



WEBROOT®

by **opentext**™

Android向けモバイルセキュリティ
ユーザーガイド

Copyright

Copyright 2023年 Webroot.無断転載禁止。

Android向けモバイルセキュリティユーザーガイド

この文書に記載されている情報は予告なく変更されることがあります。この文書で説明されているソフトウェアは、使用許諾契約または秘密保持契約に基づいて提供されています。このソフトウェアの使用または複製は、これらの契約の条件に従って行うものとします。複写や記録を含む、電子的または機械的ないかなる形態や手段によっても、書面によるWebrootの許可なく、購買者の個人的な使用以外の目的で、本書のいかなる部分についても、複製、検索システムへの保存、または転送を行うことはできません。

目次

通知	<i>ii</i>
Android向けモバイルセキュリティ	<i>iii</i>
セキュアブラウザの使用	<i>vi</i>
Webroot for Chromeの有効化	<i>viii</i>
LastPassによるパスワード管理	<i>ix</i>
アクティビティレポートの表示	<i>xi</i>
Android向けモバイルセキュリティによる脅威の管理	<i>xiii</i>
テクニカルサポート	<i>xiv</i>

通知

Android向けモバイルセキュリティユーザーガイド改訂 Tuesday, August 8, 2023

この文書に記載されている情報は、次の製品に関するものです。

- WebrootのAndroid向けモバイルセキュリティ

この製品には1件以上の特許が使用されている場合があります。詳しくは、<https://www.opentext.com/patents>を参照してください。

この文書に記載されている情報は予告なく変更されることがあります。この文書で説明されているソフトウェアは、使用許諾契約または秘密保持契約に基づいて提供されています。このソフトウェアの使用または複製は、これらの契約の条件に従って行うものとします。複製や記録を含む、電子的または機械的ないかなる形態や手段によっても、書面によるWebrootの許可なく、購買者の個人的な使用以外の目的で、本書のいかなる部分についても、複製、検索システムへの保存、または転送を行うことはできません。

© 2004年-2023年 Webroot.無断転載禁止。

Android向けモバイルセキュリティ

WebrootのAndroid向けモバイルセキュリティは、WebrootがWindowsおよびMacのコンピューターを保護するのと同様に、ウイルス、スパイウェア、その他のオンライン脅威に対する保護機能を提供します。Webroot Mobile Securityをインストールすると、デバイスのスキャンが実行され、脅威が軽減されます。オンラインでのお買い物や銀行手続きを行う際には、Webrootがフィッシングサイト、スパムサイト、マルウェアサイトなどの危険なサイトをブロックし、個人情報とデータを保護します。

Webroot Mobile Securityのライセンスは、アップグレードや機種変更の際に移行することができます。

Androidデバイスへのモバイルセキュリティのインストール

システム要件はこちらでご確認ください: <https://www.webroot.com/us/en/support/system-requirements>

有効なインターネット接続が必要です。

1. Google Playストアから、Webroot Mobile Securityアプリをダウンロードしてインストールします。
2. Webrootアプリのアイコンをタップして、アプリを起動したら「利用開始」をタップします。
3. 以前にアプリを使用していたなど、既にログイン情報をお持ちの場合は、**[ログイン]**をタップして既存の認証情報を使用します。
4. 新規ユーザーである場合は、**[アカウントの作成]**で、製品キーコードを入力します。
 - キーコードは、オンライン購入時に送信された領収書の電子メール、または店頭購入のカードに記載されている、**WSAM-ZZZZ-0000-YYYY-1111**のような形式の番号です。
 - キーコードがない場合は、**[体験版はこちら]**をタップして、14日間の体験期間用のアカウントを作成します。
5. ユーザー名として使用する電子メールアドレスまたは電話番号を入力します。
6. 表示される強力なパスワードのガイドラインに従って、パスワードを作成します。

7. Webrootによる個人データの処理方法を確認するには、[プライバシーポリシー]をタップします。
8. [アカウントの作成]をタップします。[Webrootのサブスクリプション規約]画面が表示されます。
9. [ソリューション契約]をタップして規約を確認し、[同意]をタップして続行します。
10. 「Webrootへようこそ」画面が表示されたら、[今すぐスキャン]をタップします。
11. プロンプトが表示されたら、[許可する]をタップして、アプリを正しく機能させるために必要な権限を付与します。
12. Android OS 11以降の場合は、[すべてのファイルへのアクセス]画面で、[全ファイルの管理権を付与]スイッチを有効にします。

インストールが完了すると、ただちにWebrootによるデバイスの初回スキャンが実行されます。

アプリのスキャンは継続的に行われますが、[今すぐスキャン]をタップすればいつでも手動スキャンを開始できます。

スキャンが完了すると、以下のいずれかのステータスが表示されます。

- **安全:** お使いのスマートフォンは保護されている状態です。
- **要対応:** セキュリティリスクが存在することを意味します。この場合は、対策を講じてリスクを管理することができます。

Webrootによってデバイスが安全だと判断されると、**Webroot Mobile Security**のダッシュボードが表示されます。

- 手動スキャンを実行するには、[今すぐスキャン]をタップします。
- **セキュアブラウザ**を使用すると、Webrootのセキュリティ保護されたブラウザでウェブを安全に閲覧できます。
- **Webroot for Chrome**をアクティブ化すると、Google Chromeブラウザの使用時に脅威を監視することができます。

- パスワードマネージャーでは、付属のサードパーティ製ソフトウェアを使用して強力なパスワードを作成し、管理できます。パスワードマネージャーはWebrootインターネットセキュリティプラス以上のサブスクリプションでご利用いただけます。
- アクティビティレポートには、過去30日間に検出、ブロック、削除された脅威およびマルウェアの概要が表示されます。

セキュアブラウザの使用

Webroot Mobile Securityのダッシュボードで[セキュアブラウザ]をタップして、Webrootモバイルセキュアブラウザを開きます。このブラウザは、他のあらゆるウェブブラウザと同様の機能を備えているほか、Android向けモバイルセキュリティによって安全性とセキュリティ機能が強化されています。

[設定]ボタン(:)をタップすると、セキュアブラウザの各種オプションを設定できます。

- **進む:** [戻る]を選択する前、最後に表示していたウェブページを開きます。
- **お気に入り:** 現在開いているウェブページをブックマークに保存します。
- **ダウンロード:** 現在開いているウェブページのコピーを保存し、オフラインで表示できるようにします。
- **情報:** 現在開いているウェブページのセキュリティに関する情報を確認できるほか、**サイト設定**も構成できます。
- **更新:** 現在表示しているウェブページを更新します。
- **新しいタブ:** ブラウザで新規のタブを開きます。
- **新しいシークレットタブ:** ブラウザで新規のシークレットタブを開きます。閲覧履歴、クッキー、サイト情報のほか、ウェブ上のフォームやシークレットタブに入力された情報は、Android向けモバイルセキュリティに保存されません。
- **ブックマーク:** お気に入りサイトの一覧が表示されます。
- **最近使ったタブ:** 最近閉じたすべてのウェブページの一覧が表示されます。
- **履歴:** Android向けモバイルセキュリティのブラウザの閲覧履歴が表示されます。閲覧履歴はこの画面から消去できます。
- **ダウンロード:** ダウンロードしたファイルやページにアクセスできます。

- **共有**: 読み込んだページを他の人と共有できます。
- **ページ内を検索**: 読み込んだページ上のテキストを検索できます。
- **設定**: Android向けモバイルセキュリティのすべての設定を開くことができます。
- **サポート**: Android向けモバイルセキュリティのヘルプを受けるためのリンクを表示します。
- **セキュアブラウザを終了**: ブラウザを閉じてダッシュボードに戻ります。

Webroot for Chromeの有効化

Webroot for Chromeはデフォルトでは無効になっており、赤い[X]アイコンが表示されています。

Webroot for Chromeを有効化するには:

1. ダッシュボードの画面で、**[Webroot for Chrome]**をタップします。
2. **[Google Chromeのセキュリティ]**スイッチを有効にします。
3. 表示される通知を開き、**[はい]**をタップします。
4. **[設定を開く]**をタップします。
5. 表示される**[ユーザ補助]**画面で、**[ダウンロードしたアプリ] > [Webroot]**に移動します。
6. **[許可]**をタップします。
7. 「Webrootの使用」スイッチを**有効**にします。
8. **[戻る]**ボタンを繰り返しタップして、ダッシュボードの画面に戻ります。

LastPassによるパスワード管理

LastPassでは、強力なパスワードを作成し、Carbonite/Webrootのマイアカウントポータルを利用して、暗号化されたデータ保管庫に保存することができます。LastPassアカウントを作成して認証情報を保存すると、お気に入りのウェブサイト自動的にログインしたり、ウェブフォームにデータを自動入力したりできるようになります。そのため、認証情報や個人情報、クレジットカード番号などを手動で入力する手間を省くことができます。

LastPassパスワードマネージャーはWebroot Mobile Securityのサブスクリプションに含まれており、インターネットセキュリティプラス以上のライセンスでのみご利用いただけます。ご利用のサブスクリプションにパスワードマネージャーが含まれていない場合は、Webrootサポートまたは管理者までお問い合わせのうえ、サブスクリプションのアップグレードをご検討ください。

LastPassの利用を開始するには:

1. Webroot Mobile Securityのダッシュボードで、**[パスワードマネージャー]**をタップします。
2. 新規ユーザーであり、まだ**[マイアカウント]**のアカウントを作成していない場合:
 - a. **[キーコードを取得]**をタップして、使用可能なキーコードをコピーします。
 - b. **[マイアカウントポータルに移動]**をタップします。表示されるブラウザタブで、コピーしたキーコードを含む必要な情報を入力します。
3. 既存のマイアカウントユーザーだが、LastPassアカウントを持っていない場合:
 - a. **[マイアカウントポータルに移動]**をタップします。
 - b. **[マイアカウント]**ページに表示される手順に従ってログインします。
 - c. ナビゲーションペインの**[ダウンロード]**タブに移動します。
 - d. **[LastPassパスワードマネージャー]**までスクロールダウンして、**[アクティブ化]**をクリックします。
 - e. 手順に従ってLastPassアカウントにサインアップします。

4. LastPassアカウントをお持ちの場合:
 - a. **[LastPass アプリを開く]** をタップします。Google Playストアでアプリが開きます。
 - b. **[インストール]** をタップします。インストールが完了したら、LastPassパスワードマネージャーのアプリを開いてログインします。

LastPassの詳細については、「[LastPass Reference Guide](#)」を参照してください。

アクティビティレポートの表示

アクティビティレポートでは、デバイスがWebroot Mobile Securityによってどのようにマルウェアの脅威や悪質なウェブサイトから守られているかを確認できます。過去30日間のデバイスのアクティビティを確認し、検出された脅威を解決することができます。

アクティビティレポートはWebroot Mobile Securityのサブスクリプションに含まれており、インターネットセキュリティコンプライート以上のライセンスでのみご利用いただけます。ご利用のサブスクリプションにアクティビティレポートが含まれていない場合は、Webrootサポートまたは管理者までお問い合わせの上、サブスクリプションのアップグレードをご検討ください。


Webroot Mobile Securityのダッシュボードで、**[アクティビティレポート]**をタップすると、過去30日間にWebroot Mobile Securityによって検出されたすべてのマルウェアとウェブサイトの脅威の概要が表示されます。マルウェアの脅威については、スキャンされたアプリの総数と検出された新たな脅威の数に加え、解決された脅威、無視された脅威、およびレビュー中の脅威が表示されます。ウェブサイトの脅威については、閲覧されたウェブサイトの総数と検出された新たな脅威の数のほか、ブロックされたウェブサイト、却下されたウェブサイト、およびレビュー中のウェブサイトが表示されます。

マルウェアの脅威を表示するには:

1. アクティビティ概要レポートのページで、**[詳細表示]**ボタンをタップします。
2. アクティブな脅威のみを表示するには、**[アクティビティ詳細]**ページで、**[アクティブな脅威のみを表示する]**スイッチを有効にします。
3. 一覧の中で**[保留中]**または**[レビュー中]**の脅威の横にある3つの点のアイコン(⋮)をタップして、3つのアクションのうちいずれかを選択します。
 - **削除:** アプリをデバイスからアンインストールして、マルウェアによるデバイスへの攻撃を防ぎます。
 - **レビューをリクエスト:** Webrootの脅威専門家に、アプリをレビューして検証するようリクエストを送信します。その間、脅威を削除してお使いのデバイスを安全に保つことをお勧めします。
 - **無視 (推奨されません):** マルウェアの脅威を無視し、アプリを許可リストに追加します。

Webroot Mobile Securityによって脅威として確認されたウェブサイト信頼する場合や、そのウェブサイトを一覧に表示する必要がなくなった場合は、[アクティビティ詳細]一覧からそのウェブサイトを削除します。

[アクティビティ詳細]リストからウェブサイトを削除するには:

1. アクティビティ概要レポートのページで、[詳細表示]ボタンをタップします。[アクティビティ詳細]ページの[ウェブサイトの脅威]タブが表示されます。
2. 以前却下した脅威のみを表示するには、[却下されたサイトのみを表示する]スイッチを有効にします。
3. 一覧の中で、対象ウェブサイトの横にある[削除]ボタン()をタップします。[確認]をタップすると、対象のウェブサイトが[アクティビティ詳細]一覧から削除されます。ただしこれを行っても、そのウェブサイトが[アクティビティ詳細]一覧に表示されなくなるだけで、そのサイトの脅威ステータスは変更されません。

Android向けモバイルセキュリティによる脅威の管理

Webrootでデバイスのセキュリティに対する脅威が検出されるか、対応が必要な未処理のマルウェアが見つかったら、アプリのホーム画面に通知が表示されます。その場合はその通知をタップするか、またはダッシュボードで**[アクションを実行]**をタップして、以下のいずれかのオプションを選択します。

- **削除**: セキュリティ上のリスクを削除して、マルウェアによるデバイスへの攻撃を防ぐことができます。
- **レビューをリクエスト**: Webrootの脅威研究者に、サイトをレビューして検証するようリクエストを送信します。その間、脅威を削除してお使いのデバイスを安全に保つことをお勧めします。
- **無視 (推奨されません)**: アプリで検出された高リスクの脅威を無視し、アプリを許可リストに追加します。

Webrootは、リスクの高いウェブサイトを読み込む前に警告を表示します。警告ページでは以下のオプションを選択できます。

- **安全なページに戻る**: 最後に訪問したページ、または安全な空白のページに移動し、閲覧を継続できます。初めて訪問するウェブサイトの場合は、これが最も安全なオプションです。
- **レビューをリクエスト**: Webrootの脅威専門家に、サイトをレビューして検証するようリクエストを送信します。
- **ブロック解除 (推奨されません)**: ブロックを解除して、リスクの高いウェブサイトを開きます。サイトのブロック解除は、そのサイトをよく知っているか、個人情報やセキュリティに対する脅威がないと確認済みである場合のみ行うようにしてください。

テクニカルサポート

Webrootではさまざまなサポートオプションを提供しています。次のいずれかの方法を選択します。

- [Best Buy \(米国のみ\) を介してWebrootのサブスクリプションを登録された場合は、ここをクリックして他のサポートオプションをご確認ください。](#)
 - [ヘルプのリクエストを送信する](#)
 - [オンライン文書で回答を探す](#)
 - [ナレッジベースおよびよくあるご質問で回答を探す](#)
 - [Webrootコミュニティに進む](#)
-