

2025年5月版

KINGSOFT

セキュリティ対策アプリ

Mobile Security Plus

ユーザーマニュアル

あなたのスマートフォンを狙う脅威から
クラウド技術が守ります。



Android端末向けアプリ



iOS端末向けアプリ

※操作画面、操作手順は「端末機種」や「OSバージョン」により異なる場合があります。

※内容の全部または一部は予告なく変更される場合があります。

※本資料記載の各企業名、企業ロゴ、サービス名は各社の商標、または登録商標です。

2025年5月版

目次

- P3. モバイル端末に迫る脅威
- P4. フィッシングサイト／不正アプリの脅威
- P5. KINGSOFT Mobile Security Plus製品概要
- P6. インストールと認証方法
- P7. 盗難対策機能説明
- P8.9. 盗難対策機能の初期設定の手順
- P10. 利用端末の変更方法
- P11. アドクリーナーとの機能連携の手順
- P12. サポート窓口のご案内

あなたのモバイル端末に迫る脅威

情報セキュリティ10大脅威

順位 「個人」向け脅威 ※1

1. インターネット上のサービスからの個人情報の窃取
2. インターネット上のサービスへの不正ログイン
3. クレジットカード情報の不正利用
4. スマホ決済の不正利用
5. 偽警告によるインターネット詐欺
6. ネット上の誹謗・中傷・デマ
7. フィッシングによる個人情報等の詐取
8. 不正アプリによるスマートフォン利用者への被害
9. メールやSMS等を使った脅迫・詐欺の手口による金銭要求ワンクリック請求等の不当請求による金銭被害

※1. 出典：独立行政法人情報処理推進機構 セキュリティセンター
『情報セキュリティ10大脅威 2025「個人」および「組織」向けの脅威の順位』



サイバーセキュリティ三原則※2

- 原則1 ソフトウェアの更新
- 原則2 IDとパスワードの適切な管理
- 原則3 不用意に開かない・インストールしない

※2. 出典：総務省

国民のための際—バーセキュリティサイト「サーバーセキュリティ初心者のための三原則」
https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/intro/intro_beginner.html

フィッシングサイト／不正アプリの脅威

iOS端末にも対策が必要！巧妙化するフィッシングサイト



アカウント情報の詐取を 目的にメール ⇒ 偽サイトへ

クレジットカードや銀行口座情報などに加え、アカウント情報（ID、パスワード）も狙われています。特にApple IDの場合、 iCloudへ保存されている連絡先から各サービスのID、パスワードまで、芋づる式に情報が詐取されるため、被害が拡大します。



アカウント・秘匿情報の流出

ID、パスワード情報や写真や動画といった私的な情報を詐取。これらをもとに脅迫などの犯罪リスクも。



不正購入・金銭的被害

アカウント情報流出により不正ログインされ、高額な請求がされるリスクがあります。

※出典：フィッシング対策協議会「Appleをかたるフィッシング（2019/08/20）」

実際に被害があったAndroid 端末のウイルス例

詐欺サイト



正規サイト

宅配業者を偽った 不正アプリインストール誘導

正規サイトとそっくりな偽サイトが急増。不正アプリをインストールしてしまうと、勝手にSMSで「詐欺メールのバラマキ」をされたり、iTunesなどの「プリペイドでの決済」をされたりします。家族や友人、知人へも金銭的被害が広がります。



偽バッテリー節約アプリ

「バッテリーを長持ちさせる」という無料アプリ。実際にそんな効果はなく、ユーザー登録で個人情報抜き取りうとしてきます。



アカウント乗っ取り

Xと連携するアプリの中にも危険なアプリが。一度連携すると身に覚えのない投稿を乱発します。

KINGSOFT Mobile Security Plus 製品概要

端末を保護するセキュリティ機能



アンチウイルス

Android

Android端末にインストールしたアプリをスキャンし、悪質なアプリを検出します。ウイルス情報は常に更新され、アプリのインストール時にはセキュリティ監視を行います。



セーフブラウザ

Android

iOS

不正サイトへのアクセスをブロックし、安全にWebサイトの閲覧ができます。アプリ内だけでなく、普段使用しているChromeなどのブラウザでもブロック可能です。



盗難対策

Android

iOS

端末を紛失した際に、端末の位置情報を確認することができます。Android端末であれば、画面ロックやアラームを鳴らすことも可能です。



QRコード フィッシングブロック

Android

iOS

QRコードを読み込むとフィッシングサイトの判別が行えます。アプリ内カメラのQRコードリーダーだけでなく、ライブラリ/カメラロール内に保存した画像からもQRコードを読み取れます。



アプリロック

Android

他の人がアプリを使用できないようにパスワードでロックします。誤ったパスワードを入力した人の写真を撮影し、アプリ起動時に表示します。

その他便利機能



通話時間タイマー

Android

iOS

スマホの無料通話時間をオーバーしないよう、設定した時間を超えるとパイプ通知でお知らせします。通話料の節約や使いすぎ防止に役立ちます。



ブルーライトカット

Android

iOS

6種類のフィルターから好きなものを選ぶことができ、目への負担を軽減します。強度の調整も自由に設定できます。

※iOS端末向けアプリはアプリ利用時のみ設定が反映されます。



パケットチェッカー

Android

iOS

端末の通信量(モバイル通信/Wi-Fi)を確認できます。パケット使用上限の設定も可能です。

インストール・認証方法

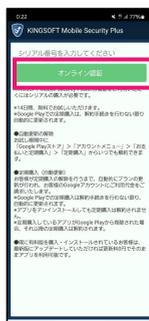
Android



① 「インストール」をタップ



② 各種権限について「許可」をタップ



③ シリアル番号を入力し、「認証」をタップ



④ 認証後、各種権限を許可するとTOP画面に遷移します。

iOS



① 「入手」をタップ



② 「許可」をタップした後、右上のメニューボタンをタップ



③ シリアル番号を入力し、「認証」をタップ



④ TOP画面に遷移します。

盗難対策

機能説明



位置検索

Android

iOS

マイページへログインすることで、紛失した端末の位置情報を調べることができます。

※電源がON状態の最終地点の位置にて検索します。

※iOS版はOSの仕様により、アプリのタスクを切ってしまうと位置確認ができなくなります。



Androidのみ対応機能



アラーム

Android

紛失した端末からアラーム音を鳴らすことができます。端末で事前に設定したパスワードを入力いただくか、盗難対策マイページで解除するまで鳴り続けます。



端末ロック

Android

端末にロックをかけます。マイページからロックをかけた場合に加え、SIMカードが抜き取られた場合でもロックをかけます。端末を拾った方へのメッセージを設定できます。



削除

Android

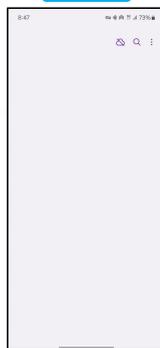
遠隔で電話帳と本体に保存された写真を削除します。大切な情報を勝手に見られることを防ぐことができます。



連絡先



画像



盗難対策

Android

初期設定手順

端末機種やOSバージョンにより、操作画面や操作手順が異なる場合がございます。

ご注意

本機能のご利用には「メールアドレス」「パスワード」の登録が必要です。
 「位置検索」をご利用の際は位置情報を「常に許可」に設定ください。
 設定がOFFになっていると正常な動作をしない場合があります。
 新規登録後はマイページ（WEB）へアクセスし位置情報を確認します。



①「盗難対策」をタップ



②「OK」をタップ



③「常に許可」を選択



④「メールアドレス」を入力し「認証メールを送る」をタップ



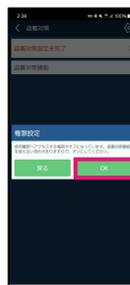
⑤メールアドレスへ届いた認証コードを確認



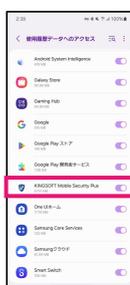
⑥認証コードを入力し「次へ」をタップ



⑦パスワードを設定し、「登録」をタップ



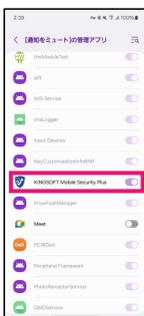
⑧「OK」をタップ



⑨「KINGSOFT Mobile Security Plus」をON



⑩「OK」をタップ



⑪「KINGSOFT Mobile Security Plus」をON



⑫「盗難対策設定未完了」をタップ



⑬解除パスワードを入力



⑭「盗難対策設定済」をタップ



⑮URLからログインを試してください。

盗難対策

iOS

初期設定手順

端末機種やOSバージョンにより、操作画面や操作手順が異なる場合がございます。

ご注意

本機能のご利用には「メールアドレス」「パスワード」の登録が必要です。「位置検索」をご利用の際は位置情報を「常に許可」に設定ください。設定がOFFになっていると正常な動作をしない場合があります。(手順⑧～)新規登録後はマイページ (WEB) へアクセスし位置情報を確認します。



①「盗難対策」をタップ



②メールアドレスを入力し「認証メールを送る」をタップ



③メールアドレスへ届いた認証コードを確認



④認証コードを入力し、「次へ」をタップ



⑤パスワードを設定し、OKをタップ



⑥「Appの使用中は許可」をタップ



⑦登録完了



⑧設定アプリにて「プライバシーとセキュリティ」をタップ



⑨「位置情報サービス」をタップ



⑩「モバイルセキュリティ」をタップ



⑪「常に」を選択

※iOS版はOSの仕様により、アプリのタスクを切ってしまうと位置確認ができなくなります。
 ※iOS12.Xの場合、OS側の問題により位置確認が正しく動作しない場合があります。その場合は最新OSへアップデートください。

シリアル番号解除方法

Android

iOS

アプリ内でシリアル番号を解除することができます。
機種変更等で新しい端末にアプリを認証することができるようになります。



① 右上の設定ボタンをタップ



② 「機種変更・シリアル番号解除」をタップ



③ 「リセット」をする前に
メール(④-a)又はスクリーン
ショット(④-b)にてシリアル番
号を保存する

④-b



④-aシリアル番号を
メールで送る
メールアプリが起動後
送りたい宛先を入力
して送信



④-bスクリーンショットを保存
保存したスクリーンショットは
画像フォルダで確認でき
ます。



⑤ 「リセット」をタップ



⑥ 確認画面で「OK」
をタップ



⑦リセット完了のメッセージが
表示されたら「OK」を
タップして完了

アドクリーナーとの機能連携

Android

iOS

広告ブロックアプリ「アドクリーナー」との機能連携ができます。
KINGSOFT Mobile Security PlusのフィッシングブロックがONの状態であれば、
フィッシングサイトのブロックと同時に広告ブロックも機能します。

①アドクリーナーを起動するポップアップが表示されます。

②アドクリーナーへ数秒間だけ遷移します。

③画面が戻り、ポップアップが出て連携完了です。



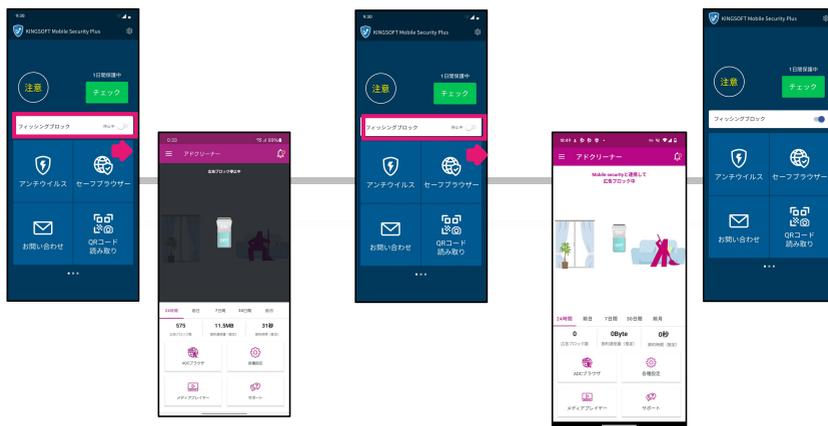
アドクリーナーとの機能連携注意事項

アドクリーナーがONの状態でもKINGSOFT Mobile Security PlusをONにする場合、
フィッシングブロックのボタンを2回ONにする必要があります。(Androidのみ)

①フィッシングブロックのボタンをON
>アドクリーナーへ遷移

②再度ON

③アドクリーナーとの連携完了



サポート窓口

KINGSOFT Mobile Security Plusの使い方のお問い合わせはこちら



お問い合わせ

kms@kingsoft.jp

よくある質問

<https://www.kingsoft.jp/is/mobile/faq>チャットサポート
24時間365日対応<https://support.kingsoft.jp/>キングソフト株式会社 〒108-0014 東京都港区芝五丁目29番11号 G-BASE田町5F <https://www.kingsoft.jp/>

動作環境

Android 5.0以上 / iOS 13.0以降 ※2

※2. OSのバージョンアップやアプリのバージョンアップにより、仕様が変更となる場合がございます。
最新の動作環境は各アプリストアページをご確認ください。

お客様のアカウント情報

シリアル番号

～盗難対策ページアカウント情報～

メールアドレス

パスワード

アプリロックパスワード (Androidのみ)