SOPHOS

Cybersecurity made simple.

Sophos Secure Workspace ヘルプ

製品バージョン: 9.6

目次

1 はじめに

Sophos Secure Workspace は、モバイルデバイスやクラウドにファイルを安全に保存し (複数のストレージサービスへの分散保存も可能)、機密データのプライバシー保護を実現するアプリです。企業では、文書ファイルやイントラネットの閲覧のほか、ファイル、ブックマーク、ログイン情報の保管を安全に行う必要があります。

Sophos Secure Workspace の主な機能は次のとおりです。

- ローカルまたはクラウド上に保存されている文書ファイルの表示。詳細は、文書ファイルの表示 (p. 7)を参照してください。
- ローカルまたはクラウド上に保存されている文書ファイルの管理。詳細は、文書ファイルの管理 (p. 8)を参照してください。
- PDF ファイルへの注釈の追加、PDF フォームの入力。詳細は、PDF ファイルの編集 (p. 12)を参照してください。
- メモの作成。詳細は、メモの作成 (p. 13)を参照してください。
- 写真の撮影。詳細は、写真の撮影 (p. 14)を参照してください。
- ZIP 形式や 7z 形式で圧縮されたファイルの管理。詳細は、圧縮ファイルの管理 (p. 17)を参照してください。
- 暗号化による文書ファイルの保護。詳細は、データのプライバシー保護 (p. 15)を参照してください。
- ユーザー間での安全な文書ファイル共有。詳細は、ユーザー間でのファイル共有 (p. 17)を参照してください。
- SafeGuard Enterprise のユーザーがパスワード保護したファイルの復号化。詳細は、ファイルのパスワード保護 (p. 23)を参照してください。
- すべてのパスワードを、内蔵のパスワードセーフに格納して管理。詳細は、パスワードの管理 (p. 31)を参照してください。

iOS では、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。

他のソフォス製品と併用すると、上記に加えて以下の機能も利用できます。

Sophos Mobile を使用している場合:

- プリインストールされている Polaris Office を使用して、Microsoft Word、Excel や PowerPoint ファイルの作成・編集。詳細は、Office ドキュメントの編集 (p. 11)を参照してください。
- 社内のイントラネットページや他の許可するページへの安全なアクセスを提供。詳細は、社内イントラネットへのアクセス (p. 20)を参照してください。
- 社内配布された文書ファイルを安全に閲覧。詳細は、社内ストレージの表示 (p. 22)を参照してください。
- ファイルをパスワード保護して (HTML5 形式に変換)、ユーザー間で共有。詳細は、ファイルのパスワード保護 (p. 23)を参照してください。
- Sophos Secure Workspace の設定やクラウドストレージのログイン情報の管理。

Windows または macOS で **SafeGuard Enterprise** を使用している場合:

- モバイルデバイス、ノートブック、デスクトップ間での安全なファイル共有。詳細は、デバイス間でのファイル共有 (p. 19)を参照してください。

- SafeGuard 鍵リングの鍵の使用。詳細は、鍵の管理 (p. 27)を参照してください。
- BitLocker および FileVault ディスク暗号化の復旧鍵の表示。詳細は、復旧鍵の表示 (p. 30)を参照してください。

Sophos Secure Workspace は、**Sophos コンテナ**経由で、ソフォスの他のアプリと情報を共有します。

- アプリのパスワードは、Sophos Secure Email と Sophos Secure Workspace の両方で使用されます。
- Sophos コンテナのアクション (ロック、ロック解除、パスワードのリセット、登録解除) はすべての Sophos コンテナアプリに適用されます。
- データやファイルは、Sophos コンテナアプリ間で安全に共有できます。

2 ローカルストレージ

「**ローカルストレージ**」ページにはデバイス上のファイルが表示されます。

Android の場合、ローカルストレージには、SD カードを除くデバイスストレージ内のファイルが含まれます。

iOS の場合、アプリからアクセスできるのはアプリのコンテナ内のファイルのみです。したがって、ローカルストレージには、新規作成したファイルや、Sophos Secure Workspace にインポートしたファイルが保存されます。

ファイルをコンピュータにコピーするには

ファイルをコピーする Windows コンピュータまたは Mac にデバイスを接続します。

Android の場合: USB の使用の下で「**ファイルの転送**」を選択します。Windows エクスプローラの「**PC**」の下にデバイスのストレージが表示されます。

iOS の場合: iTunes で、Sophos Secure Workspace の「**ファイル共有**」リストを使用します。

3 セキュアストレージ

セキュアストレージは、Sophos Secure Workspace アプリのみがアクセスできるデバイス上の安全なコンテナです。

セキュアストレージにファイルを保存すると、デバイスの鍵で暗号化されます (既に暗号化されているファイルを除きます)。

セキュアストレージからファイルを移動すると、ファイルは復号化されます (元から暗号化されていたファイルは復号化されません)。

Sophos Secure Workspace では、次のような場合に、セキュアストレージ内のファイルが自動的に削除されます。

- Sophos Secure Workspace アプリをアンインストールした場合。
- Sophos Secure Workspace アプリが Sophos Mobile の管理下から外れた場合。
- (Android で) アプリのデータを削除した場合。

4 クラウドストレージの接続

クラウドストレージのアカウントを Sophos Secure Workspace に接続する方法は次のとおりです。

1. **ホーム画面**で、次のいずれかの手順を実行します。
   - Android の場合:「**+**」をタップします。
   - iOS の場合:「「**クラウドストレージの追加**」 」アイコンをタップします。
2. ストレージサービスを選択します。
3. ログイン情報を入力します。

Sophos Secure Workspace で、接続されている各ストレージサービスの「**ホーム画面**」にタイルが作成されます。

5 お気に入り

「**お気に入り**」リストにファイルを収集すると、簡単にアクセスできます。お気に入りは、デバイスがオフラインの場合でも使用できます。

お気に入りにファイルを追加する方法は次のとおりです。

- Android: ファイル名の隣にある「「**星**」 ★」を選択します。
- iOS: ファイルを選択してから、「「**星**」 ★」を選択します。

フォルダを選択して、そのフォルダ内のすべてのファイル （サブフォルダを含む） をお気に入りに追加することもできます。

Android の場合は、ホーム画面にお気に入りを追加できます。

6 文書ファイルの表示

文書ファイルを表示するには、保存場所を参照してファイルをタップします。ファイルが、Sophos Secure Workspace の鍵リングに保存されていない鍵で暗号化されている場合は、暗号鍵のパスフレーズを入力する必要があります。暗号化されているファイルのアイコンには鍵マークが表示されます。

Sophos Secure Workspace で表示や編集が可能なファイルの種類について詳しくは、対応するサービスおよびファイル形式 (p. 39)を参照してください。

7 文書ファイルの管理

ドキュメントに対してさまざまな操作を実行できます。たとえば、ドキュメントを暗号化したり、クラウドストレージに移動したり、他のアプリと共有したりできます。

ファイルの操作

ファイルやフォルダのコピー、移動、名前変更、削除を行うことができます。

制限事項:

- ファイルやフォルダを 1つのクラウドストレージから別のクラウドストレージまたはデバイスストレージに、コピーまたは移動することはできません。
- 名前を変更できるのは、一度に 1つのファイルまたはフォルダのみです。
- Google ドライブでは、フォルダのコピーや移動はサポートされていません。
- iOS の場合: ローカルストレージにフォルダを作成することはできません。

ファイルプロパティの表示

ファイルサイズや暗号鍵の詳細などのファイルプロパティを表示できます。

Sophos Secure Workspace が Sophos Mobile の管理下にある場合、組織が定義した使用に関する制限情報を表示できます。

- Android: ファイルを選択してから、「**ファイルの操作**」 メニューから「**ファイルの詳細**」を選択します。
- iOS: ファイルを選択してから、「**詳細**」 ◦◦◦ メニューから「**ファイルの詳細**」を選択します。

ファイルのクラウドストレージへの移動

デバイスストレージからクラウドストレージにファイルを移動できます。ファイルはデバイスで削除されます。

注
クラウドストレージに移動する前にファイルを暗号化することを推奨します。

お気に入りにへのファイルの追加

「**お気に入り**」リストにファイルを収集すると、簡単にアクセスできます。お気に入りは、デバイスがオフラインの場合でも使用できます。

お気に入りにファイルを追加する方法は次のとおりです。

- Android: ファイル名の隣にある「「**星**」 ★」を選択します。
- iOS: ファイルを選択してから、「「**星**」 ★」を選択します。

フォルダを選択して、そのフォルダ内のすべてのファイル （サブフォルダを含む） をお気に入りに追加することもできます。

Android の場合は、ホーム画面にお気に入りを追加できます。

ファイルの暗号化および復号化

ファイルを暗号化したり、暗号化されている場合は復号化したりできます。

ファイルを暗号化する方法は次のとおりです。

- Android: ファイルを選択し、「**暗号化**」 「します。表示サイズによっては、最初に「**詳細**」 」を選択する必要があります。
- iOS: ファイルを選択してから、「**詳細**」 メニューから「**暗号化**」を選択します。

また、フォルダを選択して、そのフォルダ内のサブフォルダを含むすべてのファイルを暗号化することもできます。

ファイルを復号化する方法は次のとおりです。

- Android: ファイルを選択してから、「**復号化**」 」を選択します。表示サイズによっては、最初に「**詳細**」 」を選択する必要があります。
- iOS: ファイルをタップし、パスフレーズを入力してから「 **復号化**」を選択します。

他のアプリで作成されたファイルを Sophos Secure Workspace で使用する方法

他のアプリで作成されたファイルを Sophos Secure Workspace で使用する方法は次のとおりです。

- Android: 「**+**」を選択してから、 「**既存の文書ファイルのインポート**」を選択します。
- iOS: 「**詳細**」 メニューから「**既存の文書ファイルのインポート**」を選択します。

サポートされている場合は、元のアプリでファイルを選択し、「**次の方法で開く**」（Android） または「**アプリケーションを選択**」（iOS） を使用して Sophos Secure Workspace とファイルを共有することもできます。

注

- Android の場合: 暗号化されているファイルと平文のファイルを同時にインポートすると、平文のファイルを暗号化するオプションが表示されません。この場合、ファイルは、その時点での暗号化の状態のままインポートされます。
- iOS の場合: ドラッグ＆ドロップ操作で、Sophos Secure Workspace と他のアプリとの間でファイルを移動することができます。
- iOS の場合:「**Secure Workspace に保存**」と「**Secure Workspace で表示**」はデフォルトで無効になっています。有効化するには、「**共有メニュー**」の右端の「**・・・ その他**」をタップします。

Sophos Secure Workspace にあるファイルを他のアプリで使用する方法

Sophos Secure Workspace にあるファイルを他のアプリで使用できます。これを行うには、通常どおりファイルを選択して共有します。

Android: 一部のアプリでは、ファイルの選択ダイアログにある Sophos Secure Workspace からドキュメントを選択できます。たとえば Gmail では、メールの添付ファイルとして Sophos Secure Workspace からドキュメントを選択することができます。

注
Sophos Secure Workspace が Sophos Mobile の管理下にある場合、特定のストレージサービスを使用したファイルの共有が、管理者によって禁止されていることもあります。

8 Office ドキュメントの編集

注
このセクションの内容は、Sophos Secure Workspace が Sophos Mobile の管理下にある場合のみを対象としています。

Sophos Secure Workspace には Polaris Office ライブラリが含まれているため、Microsoft Word、Excel、PowerPoint ファイルを作成/編集することができます。

Microsoft Office ドキュメントの作成

Microsoft Office ドキュメントを作成する方法は次のとおりです。

1. ファイルを作成する保存先を参照して、「**+**」をタップします。
2. 「**Word**」、「**Excel**」または「**PowerPoint**」を選択して、埋め込まれている Polaris Office を開きます。

Microsoft Office ドキュメントの表示/編集

Microsoft Office ドキュメントを表示/編集する方法は次のとおりです。

1. ファイルを参照して、タップして、埋め込まれている Polaris Office で開きます。
2. Polaris Office メニューで、表示モードと編集モードを切り替えることができます。

注
暗号化された Office ドキュメントを編集すると、保存する際に再び自動的に暗号化されます。

制限

管理者は、ストレージサービスを使用した共有を制限することができます。その場合、埋め込まれている Polaris Office に次のような制限が適用されます。

- 管理者がファイルの共有を拒否した場合、Polaris Office で「**エクスポート**」を使用できません。
- 管理者がクリップボード操作を拒否した場合、Polaris Office でクリップボードを使用することはできますが、クリップボードの内容を別のアプリに貼り付けることができなくなります。

9 PDF ファイルの編集

注
このセクションの内容は、Sophos Secure Workspace が Sophos Mobile の管理下にある場合のみを対象としています。

モバイルデバイスは、手軽に文書ファイルを閲覧したり、PDF フォームに簡単なデータを入力したりするために使用できます。

Sophos Secure Workspace には、PDF ファイルのビューアとエディタが組み込まれています。

PDF ファイルを編集したり、PDF フォームに入力したりする方法は次のとおりです。

1. PDF ファイルを開きます。
   - ドキュメントに注釈を付けるには、「**注釈の追加**」ボタンをタップします。テキストを選択したり、注釈、テキスト、描画、線、四角形、矢印などのツールを使用したりできます。
   - PDF フォーム内のフィールドをタップして入力します。
2. 変更内容を保存します。
   暗号化されていたファイルは、保存する際に自動的に再び暗号化されます。

10 メモの作成

Sophos Secure Workspace では、手軽にメモを取ることができます。作成したメモは暗号化して安全な状態で保管することができます。

Android:

1. ファイルの保存先に移動します。
2. 「**+**」を選択した後、「**テキスト**」を選択します。
3. メモを入力します。
4. 完了したら、「**保存**」を選択します。
5. ファイル名を入力し、暗号鍵を選択します。

iOS:

6. ファイルの保存先に移動します。
7. 「**詳細**」 ◦◦◦ メニューから「**作成 > テキストファイル**」を選択します。
8. メモを入力します。
9. 完了したら、「**完了**」を選択します。
10. ファイル名を入力し、暗号鍵を選択します。

注
Sophos Secure Workspace が Sophos Mobile の管理下にある場合、Microsoft Office ファイルを作成・編集することもできます。詳細は、Office ドキュメントの編集 (p. 11)を参照してください。

11 写真の撮影

Sophos Secure Workspace では、撮影した写真をセキュリティ保護して保存できます。保存した写真は、明示的に共有しない限り、デバイス上の他のアプリからアクセスすることはできません。

Android:

1. 写真の保存先に移動します。
2. 「**+**」 を選択した後、「**写真**」を選択します。
3. 写真を撮ります。
4. ファイル名を入力し、暗号鍵を選択します。

iOS:

5. 写真の保存先に移動します。
6. 「**詳細**」 ◦◦◦ メニューから「**作成 > 写真**」を選択します。
7. 写真を撮ります。
8. ファイル名を入力し、暗号鍵を選択します。

12 データのプライバシー保護

データには価値があり、大切に保護する必要があります。デバイスやクラウドなど、保存先に関わらず、機密データは常に暗号化することを推奨します。

暗号化とは、許可されたユーザーだけが閲覧できるように、データを読み取り不能な書式に変換処理することです。暗号化することでデータの流出や紛失を阻止できるわけではありませんが、データを暗号化して解読不能にし、利用できなくすることで、攻撃者によるデータの悪用は阻止できます。暗号化することでファイルに鍵がかかるため、鍵の持ち主だけがファイルにアクセスできるようになります。

Sophos Secure Workspace における暗号化の仕組みの概要は、セキュリティに関する情報 (p. 38) を参照してください。

ファイルの暗号化

Sophos Secure Workspace では、簡単にファイルを暗号化できます。

Sophos Secure Workspace でファイルを新規作成したり、他のアプリからファイルをインポートしたりすると、ファイルを暗号化できます。

既に作成済みのファイルを暗号化する方法は次のとおりです。

1. リストからファイルを選択し、「**暗号化**」オプションを選択します。
2. 使用する暗号鍵を選択します。鍵が存在しない場合は、ここで作成することができます。
3. 「**OK**」をタップします。選択したファイルが暗号化されます。選択した項目にフォルダが含まれる場合は、フォルダ内のすべてのファイルが暗号化されます。

注
既に暗号化されているファイルを暗号化した場合、ファイルは新しい鍵で再度暗号化されます。古い暗号鍵の使用にパスフレーズが必要な場合で、鍵リングに鍵がないときは、パスフレーズの入力が求められます。

注
Sophos Secure Workspace が Sophos Mobile の管理下にある場合、ファイルは社内鍵リングにある鍵のみで暗号化できます。ローカル鍵では暗号化できません。社内鍵リングの使用に関する詳細は、鍵の管理 (p. 27)を参照してください。

ファイルの復号化

既存のファイルを復号化するには、ファイルの一覧から対象のファイルを選択して「**復号化**」オプションを選択します。

データにアクセスするためのパスフレーズを入力するよう、Sophos Secure Workspace にメッセージが表示されます。対象の鍵が鍵リング内にある場合は、パスフレーズの入力は求められません。

注
Sophos Secure Workspace が Sophos Mobile の管理下にある場合、ファイルは復号化できません。

13 ユーザー間でのファイル共有

Sophos Secure Workspace の暗号鍵はパスフレーズから生成されます。

暗号鍵はファイルごとに作成せず、ファイルのアクセス状況を考慮しながら作成します。

たとえば、複数のファイルを他のユーザーと共有する必要がある場合は次のようにします。

- 共有するファイルをすべて同じ暗号鍵を使用して暗号化します。
- 暗号鍵のパスフレーズを他のユーザーに通知します。
- あるユーザーが複数のユーザーが共有するファイルをクラウドストレージなどを通じてデバイスから閲覧しようとした場合、鍵リングに鍵がないと、Sophos Secure Workspace がパスフレーズの入力を求めます。ユーザーが正しいパスフレーズを入力すると、暗号鍵が鍵リングに追加されます。このため、暗号化ファイルの共有者には鍵リングではなくパスフレーズの配布が必要です。

注
同一のパスフレーズを使用して暗号鍵を 2つ作成した場合、まったく異なる 2つの鍵が生成されます。これは、セキュリティ上の理由から鍵の生成中にランダムなデータが追加されるためです。暗号化ファイルの閲覧するユーザーには、事前に暗号鍵を作成せず、ファイルを開く際にパスフレーズを入力してから暗号鍵を作成するよう案内してください。

注
Sophos Secure Workspace が Sophos Mobile の管理下にあり、送信者と受信者の双方の社内鍵リングに暗号鍵がある場合は、パスフレーズを配布することなく、ファイルを共有することができます。

13.1 圧縮ファイルの管理

Sophos Secure Workspace では、ZIP 形式や 7z 形式の圧縮ファイルを管理することができます。

圧縮ファイルの中身の表示

ZIP 形式や 7z 形式の圧縮ファイルを開いたり、圧縮ファイルを解凍せずに中のファイルを表示したりすることができます。

- ZIP 形式や 7z 形式のファイルを開くには、対象のファイルがある場所へ移動し、ファイルをタップします。圧縮ファイルがパスワードで保護されている場合は、パスワードを入力する必要があります。
- 圧縮ファイル内のファイルの内容を表示するには、対象のファイルがある場所へ移動し、ファイルをタップします。Sophos Secure Workspace でサポートされているファイル形式の場合、埋め込みのビューアにファイルが表示されます。

圧縮ファイルの展開

ZIP 形式や 7z 形式の圧縮ファイル内のファイルをすべて展開するには、次の手順を実行してください。

- 圧縮ファイルを選択し、メニューの「**展開**」をタップします。
- または、圧縮ファイルを開き、メニューの「**すべて展開**」をタップします。

圧縮ファイルからファイルを 1つのみ展開

ZIP 形式や 7z 形式の圧縮ファイル内のファイルを 1つ展開するには、次の手順を実行してください。

1. 圧縮ファイルを開きます。
2. 展開するファイルがある場所へ移動し、ファイルを選択します。
3. メニューの「**選択した項目を展開**」をタップします。

パスワード保護された ZIP 圧縮ファイルの作成

選択したファイルを圧縮し、新しい ZIP 圧縮ファイルとして保存することができます。また、パスワード付きの (暗号化した) ZIP ファイルを作成することもできます。

圧縮ファイルは、Sophos Secure Workspace の鍵リングの暗号鍵を使用して暗号化することもできます。

パスワードで保護された ZIP 圧縮ファイルを作成するには、次の手順を実行してください。

1. 圧縮するファイルが保存されているフォルダに移動します。
2. 1つまたは複数のファイルを選択し、メニューの「**圧縮**」をタップします。

   「**お気に入り**」、「**社内ストレージ**」、または「**最近使ったファイル**」からファイルを選択することはできません。

注
Sophos Secure Workspace が Sophos Mobile の管理下にあり、ストレージサービスのファイルの共有が許可されていない場合は、それらのファイルを圧縮保存することはできません。

14 デバイス間でのファイル共有

注
このセクションの内容は、Sophos Secure Workspace が Sophos Mobile の管理下にある場合のみを対象としています。

Sophos Secure Workspace と Sophos SafeGuard Enterprise には互換性があり、どちらの製品で暗号化したファイルでも閲覧・編集できます。

Sophos SafeGuard Enterprise は、ビジネス向けファイル/ディスク暗号化製品です。Windows / macOS 搭載のノート型/デスクトップ型のクライアントマシンで利用できます。Sophos SafeGuard Enterprise の「Cloud Storage」および「File Encryption」モジュールは、クラウド上のデータを透過的に暗号化します。

鍵リングに暗号鍵のないデバイスとファイルを共有する場合は、ファイルを開く際にパスフレーズを入力する必要があります。

15 社内イントラネットへのアクセス

注
このセクションの内容は、Sophos Secure Workspace が Sophos Mobile の管理下にある場合のみを対象としています。

社内ブラウザ

社内ブラウザを使えば、Sophos Mobile のポリシーの定義に従って、社内のイントラネットページや他の許可されているページに安全にアクセスすることができます。管理者は、社内ブラウザからアクセスを許可するドメインを、「社内ブックマーク」に設定できます。ユーザーは、サブページを「個人ブックマーク」に設定できます。

社内ブラウザはタブブラウザで、同時に複数の Web ページを表示することができます。社内ブラウザを起動すると、前回のセッションで開いていたタブがすべて再表示されます。

- 社内ブラウザを起動するには、「**ホーム画面**」の「**社内ブラウザ**」をタップします。
- ブックマーク設定や関連する機能を開くには、Android では画面右上の「**詳細**」⋮をタップします。iOS では、ツールバーを使用します。

ブックマーク

- 「**社内ブックマーク**」ページでは、管理者が登録したブックマークが表示されます。
- 「**個人ブックマーク**」ページには、ユーザーが登録したブックマークが表示されます。「「**星**」 ★」アイコンをタップして現在表示しているページをブックマークに登録します。
- 「**履歴**」ページには、閲覧した Web ページの一覧が時系列で表示されます。一覧から個別の項目を削除するには、その項目を右または左にスワイプします。一覧ごと消去するには、「**履歴を消去**」ボタン (Android の場合)、または「「**削除**」 🗑」アイコン (iOS の場合) をタップします。

アカウント情報

管理者が指定したポリシーで特定の Web サイトへのアクセスが許可されている場合、それらのサイト用のアカウント情報を管理することができます。

ユーザー名とパスワードを入力すると、Sophos Secure Workspace にアカウント情報を保存するようメッセージが表示されます。「**OK**」をタップして、アカウント情報マネージャにアカウント情報を保存します。次回からユーザー名とパスワードが自動的に入力されるようになります。

「**アカウント情報**」ページに保存したユーザー名とパスワードが表示されます。項目を削除するには、その項目を右か左にスワイプします。

ダウンロード

ほとんどの場合、Web ページ上のリンクの参照先は、他の Web ページです。しかし、参照先が文書ファイルであったり、SharePoint などの Web インターフェース経由で管理するファイルの一覧であったりすることもあります。文書ファイルを参照しているリンクをタップすると、社内ブラウザは、対象のドメインに対して設定されているアクセス権限をチェックします。

管理者が設定できる権限は次のとおりです。

- ファイルを閲覧する権限。
- ファイルをダウンロードし、閲覧する権限。
- ファイルをダウンロードし、他のアプリケーションで開く権限。

ファイルをダウンロードすると、「**セキュアストレージ**」に保存されます。ファイルが暗号化されていない場合は、ローカルコピーがデバイスの鍵で暗号化されます。

16 社内ストレージの表示

注
このセクションの内容は、Sophos Secure Workspace が Sophos Mobile の管理下にある場合のみを対象としています。

Sophos Mobile には、独自のファイル配信サーバーが含まれており、「**社内ストレージ**」という名前の追加のストレージサービスとして表示されます。

社内ストレージ機能は、次のように使用できます。

- 管理者は、Sophos Mobile の Web ポータルにファイルをアップロードできます。
- ファイルは読み取り専用です。ユーザーはファイルの閲覧のみ可能で編集はできません。
- 管理者は、ユーザーのグループを定義して特定のグループにのみファイルの閲覧を許可できます。
- 管理者は、データ漏えい対策として、ファイルごとに操作の許可・禁止を設定できます。詳細は、社内設定 (p. 37)を参照してください。

「**社内ストレージ**」に新規/更新された文書ファイルが配信されると、通知が表示されます。新規/更新されたファイルは、印付きで表示されます。

「**社内ストレージ**」内のファイルやフォルダを「お気に入り」に追加すると、Sophos Secure Workspace で、デバイス固有の暗号鍵を使用してオフラインのコピーが暗号化されます。

Sophos Mobile で配信するファイルを管理者が暗号化する場合は、モバイルデバイスにインストールされている Sophos Secure Workspace を利用するか (「**ローカルストレージ**」画面から簡単に暗号化できます)、あるいは Sophos SafeGuard Enterprise を利用します。

17 ファイルのパスワード保護

Sophos Secure Workspace では、鍵を使用した標準のファイル暗号化のほか、HTML5 形式でラップされるパスワード保護ファイルも作成でき、受信者側のソフトウェアのインストールは不要です。受信者は、パスワードの他に、Web ブラウザ (Windows/macOS の場合) または Sophos Secure Workspace アプリ (Android/iOS の場合) さえあれば、暗号化されたコンテンツにアクセスできます。

これはたとえば、組織外の受信者とファイルを共有する場合などに便利です。

パスワード保護されたファイルの表示/編集

Sophos Secure Workspace (Android/iOS の場合) または SafeGuard Enterprise (Windows/macOS の場合) で作成された、パスワード保護されたファイルを表示できます。

HTML コンテナをタップし、正しいパスワードを入力して、コンテナ内のファイルにアクセスします。

- コンテナに 1つのファイルしか含まれておらず、それが表示可能な種類のファイルである場合、ファイルが表示されます。編集可能な種類のファイルの場合、表示モードから編集モードに切り替えて変更を加えることができます。変更したファイルを保存する際、HTML コンテナの外に新しいファイルとして保存されます。
- コンテナに複数のファイルが含まれている場合は、HTML コンテナの外の場所をファイルの保存先として選択します。この新しい場所にあるファイルを暗号化するには、「**暗号化**」を選択します。ファイルの保存後、ファイルを表示して編集できます。

パスワード保護されたファイルの作成

注
パスワード保護されたファイルは、Sophos Secure Workspace が Sophos Mobile の管理下にある場合のみに作成できます。

1. パスワード保護するファイルを選択し、次のいずれかの操作を行います。
   - (Android) 「**詳細**」 ⋮メニューから「**パスワード保護ファイルの共有**」を選択します。
   - (iOS) 「**共有**」 ⍐ メニューから「**パスワード保護ファイルの共有**」を選択します。
2. パスワードを入力します。
3. メールアプリなど、パスワード保護ファイルの転送に使用するアプリを選択します。

注
共有するファイルが暗号化されている場合、Sophos Secure Workspace は、可能な限りファイルを復号化し、復号化されたファイルをパスワード保護します。

18 文書ファイル内の Web リンクの確認

Sophos Secure Workspace 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 Web サイトの閲覧を防止します。

- ユーザーが Microsoft Office や PDF 文書ファイル内のリンクをタップすると、Sophos Secure Workspace で、タップされた URL の確認が行われ、参照先の Web ページに関する脅威情報が表示されます。
- Web ページへのアクセスは自動的にブロックされません。ユーザーは、脅威情報を参照してから、操作を中止するか、Web ページを開くかを選択することができます。
- Web ページは、使用できる場合は社内ブラウザで表示され、そうでない場合はデフォルトのブラウザアプリで表示されます。

19 アプリのパスワード

アプリのパスワード

Sophos Secure Workspace では、パスワードを設定して Sophos Secure Workspace への不正なアクセスを防止できます。この設定を有効にすると、次回アプリを起動する際、パスワードの入力ダイアログが表示されます。アプリのパスワードは、Sophos Secure Workspace の起動時に毎回入力する必要があります。

Sophos Secure Workspace では、Sophos Secure Email と同じパスワードが使用されます。したがって、パスワードの変更は両方のアプリに適用されます。いずれか 1つのアプリにログインした後は、もう 1つのアプリを使用する際、ログイン情報を入力する必要はありません (シングル サインオン)。パスワードや管理者による設定は、Sophos コンテナに保存されます。Sophos コンテナは、デバイス上のソフォス製アプリが使用するデータを保護する領域です。

Sophos Secure Workspace には、指紋認証を使用してログインできます。ただし、指紋を読み取ることができない場合の代替手段として、アプリのパスワードを定義する必要があります。

注
Android では、Sophos Secure Workspace が Sophos Mobile の管理下にあり、デバイスが対応している場合のみ指紋認証を使用できます。

復旧パスワード

Sophos Secure Workspace では、アプリのパスワードを忘れた場合に復旧するパスワードを生成して、メールで送信することができます。アプリのパスワードを忘れた場合は、この復旧パスワードを使用して新しいアプリのパスワードを作成します。復旧パスワードを生成しておらず、アプリのパスワードを忘れた場合は、アプリの削除と再インストールが必要となります。アプリを削除すると、Sophos Secure Workspace によって保存されているすべてのローカルファイルと鍵リング内の鍵が削除されます。

注意
復旧パスワードの作成を強く推奨します。アプリのパスワードを忘れた場合は、復旧パスワードがない限り、パスワードをリセットすることができません。

注
Sophos Secure Workspace が Sophos Mobile の管理下にある場合、復旧パスワードは必要ありません。アプリのパスワードは、Sophos Mobile のセルフサービス ポータルでリセットできます。

猶予期間

利便性のために、アプリのパスワードを入力することなくアプリを起動できる期間 (猶予期間) を指定できます。猶予期間中は、パスワードの入力なしで Sophos Secure Workspace (および Sophos Secure Email) を起動できます。猶予期間は、アプリがメモリに常駐している間のみ有効です。アプリがシステムにロードされる際は、常にアプリのパスワードを入力する必要があります。

デバイスが画面ロックされている場合は、猶予期間の設定に関わらず、Sophos Secure Workspace もロックされます。

アプリのパスワードの設定

アプリのパスワード、復旧パスワード、および猶予期間は、「**設定**」画面で設定します。

アプリのパスワードの変更

アプリのパスワードは、Sophos Secure Workspace の起動時に表示される「**ログイン**」画面で変更することができます。アプリのパスワードを変更する際、同時に新しい復旧パスワードを生成することができます。新しい復旧パスワードを生成しない場合、新しいアプリのパスワードに対して引き続き同じ復旧パスワードを使用できます。

20 鍵の管理

Sophos Secure Workspace では、すべての暗号鍵は鍵リングに保管されます。暗号鍵を表示するには、メニューの「**暗号鍵**」をタップします。

鍵リングの削除

- 鍵リングは Sophos Secure Workspace をアンインストールすると同時にデバイスから削除されます。
- Android デバイスの場合、クラウドやメモリカード上の暗号化されたファイルは、暗号化された状態が保持されます。鍵リングが削除されると、これらのファイルにアクセスできなくなります。

暗号鍵の紛失

- 暗号鍵を紛失した場合でも、パスフレーズを覚えていれば、暗号化されたファイルにアクセスできます。
- パスフレーズを入力し、鍵リングにもう一度鍵を追加するよう、Sophos Secure Workspace にメッセージが表示されます。

注意
鍵を紛失し、パスフレーズも忘れてしまった場合は、暗号化されたファイルにアクセスできません。鍵もパスフレーズもない状態で暗号化ファイルを閲覧する方法はありません (攻撃可能なセキュリティホールとなるため)。

社内鍵リング

Sophos Secure Workspace が Sophos Mobile の管理下にある場合、管理者は、Sophos SafeGuard と社内鍵リングの同期を有効化できます。これによって、SafeGuard の鍵リングにある鍵は、Sophos Secure Workspace の鍵リングで使用できるようになります。

次の点に注意してください。

- 鍵リングにローカル鍵がある状態で社内鍵の同期を有効化した場合、それらの鍵を継続して使用できます。
- 社内鍵リングの同期を有効にすると、ローカル鍵は作成できなくなります。
- 管理者によって設定されている場合、デバイスがコンプライアンスルールに違反した場合などに Sophos コンテナがロックされると、デバイスから社内鍵が削除されます。

QR コードを使用して暗号鍵を共有

QR コードを使用すると、ローカル鍵を簡単に共有できます。たとえば、メールに鍵を添付し、受信者は QR コードを読み取って鍵リングに鍵を追加できます。

エクスポートされた鍵をパスフレーズで保護することを推奨します。受信者が鍵リングに鍵を追加するときは、パスフレーズを入力する必要があります。

社内鍵リングから鍵をエクスポートすることはできません。組織のポリシーで許可されている場合は、社内鍵リングの同期が有効になっているときにローカル鍵をエクスポートできます。

ローカル鍵をエクスポートする方法は次のとおりです。

1. エクスポートする鍵を選択し、次のいずれかの操作を行います。
   - Android: 「「**共有**」  」を選択します。
   - iOS: 「**エクスポート**」を選択します。
2. パスフレーズを入力して、「**保護**」(Android) を選択するか、もしくは「**パスフレーズを共有**」(iOS) を選択します。
3. QR コードが表示されたら、「**共有**」(Android) を選択するか、もしくは「**次の方法で開く**」(iOS) を選択します。
4. 鍵をメールに添付するか、保存場所を選択します。

鍵をインポートする方法は次のとおりです。

1. メニューから「**暗号鍵**」を選択し、次のいずれかの操作を行います。
   - Android: QR コードのアイコンを選択し、鍵の QR コードを読み取ります。
   - iOS: 「**+**」を選択し、「**QR コードからの鍵のインポート**」を選択し、鍵の QR コードを読み取ります。
2. 必要に応じて、パスフレーズを入力します。
3. 鍵は鍵リングに追加されます。

21 証明書の表示

注
このセクションの内容は、Sophos Secure Workspace が Sophos Mobile の管理下にある場合のみを対象としています。

表示できる証明書の種類は次のとおりです。

- SMC クライアント証明書。
- SCEP から発行されたクライアント証明書 (Sophos コンテナのポリシーで設定した場合)。
- Sophos コンテナのポリシーの一部としてデバイスに配信された、すべてのクライアント証明書とルート証明書。

証明書を表示する方法は次のとおりです。

- メニューの「**設定**」 をタップし、「**設定**」画面を開きます。「**証明書**」というセクションに、サブジェクトや用途に関する情報とともに証明書が表示されます。
- 証明書をタップすると、詳細な情報が表示されます。

22 復旧鍵の表示

注
このセクションの内容は、Sophos Secure Workspace が Sophos Mobile の管理下にある場合のみを対象としています。

BitLocker ドライブ暗号化 (Windows) や FileVault (macOS のディスク内容の暗号化機能) が有効になっているコンピュータでロックアウトされた場合、データにアクセスするには、復旧鍵を入力してロック解除を行う必要があります。

管理者が、コンピュータのロック解除に必要な復旧鍵を Sophos Secure Workspace に表示されるように設定できます。

コンピュータ用の復旧鍵を表示する方法は次のとおりです。

- メニューの「**復旧鍵**」をタップして割り当てられているコンピュータのリストを表示します。Windows コンピュータの場合、リストには各ディスクパーティションの項目が個別に表示されます。
- リストの項目をタップしてコンピュータやディスクパーティションの復旧鍵を表示します。
- コンピュータをロック解除するには、コンピュータの BitLocker (Windows の場合) または FileVault (macOS の場合) の画面に表示される手順に従ってください。

23 パスワードの管理

Sophos Secure Workspace では、KeePass Password Safe のファイルを管理することができます。

機能

- 新しいパスワードセーフのファイルの作成
- パスワードセーフのファイルの内容の編集
- パスワードや他のデータをクリップボードにコピーして、他のアプリで使用
- クラウドストレージにある既存の KeePass Password Safe ファイルの編集

対応するファイル形式と暗号化方式

- Sophos Secure Workspace は、バージョン 3 の KDBX ファイル形式に対応しています。ネイティブ KeePass 暗号化アルゴリズム (AES、ChaCha20 など) を使用しているファイルを開くことができます。
- 新しいパスワードセーフのファイルは、AES 暗号化を使用して、バージョン 3 の KDBX ファイル形式で作成されます。

23.1 パスワードセーフのファイルの作成

1. パスワードセーフのファイルの作成先に移動します。
2. 「**+**」、「**パスワードセーフ**」の順にタップします。
3. パスワードセーフのマスターパスワードを作成します。このパスワードは、パスワードセーフのファイルを開くために必要です。

   警告
   マスターパスワードを忘れた場合、パスワードやパスワードセーフの他のデータにアクセスすることはできません。

4. 任意: Android の場合は、鍵ファイルの使用を選択してください。
   マスターパスワードに加えて鍵ファイルを使用すると、パスワードセーフのファイルのセキュリティが強化されます。鍵ファイルは、任意のファイルを選択することも、新しく作成することもできます。パスワードセーフのファイルを開いたときに、利用できる状態になっている必要があります。

   「**鍵ファイルを使用する**」を選択し、「**+**」をタップしてファイルを作成するか、既存のファイルを選択します。この鍵ファイルをパスワードセーフのファイルと同じ場所に保存しないでください。

警告
鍵ファイルは、必ずバックアップを作成するようにしてください。鍵ファイルがない場合、パスワードセーフのファイルを開くことはできません。

iOS の場合は、パスワードセーフの設定で鍵ファイルを設定することができます。「**マスターパスワードの変更**」をタップして、「**鍵ファイルを使用する**」をオンにします。

5. iOS の場合は、必要なエントリをパスワードセーフのファイルに入力します。各エントリは、グループやサブグループに分類して整理することができます。

   Android の場合は、新しいパスワードセーフのファイルを保存した後で、パスワードのエントリを入力します。
6. 「**作成**」をタップして、名前、場所を入力し、「**保管**」をタップします。
7. 任意: パスワードセーフのファイルの暗号化を選択します。

   パスワードセーフのファイルは、すべて KeePass ファイル暗号化で保存されます。「**ファイルの保存**」ダイアログで暗号化オプションを選択すると、KeePass 暗号化に加えて、さらに Sophos Secure Workspace で暗号化が実行されます。

指定した場所に KDBX ファイルが作成されます。

23.2 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. パスワードセーフのファイルを開き、「**+**」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**: 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**: 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**: メモを保存するためのエントリが作成されます。iOS のみで使用できます。
   - **グループ**: エントリを整理するためのフォルダが、パスワードセーフのファイル内に作成されます。
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: Android では、「**タイトル**」 フィールドの横にあるアイコンをタップして、別のものを選択します。
5. 任意: 項目にカスタムフィールドを追加します。
   - Android の場合: 「**フィールドの追加**」をタップして、フィールド名と値を入力します。
   - iOS の場合: 「**+**」をタップして、追加するフィールドの種類を選択します。

   カスタムフィールドに対して「**保護済み**」を有効にすると、フィールドの横にある「「**目**」」アイコンをタップしない限り、フィールドの値は非表示になります。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。
6. 操作が完了したら、項目を保存します。
   - Android の場合: 「「**詳細**」」をタップします。
   - iOS の場合: 「**完了**」をタップします。

パスワードデータを使用して、簡単に Web ページやアプリにログ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ログイン (p. 33)を参照してください。

注
iOS 環境では、パスワードセーフのエントリにファイルを添付できます。サイズの大きいファイルや多数のファイルを添付すると、パフォーマンスに影響を与える場合があります。このようなファイルを安全に保管するには、Sophos Secure Workspace で暗号化することを推奨します。

23.3 パスワードの生成

Sophos Secure Workspace では、パスワードを自動生成できます。

1. パスワードセーフのファイルで、パスワードを生成するエントリを開きます。
2. 編集モードに切り替えます。
   - Android の場合:「「**編集**」」をタップします。
   - iOS の場合:「**編集**」をタップします。
3. パスワードの自動生成ダイアログを開きます。
   - Android の場合: パスワードフィールドの横にある「**+**」をタップします。
   - iOS の場合:「「**歯車**」」アイコンをタップします。
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. 条件に基づいてパスワードを生成します。
   - Android の場合: 「**パスワードの生成**」をタップします。
   - iOS の場合: 「「**更新**」」をタップします。
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。

23.4 パスワードデータを使用したログイン

- 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 ブラウザで開く方法は次のとおりです。
  - Android の場合: 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。
  - iOS の場合:「**URL**」フィールドの横にある「「**地球**」」アイコンをタップします。

ヒント
Android では、項目を開くと、Android の通知領域に Sophos Secure Workspace の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。

23.5 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。

23.6 パスワードセーフのエントリの検索

エントリの名前やエントリのフィールドの値を検索できます。Android では、グループ名を検索することもできます。

1. iOS の場合: 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。
2. 検索モードに切り替えます。
   - Android の場合: 「「**検索**」」をタップします。
   - iOS の場合: パスワードセーフの画面で下にスワイプします。
3. 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。

> **注**
> パスワードフィールドおよび「**保護済み**」に指定したフィールドは、検索の対象から除外されます。

23.7 マスターパスワードの管理

Sophos Secure Workspace で、マスターパスワードで保護されているパスワードセーフのファイルを開いた際に、「**パスワードを保存する**」を選択して、Sophos Secure Workspace の鍵リングにマスターパスワードを保存します。次回からパスワードセーフのファイルを開いたときに、マスターパスワードの入力が求められなくなります。

Sophos Secure Workspace の鍵リングに保存されたマスターパスワードを表示するには、メニューの「**パスワード**」をタップします。

Sophos Secure Workspace に保存されているマスターパスワードを削除するには、鍵リングからマスターパスワードを削除します。

24 設定

設定	説明
鍵リングの有効化	暗号鍵を鍵リングに保存する場合にオンにします。 鍵リングに保存されている鍵は、パスフレーズを入力せずに使用できます。
アプリのパスワードの有効化	アプリを起動するためのパスワードを設定します。 復旧パスワードを作成するオプションの選択も推奨します。アプリのパスワードをリセットするには、復旧パスワードが必要です。 **注意** 復旧パスワードを設定していないと、パスワードを忘れてしまった場合にアプリが使用できなくなります。
アプリのパスワードの変更	アプリのパスワードを変更する場合に使用します。
猶予期間	アプリを使わないときに、自動的にロックがかかるまでの時間を選択します。
画面キャプチャのブロック	アプリの画面キャプチャをブロックする場合にオンにします。
パスワードの非表示	アプリに入力するパスワードを隠す場合にオンにします。 このオプションをオンにすると、パスワードフィールドに入力したパスワードが隠される前に少しの間だけ表示されます。
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。
トレースの送信	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。
証明書	Sophos Mobile で管理されている証明書を表示します。詳細は、証明書の表示 (p. 29)を参照してください。

設定	説明
アプリのパスワード	アプリを起動するためのパスワードを設定します。 復旧パスワードを作成するオプションの選択も推奨します。アプリのパスワードをリセットするには、復旧パスワードが必要です。 **注意** 復旧パスワードを設定していないと、パスワードを忘れてしまった場合にアプリが使用できなくなります。
猶予期間	アプリを使わないときに、自動的にロックがかかるまでの時間を選択します。
Touch ID 認証	指紋認証によるアプリのロック解除を許可する場合にオンにします。
パスワードの文字を隠す	アプリに入力するパスワードを隠す場合にオンにします。 このオプションをオンにすると、パスワードフィールドに入力したパスワードが隠される前に少しの間だけ表示されます。
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。

25 社内設定

注
このセクションの内容は、Sophos Secure Workspace が Sophos Mobile の管理下にある場合のみを対象としています。

管理者は、Sophos コンテナのポリシーをデバイスに適用することにより、Sophos Secure Workspace アプリや Sophos Secure Email アプリの設定を行うことができます。

管理者は次の設定を行うことができます。

- アプリのパスワード機能を強制的に有効化。
- アプリのパスワードの最低要件の定義。
- 利用できるクラウド ストレージ サービスの定義。
- WebDAV 対応のクラウドストレージへアクセスするためのログイン情報の設定。
- クラウドストレージサービス、Egnyte のログイン情報の設定 (iOS)。
- Sophos Secure Workspace アプリ、もしくは社内ブラウザ (Android のみ) が表示されているスクリーンショットをブロック。
- アプリの使用の制限:
  - お気に入りの作成の禁止。
  - クリップボード操作の禁止。
  - 平分ファイルの共有の禁止。
  - 暗号化ファイルの共有の禁止。
  - ルート化された (Android) デバイス、または Jailbreak された (iOS) デバイスからのアクセスの禁止。
  - アプリの使用を特定の Wi-Fi 接続のみに限定。
  - アプリの使用を特定の時間帯や曜日に限定 (タイムフェンシング)。
  - アプリの使用を特定の地理内に限定 (ジオフェンシング)。

26 セキュリティに関する情報

セキュリティ

クラウドストレージのログイン情報とファイル暗号鍵:

- iOS の場合: iOS のキーチェーンが使用されます。
- Android の場合、システムのキーストアが使用されます。

アプリのパスワード (p. 25)の説明に従ってアプリのパスワードを設定した場合は、次のローカルデータが暗号化されます。

- デバイスの鍵 (セキュアストレージ、コアデータ、ローカルに保存される社内ストレージ、社内ブラウザでダウンロードしたファイルに対して使用)
- ローカル鍵
- SafeGuard 暗号鍵
- BitLocker および FileVault の復旧鍵
- クライアント証明書
- ルート証明書
- コンテナポリシー
- 接続設定

警告
キーストア (Android) とキーチェーン (iOS) のセキュリティを強化するため、パスワードを作成してデバイスを画面ロックすることを強く推奨します。

警告
キーストアやキーチェーンのセキュリティが低下するため、デバイスの root 化 (Android) や Jailbreak (iOS) は推奨しません。

ファイルの暗号化と鍵

- Sophos Secure Workspace は、AES-256 方式を使用してファイルを暗号化します。各ファイルには個別の DEK (データ暗号鍵) が生成されます。
- DEK 自体は、AES-256 KEK (鍵暗号鍵) によって暗号化されます。暗号化された DEK はファイルとともに保存されます。
- Sophos Secure Workspace では、ユーザーが入力したパスフレーズから、PKCS#5 暗号化標準で KEK が算出されます。
- この方法の特殊性とセキュリティ上の理由から、鍵の生成中にランダムなデータが追加されます。このため、同一のパスフレーズを使用して KEK を 2つ作成した場合でも、まったく異なる 2 つの鍵が生成されることにご注意ください。
- ユーザーが利用できる KEK は、Sophos Secure Workspace の「鍵リング」にまとめて保管されます。

27 対応するサービスおよびファイル形式

対応するクラウド ストレージ サービス

対応するクラウド ストレージ サービスは次のとおりです。

- Box
- Dropbox、Dropbox Business
- Egnyte
- Google ドライブ
- Microsoft OneDrive および OneDrive for Business (Office 365 サブスクリプションにも含まれています)
- Telekom MagentaCLOUD (旧称 Media Center)

Sophos Mobile を使用している場合は、次のクラウドストレージソリューションもサポートされます。

- すべての WebDAV 対応クラウドストレージ (例: ownCloud、Strato HiDrive など)
- 社内ストレージ

対応するファイル形式

Sophos Secure Workspace を使用して閲覧できるファイルの種類は次のとおりです。

- **閲覧と編集:**
  - PDF ファイル: PDF
  - テキストファイル: TXT、TEXT、LOG、ASC、DIFF、CONF、PROPERTIES
  - Microsoft Office (Sophos Mobile が必要です): DOCX、XLSX、PPTX
  - KeePass Password Safe のファイル: KDBX バージョン 3 (AES または ChaCha20 暗号化)
  - 圧縮ファイル: ZIP (表示、展開、作成)
- **閲覧のみ (内部ビューアによる):**
  - 画像ファイル: JPG、JPEG、PNG、GIF (アニメーション GIF 以外)、TIFF、TIF、BMP、BMPF、ICO、CUR、XBM
  - ハイパーテキスト: HTML、HTM、XHTML
  - オーディオファイル (Android): Android でサポートされるすべてのフォーマットとコーデック
  - オーディオファイル (iOS): AAC、MP3、M4A、WAV
  - 圧縮ファイル: 7z (表示、展開)
- **閲覧のみ (外部アプリと共有する場合):**
  - 画像ファイル: JPG、JPEG、PNG、GIF (アニメーション GIF 以外)、TIFF、TIF、BMP、BMPF、ICO、CUR、XBM
  - ハイパーテキスト: HTML、HTM、XHTML

— 文書ファイル: DOC、DOCX、PAGES

— 表計算ファイル: XLS、XLSX、CSV、NUMBERS

— プレゼンテーション: PPT、PPTX、KEY

— リッチテキスト: RTF

— 動画ファイル: MOV、MP4、M4V

外部アプリでは、ファイルを復号化や暗号化することはできません。

Sophos Secure Workspace が Sophos Mobile の管理下にある場合、追加で次の種類のファイルを表示・編集・作成できます。

- **表示 (内蔵の Polaris Office ライブラリが必要です):**

  太字で記載されているファイル形式は、Android 版でのみサポートされます。

  — Microsoft Word 97~2013: DOC、DOCX、**DOT**、**DOTX**

  — Microsoft Excel 97~2013: XLS、XLSX、**XLTX**、**CSV**

  — Microsoft PowerPoint 97~2013: PPT、PPTX、**PPS**、**PPSX**、**POT**、**POTX**
- **編集 (内蔵の Polaris Office ライブラリが必要です):**

  — Microsoft Word 97~2013: DOC、DOCX

  — Microsoft Excel 97~2013: XLS、XLSX

  — Microsoft PowerPoint 97~2013: PPT、PPTX
- **作成 (内蔵の Polaris Office ライブラリが必要です):**

  — Microsoft Word 2013: DOCX

  — Microsoft Excel 2013: XLSX

  — Microsoft PowerPoint 2013: PPTX

28 関連するソフォス製品

関連するソフォス製品について詳しくは以下のリンクを参照してください。

- Sophos Mobile: https://www.sophos.com/ja-jp/products/mobile-control.aspx。
- Sophos SafeGuard Encryption: https://www.sophos.com/ja-jp/products/safeguard-encryption.aspx。
- Sophos Mobile Security for Android: https://play.google.com/store/apps/details?id=com.sophos.smsec。

29 サポート

ソフォス製品のテクニカルサポートは、次のような形でご提供しております。

- ユーザー コミュニティ サイト「Sophos Community」(英語) (community.sophos.com/) のご利用。さまざまな問題に関する情報を検索できます。
- ソフォス サポートデータベースのご利用。www.sophos.com/ja-jp/support.aspx
- 製品ドキュメントのダウンロード。www.sophos.com/ja-jp/support/documentation.aspx
- オンラインでのお問い合わせ。https://secure2.sophos.com/ja-jp/support/open-a-support-case.aspx

30 利用条件