



ELECOM *apps*



**IKARUS mobile.security**

**取扱説明書**

# 目次

はじめに	3
■動作環境について	3
■画面について	3
アプリのインストール	4
■インストールの流れ	4
端末の設定	5
ダウンロードとインストール	6
初期設定をする	8
シリアル番号の入力	8
チュートリアルの実行	10
USSD プロテクト機能の設定	11
リモートコントロールの設定	12
Web フィルタリングの設定	16
初回スキャン	17
メイン画面について	18
情報エリア	18
アンチウイルス	19
セキュリティアドバイザー	20
アプリブロック	21
アプリブロックを設定するには	22
アプリブロックを設定したアプリを使用するには	22
セキュリティパスワードを設定するには	23
プライバシーコントロール	24
盗難防止	25
セキュリティパスワードおよび PIN コードを設定するには	26
URL フィルター	27
メニュー	28
情報	28
使用許諾	28
端末の問題を調査	29
お知らせ	29
監視	29
設定	30
チュートリアルウィザード	31
アンインストール	31
ウイルスや不正なアプリが見つかったら	32
不正サイトにアクセスしようとすると	34
お知らせ機能について	35
リモートコントロールで端末を保護する	36
ライセンスの更新について	37
■更新ライセンスの入手方法	37
■更新ライセンスの登録方法	37
本製品のアップデート	39
本製品のアンインストール	40
こんなときは	41
商品に関するお問い合わせは	41

# はじめに

このたびは、ELECOMApps「IKARUS mobile.security」をお買い上げいただきありがとうございます。

本マニュアルは、「IKARUS mobile.security」のダウンロード、インストール、設定方法について説明します。ご使用前に、必ずお読みください。

## ■動作環境について (2020/03 現在)

本製品は下記の環境で動作します。

- ・ 対応 OS: Google Android OS 5.0 ~ 10
- ・ 端末の空き容量 : 200MB 以上の空き容量
- ・ メモリ : 200MB 以上のメモリ

## ■画面について

本マニュアルでの画面の説明は、スマートフォン端末での表示で説明しています。

タブレット端末の場合は、表示が異なりますが、操作手順や操作内容は同じです。



スマートフォン  
端末の場合



タブレット端末の場合

# アプリのインストール

## ■インストールの流れ



各種ダウンロードのために、インターネット接続を行います。設定内容およびご契約内容によっては、パケット代が発生することがありますので、ご注意ください。

**1**

### 端末の設定

Android 端末に本製品をインストールできるように設定します。

**2**

### IKARUS mobile.security のインストール

IKARUS mobile.security をダウンロード / インストールします。

**3**

### シリアル番号の入力 / ライセンスの有効化

シリアル番号を入力して、本製品を使用できるようにします。

**4**

### 初期設定

チュートリアルウィザードにしたがって本製品を正しく使えるように設定していきます。



お使いの端末により、表示される内容が異なる場合があります。

## 7 端末の設定

Android 端末にアプリをインストールできるように設定します。  
Android8.0 以上の場合と Android8.0 未満の場合で設定方法が異なります。

### Android8.0 以上の場合

- 1 「設定」画面で[アプリと通知]をタップします。
- 2 「アプリと通知」画面の「詳細設定」の「特別なアプリアクセス」をタップし、[不明なアプリのインストール]をタップします。
- 3 リストから[Chrome]を選択して、表示された画面で「この提供元を許可する」をタップして、チェックします。



**メモ** 設定方法について、詳しくはお使いの Android 端末のメーカーの取扱説明書をお読みになるか、メーカーにお問い合わせください。



[不明なアプリのインストール]の設定は、通常お買い上げ時の設定では「許可しない」になっています。この状態では、「Play ストア」以外で提供されるアプリがインストールできなくなっています。

### Android8.0 未満の場合

- 1 「設定」画面で[セキュリティ]をタップします。
- 2 [提供元不明のアプリ]をタップして、チェックします。

**メモ** 設定方法について、詳しくはお使いの Android 端末のメーカーの取扱説明書をお読みになるか、メーカーにお問い合わせください。



[提供元不明のアプリ]の設定は、通常お買い上げ時の設定では「オフ」になっています。この状態では、「Play ストア」以外で提供されるアプリがインストールできなくなっています。



## 2 ダウンロードとインストール

アプリを弊社専用ページからダウンロードしてインストールします。

### 1 「IKARUS mobile.security」のダウンロードページにアクセスします。

ダウンロードページへのアクセスには、2つの方法があります。

#### ①以下の QR コードを撮影してアクセス



#### ② URL をブラウザに直接入力

[https://appstore.elecom.co.jp/user\\_data/ikarus\\_free.php](https://appstore.elecom.co.jp/user_data/ikarus_free.php)

### 2 「IKARUS mobile.security」のダウンロードを開始します。

「Android5 〜はこちら」をタップします。

タップ



### 3 [ダウンロードはこちら]をタップします。



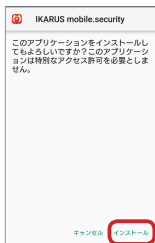
### 4 [開く]をタップします。



Android 8.0 以上の端末をお使いのときに、不明なアプリのインストールについてのメッセージ表示された場合は、[設定]をタップして、「1 端末の設定」-「Android 8.0 以上の場合」の手順③(5 ページ)を参照してインストールできるようにしてください。



### 5 [インストール]をタップします。



### 6 インストールが完了すると、「アプリをインストールしました。」と表示されます。

このあと続いて、IKARUS mobile.security の設定をおこないます。

[開く]をタップして、次の「初期設定をする」に進んでください。



[完了]をタップすると、インストール画面を閉じます。

Tips

# 初期設定をする

IKARUS mobile.security を使用するため、最初に機能の設定が必要になります。

IKARUS mobile.security では「チュートリアルウィザード」を用意しています。

「チュートリアルウィザード」では、画面の指示に従って進むだけで、機能の内容を把握しながら必要な設定ができます。

## 1 シリアル番号の入力

**メモ** シリアル番号は登録した端末1台でのみ利用可能です。

**1** トップ画面で[次へ]をタップします。



**2** [パーミッションを許可します。]をタップします。

以下のメッセージが順に表示されますので、すべて[許可]または[常に許可]をタップします。

- ・「SMS メッセージの送信と表示を「IKARUS mobile.security」に許可しますか？」
- ・「このデバイスの位置情報へのアクセスを「IKARUS mobile.security」に許可しますか？」
- ・「連絡先へのアクセスを「IKARUS mobile.security」に許可しますか？」
- ・「電話の発信と管理を「IKARUS mobile.security」に許可しますか？」
- ・「デバイス内の写真、メディア、ファイルへのアクセスを「IKARUS mobile.security」に許可しますか？」

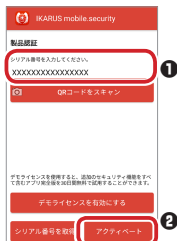




### 3 シリアル番号を入力します。

ELECOM AppsStore 等で購入したシリアル番号(16桁)を入力します。

- ①「シリアル番号」欄にシリアル番号を入力します。
- ②「アクティベート」をタップしてシリアル番号を登録します。



シリアル番号の QR コードをお持ちの場合は、「QR コードをスキャン」をタップして、QR コードを撮影して、シリアル番号を入力することもできます。



認証済の端末では本製品のシリアル番号は利用できません。  
更新用のシリアル番号をご利用ください。

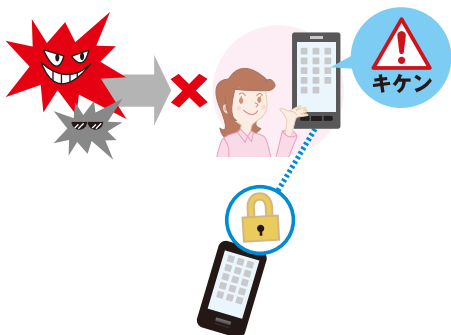
有効なライセンスが確認されると、チュートリアルウィザード画面に進みます。「2 チュートリアルの実行」に進んでください。

## 2 チュートリアルの実行

### 4 チュートリアルを実行するかどうかを確認する画面が表示されます。

このチュートリアルを利用すると、下記の順序で、本製品の基本機能を確認しながら、必要な設定が行えます。

- ・ USSD プロテクト
- ・ 遠隔操作 / 盗難防止
- ・ 遠隔操作のセキュリティパスワード
- ・ Web フィルタリング



### 5 [次へ]をタップします。

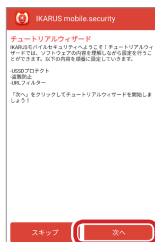
USSD プロテクト機能の設定画面に移ります。



[スキップ]をタップすると、チュートリアルを実行せず、初回スキャン実行画面が表示されます。(17 ページ)

メニューの「チュートリアルウィザード」で本ウィザードを再実行できます。(30 ページ)

必要な設定は、メイン画面からも行なうこともできます。(18 ページ)



### 3 USSD プロテクト機能の設定

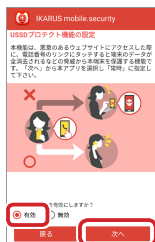
USSD プロテクト機能とは、ウェブサイトの tel: リンクにタップすると端末のデータが全消去されてしまうなどの脅威から Android 端末を保護する機能です。アクセス中のサイトに有害な USSD コードが含まれていないかを常に監視します。

※電話機能を持った端末でのみ利用できます。



**6** USSD プロテクト機能の概要を確認し、[有効]を選択してから[次へ]をタップします。

**メモ** [無効]を選択して、[次へ]をタップすると、リモートコントロールの設定画面(12ページ)に移ります。



**7** [IKARUS mobile.security]を選択した状態で、[常時]をタップします。

リモートコントロールの設定に移ります。



## 4 リモートコントロールの設定

リモートコントロール機能を利用すると、Android 端末を紛失した場合などに、他の端末から SMS(ショートメッセージ)でコマンドを送信して盗難や不正使用を防止することができます。

- ・ 端末のデータ消去
- ・ 端末のブロック
- ・ 場所の特定
- ・ アラーム
- ・ SIM ロック



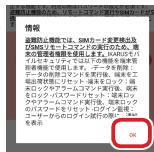
**8** リモートコントロール機能の概要を確認し、[有効]を選択してから[次へ]をタップします。



[無効]を選択して、[次へ]をタップすると、Web フィルタリングの設定画面(16 ページ)に移ります。



**9** 右の画面が表示されます。[OK]をタップします。



- 10** デバイス管理者を有効にする画面が表示されたら[この端末管理アプリを有効にする]をタップします。



- 11** 遠隔操作を設定するためのセキュリティパスワードを入力し、確認のための再入力をして、[続行]をタップします。

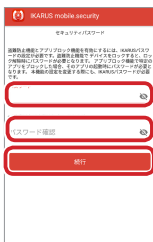


セキュリティパスワードは、6文字以上15文字以内で入力してください。アルファベットと数字が使用できます。アルファベットと数字は必ず1文字以上必要です。

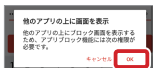


*Tips*

👁️にタップするとセキュリティパスワードがテキストで表示されます。



- 12** 「他のアプリの上に画面を表示」の画面が表示されたら[OK]をタップします。



- 13** 「他のアプリの上に重ねて表示できるようにする」をオンにします。前の画面に戻って、[続行]をタップします。



- 14** 「アクセス利用の許可」の画面が表示されたら[OK]をタップします。



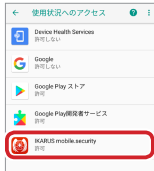
- 15** 一覧から「IKARUS mobile. security」を選択してタップします。



- 16** 「使用状況へのアクセスを許可」をオンにします。  
前の画面に戻り、「IKARUS mobile. security」が「許可」になっていることを確認します。



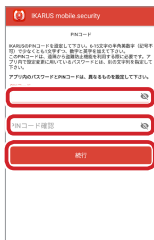
- 17** 前の画面に戻って、[続行]をタップします。



- 18** IKARUS の PIN コードを入力し、確認のための再入力をして、[続行]をタップします。



PIN コードは、6 文字以上 15 文字以内で入力してください。アルファベットと数字が使用できます。アルファベットと数字は必ず 1 文字以上必要です。セキュリティパスワードとは別の文字列を指定してください。



👁️にタップすると PIN コードがテキストで表示されます。

## 19 リモートコントロールの項目を確認します。

設定できるリモートコントロールは次の 4 種類です。

データ消去：wipe:[PIN コード] と電話番号にテキストを送信することで、デバイスを工場出荷状態にリセットし、すべてのデータを消去します。

端末のロック：lock:[PIN コード] と電話番号にテキストを送信することで、デバイスはただちにロックされます。

端末の探索：locate:[PIN コード] と電話番号にテキストを送信することで、デバイスの現在位置情報を GoogleMap の URL リンクから取得できます。

アラーム：alarm:[PIN コード] と電話番号にテキストを送信することで、デバイスはアラームを発信します。また、セキュリティパスワード入力以外でアラームを停止することはできません。



**メモ** リモートコントロールの操作の方法については、「リモートコントロールで端末を保護する」(35 ページ)をご覧ください。

## 20 [次へ]をタップします。

Web フィルタリングの設定画面に移ります。

## 5 Web フィルタリングの設定

Web フィルタリングとは、不正サイトへのアクセス時に警告メッセージを表示する機能です。個人情報の漏えいやウイルス感染を防止します。

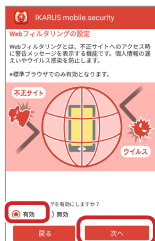
※標準ブラウザでのみ有効となります。



**21** Web フィルタリングの概要を確認し、**[有効]**を選択してから**[次へ]**をタップします。



- Android 6以降の環境では、WEB フィルタリング機能のために Android のアクセシビリティサービスを有効にする必要があります。画面の表示に従って ON にしてください。
- [無効]**を選択して、**[次へ]**をタップすると、初回スキャン画面(17 ページ)に移ります。





## 6 初回スキャン

- 22** 設定終了のメッセージを確認し、端末全体のスキャンを行う場合は、[はい]をタップします。



- 23** 「エンジンが利用できません。」と表示されますので、[アップデートします]をタップします。  
データベースの更新が開始されます。



- 24** メイン画面が表示され、スキャンが開始されます。  
これで、IKARUS mobile.security の設定は終わりました。

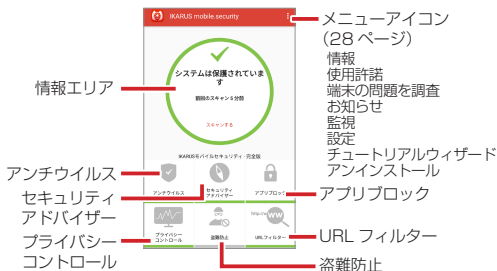


メイン画面から設定できる機能について詳しくは、「メイン画面について」(18 ページ)をご覧ください。

# メイン画面について

IKARUS mobile.security 起動すると、次のようにメイン画面が表示されます。

ここでは、メイン画面の機能について説明します。



## 情報エリア

IKARUS mobile.security の状態を表示します。



**システムは保護されています**  
正しく動作しています。



**システムは感染しています！**  
ウイルスや不正なアプリが発見されました。



**XXXXXX：無効**  
XXXXXX(機能によって異なります)が、セキュリティ設定が無効になっているなどの理由で注意が必要な状態になっています。

各機能の状態は機能の下のカラースタイルで確認できます。



正しく動作しています。

機能の一部に注意が必要な状態になっています。

機能が使用できない状態になっています。

## アンチウイルス

アンチウイルスについての操作、設定をおこないます。

### <ウィルススキャンタブ画面>

スキャンモードを選択してスキャンを実行します。

アプリスキャン：

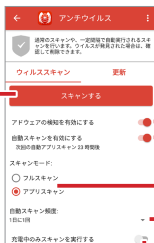
インストールされているアプリをスキャン

フルスキャン：

端末全体をデータを含めてスキャン

ファイルスキャン：

端末全体のファイルをスキャン



アドウェアの検知を有効にします。

自動スキャンを有効にします。

自動スキャンのモードを選択します。

フルスキャン：

端末全体をデータを含めてスキャン

アプリスキャン：

インストールされているアプリをスキャン

充電中のみスキャンを実行します。

自動スキャンの頻度を選択します。

1日に2回 / 1日に1回 / 2日に1回 / 週に1回

### <更新タブ画面>

ウイルス定義の更新を手動で行います。



無線 LAN 接続時のみウイルス定義の更新を行います。

ウイルス定義の自動更新を有効にします。

ウイルス定義の自動更新の頻度を選択します。

1日に2回 / 1日に1回 / 2日に1回 / 週に1回

## セキュリティアドバイザー


お使いのスマートフォンの設定を解析して、潜在的なセキュリティの脅威を検出します。

✔になっている項目は、セキュリティの脅威はありません。

⚠になっている項目は、セキュリティの危険性があります。タップして設定を変更することで、セキュリティの脅威はなくなります。

お使いの環境によっては設定を変更する必要がない場合があります。その場合は、セキュリティの危険性があることを理解したうえでご使用ください。

**メモ** 各項目の右にある **i** をタップすると、各項目についての詳しい説明が表示されます。



The screenshot shows the Security Advisor app interface. At the top, there's a title bar with a back arrow, a red icon, and the text 'セキュリティアドバイザー'. Below the title bar, there's a subtitle: 'セキュリティアドバイザー機能は、お使いのデバイスの設定を解析して、潜在的なセキュリティの脅威を検出する機能です。' Then, there's a section titled 'アンドロイドのセキュリティ設定を確認' with a warning icon. Below this, there's a list of items: '提供元不明のアプリ' (with a red arrow pointing to 'アプリを確認'), 'デバイスの暗号化' (with a green checkmark and 'デバイスが暗号化されています。'), 'USBデバッグ' (with a green checkmark and 'デバッグモードが無効です。'), 'スクリーンロック' (with a red warning icon and '画面ロックが設定されていません。'), 'デバイスのルート化' (with a green checkmark and 'このデバイスはルート化されていません。'), 'Wi-Fi接続' (with a green checkmark and '安全なWi-Fi接続: "biglink-spot", WPA2'), and '警告機能の有効化'. Red arrows point from each of these items to explanatory text on the right.

- Google Play ストア以外からのアプリのインストールの不許可 / 許可を確認できます。
- スマートフォンの暗号化の有効 / 無効を確認できます。
- USB デバッグの有効 / 無効を確認できます。
- スクリーンロックの有効 / 無効を確認できます。
- ルート化の有効 / 無効を確認できます。
- Wi-Fi 接続が安全な接続かどうかを確認できます。
- セキュリティアドバイザーの警告機能を有効にします。

## アプリブロック

選択したアプリにセキュリティパスワードを設定し、セキュリティパスワードを入力しないと利用できないようにします。



設定したセキュリティパスワードを忘れると、アプリを起動できなくなります。  
設定したセキュリティパスワードは絶対に忘れないようにしてください。

ユーザーがインストールしたアプリの一覧が表示されます。

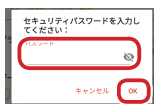


端末に最初からインストールされているアプリの一覧が表示されます。


アプリブロックの警告機能を有効にします。



設定を変更するたびにセキュリティパスワードの入力を求められます。  
セキュリティパスワードを入力して、[OK]にタップしてください。



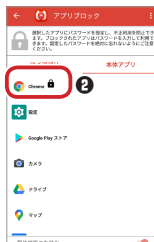
Tips

 にタップするとセキュリティパスワードがテキストで表示されます。

## アプリブロックを設定するには

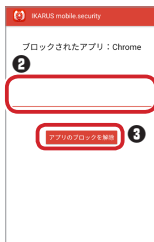


- ①「マイアプリ」タブまたは「本体アプリ」タブをタップして、アプリのリストを表示します。



- ②アプリブロックを設定したいアプリをタップします。  
アプリブロックを設定したアプリにはマークが表示されます。

## アプリブロックを設定したアプリを使用するには



- ①アプリのアイコンをタップします。  
②ブロック画面が表示されたら、セキュリティパスワードを入力します。  
③[アプリのブロックを解除]をタップします。  
④アプリが起動します。



一度ブロックを解除すると、本体をスリープ状態にするまで、セキュリティパスワードを入力する必要はありません。  
スリープ状態になったあと、アプリを使用する際には、再度セキュリティパスワードを入力するして、ブロックを解除する必要があります。



設定したセキュリティパスワードを忘れると、アプリを起動できなくなります。  
設定したセキュリティパスワードは絶対に忘れないようにしてください。

## セキュリティパスワードを設定するには

メニューの「設定」の「アプリブロック・盗難防止機能の初期化」(30 ページ)を実行してアプリブロックをリセットした場合は、セキュリティパスワードを設定しなおす必要があります。



①セキュリティパスワードを入力します。

②確認のため再度セキュリティパスワードを入力します。



セキュリティパスワードは、6 文字以上 15 文字以内で入力してください。アルファベットと数字が使用できます。アルファベットと数字は必ず 1 文字以上必要です。



*Tips*

👁️にタップするとセキュリティパスワードがテキストで表示されます。

⑤ [アプリブロックを有効にする] をタップします。

## プライバシーコントロール

各アプリのパーミッションに基づいて危険度を分析し、ランク付けを行います。

### <アプリタブ画面>



すべてのアプリをプライバシーコントロールの対象から除外します。

プライバシーコントロールの対象アプリを表示します。

プライバシーコントロールの警告機能を有効にします。

### <パーミSSIONタブ画面>



各項目のパーミSSIONをアプリごとに設定します。  
表示されたアプリをタップして、「パーミSSION」をタップすると、パーミSSIONの設定画面になります。

プライバシーコントロールの警告機能を有効にします。





## 盗難防止

リモートコントロールについて詳しくは、「4 リモートコントロールの設定」(12 ページ)をご覧ください。



各項目の右にある **i** をタップすると、各項目についての詳しい説明が表示されます。



この端末がリモートコマンドを受け取った際の状態を通知する SMS が、リモートコマンドを実行した端末に送付されます。

端末のデータをすべて消去します。

端末を操作できないようにします。

GPS がオンになっている場合に、端末の場所を表示します。

離れた場所にある端末からアラーム音を鳴らします。

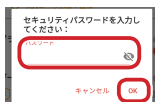
SIM カードが変更された場合に端末を操作できないようにします。

SIM カードを交換されたときに元の SIM カードの番号に SMS を送信します。


盗難防止の警告機能を有効にします。



設定を変更するたびにセキュリティパスワードの入力を求められます。  
セキュリティパスワードを入力して、[OK] にタップしてください。

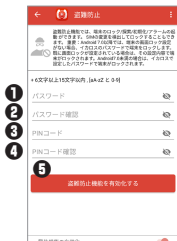


Tips

 にタップするとセキュリティパスワードがテキストで表示されます。

## セキュリティパスワードおよび PIN コードを設定するには

メニューの「設定」の「アプリブロック・盗難防止機能の初期化」(30 ページ)を実行して盗難防止機能をリセットした場合は、セキュリティパスワードと PIN コードを設定しなおす必要があります。



- ① セキュリティパスワードを入力します。
- ② 確認のため再度セキュリティパスワードを入力します。
- ③ PIN コードを入力します。
- ④ 確認のため再度 PIN コードを入力します。



メモ セキュリティパスワードおよび PIN コードは、6 文字以上 15 文字以内で入力してください。アルファベットと数字が使用できます。アルファベットと数字は必ず 1 文字以上必要です。セキュリティパスワードと PIN コードは別の文字列を指定してください。



👁️ にタップするとセキュリティパスワードまたは PIN コードがテキストで表示されます。

- ⑤ [盗難防止機能を有効化する] をタップします。
- ⑥ 「リモートコマンドの説明を添付して、パスワードと PIN コードを保存するために、メールアドレスに送付しますか？」の画面が表示された場合は、[リマインダーの送付] をタップすると、送信方法の選択ができますので、画面に従ってリマインダーを送信してください。リマインダーを送信する必要のない場合は、[キャンセル] をタップします。リモートコマンドについては、「リモートコントロールで端末を保護する」(35 ページ)を参照してください。

## URL フィルター

URL フィルターについて詳しくは、「5 Web フィルタリングの設定」(16 ページ)をご覧ください。



保護を有効にします。

URL フィルターの警告機能を有効にします。

## メニュー

右上のメニューアイコンをタップすると表示されます。



## 情報

IKARUS mobile.securityのライセンスの期限を表示します。  
ライセンスの更新については、「ライセンスの更新について」(36 ページ)をご覧ください。



本製品のバージョンを表示します。

ライセンスの期限を表示します。

ライセンスコードを表示します。

ヘルプ画面が表示されます。取扱説明書(PDF)をダウンロードすることもできます。

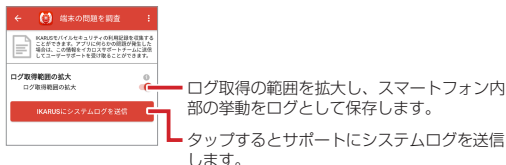
## 使用許諾

使用許諾契約書を表示します。

## 端末の問題を調査

端末の利用記録を収集し、アプリに問題が発生したときに情報をサポートに送信してユーザーサポートを受け取ることができます。

**メモ** 項目の右にある **i** をタップすると、各項目についての詳しい説明が表示されます。



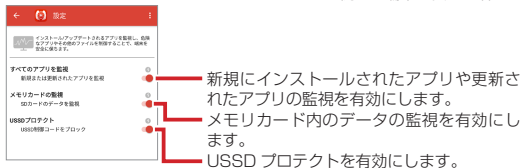
## お知らせ

エレコムからのお知らせを記載した WEB ページを開きます。

お知らせ機能(34 ページ)のポップアップや通知領域で[詳細を開く (WEB)]をタップする場合と同じ機能です。

## 監視

インストールやアップデートされるアプリを監視し、端末を安全に保ちます。



USSD プロテクトについて詳しくは、「3 USSD プロテクト機能の設定」(11 ページ)をご覧ください。

## 設定

匿名ウイルス統計にウイルスの発見数と頻度のデータを匿名で送信します。  
アプリブロック・盗難防止機能をリセットします。

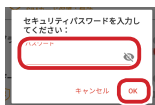
**メモ** 項目の右にある **i** をタップすると、各項目についての詳しい説明が表示されます。



品質保証プログラムに参加します。

アプリブロック・盗難防止機能をリセットします。  
リセットするとセキュリティパスワードとPINコードを設定しなおす必要があります。

**メモ** [機能をリセット] をタップすると、セキュリティパスワードの入力を求められます。  
セキュリティパスワードを入力して、[OK] にタップしてください。



**Tips** **i** にタップするとセキュリティパスワードがテキストで表示されます。

*Tips*

## チュートリアルウィザード

チュートリアルウィザードを使用し、再設定を行います。

## アンインストール

IKARUS mobile.security をアンインストールします。  
アンインストールについては、「本製品のアンインストール」(39 ページ)をご覧ください。

# ウイルスや不正なアプリが見つかったら

お使いの端末にウイルスや不正なアプリが、見つかったら次の画面が表示されます。



検出されたウイルスや不正なアプリは、次の手順で処理してください。

**1** [アンチウイルス]をタップします。



**2** [感染ファイルを表示]をタップします。



- 3** [すべての感染ファイルを消去]をタップすると、検出されたすべてのウイルスや不正アプリを削除できます。



- 4** [OK]をタップします。



- 5** アプリのアンインストール画面が表示された場合は、[OK]をタップします。



- 6** アンチウイルス画面に戻ります。





# 不正サイトにアクセスしようとすると

不正サイトへのアクセスしようとすると、次の警告画面が表示されます。



警告画面が表示された場合は、次の手順で処理してください。

## ■[ウェブサイトブロック]をタップします。

Web サイトへのアクセスを遮断して、ブラウザにサイトを表示しません。



## ■[ウェブサイト解放]をタップします。

Web サイトへのアクセスを遮断せず、ブラウザにサイトを表示します。



不正なサイトとして警告されたサイトにアクセスする場合は、十分に注意してください。



# お知らせ機能について

初回起動時及びお知らせ内容の更新があるたびに、本アプリを起動すると、ポップアップおよび通知領域にお知らせを通知します。  
メッセージ中の[詳細を開く(WEB)]をタップすると弊社 WEB ページを開きます。

## <ポップアップ>



## <通知領域>



# リモートコントロールで端末を保護する

Android 端末を紛失した場合に、次の手順で他の端末から SMS(ショートメッセージ)でコマンドを送信して盗難や不正使用を防止します。

- 1** 他の端末で、SMS を送信するアプリを起動します。
- 2** 宛先にご使用の端末の電話番号を入力します。
- 3** メッセージ本文に下記のフォーマットで入力します。

(コマンド) : (PIN コード)

	設定した PIN コード を入力します。
遠隔操作の動作に合わせたコマンドを 入力します。	
データ消去	wipe
端末のロック	lock
端末の探索	locate
アラーム	alarm

- 4** SMS を送信します。



リモートコマンドを送信して盗難保護機能を動作させるには、あらかじめ「盗難防止」の機能を有効にしておく必要があります。また、「端末の探索」を使用するには、端末の GPS 機能が ON になっている必要があります。  
メイン画面の「盗難防止」(25 ページ)をお読みください。

例 「データ消去」コマンドで、PIN コードが「password」の場合

wipe : password

# ライセンスの更新について

お買い上げの際のライセンスは、1 年間です。続けて本製品を使用する場合は、更新ライセンスを購入していただくことになります。



携帯ショップや弊社 EC サイトで「月額継続版」を購入された場合は、自動的にライセンスが更新されますので、本手順は必要ありません。

## ■更新ライセンスの入手方法

更新ライセンスは、下記の弊社購入サイトで購入できます。

[http://appstore.elecom.co.jp/ikarus/update\\_license.html](http://appstore.elecom.co.jp/ikarus/update_license.html)



## ■更新ライセンスの登録方法

- 1 ライセンスの有効期限が近づくと、「ライセンスの有効期限が近づきました」というメッセージが表示されます。



- 2 メイン画面で「アップグレード」をタップします。



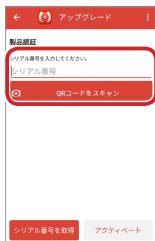
- 3 [シリアル番号の入力 / 読み取り]をタップします。

シリアル番号を入力する画面が表示されます。



## 4 シリアル番号を入力します。

シリアル番号欄に新しく購入したライセンスのシリアル番号を入力するか、[QRコードをスキャン]をタップして、弊社購入サイトで表示される QR コードを読み取ります。



## 5 [アクティベート]をタップします。



## 6 シリアル番号の登録が正しく終了すると、「情報」画面が表示されます。

ライセンス期限が更新されていることを確認してください。



**メモ** ライセンス切れの場合は、「有効なライセンスがありません!」と表示されます。その場合は、画面の[アップグレード]をタップして、3～6の操作を行ってください。



# 本製品のアップデート

本製品のプログラムに更新がある場合は、次の手順で最新プログラムを入手します。

- 1 ステータスバーに↓↓マークが表示されたら、ステータスバーを下方方向になぞって、通知パネルを開き、[最新バージョン]と表示されたパネルをタップします。



- 2 「新しいバージョンのアプリが利用可能です」というメッセージが表示されます。  
[アップデートします]をタップします。



- 3 弊社 web サイトにアクセスし、最新版のプログラムをダウンロードします。

[https://appstore.elecom.co.jp/user\\_data/ikarus\\_free.php](https://appstore.elecom.co.jp/user_data/ikarus_free.php)



# 本製品のアンインストール

本製品をアンインストールときは、次の手順で行います。

- 1 メニューアイコンをタップし、「アンインストール」をタップします。



- 2 [OK]をタップします。



- 3 セキュリティパスワードを入力して、[OK]をタップします。



🔒にタップするとセキュリティパスワードがテキストで表示されます。

*Tips*



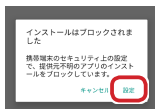
- 4 [OK]をタップします。  
本製品のアンインストールが終了します。



## こんなときは

**Q** 「インストールはブロックされました」という画面が表示される

**A** 提供元不明のアプリケーションのインストールを許可にする必要があります。[設定]をタップして、提供元不明のアプリがインストールできるように設定してください。設定については詳しくは「端末の設定」(5 ページ)をご覧ください。



**Q** ダウンロードできない

**A** 回線が不安定な場合は、エラーが起きやすくなりますので、安定した回線状態でダウンロードしてください。

**Q** 機種変更したい

**A** 新しい機種に元の端末で利用したシリアル番号を入力してください。新しい端末へライセンスが移行されます。

その他、よくある質問に関しては、弊社 Web サイトをご覧ください。

FAQ URL :

[http://appstore.elecom.co.jp/user\\_data/faq.php](http://appstore.elecom.co.jp/user_data/faq.php)



## 商品に関するお問い合わせは

**【よくあるご質問とその回答】**

こちらからソフトウェアの FAQ をご覧ください。

[https://appstore.elecom.co.jp/user\\_data/faq.php](https://appstore.elecom.co.jp/user_data/faq.php)

ご質問がある場合には下記 URL よりお問い合わせください。

<https://appstore.elecom.co.jp/contact/>

**【お電話・FAX によるお問い合わせ(ナビダイヤル)】**

**エレコム総合インフォメーションセンター**

TEL : 0570-084-465

FAX : 0570-050-012

**【受付時間】**

10:00 ~ 19:00

年中無休



## IKARUS SECURITY ソフトウェア使用許諾及びサービス契約書

本契約書を注意してお読みください。提供されたソフトウェアをインストールすることにより、以下の許諾条件に合意されたものとします。条件に合意されない場合、インストール処理をキャンセルし、配布されたソフトウェアをそれ以上使用しないでください。許諾条件に違反することは著作権侵害と見做され、民事及び刑事訴追となる場合があります。

### 1. 使用許諾

1.1. 使用許諾者は、IKARUS Security Software GmbH です。本使用許諾契約書は、CD、DVD、又はその他の磁器やデジタルメディアに含まれるプログラム、また被許諾者に提供されるプログラム記述、操作マニュアル及び書類に対する譲渡不能及び非独占の使用権の条件について示します。明確にするため、以下パッケージ全体を「ソフトウェア」と言及するものとします。

1.2. 本契約書の条件は、今後のソフトウェアアップデートにも適用されます。本使用許諾契約の締結により、提供されたソフトウェアの定期アップデートを含め、サービス契約にも合意したものとします。

### 2. 使用許諾の範囲

2.1. 本ソフトウェアは、1カ所まで1つのコンピューターシステム(1つの中央CPU)、又は1台のモバイル機器で、本契約条件の下においてのみ使用することができます。ネットワークを介してや、複数のPC上でソフトウェアを使用することは、追加のマルチクライアント、又はソフトウェアを使用するPCの台数分のネットワークライセンスを購入しない限り許可されていません。これらのライセンスを所有しない場合、この点においての契約をIKARUS Security Softwareと締結し、必要数の追加ライセンスを購入するものとします。本ソフトウェアを他のコンピューターに添付転送することは許可されません。特に、1クライアント又はマルチクライアントのソフトウェアライセンスをいかなる種類であれ第三者団体に提供することや、無料の場合も、直接又は間接で支払いを受ける場合も、いずれも使用を可能にすることは許可されません。サーバー上でいかなるソフトウェアも、ウイルスや同様のプログラムを検査するために、第三者団体のデータ通信をスキャンする目的で使用することは、それが被許諾者の契約上の共同経営者(例: アクセスするお客様、メールボックスのクライアント)であっても許可されません。この目的でソフトウェアを使用するには、書面での使用許諾者の同意が必要です。

2.2. 本ソフトウェアのCD、DVD、又はその他の磁器やデジタルメディア、その他コピーは、個人使用目的でも、弊社の書面による合意がなければ譲渡することはできません。法的に認められている強制介入以外で、本ソフトウェアを逆コンパイル、リバースエンジニアリング、逆アセンブル又はその他の人が認知できる形式に分解することはできません。さらに、本契約書で許可されるか法律で定められない限り、いかなる手法の使用でも、無料又は有料のいずれの場合も、合意の有無に関わらず、ソフトウェアを修正、改造、解析、販売、又は第三者団体に譲渡することはできません。

### 3. 保証

3.1. IKARUS Security Softwareは、ソフトウェアが本書で定義する最新の状態で出荷時に正常に作動することを、想定される全アプリケーションの要件を順守しているかによらず保証します。お客様は、現在の最新技術ではエラーのないソフトウェアを開発できないことを理解し合意します。これは特に、アンチウイルスプログラムからの検知を防ぐように作成された新しいウイルス、トロイの木馬、ワームや同様のプログラムに対するアンチウイルスの保護分野に適用されます。

3.2. 従って、IKARUS Security Softwareはソフトウェアがお客様の全要件を満たし、ソフトウェアの機能が破壊されることなく、データ、プログラム及びITシステムの全ての組み合わせでエラーなしに使用でき、また、ソフトウェアのデバッグが他のソフトウェアエラーによって発生しないことを保証しません。さらに、不適切な操作、送信中の損傷、運用システムのエラー、運用システムコンポーネント、インターフェース及びパラメーターの修正、不適切な組織のツールやデータメディアの使用によるエラー、破壊又は損傷に対して保証しません。

3.3. お客様又は第三者団体が、書面による合意なくソフトウェアの修正又は修理を行った場合、保証は終了します。また、IKARUS Security Softwareはそれに関連する費用を認めることはありません。修正、アップグレードや損傷、又は契約で規定した使用条件以外の方法で使ったソフトウェアに対して、修正、アップグレード又は損傷が、損害に関与していない場合を除き、保証しません。

3.4. ソフトウェアの不良に対する通知は、検知されてから8日以内(小売店のお客様の場合、法定通知期間内)に書面で提出する必要があります。これ以外の場合、保証は失効するものとします。双方の合意により、保証期間は小売店のお客様の場合は2年間、その他のお客様は6カ月間です。

#### 4. 損害賠償請求：

4.1. IKARUS Security Software に対して主張する全ての損害賠償請求は、悪質又は重大な過失で責任が法的に定められた場合を除き、除外されます。特に現在の最新技術で、誰にでも使用できるウイルス保護を提供できないウイルス又は同様のプログラムによって生ずる損害は、責任から除外されます。利益損失を含む結果的損害及び間接的損害に対する責任も除外されます。無許可の第三者団体の修正に起因する損害、また不適切な操作やインストールに対する責任も除外されます。

4.2. IKARUS Security Software は、お客様がご使用のコンピューターでファイルのバックアップを定期的に作成されることを明確にお勧めします。お客様が損失を回避、最小化又は軽減する義務を怠った場合、義務不履行によるいかなる損害にも責任を負うものではありません。重大な過失又は悪質な要因による損害が発生した場合、この損害制限は適用されません。バックアップのコピーを作成しない場合、補償を決定する際に寄与過失として考慮されます。

#### 5. 使用許諾契約書の開始日及び期間：

5.1. 本契約書は両当事者の合意を得た上で効力が生じます。ただし、ご使用の PC に本ソフトウェアを実際にインストールするより前の日付とします。明確な双方の合意は、郵便、E メール又は個人的に書類を受け取る、或いはお客様が受け渡すことによって書面で行われます。

5.2. 本契約書は契約上の両当事者が、特約で最初に合意した最少の条件で遂行されます（送り状を参照）。満了時は、本契約の条件によって延長されます。本契約期間中、IKARUS Security Software は継続して配信したソフトウェアの最新アップデートを、お客様に提供するものとします。具体的には、本ソフトウェアがご使用のコンピューターで、既知のウイルスや同様の脅威を検知できることを保証します。必要なプログラムアップデートは、お客様が事前に指定したアドレスに送信されます。また、オンラインアップデートのために、IKARUS Security Software のウイルスデータベースにアクセスすることもできます。お客様に提供する本製品のパスワードは、納品時に含まれています。

5.3. 手数料は使用許諾及びサービス契約の一部として定期的に実施される更新に合意します。IKARUS Security Software は価格を変更する権利を保有します。値上げが発表される場合、お客様は契約の通知期間に従って、契約を終了する権利を有します。

5.4. 本契約書はお客様が選択された使用許諾期間実施されるものとし、契約年終了前 2 カ月の通知期間に基づいて終了しない限り、満了時にその使用許諾期間で延長されます。小売店のお客様は、最初の契約年は終了時に、その後の契約年では 6 カ月ごとに通知期間に基づいて、本契約書を終了する権利を有します。契約満了後に本ソフトウェアを継続して使用することは許可されません。お客様は元の CD 及びそのコピー、付属文書を処分する義務があります。契約終了日後に本ソフトウェアを継続して使用することは、著作権侵害を意味します。

5.5. お客様が本契約書の条件、特にここでお客様に付与された権利の範囲に関して違反する場合、IKARUS Security Software は本契約書を即効で遅延することなく終了する権利を与えられます。この場合、いかなる種類であれソフトウェアの継続使用は許可されません。

#### 6. 最終規定：

6.1. 国連国際物品売買条約ではなく、オーストリアの法律が本契約書に適用されます。本契約書やその満了によって起こるあらゆる紛争を扱う裁判地は、ウィーンに所在する管轄商事裁判所となります。小売店のお客様はこの対象ではなく、管轄区域の公判廷となります。本契約書に対する修正や補足は、契約の両当事者が書面に正式な署名をされた場合にのみ有効となります。権利放棄の証書の場合も、これが適用されます。

本使用許諾契約書の条件に合意されない場合、いかなる契約も IKARUS Security Software との間に締結されず、お客様は本ソフトウェアをインストールも操作を行うことはできません。本ソフトウェアをインストール及び／又は操作することにより、お客様は使用許諾の条件に同意します。本契約を終了されたい場合は、IKARUS Security Software までご連絡ください。

IKARUS mobile.security  
取扱説明書  
2020 年 4 月 1 日 第 3 版  
エレコム株式会社

- 本書の著作権は、エレコム株式会社が保有しています。
- 本書の内容の一部または全部を無断で複製 / 転載することを禁止させていただきます。
- 本書の内容に関するご意見、ご質問がございましたら、エレコム総合インフォメーションセンターまでご連絡ください。
- 本製品を使用したことによる他の機器の故障や不具合等につきましては、責任を負いかねますのでご了承ください。
- 改良などのため、商品の仕様は予告なく変更することがあります。あらかじめご了承ください。
- イラストはイメージです。実際の商品とは異なる場合がありますので、あらかじめご了承ください。
- IKARUS mobile.security は、IKARUS Security Software Gmbh の登録商標です。
- 本マニュアルの一部は、Google が作成および提供している作品から複製または変更したものであり、Creative Commons 3.0 Attribution ライセンス (<https://creativecommons.org/licenses/by/3.0/deed.ja>) に記載された条件に従って使用しています。
- 本製品のパッケージ等に記載されている会社名・製品名等は一般に各社の商標または登録商標です。