用します。

Firebase Cloud Messaging サービスを使用するには、Kaspersky Security Center でこのサービスを設定する必要があります。Kaspersky Security Center での Firebase Cloud Messaging の設定の詳細については、*Kaspersky Security Center のヘルプ*を参照してください。Firebase Cloud Messaging の設定が行われていない場合、モバイルデバイスのコマンドは、ポリシーで設定されたスケジュールに従ってデバイス と Kaspersky Security Center が同期される時に実行されます（たとえば 24 時間ごと）。つまり、コマンドやポリシーの設定は、すぐには反映されません。

本アプリの主要な機能をサポートする目的で、本アプリのインストールの一意な識別子（インスタンス ID）と次のデータを Firebase Cloud Messaging サービスに自動的に提供することにお客様は同意するものとします：

- インストールされた本ソフトウェアに関する情報：アプリのバージョン、アプリの識別子、アプリのビルドバージョン、アプリのパッケージ名。
- 本ソフトウェアがインストールされた端末に関する情報：OS バージョン、デバイスの識別子、Google サービスのバージョン。
- FCM に関する情報：FCM 内のアプリの識別子、FCM のユーザーの識別子、プロトコルのバージョン。

データはセキュアな通信で Firebase サービスへ転送されます。情報へのアクセスと保護は、Firebase サービスの利用に対応する条件により規制されます：https://firebase.google.com/terms/data-processing-terms/ 、https://firebase.google.com/support/privacy/

Firebase Cloud Messaging サービスとの情報交換を停止するには：

1. コンソールツリーで、［**モバイルデバイス管理**］→［**モバイルデバイス**］の順に選択します。
2. ［**モバイルデバイス**］フォルダーのコンテキストメニューから［**プロパティ**］を選択します。
3. ［**モバイルデバイス**］フォルダーのプロパティウィンドウで、［**Google Firebase Cloud Messaging 設定**］セクションを選択します。
4. ［**設定をリセット**］をクリックします。

Firebase 向け Google アナリティクス、SafetyNet Attestation、Firebase Performance Monitoring、Crashlytics との情報交換

以前のバージョンの管理プラグインを使用し、Google アナリティクスサービスとのデータ交換を有効にしている場合、Kaspersky Endpoint Security for Android Service Pack 4 Maintenance Release 3 は Firebase 向け Google アナリティクスサービスとのデータ交換を実行します。Google アナリティクスのサポートは終了しました。

Kaspersky Security for Mobile による Firebase 向け Google アナリティクス、SafetyNet Attestation、Firebase Performance Monitoring、Crashlytics サービスとの情報交換の目的は次の通りです：

- 本アプリのパフォーマンスの向上

  本アプリのパフォーマンスの向上を目的として、Firebase 向け Google アナリティクス、SafetyNet Attestation、Firebase Performance Monitoring、Crashlytics サービスと情報交換するには、次の条件を満たす必要があります：

  - Kaspersky Security Network に関する声明に管理者またはモバイルデバイスユーザーが同意する。ユーザーによる声明の同意を必要とする選択をした場合、ユーザーが使用する本アプリのメイン画面に、声明の条項への同意を要求する通知が表示されます。ユーザーは、本アプリの設定の［**製品情報**］セクションから声明に同意することもできます。

    声明にグローバルに同意することを選択した場合、Kaspersky Security Center を使用して同意する声明のバージョンが、ユーザーが同意済みである声明のバージョンと一致する必要があります。一致しない場合、ユーザーにその問題が通知され、管理者がグローバルに同意した声明と同じバージョンの声明への同意が要求されます。Kaspersky Security for Mobile (Devices) プラグインのデバイスステータスも、「*警告*」に変更されます。

  - グループポリシーの設定で、KSN への統計情報の送信を許可するように管理者が設定する（下図を参照）。

- カスペルスキーがより効果的なマーケティング資料を作成できるように協力する。

  カスペルスキーによる効果的なマーケティング資料の作成に協力する目的で Firebase 向け Firebase 向け Google アナリティクス、SafetyNet Attestation、Firebase Performance Monitoring、Crashlytics サービスと情報交換するには、次の条件を満たす必要があります：

  - 管理者またはモバイルデバイスユーザーが、マーケティング目的に沿ったデータ処理に関する声明の条項を確認して同意する。ユーザーによる声明の同意を必要とする選択をした場合、ユーザーは本アプリのインストール時に声明の条項に同意できます。またはインストール後に本アプリの設定の［**製品情報**］セクションから同意することもできます。

  - Firebase 向け Google アナリティクス、SafetyNet Attestation、Firebase Performance Monitoring、Crashlytics へのデータの送信をグループポリシーで許可するように管理者が設定する必要があります（下を参照）。

マーケティング目的に沿ったデータ処理に関する声明に基づく Firebase 向け Google アナリティクス、SafetyNet Attestation、Firebase Performance Monitoring、Crashlytics へのデータ提供

権利者はサードパーティの事業者の情報環境を使用してデータを処理します。このようなサードパーティ事業者の情報環境によるデータ処理は、サードパーティの情報環境に適用されるプライバシー声明によって規定されています。権利者が使用するサービスと、処理するデータは次の通りです：

Firebase 向け Google アナリティクス

本ソフトウェアの使用中に、次に記載する目的のため、次のデータが定期的に Firebase 向け Google アナリティクスに自動送信されます：

- アプリ情報（アプリのバージョン、アプリの識別子、Firebase サービスのアプリの識別子、Firebase サービスのインスタンス ID、製品を入手した店舗の名前、ソフトウェアを最初に起動した日時）
- デバイスへの製品のインストールの ID とデバイスへのインストールの方法。
- 地域と使用言語に関する情報
- デバイスの画面解像度に関する情報
- ルートを取得しているユーザーに関する情報
- SafetyNet Attestation サービスによる端末に関する診断情報
- ユーザー補助機能としての Kaspersky Endpoint Security for Android の設定に関する情報
- アプリケーションスクリーンの遷移、セッションの長さ、スクリーンセッションの開始および終了、スクリーン名に関する情報
- Firebase サービスへのデータの送信に使用されるプロトコル、バージョン、使用されるデータ送信方法の識別子に関する情報
- データが提供されるイベントの種別とパラメータの詳細
- 本アプリのライセンスとその使用可否、デバイスの数に関する情報
- 定義データベースのアップデート頻度、および管理サーバーとの同期の頻度に関する情報
- 管理コンソールに関する情報（Kaspersky Security Center またはサードパーティ製の EMM システム）
- Android ID
- 広告識別子（Advertising ID）
- ユーザーに関する情報： 年齢カテゴリと性別、居住国の識別子、関心のリスト
- 本ソフトウェアがインストールされた端末に関する情報： 端末の製造元の名前、端末の種別、型番、オペレーティングシステムのバージョンおよび言語（地域）、本ソフトウェアが最近の 7 日間またはそれ以前に初回起動されたかに関する情報

  データはセキュアな通信で Firebase に転送されます。データが Firebase でどのように処理されるかの詳細は、次を参照してください：https://firebase.google.com/support/privacy

SafetyNet Attestation

本ソフトウェアの使用中に、本声明に記載の目的で、次のデータが定期的に自動で SafetyNet Attestation 宛てに送信されます：

- デバイスを確認する時間

- 本アプリに関する情報、本アプリの証明書の名前とデータ
- デバイスの確認結果
- デバイスの確認結果を検証するためのランダムな識別子チェック

  データはセキュアな通信で SafetyNet Attestation に転送されます。SafetyNet Attestation においてデータがどのように処理されるかの情報は、次を参照してください：https://policies.google.com/privacy

Firebase Performance Monitoring

本ソフトウェアの使用中に、以下に記載する目的のため、次のデータが定期的に Firebase Performance Monitoring に自動で送信されます：

- 本ソフトウェアのインストールの一意な識別子
- 本ソフトウェアのパッケージ名
- インストールされた本ソフトウェアのバージョン
- バッテリーレベルおよびバッテリー充電状態
- 通信事業者
- アプリがフォアグラウンドかバックグラウンドかの状態
- 地域
- IP アドレス
- 端末の言語コード
- 電波の受信状況およびデータ通信の接続状況に関する情報
- 匿名化されたソフトウェアのインスタンスの識別子
- RAM およびディスクサイズ
- 端末がジェイルブレイクまたはルート化されているかを示すフラグ
- 信号強度
- 自動トレースの期間
- ネットワーク、および次に対応する情報： 応答コード、ペイロードのサイズ（バイト）、応答時間
- 端末の説明

  データはセキュアな通信で Firebase Performance Monitoring に転送されます。Firebase Performance Monitoring においてデータがどのように処理されるかの情報は、次を参照してください：https://firebase.google.com/support/privacy

Crashlytics

本ソフトウェアの使用中に、以下に記載する目的のため、次のデータが定期的に Crashlytics に自動で送信されます：

- ソフトウェア識別子

- インストールされた本ソフトウェアのバージョン
- 本ソフトウェアがバックグラウンドで実行しているかどうかを示すフラグ
- CPU アーキテクチャ
- イベントの一意な識別子
- イベントの日時
- 端末の機種
- ディスク容量の合計および現在の使用量
- OS の名前およびバージョン
- 合計 RAM および現在の使用量
- 端末がルート化されているかを示すフラグ
- イベント時の画面の向き
- 製品または端末の製造元
- 本ソフトウェアのインストールの一意な識別子
- 送信中の統計情報のバージョン
- 本ソフトウェアのインストール種別
- エラーメッセージ本文
- 本ソフトウェアの例外が、例外のネストによって発生したかどうかを示すフラグ
- スレッド ID
- フレームが本ソフトウェアのエラーの原因であるかどうかを示すフラグ
- 本ソフトウェアの予期しない終了の原因となったスレッドを示すフラグ
- 本ソフトウェアの予期しない終了の原因となった信号に関する情報： 信号の名前、信号のコード、信号のアドレス
- スレッド、例外、エラーに関連付けられた各フレーム： フレームファイルの名前、フレームファイルの行番号、デバッグ記号、バイナリイメージ内のアドレスおよびオフセット、フレームを含むライブラリの表示名、フレームの種別、フレームがエラーの原因かどうかを示すフラグ
- OS の識別子
- イベントに関連付けられた問題の識別子
- 本ソフトウェアが予期せず終了する前に発生したイベントに関する情報： イベントの識別子、イベントの日時、イベントの種別と値
- CPU レジスタ値

- イベントの種別と値

  データはセキュアな通信で Crashlytics に転送されます。Crashlytics においてデータがどのように処理されるかの情報は、次を参照してください：https://firebase.google.com/terms/crashlytics-app-distribution-data-processing-terms

上記の情報をマーケティング目的で処理するために提供するかどうかは任意です。

Firebase 向け Google アナリティクス、SafetyNet Attestation、Firebase Performance Monitoring、Crashlytics サービスとのデータ交換を無効にするには：

1. Kaspersky Endpoint Security for Android アプリがインストールされているモバイルデバイスの管理ポリシーの設定ウィンドウを開きます。
2. ポリシーの**プロパティ**ウィンドウで、［**詳細**］セクションを選択します。
3. ［**データ転送**］セクションで、［**データ転送の許可により、本アプリの品質、デザイン、パフォーマンスの改善にご協力いただけると幸いです**］をオフにします。
4. ［**適用**］をクリックして、変更を保存します。

モバイルデバイスと Kaspersky Security Center との次回の同期時に、デバイスに設定が適用されます。

追加声明へのグローバルな同意

Kaspersky Endpoint Security for Android による保護を有効にするには、使用許諾契約書と追加声明（下を参照）の条項に同意する必要があります。全ユーザーのためにグローバルに同意するようにポリシーを設定できます。グローバルに同意された次の契約書と声明の条項を確認し同意するように、ユーザーが要求されることはありません：

- Kaspersky Security Network に関する声明
- 危険サイトブロックの使用を目的としたデータ処理に関する声明
- マーケティング目的に沿ったデータ処理に関する声明

声明にグローバルに同意することを選択した場合、Kaspersky Security Center を使用して同意する声明のバージョンが、ユーザーが同意済みである声明のバージョンと一致する必要があります。一致しない場合、ユーザーにその問題が通知され、管理者がグローバルに同意した声明と同じバージョンの声明への同意が要求されます。Kaspersky Security for Mobile (Devices) プラグインのデバイスステータスも、「*警告*」に変更されます。

条項にグローバルに同意するか、グループポリシーを適用してユーザーが同意するかを選択するには：

1. コンソールツリーの［**管理対象デバイス**］フォルダーで、デバイスが属する管理グループを選択します。
2. 選択したグループの作業領域で、［**ポリシー**］タブを選択します。
3. 任意の列をダブルクリックして、ポリシーのプロパティウィンドウを開きます。
4. ポリシーの**プロパティ**ウィンドウで、［**詳細**］セクションを選択します。

5. ［**データ転送**］セクションで、マーケティング目的に沿ったデータ処理に関する声明への同意を、グローバルかユーザーごとかを選択します。

6. ［**Kaspersky Security Network（KSN）への参加の設定**］セクションで、Kaspersky Security Network に関する声明に、グローバルに同意するかユーザーが同意するかを選択します。

7. ［**適用**］をクリックして、変更を保存します。

声明に同意するかどうかは、Kaspersky Endpoint Security for Android の［**製品情報**］セクションで、いつでも選択できます。

Samsung KNOX

Samsung KNOX は、Android オペレーティングシステムを実行する Samsung モバイルデバイスを設定し保護するモバイルソリューションです。Samsung KNOX の詳細については、*Samsung のテクニカルサポートサイト* を参照してください。

KNOX Mobile Enrollment を使用した Kaspersky Endpoint Security for Android アプリのインストール

KNOX Mobile Enrollment (KME) は、Samsung KNOX モバイルソリューションの一部です。KNOX Mobile Enrollment は、承認済みリセラーから購入した Samsung デバイスへのアプリのインストールと初期設定を一括で処理するのに使用されます。

Kaspersky Endpoint Security for Android アプリを KNOX Mobile Enrollment を使用してインストールするには、次のステップを実行します：

1. **Kaspersky Endpoint Security for Android アプリの KNOX MDM プロファイルの作成**
2. **KNOX Mobile Enrollment でのデバイスの追加**
3. **ユーザーのモバイルデバイスに Kaspersky Endpoint Security for Android アプリをインストール**

KNOX Mobile Enrollment の詳細は、*KNOX Mobile Enrollment User Guide* を参照してください。

KNOX Mobile Enrollment を使用した導入は、Samsung デバイスでのみ使用可能です。詳細は、*Samsung のテクニカルサポートサイト* を参照してください。

KNOX MDM プロファイルの作成

KNOX MDM プロファイルは、アプリへのリンクが含まれており、モバイルデバイスへのアプリの導入と初期設定が簡単にできます。

KNOX MDM プロファイルを作成するには：

1. Samsung KNOX コンソールへログインし、**KNOX Mobile Enrollment** を選択します。
2. ［**MDM profiles**］を選択します。

3. ［**追加**］をクリックします。

   KNOX MDM Profile Wizard が開始されます。

4. ［**MDM server connection**］で、［**Server URI is not required for my MDM service**］を選択し、［**Next**］をクリックします。

5. ［**MDM profile info**］で、次の手順を実行します：

   a. KNOX MDM プロファイルの次の一般的な情報を入力します：**プロファイル名**、**説明**。

   b. ［**Add MDM apps**］をクリックし、APK インストールファイルのパスを入力します。

   Kaspersky Endpoint Security for Android のインストールファイルは、Kaspersky Security for Mobile 配布キットに含まれています。事前に、Kaspersky Security Center Web サーバー、またはデバイスからアクセス、ダウンロード可能な他の場所に、APK インストールファイルを配置しておいてください。

   c. Kaspersky Security Center にデバイスを接続するための情報を［**JSON user data**］フィールドに次の形式で入力します：
   `{"serverAddress":"ksc.server.com","serverPort":"12345","groupName":"MOBILE GROUP"}`。

   本アプリをアクティベートし、デバイスを設定し、コマンドを送信するには、デバイスが Kaspersky Security Center に接続されている必要があります。

   d. ［**Add Knox agreements**］をオンにします。

   Kaspersky Endpoint Security for Android を KNOX Mobile Enrollment を使用してインストールするには、モバイルデバイスのユーザーが Samsung の使用許諾契約の諸条件に同意する必要があります。Samsung の使用許諾契約の諸条件は、［**End User License Agreements, Terms of Service, and User Agreements**］というセクションで確認できます。KNOX MDM プロファイルの導入に必要な、その他の自社の法的文書は、［**Add user agreement**］をクリックして追加できます。

   e. ［**Bind Knox license to this profile**］をオフにします。

   Samsung KNOX のライセンス情報は、Kaspersky Security Center とモバイルデバイスの同期時に、ポリシーと一緒にデバイスに送信されます。

6. ［**Save**］をクリックします。

これにより、Kaspersky Endpoint Security for Android アプリの情報が追加された KNOX MDM プロファイルが、KME コンソールのリストに追加されます。

KNOX Mobile Enrollment でのデバイスの追加

KNOX Mobile Enrollment (KME) コンソールを使用して、次の方法でデバイスを追加できます：

- デバイスの購入後に、リセラーの手により KME コンソールで自動的にデバイスを追加する。

  Samsung デバイスの承認済みリセラーが自分の組織と協業関係にある場合は、この方法を選択できます。

- 管理者が KNOX Deployment アプリを Google Play からモバイルデバイスへインストールし、KNOS MDM プロファイルをユーザーのデバイスへ移行する（Bluetooth または Near Field Communication（NMC）を使用して移行）KNOX MDM プロファイルの導入後、デバイスが自動的に KME コンソールに追加されます。

  承認済みリセラー以外から Samsung デバイスを購入した場合は、この方法を選択できます。

リセラーによるデバイスの追加

Samsung デバイスの承認済みリセラーが Samsung KNOX に登録されています。詳細は、*Samsung のテクニカルサポートサイト*をご参照ください。デバイスの購入後すぐに、リセラーが自動的にデバイスを KME コンソールに追加し、購入者の Samsung アカウントに反映されます。リセラーによるデバイスの追加には、KME コンソールでリセラーを購入者の Samsung アカウントに登録する必要があります。Samsung デバイスのリセラーを KME コンソールで追加するには、リセラー ID が必要です。リセラー ID を受け取るには、リクエストをリセラーに送信する必要があります。リクエストに、自分の KNOX クライアント ID を指定してください。

自分の KNOX クライアント ID を表示するには：

1. Samsung KNOX コンソールへログインし、**KNOX Mobile Enrollment** を選択します。
2. ［**Reseller**］セクションを選択します。
3. ［**KNOX client ID**］フィールドに、ID が表示されています。

リセラーから、リセラー ID に関する返答を受け取った後、リセラーを KME コンソールで登録します。リセラーの登録前に、KNOX MDM プロファイルを作成し、新しいデバイスの追加時にプロファイルが自動的に導入されるようにすることができます。

承認済みリセラーを KME コンソールで登録するには：

1. Samsung KNOX コンソールへログインし、**KNOX Mobile Enrollment** を選択します。
2. ［**Reseller**］セクションを選択します。
3. ［**Register reseller**］をクリックします。
   リセラーを登録するウィンドウが開きます。
4. ［**Reseller Id**］フィールドに、受け取った Samsung デバイスの承認済みリセラーの ID を入力します。
5. KNOX MDM プロファイルを作成済みの場合、KNOX MDM プロファイルをリセラーの登録ウィンドウで選択します。
   新しいデバイスの追加時に、KNOX MDM プロファイルが自動的にインストールされます。
6. ［**Preferred download confirmation method**］リストで、デバイスの追加方法を選択しリセラーに確認します。
   - **All downloads must be confirmed**：リセラーによるデバイスの追加時に、操作を確認する必要があります。
   - **Automatically confirm all downloads of this reseller**：リセラーによりデバイスが自動的に KME コンソールに追加されます。
7. ［**OK**］をクリックします。

Samsung デバイスのリセラーが、KME コンソール上のリセラーのリストに追加されます。

新しいデバイスを承認済みリセラーから購入した後、インターネットに接続されたデバイスに Kaspersky Endpoint Security for Android が自動的にインストールされます。KNOX Mobile Enrollment の詳細は、*KNOX Mobile Enrollment User Guide を参照してください*。KME コンソール上にデバイスのリストが存在する場合は、KNOX MDM プロファイルと KNOX MDM アプリをデバイスに追加します。

KNOX MDM プロファイルをデバイスに配信するには：

1. Samsung KNOX コンソールへログインし、**KNOX Mobile Enrollment** を選択します。

2. ［**Devices**］-［**All devices**］の順に選択します。

3. KNOX MDM プロファイルをインストールするデバイスを選択します。

4. ［**Configure**］をクリックします。
［**Device info**］ウィンドウが開きます。

5. ［**MDM profile**］リストで、Kaspersky Endpoint Security for Android アプリの情報が含まれる KNOX MDM プロファイルを選択します。

6. ［**Tags**］フィールドで、デバイスのグループ化やラベルの付与に使用するタグを入力し、KME コンソール上で最適化されるように調整します。

7. デバイスのユーザーアカウントの認証情報を、［**User ID**］と［**Password**］のフィールドに入力します。
アカウントの認証情報は、証明書の受信に必要です。ユーザー ID とパスワードは、Kaspersky Security Center のユーザーアカウントの認証情報（ユーザーアカウントのプロパティの［名前］と［パスワード］）と一致する必要があります。

8. 残りのデバイス用の KNOX MDM プロファイルを選択します。

9. ［**Save**］をクリックします。

デバイスがインターネットに接続されると、KNOX MDM プロファイルのインストールを要求する通知が表示されます。

KNOX Deployment アプリを使用したデバイスの追加

Samsung デバイスを承認済みリセラーから購入していない場合は、Bluetooth または NFC を使用してデバイスを KNOX Mobile Enrollment に追加できます。この追加方法には、ユーザーのモバイルデバイスへの KNOX MDM プロファイルの配信に使用する管理者用のモバイルデバイスが必要です。

KNOX Deployment アプリを使用してデバイスを追加するには、次の条件を満たす必要があります：

- 選択した配信方法に応じて、Bluetooth または NFC モジュールがモバイルデバイスで有効にされている。
- モバイルデバイスがインターネットに接続している。

KNOX MDM プロファイルを KNOX Deployment アプリを使用して配信するには：

1. KNOX Deployment アプリを Google Play から管理者用モバイルデバイスにインストールします。

2. KNOX Deployment アプリを起動します。

3. Samsung アカウントの認証情報を入力します。

4. ［**KNOX Deployment**］ウィンドウで、KNOX MDM プロファイルの導入設定を指定します：

   - KNOX MDM プロファイルを選択します。
   - 導入方法を次から選択します：**Bluetooth** または **NFC**。
     Bluetooth を使用する場合、KNOX MDM プロファイルを複数の端末に同時に追加できます。

5. ［**Start deployment**］をクリックします。

- **Bluetooth**：ユーザーのモバイルデバイスで、https://configure.samsungknox.com を開きます。

  Samsung KNOX Device Registration Wizard が開始されます。画面の指示に従います。

  KNOX MDM プロファイルのインストール後、［**Bluetooth**］タグが KME コンソールに追加されます。

- **NFC**：管理者用モバイルデバイスをユーザーのモバイルデバイスに近づけ、KNOX MDM プロファイルを転送します。

  ユーザーのモバイルデバイス上に、KNOX MDM プロファイルのインストールを要求する通知が表示されます。［**NFC**］タグが KME コンソールに追加されます。

本アプリのインストール

Kaspersky Endpoint Security for Android アプリのインストール前に、 モバイルデバイスユーザー向けの証明書を、Kaspersky Security Center 管理コンソールで発行します。証明書は、Kaspersky Security Center 管理コンソールで、モバイルデバイスユーザーを特定するのに必要です。

KNOX MDM プロファイルの導入の開始後、APK インストールファイルがモバイルデバイスに自動的にダウンロードされます。Kaspersky Endpoint Security for Android アプリのインストールが自動的に開始されます。Samsung KNOX および Kaspersky Endpoint Security for Android の使用許諾契約書に同意する必要があります。本アプリに対して、追加で設定する必要がある項目はありません本アプリのインストール後、Kaspersky Security Center との同期が自動的に開始されます。モバイルデバイスが、KNOX MDM プロファイルの設定 (`groupName`)で指定された管理グループ名で Kaspersky Security Center 管理コンソールに追加されます。

KNOX コンテナーの設定

このセクションでは、Android の Samsung デバイスでの KNOX コンテナーの使用方法について説明します。

KNOX コンテナーは、Android バージョン 6.0 以降の Samsung デバイスでのみ使用できます。

KNOX コンテナーについて

*KNOX コンテナー*は、独自のデスクトップ、起動パネル、アプリ、ウィジェットを持つ、ユーザーのデバイス上の安全な環境です。KNOX コンテナーにより、企業のアプリとデータを個人のアプリとデータから分離できます。KNOX コンテナーは、Samsung KNOX モバイルソリューションのコンポーネントです。

Samsung KNOX は、Android オペレーティングシステムを実行する Samsung モバイルデバイスを設定し保護するモバイルソリューションです。Samsung KNOX の詳細については、*Samsung のテクニカルサポートサイト* を参照してください。

KNOX コンテナーにより、モバイルデバイスで個人データと企業データを分けることができます。たとえば、個人のメールボックスを使用して KNOX コンテナーに配置されているファイルを送信することはできません。社員の個人所有のモバイルデバイスを企業データの作業に使用する場合は、KNOX コンテナーを導入することを推奨します。

KNOX コンテナーを使用するには、Samsung KNOX をアクティベートする必要があります。デバイスを Kaspersky Security Center と同期した後、モバイルデバイスのユーザーは KNOX コンテナーのインストールを求められます。KNOX コンテナーをインストールする前に、ユーザーは Samsung からの使用許諾契約書に同意する必要があります。

KNOX コンテナーをインストールすると、KNOX アイコン  がモバイルデバイスのデスクトップに追加されます。または、作業領域がモバイルデバイスのアプリのリストに追加されます。企業データで作業するには、ユーザーは KNOX コンテナーからアプリを起動する必要があります。

Kaspersky Endpoint Security for Android が KNOX コンテナーにインストールされておらず、企業データが保護されていません。Kaspersky Endpoint Security for Android は KNOX コンテナーにダウンロードされた悪意のあるファイルを検知せず、悪意のあるサイトをブロックしません。KNOX コンテナー内でアプリの起動を制御したり、カメラの使用を禁止したりすることはできません。Kaspersky Endpoint Security for Android は、個人データのみを保護します。企業データは Samsung KNOX ツールを使用して保護できます。Samsung KNOX の詳細については、*Samsung のテクニカルサポートサイト*を参照してください。

Samsung KNOX のアクティベーション

ユーザーのモバイルデバイスで KNOX コンテナーを使用するには、Samsung KNOX をアクティベートする必要があります。Samsung KNOX のアクティベート手順は、ユーザーデバイスにインストールされた Kaspersky Endpoint Security for Android バージョンによって異なります：

- Kaspersky Endpoint Security for Android の最新バージョンがデバイスにインストールされている場合、Samsung KNOX のアクティベーションにライセンスは必要ありません。
- Kaspersky Endpoint Security for Android の旧バージョン（10.8.3.174 以前）がデバイスにインストールされている場合、KNOX License Manager ライセンス（以降「KLM ライセンス」と表記）を Samsung から入手する必要があります。*KNOX License Manager ライセンス*は、Samsung KNOX ライセンスシステムによって使用される一意のコードです。KLM ライセンスの詳細については、Samsung KNOX のテクニカルサポートサイトを参照してください。

KNOX コンテナーは、Samusung デバイスでのみ使用可能です。

Samsung KNOX をアクティベートするには：

1. コンソールツリーの［**管理対象デバイス**］フォルダーで、デバイスが属する管理グループを選択します。
2. 選択したグループの作業領域で、［**ポリシー**］タブを選択します。
3. 任意の列をダブルクリックして、ポリシーのプロパティウィンドウを開きます。
4. ポリシーの**プロパティ**ウィンドウで、［**Samsung KNOX の管理**］→［**KNOX コンテナー**］セクションを順に選択します。
5. ［**KNOX License Manager ライセンス**］フィールドで、次を指定します：
   - Kaspersky Endpoint Security for Android の最新バージョンがデバイスにインストールされている場合、任意の文字を入力します。
   - Kaspersky Endpoint Security for Android の旧バージョン（10.8.3.174 以前）がデバイスにインストールされている場合、Samsung から受け取った KLM ライセンスを入力します。

6. 「ロック」アイコン をロック状態に設定します。

7. ［**適用**］をクリックして、変更を保存します。

Samsung KNOX は、デバイスと Kaspersky Security Center との次回の同期時にアクティベートされます。Samsung からの使用許諾契約書に同意し、KNOX コンテナーをインストールするように求められます。

Samsung KNOX のアクティベーションを解除するには：

1. コンソールツリーの［**管理対象デバイス**］フォルダーで、デバイスが属する管理グループを選択します。

2. 選択したグループの作業領域で、［**ポリシー**］タブを選択します。

3. 任意の列をダブルクリックして、ポリシーのプロパティウィンドウを開きます。

4. ポリシーの**プロパティ**ウィンドウで、［**Samsung KNOX の管理**］→［**KNOX コンテナー**］セクションを順に選択します。

5. ［**KNOX License Manager ライセンス**］フィールドの値をクリアします。

6. ［**適用**］をクリックして、変更を保存します。

デバイスと Kaspersky Security Center との次回の同期時に、Samsung KNOX のアクティベーションが解除されます。KNOX コンテナーへのアクセスはブロックされます。

Samsung KNOX の制限事項

- KNOX コンテナーは、Samusung デバイスでのみ使用可能です。
- KNOX 2.6、2.7、2.7.1 をサポートする Samsung デバイスでは、危険サイトブロックとアプリ管理が KNOX コンテナーで動作しません。この問題は、KNOX コンテナーで必要な権限が不足していることに関係しています（ユーザー補助機能サービス）。KNOX 2.8 以降をサポートするデバイスでは、本アプリの全コンポーネントを制限なしで使用できます。
- Kaspersky Endpoint Security for Android Service Pack 4 Maintenance Release 3 Update 2 よりも前のバージョンは、Samsung Android 10 デバイスで使用すると、Samsung KNOX のアップデートが原因で動作が不安定になる可能性があります。Kaspersky Endpoint Security for Android のバージョンを Service Pack 4 Maintenance Release 3 Update 2 にアップデートすることを推奨します。

KNOX でのファイアウォールの設定

KNOX コンテナーでネットワーク接続を監視するためのファイアウォールを設定する必要があります。

KNOX コンテナーでファイアウォールを設定するには：

1. コンソールツリーの［**管理対象デバイス**］フォルダーで、デバイスが属する管理グループを選択します。

2. 選択したグループの作業領域で、［**ポリシー**］タブを選択します。

3. 任意の列をダブルクリックして、ポリシーのプロパティウィンドウを開きます。

4. ポリシーの**プロパティ**ウィンドウで、［**Samsung KNOX の管理**］→［**KNOX コンテナー**］セクションを順に選択します。

5. ［**ファイアウォール**］ウィンドウで、［**設定**］をクリックします。
   ［**ファイアウォール**］ウィンドウが表示されます。

6. ファイアウォールのモードを選択します：

   - すべてのインバウンド接続とアウトバウンド接続を許可するには、スライダーを［**すべて許可**］まで移動します。
   - 除外リストのアプリを除くすべてのネットワーク活動をブロックするように設定する場合は、スライダーを［**すべてブロック（例外あり）**］まで移動させます。

7. ファイアウォールモードを［**すべてブロック（例外あり）**］に設定した場合は、除外リストを作成します：

   a. ［**追加**］をクリックします。
      ［**ファイアウォールで信頼するオブジェクト**］ウィンドウが開きます。

   b. ［**アプリの名前**］に、モバイルアプリの名前を入力します。

   c. ［**パッケージ名**］にモバイルアプリのパッケージのシステム名を入力します（例：`com.mobileapp.example`）。

   d. ［**OK**］をクリックします。

8. ［**適用**］をクリックして、変更を保存します。

モバイルデバイスと Kaspersky Security Center との次回の同期時に、デバイスに設定が適用されます。

KNOX での Exchange メールボックスの設定

KNOX コンテナーで企業のメール、連絡先、カレンダーを使用するには、Exchange メールボックスを設定する必要があります。

KNOX コンテナーで Exchange メールボックスを設定するには:

1. コンソールツリーの［**管理対象デバイス**］フォルダーで、デバイスが属する管理グループを選択します。

2. 選択したグループの作業領域で、［**ポリシー**］タブを選択します。

3. 任意の列をダブルクリックして、ポリシーのプロパティウィンドウを開きます。

4. ポリシーの**プロパティ**ウィンドウで、［**Samsung KNOX の管理**］→［**KNOX コンテナー**］セクションを順に選択します。

5. ［**Exchange ActiveSync**］ウィンドウで、［**設定**］をクリックします。
   ［**Exchange メールサーバーの設定**］ウィンドウが表示されます。

6. ［**サーバーのアドレス**］に、メールサーバーをホスティングしているサーバーの IP アドレスまたは DNS 名を入力します。

7. ［**ドメイン**］に、会社のネットワークでのモバイルデバイスユーザーのドメイン名を入力します。

8. ［**同期間隔**］ドロップダウンリストで、モバイルデバイスと Microsoft Exchange サーバーとの同期の間隔を選択します。

9. SSL（Secure Sockets Layer）データ転送プロトコルを使用する場合は、［**SSL 接続を使用する**］をオンにします。

10. モバイルデバイスと Microsoft Exchange サーバー間でのデータ転送を保護するためにデジタル証明書を使用する場合は、［**サーバー証明書を確認する**］をオンにします。

11. ［**適用**］をクリックして、変更を保存します。

モバイルデバイスと Kaspersky Security Center との次回の同期時に、デバイスに設定が適用されます。

付録

このセクションでは、このヘルプの補足情報を説明します。

グループポリシーの設定権限

Kaspersky Security Center の管理者は、様々なアプリケーション機能を対象とした管理コンソールユーザーのアクセス権限を、ユーザーの職務に応じて設定することができます。

各機能分野に対して、管理者は以下の権限を割り当てられます：

- **編集を許可する**：管理コンソールのユーザーは、プロパティウィンドウでポリシー設定を変更することができます。
- **編集をブロックする**：管理コンソールのユーザーは、プロパティウィンドウでポリシー設定を変更することができません。この権限が割り当てられている機能の範囲に属するポリシータブは、インターフェイスには表示されません。

Kaspersky Endpoint Security 管理プラグインの各セクションへのアクセス権限

機能の範囲	ポリシーのセクション
Android Enterprise	Android 仕事用プロファイル
盗難対策	盗難対策
アプリ管理	アプリ管理
プロテクション	プロテクション、スキャン、定義データベースのアップデート
コンプライアンスコントロール	コンプライアンスコントロール
コンテナー	コンテナー
デバイスの設定	デバイス管理、同期
Samsung デバイスの管理	APN、Samsung デバイスの管理、KNOX コンテナー
システム管理	詳細、Wi-Fi
危険サイトブロック	危険サイトブロック

Kaspersky Device Management for iOS 管理プラグインの各セクションへのアクセス権限

機能の範囲	ポリシーのセクション

詳細	Web クリップ、フォント、AirPlay、AirPrint
Exchange ActiveSync	全般、パスワード、同期、機能の制限、アプリの制限
全般	全般、シングルサインオン、危険サイトブロック、Wi-Fi、アクセスポイント名（APN）、Exchange ActiveSync、メール、カスタムペイロード
LDAP（カレンダー / 連絡先）	LDAP、カレンダー、連絡先、購読したカレンダー
制限 / セキュリティ	機能の制限、アプリケーションの制限、メディアコンテンツの制限、パスワード、VPN、グローバル HTTP プロキシ、証明書、SCEP

アプリのカテゴリ

アプリは、アプリ管理によってカテゴリに分類されます。アプリのカテゴリに対して設定された動作モードは、このカテゴリのすべてのアプリに適用されます。各アプリのカテゴリは、Kaspersky Security Network クラウドサービスによって決定されます。

アプリのカテゴリ

カテゴリ	説明
エンターテインメント	インタラクティブなエンターテインメントアプリ。
IM クライアント、モバイルメッセージングアプリ	インスタントメッセージアプリ、IP による音声および動画通信アプリ。
SNS	SNS やブログを使用するためのアプリ。
ビジネス用ソフト	税金計算アプリ、銀行業務の管理アプリ、表計算用アプリ、財務会計アプリなどのビジネス向けアプリ。テキストエディタ。
家庭、家族、ライフススタイル、健康	レシピアプリ、生活の知恵アプリ。エクササイズ用アプリ、運動のスケジュール管理アプリ、ダイエット、健康的な食生活、安全、事故防止に関するヒントのアプリ。
医療	症状や薬剤の一覧のアプリ、ヘルスケアの専門家向けアプリ、ヘルスケアの雑誌およびニュースのアプリ。
マルチメディア	映画の定額制サービス、メディアおよび動画の再生サービス。音楽サービス、プレーヤー、ラジオ放送。
グラフィックデザインソフト	カメラと一緒に使用するアプリ、グラフィックエディタ、写真の管理および公開アプリ。
ニュースフィードや RSS 用プラグイン	新聞、雑誌、ブログ、ニュースアグリゲーターの閲覧用アプリ。
天気	天気予報を表示するアプリ。
教育用ソフト	ブックリーダー、マニュアル、教科書、辞書、類語辞典、百科事典。試験勉強のサポートアプリ、トレーニング教材、辞書、発育用ゲーム、言語学習ツール。

オンラインショッピング	オンラインショッピングアプリ、オークション入札アプリ、ギフトクーポン、価格比較ツール、ショッピングリストアプリ、商品の口コミアプリ。
起動ツール	デスクトップ、ウィジェット、ショートカットの設定を変更するためのアプリ。
オペレーティングシステムとツール	オペレーティングシステム管理、ユーザーインタラクション、RAM 管理を提供するシステムアプリ。
地図表示アプリ	タウンガイド、地元の商業に関する情報、旅行計画作成ツール。
その他のソフトウェア	ソフトウェアのライブラリ、技術デモ版のアプリ。どのカテゴリにも含まれないアプリ。
輸送	公共交通機関を利用するためのアプリ、ナビツール、ドライバー向けアプリ。
ゲーム	アーケードゲーム、懸賞アプリ、レーシングゲーム、その他のゲーム、カジノゲーム、カードゲーム、音楽ゲーム、ボードゲーム、チュートリアル、パズルゲーム、アドベンチャーゲーム、ロールプレイングゲーム、シミュレーションゲーム、ワードゲーム、スポーツゲーム、戦略ゲーム、アクションゲーム。
ブラウザー	Web サイトの閲覧用アプリ、Web ドキュメントおよびファイルの内容を閲覧するためのアプリ。Web アプリケーションの管理用アプリ。
開発用ツール	ソフトウェアの開発用アプリ。デバッグ用アプリ、コンパイラ、コードエディタ、グラフィックユーザーインターフェイスエディタ。
ゴールデンイメージ	オペレーティングシステムと一緒に提供され、オペレーティングシステムが正常に動作するために必要なアプリ。
インターネットアプリ	ダウンロードマネージャー、メールクライアント、Web 検索アプリ、その他インターネットを快適に閲覧するためのアプリ。
ネットワーク環境用ソフト	サーバー管理アプリ、データ記憶装置管理アプリ、ネットワーク装置管理アプリ、会社のネットワーク内のソフトウェア管理アプリ、完全なインフラストラクチャの自動化および統合管理アプリ。
ネットワーキングソフト	複数のデバイスでのユーザーグループの協業を調整するアプリ、デバイス間での通信を調整するアプリ。
システムツール	ファイルマネージャー、アーカイブツール、ハードウェアおよびソフトウェアの診断ユーティリティ、メモリ最適化ツール、アンインストーラー、プロセッサ管理ユーティリティなど、オペレーティングシステムと同時に提供されるアプリ。
セキュリティソフト	デバイスデータの保護アプリ。デバイスの脅威を検知し無害化するアプリ。ファイアウォールデータの暗号化アプリ。
ダウンロードマネージャー	外部ソースからファイルをダウンロードするためのアプリ。
オンラインストレージソフト	ファイル、メモ、マルチメディアのオンラインでの保管を管理するためのアプリ。
辞書ソフト	ブックリーダー、マニュアル、教科書、辞書、類語辞典、ウィキ百科事典。
メールアプリ	メールメッセージの送受信に使用するアプリ。

Kaspersky Endpoint Security for Android の使用

このセクションでは、Kaspersky Endpoint Security for Android アプリでユーザーが使用可能な機能と動作について説明します。

このセクションの記事には、モバイルデバイスで使用または表示できるすべてのオプションが含まれています。本アプリの実際のレイアウトと動作は、実装されているリモート管理システムや、企業のセキュリティ要件に従って管理者がデバイスを設定する方法によって異なります。このセクションで説明する一部の機能とオプションは、アプリの実際のエクスペリエンスには適用されない場合があります。特定のデバイスの本アプリについて質問がある場合は、管理者にお問い合わせください。

アプリの機能

Kaspersky Endpoint Security で提供する主な機能は、次の通りです。

ウイルスやその他のマルウェアからの保護

アンチウイルスを使用して、ウイルスやその他のマルウェアからデバイスを保護します。

アンチウイルスは次の機能を実行します：

- デバイス全体、インストールされたアプリ、または選択されたフォルダーの脅威をスキャンする
- デバイスをリアルタイムで保護する
- 新しくインストールされたアプリを初めて起動する前にスキャンする
- 定義データベースをアップデートする

情報を収集し、処理する目的で送信するアプリがモバイルデバイスにインストールされている場合、Kaspersky Endpoint Security for Android によってマルウェアに分類される可能性があります。

アプリ管理

企業のセキュリティ要件に応じて、*リモート管理システムの管理者*（以降、「管理者」）は、推奨されるアプリ、ブロックされるアプリ、必須のアプリのリストを作成します。アプリ管理を使用して、推奨アプリと必須アプリのインストール、アップデート、およびブロックされたアプリの削除を行います。

アプリ管理では、配布パッケージへの直リンクまたは Google Play へのリンクから、推奨アプリと必須アプリをデバイスにインストールできます。アプリ管理では、企業のセキュリティ要件に違反してブロックされているアプリを削除できます。

アプリ管理を正常に動作させるには、Kaspersky Endpoint Security をユーザー補助機能として設定しておく必要があります。本アプリの初期設定ウィザードでこのサービスを有効にしなかった場合、該当の通知を選択すると表示される［**状態**］セクションや、デバイスの設定（Android の［**設定**］→［**ユーザー補助**］→［**サービス**］）でユーザー補助機能サービスとして Kaspersky Endpoint Security を有効にできます。

盗難または紛失時のデバイスデータの保護

盗難対策は、不正なアクセスからデータを保護し、デバイスの紛失時や盗難時にデバイスを見つけるのに役立ちます。

盗難対策では、次の操作を遠隔で実行できます：

- デバイスをロックする。

  ハッカーがデバイスロックを解除する可能性を防ぐために、Android 7.0 以降のモバイルデバイスでは、ユーザー補助機能サービスとして Kaspersky Endpoint Security を有効にしておく必要があります。

- デバイスのアラームを大音量で作動させる（デバイスの音量のオン/オフに関係なく）。
- デバイスの位置情報を取得する。
- デバイスに保存されているデータを消去する。
- 出荷時の既定値にリセットする。
- デバイスを使用している人物の顔写真をひそかに撮影する。

盗難対策の機能を有効にするには、Kaspersky Endpoint Security をデバイス管理者として有効にしておく必要があります。本アプリの初期設定時にデバイス管理者の権限を付与しなかった場合、該当の通知を選択すると表示される［**状態**］セクションや、デバイスの設定（Android の［**設定**］→［**セキュリティ**］→［**デバイス管理者**］）で Kaspersky Endpoint Security に管理者権限を付与できます（ご利用の端末によって、設定項目の表記が異なる場合があります）。

オンライン上の脅威からの保護

危険サイトブロックは、オンライン上の脅威から保護します。

危険サイトブロックは、悪意のあるコードを配信する Web サイトや、個人情報を盗んで金融機関のアカウントにアクセスする目的で設計されたフィッシングサイトをブロックします。危険サイトブロックは、Web サイトを開く前に、Kaspersky Security Network クラウドサービスを使用して、その Web サイトをスキャンします。

危険サイトブロックを有効にするには：

- Kaspersky Endpoint Security をユーザー補助機能サービスに設定しておく必要があります。
- また、危険サイトブロックの使用を目的としたデータ処理に関する声明（「危険サイトブロックに関する声明」）に同意する必要があります。Kaspersky Endpoint Security は、Kaspersky Security Network（KSN）

を Web サイトのスキャンに使用します。危険サイトブロックに関する声明は、KSN とのデータ交換に関する条件を含んでいます。

Kaspersky Security Center を使用して、管理者は危険サイトブロックに関する声明にユーザーの代わりに同意できます。この場合、ユーザーは何も操作する必要はありません。

危険サイトブロックに関する声明に管理者が同意せず、ユーザーに同意の要求を送信した場合は、本アプリ内の設定でユーザー自身が本声明に同意する必要があります。

危険サイトブロックに関する声明に管理者が同意しなかった場合は、危険サイトブロックは利用できません。

危険サイトブロックは、Google Chrome（カスタムタブ機能を含む）、Huawei Browser、Samsung Internet Browser でのみ動作します。仕事用プロファイルを使用しており、危険サイトブロックが仕事用プロファイルでのみ有効となるよう設定されている場合は、Samsung Internet Browser 用の危険サイトブロックはモバイルデバイス上でサイトをブロックしません。

メインウィンドウの概要

メインウィンドウの外観は、画面の解像度に応じて若干の違いがあります。

保護のレベルの低下や、デバイスの感染、情報の紛失を引き起こす可能性がある問題が発生した場合、メイン画面の表示が変わります。

［**状態**］セクションには、次の情報が表示されます：

- デバイスの保護に関する問題
- デバイスが企業のセキュリティ要件に準拠しているかどうかの情報
- デバイスの保護ステータスに関する情報

［**状態**］セクションは、Kaspersky Endpoint Security のメインウィンドウの一番上をタップすると開きます。

デバイスの保護に関する問題

保護に関する問題はカテゴリによってグループ化されています。問題ごとに考えられる解決方法が表示されます。

［**状態**］セクションには、本アプリによって検知されてスキップされたオブジェクトのリストも表示されます。スキップされたオブジェクトのリストは、悪意のあるファイルが削除または移動された時などに変わることがあります。最新の脅威のリストを取得するには、完全スキャンを実行します。信頼性が高いレベルでデータを保護するには、検知されたすべての脅威を取り除きます。

保護に関する問題には、2 つの種別があります：

- *注意：*黄色で強調表示されます。注意の問題では、デバイスのセキュリティに影響を及ぼす可能性があるイベントについてユーザーに通知します（たとえば、前回のスキャンが 14 日以上前である場合や、インストールされたアプリがスキャンされていない場合など）。注意の問題を非表示にすることができます。非表示にした後は、［**無視された問題を表示**］から問題に関する情報にアクセスできます。

- *重要：*赤で強調表示されます。重要な問題は、デバイスのセキュリティに重要な影響を与えるイベントについてユーザーに通知します（定義データベースが長期間アップデートされていない場合や、ブロックされているアプリがデバイスにインストールされた場合など）。重要な問題は非表示にできません。

コンプライアンスコントロール

デバイスが企業のセキュリティの要件を満たしているかどうかが自動的に確認されます。［**状態**］セクションには、デバイスが企業のセキュリティの要件を満たしているかどうかの情報も表示されます。

- デバイスが企業のセキュリティ要件を準拠していない理由（例：ブロックするアプリがデバイスで検知された）。
- ルール違反を取り除く期限（例：24 時間）。
- 指定された期間内にルール違反を取り除かない場合にデバイスで実行される処理（例：デバイスのロック）。
- 企業のセキュリティ要件に従ってデバイスのルール違反を修正するために実行される処理。

ステータスバーのアイコン

初回起動ウィザードが終了すると、Kaspersky Endpoint Security のアイコンがステータスバーに表示されます。

アイコンは、アプリの動作を示します。また、ここから Kaspersky Endpoint Security のメインウィンドウにアクセスできます。

アイコンは、Kaspersky Endpoint Security の動作を通知し、デバイスの保護ステータスを表示します：

– デバイスは保護されています。

– 保護に問題があります（定義データベースがアップデートされていない、新たにインストールされたアプリがスキャンされていない、など）。

デバイスのスキャン

アンチウイルスには制限事項があります：

- アンチウイルスの実行中、デバイスの外部ストレージ（SD カードなど）で検知された脅威は、仕事用プロファイルでは自動的に処理されません（ブリーフケースのアイコンが表示されたアプリケーション、Android 仕事用プロファイルの設定）。Kaspersky Endpoint Security for Android は、仕事用プロファイルでは外部ストレージにアクセスできません。検知したオブジェクトの情報は、本アプリの［**状態**］セクションに表示されます。外部ストレージで検知されたオブジェクトを処理するには、手動でオブジェクトを削除し、デバイスのスキャンを再開する必要があります。
- 技術的な制限により、Kaspersky Endpoint Security for Android はサイズが 2 GB 以上のファイルをスキャンできません。スキャン中、そのようなファイルがスキップされたことを通知せずに、ファイルはスキップされます。

デバイスのスキャンを開始するには：

1. Kaspersky Endpoint Security のメインウィンドウにあるクイック起動パネルで、［**スキャン**］をタップします。

2. デバイスのスキャン範囲を選択します：

- **デバイス全体のスキャン**：デバイスのファイルシステム全体をスキャンします。
- **インストール済みアプリのスキャン**：インストールされたアプリのみをスキャンします。
- **オブジェクトスキャン**：選択したフォルダーまたは個々のファイルをスキャンします。各オブジェクト（フォルダーまたはファイル）、またはデバイスのメモリに存在する次のパーティションのいずれかを選択できます：
  - **デバイスのストレージ**：デバイス全体のアクセス可能なストレージを読み取ります。これには、オペレーティングシステムのファイルを保存するシステムストレージのパーティションも含まれます。
  - **内部ストレージ**：アプリのインストールと、メディアコンテンツやドキュメント、およびその他のファイルの保存を目的とした、デバイスのストレージのパーティション。
  - **外部ストレージ**：外部 SD カードのストレージ。外部 SD カードが挿入されていない場合、このオプションは非表示になります。

スキャンの設定へのアクセスは、管理者により制限されている場合があります。

スキャンを設定するには：

1. Kaspersky Endpoint Security のメインウィンドウのクイック起動パネルで、→［**設定**］→［**アンチウイルス**］→［**スキャン**］の順にタップします。
2. アドウェアや、デバイスやデータに損害を与える目的で悪用される可能性のあるアプリを本アプリが検知するようにするには、［**アドウェア、ダイヤラー、その他**］のトグルボタンをオンにします。
3. ［**脅威の検知時の処理**］をタップして、本アプリの既定の処理を選択します。
   - **隔離**

     隔離に移動されたファイルは、デバイスに損害を与えないよう、圧縮ファイルとして保管されます。隔離では、隔絶された保管領域に移動されたファイルを削除したり、復元したりできます。
   - **手動選択**

     検知したオブジェクトごとに、処理（スキップ、隔離、削除）の選択を要求します。複数のオブジェクトを検知した場合は、選択したアクションをすべてのオブジェクトに適用できます。
   - **削除**

     検知したオブジェクトを自動的に削除します。追加の処理は必要ありません。オブジェクトの削除前に、オブジェクトの削除に関する通知が一時的に表示されます。
   - **スキップ**

     検知したオブジェクトがスキップされると、Kaspersky Endpoint Security for Android はデバイス保護の問題についてユーザーに警告します。スキップされた脅威に関する情報は、アプリの［**状態**］セクションに表示されます。スキップされた各脅威について、脅威を除去するために実行できる処理が示されます。スキップされたオブジェクトのリストは、悪意のあるファイルが削除または移動された時などに変わることがあります。最新の脅威のリストを取得するには、完全スキャンを実行します。信頼性が高いレベルでデータを保護するには、検知されたすべての脅威を取り除きます。

検知した脅威に関する情報と、脅威に対して実行した処理は、アプリのレポートに記録されます（→［**レポート**］）。アンチウイルスの動作に関するレポートの表示を選択できます。

定期スキャンの実行

アンチウイルスには制限事項があります：

- アンチウイルスの実行中、デバイスの外部ストレージ（SD カードなど）で検知された脅威は、仕事用プロファイルでは自動的に処理されません（ブリーフケースのアイコンが表示されたアプリケーション、Android 仕事用プロファイルの設定）。Kaspersky Endpoint Security for Android は、仕事用プロファイルでは外部ストレージにアクセスできません。検知したオブジェクトの情報は、本アプリの［**状態**］セクションに表示されます。外部ストレージで検知されたオブジェクトを処理するには、手動でオブジェクトを削除し、デバイスのスキャンを再開する必要があります。

- 技術的な制限により、Kaspersky Endpoint Security for Android はサイズが 2 GB 以上のファイルをスキャンできません。スキャン中、そのようなファイルがスキップされたことを通知せずに、ファイルはスキップされます。

デバイスの完全スキャンのスケジュールを設定するには：

1. Kaspersky Endpoint Security のメインウィンドウのクイック起動パネルで、→［**設定**］→［**アンチウイルス**］→［**スキャン**］の順にタップします。
2. ［**スケジュール**］をタップして、完全スキャンの頻度を選択します：
   - **毎週**
   - **毎日**
   - **無効**
   - **定義データベースのアップデート後**
3. ［**曜日**］をタップして、完全スキャンを開始する曜日を選択します。
4. ［**時刻**］をタップして、完全スキャンを開始する時刻を選択します。

スケジュールに従って、デバイスの完全スキャンが開始されます。

Android 12 以降のデバイスでは、バッテリー節約モードの場合、タスクの実行が指定よりも遅れる場合があります。

保護モードの変更

リアルタイム保護は、開いているファイルに存在する脅威の検知や、デバイスにリアルタイムでインストール中の新しいアプリのスキャンが可能です。定義データベースと Kaspersky Security Network クラウドサービス（クラウドプロテクション）が自動的に使用され、セキュリティを確保します。

デバイスの保護モードを変更するには：

1. Kaspersky Endpoint Security のメインウィンドウのクイック起動パネルで、→［**設定**］→［**アンチウイルス**］→［**リアルタイム保護モード**］の順にタップします。

2. デバイスの保護モードを選択します：

- **無効**：プロテクションが無効になります。
- **推奨**：インストール済みのアプリおよびダウンロードフォルダーにあるファイルのみをスキャンします。新しいアプリをインストールした際も、すぐにスキャンします。
- **拡張**：ファイルに対して何らかの操作（オープン、実行、コピー、保存、移動、変更など）が行われた場合に、デバイスにあるすべてのファイルをスキャンします。新しいアプリをインストールした際も、すぐにスキャンします。

現在の保護モードの情報は、本コンポーネントの説明の下に表示されます。

リアルタイム保護の設定へのアクセスは、管理者により制限されている場合があります。

クラウドプロテクション（KSN）を有効にするには：

1. Kaspersky Endpoint Security のメインウィンドウにあるクイック起動パネルで、→［**設定**］→［**アンチウイルス**］の順にタップします。
2. ［**クラウドプロテクション（KSN）**］のトグルボタンをオンにします。

   ［**クラウドプロテクション（KSN）**］のトグルボタンで、Kaspersky Security Network をデバイスのリアルタイム保護のみに使用するように設定できます。トグルボタンをオフにすると、KSN は本アプリの他のコンポーネントの動作にも使用されます。

   これにより、本アプリはカスペルスキーのオンラインナレッジベースへアクセスし、ファイルやアプリに関する評価の情報を取得します。定義データベースには追加されていないが、KSN では確認できる情報を持つ脅威に対して、このスキャンが実行されます。Kaspersky Security Network クラウドサービスにより、アンチウイルスの機能が制限なく発揮され、また誤検知の可能性も低減されます。管理者のみが、Kaspersky Security Network の使用を全面的に無効化できます。

リアルタイム保護を設定するには：

1. Kaspersky Endpoint Security のメインウィンドウのクイック起動パネルで、> ［**設定**］→［**アンチウイルス**］→［**リアルタイム保護モード**］をタップします。
2. アドウェアや、デバイスやデータに損害を与える目的で悪用される可能性のあるアプリを本アプリが検知するようにするには、［**アドウェア、ダイヤラー、その他**］のトグルボタンをオンにします。
3. ［**脅威の検知時の処理**］をタップして、本アプリの既定の処理を選択します。

   - **隔離**

     隔離に移動されたファイルは、デバイスに損害を与えないよう、圧縮ファイルとして保管されます。隔離では、隔絶された保管領域に移動されたファイルを削除したり、復元したりできます。

   - **削除**

     検知したオブジェクトを自動的に削除します。追加の処理は必要ありません。オブジェクトの削除前に、オブジェクトの削除に関する通知が一時的に表示されます。

   - **スキップ**

検知したオブジェクトがスキップされると、Kaspersky Endpoint Security for Android はデバイス保護の問題についてユーザーに警告します。スキップされた脅威に関する情報は、アプリの［**状態**］セクションに表示されます。スキップされた各脅威について、脅威を除去するために実行できる処理が示されます。スキップされたオブジェクトのリストは、悪意のあるファイルが削除または移動された時などに変わることがあります。最新の脅威のリストを取得するには、完全スキャンを実行します。信頼性が高いレベルでデータを保護するには、検知されたすべての脅威を取り除きます。

検知した脅威に関する情報と、脅威に対して実行した処理は、アプリのレポートに記録されます（ → ［**設定**］→［**レポート**］）。アンチウイルスの動作に関するレポートの表示を選択できます。

定義データベースのアップデート

本アプリの定義データベースをアップデートするには：

Kaspersky Endpoint Security のメインウィンドウにあるクイック起動パネルで、［**定義データベースのアップデート**］をタップします。

定義データベースの定期アップデート

本アプリでは、指定したスケジュールに従い、定義データベースを自動的にアップデートできます。

アップデートのスケジュールを設定するには：

1. Kaspersky Endpoint Security のメインウィンドウのクイック起動パネルで、 →［**設定**］→［**アンチウイルス**］→［**定義データベースのアップデート**］の順にタップします。
2. ［**スケジュール**］をタップして、アップデートの頻度を選択します：
   - **毎週**
   - **毎日**
   - **無効**
3. ［**曜日**］をタップして、アップデートを実行する曜日を選択します。
4. ［**時刻**］をタップして、アップデートを開始する時刻を指定します。

スケジュールに従って、定義データベースのアップデートが開始されます。

Android 12 以降のデバイスでは、バッテリー節約モードの場合、タスクの実行が指定よりも遅れる場合があります。

デバイスの紛失時または盗難時の対処

デバイスの紛失時または盗難時には、システム管理者にお問い合わせください。管理者は企業のセキュリティ要件に従い、デバイスに対して遠隔操作で盗難対策コマンドを実行できます。

デバイスに完全リセットのコマンドを送信すると、デバイスの制御は完全に失われ、盗難対策コマンドが動作しなくなります。

危険サイトブロック

危険サイトブロックを有効にするには：

- Kaspersky Endpoint Security をユーザー補助機能サービスに設定しておく必要があります。
- また、危険サイトブロックの使用を目的としたデータ処理に関する声明（「危険サイトブロックに関する声明」）に同意する必要があります。Kaspersky Endpoint Security は、Kaspersky Security Network（KSN）を Web サイトのスキャンに使用します。危険サイトブロックに関する声明は、KSN とのデータ交換に関する条件を含んでいます。

  Kaspersky Security Center を使用して、管理者は危険サイトブロックに関する声明にユーザーの代わりに同意できます。この場合、ユーザーは何も操作する必要はありません。

  危険サイトブロックに関する声明に管理者が同意せず、ユーザーに同意の要求を送信した場合は、本アプリ内の設定でユーザー自身が本声明に同意する必要があります。

  危険サイトブロックに関する声明に管理者が同意しなかった場合は、危険サイトブロックは利用できません。

危険サイトブロックは、Google Chrome（カスタムタブ機能を含む）、Huawei Browser、Samsung Internet Browser でのみ動作します。仕事用プロファイルを使用しており、危険サイトブロックが仕事用プロファイルでのみ有効となるよう設定されている場合は、Samsung Internet Browser 用の危険サイトブロックはモバイルデバイス上でサイトをブロックしません。

Web サイトを閲覧している時に危険サイトブロックが常に適用されるようにするには、Google Chrome または Samsung Internet Browser を通常使うブラウザーに設定します。

危険サイトブロックをサポートするブラウザーを通常使うブラウザーに設定し、Web サイトを常にスキャンするには：

1. Kaspersky Endpoint Security のメインウィンドウにあるクイック起動パネルで、→［**設定**］→［**危険サイトブロック**］の順にタップします。
2. ［**危険サイトブロック**］のトグルボタンをオンにします。
3. ［**通常使うブラウザーの設定**］をタップします。

   このボタンは、危険サイトブロックが有効で、かつ 危険サイトブロックをサポートするブラウザーが通常使うブラウザーとして設定されていない場合に表示されます。

   通常使うブラウザーの選択ウィザードが起動します。
4. ウィザードの指示に従います。

Google Chrome、Huawei Browser または Samsung Internet Browser が通常使うブラウザーとして設定されます。Web サイトの閲覧中、危険サイトブロックが常に Web サイトをスキャンします。

アプリ管理

*アプリ管理*は、モバイルデバイスにインストールされているアプリが企業のセキュリティ要件に準拠しているか確認します。Kaspersky Security Center では、管理者が企業のセキュリティ要件に従い、許可するアプリ、ブロックするアプリ、必須アプリ、および推奨アプリのリストを作成します。アプリ管理の結果に応じて、Kaspersky Endpoint Security は必須アプリおよび推奨アプリをインストールし、ブロックするアプリを削除するよう求めます。モバイルデバイスでブロックするアプリを開始することはできません。

必須アプリおよび推奨アプリをインストールする、またはブロックするアプリを削除するには：

1. Kaspersky Endpoint Security の［**状態**］セクションに移動します。
2. アプリ管理のタスクを選択します。
3. 推奨する処理を実行します。

証明書の取得

会社のネットワークリソースにアクセスするための証明書を取得するには：

1. Kaspersky Endpoint Security のメインウィンドウにあるクイック起動パネルで、→［**設定**］→［**詳細**］→［**証明書の取得**］の順にタップします。
2. 企業ネットワークのアカウントの認証情報を指定します。
3. 管理者から1回限り有効なパスワードを受け取った場合は、［**ワンタイムパスワード**］をオンにしてから、受け取ったパスワードを入力します。

   証明書インストールウィザードが起動します。
4. ウィザードの指示に従います。

Kaspersky Security Center との同期

お客様のデバイスを企業のセキュリティ要件に従って保護および設定するには、モバイルデバイスと Kaspersky Security Center のリモート管理システムを同期する必要があります。デバイスは、自動的に Kaspersky Security Center と同期されます。同期は、手動で行うこともできます。最初の同期が完了すると、Kaspersky Security Center で管理されるモバイルデバイスのリストにお使いのデバイスが追加されます。その後、管理者によって企業のセキュリティ要件に従ってデバイスを設定できます。

同期の設定は、初期設定ウィザードの実行中、または Kaspersky Endpoint Security の設定で行えます。Google Play を使用して Kaspersky Endpoint Security をインストールした場合、同期の設定は必ず行う必要があります。システム管理者から同期設定の値を要求してください。

デバイスと Kaspersky Security Center リモート管理システムの同期の設定は、管理者から指示があった場合にのみ変更してください。

デバイスと Kaspersky Security Center を同期するには：

1. Kaspersky Endpoint Security のメインウィンドウにあるクイック起動パネルで、→［**設定**］→［**同期**］の順にタップします。

2. ［**同期の設定**］セクションで、次の設定の値を指定します：

   - **サーバー**
   - **ポート**
   - **グループ**
   - **企業メールアドレス**

   同期の設定は管理者により非表示にできます。

3. ［**同期**］をタップします。

Kaspersky Security Center を使用しない Kaspersky Endpoint Security for Android のアクティベーション

ほとんどの場合、デバイスにインストールされた Kaspersky Endpoint Security for Android は管理者によって Kaspersky Security Center の遠隔管理システムで一元的にアクティベートされています。デバイスが Kaspersky Security Center に接続されていない場合は、アクティベーションコードを手動で入力できます。アクティベーションコードを入手するには、管理者にお問い合わせください。

本製品の手動でのアクティベーションは、管理者から指示があった場合にのみ行ってください。

アクティベーションコードを入力するには：

1. ライセンスの有効期間がまもなく終了する、もしくは終了したというエラーメッセージが表示されて、デバイスが管理サーバーに接続されていない場合は［**アクティベート**］をタップします。
2. アクティベーションのウィンドウで、管理者にもらったアクティベーションコードを入力して［**アクティベート**］をタップします。
3. アクティベーションコードが正しい場合、本アプリがアクティベートされたこととライセンスの有効期限が、通知に表示されます。

   デバイスの Kaspersky Endpoint Security for Android がアクティベートされました。

本アプリのアップデート

Kaspersky Endpoint Security は、次の方法でアップデートできます：

- Google Play を使用した手動アップデート：Google Play から本アプリの新しいバージョンをダウンロードし、デバイスにインストールします。
- 管理者による遠隔アップデート：Kaspersky Security Center のリモート管理システムから、お使いのデバイスにインストールされている本アプリのバージョンを、管理者が遠隔操作でアップデートします。

Google Play からの本アプリのアップデート

管理者は、本アプリの Google Play からのアップデートをブロックできます。

Android プラットフォームの標準的なアップデート方法で、Google Play から本アプリをアップデートします。製品をアップデートするには、次の条件を満たす必要があります：

- Google アカウントを持っている。
- デバイスが Google アカウントに紐づけられている。
- デバイスがインターネットに接続している必要があります。

Google アカウントの作成、デバイスと Google アカウントの紐づけ、Google Play ストアの使用については、Google のサポートサイト を確認してください。

Kaspersky Security Center からの製品のアップデート

Kaspersky Security Center から本アプリをアップデートするステップは、次の通りです：

1. 管理者は、企業のセキュリティ要件を満たす製品バージョンの配布パッケージをモバイルデバイスに送信します。

   デバイスに Kaspersky Endpoint Security for Android をインストールするよう促す通知が表示されます。

2. アップデートの条項に同意します。

   製品の新しいバージョンがデバイスにインストールされます。アップデート後に追加の設定は要求されません。

本アプリの削除

ユーザー個人による本アプリの削除は、管理者によってブロックできます。この場合、ユーザーは Kaspersky Endpoint Security を削除できません。

Kaspersky Endpoint Security は、次の方法で削除できます：

- 本アプリの設定からの手動による削除。
- デバイスの設定からの手動による削除。
- 管理者による遠隔アップデート：Kaspersky Security Center のリモート管理システムから、お使いのデバイスにインストールされている本アプリを、管理者が遠隔操作で削除します。

本アプリの設定からの削除

デバイスから Kaspersky Endpoint Security を削除するには：

1. Kaspersky Endpoint Security のメインウィンドウにあるクイック起動パネルで、→［**アプリをアンインストール**］を順にタップします。

アプリの削除ウィザードが起動します。

2. ウィザードの指示に従います。

デバイスの設定からの削除

Android プラットフォームの以下の標準的な手順で削除できます。本アプリを削除するには、デバイスのセキュリティ設定で Kaspersky Endpoint Security の管理者権限を無効にしておく必要があります。

Android 7.0 以降のデバイスでは、管理者によって削除がブロックされている場合、Android の設定から本アプリを削除しようとするとデバイスがロックされます。デバイスのロックを解除するには、管理者に連絡してください。

Kaspersky Security Center からの削除

Kaspersky Security Center から製品を削除するステップは、次の通りです：

1. 管理者が、製品を削除するデバイスをお使いのデバイスに送信します。

   Kaspersky Endpoint Security の削除の確認を要求する通知がモバイルデバイスに表示されます。

2. 本アプリの削除を確定します。

   お使いのデバイスから製品が削除されます。

ブリーフケースのアイコンが表示されたアプリケーション

Android 仕事用プロファイルのアプリケーションのアイコン

ブリーフケースのアイコンが表示されるアプリ（企業アプリ）は、デバイスの Android 仕事用プロファイル（以降、「仕事用プロファイル」とも表記）に保存されます。*Android 仕事用プロファイル*は、ユーザーのデバイスにある安全な環境で、管理者は、ユーザーによる個人情報の使用を制限することなくアプリやアカウントの管理ができます。

仕事用プロファイルを使用すれば、会社のデータと個人情報を分けて保存できます。これにより、会社のデータの機密性が保持され、マルウェアからそれらのデータを保護できます。デバイスに仕事用プロファイルが作成されると、次の企業向けアプリが自動的にインストールされます：Google Play Market、Google Chrome、Downloads、Kaspersky Endpoint Security for Android など。

KNOX アプリ

KNOX アイコン

KNOX アプリはデバイスの KNOX コンテナーを開きます。*KNOX コンテナー*は、デバイス上の安全な領域です。独自のデスクトップ、起動パネル、アプリ、ウィジェットを持っています。管理者は、ユーザーの個人情報の使用を制限することなく、KNOX コンテナーのアプリやアカウントの管理ができます。

KNOX コンテナーを使用すれば、会社のデータと個人情報を分けて保存できます。これにより、会社のデータの機密性が保持され、マルウェアからそれらのデータを保護できます。

KNOX コンテナーでは、会社のメールボックス、会社の従業員の連絡先情報、ファイルの保管やその他のアプリケーションにアクセスできます。

KNOX の詳細は、*Samsung のテクニカルサポートサイト*を参照してください。

Kaspersky Security for iOS の使用

このセクションでは、Kaspersky Security for iOS アプリでユーザーが使用可能な機能と動作について説明します。

このセクションの記事には、モバイルデバイスで使用または表示できるすべてのオプションが含まれています。本アプリの実際のレイアウトと動作は、実装されているリモート管理システムや、企業のセキュリティ要件に従って管理者がデバイスを設定する方法によって異なります。このセクションで説明する一部の機能とオプションは、アプリの実際のエクスペリエンスには適用されない場合があります。特定のデバイスの本アプリについて質問がある場合は、管理者にお問い合わせください。

アプリの機能

Kaspersky Security for iOS で提供する主な機能は、次の通りです。

オンライン上の脅威からの保護

危険サイトブロックは、オンライン上の脅威から保護します。

危険サイトブロックは、悪意のあるコードを配信する Web サイトや、個人情報を盗んで金融機関のアカウントにアクセスする目的で設計されたフィッシングサイトをブロックします。危険サイトブロックは、Web サイトを開く前に、Kaspersky Security Network クラウドサービスを使用して、その Web サイトをスキャンします。危険サイトブロックは、デバイスのアプリのオンライン動作もチェックします。

危険サイトブロックを動作させるには、本アプリによる VPN 設定の追加を許可する必要があります。

ジェイルブレイクの検知

Kaspersky Security for iOS がジェイルブレイクを検知すると、重大な問題であることを示すメッセージが表示され、この問題が管理者へ通知されます。

本アプリはデバイスのセキュリティを保証できません。ジェイルブレイクはセキュリティ機能を迂回し、次のような数々の問題の原因となる可能性があるためです：

- セキュリティが脆弱になる
- 安定性に問題が生じる
- Apple のサービスが正常に享受できなくなる
- クラッシュ、フリーズの可能性がある
- バッテリー寿命が短くなる
- iOS アップデートができなくなる

本アプリのインストール

Kaspersky Security for iOS アプリをインストールするには：

1. 管理者から送信された、App Store からの Kaspersky Security for iOS のインストールを案内するメールメッセージを探します。
2. App Store へ、次のいずれかの方法で移動します：
   - 本アプリをインストールする iOS デバイスでメールメッセージを読んでいる場合、メッセージ内のリンクをタップします。
   - コンピューターでメッセージを読んでいる場合、本アプリをインストールする iOS デバイスを使用して QR コードをスキャンします。

   メッセージ内のリンクの有効期間は 24 時間です。本アプリをこの時間内にインストールできない場合は、新しいメールメッセージの送信を管理者に依頼してください。
3. iOS プラットフォームの標準のインストール手順に従って、App Store から本アプリをダウンロードし、デバイスへインストールします。

Kaspersky Security for iOS がデバイスにインストールされます。デバイスを保護するには、本アプリをアクティベートします。

本アプリのアクティベート

Kaspersky Security for iOS アプリをアクティベートするには：

1. 本アプリをデバイスで起動します。
2. ［**使用許諾契約書**］と［**製品およびサービスに関するプライバシーポリシー**］のチェックボックスをオンにして、契約書と声明に同意します。

   ［**Kaspersky Security Network に関する声明**］に同意して、Kaspersky Security Network への統計情報の送信を許可します（任意）。統計情報を送信することにより、本アプリのパフォーマンスが向上し、アプリの動作の連続性が確保されます。
3. ［**次へ**］をタップします。本アプリは Kaspersky Security Center のリモート管理システムへ接続し、ライセンスの情報を自動的に取得します。
4. 本アプリによる VPN 設定の追加を許可します。本アプリは VPN 設定を使用して、Web サイトがフィッシングサイトかどうかをチェックし、デバイスをマルウェアから保護します。
5. 本アプリによるプッシュ通知の送信を許可します。本アプリは通知を使用して、セキュリティ上の問題およびライセンスのステータスを通知します。

デバイスの Kaspersky Security for iOS がアクティベートされます。

アクティベーションコードで本アプリをアクティベート

Kaspersky Security for iOS のデバイスへのインストール時に、本アプリは Kaspersky Security Center のリモート管理システムへ接続し、ライセンスの情報を自動的に取得します。デバイスが Kaspersky Security Center に接続されていない場合は、アクティベーションコードを手動で入力できます。アクティベーションコードを入手するには、管理者にお問い合わせください。

管理者から指示があった場合にのみ、本アプリを手動でアクティベートしてください。

アクティベーションコードを入力するには：

1. 本アプリがアクティベートされていないことを通知するメッセージで、［**アプリをアクティベート**］をタップします。
2. アクティベーションのウィンドウで、管理者から受け取ったアクティベーションコードを入力して［**アクティベート**］をタップします。

   アクティベーションコードが正しい場合、本アプリがアクティベートされたこととライセンスの有効期限が、通知に表示されます。

デバイスの Kaspersky Security for iOS がアクティベートされます。

メインウィンドウの概要

メインウィンドウの外観は、画面の解像度に応じて若干の違いがあります。

メインウィンドウには次が表示されます：

- デバイスの全体的な保護のステータス。
- アプリのコンポーネントの状態と保護に関する問題を通知するメッセージ。

メッセージは 3 種類あります：

- 緑のハイライト。指定した領域の保護がアクティブであることを通知するステータスメッセージです。
- 黄色のハイライト。デバイスのセキュリティに影響を及ぼす可能性があるイベントを通知する情報メッセージです。
- 赤のハイライト。デバイスのセキュリティにとって重大なイベントを通知する緊急メッセージです。

メッセージをタップすると詳細を確認できます。

本アプリのアップデート

Kaspersky Security for iOS の最新バージョンは、iOS プラットフォームをアップデートする標準の手順に従って、App Store からダウンロードし、デバイスへインストールできます。自動アップデートを有効にすることもできます。アップデート後に追加の設定は要求されません。

本アプリをアップデートするには、次の条件を満たす必要があります：

- Apple ID を持っている必要があります。
- デバイスが Apple ID に紐づけられている必要があります。

- デバイスがインターネットに接続している必要があります。

Apple ID の作成、Apple ID とデバイスの紐づけ、App Store での操作の詳細は、Apple のサポートサイトを参照してください。

本アプリの削除

Kaspersky Security for iOS を削除するには、iOS プラットフォームの標準の手順に従います：

1. ホーム画面で、アプリのアイコンをタップし長押しします。
2. 本アプリを削除します。

Kaspersky Security for iOS がデバイスから削除されます。

製品のライセンス

このセクションでは、Kaspersky Security for Mobile のライセンスに関連する一般的なご利用条件の情報について説明します。

使用許諾契約書について

*使用許諾契約書*は、ユーザーと AO Kaspersky Lab との間で交わされる契約であり、製品を使用する際の条項が定められています。

Kaspersky Security for Mobile をご利用になる前に、使用許諾契約書の条項をよくお読みください。

使用許諾契約書の条項は次の方法で表示できます：

- Kaspersky Security for Mobile のコンポーネントのインストール時。
- ファイル license.txt を確認する。このファイルは Kaspersky Endpoint Security for Android のインストール用配布キットの自己解凍圧縮ファイルに含まれています。
- Kaspersky Endpoint Security for Android の［**製品情報**］セクションを確認する。
- Kaspersky Security for iOS の［**製品情報**］→［**契約書と声明**］セクション。
- 管理サーバーのプロパティの［**詳細**］→［**同意済みの使用許諾契約書**］セクション。この機能は、Kaspersky Security Center バージョン 12.1 以降でのみ使用可能です。

Kaspersky Security for Mobile のコンポーネントのインストール時に使用許諾契約書への同意を確認すると、使用許諾契約書の条項に同意したことになります。使用許諾契約書の条項に同意しない場合は、Kaspersky Security for Mobile コンポーネントのインストールを中止し、使用をお控えください。

ライセンスについて

*ライセンス*とは、使用許諾契約書の条項に基づいて提供される、Kaspersky Security for Mobile 統合ソリューションを使用するための期限付きの権利です。

現在のライセンスにより、次の種別のサービスを受ける権利が与えられます：

- 使用許諾契約書の条件に従い、モバイルデバイスのアプリを使用する。
- テクニカルサポートを受ける。

利用可能なサービスの範囲とアプリの使用に関する条件は、アプリがアクティベートされたライセンスの種別に応じて異なります。

次のライセンスの種別が提供されます：

- *試用版*：

  Kaspersky Security for Mobile の試用を目的とした無料のライセンス。

試用版ライセンスの有効期間は、30 日です。試用版ライセンスの有効期間が終了すると、Kaspersky Endpoint Security for Android と Kaspersky Security for iOS モバイルアプリは、管理サーバーとの同期以外の大部分の機能の実行を停止します。引き続き製品を使用するには、製品版ライセンスを購入してください。

- *製品版*:

  Kaspersky Security for Mobile の購入時に提供されるライセンスです。

  製品版ライセンスの有効期限が切れると、製品は引き続き動作しますが、機能が制限されます。

  機能が制限された状態で、アプリごとに使用可能な機能は次の通りです。

  - Kaspersky Endpoint Security for Android アプリ：
    - **アンチウイルス**：デバイスのリアルタイム保護とウイルススキャンが使用可能ですが、定義データベースのアップデートが使用できません。
    - **盗難対策**：モバイルデバイスへのコマンド送信のみが使用可能です。
    - **管理サーバーとの同期**：

    Kaspersky Endpoint Security for Android による Kaspersky Security Network、Firebase 向け Google アナリティクス、SafetyNet Attestation、Firebase Performance Monitoring、Crashlytics とのデータ送受信は、次の場合に停止します：カスペルスキーのライセンスがブロックされた場合、試用版ライセンスの有効期間が終了した場合、ライセンスがない場合（アクティベーションコードがグループポリシーから削除された場合など）。

  - Kaspersky Security for iOS アプリ：
    - **管理サーバーとの同期**：

    Kaspersky Security for iOS による Kaspersky Security Network とのデータ送受信は、試用版ライセンスの有効期間が終了した場合、またはライセンスがない場合（アクティベーションコードがグループポリシーから削除された場合など）に停止します。

  上記以外のモバイルアプリのコンポーネントをモバイルユーザーは使用できません。管理者は、グループポリシーを使用して、機能制限されたこれらのコンポーネントを管理できます。グループポリシーを使用して、本アプリのその他のコンポーネントを設定することはできません。

  機能の制限がない状態で製品の使用を継続するには、製品版ライセンスを更新する必要があります。セキュリティのあらゆる脅威に対してコンピューターを最大限に保護するには、現在のライセンスの有効期限が切れる前にライセンスを更新するか、新しいライセンスを購入することを推奨します。

定額制サービスについて

*Kaspersky Security for Mobile の定額制サービス*は、選択したパラメータ（定額制サービスの有効期限、保護されるモバイルデバイスの台数）を指定して製品を使用するための注文です。Kaspersky Security for Mobile の定額制サービスは、サービスプロバイダー（お使いの ISP など）から注文できます。定額制サービスは、手動または自動で更新でき、定額制サービスをキャンセルすることもできます。定額制サービスは、サービスプロバイダーの Web サイトで管理できます。

定額制サービスは、制限付き（1年間など）と、無制限（有効期限なし）があります。定額制サービスの有効期限が切れた後も Kaspersky Security for Mobile を引き続き動作させるには、定額制サービスを更新する必要があります。無制限の定額制サービスは、サービスプロバイダーへの前払いが適切な場合に、自動的に更新されます。

制限付き定額制サービスの場合、有効期限が切れると、定額制サービスを更新するための猶予期間が提供されることがあります。その期間は製品の機能が保持されます。そのような猶予期間が提供されるか、提供された場合の期間の長さは、サービスプロバイダーによって異なります。

定額制サービスで Kaspersky Security for Mobile を使用するには、サービスプロバイダーから提供されるアクティベーションコードを適用する必要があります。アクティベーションコードが適用されると、定額制サービスで製品を使用するためのライセンスがインストールされます。

定額制サービスで使用可能な管理オプションは、サービスプロバイダーごとに異なります。サービスプロバイダーは、定額制サービス更新の猶予期間（アプリの機能が保持される期間）を提供していないこともあります。

定額制サービスで購入したアクティベーションコードは、Kaspersky Security for Mobile の旧バージョンのアクティベーションには使用できません。

ライセンス情報について

*ライセンス情報*とは、統合セキュリティ製品 Kaspersky Security for Mobile のアクティベーション時に適用するビット列です。アクティベーション後は、ライセンス使用許諾契約書の諸条件に基づいて製品を使用できるようになります。ライセンス情報はカスペルスキーにより生成されます。

ライセンス情報ファイルまたはアクティベーションコードを使用して、モバイルアプリのライセンス情報を追加できます：

- 組織で Kaspersky Security Center ソフトウェアスイートを導入している場合は、ライセンス情報ファイルを適用して Android モバイルアプリに配信する必要があります。ライセンス情報は Kaspersky Security Center のインターフェイスと Android モバイルアプリのインターフェイスに一意の英数字の並びとして表示されます。

  ライセンス情報は、追加した後に他のライセンス情報と置き換えることができます。

  Kaspersky Security for iOS をライセンス情報ファイルでアクティベートすることはできません。

- 組織で Kaspersky Security Center を使用していない場合は、アクティベーションコードをユーザーと共有する必要があります。ユーザーがこのアクティベーションコードを Android または iOS モバイルアプリに入力します。ライセンス情報は、一意の英数字の並びとしてモバイルアプリのインターフェイスに表示されます。

使用許諾契約書の条件に違反すると、ライセンス情報はカスペルスキーによってブロックされます。ライセンス情報がブロックされると、モバイルアプリは、管理サーバーとの同期以外のすべての機能の実行を停止します。本アプリを継続して使用するには、別のライセンスを追加する必要があります。

アクティベーションコードについて

*アクティベーションコード*とは、20 文字の英数字の一意の並びです。アクティベーションコードを入力して、Kaspersky Endpoint Security for Android または Kaspersky Security for iOS モバイルアプリをアクティベートするライセンス情報を追加します。アクティベーションコードは、Kaspersky Security for Mobile の購入時、または Kaspersky Security for Mobile の試用版の注文時に指定したメールアドレスに送られます。

アクティベーションコードを使用して本モバイルアプリをアクティベートするには、カスペルスキーのアクティベーションサーバーに接続するためのインターネットアクセスが必要です。

製品をアクティベートした後にアクティベーションコードを紛失してしまった場合は、復元できます。アクティベーションコードは、カスペルスキーカンパニーアカウントへの登録時などに必要となる場合があります。アクティベーションコードを復元するには、カスペルスキーのテクニカルサポートにお問い合わせください。

ライセンス情報ファイルについて

*ライセンス情報ファイル*は、カスペルスキーから受け取る、拡張子 KEY のファイルです。ライセンス情報ファイルの目的は、Kaspersky Endpoint Security for Android をアクティベートするライセンス情報を追加することです。

Kaspersky Security for iOS をライセンス情報ファイルでアクティベートすることはできません。

ライセンス情報ファイルは、 Kaspersky Security for Mobile 統合ソリューションの購入時、または Kaspersky Security for Mobile の試用版の注文時に指定したメールアドレスに送られます。

ライセンス情報ファイルで製品をアクティベートする場合、カスペルスキーのアクティベーションサーバーに接続する必要はありません。

誤ってライセンス情報ファイルを削除してしまった場合は、復元できます。ライセンス情報ファイルは、カスペルスキーカンパニーアカウントへの登録時などに必要となります。

ライセンス情報ファイルを修復するには、次の操作を行います：

- ご購入元の販売代理店へお問い合わせ。
- 有効なアクティベーションコードを使用して、カスペルスキーの Web サイトからライセンス情報ファイルを取得する。

Kaspersky Endpoint Security for Android でのデータ提供

Kaspersky Security for Mobile は、一般データ保護規則（General Data Protection Regulations：GDPR）に準拠しています。

本アプリをインストールするには、管理者またはデバイスユーザーが使用許諾契約書の条件に同意する必要があります。また、下にリストした声明へ全ユーザーを代表してグローバルに同意するようにポリシーを設定することもできます。上記のように設定しない場合、ユーザーが使用する本アプリのメイン画面に、ユーザーの個人データの処理に関する次の声明への同意の要求が通知されます：

- Kaspersky Security Network に関する声明
- 危険サイトブロックの使用を目的としたデータ処理に関する声明
- マーケティング目的に沿ったデータ処理に関する声明

声明にグローバルに同意することを選択した場合、Kaspersky Security Center を使用して同意する声明のバージョンが、ユーザーが同意済みである声明のバージョンと一致する必要があります。一致しない場合、ユーザーにその問題が通知され、管理者がグローバルに同意した声明と同じバージョンの声明への同意が要求されます。Kaspersky Security for Mobile (Devices) プラグインのデバイスステータスも、「*警告*」に変更されます。

声明に同意するかどうかは、Kaspersky Endpoint Security for Android の［**製品情報**］セクションで、いつでも選択できます。

Kaspersky Security Network との情報交換

リアルタイム保護を改善するため、Kaspersky Endpoint Security for Android は次のコンポーネントの動作で Kaspersky Security Network クラウドサービスを使用します：

- **アンチウイルス**：本アプリはカスペルスキーのオンラインナレッジベースへアクセスし、ファイルやアプリに関する評価の情報を取得します。定義データベースには追加されていないが、KSN では確認できる情報を持つ脅威に対して、このスキャンが実行されます。Kaspersky Security Network クラウドサービスにより、アンチウイルスの機能が制限なく発揮され、また誤検知の可能性も低減されます。

- **危険サイトブロック**：KSN から取得したデータを使用して、Web サイトが開かれる前にそのサイトをスキャンします。また、Web サイトのカテゴリを判別し、許可するカテゴリとブロックするカテゴリのリストに基づいてユーザーのインターネットアクセスを制御します（たとえば、「インターネットコミュニケーション」カテゴリなど）。

- **アプリ管理**：アプリのカテゴリを判別し、許可するカテゴリとブロックするカテゴリのリストに基づいて、企業のセキュリティ要件を満たさないアプリの開始を制限します（たとえば「ゲーム」カテゴリなど）。

アンチウイルスおよびアプリ管理の動作中、KSN を使用している時にカスペルスキーに送信されるデータの種別に関する情報は、使用許諾契約書に記載されています。使用許諾契約書の諸条項に同意すると、この情報の送信に同意したことになります。

危険サイトブロックの動作中、KSN を使用している時にカスペルスキーに送信されるデータの種別に関する情報は、データ処理に関する声明に記載されています。声明の諸条項に同意すると、この情報の送信に同意したことになります。

Kaspersky Endpoint Security for Android モバイルアプリの動作中、KSN の使用時にカスペルスキーに送信されるデータの種別に関する情報は、使用許諾契約書に記載されています。声明の諸条項に同意すると、この情報の送信に同意したことになります。

使用許諾契約書に基づくデータ提供

本ソフトウェアをアクティベートする際にアクティベーションコードを使用すると、お客様が本ソフトウェアを正規の用途で利用していることを確認するために、次の情報を定期的に権利者に提供することに同意したことになります：

- 権利者のインフラストラクチャへのリクエストに含まれるデータの形式、 アクセスされた Web サービスの IPv4 アドレス、 権利者のインフラストラクチャへのリクエストに含まれる内容のサイズ、 プロトコルの識別子、 本ソフトウェアのアクティベーションコード、 データ圧縮種別、 本ソフトウェアの識別子、 ユーザーの端末でアクティベートできるソフトウェアの識別子セット、 ソフトウェアの言語版、 本ソフトウェアの詳細バージョン、 一意な端末の識別子、 お客様の端末の日時、 ソフトウェアのインストール識別子（PCID）、 OS バージョン、OS ビルド番号、OS アップデート番号、OS のエディション、OS のエディションに関する詳細情報、 端末の機種、 オペレーティングシステムのグループ、 権利者のインフラストラクチャへのリクエストに含まれるデータの形式、 処理中のオブジェクトのチェックサム種別、 ソフトウェア

のライセンスのヘッダー、 地域のアクティベーションセンターの識別子、 ソフトウェアのライセンス情報ファイルの作成日、 ソフトウェアのライセンスの識別子、 本ソフトウェアのライセンスの提供に使用された情報形式の識別子、 ソフトウェアのライセンスの有効期限、 本ソフトウェアのライセンス情報ファイルの現在のステータス、 適用されたライセンスの種別、 本ソフトウェアをアクティベートするのに使用したライセンスの種別、 ライセンスに基づく本ソフトウェアの識別子。

デバイスを情報セキュリティ上の脅威から保護する目的で、エンドユーザーは次の情報を権利者に定期的に送信することに同意したことになります：

- 処理中のオブジェクトのチェックサム種別、 処理中のオブジェクトのチェックサム、 本ソフトウェアのコンポーネントの識別子、
- トリガーされた本ソフトウェアの定義データベースのレコードの識別子、 トリガーされた本ソフトウェアの定義データベースのレコードのタイムスタンプ、 トリガーされた本ソフトウェアの定義データベースのレコードの種別、 検知されたマルウェアの名前、ユーザーの端末またはデータに損害を与える目的で使用される可能性がある正規のソフトウェアの名前、
- アプリケーションがインストールされたストア名、 本ソフトウェアのパッケージ名、 APK ファイルの署名に使用された公開鍵、 APK ファイルの署名に使用された証明書のチェックサム、 デジタル署名のタイムスタンプ、
- 本ソフトウェアの詳細バージョン、 ソフトウェアアップデートの識別子、 インストールされた本ソフトウェアの種別、 設定の識別子、 本ソフトウェアの動作の結果、 エラーコード、
- Android アプリケーション APK ファイルから特定の数学的ルールに基づき算出され、当初のファイル形式の復元が許可されない数字、 このデータには、ファイル名、ファイルのパス、アドレス、電話番号、その他のユーザーの個人的な情報は含まれません。

お客様が権利者のアップデートサーバーを使用してアップデートをダウンロードする場合、アップデート手順の効率を向上させる目的で、お客様は権利者に次の情報を定期的に提供することに同意したことになります：

- ライセンスに基づく本ソフトウェアの識別子、 本ソフトウェアの詳細バージョン、 ソフトウェアのライセンスの識別子、 適用されたライセンスの種別、 ソフトウェアのインストール識別子（PCID）、 ソフトウェアアップデートの開始の識別子、 処理中の Web アドレス。

カスペルスキーは、本ソフトウェアの配布および使用に関する統計情報を受信する目的にも、これらの情報を使用する場合があります。

カスペルスキーは、法定要件に従って、収集した情報を保護します。受け取ったオリジナルの情報は暗号化した形式で保存され、蓄積すると消去されます（年に 2 回）。一般的な統計は無期限に保存されます。

Kaspersky Security Network に関する声明に基づくデータ提供

KSN の使用は、情報やネットワーク上のセキュリティの脅威に対して本ソフトウェアが提供する保護機能の有効性の向上に役立ちます。

5 ノード以上用のライセンスを使用している場合、権利者は KSN の使用中に次のデータを自動的に受け取り処理します：

- トリガーされた本ソフトウェアの定義データベースのレコードの識別子、 トリガーされた本ソフトウェアの定義データベースのレコードのタイムスタンプ、 トリガーされた本ソフトウェアの定義データベースのレコードの種別、 本ソフトウェアの定義データベースのリリース日時、 OS バージョン、OS ビルド番号、OS アップデート番号、OS のエディション、OS のエディションに関する詳細情報、 OS のサービスパックのバージョン、 検知の特性、 処理中のオブジェクトのチェックサム（MD5）、 処理中のオブジェクトの名前、 処理中のオブジェクトが PE ファイルであることを示すフラグ、 Web サービスをブロックしたマスクのチェックサム（MD5）、 処理中のオブジェクトのチェックサム（SHA256）、 処理中のオブジェクトの

サイズ、 オブジェクト種別のコード、 処理中のオブジェクトに対する本ソフトウェアの判断、 処理中のオブジェクトへのパス、 ディレクトリコード、 本ソフトウェアの機能のバージョン、 送信中の統計情報のバージョン、 アクセスされた Web サービスのアドレス（URL、IP）、 Web サービスへのアクセスに使用したクライアントの種別、 アクセスされた Web サービスの IPv4 アドレス、 アクセスされた Web サービスの IPv6 アドレス、 Web サービスのリクエスト元の Web アドレス（リファラー）、 処理中の Web アドレス、

- スキャンされたオブジェクトに関する情報（AndroidManifest.xml からのアプリケーションバージョン、 本製品のアプリケーションに対する判断、 本製品のアプリケーションに対する判断に使用された方法、 ストアのインストールパッケージ名、 AndroidManifest.xml からのパッケージ名（またはバンドルの名前）、 Google SafetyNet のカテゴリ、 端末で SafetyNet が有効になっているかどうかを示すフラグ、 Google SafetyNet の応答の SHA256 値、 APK 証明書の APK 署名スキーム、 インストールされた本ソフトウェアのバージョンコード、 APK ファイルの署名に使用された証明書のシリアル番号、 インストール中の APK ファイルの名前、 インストール中の APK ファイルのパス、 APK ファイルの署名に使用された証明書の発行元、 APK ファイルの署名に使用された公開鍵、 APK ファイルの署名に使用された証明書のチェックサム、 証明書の有効期限の日時、 証明書の発行日時、 送信中の統計情報のバージョン、 デジタル証明書のサムプリントの計算アルゴリズム、 インストールされた APK ファイルのハッシュ（MD5）、 APK ファイル内にある DEX ファイルのハッシュ（MD5）、 アプリケーションに動的に付与されている権限、 サードパーティ製ソフトウェアのバージョン、 アプリケーションが既定の SMS メッセンジャーであるかどうかを示すフラグ、 アプリケーションが端末の管理者権限を持つかどうかを示すフラグ、 アプリケーションがシステムカタログにあるかどうかを示すフラグ、 アプリケーションがアクセシビリティサービスを使用しているかどうかを示すフラグ）、

- 悪意のある可能性のあるすべてのオブジェクトおよび動作に関する情報（処理中のオブジェクトのフラグメントコンテンツ、 証明書の有効期限の日時、 証明書の発行日時、 暗号化に使用されるキーストアからの鍵、 KSN を介したデータ交換に使用されたプロトコル、 処理中のオブジェクトのフラグメントの順番、 処理中のオブジェクトに対してアンチウイルス製品のモジュールが生成した内部ログのデータ、 証明書の発行者の名前、 証明書の公的鍵、 証明書の公的鍵の計算アルゴリズム、 証明書のシリアル番号、 オブジェクトの署名日時、 証明書の所有者名と設定、 スキャンしたオブジェクトのデジタル証明書のサムプリントとハッシュアルゴリズム、 処理中のオブジェクトが最後に変更された日時、 処理中のオブジェクトの作成日時、 処理中のオブジェクトまたはその一部、 オブジェクトのプロパティで定義されている処理中のオブジェクトの説明、 処理中のオブジェクトの形式、 処理中のオブジェクトのチェックサム種別、 処理中のオブジェクトのチェックサム（MD5）、 処理中のオブジェクトの名前、 処理中のオブジェクトのチェックサム（SHA256）、 処理中のオブジェクトのサイズ、 ソフトウェア開発元の名前、 処理中のオブジェクトに対する本ソフトウェアの判断、 処理中のオブジェクトのバージョン、 処理中のオブジェクトに対する判定のソース、 処理中のオブジェクトのチェックサム、 親アプリケーションの名前、 処理中のオブジェクトへのパス、 ファイル署名のチェックの結果に関する情報、 ログオンセッションのキー、 ログオンセッションのキーの暗号化アルゴリズム、 処理中のオブジェクトが保管されている時間、 デジタル証明書のサムプリントの計算アルゴリズム）、

- ビルド種別（例：「user」 または「eng」）、 詳細な製品名、 製品または端末の製造元、 Google Play の外部でアプリがインストールできるかどうか、 アプリケーションの安全性をチェックするクラウドサービスである「Google Play プロテクト」の動作状況を示すフラグ、 Google Play プロテクトの設定 が Android Debug Bridge（ADB）からインストールしたアプリケーションとして有効になっているかどうかを示すフラグ、 現在の開発コード名、または「REL」（製品ビルド用）、 ビルドの差分番号、 ユーザーが確認できるバージョン文字列、 ユーザーのデバイス名、 ユーザーが確認できるソフトウェアのビルド識別子、 ファームウェアのフィンガープリント、 ファームウェアの識別子、 端末がルート化されているかを示すフラグ、 オペレーティングシステム、 本ソフトウェアの名前、 適用されたライセンスの種別、

- KSN サービス動作の品質に関する情報（KSN とのデータ交換に使用されたプロトコル、 本ソフトウェアがアクセスした KSN サービスの識別子、 統計の収集を停止した日時、 キャッシュから取得された KSN 接続の数、 ローカルのリクエストデータベースにある応答ありのリクエストの数、 失敗した KSN 接続の数、 失敗した KSN トランザクションの数、 KSN へのリクエストのキャンセルの時間分布、 失敗した KSN への接続の時間分布、 失敗した KSN のトランザクションの時間分布、 成功した KSN への接続の時間分布、 成功した KSN の処理の時間分布、 成功した KSN へのリクエストの時間分布、 タイムアウトした KSN へのリクエストの時間分布、 新規の KSN 接続の数、 ルーティングのエラーによって失敗した KSN へのクエリの数、 本ソフトウェアの設定で KSN が無効にされているために失敗したクエリの数、 ネットワークの問題によって失敗した KSN へのクエリの数、 成功した KSN 接続の数、 成功した KSN トランザクションの数、 KSN へのクエリの合計数、 統計の収集を開始した日時）、

- デバイス ID、 本ソフトウェアの詳細バージョン、 ソフトウェアアップデートの識別子、 ソフトウェアのインストール識別子（PCID）、 インストールされた本ソフトウェアの種別、

- 端末の画面の高さ、 端末の画面の幅、 オーバーラップされているアプリケーションに関する情報： APK ファイルのハッシュ（MD5）、 オーバーラップされているアプリケーションに関する情報： ファイル classes.dex の MD5 ハッシュ、 オーバーラップされているアプリケーションに関する情報： APK ファイルの名前、 オーバーラップされているアプリケーションに関する情報： ファイル名を含まない APK ファイルのパス、 オーバーラップの高さ、 オーバーラップされているアプリケーションに関する情報： APK ファイルのハッシュ（MD5）、 オーバーラップされているアプリケーションに関する情報： ファイル classes.dex の MD5 ハッシュ、 オーバーラップされているアプリケーションに関する情報： APK ファイル名、 オーバーラップされているアプリケーションに関する情報： ファイル名を含まない APK ファイルへのパス、 オーバーラップされているアプリケーションに関する情報： アプリケーションのパッケージ名（オーバーラップされているアプリケーション： 広告画面が何も表示されていないホーム画面の上に表示された場合、値は「launcher」となります）、 オーバーラップの日時、 オーバーラップされているアプリケーションに関する情報： 本ソフトウェアのパッケージ名、 オーバーラップの幅、

- 使用中のWi-Fi アクセスポイントの設定（検出された端末種別、 DHCP 設定（ローカル IPv6、DHCP IPv6、DNS1 IPv6、DNS2 IPv6 のゲートウェイのチェックサム、 ネットワークプレフィックス長のチェックサム、ローカル IPv6 アドレスのチェックサム）、 DHCP 設定（ゲートウェイのローカル IP アドレス、DHCP IP、DNS1 IP、DNS2 IP、およびサブネットマスクのチェックサム）、 DNS ドメインが存在するかどうかのフラグ、 割り当てられたローカル IPv6 アドレスのチェックサム、 割り当てられたローカル IPv4 アドレスのチェックサム、 端末がルート化されているかを示すフラグ、 Wi-Fi ネットワーク認証の種別、 利用可能な Wi-Fi ネットワークの一覧とその設定、 アクセスポイントの MAC アドレスのチェックサム（修飾子を含む MD5）、 アクセスポイントの MAC アドレスのチェックサム（修飾子を含む SHA256）、 Wi-Fi アクセスポイントでサポートされる接続種別、 Wi-Fi ネットワークの暗号化種別、 Wi-Fi ネットワーク接続を開始および終了したローカル時刻、 アクセスポイントの MAC アドレスに基づく Wi-Fi ネットワークの識別子、 Wi-Fi ネットワーク名に基づく Wi-Fi ネットワークの識別子、 アクセスポイントの MAC アドレスおよび Wi-Fi ネットワーク名に基づく Wi-Fi ネットワークの識別子、 Wi-Fi 信号強度、 Wi-Fi ネットワークの名前、 現行設定でサポートされるセキュリティプロトコルの一式、 WPA-EAP 接続で使用される認証プロトコル、 内部認証プロトコル、 現行設定でサポートされるストリーム暗号の一式、 現行設定で鍵管理プロトコルの一式、 本ソフトウェア内でのネットワークの最終的なプライバシーカテゴリ、 本ソフトウェア内でのネットワークの最終的なセキュリティカテゴリ、 この設定でサポートされる WPA のブロック暗号の一式、 現行設定でサポートされるセキュリティプロトコルの一式）、

- 本ソフトウェアのインストールの日時、 ソフトウェアのアクティベーション日、 本ソフトウェアのライセンスの注文を受けた代理店組織の識別子、 ライセンスに基づく本ソフトウェアの識別子、 本ソフトウェアのライセンス情報ファイルのシリアル番号、 ソフトウェアの言語版、 KSN への参加が有効になっているかどうかを示すフラグ、 ライセンス済みの本ソフトウェアの識別子、 ソフトウェアのライセンスの識別子、 OS の識別子、 OS のビット数。

また、本ソフトウェアの提供する保護機能の効率性を向上させるため、権利者は、端末に損害を与え、情報セキュリティ上の脅威を作成する目的で侵入者に悪用される可能性のあるオブジェクトを受け取ることがあります。

上記の情報の KSN へのご提供は任意です。Kaspersky Security Network への参加を取りやめることは、いつでも可能です。

危険サイトブロックの使用を目的としたデータ処理に関する声明に基づくデータ提供

危険サイトブロックに関する声明に基づき、危険サイトブロックを機能させる目的で、権利者はデータを処理します。ここに記載する目的には、クラウドサービス Kaspersky Security Network（KSN）を使用した Web 上の脅威の検知、および閲覧した Web サイトのカテゴリの決定が含まれます。

お客様の同意を得た上で、本声明に従って、次のデータが自動的かつ定期的に権利者へ送信されます：

- 本ソフトウェアのバージョン、端末の一意な識別子、インストールの一意な識別子、本ソフトウェアの種別。
- ページの URL、ポート番号、URL のプロトコル、リクエストされた情報を参照する URL。

マーケティング目的に沿ったデータ処理に関する声明に基づくデータ提供

権利者はサードパーティの事業者の情報環境を使用してデータを処理します。このようなサードパーティ事業者の情報環境によるデータ処理は、サードパーティの情報環境に適用されるプライバシー声明によって規定されています。権利者が使用するサービスと、処理するデータは次の通りです：

Firebase 向け Google アナリティクス

本ソフトウェアの使用中に、次に記載する目的のため、次のデータが定期的に Firebase 向け Google アナリティクスに自動送信されます：

- アプリ情報（アプリのバージョン、アプリの識別子、Firebase サービスのアプリの識別子、Firebase サービスのインスタンス ID、製品を入手した店舗の名前、ソフトウェアを最初に起動した日時）
- デバイスへの製品のインストールの ID とデバイスへのインストールの方法。
- 地域と使用言語に関する情報
- デバイスの画面解像度に関する情報
- ルートを取得しているユーザーに関する情報
- SafetyNet Attestation サービスによる端末に関する診断情報
- ユーザー補助機能としての Kaspersky Endpoint Security for Android の設定に関する情報
- アプリケーションスクリーンの遷移、セッションの長さ、スクリーンセッションの開始および終了、スクリーン名に関する情報
- Firebase サービスへのデータの送信に使用されるプロトコル、バージョン、使用されるデータ送信方法の識別子に関する情報
- データが提供されるイベントの種別とパラメータの詳細
- 本アプリのライセンスとその使用可否、デバイスの数に関する情報
- 定義データベースのアップデート頻度、および管理サーバーとの同期の頻度に関する情報
- 管理コンソールに関する情報（Kaspersky Security Center またはサードパーティ製の EMM システム）
- Android ID
- 広告識別子（Advertising ID）
- ユーザーに関する情報： 年齢カテゴリと性別、居住国の識別子、関心のリスト
- 本ソフトウェアがインストールされた端末に関する情報： 端末の製造元の名前、端末の種別、型番、オペレーティングシステムのバージョンおよび言語（地域）、本ソフトウェアが最近の 7 日間またはそれ以前に初回起動されたかに関する情報

  データはセキュアな通信で Firebase に転送されます。データが Firebase でどのように処理されるかの詳細は、次を参照してください：https://firebase.google.com/support/privacy

SafetyNet Attestation

本ソフトウェアの使用中に、本声明に記載の目的で、次のデータが定期的に自動で SafetyNet Attestation 宛てに送信されます：

- デバイスを確認する時間
- 本アプリに関する情報、本アプリの証明書の名前とデータ
- デバイスの確認結果
- デバイスの確認結果を検証するためのランダムな識別子チェック

  データはセキュアな通信で SafetyNet Attestation に転送されます。SafetyNet Attestation においてデータがどのように処理されるかの情報は、次を参照してください：https://policies.google.com/privacy

Firebase Performance Monitoring

本ソフトウェアの使用中に、以下に記載する目的のため、次のデータが定期的に Firebase Performance Monitoring に自動で送信されます：

- 本ソフトウェアのインストールの一意な識別子
- 本ソフトウェアのパッケージ名
- インストールされた本ソフトウェアのバージョン
- バッテリーレベルおよびバッテリー充電状態
- 通信事業者
- アプリがフォアグラウンドかバックグラウンドかの状態
- 地域
- IP アドレス
- 端末の言語コード
- 電波の受信状況およびデータ通信の接続状況に関する情報
- 匿名化されたソフトウェアのインスタンスの識別子
- RAM およびディスクサイズ
- 端末がジェイルブレイクまたはルート化されているかを示すフラグ
- 信号強度
- 自動トレースの期間
- ネットワーク、および次に対応する情報： 応答コード、ペイロードのサイズ（バイト）、応答時間
- 端末の説明

  データはセキュアな通信で Firebase Performance Monitoring に転送されます。Firebase Performance Monitoring においてデータがどのように処理されるかの情報は、次を参照してください：https://firebase.google.com/support/privacy

Crashlytics

本ソフトウェアの使用中に、以下に記載する目的のため、次のデータが定期的に Crashlytics に自動で送信されます：

- ソフトウェア識別子
- インストールされた本ソフトウェアのバージョン
- 本ソフトウェアがバックグラウンドで実行しているかどうかを示すフラグ
- CPU アーキテクチャ
- イベントの一意な識別子
- イベントの日時
- 端末の機種
- ディスク容量の合計および現在の使用量
- OS の名前およびバージョン
- 合計 RAM および現在の使用量
- 端末がルート化されているかを示すフラグ
- イベント時の画面の向き
- 製品または端末の製造元
- 本ソフトウェアのインストールの一意な識別子
- 送信中の統計情報のバージョン
- 本ソフトウェアのインストール種別
- エラーメッセージ本文
- 本ソフトウェアの例外が、例外のネストによって発生したかどうかを示すフラグ
- スレッド ID
- フレームが本ソフトウェアのエラーの原因であるかどうかを示すフラグ
- 本ソフトウェアの予期しない終了の原因となったスレッドを示すフラグ
- 本ソフトウェアの予期しない終了の原因となった信号に関する情報： 信号の名前、信号のコード、信号のアドレス
- スレッド、例外、エラーに関連付けられた各フレーム： フレームファイルの名前、フレームファイルの行番号、デバッグ記号、バイナリイメージ内のアドレスおよびオフセット、フレームを含むライブラリの表示名、フレームの種別、フレームがエラーの原因かどうかを示すフラグ
- OS の識別子
- イベントに関連付けられた問題の識別子

- 本ソフトウェアが予期せず終了する前に発生したイベントに関する情報： イベントの識別子、イベントの日時、イベントの種別と値
- CPU レジスタ値
- イベントの種別と値

  データはセキュアな通信で Crashlytics に転送されます。Crashlytics においてデータがどのように処理されるかの情報は、次を参照してください：https://firebase.google.com/terms/crashlytics-app-distribution-data-processing-terms

上記の情報をマーケティング目的で処理するために提供するかどうかは任意です。

Kaspersky Security for iOS でのデータ提供

Kaspersky Security for Mobile は、一般データ保護規則（General Data Protection Regulations：GDPR）に準拠しています。

本アプリをインストールするには、モバイルデバイスユーザーが、ユーザーの個人データの処理に関する次の声明の条項に同意する必要があります：

- 使用許諾契約書
- カスペルスキーの製品およびサービスに関するプライバシーポリシー

オプションとして、ユーザーは、次の声明の条項に同意することができます：

- Kaspersky Security Network に関する声明

ユーザーは、Kaspersky Security for iOS の［**製品情報**］→［**契約書と声明**］セクションで、これらのドキュメントの条項をいつでも表示できます。このセクションで、ユーザーは KSN 声明の条項に同意するか、拒否するかを選択することもできます。

Kaspersky Security Network との情報交換

リアルタイム保護を改善するため、Kaspersky Security for iOS は**危険サイトブロック**コンポーネントの動作で Kaspersky Security Network クラウドサービスを使用します。KSN から取得したデータを使用して、Web リソースが開かれる前にそのリソースをスキャンします。

危険サイトブロックの動作中、KSN を使用している時にカスペルスキーに送信されるデータの種別に関する情報は、使用許諾契約書に記載されています。使用許諾契約書の諸条項に同意すると、この情報の送信に同意したことになります。

Kaspersky Security for iOS モバイルアプリの動作中、KSN の使用時にカスペルスキーに送信されるデータの種別に関する情報は、使用許諾契約書に記載されています。声明の諸条項に同意すると、この情報の送信に同意したことになります。

使用許諾契約書に基づくデータ提供

本ソフトウェアをアクティベートする際にアクティベーションコードを使用すると、お客様が本ソフトウェアを正規の用途で利用していることを確認するために、次の情報を定期的に権利者に提供することに同意したことになります：

- 権利者のインフラストラクチャへのリクエストに含まれるデータの形式、 アクセスされた Web サービスの IPv4 アドレス、 権利者のインフラストラクチャへのリクエストに含まれる内容のサイズ、 プロトコルの識別子、 本ソフトウェアのアクティベーションコード、 データ圧縮種別、 本ソフトウェアの識別子、 ユーザーの端末でアクティベートできるソフトウェアの識別子セット、 ソフトウェアの言語版、 本ソフトウェアの詳細バージョン、 一意な端末の識別子、 お客様の端末の日時、 ソフトウェアのインストール識別子（PCID）、 現在使用されている本ソフトウェアのアクティベーションコード、 OS バージョン、OS ビルド番号、OS アップデート番号、OS のエディション、OS のエディションに関する詳細情報、 端末の機種、 通信事業者のコード、 オペレーティングシステムのグループ、 ライセンスに基づく本ソフトウェアの識別子、 本ソフトウェアがユーザーに表示した契約のリスト、 本ソフトウェアの使用中にユーザーが同意した法的文書の種別、 本ソフトウェアの使用中にユーザーが同意した法的文書のバージョン、 本ソフトウェアの使用中にユーザーが法的文書の項目に同意したかどうかを示すフラグ、 処理中のオブジェクトのチェックサム種別、 ソフトウェアのライセンスのヘッダー、 地域のアクティベーションセンターの識別子、 ソフトウェアのライセンス情報ファイルの作成日、 ソフトウェアのライセンスの識別子、 本ソフトウェアのライセンスの提供に使用された情報形式の識別子、 ソフトウェアのライセンスの有効期限、 本ソフトウェアのライセンス情報ファイルの現在のステータス、 適用されたライセンスの種別、 本ソフトウェアをアクティベートするのに使用したライセンスの種別、 ライセンスに基づく本ソフトウェアの識別子。

権利者は、このような情報を権利者の本ソフトウェアの使用および配布状況の統計情報を収集するために使用することがあります。

デバイスを情報セキュリティ上の脅威から保護する目的で、エンドユーザーは次の情報を権利者に定期的に送信することに同意したことになります：

- 権利者のインフラストラクチャへのリクエストに含まれるデータの形式、 アクセスされた Web サービスのアドレス（URL、IP）、 ポート番号、 Web サービスのリクエスト元の Web アドレス（リファラー）、

- 本ソフトウェアの詳細バージョン、 ソフトウェアアップデートの識別子、 インストールされた本ソフトウェアの種別、 本ソフトウェアの識別子、 設定識別子、 本ソフトウェアの動作の結果、 エラーコード。

- 処理中の Web アドレス、 アクセスされた Web サービスの IPv4 アドレス、 スキャンしたオブジェクトのデジタル証明書のサムプリントとハッシュアルゴリズム、 証明書の種別、 処理中のデジタル証明書の内容。

Kaspersky Security Network に関する声明に基づくデータ提供

KSN 声明に同意した場合、権利者は自動的に次のデータを収集および処理します：

- KSN サービス動作の品質に関する情報（KSN とのデータ交換に使用されたプロトコル、 本ソフトウェアがアクセスした KSN サービスの識別子、 統計の収集を停止した日時、 キャッシュから取得された KSN 接続の数、 ローカルのリクエストデータベースにある応答ありのリクエストの数、 失敗した KSN 接続の数、 失敗した KSN トランザクションの数、 KSN へのリクエストのキャンセルの時間分布、 失敗した KSN への接続の時間分布、 失敗した KSN のトランザクションの時間分布、 成功した KSN への接続の時間分布、 成功した KSN の処理の時間分布、 成功した KSN へのリクエストの時間分布、 タイムアウトした KSN へのリクエストの時間分布、 新規の KSN 接続の数、 ルーティングのエラーによって失敗した KSN へのクエリの数、 本ソフトウェアの設定で KSN が無効にされているために失敗したクエリの数、 ネットワークの問題によって失敗した KSN へのクエリの数、 成功した KSN 接続の数、 成功した KSN トランザクションの数、 KSN へのクエリの合計数、 統計の収集を開始した日時）。

- デバイス ID、 本ソフトウェアの詳細バージョン、 ソフトウェアアップデートの識別子、 ソフトウェアのインストール識別子（PCID）、 インストールされた本ソフトウェアの種別。

- 本ソフトウェアのインストールの日時、 ソフトウェアのアクティベーション日、 ソフトウェアの言語版、 KSN への参加が有効になっているかどうかを示すフラグ、 ライセンス済みの本ソフトウェアの識別子、 ソ

フトウェアのライセンスの識別子、 OS の識別子、 お客様の端末にインストールされているオペレーティングシステムのバージョン、 OS のビット数。

上記の情報の KSN へのご提供は任意です。Kaspersky Security Network への参加を取りやめることは、いつでも可能です。

テクニカルサポートへの問い合わせ

このセクションでは、テクニカルサポートを受ける方法と、ご利用条件について説明します。

テクニカルサポートのご利用方法

本製品のガイドや、本製品のその他のどの情報源でも問題を解決できない場合、テクニカルサポートにお問い合わせください。テクニカルサポート担当者が、本製品のインストール方法や使用方法についてのお問い合わせに回答いたします。

カスペルスキーによる本製品のサポートは、本製品のライフサイクル期間中に提供されます（製品のサポートライフサイクルのページを参照）。テクニカルサポートに連絡する前に、「サポートサービス規約」をお読みください。

テクニカルサポートへのご連絡方法は、次のページをご参照ください：

- テクニカルサポートサイトを参照する
- カスペルスキーカンパニーアカウントポータルからカスペルスキーのテクニカルサポートに問い合わせる

カスペルスキーカンパニーアカウントによるテクニカルサポート

カスペルスキーカンパニーアカウントは、カスペルスキー製品をご利用中のお客様に提供される、法人向けのポータルです。カスペルスキーカンパニーアカウントポータルは、ユーザーとカスペルスキーの担当者が、オンラインでのやりとりをスムーズに行えるよう設計されています。カンパニーアカウントを利用すると、オンラインでのお問い合わせの進捗状況を確認したり、履歴を保管したりすることができます。

カンパニーアカウントは、1つのアカウントにお客様の社員全員を登録できます。1つのアカウントによって、登録された社員が送信するオンラインでのお問い合わせを一元的に管理することができます。また、カンパニーアカウントを使用して、社員の権限を管理することもできます。

カンパニーアカウントポータルは、次の言語でご利用になれます：

- 英語
- スペイン語
- イタリア語
- ドイツ語
- ポーランド語
- ポルトガル語
- ロシア語
- フランス語

- 日本語

カンパニーアカウントの詳細については、テクニカルサポートサイトにアクセスしてください。

製品に関する情報源

カスペルスキーの Web サイトの Kaspersky Security for Mobile のページ

Kaspersky Security for Mobile のページでは、製品とその機能や操作パラメータについて、全般的な情報を確認できます。

本製品のご購入に関するリンクや、販売代理店の一覧へのリンクも含まれています。

ナレッジベースの Kaspersky Security for Mobile のページ

*ナレッジベース*は、テクニカルサポートサイトの一部です。

ナレッジベースの Kaspersky Security for Mobile のページに、製品の購入、インストール、使用方法について、役立つ情報、推奨事項、およびよくある質問への回答が掲載されています。

ナレッジベースの回答には、Kaspersky Security for Mobile だけでなく、他のカスペルスキー製品に関するものなども含まれています。また、テクニカルサポートからのニュースを含む場合もあります。

ヘルプ

製品にはヘルプファイルが付属しています。

Kaspersky Security for Mobile の管理プラグインのコンテキストヘルプでは、Kaspersky Security Center の各ウィンドウの情報を確認できます。Kaspersky Security for Mobile の設定の説明や、それらの設定を使用するタスクの説明へのリンクが記載されています。

フルヘルプでは、Kaspersky Endpoint Security for Android アプリおよび Kaspersky Security for iOS アプリの設定方法および使用方法に関する情報が記載されています。

カスペルスキーのコミュニティ

特に緊急の対応が必要ではない場合は、カスペルスキーのフォーラムをご利用ください。ここでは、カスペルスキーのエキスパートやカスペルスキー製品のユーザーが様々なトピックで意見を交換しています。

このフォーラムでは、既存のトピックの参照、コメントの書き込み、新しいトピックの作成ができます。

用語解説

Android 仕事用プロファイル

ユーザーのデバイスにある安全な環境。管理者はこの環境の中で、ユーザーによる個人情報の使用を制限することなくアプリとユーザーアカウントの管理ができます。ユーザーのモバイルデバイスに仕事用プロファイルが作成されると、次の企業アプリが仕事用プロファイルに自動インストールされます：Google Play Market、Google Chrome、Downloads、Kaspersky Endpoint Security for Android など。仕事用プロファイルにインストールされた企業アプリとそれらのアプリの通知は、赤いブリーフケースのアイコンで表示されます。Google Play アプリを使用するには、Google の企業アカウントを別途作成する必要があります。仕事用プロファイルにインストールされたアプリは、アプリの共通リストに表示されます。

Apple Push Notification サービス（APNs）証明書

Apple Push Notification の使用を可能とする、Apple により署名された証明書。Apple Push Notification を使用すると、iOS MDM サーバーで iOS 端末を管理できます。

EAS デバイス

Exchange ActiveSync プロトコルを介して管理サーバーに接続されるモバイルデバイス。

Exchange モバイルデバイスサーバー

Kaspersky Endpoint Security のコンポーネントの 1 つ。Exchange ActiveSync モバイルデバイスを管理サーバーに接続できるようにします。

IMAP

メールにアクセスするためのプロトコル。POP3 プロトコルと異なり、IMAP はメールボックスを操作するための拡張機能を提供します。フォルダー管理や、メールボックスサーバーからコンテンツをコピーせずに行えるメッセージ処理などの機能があります。IMAP プロトコルはポート 134 を使用します。

iOS MDM サーバー

Kaspersky Endpoint Security のコンポーネント。クライアントデバイスにインストールされ、iOS モバイルデバイスを管理サーバーに接続できるようにします。また、Apple Push Notifications サービス（APNs）によりこれらの iOS モバイルデバイスを管理できるようにします。

iOS MDM デバイス

iOS MDM サーバーによって制御される iOS モバイルデバイス。

iOS MDM プロファイル

iOS モバイルデバイスを管理サーバーに接続するための設定のセットが指定されたプロファイル。iOS MDM プロファイルにより、iOS MDM サーバーを使用してバックグラウンドモードで iOS 設定プロファイルを配信できます。また、モバイルデバイスに関する拡張診断情報を受信できます。iOS MDM サーバーがユーザーの iOS モバイルデバイスを検出し、接続できるようにするため、iOS MDM プロファイルへのリンクをユーザーに送信する必要があります。

Kaspersky Private Security Network（プライベート KSN）

Kaspersky Private Security Network を使用すると、カスペルスキー製品がインストールされたユーザーデバイスから Kaspersky Security Network の評価データベースやその他の統計データへアクセスできます。デバイスからデータが Kaspersky Security Network へ送信されることはありません。Kaspersky Private Security Network は、Kaspersky Security Network への参加が次のいずれかの理由で不可能である企業のお客様向けに設計されています：

- ユーザーデバイスがインターネットに接続されていない。
- 国外、または企業 LAN の外部へのデータ転送が、法律や企業のセキュリティポリシーで禁止されている。

Kaspersky Security Center Web サーバー

管理サーバーとともにインストールされている Kaspersky Security Center のコンポーネント。Web サーバーは、スタンドアロンのインストールパッケージ、iOS MDM プロファイル、および共有フォルダーのファイルをネットワーク経由で転送するためのものです。

Kaspersky Security Center 管理者

Kaspersky Security Center の一元化された遠隔管理システムを使用して、製品の動作を管理する担当者。

Kaspersky Security Network（KSN）

Kaspersky Security Network は、カスペルスキーのデータベースへのアクセスを提供する、クラウドサービスの基盤です。このデータベースにはファイル、Web リソース、ソフトウェアの評価に関する情報が含まれており、それらの情報は常に更新されています。Kaspersky Security Network により、脅威に対するカスペルスキー製品の対応が迅速化され、保護コンポーネントのパフォーマンスが向上し、誤検知の可能性も低減されます。

POP3

メールサーバーからメッセージを受信するため、メールクライアントで使用するネットワークプロトコル。

SSL

ローカルネットワークとインターネットで使用するデータ暗号化プロトコル。Secure Sockets Layer（SSL）プロトコルはクライアントとサーバー間のセキュアな接続を確立するために Web アプリケーションで使用されます。

アクティベーションコード

Kaspersky Endpoint Security の使用に必要なライセンスの購入時に受け取るコード。このコードは製品のアクティベーションに必要です。

アクティベーションコードは、XXXXX-XXXXX-XXXXX-XXXXX の形式の 20 文字の一意な英数字です。

アプリケーション管理プラグイン

管理コンソールを使用してカスペルスキー製品を管理するためのインターフェイスを備えた専用のコンポーネント。Kaspersky Security Center SPE で管理できるアプリケーションごとに、独自の管理プラグインがあります。この管理プラグインは、Kaspersky Security Center から管理できるすべてのカスペルスキー製品に含まれています。

インストールパッケージ

カスペルスキー製品のリモートインストール用に作成されるファイルセット。リモート管理システムを使用して作成します。インストールパッケージは、アプリケーションの配布パッケージに含まれる特別なファイルから作成されます。パッケージには、アプリケーションのインストールやインストールの直後にアプリケーションを実行するための様々な設定が含まれています。配布キットの設定値は、アプリ設定の既定値に対応しています。

ウイルス

他のソフトウェアに自分自身のコードを追加することによって、そのソフトウェアに感染するプログラム。感染したファイルが実行されると、ウイルスにコントロールを奪われます。この単純な定義により、ウイルスにより実行される主な動作（感染）を特定できます。

隔離

カスペルスキー製品が検知した、感染の可能性があるオブジェクトを移動するフォルダー。隔離されたオブジェクトは、コンピューターに影響を与えないようにするために暗号化された形式で隔離に保管されます。

カスペルスキーのアップデートサーバー

カスペルスキーの HTTP サーバー。カスペルスキー製品はここから定義データベースや製品モジュールのアップデートをダウンロードします。

カスペルスキーのカテゴリ

カスペルスキーにより開発された事前定義済みデータカテゴリ。カテゴリは定義データベースのアップデート中にアップデートされることがあります。セキュリティ担当者が事前定義済みカテゴリを変更または削除することはできません。

監視対象のデバイス

Apple Configurator で設定が監視される iOS デバイスです。Apple Configurator は、iOS デバイスにグループ設定を適用するアプリケーションです。Apple Configurator では、監視対象のデバイスは「*管理されています*」と表示されます。監視対象のデバイスがコンピューターに接続するたびに、Apple Configurator はその設定が指定された設定に準拠しているかどうか確認し、必要に応じて修正します。監視対象のデバイスと、別のコンピューターにインストールされている Apple Configurator とを同期させることはできません。

Kaspersky Device Management for iOS のポリシーを使用して再設定する監視対象の全デバイスの設定項目は、監視対象でないデバイスよりも多くなります。たとえば、企業ネットワーク内のデバイスのインターネットトラフィックを監視する目的で、HTTP プロキシサーバーの設定を指定することができます。既定では、すべてのモバイルデバイスは監視対象外です。

管理グループ

管理対象デバイスのセット。モバイルデバイスは、実行する機能やインストール済みのアプリのセットなどによってグループ分けされます。管理対象デバイスは、全体として1つのものとして管理できるようにグループ分けされます。たとえば、同じオペレーティングシステムを持つモバイルデバイスを1つの管理グループにまとめることができます。1つのグループに他の管理グループを含めることができます。グループ内のデバイスに対して、グループポリシーやグループタスクを作成できます。

管理サーバー

企業ネットワークにインストールされているすべてのカスペルスキー製品に関する情報を一元的に保管する Kaspersky Security Center のコンポーネント。これらのカスペルスキー製品の管理にも使用できます。

管理者用ワークステーション

Kaspersky Security Center 管理コンソールが導入されたコンピューター。管理者用ワークステーションにアプリケーション管理プラグインがインストールされている場合、管理者はユーザーのデバイスに導入された Kaspersky Endpoint Security モバイルアプリを管理できます。

グループタスク

管理グループ用に作成され、そのグループに含まれるすべての管理対象デバイスで実行されるタスク。

コンプライアンスコントロール

モバイルデバイスと Kaspersky Endpoint Security for Android の設定が企業のセキュリティ要件に準拠していることの確認。企業のセキュリティ要件には、ユーザーがデバイスをどのように使用できるかが規定されています。たとえば、デバイスでリアルタイム保護を必ず有効にすること、定義データベースを必ずアップデートすること、デバイスのパスワードが十分な強度であることなどです。コンプライアンスコントロールは、ルールのリストに基づきます。コンプライアンスルールには、次の項目が含まれます：

- デバイスチェック基準（例：デバイスでブロックされたアプリがない）。
- ルール違反を修正するまでユーザーに与えられる期間（例：24 時間）。
- 設定された期間内にルール違反を是正しない場合にデバイスで実行される処理（例：デバイスのロック）。

使用許諾契約書

お客様と AO Kaspersky Lab との間で締結され、本アプリを使用する条件を規定する拘束力のある契約。

証明書署名依頼

管理サーバーの設定が入ったファイル。カスペルスキーの確認を受けた後、APNs 証明書を取得するために Apple に送信します。

スタンドアロンインストールパッケージ

Android オペレーティングシステム用の Kaspersky Endpoint Security のインストールファイル。管理サーバーに Kaspersky Endpoint Security を接続するための設定が入っています。Kaspersky Endpoint Security のインストールパッケージをベースに作成される、特別なモバイルアプリパッケージです。

定額制サービス

選択した設定（有効期限やデバイスの台数）に従ってアプリケーションを使用できるようにします。定額制サービスは一時停止したり再開したりできます。また、自動的に更新することも、定額制サービスをやめることもできます。

定義データベース

定義データベースの公開日の時点でカスペルスキーが把握しているコンピューターセキュリティの脅威に関する情報が含まれたデータベース。定義データベースのレコードにより、悪意のあるコードをオブジェクトのスキャン中に検知することが可能になります。定義データベースはカスペルスキーにより作成され、1時間ごとにアップデートされます。

デバイス管理者

Android におけるアプリの権限のセットで、アプリに対してデバイス管理ポリシーを使用できるようにします。Android デバイスでは、Kaspersky Endpoint Security のすべての機能を実装する必要があります。

フィッシング

ユーザーの機密情報への不正アクセスを目的としたオンライン詐欺の一種。

プロキシサーバー

ユーザーが他のネットワークサービスに間接的に要求を行えるようにするコンピューターネットワークサービス。まず、ユーザーはプロキシサーバーに接続し、別のサーバーにある特定のリソース（ファイルなど）を要求します。次に、プロキシサーバーは、指定されたサーバーに接続してそこからリソースを取得するか、自身のキャッシュからリソースを返します（プロキシに独自のキャッシュがある場合）。場合によっては、ユーザーの要求またはサーバーの応答を特定の目的のためにプロキシサーバーが修正することがあります。

プロビジョニングプロファイル

iOS モバイルデバイスを使用するために必要なアプリの設定群。プロビジョニングプロファイルは、ライセンス情報を含んでおり、特定のアプリにリンクされます。

ポリシー

管理グループ内のデバイスまたは個々のデバイスに適用されるアプリと Kaspersky Endpoint Security モバイルアプリの設定のセット。管理グループごとに異なるポリシーを適用できます。ポリシーには、Kaspersky Endpoint Security モバイルアプリのすべての機能の設定が定義されています。

本アプリのアクティベーション

本アプリの機能を制限のない状態で使用できるようにします。アクティベーションは、アプリのインストール中またはインストール後にユーザーが実行します。アクティベーションコードかライセンス情報ファイルが、アクティベーションには必要です。

マニフェストファイル

Web サーバーに配置されているアプリのファイル（IPA ファイル）へのリンクが記載された PLIST 形式のファイル。iOS デバイスが Web サーバーでアプリを見つけ、ダウンロードし、インストールするために使用します。

ライセンス

使用許諾契約書に基づいて許可された本アプリを使用するための期限付きの権利。

ライセンス期間

製品機能へのアクセスと追加サービスを使用する権利を持つ期間。使用可能なサービスは、ライセンスの種別により異なります。

ライセンス情報ファイル

xxxxxxxx.key 形式のファイル。試用版ライセンスまたは製品版ライセンスに基づいてカスペルスキー製品の使用を有効にします。ライセンス情報ファイルは、アクティベーションコードに基づいて生成されます。本製品は、ライセンス情報ファイルがある場合のみ利用可能です。

ロック解除コード

Kaspersky Security Center で取得可能なコード。**ロックと GPS 追跡**、**遠隔アラーム**、**遠隔撮影**のコマンドの実行後、またはセルフディフェンスの起動後は、デバイスのロックを解除しておく必要があります。

サードパーティ製のコードに関する情報

サードパーティ製コードに関する情報は、次のファイルをダウンロードして読むことができます：

- legal_notices_Android.txt（Kaspersky Endpoint Security for Android アプリ用）
- legal_notices_iOS.txt（Kaspersky Security for iOS アプリ用）

モバイルデバイスでは、サードパーティ製のコードに関する情報は、モバイルアプリの［**製品情報**］セクションで確認できます。

商標に関する通知

登録商標とサービスマークに関する権利は各所有者に帰属します。

PostScript は Adobe の米国およびその他の国における商標または登録商標です。

AirDrop、 AirPrint は Apple Inc. の商標です。

Apple、Apple Configurator、AirPlay、AirPort Express、App Store、 Apple TV、Bonjour、Face ID、FaceTime、FileVault、iBooks、iCal、iCloud、iPad、iPadOS、iPhone、iTunes、OS X、Safari、Spotlight、Touch ID は Apple Inc. の商標であり、米国およびその他の国と地域で登録されています。

Aruba Networks は、 Aruba Networks, Inc. の商標であり、米国およびその他の一部の国で登録されています。

Bluetooth のワードマーク、およびロゴは Bluetooth SIG, Inc. の所有財産です。

Cisco、Cisco AnyConnect、IOS は、 Cisco Systems, Inc. およびその子会社の商標であり、米国およびその他の一部の国で登録されています。

SecurID は EMC Corporation の商標または登録商標であり、米国およびその他の国で登録されています。

Google、Android、Chrome、Chromebook、Chromium、Crashlytics、Firebase、Google Analytics、Google Chrome、Google Mail、Google Maps、Google Play、Nexus、SPDY は Google LLC の商標です。

HTC は HTC Corporation の商標です。

Huawei、HUAWEI、および EMUI は Huawei Technologies Co., Ltd の商標であり、中国およびその他の国で登録されています。

IBM、 Maas360 は International Business Machines Corporation の商標であり、世界各国の多くの地域で登録されています。

Juniper Networks、 Juniper、 JUNOS は Juniper Networks, Inc. の商標であり、米国およびその他の国で登録されています。

Microsoft、 ActiveSync、 Microsoft Intune、 Tahoma、 Windows、 Windows Mobile、 Windows Phone は、 Microsoft グループ企業の商標です。

MOTOROLA、図案化された M ロゴは、 Motorola Trademark Holdings, LLC の商標または登録商標です。

Oracle、 JavaScript は Oracle およびその子会社の登録商標です。

BlackBerry の商標は Research In Motion Limited の所有財産であり、米国で登録済み、他の国で登録済みまたは登録申請中です。

Samsung は SAMSUNG の米国および他の国における商標です。

SonicWALL、 Aventail、 SonicWALL Mobile Connect は SonicWall, Inc. の商標です。

SOTI、MobiControl は SOTI Inc. の登録商標であり、米国およびその他の地域で登録されています。

Symantec は Symantec Corporation またはその子会社の商標または登録商標であり、米国およびその他の国で登録されています。

Symbian の商標は Symbian Foundation Ltd. の所有財産です。