モバイルセキュリティ　セキュリティ対策アプリ

Mobile Security

初期設定マニュアル

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

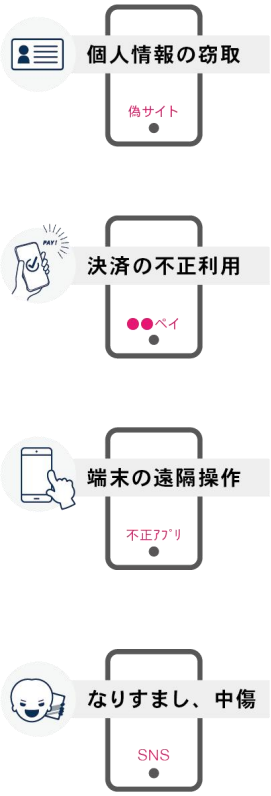
※操作画面、操作手順は「端末機種」や「OSバージョン」により異なる場合があります。
※内容の全部または一部は予告なく変更される場合があります。
※本資料記載の各企業名、企業ロゴ、サービス名は各社の商標、または登録商標です。

2026年1月版

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	フィッシングによる個人情報等の搾取
2	ネット上の誹謗・中傷・デマ
3	メールやSMS等を使った脅迫・詐欺の手口による金銭要求
4	クレジットカード情報の不正利用
5	スマホ決済の不正利用
6	不正アプリによるスマートフォン利用者への被害
7	偽警告によるインターネット詐欺
8	インターネット上のサービスからの個人情報の窃取
9	インターネット上のサービスへの不正ログイン
10	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　2023「個人」および「組織」向けの脅威の順位』

情報セキュリティ対策の基本

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 ウイルス対策ソフト（ウイルス対策サービス）の導入

※2. 出典：総務省
国民のための際一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

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拡がります。

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を抜き取ろうとしてきます。

アカウント乗っ取り

Twitter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。

Mobile Security 機能概要

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。

セーフブラウザー

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。

盗難対策機能

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コード機能

Android™ iOS®

QRコードを読み取る事で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コードだけでなく、ライブラリ/カメラロール内の画像からも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することもできます。

プライバシー管理

Android™

どのアプリが、どの権限を使用しているか確認することができます。アプリ名から、アプリのアンインストールなどの操作ができます。

その他便利機能

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。パケットの使用上限設定も可能です。

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。

クリーナー

Android™

アプリ内の不要なファイルや大容量のファイルをクリアできます。不要ファイルを消すことで、操作感向上に繋がります。

Mobile Security 機能紹介

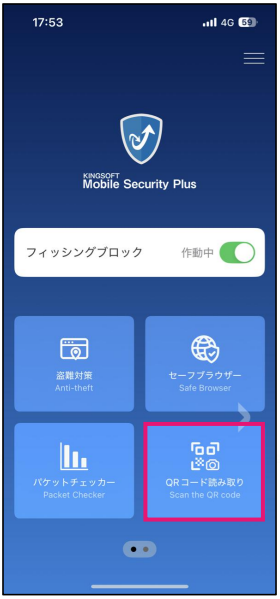
端末を保護するセキュリティ機能

QRコード読み取り機能

QRコードフィッシングブロック機能

Android™ iOS®

QRコードを読み込むことで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。

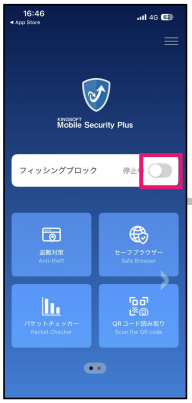


フィッシング ブロック 初期設定手順

iOS® Android™

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。

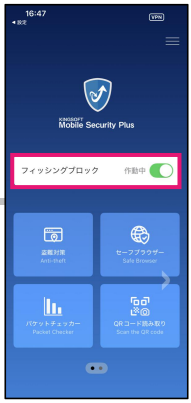
iOS®



①「停止中」をタップ

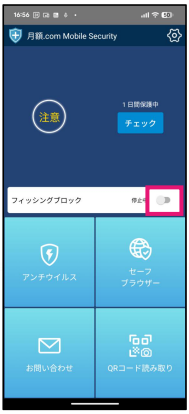
②「OK」をタップ

③「許可」をタップ

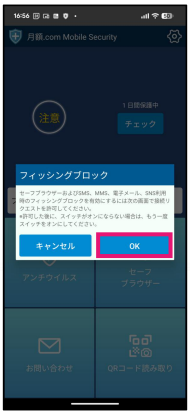


④設定完了

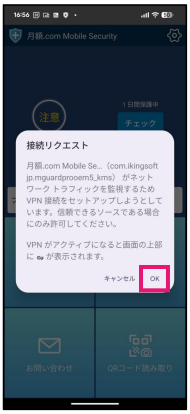
Android™



①「停止中」をタップ



②「OK」をタップ



③「OK」をタップ

④設定完了

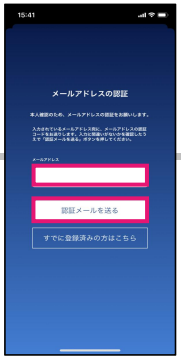
盗難対策 初期設定手順

iOS®

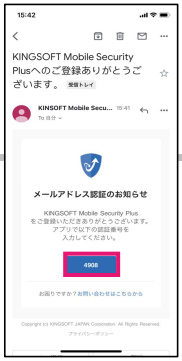
端末機種やOSバージョンにより、操作画面や操作手順が異なる場合がございます。

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。
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（4桁）」を確認

④「認証ｺｰﾄﾞ」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
※設定変更推奨

⑦登録完了

※設定変更画面

※「位置検索」をご利用の際は端末の「設定＞プライバシー＞位置情報サービス＞KINGSOFT Mobile Security Plus」より「常に許可」を選択して下さい。
「常に許可」以外を選択すると正常な動作をしない場合があります。

※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。
※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。

盗難対策 初期設定手順 Android™

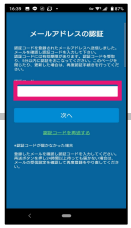
端末機種やOSバージョンにより、操作画面や操作手順が異なる場合がございます。

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。
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（4桁）」を確認



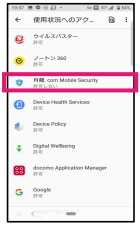
④「認証コード」を入力し、「次へ」をタップ

⑤パスワードを設定し、「登録」をタップ

⑥「OK」をタップ

⑦「常に許可」をタップ

⑧「OK」をタップ



⑨「月額. com Mobile Security」をタップ

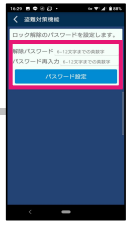
⑩「使用状況へのアクセス許可」をタップ

⑪「アプリの使用中のみ許可」をタップ

⑫「月額. com Mobile Security」をタップ

⑬「許可」をタップ

⑭「盗難対策機能オフ」をタップ



⑮解除パスワードを入力

⑯「盗難対策起動中」をタップ

⑰URLからログインしてお試しください。

※「位置検索」をご利用の際は下記の手順で端末の設定をして下さい。
「設定＞アプリと通知＞月額. com Mobile Security＞許可＞位置情報」より設定をONにしてください。
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。

※アプリから求められる権限は必ず許可してください。機能が正常に動作いたしません。

※ロック解除パスワードを忘れないようにご注意ください。

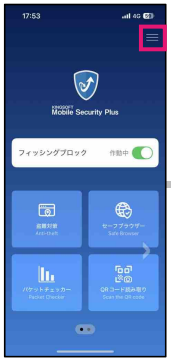
※「盗難対策」機能は、下記専用サイトからご利用いただけます。
●Android版 「盗難対策」専用サイトはこちら
https://anmagkms.kingsoft.jp/management/login

Android版

機種変更・シリアル解除方法

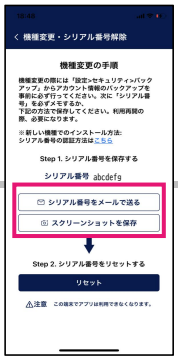
iOS® Android™

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。



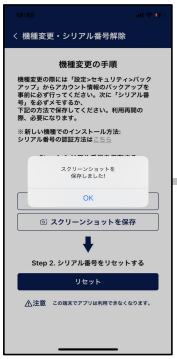
①右上の三本線をタップ

②「機種変更・シリアル番号解除」をタップ



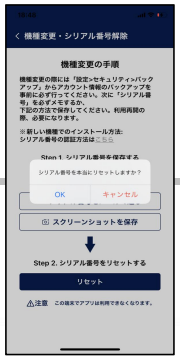
③「リセット」をする前に
④-①「シリアル番号をメールで送る」
又は
④-②「スクリーンショットを保存」

④-①シリアル番号をメールで送る
メールアプリが起動しますので
送りたい宛先を入力して送信

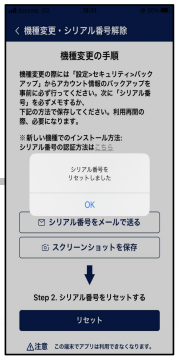


④-②スクリーンショットを保存
保存したスクリーンショットは
画像フォルダで確認できます

⑤「リセット」をタップ



⑥確認画面で「OK」を選択



⑦リセット完了のメッセージが出たら
「OK」を選択して完了

AD Cleanerとの機能連携

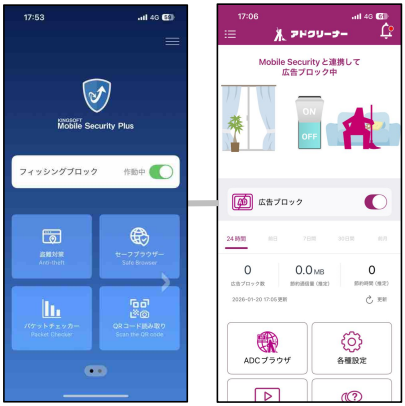
広告ブロックアプリ「AD Cleaner」との機能連携ができます。
Mobile Securityのフィッシングブロックが**ON**の状態であれば、フィッシングサイトのブロックと同時に広告ブロックも機能します。

①AD Cleanerを起動するポップアップがでます。

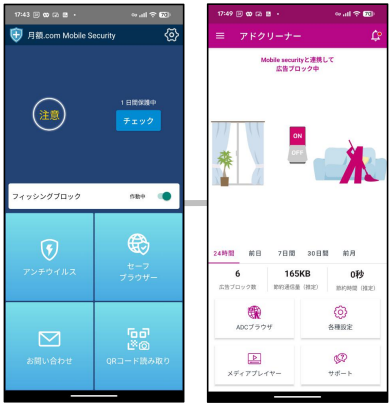
②AD Cleanerへ画面が数秒間だけ遷移します。

③画面が戻り、ポップアップが出て連携完了です。

iOS®



Android™



盗難対策

専用サイト（マイページ）※1へアクセスすることで、端末の位置確認や画面ロック、データの消去や警告音を鳴らしたりすることができます。

ご利用可能デバイスと動作環境

ご利用可能台数

※1.パソコン（Windows® / Mac）ではご利用できません。

モバイル端末（Android™ or iOS®）×1台 ※1

スマートフォン

or

タブレット

動作環境

Android™ 5.0以上 ／ iOS® 11.0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。

お客様のご利用製品情報

お客様がご契約されたセキュリティソフトは

☐ 月額.com Mobile Security （for Android）

☐ KINGSOFT Mobile Security Plus（for iOS）

※ご契約された製品へ☑チェックを入れて下さい。

お客様のアカウント情報

お名前

メールアドレス

シリアルコード

サポート窓口

Mobile Securityの使い方のお問い合わせはこちら

KINGSOFT　サポート

よくある質問　https://www.kingsoft.jp/is/mobile/faq

電話サポート　03-4226-8233

メールサポート　kms@kingsoft.jp

受付時間：平日10:00～13:00、14:00～17:00（土日祝日、年末年始を除く）

チャットサポート
24時間365日対応　https://support.kingsoft.jp/chat

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/

お申し込みサービス内容のお問い合わせはこちら

月額ドットコム　サポート

Q.「月額ドットコムへのログインできない」Q.「メールアドレス・または電話番号、パスワードがわからない」
Q.「決済、解約について問い合わせたい」　Q.「アプリの初回起動ができない」　・・・　など

電話サポート　050-8885-9425

メールサポート　send@ggd.jp

受付時間：平日10:00～13:00、14:00～18:00（土日祝日、年末年始を除く）

TELESTATION

株式会社テレステーション
〒100-6216
東京都千代田区丸の内1-11-1 パシフィックセンチュリープレイス丸の内16階