

WEBROOT®

ウェブルート セキュアエニウェア

モバイル コンプリート

リファレンスガイド

Table of Contents

はじめに	2
アカウントの登録.....	2
セキュアエニウェア モバイル コンプリートのインストール.....	5
セキュアエニウェア Web サイトの使用.....	10
ステータスの確認.....	13
警告への対処.....	15
スキャンの実行.....	17
シールドの使用.....	18
スケジュールの調整 (自動更新).....	19
隔離フォルダの管理.....	20
除外された脅威の管理.....	21
セキュア Web ブラウザの使用.....	23
紛失デバイス保護の使用.....	24
着信および SMS ブロックの使用.....	26
アプリケーション検査の使用.....	30
設定の変更.....	31
アプリケーションのアンインストール.....	35
セキュアウェブの使用.....	35
パスワード管理の使用.....	36
セキュアシンクの概要.....	38
同期されたファイルを他のデバイスで見る.....	39
自分のモバイル デバイスにファイルをダウンロードする.....	40
写真やビデオをアップロードする.....	40
自分のオンライン アカウントにファイルをアップロードする.....	41
ファイルや写真を削除する.....	41

はじめに

ウェブルート セキュアエニウェア モバイルをインストールし、アカウントを作成いただくと、Android デバイスに対して保護機能を提供します。

- アカウント作成後に 1 回、それ以降は週に 1 回スキャンを実行します。また定義ファイルの更新を毎日確認します("定義ファイル" とは、ウイルス、スパイウェア、またはその他の種類の不正なアイテムを判別するために必要な情報ファイルです)。スケジュールを変更する場合は、「[スケジュールの調整 \(自動更新\)](#)」を参照してください。
- セキュリティ問題の可能性のあるファイルやウェブページを検出した場合、ユーザーへ即座に警告します。詳細については、「[ステータスの確認と警告への対処](#)」を参照してください。
- 新しくインストールされたメモリ カードやアプリケーションすべてに脅威がないかを監視します。詳細については、「[シールドの使用](#)」を参照してください。
- 訪問するすべての Web サイトにマルウェアやフィッシングの危険がないかを監視し、悪意のある可能性のあるサイトをブロックします。詳細については、「[セキュア Web ブラウザの使用](#)」を参照してください。
- 迷惑な着信およびテキスト メッセージをブロックします。ブロック リストを作成するには、「[着信および SMS ブロックの使用](#)」を参照してください。
- デバイスの紛失や盗難の場合、デバイスの情報を保護します。詳細については、「[紛失デバイス保護の使用](#)」を参照してください。

アカウントの登録

はじめに、以下のようにアカウントを登録する必要があります。以下の操作はモバイルデバイスにて行う事も可能ですが、PC 上での操作として記載してございますのでご注意ください。 :

1. 下記の URL にアクセスして、アカウント登録を開始します。

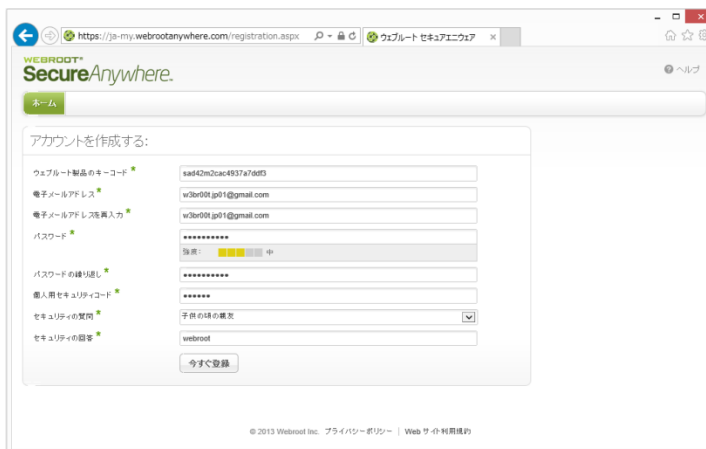
<https://my.webrootanywhere.com/>



2. この画面で「今すぐ登録する」をクリック



3. 情報を入力します



4. 登録が完了すると、電子メールが登録時のメールアドレスに届きます。



メール内にあるリンクをクリックして、コンソールをアクティブにします。

5. セキュリティコードを確認する画面になりますので登録時に設定したセキュリティコードの指定された文字を入力して「今すぐ登録確認する」をクリックします。



6. 確認が完了すると、コンソールの画面に変わります。パスワード機能を有効にするためにパスワードの「アカウントを設定する」ボタンをクリックします。クリックすると、確認のダイアログが表示されますので左側の「閉じる」ボタンをクリックしてください。



7. 上記操作を行うと、表示がグリーンに変更されます。しばらく待つとパスワード機能が有効になります。



セキュアエニウェア モバイル コンプリートのインストール

セキュアエニウェア モバイルを下記の方法でインストールします。あらかじめアカウントを登録しておいていただく必要があります。アカウントの登録方法につきましては、「アカウントの登録」をご参照ください。

1. Google Play ストアにアクセスしてセキュアエニウェアのアプリを検索します。
検索ワードは「セキュアエニウェア」で行います。

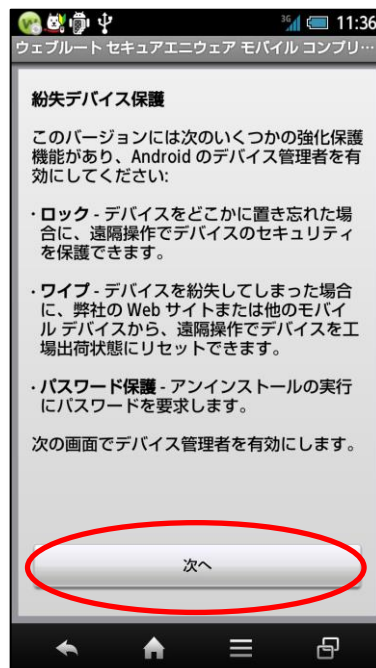
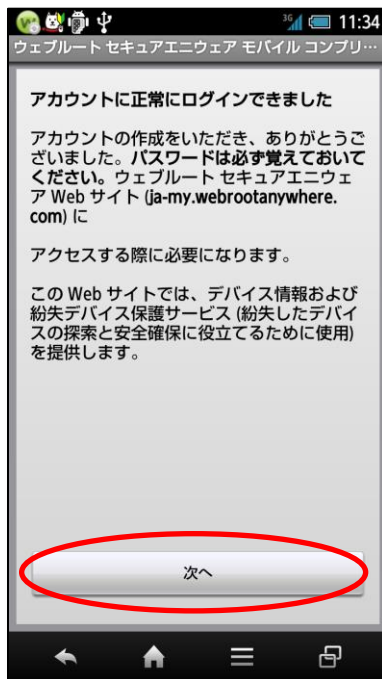


2. インストールの完了後、「開く」をタップするとセキュアエニウェアが起動します。ライセンスの認証を求められますので、「同意」をタップしてください。



3. セットアップ画面に移行しますので画面の指示に従って初期セットアップを行ってください。





4. デバイスマネージャーを有効にするかどうかを確認されます。これを有効にしないと「紛失デバイス保護」機能を利用し、ワイプ機能（デバイスを初期状態にクリアし、個人情報を見えなくする機能）が完全に動作しなくなります。「有効にする」をタップして、デバイスマネージャーを有効にさせていただくことをお勧めいたします。

この選択が完了すると、セットアップの完了画面が表示されます。



- 完了をタップ後、「警告」の表示が現れる場合がありますが、ここで「今すぐ修正」をタップし、画面の指示に従って問題を修正してください。
修正が完了すると、全て終了です。



6. アプリ一覧に3つのアイコンができている事を確認してください。(下記の画面は一例となります。各デバイスのメーカーや機種によって異なりますのでご注意ください)
- ・セキュアエニウェア ... アンチウイルスの本体画面となります
 - ・セキュアウェブ ... インターネットを安全に見ることができるウェブブラウザです
 - ・Backup&Sync ... PC や iPhone, Android で写真やファイルを共有する機能です



セキュアエニウェア Web サイトの使用

セキュアエニウェア Web サイトには、お使いのウェブルート アカウント内の各 PC やモバイル デバイスについてのステータスと履歴が表示されます。この Web サイトからは、電話またはタブレットに紛失デバイス保護コマンドを送信することもできます。

※これらの操作は Android デバイスからでも可能ですが、PC よりログインして利用可能です。下記の解説では、PC からの操作を前提としています。

セキュアエニウェア Web サイトを使用する手順:

1. <https://my.webrootanywhere.com> に移動し、登録済みの電子メール アドレスとウェブルート パスワードを使用してログインします。ログインには、デバイス上でのウェブルート アカウントの作成に使用したのと同じアドレスとパスワードを使用する必要があります(忘れた場合は、[パスワードを忘れた場合] リンクをクリックします)。すべてのデバイスのステータスが一目で確認できます。



WEBROOT®
SecureAnywhere.

ホーム

ログイン確認:

セキュリティコードの 2 番目と 4 番目の文字を入力してください (大文字と小文字は区別されます)

 [ログインできない場合](#)

WEBROOT®
SecureAnywhere. wj2013-hfu01@mail.goo.ne.jp

ホーム PCセキュリティ モバイルセキュリティ バックアップと同期 パスワード 名前のみ | ログイン | ログアウト

PCセキュリティ

1 台の PC が保護されています
0 台の PC が現在感染しています
0 台の PC が感染しています (過去 24 時間)

モバイルセキュリティ

1 台のデバイスを保護しています
0 台のデバイスに対応が必要です
0 台のデバイスが感染しています

バックアップと同期

1 MB 使用中 (1% 未満)
ストレージ容量合計 10 GB

パスワード

保護された Web サイトに関するプロファイルおよびパスワードの情報を、インターネットアクセスのあるどのコンピュータからでも安全に編集できます。

2. スマホ等、モバイルデバイスに関する詳細を表示するには、「モバイルセキュリティに進む」をクリックし Web ページのデバイス名をクリックします。
詳細を表示するパネルが開きます。



3. パネルの上部でセキュリティ ステータスや操作履歴、紛失デバイス保護コマンドのタブをクリックすることもできます (これらのコマンドの使用の詳細については、「[紛失デバイス保護の使用](#)」を参照)。

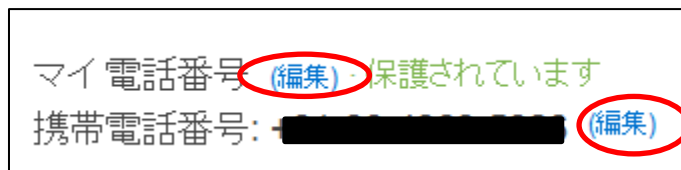
注意： 消去コマンドは、セキュアエニウェア モバイルのプレミアム/コンプリートバージョンでのみ使用できます。



4. デバイスの表示名は、デバイス名の横にある [編集] リンクをクリックすると、変更できます。

注意： 電話番号が変更した場合、表示番号の横にある [編集] リンクをクリックし新し

い番号を入力してください。(Android タブレットのバージョン 3.0 以上では、電話番号はタブレットには表示されません。)



この Web サイトに表示されているモバイル デバイスを使用しなくなった場合、リストからそのデバイスを削除することができます。パネルの下部でデバイス画像 (どのタブからもアクセス可能) の下にある [このデバイスを削除] をクリックします。Web サイトからデバイスを削除しても、アプリケーションは電話またはタブレットからアンインストールされないことに注意してください。後でデバイスの電源をオンにし、デバイスがセキュアエニウェア アプリケーションと再接続する場合、このデバイスはウェブルート セキュアエニウェア Web サイトにまた表示されます。



ステータスの確認

デバイスのステータスは、アプリケーションまたはウェブルート セキュアエニウェア Web サイトから確認できます:

- **デバイス アプリケーションから操作する場合:**ウェブルートのアイコンがデバイスのホーム パネル (上部または下部のいずれか) に表示されます。セキュアエニウェア モバイルがシステム ステータスについて警告する必要がある場合、ウェブルート アイコンのインジケータが黄または赤に変わります (🚫)。アイコンをタップするか Android

バーをドラッグすると、問題点の詳細が表示されます。



- ウェブルート セキュアエニウェア Web サイトから操作する場合: Web ブラウザで、<https://my.webrootanywhere.com> に移動し、電子メール アドレスとウェブルート パスワードを使用してログインします。パネルが開き、お使いのウェブルート アカウント内のすべてのデバイスが表示されます。各デバイスで、ステータスやアクティビティ履歴を確認できます。



警告への対処

セキュアエニウェア モバイルが潜在的脅威を検出すると、赤または黄色の警告メッセージを表示します。メッセージはデバイス上とセキュアエニウェア Web サイトにて確認できます。セキュリティ上の重大な危険にさらされている可能性がある脅威の場合または更新サービスの期限が切れた場合、赤の！マークが表示されます。重大ではないが注意が必要な可能性がある他のアイテムの場合、黄色の！マークが表示されます。

問題は、デバイス上のみで修正することができます。

問題を修正する手順は以下のとおりです。

1. セキュアエニウェア モバイルのアプリケーションを開きます。

メイン パネルに、問題に関する詳細情報と、問題を修正するためのオプションが表示されます。

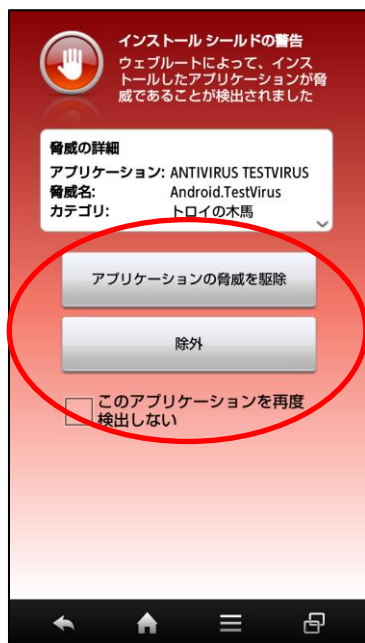


2. [修正] ボタンが表示された場合には、ボタンをタップして問題を解決します。脅威が検出された場合、セキュアエニウェア モバイルに、その脅威を駆除するか除外するかと

いうオプションが表示されます。



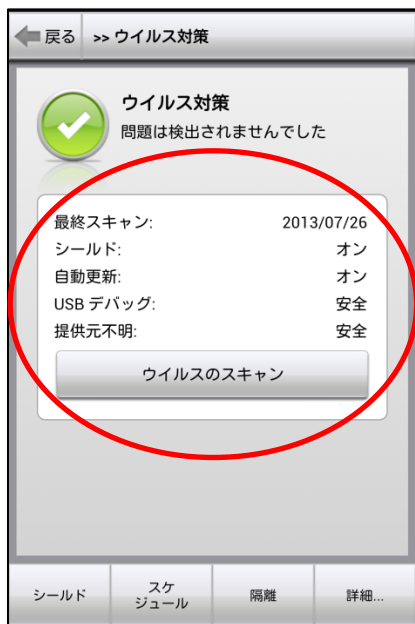
- **駆除**。アイテムを駆除することが最も安全な処理です。セキュアエニウェア モバイルによって脅威が隔離フォルダに移動され、デバイス上で動作できなくなります。(駆除したアイテムが後で必要になった場合には隔離フォルダから復元することができます。)詳細については、「[隔離フォルダの管理](#)」を参照してください。
- **除外**。アイテムが無害であることが確実な場合、セキュアエニウェア モバイルがスキャン時にそのアイテムを検出しないように除外します。詳細については、「[除外された脅威の管理](#)」を参照してください。



スキャンの実行

セキュアエニウェア モバイルは、毎週自動的に対象のデバイスをスキャンします。即座にスキャンを実行する場合は、メインパネルの[今すぐ脅威をスキャン]をタップします。スキャンが終了し、[完了]をタップすると全体のシステムステータスが表示されます。

- **最終スキャン。**最後に実行したスキャンの日付と時刻が表示されます。8日以上スキャンが行われていない場合、ステータスアイコンが黄色になります。
- **シールド。**すべてのシールドが有効な場合、[オン]と表示されます。1つ以上のシールドが無効な場合、黄色いアイコンと[修正]ボタンが表示されます。すべてのシールドを有効にするには、[修正]をタップします。
- **自動更新。**スキャンおよび定義ファイルが、いずれも自動更新用にスケジュールされている場合は、緑色のアイコンが表示されます。これらがスケジュールされていない場合、黄色いアイコンと[修正]ボタンが表示されます。[修正]をタップすると、スケジュールが既定値(週一度のスキャン、毎日の定義の更新)に戻ります。
- **[USB デバッグ] 設定。**[安全]という表示は、Android デバイスの USB デバッグ設定が "安全"、つまり、USB ポートがコンピュータと通信できない設定であることを示します。
- **[提供元不明] 設定。**[安全]という表示は、Android デバイスの [提供元不明] の設定が "安全"、つまり、Android マーケット以外からのアプリケーションのインストールを許可しない設定であることを示します。



シールドの使用

セキュアエニウェア モバイルには、シールドと呼ばれるアクティブ保護機能が搭載されています。これは潜在的な脅威または脆弱性が検出されると即座に警告する機能です。



- **インストール シールド**。新しいアプリケーションまたは更新されたアプリケーションに潜在的な脅威が含まれている場合、即座に警告し、インストールをブロックします。セキュアエニウェア モバイルは、脅威を駆除するか（隔離フォルダに隔離）または除外してダウンロードを続行するかを選択するオプションを提供します。
- **ファイル システム シールド**。デバイス内のメモリ カードに潜在的脅威（デバイスの再起動時や電源をオンにしたときに起動される脅威など）が含まれている場合に警告します。脅威が検出されると、脅威を駆除するか（隔離フォルダに隔離）または除外するかを選択するオプションが提供されます。
- **実行シールド**。疑わしいアプリケーションやファイルが、デバイス上でインストールまたは起動を試みた場合に警告します。脅威が検出されると、そのアイテムが実行されないようにするか（隔離フォルダに隔離）または警告を無視してアイテムを実行するかを選択するオプションが提供されます。
- **ダイアラー シールド**。デバイスの IMEI 番号（国際移動体装置識別番号）の漏洩、デバイス データの消去など、何らかの問題があるまたは損傷を与える行為につながる可能性がある、Web サイトによる電話番号のダイヤルをブロックします。
- **提供元不明シールド**。[提供元不明] 設定が有効な場合に警告します。[提供元不明] 設定は、Android デバイスの [設定] から変更できるモバイル デバイスの設定です。有効にすると、Android マーケット以外からアプリケーションをダウンロードできるようになります。（注意：AT&T のデバイスでは、[提供元不明] の設定は常に安全と表示されます。これは設定が無効であることを意味します。）

- **USB デバッグ シールド。** [USB デバッグ] 設定が有効な場合に警告します。[USB デバッグ] 設定は、[設定] から変更できる Android デバイスの設定で、USB ポート経由でコンピュータと通信できます。モバイル デバイスを USB 経由で接続すると、このポート経由でダウンロード可能なマルウェアから攻撃を受けやすくなります。

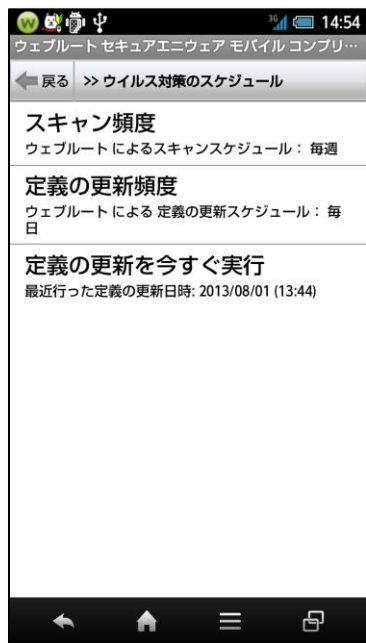
シールド設定を変更する手順は以下のとおりです。

1. セキュアエニウェア モバイルのメイン パネルの下部にある[セキュリティ] をタップします。
2. [ウイルス対策] (🔍) をタップします。
3. 下部の [シールド] をタップします。
4. シールドのオン/オフを切り替えるには、シールド オプションのチェックボックスをタップします。
緑色のチェックマークは、設定がオンであることを示します。

注意：シールド設定を無効にすると、セキュアエニウェア モバイルに警告が黄色で表示されません。

スケジュールの調整 (自動更新)

セキュアエニウェア モバイルは、対象のデバイスを週に一度スキャンし、定義ファイルを毎日更新します。これらのスキャンと更新スケジュールの頻度は、必要に応じて変更できます。



スケジュールを変更する手順は次のとおりです。

1. セキュアエニウェア モバイルのメイン パネル下部にある [セキュリティ] をタップします。

2. [ウイルス対策] (👉) をタップします。
3. 下部の [スケジュール] をタップします。
4. 調整する対象に応じて、[スキャン頻度] または [定義の更新頻度] をタップします。
5. 次のパネルで、[なし]、[1 時間ごと]、[毎日]、または [毎週] をタップします。

また定義を即座に更新するオプションもあります。これには、[定義の更新を今すぐ実行] をタップします。セキュアエニウェア モバイルは、ウェブルートの Web サイトに接続し、最新の定義ファイル (存在する場合に) をダウンロードします。

隔離フォルダの管理

検出されたアイテムを駆除すると、ファイルはセキュアエニウェア モバイルによって隔離フォルダに移動されます。このエリアでは ファイルが動作不可能になり、デバイス上で実行できなくなります。検出されたアイテムを駆除しても、後でそれが必要になった場合は元の場所に復元できます。また隔離フォルダからアイテムを永久に削除して、デバイス上の空き容量を確保することもできます。



隔離フォルダのアイテムを表示する手順:

1. セキュアエニウェア モバイルのメイン パネル下部にある [セキュリティ] をタップします。
2. [ウイルス対策] (👉) をタップします。

3. 下部にある [隔離] をタップします。
[隔離] パネルに、脅威名と検出された場所が表示されます。

隔離されたアイテムを復元または完全に削除する手順:

1. アイテム名をタップします。
別のパネルが開き、アイテムの詳細およびアイテムを復元または削除するためのオプションが表示されます。(提供元不明アプリケーションのインストールを禁止するように設定されている場合、[提供元不明] の設定を一時的に無効にするまで、セキュアエニウェア モバイルによってアイテムを復元できません。この場合、メッセージ ボックスに、アプリケーションを復元する手順が表示されます。)
2. 複数のアイテムを削除する場合は、モバイル デバイスのメニューボタンを押し、[隔離フォルダを消去] をタップします。

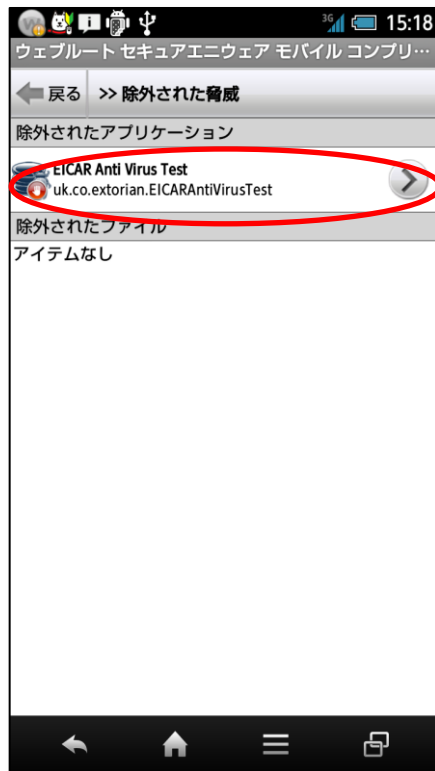
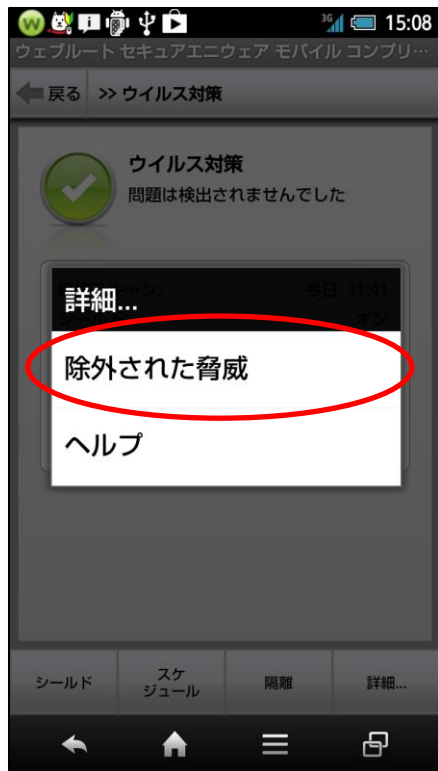
※AT&T が同社の Android 携帯に課している制約事項のために、AT&T 携帯で隔離されたアプリケーションは復元できません。この場合、Android マーケットからアプリケーションを再度ダウンロードする必要があります。

除外された脅威の管理

隔離フォルダから脅威を復元するか、脅威を除外することを選択すると、アイテムがセキュアエニウェア モバイルによって [除外された脅威] リストに追加されます。このリストに追加すると、今後のスキャンでセキュアエニウェア モバイルによって同じ脅威が何度も検出されることがなくなります。このアイテムを再度検出する必要がある場合には、このリストからそのアイテムを削除します。

[除外された脅威] リストからアイテムを削除する手順:

1. セキュアエニウェア モバイルのメイン パネル下部にある [セキュリティ] をタップします。
2. [ウイルス対策] (🔍) をタップします。
3. 下部の [詳細...] をタップします。
4. [除外された脅威] をタップします。
5. [除外された脅威] パネルでは、除外する個別の脅威またはすべての脅威を選択できます。個別の脅威を除外から削除するには、脅威名を選択し、リストから脅威を削除するオプションのパネルが開くまで待ちます。このパネルのすべての脅威を除外から削除するには、モバイル デバイスのメニューボタンを押し、[除外リストの消去] をタップします。



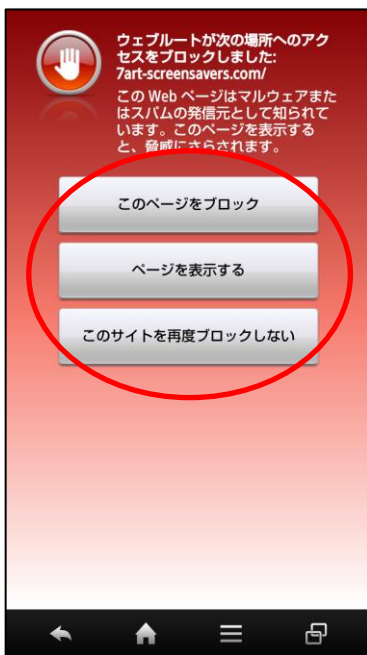
セキュア Web ブラウザの使用

セキュア Web ブラウザを使用すると、Web サイトへアクセスする前、読み込みから悪意のある Web サイトをブロックするので、安全にアクセスすることができます。マルウェアを拡大させることが知られている Web サイトにアクセスしようとする、アラートが表示され、次のオプションが示されます:このサイトをブロック、このサイトへ進む、またはこのサイトを再度ブロックしない、というオプションが表示されます。セキュア Web ブラウザを常に有効にし、悪意のある可能性ありと分類されるすべてのサイトを常にブロックすることをお勧めします。

注意:現在、セキュア Web ブラウザは、標準搭載されている Android ブラウザとコンプリートバージョンのセキュアウェブ アプリにてサポートしています。

セキュア Web ブラウザを無効化または有効化する手順:

- 1.セキュアエニウェア モバイルのメイン パネル下部にある [セキュリティ] をタップします。
- 2.[セキュア Web ブラウザ] (🔒) をタップします。
既知の脅威をブロック機能が有効な場合、[既知の脅威をブロック] パネルに [オン] ボタンが表示されます。
- 3.このボタンをタップすると、機能を有効あるいは無効に切り替えられます。
セキュア Web ブラウザをオフにすると、セキュアエニウェア モバイルに黄色の！マークが表示され、使用しているデバイスが危険にさらされていることを警告します。



脅威を除外すると選択したサイトのリストを確認または編集するには、[セキュア Web ブラウザ] パネル下部にある [除外された Web サイト] をタップします。[除外された Web サイト] リストからサイトを削除する場合は、サイト名を押したままにし、[選択された除外アイテム] パネルが開くのを待って [除外を停止] をタップします。パネルのメニューボタンをタップし、

[除外リストの消去] をタップして、リストにあるすべてのサイトの除外を停止します。リストからサイトを削除すると、アクセスを試みるとセキュア Web ブラウザはそのサイトを再度検出します。

紛失デバイス保護の使用

紛失デバイス保護は、紛失した携帯などの位置を特定し、必要に応じてロックする機能です。これらのコマンドは別のモバイル デバイスまたはセキュアエニウェア Web サイト利用して送信することができます。:

- **Lock(ロック):** 離れた場所からデバイスをロックし、不正使用を防止します。デバイスがいったんロックされると、ロックを解除するためにアカウント パスワードを入力する必要があります。
- **Wipe(消去) (プレミアム/コンプリート バージョンのみ):** すぐにデバイスをロックし、出荷時の既定値にリセットして、携帯から個人データ、アプリケーション、アカウントを含むすべてを消去します。(Android OS 2.2 以前のバージョンをお持ちの場合、出荷時の既定値へのリセットや、アカウントの消去はできませんが、すべての個人データが消去されます。) **デバイスが永久に紛失し完全に消去してもよい場合以外は、このコマンドを使用しないでください。** データを消去する前に、セキュアエニウェア モバイルによって自動同期機能がオフになるため、それまでに Gmail サーバーにアップロードした連絡先やカレンダー エントリなどのアイテムが削除されることはありません。
- **Locate(探索):** 電話をロックして (前述の lock コマンドと同様)、携帯の現在位置を示す Google マップ ページへのリンクを応答します。**注意:** Locate コマンドを有効にするには、デバイスに GPS、Wi-Fi、またはテレフォニー接続が必要です。また、デバイスが SMS に対応していない、またはウェブルートがお客様のキャリアに対応していない場合には、Android バージョン 2.2 以降でデータ接続を実行しているデバイスで Android マーケットプレイスにログインしている必要があります。
- **Scream(サイレン):** 電話をロックして (前述の lock コマンドと同様)、電話からサイレン音を大きな音で鳴らし、デバイスの場所を特定したり、泥棒を驚かせたりします。この音は、最大 2 分間鳴り続けるか、またはパスワードを使用してデバイスのロックを解除するまで鳴り続けます。
- **[Customize Lock Screen (ロックスクリーンのカスタマイズ)] (セキュアエニウェア Web サイトからのみ使用できます):** 電話をロックし (前述の Lock コマンドと同様)、パネルにテキスト メッセージを表示します。このコマンドを使用すると、「この電話を見つけたら 555-5555 までお電話ください。」のようにメッセージを表示できます。

注意: GSM 規格の携帯電話では、セキュアエニウェア モバイルの**プレミアム/コンプリート** バージョンの追加機能として、SIM カードを取り外すとロックがかかる機能が搭載されています。ロックはウェブルートパスワードを入力することによって解除できます(SIM カード ロック機能を無効にするには、メイン パネルから [個人情報とプ

ライバシー]に移動し、[紛失デバイス保護]をタップして、SIMカードロックの設定を確認します)。

紛失デバイス保護のご利用方法:



1. [紛失デバイス保護] が有効であることを確認します。この機能をデバイスから有効にするには、[個人情報とプライバシー] をタップし、[紛失デバイス保護] (➡) をタップします。
[紛失デバイス保護] パネルの [紛失デバイス保護] 設定に [オン] ボタンが表示されません。
注意: セキュアエニウェアの **プレミアム/コンプリート**バージョンでは、Android のデバイス管理者設定の変更またはセキュアエニウェア アプリケーションのアンインストール前に、ウェブルート パスワードを入力するよう求められます。デバイスが盗難に遭った場合、この機能によって、セキュアエニウェアをアンインストールして紛失デバイス保護を無効にできないようになっています。
2. ボタンが [オフ] と表示されている場合は、ボタンをタップしてください。
3. Android OS バージョン 2.2 以降では、デバイス管理を動作させる方法を指示する別のパネルが現れます。デバイス管理者を有効にすることにより、高度な Wipe コマンド機能が有効になります (Wipe を開始すると、セキュアエニウェア モバイルは出荷時の既定値にリセットを実行します)。このパネルの [ライセンス認証] をタップします。
4. ウェブルート アカウント パスワードを入力します。
注意: パスワードを忘れた場合は、パスワード ダイアログの [パスワードを忘れた場合] をタップして新しいパスワードを取得します。(パスワード ダイアログは、すべての紛失デバイス保護機能で必ず表示されます。)

5. 紛失デバイス保護を有効にすると、別の電話またはウェブルート セキュアエニウェア Web サイトから紛失デバイス保護機能のコマンドを使用できます。

- **デバイスから操作する場合：**
コマンドの後にパスワードを指定して、テキスト メッセージ経由で送信します。
たとえば、自分のパスワードが **check123** の場合に Lock コマンドを送信するには、テキスト メッセージ **lock check123** を別の電話から送信してロックします。
- **ウェブルート セキュアエニウェア Web サイトから操作する場合：**
<https://my.webrootanywhere.com> に移動し、登録済みの電子メール アドレスとウェブルート パスワードを使用してログインします。使用しているデバイスの [紛失デバイス保護] のタブをクリックします。パネルでいずれかのコマンドを選択します。

電話を探す場合、パスワードを使用してデバイスのロックを解除するためのオプション ダイアログが表示されます。

送信されたコマンドのリストを表示するには、セキュアエニウェア モバイル アプリケーションの [紛失デバイス保護] パネルに移動し、[**コマンド ログ**] をタップします。

着信および SMS ブロックの使用

着信および SMS ブロックを使用すると、不適切あるいは不明な電話番号からの着信およびテキスト メッセージをフィルタできます (SMS (Short Message Service) は、モバイル デバイス用に使用されるテキスト通信サービスです)。ブロックリストに電話番号を入力すると、その番号からの着信は留守番電話に直接送信され、テキスト メッセージはブロックされます。着信またはテキストがブロックされると、セキュアエニウェア モバイルが通知を表示します。

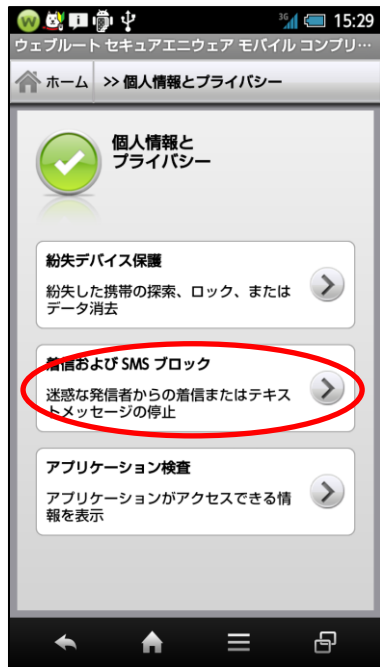
注意： 呼び出しおよび SMS のブロック機能は、電話機能のないタブレットでは使用できません。

着信と SMS メッセージをより詳細に制御できるように、着信および SMS のブロックには次の追加設定が用意されています：

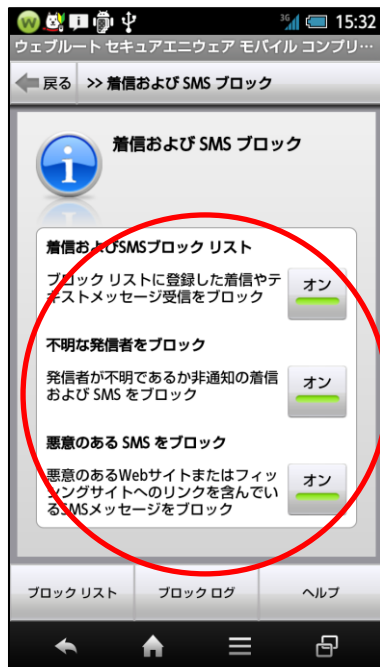
- **不明な発信者をブロック。** 電話番号が不明な着信は、直接留守番電話に転送されます。不明な連絡先からの SMS メッセージはブロックされます。
- **悪意のある SMS をブロック。** 悪意のある Web サイトへのリンクを含む SMS メッセージは、送信者が問題のない連絡先の場合も常にブロックされます。悪意のある Web サイトには、ウイルス、マルウェアあるいはフィッシング詐欺などが仕掛けられていることがあります。SMS メッセージに疑わしい Web サイト (「悪意のある」とは分類できなくても、脅威が含まれている可能性のある Web サイト) のリンクが含まれている場合、SMS は受信することができます。ただしリンクをクリックすると黄色の警告が表示され、処理を続行するかどうかを判断する必要があります。

着信および SMS ブロック機能を無効化または有効化する手順：

1. セキュアエニウェア モバイルのメイン パネル下部にある [個人情報とプライバシー] をタップします。



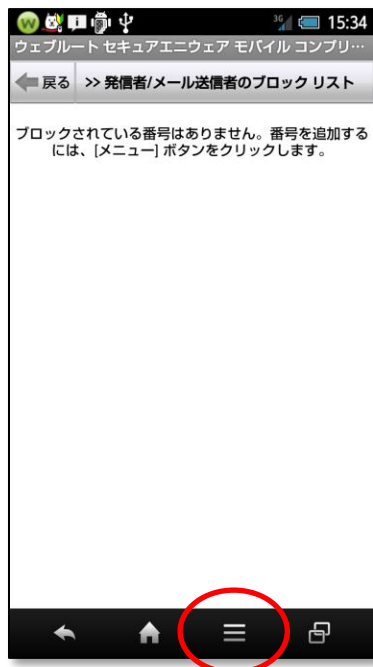
2. [着信およびSMS ブロック] (👉) をタップします。
機能が有効な場合、横に [オン] ボタンが表示されます。



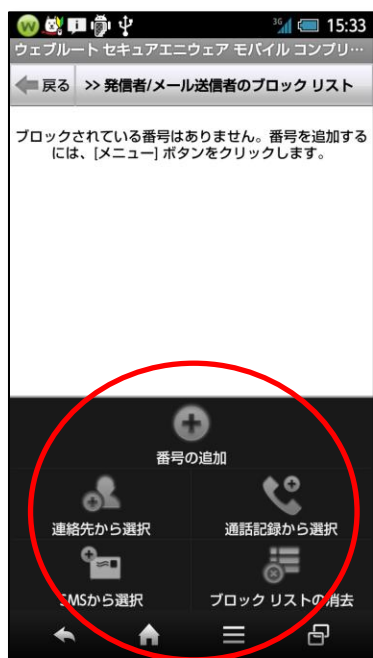
3. このボタンをタップすると、機能を有効あるいは無効に切り替えられます。

ブロックするリストを作成する手順:

1. [着信および SMS ブロック] パネルの下部にある [ブロック リスト] をタップします。
ブロック リストにこれまで入力した番号がパネルに表示されます。

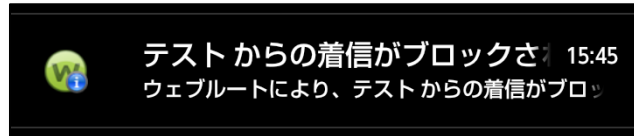


2. ブロックする番号や短縮番号を追加するには、モバイル デバイスのメニューボタンを押し、次のオプションのいずれかをタップします。
 - 番号の追加
 - 連絡先から選択
 - 通話記録から選択
 - メールから選択

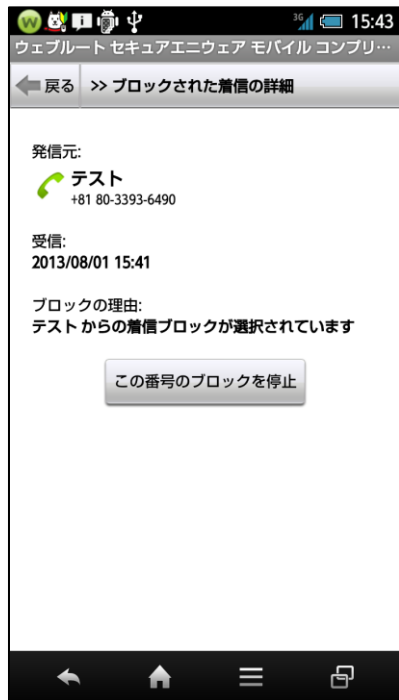
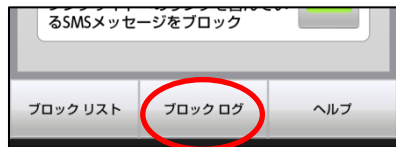


3. 番号を入力する場合、市外局番を含む 10 桁の番号が完全に入力されていることを確認してください。

ブロックするリストに番号を入力すると、その番号からの着信は留守番電話に直接送信されます。SMS メッセージは単純にブロックされます。デバイスの上部にある [通知] バーに、セキュアエニウェア モバイルによってブロックされた着信に関するメッセージが表示されます。メッセージをタップすると、ブロックされたメッセージに関する詳細が表示されます。

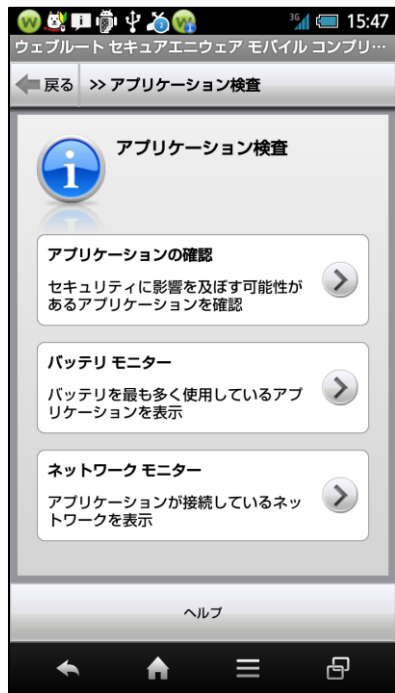


4. これまでにブロックしたすべての着信とテキスト メッセージのログを表示する場合は、[着信および SMS ブロック] パネルに戻り、[ブロック ログ] をタップします。



アプリケーション検査の使用

アプリケーション検査を使用して、プライバシーの侵害や料金の発生、バッテリー消耗の懸念があるアプリケーションを特定できます。



アプリケーション検査の利用手順:

1. セキュアエニウェア モバイルのメイン パネル下部にある [個人情報とプライバシー] をタップします。
2. [アプリケーション検査] (🔍) をタップします。
3. 以下のいずれかを選択します。

アプリケーションの確認。

このオプションは、セキュリティに影響を及ぼす可能性があるアプリケーションを特定します。次のパネルが表示されたら、🔍 をタップして特定されたアプリケーション一覧を表示します。その一覧に示される行為は、次のとおりです。

- SMS (Short Message Service) および MMS (Multimedia Messaging Service) を利用する。SMS は、モバイル デバイス用に使用されるテキスト通信サービスです。MMS は SMS を拡張したサービスで、画像やビデオなどのマルチメディア コンテンツを送信できます。
- ユーザーに確認を行わず、料金のかかる電話をかける。
- アカウントに登録された、個人情報を盗む可能性があるアクセス。
- ネットワークまたは GPS (Global Positioning System、衛星を利用したナビゲーション システム) を介してユーザーの場所を追跡する。

スキャンが完了すると、ウェブルート セキュアエニウェアにより、セキュリティの脆弱性に基づいてアプリケーションが一覧表示されます。課金アプリケーションにリストされているアプリケーションの中には、適正であり、電話機能へのアクセス許可を必要とするものもあれば、アクセス許可を必要とせず、余計な課金がされるものもあることに注意してください (たとえば、SMS 機能の許可を要求するカード ゲームを持っている場合など)。

バッテリー モニター。

このオプションでは、次の情報が表示されます：

- **バッテリー情報。** バッテリーに関するリアルタイムの統計情報 (残りの充電率、温度など)。
- **アプリケーションによる電力使用量。** 各アプリケーションが使用しているバッテリー電源の利用率。バッテリー消耗の懸念があるアプリケーションを特定できます。[アプリケーションによる電力使用量] には、時間の経過に伴う統計情報が表示されます。
- **Current Usage (現在の使用量)。** リアルタイムの使用量統計情報です。パネルの一番下で、[Current Usage (現在の使用量)] ボタンをタップすると利用できます (デバイスが USB またはコンセントに現在接続されている場合、デバイスがバッテリーで作動していた前回の統計情報が表示されます)。

ネットワーク モニター。

このオプションでは、ネットワークに現在アクセスしているアプリケーションを確認できます。使用中のネットワーク プロトコル、ローカル IP およびリモート IP のアドレス、ポート接続ステータスなどの統計情報が提示されます。この情報によって、国外のリモート ホストに接続された不正アプリケーションを検出するのに役立ちます。

リストのアイテムをクリックして、インターネットの WhoIs データベースに照会できます。この情報によって、リモート IP アドレス、この IP アドレスに対応する DNS 名、接続元の国と地域、リモート ホストのインターネット サービス プロバイダーと組織、およびリモート ホストの緯度と経度が分かります。Google マップでホストの位置を表示したい場合は、[Pinpoint (詳細位置)] をタップします。

設定の変更

セキュアエニウェア モバイルでは次の設定の変更を行うことができます：自分のアカウントのパスワード、ウェブルートアイコンのステータス表示 (通知バー)、セキュアエニウェア モバイルに保存されている電話番号、WARN (Webroot Automated Research Network) への送信。

注意： WARN は、スキャンおよびシールドで検出された脅威をウェブルートに提供することで、新しい脅威の特定と対処を行うグローバル コミュニティです。

アカウント パスワードを変更する手順：

1. セキュアエニウェア モバイルのメイン パネルで、モバイル デバイスのメニューボタンを押します。



2. [パスワードの変更] をタップします。
3. 現在のパスワードと新しいパスワードを入力します。

アカウントパスワードの変更

現在のパスワード

新しいパスワード

パスワードの確認

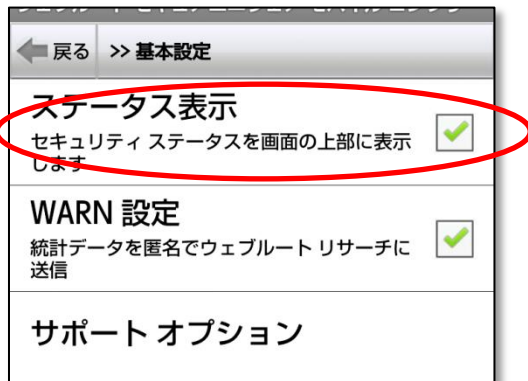
OK キャンセル

4. [OK] をタップします。

ウェブルートアイコンのステータス表示を変更する手順:

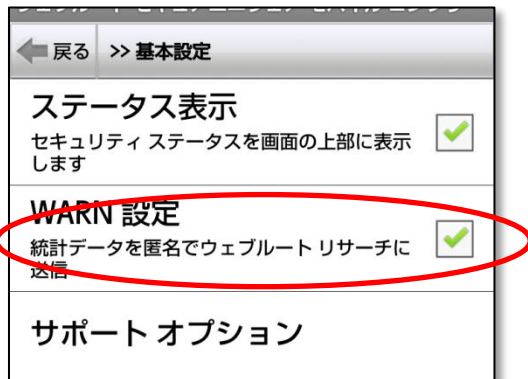
1. セキュアエニウェア モバイルのメイン パネルで、モバイル デバイスのメニューボタンを押します。
2. [基本設定] をタップします。
3. [ステータス表示] の横のチェックボックスをタップします。
緑色のチェックマークは、ウェブルート アイコンがデバイスの上部のバーに表示されていることを示します。チェックマークがグレー表示の場合、上部のバーにアイコンが表示されていませ

ん。



WARN を無効にする手順:

1. セキュアエニウェア モバイルのメイン パネルで、モバイル デバイスのメニューボタンを押します。
2. [設定] パネルで、[基本設定] をタップします。
3. [WARN 設定] の横のチェックボックスをタップして、チェックマークをグレーアウトします。



ウェブルート セキュアエニウェア モバイルに保存されている電話番号を変更する手順:

1. <https://my.webrootanywhere.com> に移動し、登録済みの電子メール アドレスとウェブルート パスワードを使用してログインします。



2. デバイス名をクリックします。



3. [概要] タブで、電話番号の横の [編集] をクリックします。



4. 新しい番号を入力し、[保存] をクリックします。



アプリケーションのアンインストール

セキュアエニウェア モバイルをデバイスからアンインストールする手順は次のとおりです。

1. セキュアエニウェア モバイルのメイン パネルで、モバイル デバイスのメニューボタンを押します。
2. [設定] パネルで、[アンインストール] をタップします。
3. 表示されたら、ウェブルート パスワードを入力し、[OK] をタップして続行します。
4. 確認パネルで、[OK] をタップしてデバイスからセキュアエニウェアを削除します。


注意：アンインストールで問題が発生した場合、ウェブルート サポートにご連絡いただくか、forums.webroot.com からフォーラム モデレータ（フォーラムは英語のみの提供となっておりますのでご了承ください。）にお問い合わせください。

デバイス管理者の設定がされている場合にはアンインストールを実行することができません。デバイス管理者の設定を外してからアンインストールを実行するようにしてください。

セキュアウェブの使用

セキュアウェブを使用すると、Web サイトにアクセスする前のロード時点で悪意のある Web サイトをブロックするため、安全にサイトを閲覧することができます。

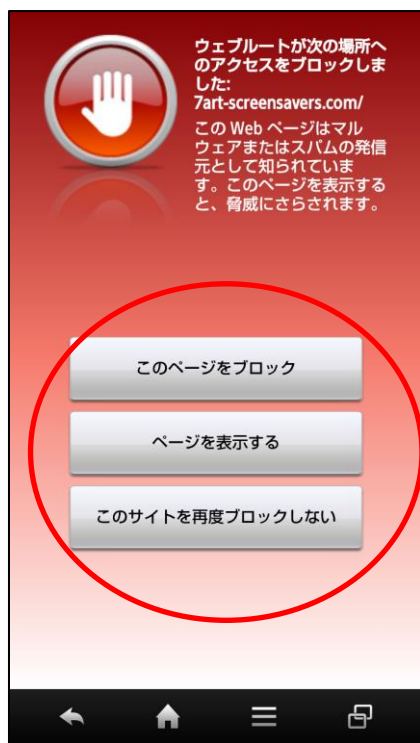
セキュアウェブを使用する手順は次のとおりです。

1. [ホーム] パネルで、セキュアウェブ アイコンをタップします。  をタップします。セキュア ブラウズが有効になったウェブルート ブラウザが開きます。



2. このブラウザを使用して Web サイトを閲覧すると、マルウェアやフィッシングの危険から自動的に保護されます。
マルウェアの拡大やフィッシングサイトであることが知られている Web サイトにア

アクセスしようとする、アラートが表示され、次のオプションが示されます:




- このサイトへ進む: 警告を無視してそのサイトに進みます。
- このサイトをブロック: このサイトを開きません。悪意の可能性があるとして分類されるサイトにはアクセスしないことをお勧めします。
- このサイトを再度ブロックしない: サイト接続を続行し次から確認しません。

パスワード管理の使用

セキュアウェブを使用すると、パスワードで管理されたサイトを表示して開いたり、個人データをウェブサイトのフォームに自動的に入力したり、自動入力機能を使用してログインページに認証情報を入力できます。

注意: お使いの Android デバイスでパスワード管理を使用するには、まずパスワードで管理されているサイトを定義する必要があります。詳細については、「my.webrootanywhere.com」でウェブルート セキュアエニウェア アカウントにログインしてください。

パスワード管理を使用する手順は次のとおりです。

1. お使いのデバイスにある [ホーム] パネルで、セキュアウェブのアイコンをタップします。  をタップします。
セキュア ブラウズが有効になったウェブルート ブラウザが開きます。
2. ブラウザを使用してパスワードで管理されている Web サイトを開きます。


3. Android デバイスのメニューボタンをタップします。
次のオプションが表示されます。



- **自動入力。** 自動入力がプリセットされていないサイトのログイン ページに認証情報の入力を行います。[自動入力] をタップすると、パスワードで管理されているサイト名が表示されます。サイト名をタップしてフィールドにログイン認証情報を入力します。1 つのウェブサイト異なる 2 つのログインを定義している場合 (例えば、あなたと配偶者が銀行のサイトを共有しているが、それぞれの預金口座に別のログインを使用している場合等)、[自動入力] をタップして異なるサイトの定義を表示し、次に希望のサイト名をタップしてログインします。
- **入力フォーム。** あらかじめ定義されている入力プロファイルが表示されます。[入力フォーム] をタップし、入力プロファイルを選択し、個人データをウェブ サイトのフィールドに入力します。
- **サイト。** パスワードで管理されているすべてのサイトを表示します。サイトの 1 つにアクセスするには、サイト名をタップします。(そのサイトに "自動ログイン" を指定している場合、自動的にログインします。) [サイトの詳細を表示] が表示されるまでサイト名を押したままにするとそのサイトのログイン認証情報が表示できます。[サイトの詳細を表示] をタップしてログイン認証情報とサイトの定義についての他の情報を表示するパネルを確認します。
- **詳細。** [サイトの更新] および [ヘルプ] に移動します。パスワードで管理されたサイトを PC から最近変更した場合、[サイトの更新] をタップしてモバイル デバイスに変更をダウンロードします。

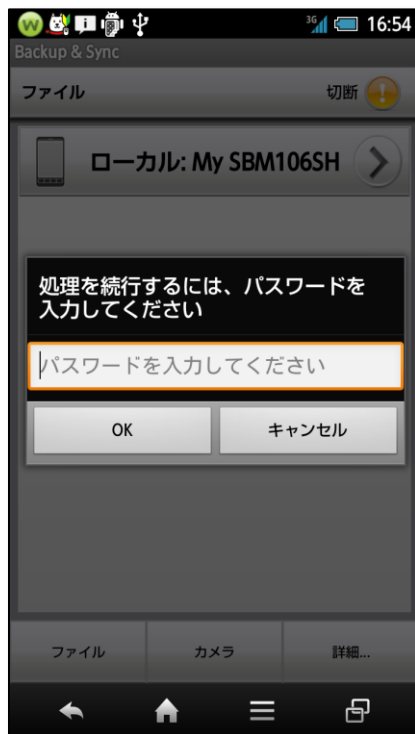
セキュアシンクの概要

セキュアシンクのご利用方法:

1. お使いのモバイル デバイスにアプリケーションをダウンロードしたら、[ホーム] パネルのセキュアシンク アイコンを見つけます。 . セキュアシンクのアイコンをタップします。



2. ウェブルート セキュアエニウェア コンプリートで登録したアカウントのユーザー名（メールアドレス）、パスワード、およびキーコードを入力します。インストール時に既に入力が完了している場合にはパスワードのみ確認されます。



3. セキュアシンクの中央パネルに同期されたデバイスとフォルダが表示されます。下部のタブバーを使用して、以下のタスクを切り替えることができます。



- [ファイル] では、Anywhere フォルダとバックアップ、モバイルデバイスのファイル、およびウェブルート アカウントの他のデバイスの同期されたファイルにアクセスできます。Anywhere フォルダは、お使いのコンピュータ内のすべてのファイルをオンライン アカウントと自動的に同期するフォルダです。バックアップフォルダや各デバイスの名称がついたフォルダは、オンラインのファイル格納場所です。
- [写真] では、ウェブルート アカウントにアップロードされた写真やアルバムにアクセスできます。ここから、写真の表示、共有を行うことができます。
- [カメラ] では、写真やビデオを撮影し、それらのファイルをオンライン アカウントに自動的にアップロードできます。ファイルは Anywhere フォルダ/モバイル フォルダ/マイ(デバイス名)/メディア ファイルにアップロードされます。
- [詳細...] は、アップロードまたはダウンロードの転送ステータスを表示する、セキュアシンクからログアウトする、ウェブルート サーバーに再接続する、ヘルプファイルを表示するための追加オプションを提供します。

同期されたファイルを他のデバイスで見る

セキュアシンクを使用して、他のデバイスやオンラインのウェブルート アカウントに保存されている同期ファイルにアクセスできます。

ファイルを表示する手順は次のとおりです。

1. タブ バーで [ファイル] をタップします。
ローカルのデバイスフォルダが先頭に表示され、Anywhere フォルダと各デバイスのオンラインフォルダ、バックアップフォルダが [リモートコンテナ] の下に表示されます。
2. アクセスしたいデバイスや同期フォルダの名前をタップします。
次のパネルに、同期されたフォルダやファイルが表示されます。
3. フォルダ内のファイルを表示するには、フォルダ名をタップします。
単一のファイルを表示するには、メニューパネルが開くまでファイル名を押したままにして [開く] をタップします。
注意:お使いのモバイル デバイスはそのファイル形式を表示できる必要があります。
必要に応じて、表示または編集用のアプリケーションをダウンロードしてください。
4. モバイル デバイスがオフラインのときにファイルを表示する場合は、「**自分のモバイル デバイスにファイルをダウンロードする**」を参照してください。

自分のモバイル デバイスにファイルをダウンロードする

セキュアシンクを使用して、オンライン アカウントからモバイル デバイスにファイルや写真をダウンロードできます。この機能は、モバイル デバイスがオフラインになっているときに同期されたファイルにアクセスしたい場合に便利です。

ファイルをダウンロードする手順は次のとおりです。

1. タブ バーで [ファイル] をタップします。
2. アクセスしたい同期フォルダの名前をタップします。
次のパネルに、アカウントの同期されたフォルダとファイルが表示されます。
3. フォルダまたはファイル名を押したままにし、メニューパネルが開くまで待ち、[ダウンロード] をタップします。
4. 転送の状態を調べるには、タブ バーの [詳細] をタップし、[転送状態] をタップします。

写真やビデオをアップロードする

セキュアシンク アプリケーションを使用して写真を撮り、写真ファイルをすぐにウェブルートアカウントのコンピュータにアップロードできます。また、モバイル デバイスのギャラリーからファイルをアップロードすることもできます。(デバイスのカメラで撮影された写真はウェブルート アカウントに自動的にアップロードされません。ギャラリーからアップロードする必要があります。)

写真を撮ってただちに同期する手順は次のとおりです。

1. タブ バーで、[カメラ] をタップします。
2. [写真を撮る] または [ビデオを録画する] のどちらかをタップします。
ファイルはただちにコンピュータの Anywhere フォルダ/モバイル フォルダに同期されます。

モバイル デバイスのギャラリーから写真をアップロードする手順は次のとおりです。

1. タブ バーで、[カメラ] をタップします。
2. [現在のメディアをアップロードする] をタップします。
セキュアシンクはギャラリーで JPG ファイルを探してアップロードを開始するよう表示します。
3. [OK] をタップします。
ファイルはただちにコンピュータの Anywhere フォルダ/モバイル フォルダに同期されます。

自分のオンライン アカウントにファイルをアップロードする

セキュアシンクを使用して、モバイル デバイスからオンライン ウェブルート アカウントにファイルをアップロードできます。

ファイルをアップロードする手順は次のとおりです。

1. タブ バーの [ファイル] をタップします。
2. お使いのモバイル デバイスの名前「ローカル：～」をタップします。
3. アクセスしたいフォルダの名前をタップします。
次のパネルに、そのデバイス上のフォルダとファイルが表示されます。
4. フォルダまたはファイル名を押したままにし、メニューパネルが開くまで待ち、[サーバーへアップロード] をタップします。
5. 転送の状態を調べるには、タブ バーの [詳細] をタップし、[転送状態] をタップします。
ファイルはただちにコンピュータの Anywhere フォルダ/モバイル フォルダに同期されます。

ファイルや写真を削除する

セキュアシンクから、同期されたフォルダ内のファイルや写真の削除を行うことができます。これらのフォルダに対する変更は、他のデバイスにも反映されることに注意してください。例えば、マジック ブリーフケースからファイルを削除すると、そのファイルはセキュアエニウェア アカウントすべてのデバイスから削除されます。

ファイルや写真を削除する手順は次のとおりです。

1. タブ バーで [ファイル] をタップします。
ローカルのデバイスが先頭に表示され、Anywhere フォルダと各デバイスのオンラインフォルダ、バックアップフォルダが [リモートコンテナ] の下に表示されます。
2. アクセスしたいデバイスや同期フォルダの名前をタップします。
次のパネルに、同期されたフォルダやファイルが表示されます。

3. フォルダ内のファイルにアクセスするには、フォルダ名をタップします。
単一のファイルにアクセスするには、メニューパネルが開くまでファイル名を押したままにして [削除] をタップします。