SOPHOS

Cybersecurity made simple.

Sophos Intercept X for Mobile

ヘルプ (iOS)

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、iOS デバイスに搭載されている VoiceOver スクリーンリーダーと Zoom 拡大ソフトウェアで使用することを推奨します。VoiceOver および Zoom 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。VoiceOver または Zoom についてご不明の点は、Apple 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。

関連情報

Web Content Accessibility Guidelines
iPhone ユーザーガイド：iPhone で VoiceOver をオンにして練習する
iPhone ユーザーガイド：iPhone 画面で拡大する

2 Sophos Intercept X for Mobile について

Sophos Intercept X for Mobile は、iPhone や iPad を安全に利用するためのアプリです。

Sophos アイコンを長押しすることで、クイックアクションのメニューを表示できます。3D Touch デバイスでは、アイコンを短くタップするだけでメニューを表示できます。

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

「**デバイスセキュリティ**」で、デバイスのセキュリティ状態を確認できます。

Sophos Intercept X for Mobile は、次の情報を表示します。

- 機種名や iOS バージョンなど、デバイスの一般的な情報。
- 使用可能な最新の iOS バージョンがインストールされていない場合は、アップデートに関する推奨情報。
- Sophos Intercept X for Mobile がデバイスで Jailbreak を検出した場合は、Jailbreak 情報。

5 Web フィルタリング

「Web フィルタリング」を使用して、管理者は悪意のあるコンテンツや不適切または違法なコンテンツを掲載するサイトをユーザー閲覧することを防止できます。

管理者がユーザーのデバイスを管理している場合、カテゴリに基づいて、Web サイトの閲覧前に警告を表示したり、アクセスをブロックしたりできます。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。

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。

注

- 使用するには、管理者がこの機能をオンにする必要があります。

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 要求がブロックされました**」という通知を下にスワイプして、「**許可リストに追加**」をタップします。

「**許可リスト**」の下に、許可された Web ページの数が表示されます。カウンターをタップすると、すべてのページを表示できます。

ユーザーが追加した項目と、管理者が事前に定義した項目は、それぞれ異なるセクションに表示されます。

再びページをブロックするには、項目を左にスワイプして削除します。この操作は、ユーザーが自分で追加した項目のみに対して実行できます。

ブロックリスト

警告の対象になる Web ページをブロックリストに追加すると、そのページの閲覧は常にブロックされるようになります。「**Web 要求がブロックされました**」という通知を下にスワイプして、「**ブロックリストに追加**」をタップします。

「**ブロックリスト**」の下に、ブロックする Web ページの数が表示されます。カウンターをタップすると、すべてのページを表示できます。

ユーザーが追加した項目と、管理者が事前に定義した項目は、それぞれ異なるセクションに表示されます。

再び警告を表示するには、項目を左にスワイプして削除します。この操作は、ユーザーが自分で追加した項目のみに対して実行できます。

6 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。 iOS 10.3 以降のデバイスでは、ARP スプーフィングを検知できません。
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。

問題の非表示

特定のネットワークに関する Wi-Fi 問題を非表示にすることができます。非表示にした問題は、デバイスのセキュリティ状態には影響を与えません。

すべての Wi-Fi 問題を再度表示するには、アプリの設定で「**すべての Wi-Fi の問題の表示**」を選択します。

7 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. 8)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、「**タップして表示**」をタップして最初のコードを作成するか、「**次へ**」をタップして次のコードを作成します。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。
- 表示中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、対象のアカウントのワンタイムパスワードをタップします。
- アカウントの詳細を編集するには、「**編集**,」をタップしてアカウントの項目を選択し、「**変更**」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、「**編集**」をタップしてアカウントの項目を選択し、「「**削除**」 🗑」アイコンをタップします。

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。

7.1 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。

7.2 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. 「**作成 > QR コードの読み取り**」を選択します。
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。

7.3 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. 「**作成 > 手動追加**」を選択します。
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. アカウントの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、次のフィールドに設定内容を入力します。

   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。

   - 「**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。
   - 「**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「**保存**」 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。

8 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。
- 既存の KeePass KDBX ファイルを開きます。パスワードの項目を編集すると、元のファイルが変更されます。

「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。

8.1 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、「「**プラスマーク**」 ⊕」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。
   - **メモ**: 暗号化されたメモのエントリを作成します。
   - **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: 「「**プラスマーク**」 ⊕」、「**フィールドの追加**」の順に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。

「「**プラスマーク**」 ⊕」をタップしてエントリにファイルや写真を追加することもできます。

5. 「**完了**」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. 11)を参照してください。

注
サイズの大きいファイルや多数のファイルをエントリに添付すると、パフォーマンスに影響を及ぼす場合があります。このようなファイルは、Sophos Secure Workspace アプリで暗号化して安全に保管することを推奨します。

8.2 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. 「「**歯車**」 ⚙」アイコンをタップして、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. 「「**更新**」 ↻」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。

8.3 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 Safari で開くには、「**URL**」フィールドの横にある「「**地球**」 🌐」アイコンをタップします。

8.4 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。

8.5 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。

ヒント
パスワードセーフのファイル全体を検索せずに、グループやサブグループに限って検索することもできます。各グループ内のアイテムは再帰的に検索されます。

1. パスワードセーフで、下にスワイ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。

8.6 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. アプリのダッシュボードのパスワードセーフのタイルで、「「**情報**」」をタップします。
2. 「**パスワードセーフのファイルのバックアップ**」をタップします。
3. バックアップコピーの作成先を選択します。

注
また、マスターパスワードを忘れてしまったり、鍵ファイルを紛失してしまった場合などに備えて、パスワード情報を記入した復旧シートを印刷しておくことも推奨します。詳細は、パスワードセーフの復旧詳細シートの印刷 (p. 13)を参照してください。

8.7 パスワードセーフの復旧詳細シートの印刷

パスワードセーフのマスターパスワードを忘れてしまったり、鍵ファイルを紛失してしまった場合、パスワードセーフに保存されているデータにアクセスできなくなります。こういった事態を防ぐには、復旧に必要な情報が記載されている復旧詳細シートを印刷しておきます。

警告
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、パスワード情報を回復するのに復旧詳細シートだけでは十分ではありません。詳細は、パスワードセーフのバックアップ (p. 12)を参照してください。

1. アプリのダッシュボードのパスワードセーフのタイルで、「「**情報**」 ⓘ」をタップします。
2. 「**復旧詳細シートの印刷**」をタップします。
3. プリンタと印刷枚数を選択し、「**印刷**」をタップします。
4. 印刷したシートに次の情報を記入します。
   - マスターパスワード
   - パスワードセーフのファイルの保存場所
   - バックアップコピーの保存場所
5. 復旧詳細シートは安全な場所に保管してください。
   復旧詳細シートとパスワードセーフにアクセスできる全ユーザーは、パスワード情報を読み取ることができます。

パスワードセーフのファイルを鍵ファイルで暗号化した場合は、鍵ファイルのフィンガープリントが QR コードとして復旧詳細シートに記載されます。鍵ファイルの代わりに QR コードを使用してパスワードセーフを開くことができます。

9 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、「**続行**」をタップして Safari で開きます。

連絡先

QR コードを読み取り、「**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。

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、「**コピー**」をタップしてパスワードをクリップボードにコピーします。「**設定**」アプリで「**Wi-Fi**」を開きます。ネットワークを選択し、メッセージが表示されたらコピーしたパスワードを貼り付けます。

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。

10 メッセージフィルタリング

「メッセージフィルタリング」を使用して、管理者は受信 SMS/MMS メッセージでフィッシング攻撃用 URL を検索できます。

疑わしいメッセージは、個別の「**迷惑 SMS** 」タブにフィルタリング表示されます。

アプリの設定で「**メッセージフィルタリングをオンにする**」が表示されている場合は、組織のポリシーに応じて、「**設定**」アプリでメッセージフィルタリングをオンにする必要があります。

メッセージフィルタリングをオンにする

iOS の「**設定**」アプリの「**メッセージ**」で、「**不明な送信者および迷惑メッセージ**」をタップし、「**SMS フィルタリング**」で「**Intercept X**」をオンにします。

「メッセージ」アプリの「迷惑 SMS」タブ

知らない差出人からのメッセージがスパムとして分類された場合、そのメッセージは、「メッセージ」アプリの「**迷惑 SMS** 」タブに移動されます。同じ送信者からの既存のメッセージと今後送信されるメッセージも「**迷惑 SMS**」に移動されます。

注

- 既知の連絡先からのメッセージがスパムとして分類されることはありません。
- メッセージフィルタリング機能は、iMessages では動作しません。

11 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。
- 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. 16)を参照してください。

11.1 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。

11.2 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。

12 設定

設定	説明
メッセージフィルタリングをオンにします	受信 SMS/MMS メッセージでフィッシング攻撃用 URL を検索します。使用するには、管理者がこの機能をオンにする必要があります。詳細は、メッセージフィルタリング (p. 15)を参照してください。
Web フィルタリングをオンにします	悪意のある Web ページや、カテゴリ分けされた Web ページへの接続をブロックします。使用するには、管理者がこの機能をオンにする必要があります。詳細は、Web フィルタリング (p. 5)を参照してください。
すべての Wi-Fi 問題の表示	非表示にしたものも含め、すべての Wi-Fi 問題を表示します。
ログレベル	ソフォスのサポートから指示を受けた場合に、ログ情報のレベルを選択します。
ログファイルの送信	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。
データの追跡	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。

13 バックアップと復元

認証アカウントをバックアップして、新しい iOS デバイスや Android デバイスに移動できます。

アカウントのバックアップ

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. バックアップコピーの名前を入力します
4. 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。
5. 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。

6. 「**追加**」をタップします。

アカウントの復元

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。

14 利用条件