

6. セキュリティアプリ（Android版）

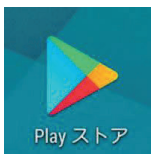
Android端末およびお使いのSDカードを安全に使うためのセキュリティアプリです。
Android端末を紛失・盗難の際にも遠隔で端末のロックを行ったり、端末の位置情報を
知ることができます。

※Wi-Fiご利用時も本設定の際は、予めモバイルデータ通信もONとなっていることを
確認してください。

アプリのインストール方法

◆Android9シリーズまでのスマートフォンをお使いの場合

『Playストア』を起動し、
『スマートフォンセキュリティ
特別版』を検索します。



または

下記のQRコードを
読み込みます。



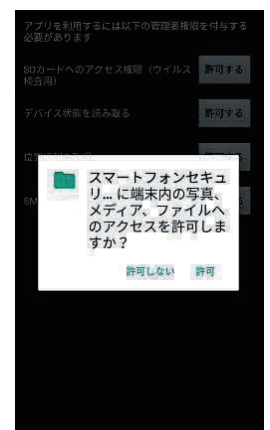
『スマートフォンセキュリティ
特別版』が表示されたら
『インストール』をタップ
します。



インストールが完了した後
「開く」をタップします。



上記の画面が表示された
場合は、管理者権限を付
与する必要があります。
それぞれの権限の横にある
「許可する」をタップしてく
ださい。

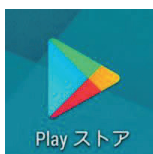


それぞれの「許可する」
のボタンを押すと画面が
出てくるので、「許可」
をタップします。

◆Android10以降のバージョンのスマートフォンをお使いの場合 【初めてイッツコムスマホをご利用の場合】

①アプリのインストール

『Playストア』を起動し、
『スマートフォンセキュリティ
特別版』を検索します。



または

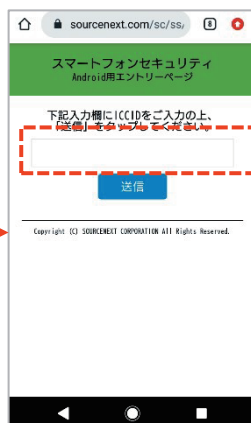
下記のQRコード
を読み込みます。



『スマートフォンセキュリティ
特別版』が表示されたら
『インストール』をタップします。

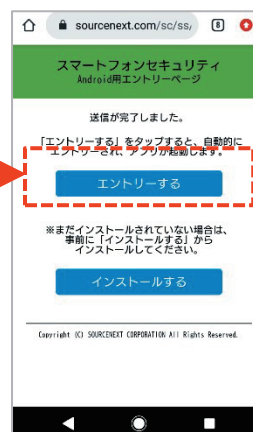
②SIMエントリーの方法

<https://rd.snxt.jp/88214>



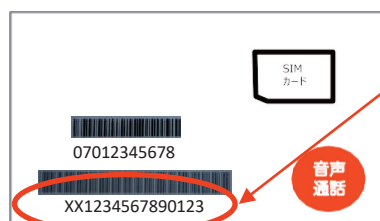
Webブラウザで、上記
URLを入力するか、
QRコードを読み込みます。

上記画面が表示されるので
ICCIDを入力し、「送信」を
タップします。



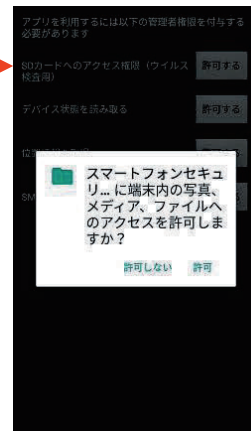
「エントリーする」をタップして、
エントリーします。

★ICCIDが記載されている場所



SIMカードのバーコード情報の下に
書いてある英数字になります。

③アプリの立ち上げ



「スマートフォンセキュリティ特別版」のアプリをタップします。

上記の画面が表示された場合は、管理者権限を付与する必要があります。それぞれの権限の横にある「許可する」をタップしてください。

それぞれの「許可する」のボタンを押すと画面が出てくるので、「許可」をタップします。

※ シリアルコードの入力を求められた場合は、アプリを一度閉じ、前ページの「②SIMのエントリー方法」を再度行ってください。

◆Android10以降のバージョンのスマートフォンをお使いの場合 【機種変更の場合】

・旧スマートフォンで対応すること
・新スマートフォンで対応すること
があります。
ご利用ガイドに従い、作業をしてください。

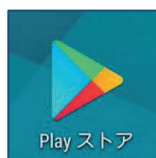
①旧スマートフォンでシリアルナンバーを取得する

- 1) 移行前の端末で、アプリを最新のバージョンにアップデートします。
- 2) アプリを起動し、「設定」をタップします。
- 3) 表示されたシリアルナンバーを控えます。



②新スマートフォンでセキュリティアプリを設定する

新スマートフォンの『Playストア』を起動し、『スマートフォンセキュリティ 特別版』を検索します。



または

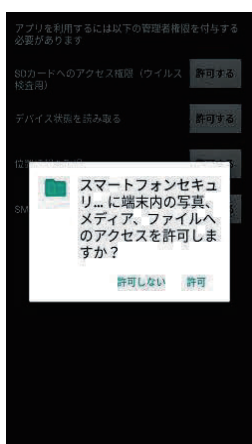
下記のQRコードを読み込みます。



『スマートフォンセキュリティ 特別版』が表示されたら『インストール』をタップします。

インストールが完了した後「開く」をタップします。

上記の画面が表示された場合は、管理者権限を付与する必要があります。それぞれの権限の横にある「許可する」をタップしてください。



それぞれの「許可する」のボタンを押すと画面が出てくるので、「許可」をタップします。

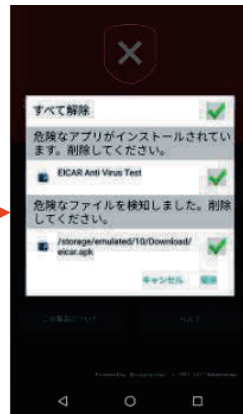


全ての許可が完了するとシリアルナンバーの入力画面が表示されますので、メモしたシリアルナンバーを入力します。

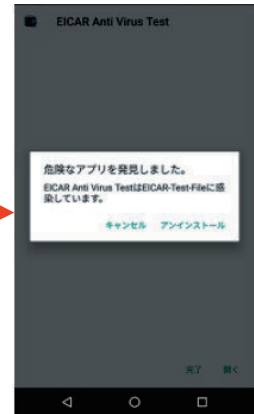
アプリの使い方（ウイルス検査）



ホーム画面の「ウイルス検査」をタップすると、インストールされているアプリやファイルの検査を実行できます。



ウイルスを検知した場合は、上記のようなアラートが表示されます。駆除したいものにチェックを入れて「駆除」をタップすると駆除ができます。



アプリのインストールやバージョンアップ時に自動でウイルス検査が行われます。ウイルスを検知した場合は、上記のようなアラートが表示されます。「アンインストール」をタップするとアンインストールができます。

アプリの使い方（Web保護の設定）



ホーム画面の「Web保護」をタップして設定画面を開きます。

「Web保護が無効です」と表示される場合は、「OFF」と表示されているボタンをタップします。

「スマートフォンセキュリティ 特別版」をタップします。

OFFと表示されている横にあるスイッチをタップします。



確認して「OK」をタップします。

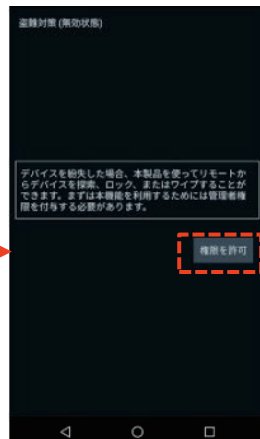
前の画面に戻り、「アクセサビリティステータス」がONになったことを確認し、「有効にする」をタップします。

「Web保護」が有効であれば、対応ブラウザ（Chrome、Android標準ブラウザ）は自動で保護されます。対応ブラウザでフィッシングサイトや危険なサイトを表示しようとした場合は、次のようなブロックページが表示されます。

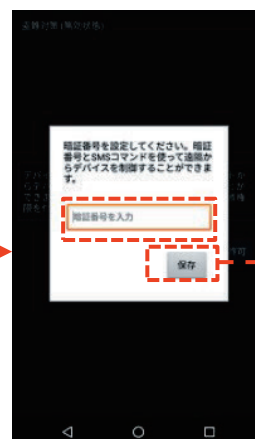
アプリの使い方（盗難対策の設定）



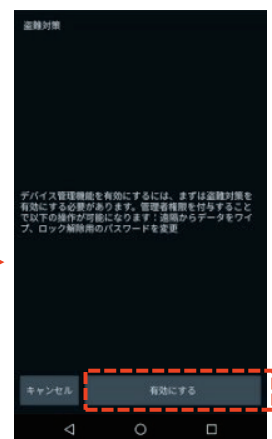
ホーム画面の「盗難対策」をタップします。



「権限を許可」をタップします。



任意の暗証番号（4桁の数字）を入力して「保存」をタップします。ここで設定した暗証番号は、盗難対策の遠隔制御や設定変更を行う際に必要になります。



「有効にする」をタップします。



ソースネクストアカウント（マイページID）とパスワードを入力して、「ログイン」をタップします。

※ソースネクストアカウントをお持ちでない場合は、「新規作成」をタップして手順に沿って作成してください。



盗難対策の設定画面が表示されます。

■ Webページから管理する

「デバイス探索」

Web管理ページ上から、デバイスの現在の位置情報を確認できます。

「遠隔ロック」

Web管理ページ上から、デバイスにロックをかけることができます。

「遠隔ワイプ」

Web管理ページ上から、デバイス内のデータを削除することができます。

「遠隔アラーム」

Web管理ページ上から、デバイスのアラームを鳴らしたり、メッセージを送ることができます。

■ SMSを使って管理する

「SMSコマンド」

SMSメッセージを送信して、デバイスを遠隔制御することができます。（※送信方法などについては27ページ下部を参照のこと）

「SIMカード差し替え警告」

SIMカードが差し替えられた場合に、信頼する電話番号に対してSMSメッセージを送信します。予め信頼する番号を設定しておく必要があります。

「信頼する番号を設定」

SIMカードが差し替えられた場合に通知する電話番号を設定します。SMSコマンドのリモートワイプを実行できるのもこの電話番号からのみとなります。

盗難対策の各機能は初めは無効になっています。各機能を有効にするには、その横の「OFF」と表示されているボタンをタップします。



機能の有効/無効を変更する際には、暗証番号の入力が必要です。事前に設定した暗証番号を入力して「送信」をタップします。

次の画面が表示された場合は、「有効にする」をタップして管理者権限を有効にします。
※表示される画面はOSのVer.によって違う場合があります。

次の画面が表示された場合は、「スマートフォンセキュリティ 特別版」の横にあるスイッチをタップします。

「許可」をタップします。

- SMSコマンドの送信方法
別のスマートフォンや携帯電話などから、遠隔制御するデバイスの電話番号宛に以下のようなSMSを送信します。

「BD-xxxx SMSコマンド」(xxxx は予め設定した暗証番号です。)
(例) 暗証番号でデバイスをロックしたい場合には、「BD-1234 LOCK」という文字列をSMSで送ります。

- 使用できるSMSコマンド

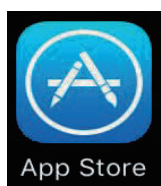
LOCATE	: デバイスの位置情報がSMSで返信されます。
SCREAM	: デバイスのアラームを鳴らして探しやすくします。
LOCK	: 暗証番号でデバイスをロックします。
WIPE	: デバイス上のすべてのデータを消去します。 (このコマンドは、予め設定した信頼する番号からのみ送信できます)
CALLME	: コマンドを送信したデバイス宛にサイレントに電話をかけることができます。 本機能を使えば、デバイスを盗んだ犯人に気付かれることなく、辺りの会話内容を聞き取ることができます。
HELP	: 使用できるSMSコマンドの一覧がSMSで返信されます。

6. セキュリティアプリ（iOS版）

iPhoneで使う専用ブラウザを提供。専用ブラウザを使い、フィッシング/詐欺サイトへのアクセスをブロックしたり、URLが安全であるかチェックすることができます。

アプリのインストール方法

『App Store』を起動し、
『スマートフォン
セキュリティ』を検索



または

下記のQRコードを
読み込みます。



アプリをインストールします。

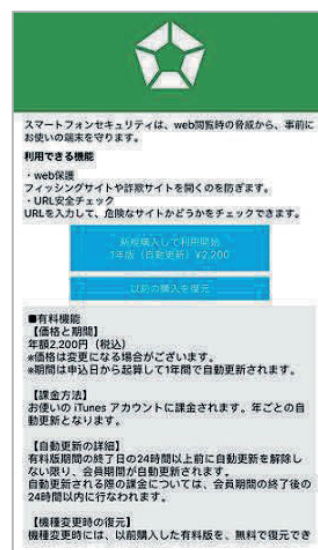


インストールが終了しましたら、
画面を閉じます。



画面を閉じます
※下記のような購入画面が出ますが、
画面を閉じてください。

⇒次頁へ



続いて、SIMカードのエントリーを実施します。
 下記のURLまたは、QRコードを読み込み、Webサイトにアクセスを行ってください。
 ※前ページのアプリインストールとは別のQRコードになります。

Webブラウザで、下記URL
 を入力するか、QRコードを
 読み込みます。

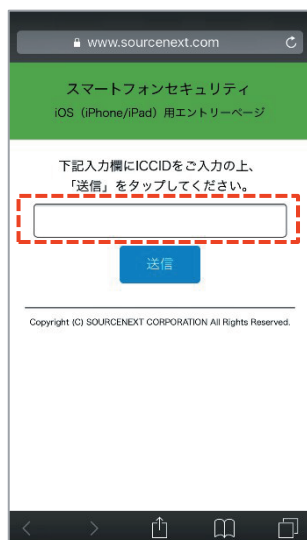
<https://rd.snxt.jp/68331>

または

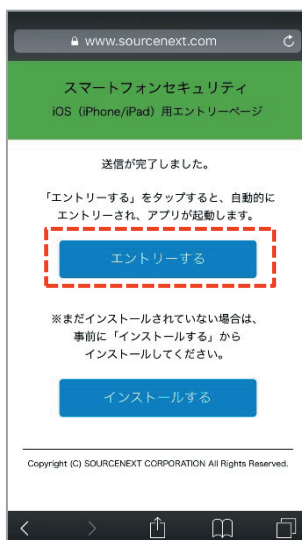
下記のQRコードを
 読み込みます。



下記の画面が表示されますので、
 ICCIDを入力し、「送信」を
 タップします。

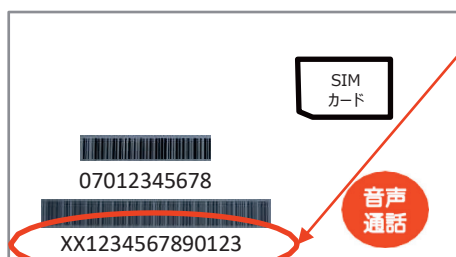


下記の画面が表示されますので、
 「エントリーする」をタップして、
 エントリーします。



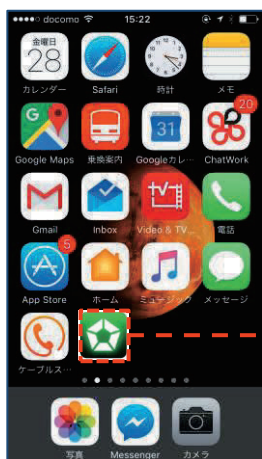
以上でSIMのエントリーが
 完了です。

★ICCIDが記載されている場所

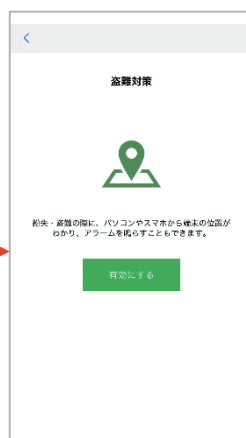


SIMカードのバーコード情報の下に
 書いてある英数字になります。

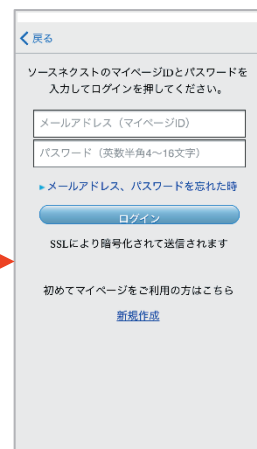
アプリの使い方（盗難対策）



『盗難対策』をタップします。



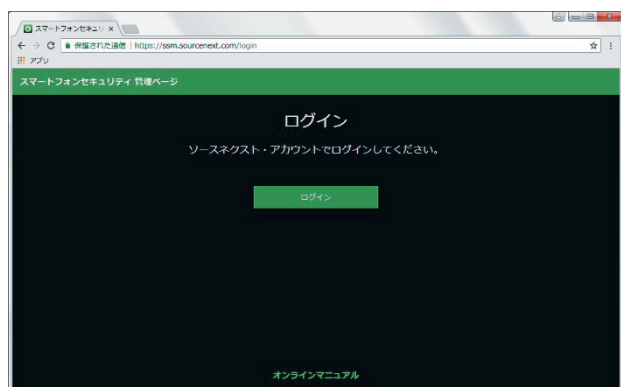
「有効にする」をタップします。



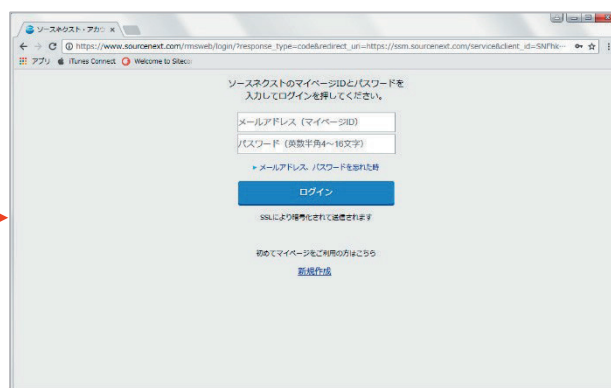
ソースネクストのマイページにログインします。
ログインが完了すると、盗難対策が、「有効」に変わります。

<https://ssm.sourcenext.com>

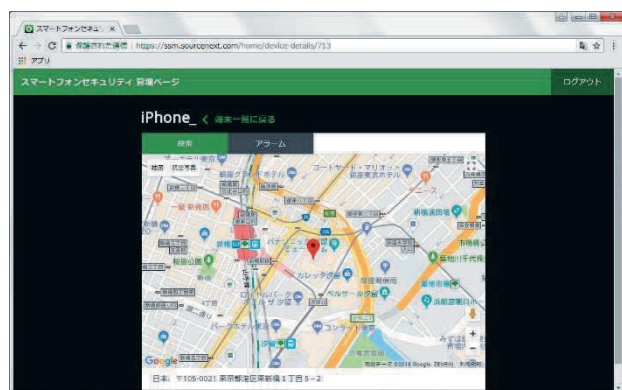
管理画面にパソコンやスマホからアクセスし、端末の位置情報の取得、アラーム、メッセージ表示を行えます。



『ログイン』をタップします。



ソースネクストのマイページにログインします。



端末を選択後、上記のページで「探索」をクリックすると、端末の位置情報を確認することができます。



アラームをクリックするとメッセージの送信などの画面が表示されます。
アラームやメッセージを送りたい場合は、メッセージ内容などを入力し、「送信」をクリックしてください。

アプリの使い方（SNSプライバシー設定）



※2023年12月現在「X」ではなく「Twitterにログイン」の表示になっています。

アプリの使い方（データ通信量チェック）

※iPhone内のデータ容量から算出をしているため、イツコム マイページとの差がある場合があります。

