SOPHOS

Cybersecurity made simple.

Sophos Intercept X for Mobile

ヘルプ (Android)

製品バージョン: 9.6

目次

(2020/04/30)

1 アクセシビリティ

Sophos Intercept X for Mobile は、Web Content Accessibility Guidelines (WCAG) 2.1 レベル AA に準拠しています。このガイドラインの詳細については、関連情報を参照してください。

Sophos Intercept X for Mobile を、Android デバイスに搭載されている Google のスクリーンリーダーである TalkBack で使用することを推奨します。TalkBack を使用するためのリンクは、関連情報を参照してください。TalkBack についてご不明の点は、Google のテクニカルサポートにお問い合わせください。

支援技術製品をソフォスのソフトウェアでご使用になる場合は、対象となるソフォス製品の動作および使用可能なキーボードコマンドについてよく理解しておくことを推奨します。

既知の制限事項

Android OS の制限により、スクリーンリーダーのユーザーは、 Android 9 以降を使用している場合のみに見出しを使用して操作できます。

関連情報

Web Content Accessibility Guidelines
Android アクセシビリティヘルプ：Android で TalkBack を使ってみる

2 Sophos Intercept X for Mobile について

Sophos Intercept X for Mobile は、処理速度やバッテリーの持ちに影響を及ぼすことなく、Android デバイス上のデータを保護し、プライバシー情報を守ります。アプリのインストール時には、SophosLabs が提供する最新の解析情報をリアルタイムで利用して自動スキャンを実行し、データ流出や想定外の課金を防止します。

3 ダッシュボード

Sophos Intercept X for Mobile のダッシュボードには、デバイスの状態の概要が表示されます。

各機能の色は、そのステータスによって異なります。

- 緑: 問題は検出されませんでした
- 赤: 問題が検出されました
- 青: 機能がオンになっています
- グレー: 機能がオフになっているか、設定されていません

4 デバイスセキュリティ

他の OS と同様、Android でもセキュリティレベルの低下につながる設定を行うことができます。Sophos Intercept X for Mobile は、このようなセキュリティに関連する設定を確認し、デバイスのセキュリティを強化するための推奨事項を提供します。

注
Sophos Intercept X for Mobile が Sophos Mobile の管理下にある場合、セキュリティに関連するシステム設定は、組織の管理者によって設定されます。

「**デバイスセキュリティ**」の下に表示される設定の色は、そのステータスによって異なります。

- 緑 (安全): デバイスのセキュリティを最大限に確保する設定内容です。
- 赤 (安全ではない): セキュリティ上の問題につながる可能性のある設定内容です。推奨事項に従って変更してください。
- 黄色 (不明): Android デバイスの設定は、デバイスの機種と Android のバージョンによって異なります。設定が安全かどうかを Sophos Intercept X for Mobile が判断できない場合は、黄色で表示されます。変更することを考慮してください。
- グレー (オフ): チェックはオフになっています。設定は、デバイスのセキュリティ状態を判断する際に考慮されません。

設定をタップすると、それを変更したり、デバイスのセキュリティに与える影響の詳細を確認したりできます。

4.1 アップデートアドバイザー

「アップデートアドバイザー」は、使用している Android バージョンに関する情報を表示し、より新しいバージョンがあるかを確認します。

アップデートアドバイザーは、ソフォス製品から収集したデータを基に、ユーザーのデバイスで使用できる、より新しいバージョンの Android があるかを確認します。

アップデートアドバイザーを開くには、「**デバイスセキュリティ**」ページで、「**最新の Android バージョン**」を選択します。

アップデートを自動インストールすることを推奨します。デバイスにこれを設定するオプションがある場合は、「**設定内容を確認する**」をタップして、デバイスの「**設定**」アプリで自動更新をオンにします。

5 Web フィルタリング

「Web フィルタリング」は、カテゴリに基づいて、Web サイトへのアクセスを制御する機能です。悪意のあるコンテンツや不適切/違法なコンテンツを掲載する Web サイトの閲覧を防止できます。

Web フィルタリングの設定

Wi-Fi フィルタリングは、ダッシュボードの「**ネットワークセキュリティ**」にあります。

- 「**Web フィルタリング**」ページで、Web フィルタリングをオンにします。
- 悪質な Web サイトのフィルタリングを有効にするには、「**悪意のあるコンテンツ**」をタップして、「**警告**」または「**ブロック**」を選択してください。
- 特定のカテゴリに属する Web サイトのフィルタリングを有効にするには、対象のカテゴリをタップして「**警告**」または「**ブロック**」を選択します。
- **許可リスト:** 特定の悪意のあるページや、指定されたカテゴリに属するページに関する警告を、常に表示しないようにすることもできます。この機能は、よく閲覧するページが警告やブロックの対象となっているカテゴリに属する場合に便利です。「**Web フィルタリング**」の警告ダイアログで「**常にこのページへのアクセスを許可する**」を選択します。許可したページが再度フィルタリングされるように設定するには、「**許可するページのリストを消去する**」をタップします。

ヒント
ソフォスは、Web フィルタリング機能をテストいただけるよう、各サイトカテゴリのテスト用リンクをまとめた Web サイト「sophostest.com」をご用意しました。一部のリンクは、不快あるいは危険なページとして分類されますが、リンク先のコンテンツ自体はすべて無害なものです。

対応している Web ブラウザ

Web フィルタリングは、「**保護されているブラウザ**」にあるアプリのいずれかを使用する場合、保護を提供します。

対応ブラウザは次のとおりです。

- Google Chrome
- Firefox
- Android の Web ブラウザ
- Microsoft Edge

「**保護されているブラウザ (未検証)**」には、検証されていないが、動作すると思われるアプリが表示されます。

ヒント
サポートされている Web ブラウザがデバイスにインストールされているにもかかわらず、「**保護されているブラウザ**」の下に表示されない場合は、システム設定の「**ユーザー補助**」で、Sophos Accessibility Service がオンになっていることを確認してください。

6 リンクチェッカー

「リンクチェッカー」は、悪意のあるコンテンツや不適切なコンテンツについて、メールやドキュメント内の URL をチェックする機能です。

リンクチェッカーは、ブラウザ以外のアプリでタップされたリンクをすべてチェックします。Web ページのリンクは、Web フィルタリングでチェックされます。詳細は、Web フィルタリング (p. 5)を参照してください。

リンクチェッカーは、ダッシュボードの「**ネットワークセキュリティ**」にあります。

リンクチェッカーを設定する方法は次のとおりです。

1. 「**リンクチェッカー**」ページで、リンクチェッカーをオンにします。
2. Web リンクを開くアプリとして、通常使用しているブラウザアプリを選択します。
3. リンクチェッカーをオンにした後、最初にリンクをタップすると、リンクを開くアプリを選択するよう Android のメッセージが表示されます。「**Sophos Link Checker**」を選択します。

リンクをタップすると、リンクチェッカーに情報が渡され、SophosLabs が分類するカテゴリに基づいて悪意のあるコンテンツや不適切なコンテンツに関する URL チェックが行われます。チェック後、ブラウザにリンク先が表示されます。

注
ブラウザアプリを起動せずアプリ内で開いた Web サイトのリンクは、リンクチェッカーでチェックされません。リンクの開き方を選択できる場合は、ブラウザを使用するように設定し、リンクチェッカーでリンクが処理されるようにします。

たとえば、Gmail の場合、この設定は「**Gmail でウェブリンクを開く**」で変更できます。この設定をオフにすると、リンクチェッカーでメール内のリンクがチェックされるようになります。

7 Wi-Fi セキュリティ

「Wi-Fi セキュリティ」では、Wi-Fi 接続をチェックし、ネットワークベースの脅威を検出することができます。

注
Sophos Intercept X for Mobile が Sophos Mobile に登録されている場合、この機能は組織によって管理されます。

Wi-Fi セキュリティは、ダッシュボードの「**ネットワークセキュリティ**」にあります。

検出される問題

Sophos Intercept X for Mobile で検出される問題は次のとおりです。

ARP スプーフィング	ARP スプーフィングは、攻撃者が不正な ARP (Address Resolution Protocol) メッセージをユーザーのコンピュータに送信することで、攻撃者の MAC アドレスがユーザーのネットワークゲートウェイの IP アドレスに関連付けられているように見せかける攻撃手法です。これにより、プライベートネットワークへのアクセスや機密データの窃取が可能になるほか、サービス拒否攻撃や中間者攻撃対策など、別の攻撃を起動することもできるようになります。
キャプティブポータル	キャプティブポータルは、公衆無線 LAN に接続する際、ネットワークへのアクセスを許可する前にユーザー認証を要求する仕組みです。すべてのトラフィックがキャプティブポータルにリダイレクトされるため、追加で警告が送信される場合があります。
コンテンツ改ざん	コンテンツ改ざんは、攻撃者が Web サイトのコンテンツを改ざんすることで、ユーザーに悪影響のある操作をさせようとする手法です。これにより、認証のバイパスやデータの削除などができるようになります。
SSL インターセプト	SSL インターセプトは、攻撃者が偽のサーバー証明書を使用することで、ユーザーのコンピュータと Web サイトとの間の暗号化された通信内容をインターセプトする手法です。攻撃者は、セキュア通信をしているように見せかけ、機密データを復号化することができます。
SSL ストリップ	SSL ストリップは、Web サイトへの接続を、セキュアな HTTPS から暗号化されていない HTTP にダウングレードさせる攻撃手法です。攻撃者は、ユーザーのコンピュータと Web サイトの間に流れるすべてのトラフィックを、攻撃者のプロキシサーバーを介してリダイレクトできます。これにより、HTTPS 通信をしているように見せか

け、機密データを復号化することが可能となります。

チェックの実行

- 接続中の Wi-Fi ネットワークをチェックするには、「**Wi-Fi のチェック**」をタップします。
- バックグラウンドで自動的にネットワークのチェックを実行するには、「**バックグラウンドチェック**」をオンにします。デバイスが Wi-Fi ネットワークに接続するたびにチェックが実行されるようになります。

8 アプリセキュリティ

デバイスに悪意のあるアプリやファイルがないかどうかを検索できます。

Sophos Intercept X for Mobile はデバイスのマルウェア検索を実行し、悪質なアプリや業務上不要と思われるアプリを報告します。オンライン、オフラインを問わず、ビルトインの全機能型検索エンジンで詳細なスキャンを実行するほか、クラウド上の SophosLabs のデータベースが保有する最新の脅威データを照会してアプリのチェックを行います。この脅威データは、SophosLabs (Android を狙う脅威を 24時間体制で解析) によって絶えず更新されます。

スキャンの実行

インストールされると、Sophos Intercept X for Mobile は自動的にアプリを検索します。また、スケジュール検索を設定したり、手動検索を実行したりすることもできます。

スケジュール検索を設定する方法は次のとおりです。

アプリ設定で「**スケジュール検索**」を選択し、「**スケジュール検索の頻度**」で検索の頻度を選択します。また、デバイスのどの部分を検索し、どの種類のアプリを報告するかを設定することもできます。

手動検索を実行する方法は次のとおりです。

「**アプリセキュリティ**」ページで、「**スキャンの詳細を表示**」、「**開始**」の順に選択します。

スキャン結果の表示

「**アプリセキュリティ**」ページの「**アプリのセキュリティ問題**」に、検索結果の概要が表示されます。

問題をそれぞれ表示するには、「**スキャンの詳細を表示**」を選択します。

問題の詳細を表示するには、「**脅威および不要と思われるアプリ**」で各アプリを選択し、該当する「**オブジェクトの詳細**」ページを開きます。そのページで、次の操作を行うことができます。

- アプリのインストール方法と、アプリが要求したパーミッションを表示します。
- 脅威の説明を表示します。
- 詳細な脅威情報が表示された Web ページをブラウザで開きます。
- アプリをアンインストールします。
- アプリを許可します。

関連資料

設定 (p. 23)

9 認証

「認証」では、ワンタイムパスワード (認証コードとも呼ばれます) を生成し、多要素認証でアカウントにサインインすることができます。

多要素認証の対応状況や、有効にする方法については、アカウント発行元に確認してください。

認証では、**タイムベース**または**カウンターベース**のワンタイムパスワードを使用できます。詳細は、ワンタイムパスワードについて (p. 10)を参照してください。

認証を起動するには、Sophos アイコンを長押しした後、「**認証**」をタップします。

機能:

- **タイムベース**のパスワードの場合、認証には、現在有効なワンタイムパスワードのほか、表示中のコードが無効になり、次のコードに切り替わるまでの残り時間がアイコンで表示されます。
- **カウンターベース**のパスワードの場合は、項目の右横の「「**更新**」 」をタップして、新しいワンタイムパスワードを生成します。誤操作によって、連続して複数のコードが生成されることを防ぐため、次のコードが生成されるまで、数秒の待機時間があります。
- アカウントのワンタイムパスワードをクリップボードにコピーするには、ワンタイムパスワードを長押しした後、「「**コピー**」」をタップします。
- アカウントの詳細を編集するには、該当する項目を長押しした後、「「**編集**」」をタップします。セキュリティ上の理由から、シークレット鍵を表示したり、編集したりすることはできません。
- アカウントを削除するには、アカウントを長押しした後、「「**削除**」」をタップします。

警告
認証の項目を削除すると、削除したアカウントのワンタイムパスワードを生成することができなくなります。この操作を行っても、多要素認証は無効化されません。認証の項目を削除すると、アカウントにサインインできなくなることがあります。

項目を削除する前に、別の方法でワンタイムパスワードを生成できること、または多要素認証を行わずに別の方法でアカウントにサインインできることを確認してください。

9.1 ワンタイムパスワードについて

ワンタイムパスワード (認証コードと呼ばれることもあります) は、数桁の数字から構成されます。次のようなパラメータを基に算出されます。

- アカウント発行元 (認証サーバー) とユーザーのみが知っている共有シークレット鍵。
- アカウント発行元固有の設定値。
- カウンター。

ワンタイムパスワードによる認証では、特定のカウンター値に基づき生成されるパスワードを認証サーバーに提示します。「認証」は、認証サーバーと同じルールを用いてカウンター値を決定するため、認証サーバーでワンタイムパスワードが許可されます。

認証では、**タイムベース**または**カウンターベース**のワンタイムパスワードを使用できます。カウンター値の算出方法は、それぞれの方式で異なります。

- **タイムベースのワンタイムパスワード** (TOTP、RFC 6238 に準拠): カウンターの数値は、一定の時間が経過すると更新されます。次回の検証コードは、一定の時間が経過すると生成されます。

- **カウンターベースのワンタイムパスワード** (HOTP、RFC 4226 に準拠): カウンターの数値は、オンデマンドで更新されます。次回の検証コードは、ユーザーが認証を要求すると生成されます。

9.2 QR コードからアカウントを追加

アカウントの多要素認証を有効化済みで、設定情報を含む QR コードをアカウント発行元から入手した場合は、ここで説明する方法を使用してください。

1. 「**+**」、「**QR コードの読み取り**」の順にタップします。
2. デバイスで QR コードを読み取ります。

QR コードから設定情報を読み込むと、アプリで新しい認証アカウントが作成されます。

9.3 アカウントを手動追加

アカウントの多要素認証が有効になっており、アカウント発行元から設定情報が提供されている場合は、ここで説明する手順を実行します。

1. 「**+**」、「**手動追加**」の順にタップします。
2. 「**名前**」フィールドに、認証用の新しいアカウント名を入力します。
3. 「**鍵**」フィールドに、アカウント発行元が指定したシークレット鍵を入力します。鍵はアカウントに特有のもので、ワンタイムパスワードの算出に使用されます。
4. 「**種類**」フィールドにアカウント発行元で指定されている算出方式を選択します。
5. アカウント発行元によって追加の設定内容が指定されている場合は、「**詳細設定**」をタップして追加の入力フィールドを表示します。

   注意
   アカウント発行元で指定されている情報のみを入力してください。

   - 「**発行者**」フィールドにアカウントの発行元を入力します。
   - 「**期間**」フィールドに有効期間を秒単位で入力します。タイムベースのワンタイムパスワードを選択した場合のみに表示されます。
   - 「**カウンター**」フィールドにカウンターの初期値を入力します。カウンターベースのワンタイムパスワードを選択した場合のみに表示されます。
   - 「**コードの文字数**」フィールドで、ワンタイムパスワードの数字の桁数を選択します。
   - 「**ハッシュアルゴリズム**」フィールドで、ワンタイムパスワードの算出に使用するハッシュアルゴリズムを選択します。
6. 任意: 「**背景色**」フィールドで、アカウントリストのエントリを見分けやすくするために、アカウントの表示色を選択します。
7. 設定が終わったら「「**OK**」 ✓」をタップします。

これで新しい認証アカウントが設定されます。

10 パスワードセーフ

「パスワードセーフ」は、すべてのアカウント情報を 1箇所に保存して、1つのマスターパスワードで保護する機能です。

パスワードセーフを起動するには、Sophos アイコンを長押しした後、「**パスワードセーフ**」をタップします。

次のオプションがあります。

- 新しいパスワードセーフのファイルを作成します。
- 既存の KeePass KDBX ファイルをインポートします。パスワードの項目を編集すると、ローカルコピーのみが変更されます。

「パスワードを自動入力」をオン

iOS 12 以降では、パスワードセーフで、パスワードを自動入力できます。

パスワードセーフに対して、「**パスワードを自動入力**」をオンにする方法は次のとおりです。

1. 「**設定**」アプリで、スクロールダウンして「**パスワードとアカウント**」を表示します。
2. 「**パスワードを自動入力**」をタップして、「**パスワードを自動入力**」をオンにします。
3. 「**入力を許可:**」で、「**Intercept X**」を選択します。

これで、認証情報を入力する際、キーボードの上部に表示される QuickType バーで「**パスワード**」をタップするだけで、パスワードセーフにアクセスできるようになります。

10.1 パスワードセーフのエントリの作成

パスワードセーフのファイルに、エントリやエントリのグループを追加する方法は以下のとおりです。

1. パスワードセーフで、「**+**」をタップします。
2. 作成するエントリのタイプを選択します。
   - **アカウントエントリの追加**: Web サイトのアカウントなどに適した、事前に設定したフィールドを含むエントリが作成されます。
   - **クレジットカードエントリの追加**: クレジットカードなどに適した、事前に設定したフィールドを含むエントリが作成されます。
   - **グループの追加**: エントリを整理するためのフォルダが、パスワードセーフ内に作成されます。
3. 各エントリのフィールドにデータを入力します。
4. 任意: 「**フィールドの追加**」をタップしてエントリにカスタムフィールドを追加します。

   カスタムフィールドに対して「**保護済み**」をオンにした場合は、フィールドの横にある目の形をしたアイコンをタップして値を表示する必要があります。なお、保護済みのフィールドは検索結果にも表示されません。
5. 「**ディスク**」アイコンをタップしてエントリを保存します。

パスワードデータを使用して、簡単に Web ページやアプリにサインインすることができます。詳細は、パスワードデータを使用したサインイン (p. 13)を参照してください。

10.2 パスワードの生成

1. パスワードセーフで、パスワードを生成するエントリを開きます。
2. 「「**編集**」 」をタップして、編集モードに切り替えます。
3. パスワードフィールドの横にある「**+**」をタップして、パスワード自動生成ダイアログを開きます。
4. パスワードの文字数と、指定が必要な文字の種類を定義します。
5. 「**パスワードの生成**」をタップして、条件に基づいたパスワードを生成します。
6. 生成されたパスワードに問題がない場合は、パスワード自動生成ダイアログを閉じます。生成された値でパスワードが更新されます。
7. エントリを保存します。

10.3 パスワードデータを使用したサインイン

- フィールドの値をクリップボードにコピーするには、該当するフィールドをタップします。
- 保護済みのフィールドの値を表示するには、フィールドの横にある「「**目**」 」アイコンをタップします。
- URL を Web ブラウザで開くには、URL をタップします。URL をクリップボードにコピーする場合は、URL を長押しします。

ヒント
パスワードセーフのエントリを開くたびに、Android の通知領域に通知が追加されます。その通知から、ユーザー名とパスワードをクリップボードにコピーできます。

10.4 パスワードセーフのエントリの管理

1. エントリを長押しして、モードを切り替えます。
2. 任意: 同じアクションを実行する他のエントリも選択します。
3. 該当するアイコンをタップして、次のようなアクションを実行します。
   - 「**編集**」 : エントリの内容を編集します。単一のエントリを選択している場合のみに表示されます。
   - 「**切り取り**」 : 選択したエントリを、パスワードセーフのファイルの別のグループに移動します。
   - 「**コピー**」 : 選択したエントリを、パスワードセーフのファイルの別のグループにコピーします。
   - 「**削除**」 : 選択したエントリを、特別な「**ごみ箱**」グループに移動します。エントリを完全に削除するには、「**ごみ箱**」グループのエントリに対して「「**削除**」 」を使用します。
   - 切り取ったエントリやコピーしたエントリを貼り付けるには、貼り付け先を参照して「「**クリップボード**」 」をタップします。

10.5 パスワードセーフのエントリの検索

パスワードセーフでは、エントリ名、グループ名、およびエントリのフィールドの値を検索できます。

注
パスワードフィールドや「**保護済み**」に設定したフィールドを検索することはできません。

1. パスワードセーフで、「「**検索**」 🔍」をタップして検索モードに切り替えます。
2. 検索文字列を入力します。結果の一覧は、入力のたびごとに更新されます。

10.6 パスワードセーフのバックアップ

パスワードセーフのファイルは、定期的にバックアップする必要があります。操作ミスやデバイスの紛失などにより、パスワードセーフのファイルがなくなってしまった場合、パスワード情報を復旧するのに最新のバックアップが必要となります。

1. パスワードセーフで、「「**詳細**」⋮」、「**エクスポート**」の順にタップします。
2. パスワードセーフのファイルをエクスポートするアプリを選択します。
   選択したアプリが起動し、パスワードセーフのファイルのコピーが表示されます。

注
バックアップコピーの保存先をメモし、安全な場所に保管することを推奨します。

11 QR コードスキャナ

「QR コードスキャナ」は、QR コードを読み取り、埋め込まれているコードを処理する機能です。

QR コードスキャナを起動するには、Sophos アイコンを長押しした後、「**QR コードスキャナ**」をタップします。

Web アドレス

QR コードを読み取ると、SophosLabs で設定されるカテゴリに基づいて、埋め込まれている URL のスキャンが実行されます。

- URL が安全であるというメッセージが表示されたら、「**開く**」をタップして、Web ブラウザで開きます。

連絡先

QR コードを読み取って、次の手順を実行します。

- 「**連絡先の追加**」をタップして、コードに含まれる名刺情報で連絡先の項目を作成します。
- 「**地図表示**」をタップして、コードに含まれる位置情報を地図アプリ (デフォルトは Google マップ) で表示します。
- 「**電話をかける**」をタップして、コードに含まれる番号に電話をかけます。QR コードに複数の電話番号が含まれている場合は、次の順番で使用されます。
  1. 携帯電話番号
  2. 勤務先の電話番号
  3. 自宅の電話番号
- 「**メールの送信**」をタップして、コードに含まれるアドレス宛てのメールを新規作成します。QR コードに複数のメールアドレスが含まれている場合は、すべてが「**宛先**」フィールドに追加されます。

Additional information
Sophos Intercept X for Mobile は、vCard 2.1 および 3.0 形式の電子名刺の情報を読み取ることができます。

Wi-Fi の設定

QR コードを読み取り、「**ネットワークに接続**」をタップして、QR コードで設定されている Wi-Fi ネットワークに接続します。

注
安全でないネットワーク (つまり、WPA や WPA2 で暗号化されていないネットワーク) に接続しようとすると、警告が表示されます。

12 アプリのロック

「アプリのロック」では、起動時に認証を要求するアプリの一覧を設定できます。特定のアプリを使用できないようにロックできるので、誰かにデバイスを貸す場合などに便利です。

注
Sophos Intercept X for Mobile が Sophos Mobile に登録されている場合は、アプリのロックは利用できません。アプリのアクセスは組織によって管理されます。

1. アプリメニューで、「**アプリのロック**」を選択します。
2. 「**基本設定**」でアプリのロックをオンにします。
3. Intercept X アプリを Android のデバイス管理者として設定する必要があります。まだ有効にしていない場合は、該当する Android の「**設定**」ページにリダイレクトされます。「**有効にする**」をタップします。
4. 「**アプリのロック**」の認証の種類を選択します。
   「**パターン**」、「**PIN**」、「**パスワード**」または「**指紋**」 (デバイスに指紋センサーがある場合) から選択できます。

   注
   Sophos Intercept X for Mobile が Sophos Mobile の管理下にある場合、管理者は指紋認証をオフにできます。

5. タスクマネージャの中には、プロセスを停止することで「**アプリのロック**」を無効にできるものもあります。タスクマネージャによる操作を防止するには、Sophos Security & Antivirus Guard アプリをインストールする必要があります。「**基本設定**」のメッセージにも同様の注意が表示されます。メッセージをタップして、アプリを Google Play で開き、インストールします。
6. 「**猶予期間**」をタップして、アプリを閉じた後、パスワードを記憶しておく時間を選択します。
7. 「**保護設定**」の下にアプリのロックをアンインストールまたは無効化できるアプリが一覧表示されます。また、Google Play や他のインストーラを保護してデバイスに無制限にアプリがインストールされることを防止することもできます。
8. 左にスワイプします。「**アプリの選択**」画面が表示されます。次の項目を実行できます。
   - 「**保護対象外**」リストのアプリを選択すると、アプリが保護の対象となります。アプリは「**保護対象**」リストに表示されます。
   - 「**保護対象**」リストに表示されているアプリのチェックを外すと、アプリの保護が解除されます。アプリは「**保護対象外**」リストに表示されます。

Sophos Mobile Security Guard は「**アプリのロック**」のプロセスを監視し、必要に応じて再起動を行います。

注
Sophos Mobile Security Guard をインストールしないまま「**アプリのロック**」の設定を終了すると、インストールを促すメッセージが表示されます。インストールすることを強く推奨します。

13 プライバシーアドバイザー

「プライバシーアドバイザー」には、デバイスにインストールされているアプリに許可されているパーミッションに関する情報が表示されます。

注
このセクションでは、Android 6 以降対応のプライバシーアドバイザーについて説明します。Android 5 対応のプライバシーアドバイザーについては、プライバシーアドバイザー (Android 5) (p. 19)を参照してください。

Android でのパーミッション処理

パーミッションは Android の最も重要なセキュリティ機能で、アプリに特定の権限を付与します。Android バージョン 6 では、アプリによるパーミッションの要求方法が変更されています。

- Android 6 以降では、**アプリの実行時** (つまり、アプリケーションの実行中に必要になった時点で) にパーミッションの許可が求められます。
- Android 5 以前を対象にしたアプリ (以降、「旧アプリ」とします) では、**アプリのインストール時**にすべての必要なパーミッションの許可が求められます。旧アプリを Android 6 以降にインストールした場合、パーミッションを個別に拒否することはできます。しかし、このような操作に対応できるよう設計されていないため、アプリが動作しなくなることがあります。

プライバシーアドバイザーに表示される内容

Google によって「Dangerous」(リスクが高い) と分類されるパーミッションは、ユーザーのプライバシーや他のアプリの操作への影響が大きいため、プライバシーアドバイザーに表示されます。

- 「**カレンダーのパーミッション**」 **カレンダー**
- 「**カメラのパーミッション**」 **カメラ**
- 「**連絡先のパーミッション**」 **連絡先**
- 「**位置情報のパーミッション**」 **位置情報**
- 「**マイクのパーミッション**」 **マイク**
- 「**電話/通話のパーミッション**」 **電話**
- 「**ボディセンサーのパーミッション**」 **ボディセンサー**
- 「**SMS のパーミッション**」 **SMS**
- 「**ストレージのパーミッション**」 **ストレージ**

次のいずれかのパーミッションの状態が表示されます。

- 「**許可**」 要求され許可した状態
- 「**拒否**」 要求され拒否した状態

注
古いバージョンのアプリのパーミッションは、アプリの設定でパーミッションをオフにした場合でも、「要求され許可した状態」と表示されます。

プライバシーアドバイザーで行える操作

- アプリが要求したすべてのパーミッションの詳細を表示する (リスクのないパーミッションも含む): アプリのアイコンをタップします。
- パーミッションを許可または拒否する: アプリのアイコン、「**パーミッションの変更**」の順にタップし、アプリの「**アプリ情報**」ページを開きます。開いたページで「**権限**」をタップします。
- パーミッションの変更履歴を表示する: タイトルバーで、「**パーミッションの変更履歴**」 をタップします。
- プライバシーアドバイザーに表示される項目を設定する: 「**フィルタ**」をタップします。システムアプリや旧アプリなど、特定のパーミッションや特定の種類のアプリを表示しないようにすることができます。
- アプリの表示順序を変更する: 「「**並び替え**」 」をタップし、並び替えの方法を選択します。

14 プライバシーアドバイザー (Android 5)

「プライバシーアドバイザー」には、デバイスにインストールされているアプリに許可されているパーミッションに関する情報が表示されます。

注
このセクションでは、Android 5 対応のプライバシーアドバイザーについて説明します。Android 6 以降対応のプライバシーアドバイザーについては、プライバシーアドバイザー (p. 17)を参照してください。

パーミッションのフィルタには以下の 3種類があります。

- **料金の発生するアプリ**

  アプリの中には追加料金が発生するものもあります。アプリが要求するパーミッションによっては、プレミアムレートの電話番号にダイヤルしたり、電話のネットワーク状態を変更したり(ローミングサービスを使用する場合に料金が発生する可能性があります)、あるいはユーザーの確認なしで SMS を送信したりすることが可能なものもあります。

- **プライバシー侵害の恐れがあるアプリ**

  スマートフォンやタブレットには個人情報が保存されています。特定のパーミッションが付与されているアプリは、連絡先リストを読み取ることができます。アプリにパーミッションを付与した以上、この情報をアプリがどのように使用するかを制御することはできません。特定の接続パーミッションと組み合わせることで、デバイス内のすべての連絡先がユーザーの知らないうちに第三者に送信されてしまう可能性もあります。このようなアプリはプライバシーを侵害する恐れがあります。

- **インターネットにアクセスする可能性のあるアプリ**

  現在あるアプリの多くは、インターネットへの接続にパーミッションを必要とします。他のパーミッションと組み合わせると、深刻なセキュリティ問題につながる可能性があります。インターネットとの間で送受信される情報を監視することはできません。各アプリの信頼性とインターネット接続の必要性を確認してください。

プライバシーアドバイザーには、デバイスにインストールされているすべてのアプリが一覧表示されます。画面の一番下に「プライバシーアドバイザー」のフィルタを表すアイコンが表示されます。フィルタをオン/オフに切り替えるには、各フィルタをタップします。

フィルタは複数選択することが可能で、選択したカテゴリに関連するパーミッションを持つすべてのアプリがハイライト表示されます。

アプリのパーミッションと選択したカテゴリの関連性に基づいたリスクのレベルは以下のとおりです。

- 赤で表示されるアプリ: 選択したカテゴリに対して、アプリが要求するパーミッションのリスクが高いことを表します。
- 黄色で表示されるアプリ: 選択したカテゴリに対して、アプリが要求するパーミッションのリスクが中程度であることを表します。
- 白で表示されるアプリ: 選択したカテゴリに対して、アプリが要求するパーミッションのリスクが低いことを表します。

リストの項目をタップしてアプリの詳細情報を表示します。アプリが持つパーミッションとそのパーミッションの使用目的が表示されます。

デバイスからアプリをアンインストールする場合は、「**アンインストール**」をタップします。

15 社内管理

企業環境の場合、Sophos Intercept X for Mobile は、Sophos Mobile で一元管理することができます。これによって、組織の管理者は、ユーザーのデバイスのコンプライアンス状況を監視することができます。

Sophos Intercept X for Mobile を Sophos Mobile に登録するには、組織内の管理者から案内される手順に従います。

Sophos Intercept X for Mobile が Sophos Mobile の管理下にある場合、次のような点が異なります。

- アプリの設定は、社内で規定されている設定が一元的に適用されます。
- 組織は、デバイスに対して検索を実行し、セキュリティのステータスを確認することができます。
- デバイスが組織のポリシーに違反した状態の場合、ネットワークへのアクセスや、他の機能の利用が制限されることがあります。アプリのダッシュボードにコンプライアンス状態が表示されます。詳細は、コンプライアンス違反の解消 (p. 21)を参照してください。

注
別の方法として、組織が Sophos Mobile Control を使用し、デバイスやデバイスの仕事領域を管理することもできます。デバイスにアプリをインストール/アンインストールしたり、デバイスの機能をオフにしたりするなど、組織による詳細な制御が可能になります。この場合、ユーザーはデバイスのコンプライアンス状態を確認し、Sophos Mobile Control アプリから IT 部門に問い合わせることができます。詳細は、Sophos Mobile ユーザーヘルプを参照してください。

15.1 コンプライアンス違反の解消

Sophos Intercept X for Mobile が Sophos Mobile の管理下にある場合、組織のポリシーに基づいたコンプライアンスの状態が表示されます。

コンプライアンス違反を表示し、解消する方法は次のとおりです。

1. ダッシュボードで「**社内管理**」をタップします。
   コンプライアンス違反がある場合、タイルには赤いアイコンが表示されます。
2. コンプライアンス違反の項目をタップし、指示に従って解決します。

注
デバイスがコンプライアンスに違反した状態の場合、ネットワークへのアクセスや、他の機能の利用が制限されることがあります。

15.2 サポートへの問い合わせ

Sophos Intercept X for Mobile が Sophos Mobile の管理下にある場合、IT 部門への問い合わせ情報やその他の詳細な情報を表示できます。

ダッシュボードで「**社内管理**」をタップします。

連絡先は、「**IT 問い合わせ**」および「**追加情報**」に表示されます。

ヒント
「**メール**」、「**電話番号**」、「**携帯電話番号**」フィールドのいずれかをタップして、メールや電話で IT 部門に問い合わせをすることができます。

16 設定

設定	説明
スケジュール検索	定期的に自動検索を実行します。
スケジュール検索の頻度	スケジュール検索の頻度。 「**毎日 (充電時)**」を選択すると、デバイスが 30分以上電源につながっていると検索が実行されます。
許可されたアプリの管理	タップすると、許可されたアプリの一覧が表示されます。このリストに表示されるアプリは検索結果には表示されません。各アプリはリストから削除できます。削除したアプリは、再び「**脅威および不要と思われるアプリケーション**」リストに表示されるようになります。
デフォルトのクリア	リンクを開くデフォルトのアプリとして Intercept X が指定されている場合、タップすると設定を解除できます。
システム アプリの検索	Android システムアプリを検索の対象にするには、これを選択します。 システム アプリは Android で保護されており、ユーザーは削除できないため、デフォルトで検索されません。
ストレージの検索	SD カードや USB ストレージデバイスを検索の対象にするには、これを選択します。
不要と思われるアプリの検出	不要と思われるアプリ (PUA) の検出をオンにするには、これを選択します。 不要と思われるアプリは悪質ではないものの、一般に業務には不適切と考えられているアプリです。不要と思われるアプリには主に、アドウェア、ダイヤラー、システムモニター、リモート管理ツール、ハッキングツールなどがあります。ただし、このカテゴリに分類されているアプリのなかにも、一部ユーザーで有用と捉えられているものもあります。
アプリのレピュテーション	レピュテーションの低いアプリの検索をオンにするには、これを選択します。 レピュテーションの低いアプリは、Sophos Live Protection のデータに基づいて信頼度が低いと識別されるアプリです。

設定	説明
検索の通知	検索後、アプリが感染していないことを通知するには、これを選択します。 選択を解除した場合、マルウェア、不要と思われるアプリ、およびレピュテーションの低いアプリに関する通知のみが表示されます。 Android デバイスにアプリをインストールしたり、SD カードや USB ストレージデバイスからアプリを起動すると、Sophos Intercept X for Mobile でアプリの検索が実行されます。通知は通知パネルに表示されます。
ストレージの監視	SD カードや USB ストレージデバイスに新たにダウンロードまたはコピーされたアプリやファイルすべてを検索するには、これを選択します。新しくストレージデバイスを接続すると、自動的に検索が開始します。
バージョン	ウイルス対策エンジンとウイルス対策データのバージョン。
前回の更新日時	ソフォスからウイルス対策データを取得した日時。 タップすると、アップデートを確認できます。
更新モード	Sophos Intercept X for Mobile がウイルス検出データの更新ファイルをダウンロードする際に使用するデータ接続を指定します。
ログのメール送信	タップすると、アプリのログファイルを添付したメールを送信できます。 デフォルトでソフォスのサポートのメールアドレスが宛先フィールドに挿入されます。
ユーザビリティ向上のためのデータ追跡	アプリの品質向上のために使用状況に関する匿名データをソフォスに送信することが許可されます。
Sophos Intercept X for Mobile のアンインストール	タップすると、Intercept X アプリ、およびインストールされている場合は、関連付けられている Security & Antivirus Guard アプリがアンインストールされます。

17 バックアップと復元

アプリの設定をバックアップして、別のデバイスで使用したりできます。

次の項目をバックアップできます。

- 設定
- スキャナ
- Web フィルタリング
- アプリのロック
- 認証

Sophos Intercept X for Mobile が Sophos Mobile の管理下にある場合は、認証アカウントのみをバックアップできます。

バックアップの設定

1. アプリメニューで「**バックアップと復元**」を選択します。
2. 「**バックアップ**」をタップします。
3. エクスポートする設定を選択します。
4. 「**バックアップ**」をタップします。
5. デバイスの認証情報を入力して、「**次へ**」をタップします。
6. バックアップコピーの作成先を選択します。

   ヒント
   バックアップをクラウドストレージに保存すると、他のデバイスでも使用できます。

7. ファイル名を入力して、「**保存**」をタップします。
8. バックアップコピーのパスワードを入力し、確認のために再入力して、「**OK**」をタップします。

復元の設定

1. 「**バックアップ/復元**」ページで、「**復元**」をタップします。
2. バックアップコピーを保存した場所を入力して、バックアップコピーをタップします。
3. バックアップコピーのパスワードを入力して、「**OK**」をタップします。
4. 復元する設定を選択します。
5. 「**復元**」をタップします。

18 ログ

Sophos Intercept X for Mobile では、アプリ本体のログに重要な操作が記録されます。このログは、Android のログとは別です。他のアプリをインストールした際のマルウェアスキャンなど、アプリがバックグラウンドで実行する操作の結果は直接表示されません。ログでは、このような操作の詳細な記録を確認できます。操作が行われた日時やその結果がログに記録されます。

- ログを表示するには、「「**メニュー**」 ≡」をタップした後、「**ログ**」をタップします。
- ログを消去するには、タイトルバーで「「**削除**」 🗑」をタップします。

19 利用条件