SOPHOS

Cybersecurity made simple.

SafeGuard Enterprise クイックスタート&ベストプラクティス ガイド

製品バージョン: 8.3

目次

(2019/11/14)

1 このガイドについて

このガイドは、SafeGuard Enterprise の次のような新機能の利用開始にあたり、最初に行う設定について説明します。

- Synchronized Encryption で複数の鍵に対応
- ファイルのパスワード保護の改善
- ロケーションベースの暗号化用の Outlook アドイン

機能や仕組みのほか、お使いの環境への導入方法を概説します。Synchronized Encryption モジュールの詳細については、SafeGuard Enterprise 管理者ヘルプを参照してください。

このガイドは、すべての手順が網羅されているインストールガイドではありません。本製品を熟知しているユーザーを主な対象としています。インストールと管理の詳細については、SafeGuard Enterprise 管理者ヘルプを参照してください。

2 ベストプラクティス: Synchronized Encryption で複数の鍵に対応

SafeGuard Enterprise では、Synchronized Encryption を使用している場合、特定の場所に対して使用する、暗号化鍵を追加で設定することができます。

ここでの説明では、以下のシナリオを想定しています。

- 一般に使用されるアプリケーションで作成されたファイルすべてを、デフォルトの「**Synchronized Encryption 鍵**」を使用して「**アプリケーションベース (Synchronized Encryption)**」で暗号化することが社内ポリシーで選択されました。
- ユーザーの「ドキュメント」フォルダにあるファイルは、「**個人鍵**」で暗号化します。
  - 暗号化されていないファイルを保存できる /unencrypted フォルダを、ユーザーの「ドキュメント」フォルダに含める必要があります。
- エンドポイント上のファイルすべてが、社内ポリシーに準じて暗号化されているようにするため、初期暗号化を有効にする必要あります。

2.1 複数の鍵ファイルのある暗号化ポリシーの作成

1. Management Center で、「**(デフォルト) ファイル暗号化**」ポリシーを選択して、「**暗号化の種類**」で「**アプリケーションベース (Synchronized Encryption)**」を選択します。
2. 「**アプリケーションリスト**」で、「**テンプレート**」を選択します。
   デフォルトでアプリケーションリストは「**テンプレート**」と呼ばれます。最も一般的に使用されるアプリケーションが含まれています。
3. 「**暗号化の適用先**」で、「**すべて**」を選択します。これは、通常 Windows エンドポイントに対して使用される、最も安全なオプションです。
   これによって、あらゆる場所にあるファイルを「**Synchronized Encryption 鍵**」で暗号化するルールが作成されます。ルールは、アプリケーションベースの暗号化が適用される場所の一覧に追加されます。

   次に、別の暗号化鍵で暗号化する場所に対する、特別のルールを追加できます。ローカルまたはネットワークにある場所のどちらでも指定できます。事前に定義した値を使用して指定することもできます。

   ここでは、ユーザーの「ドキュメント」フォルダを暗号化する例について説明します。
4. ルールを追加するには、「**パス**」編集フィールドをクリックして、ドロップダウンメニューで「**<ドキュメント>**」を選択します。

   注
   暗号化の適用先を変更することはできません。

   デフォルトの鍵は「**Synchronized Encryption 鍵**」ですが、それ以外の鍵を選択することもできます。たとえば、ドメイン鍵または組織単位の鍵を選択できます。また、ユーザーごとに固有の「**個人鍵**」を選択することもできます。

5. 「**鍵**」編集フィールドで、「**個人鍵**」アイコンをクリックしてユーザーの個人鍵を選択し、「ドキュメント」フォルダを暗号化します。鍵アイコンにカーソルを移動すると、その機能の説明が表示されます。

   暗号化しないフォルダを設定するには、そのフォルダに対する例外ルールを定義する必要があります。
6. 「**パス**」編集フィールドをクリックし、ドロップダウンメニューで「**<ドキュメント>**」を選択し、「**<Documents>** プレースホルダの後に ¥unencrypted と入力します。
7. 「**動作モード**」カラムで、ドロップダウンメニューから「**除外**」を選択します。
8. エンドポイントで初期暗号化を有効にするには、「**初期暗号化: 次のような既存ファイルを自動的に暗号化する**」の下にある「**ローカルディスクに保存されているファイル**」を「**はい**」に設定します。
9. ポリシーを保存して、適用します。

注
このようなポリシー (別の暗号化鍵で暗号化する場所に対する特別なルールを含む) を、SafeGuard Enterprise 8.0 がインストールされているエンドポイントに適用した場合、設定したルールは正しく適用されます。指定したすべての場所は、選択した鍵で暗号化されます。ただし、ポリシーの設定に「**暗号化の適用先**」を「**すべて**」に指定している項目が含まれている場合は、「**Synchronized Encryption 鍵**」が使用されます。指定した場所に保存されているファイルもすべて「**Synchronized Encryption 鍵**」で暗号化されます。

2.2 エンドポイントで実行する、複数の鍵に対応したアプリケーションベースの暗号化

エンドポイントに SafeGuard Enterprise 暗号化ソフトウェアがインストールされているが、ポリシーは適用されていない状態を想定します。

SafeGuard Enterprise システム トレイ アイコンで「**同期**」をクリックすると、エンドポイントに更新されたポリシーが適用されます。ポリシーの変更内容として、新しいファイルに対して暗号化が自動的に実行されるアプリケーションのリストがあります。このリストには Microsoft Office が含まれているため、新しい Microsoft Office ファイルはすべて暗号化されるようになります。

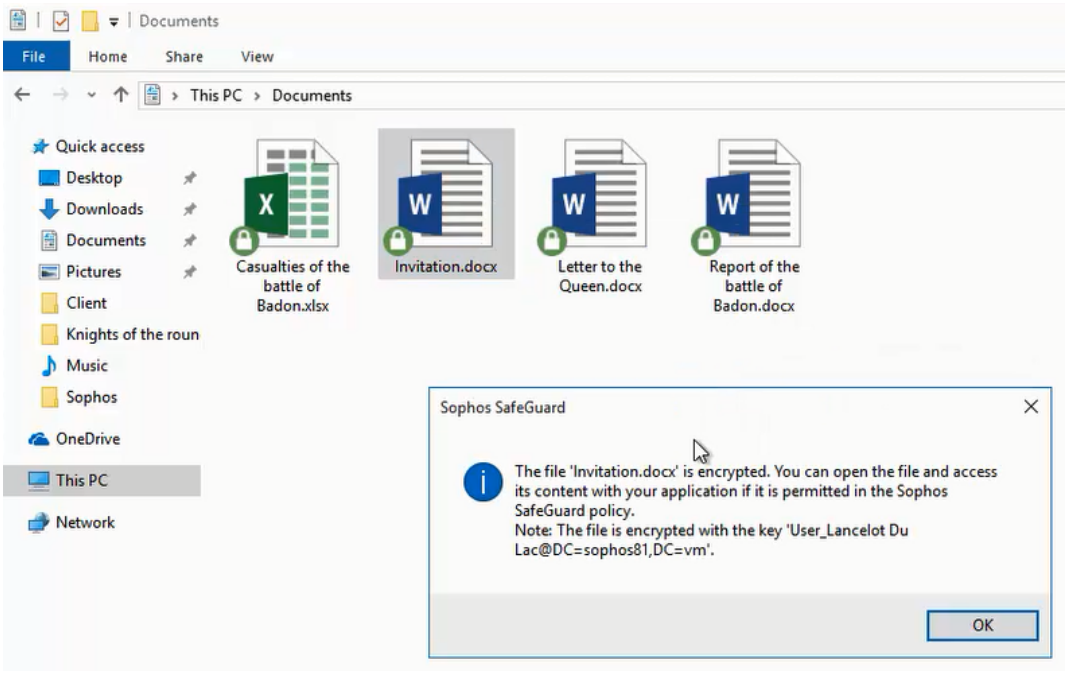
すべてのローカルドライブに対して初期暗号化を有効にすると、既にコンピュータにあったファイルもすべて暗号化されます。

注
アプリケーションリストを作成する際、初期暗号化の対象にするファイルの拡張子を指定する必要があります。「**テンプレート**」アプリケーションリストには、各アプリケーションで使用される最も一般的な拡張子が含まれています。

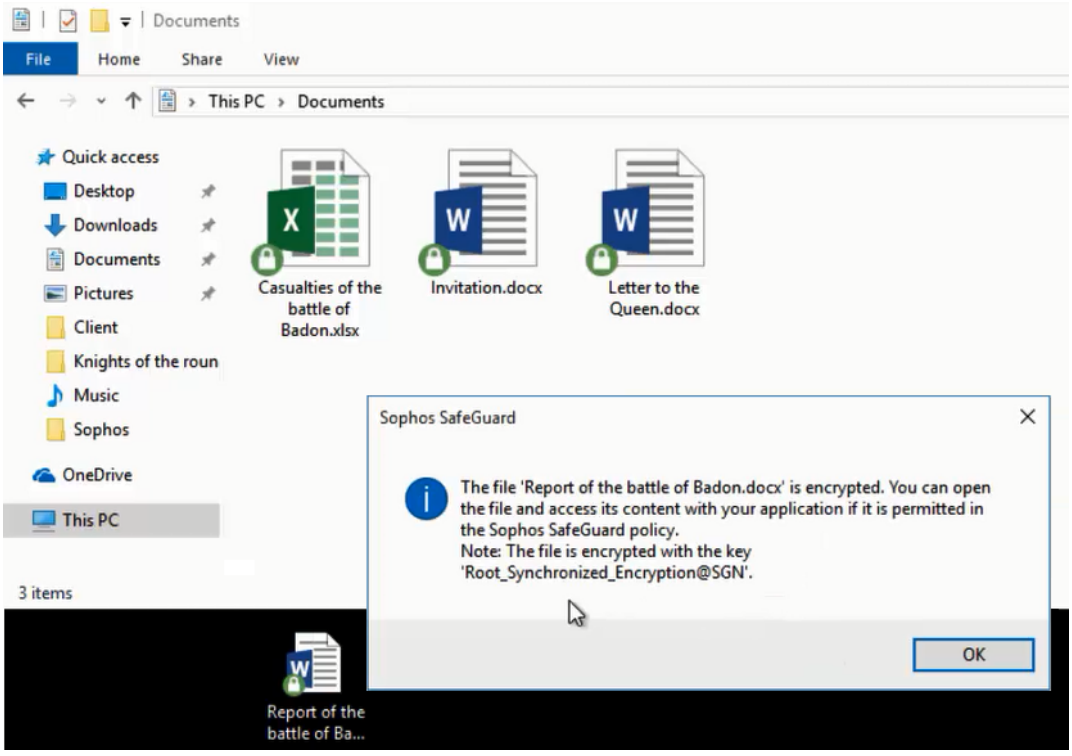
- 「ドキュメント」フォルダにあるファイルは、ユーザーの「**個人鍵**」で暗号化されます。
- それ以外のファイルで、アプリケーションリストに従って暗号化が必要なものは、すべて「**Synchronized Encryption 鍵**」で暗号化されます。

暗号化の適用先: 「すべて」と「指定した場所のみ」の比較

暗号化の適用先「すべて」では「**Synchronized Encryption 鍵**」を使用し、「**<ドキュメント>**」フォルダに限っては、ユーザーの「**個人鍵**」を使用することを選択しました。



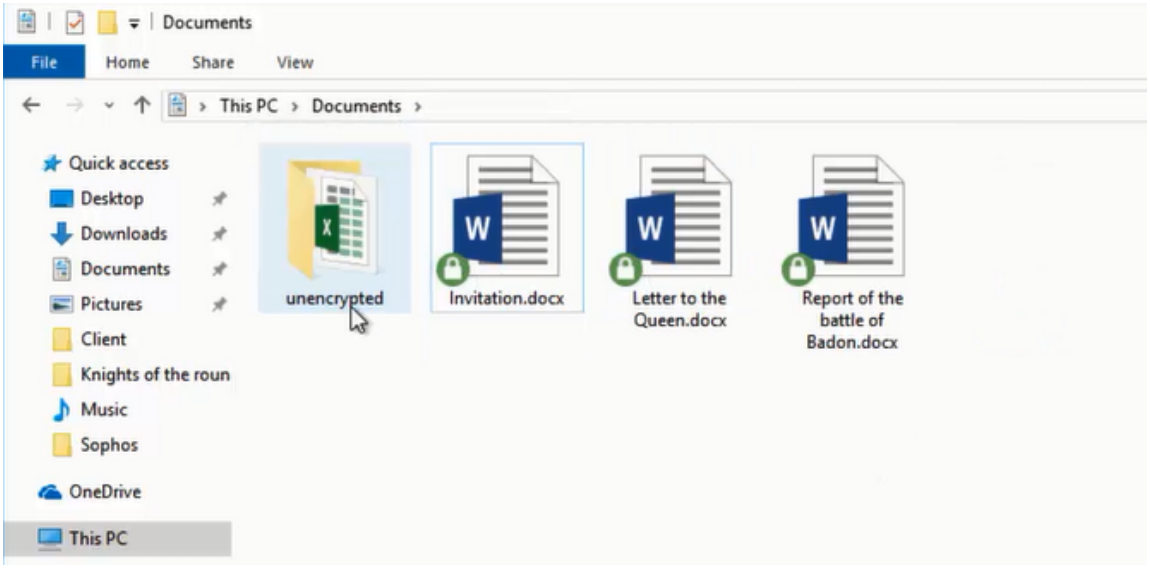
ファイルを移動またはコピーすることによって、使用される暗号化鍵が変わります。新しい場所は「**すべて**」ルールの対象になるため、「**Synchronized Encryption 鍵**」が使用されます。



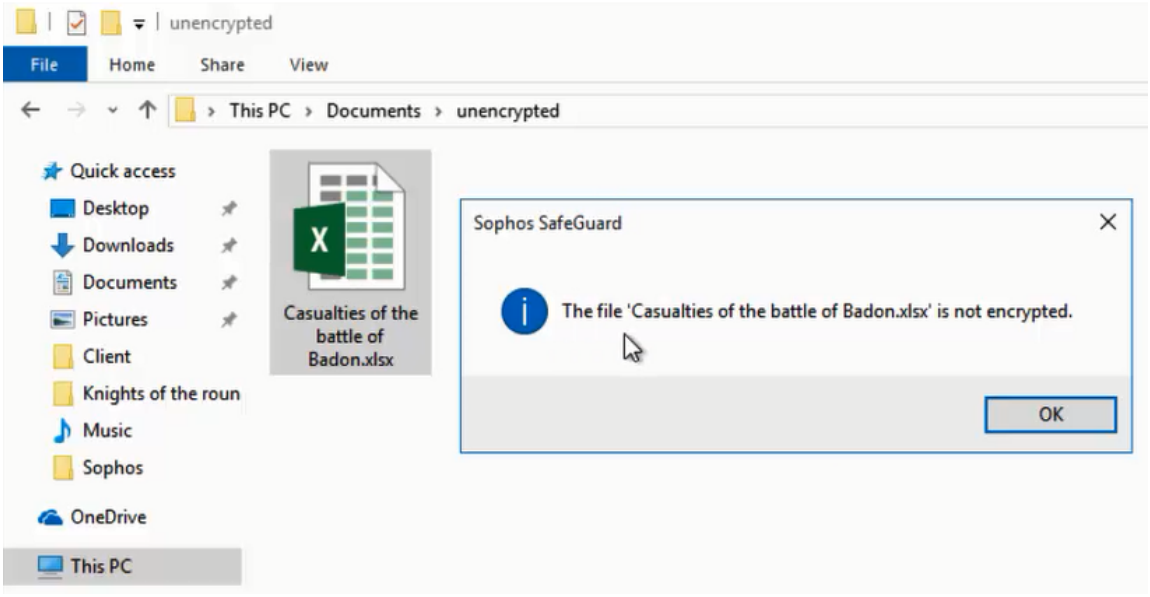
暗号化されていないファイルや既に暗号化されているファイルを「**<ドキュメント>**」フォルダに移動すると、ファイルはユーザーの「**個人鍵**」で暗号化されます。

暗号化の対象から除外するフォルダ

ファイル暗号化の対象から除外する場所として、ポリシーで「**<ドキュメント>**¥unencrypted」フォルダを指定します。



「unencrypted」フォルダに移動したファイルは、復号化されます。



SafeGuard Enterprise では、暗号化対象でない場所に、1つまたは複数の個別のファイルを配置した場合に限り、ファイルが自動的に復号化されます。フォルダを除外対象フォルダに移動したり、除外対象フォルダと同じ名前にフォルダの名前を変更したりした場合は、誤操作の可能性を考慮して、フォルダ内のファイルは自動的に復号化されません。手動でファイルを復号化するか、フォルダの SafeGuard Enterprise のショートカット メニューで、「ポリシーに基づいて暗号化」オプションを使用するようにしてください。

3 ロケーションベース暗号化用の Outlook アドイン

バージョン 8.1 以降では、ロケーションベースの暗号化で、Windows 用の SafeGuard Enterprise Outlook アドインを使用できます。これは、ロケーションベースのいずれかの File Encryption モジュールをインストールすると、エンドポイントで使用できます。

一般に、外部メールを送信する機能は、アプリケーションベース暗号化での機能と同じです。しかし、ホワイトリストに登録済みのドメインに添付ファイルのあるメールを送信する場合、ロケーションベースの暗号化の機能、および複数の鍵に対応する Synchronized Encryption の機能上、注意する点がいくつかあります。

「**デフォルトの全般設定**」ポリシーで、ホワイトリストに登録済みのドメイン (通常、社内のドメイン) に送信されるメールの添付ファイルの処理方法を指定できます。「**ホワイトリストに登録済みドメインの設定**」で使用できるオプションは次のとおりです。

- **暗号化する**
- **暗号化なし**
- **常に確認する**
- **変更しない (Synchronized Encryption)**

「**暗号化なし**」または「**常に確認する**」を選択した際の動作は、すべての File Encryption モジュールで同じです。

「**暗号化する**」または「**変更しない (Synchronized Encryption)**」を選択した際の動作は、Synchronized Encryption またはロケーションベースの暗号化のどちらで使用されるかによって異なります。

暗号化する

- Synchronized Encryption

  暗号化されたファイルは暗号化されたままで残り、暗号化鍵は変更されません。ファイル拡張子が IN アプリの一覧で定義されている場合に限って、暗号化されていないファイルは「**Synchronized Encryption 鍵**」で暗号化されます。

- ロケーションベースの暗号化

  ファイル拡張子や暗号化の状態に関わらず、添付ファイルはすべて、「**Synchronized Encryption 鍵**」で暗号化されます。

変更しない (Synchronized Encryption)

- Synchronized Encryption

  暗号化されたファイルは暗号化されたままで送信され、平文ファイルは平文のままで送信されます。

- ロケーションベースの暗号化

  すべてのファイルは、「**Synchronized Encryption 鍵**」で暗号化されます。

4 パスワード保護されたファイル

Synchronized Encryption で、ファイルのパスワード保護機能が導入されました。これは、暗号化された HTML ファイルをユーザーが作成して、その復号化にはパスワードが必要になる、という機能です。

この機能は、SafeGuard Enterprise 8.1 から、Windows 環境のロケーションベースの暗号化でも使用できるようになりました。

注
macOS 環境では、バージョン 8 から既に使用可能になっています。

4.1 ファイルのパスワード保護

社外のユーザーにメールを送信する際は、パスワードを使用してファイルを暗号化することを推奨します。この場合、SafeGuard Enterprise がインストールされていなくても、受信者は、暗号化されたファイルにアクセスできます。

以下の手順を実行してください。

1. 送信するファイルを右クリックして、「**ファイルのパスワード保護**」を選択します。
2. 送信するファイルを右クリックして、「**ファイルのパスワード保護**」を選択します。
   エラーメッセージが表示されたら、Finder で「**表示 > プレビューを隠す**」を選択して、もう一度やり直してください。
3. 画面上の指示に従って、パスワードを作成します。パスワードは、推測されにくいものを選び、添付ファイルと同じメールで送信しないことを推奨します。
   ファイルは暗号化され、HTML ファイルとして保存されます。この HTML ファイルは、添付ファイルとして安全に送信できます。

   注
   - 暗号化するためには十分なディスク領域が必要です。
   - 暗号化された HTML ファイルのファイルサイズは、元のファイルより大きくなります。
   - 対応しているファイルサイズの最大は 50MB です。
   - 一度に複数のファイルを送信する場合は、ZIP ファイルとして圧縮した後、その圧縮ファイルを暗号化できます。

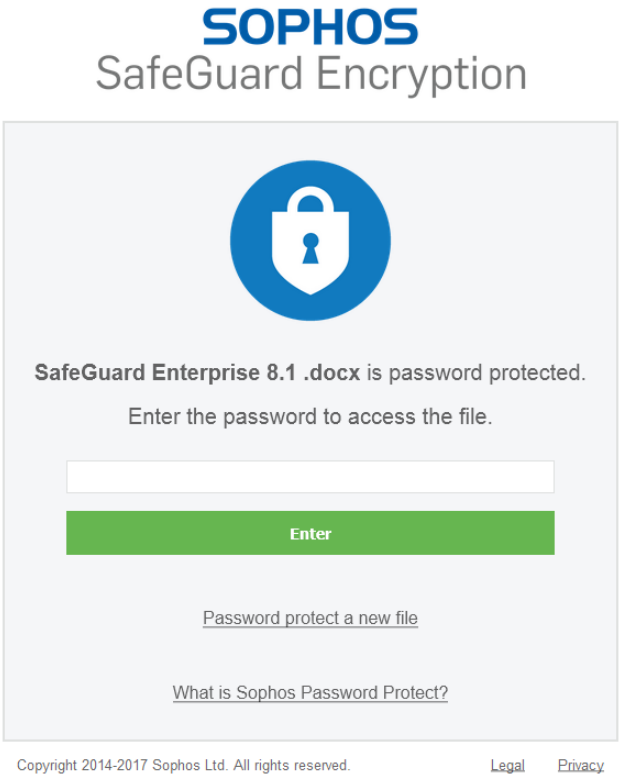
4. パスワードは、電話やその他の方法で受信者に通知します。
   受信者は、次のいずれかのブラウザを使用して、パスワード保護された添付ファイルを開くことができます。
   - Mozilla Firefox
   - Google Chrome
   - Microsoft Internet Explorer 11
   - Microsoft Edge
5. ファイルをダブルクリックし、画面に表示される指示に従って、次のいずれかの操作を実行するよう、受信者に伝えます。
   - パスワードを入力し、「**Enter**」をクリックしてファイルにアクセスします。

- 「**新しいファイルをパスワード保護する**」をクリックして、別のファイルをパスワード保護します。

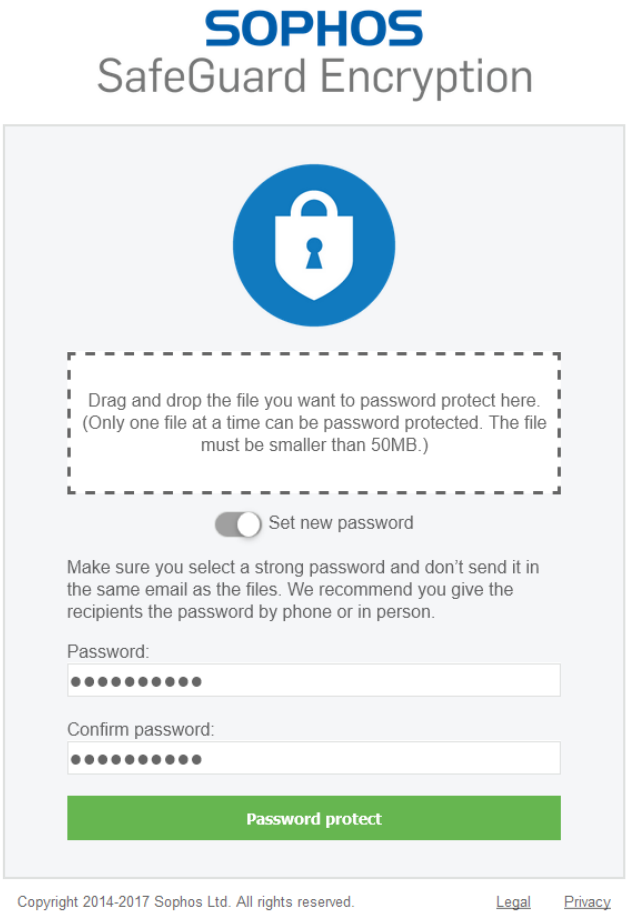
これで受信者は、パスワード保護されたファイルにアクセスできます。受信者は、返信するファイルをパスワード保護することもできます。その際、同じパスワードを使用するか、または新しいパスワードを作成することができます。さらに、別のファイルをパスワード保護することもできます。

4.2 新しいファイルのパスワード保護

SafeGuard Enterprise 8.1 環境でパスワード保護されたファイルを受信したユーザーは、新しいファイルをパスワード保護することができます。その際、先に元のファイルを復号化する必要はありません。はじめに元のパスワードを入力する必要もないので、時間を節約できます。



ユーザーは、暗号化された HTML ファイルをダブルクリックした後、「**新しいファイルをパスワード保護する**」をクリックするだけです。



ユーザーは、ファイルを枠内にドラッグ&ドロップし、強度の高いパスワードを入力して、「**パスワード保護**」をクリックします。

5 Synchronized Encryption

Synchronized Encryption は、Sophos SafeGuard Enterprise のアプリケーションベースのファイル暗号化モジュールです。ロケーションベースのファイル暗号化と異なる点は次のとおりです。

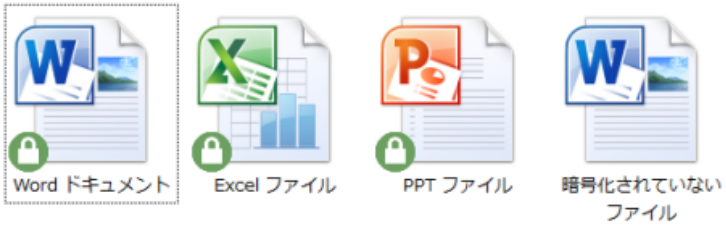
- あらかじめ指定したアプリケーション (IN アプリ) で作成または編集したファイルを自動的に暗号化。
- ファイルの読み取りは指定したアプリケーションのみで可能。
- ファイルの保存場所にかかわらず暗号化が可能。
- セキュリティ脅威の存在が疑われるユーザーのデバイスから、暗号化鍵の自動削除が可能。

> **注**
> この機能は、SafeGuard Enterprise と共に Web ベースの Sophos Central Endpoint Protection を使用している場合のみに使用できます。SafeGuard Enterprise のポリシーで、暗号化鍵の削除を設定しておく必要があります。この機能は、Windows エンドポイントと Mac OS X エンドポイントに対して適用することができます。

5.1 標準的なアプリケーションとの連係

Synchronized Encryption では、暗号化を意識する必要がないため、ユーザーは通常どおりに作業ができます。社外のユーザーにファイルを共有する場合のみに、送信先に応じたセキュリティレベルを考慮する必要があります。

たとえば、Excel や PowerPoint では、通常どおりにファイルを作成できます。作成したファイルは、保存する際に自動的に暗号化されます。暗号化されたファイルのアイコンは小さな鍵マーク付きで表示されます。



5.2 社内でのデータ共有

SafeGuard Enterprise の「**Synchronized Encryption 鍵**」を使用すると、簡単に社内でデータを共有できます。SafeGuard で暗号化されたデータは、社内の SafeGuard Enterprise ユーザーであれば誰でも閲覧できます。

このバージョンの SafeGuard Enterprise (SGN 8.1) では、特定の場所に対して、追加の暗号化鍵を設定することができます。Synchronized Encryption 鍵以外の鍵で暗号化されているファイルを読むには、その鍵がユーザーの鍵リングにある必要があります。詳細は、ベストプラクティス: Synchronized Encryption で複数の鍵に対応 (p. 2)を参照してください。

注
ユーザーは、Windows タスクバーの SafeGuard Enterprise システム トレイ アイコンを右クリックして、「**表示 > 鍵リング**」をクリックして、鍵リングを表示できます。

暗号化されたファイルは、メールで送信したり、ネットワーク共有に置いたり、あるいはリムーバブルストレージデバイスにコピーしたりするなど、通常と同じように共有できます。

Synchronized Encryption モジュールは、社内の共有データへのアクセスが必要なユーザーすべてのコンピュータにインストールする必要があります。

注
SafeGuard Enterprise は、すべての Windows エンドポイントと Mac OS X エンドポイントにインストールするようにしてください。

5.3 社外とのデータ共有

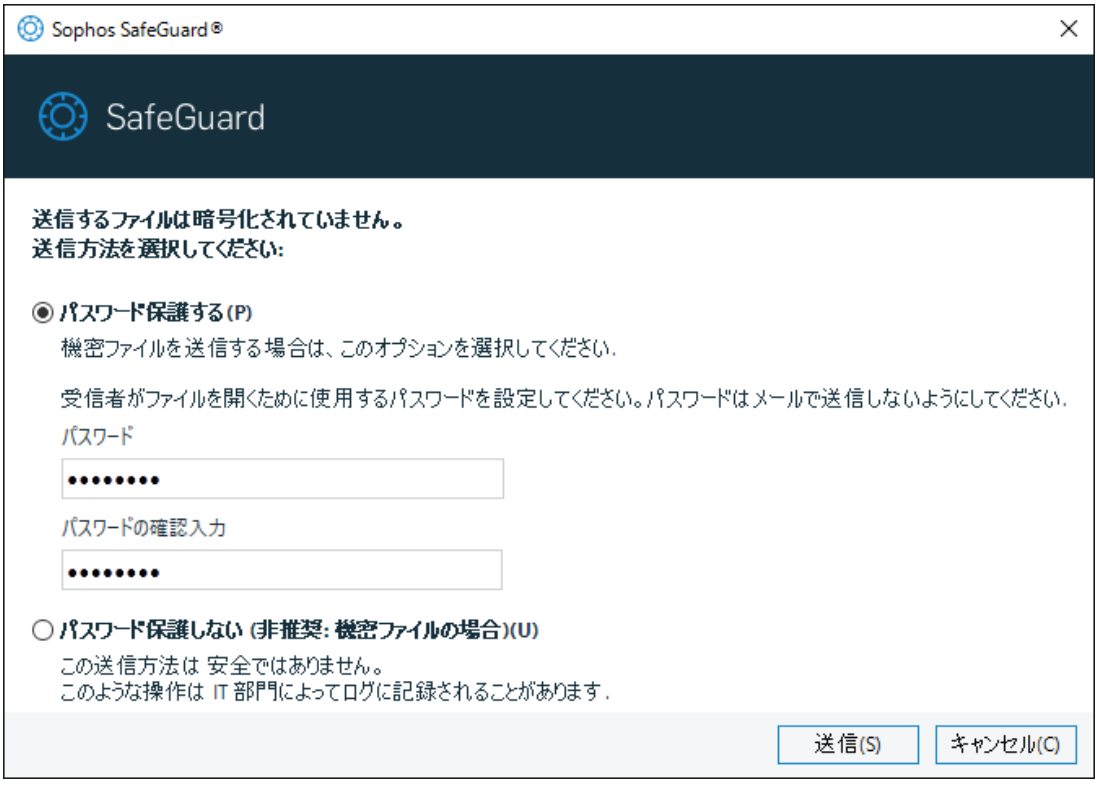
データ暗号化の目的は、機密データへのアクセスを制限することです。たとえば、財務情報や最新の知的財産などは、広く一般に公開するタイプの情報ではありませんが、場合によっては、こういった情報を社外と共有することもあります。暗号化した状態で共有することもあれば、すでに機密性はないと判断することもあります。

処理フローは、Microsoft Outlook を使用している場合と、使用していない場合で異なります。

ヒント
ユーザーには SafeGuard Enterprise ユーザーヘルプを案内してください。

Microsoft Outlook を使用している場合

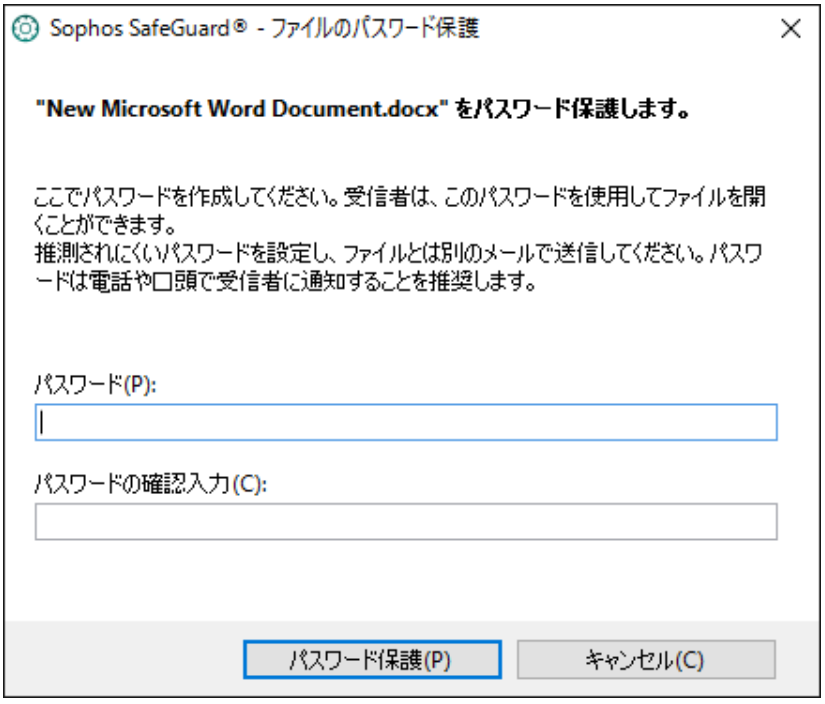
Microsoft Outlook (32ビット版 Office のみ) がインストールされている Windows コンピュータの場合、ユーザーは暗号化を意識する必要はありません。Synchronized Encryption では、ユーザーが少なくとも 1人の社外ユーザーに添付ファイルメールを送信しようとすると、ファイルの処理を確認するメッセージを表示するように設定を行うことができます。



Microsoft Outlook 以外を使用している場合

Windows ユーザーや Mac ユーザーは、ファイルを復号化してから平文で送信したり、ファイルをパスワードで保護してから送信したりできます。

ファイルを右クリックし、「**SafeGuard ファイル暗号化 - 選択したファイルの復号化**」の順に選択します。または、ファイルを右クリックし、「**SafeGuard ファイル暗号化 - ファイルのパスワード保護**」の順に選択します。この場合、HTML 拡張子を持つ新しいファイルが作成され、受信者は送信者があらかじめ設定したパスワードでファイルを開くことができます。



詳細は、SafeGuard Enterprise ユーザーヘルプのメールの添付ファイルを安全に送信する方法を参照してください。

5.4 IN アプリの指定

IN アプリとは、ファイルを作成・保存時に暗号化し、暗号化されたファイルを閲覧できるアプリケーションを指します。IN アプリは、SafeGuard Enterprise のセキュリティ担当者が、アプリケーションリストにアプリケーションのフルパスを追加して指定します (Windows と Mac OS X で個別に設定します)。

ヒント
アプリケーションは、すべてのコンピュータで同じ場所にインストールされている必要があります。コンピュータによってインストール先が異なる場合は、すべてのインストール先パスをアプリケーションリストに追加する必要があります。

5.4.1 IN アプリに指定するべきアプリケーション

IN アプリのみが、ファイルを作成・保存時に自動的に暗号化し、暗号化されたファイルを閲覧できます。ファイルの作成・保存時に暗号化を実行するアプリケーションや、暗号化済みファイルの閲覧に使用するアプリケーションは、すべて IN アプリに指定する必要があります。

ファイル作成アプリケーションの一般例は次のとおりです。

- オフィススイート (Microsoft Office、OpenOffice、FreeOffice など)
- デザインソフトウェア (Adobe Creative Suite など)

ファイル閲覧アプリケーションの一般例は次のとおりです。

- Office Viewer
- PDF ビューア
- 画像ビューア

注
Windows ストア アプリは、IN アプリとしてアプリケーションリストに追加できません。

ヒント
ファイル作成ソフトウェアで使用可能な拡張子すべてを指定するようにしてください。たとえば、Microsoft Word の場合、.docx のほかに .rtf や .odt なども指定する必要があります。

場合によっては、特定のユーザーのみが使用するアプリケーションも追加することも考えられます。その場合、特定のユーザーのみにポリシーを適用する必要はありません。コンピュータにインストールされていないアプリケーションに関するポリシーを受信した場合、その部分のポリシーは無視されます。

5.4.2 INアプリに指定するべきではないアプリケーション

暗号化の目的は、外部への情報漏えい防止であるため、社外への情報送信に使用する可能性のあるアプリケーションは、IN アプリに指定しないでください。指定した場合、送信する前にすべてのデータが復号化され、データが保護されていない状態になります。

メールクライアント、Web ブラウザ、バックアップ作成ソフトウェアなどは、決して IN アプリに指定しないでください。

注
Mac OS X の場合、Outlook アドインを利用できないため、メールプログラムを追加したほうが便利な場合もあります。

5.5 インストールにあたっての注意事項

Synchronized Encryption をインストールする際、まずは限定したユーザーのみ (テストグループ) にインストールすることを検討してください。それ以外のユーザーに対しては、読み取り専用ポリシーを適用し、社内で暗号化されたファイルの閲覧ができるようにします。詳細は、読み取り専用ポリシーの作成 (p. 16)を参照してください。

Synchronized Encryption のインストールにあたっては、状況に応じて、以降のセクションで説明する事柄を考慮してください。

5.5.1 ファイル作成に使用したアプリケーションとは異なるアプリケーションでファイルを開く

アプリケーションの中には、さまざまな形式のファイルを作成できるものがあります。たとえば、PDF 形式のファイルは Microsoft Word でも作成できます。Microsoft Word を IN アプリとして指定すると、Word で PDF 化したファイルも暗号化されます。データに機密情報が含まれる可能性があるので、これは正しい動作といえます。

しかし、この際、出力したファイルをどのアプリケーションで閲覧するのかを考慮する必要があります。この例では PDF リーダーを使用することにします。一般に、PDF リーダーを使用してファイルを作成することはありませんが、この場合、IN アプリとしてアプリケーションリストに追加する必要があります。リストに追加しないと、PDF リーダーでファイルを閲覧することができなくなります。このようなことから、SafeGuard Management Center のアプリケーションリストのテンプレートには、あらかじめ一般的な PDF リーダーが含まれています。

他には次のようなアプリケーションがあります。

- 画像を出力するアプリケーション
- TXT、RTF、CSV など、さまざまな形式でテキストを出力するアプリケーション

ヒント
指定した IN アプリで作成可能な種類のファイルを閲覧できる、デフォルトのリーダーが何であるかを検討します。このようなリーダーがすべてのコンピュータにインストールされていることを確認し、暗号化されたコンテンツを読み取れるように、IN アプリとしてアプリケーションリストに追加するようにしてください。

Windows 10 での PDF リーダー

Windows 10 のデフォルトの PDF リーダーは、新しい Web ブラウザ「Edge」です。Edge は IN アプリに指定できますが、指定すると、その後 Edge を使用してインターネットにアップロードするファイルはすべて復号化され、平文としてアップロードされるようになってしまいます。

重要
ビルトインの規定リーダーの Edge 以外に、Adobe Acrobat Reader または Foxit Reader などの PDF リーダーをWindows 10 コンピュータにインストールするようにしてください。

5.5.2 Java アプリケーション

多くの場合、Java アプリケーションの起動には java.exe という実行ファイルが使われます。したがって、java.exe を実行するパスから、現在どの Java アプリケーションが起動しているかを識別することはできません。java.exe を IN アプリに指定する場合、この実行ファイルを使用するすべてのアプリケーションで作成されるコンテンツが暗号化され、また暗号化されたファイルにアクセスできるようになることを考慮するようにしてください。

5.5.3 Web ベースのアプリケーション

複数のユーザーによる作業の効率化にあたって、Web にファイルをアップロードして共有できる Web ベースのアプリケーションがよく利用されます。暗号化されたファイルは、暗号化された状態が保持されるため、使用した元のシステムではファイルを読むことができません。つまり、以下の状況が発生します。

- ファイルの内容をインデックス化できません。
- 社外のユーザーがこれらのファイルを読むことはできません。

このようなファイルを社外のユーザーに共有する場合は、ファイルをアップロードする前に復号化してください。または、ファイルを暗号化せずに保存できるフォルダを作成してください。

このような暗号化の対象外とするフォルダは、この目的に限ってのみ使用するようにしてください。ユーザーに対しても明確にその旨を伝えてください。

ヒント
暗号化の除外を設定するには、対象となるフォルダの絶対パス (c:¥unencrypted など) を指定するか、相対パス (Windows クライアントのみに適用できます) を作成します。相対パスで除外を設定した場合、ユーザーは、相対パスで指定されているフォルダ名と同じ名前のフォルダを作成するだけです。たとえば、除外に指定したフォルダの名前が「¥unencrypted」の場合、作成場所にかかわらず、「¥unencrypted」という名前のすべてのフォルダ内のファイルとそのサブフォルダが暗号化されるようになります。

5.5.4 SafeGuard の暗号化機能がインストールされていないプラットフォームとのデータ交換

ユーザーは、作成したファイルを別の環境で使用する場合があります。たとえば、Windows や Mac OS X クライアントで作成されたファイルをターミナルサーバー環境で使用する場合などです。SafeGuard Enterprise はターミナルサーバー環境では利用できないので、SafeGuard で暗号

化されたファイルは、暗号化された状態が保たれ、ターミナルサーバー環境のアプリケーションで閲覧することはできません。

この問題は、該当するパスを暗号化の対象から除外するように暗号化ポリシーを設定することで回避できます。

5.5.5 プレビュー表示について

Windows エクスプローラや Finder などのファイル閲覧機能では、画像やテキストファイル、表計算ファイル、PDF など、さまざまな種類のファイルをプレビュー表示できます。このようなプレビューは、通常、ファイルを保存したときや変更したときに作成されます。プレビュー表示するには、プレビューを作成するアプリケーションが、(暗号化されていない) ファイルの内容にアクセスできなくてはなりません。したがって、該当するアプリケーションを IN アプリのリストに追加する必要があります。Mac OS X の場合、別の異なるアプリケーションでプレビューが作成されるので、それをアプリケーションリストに追加できます (デフォルトですでに追加されています)。

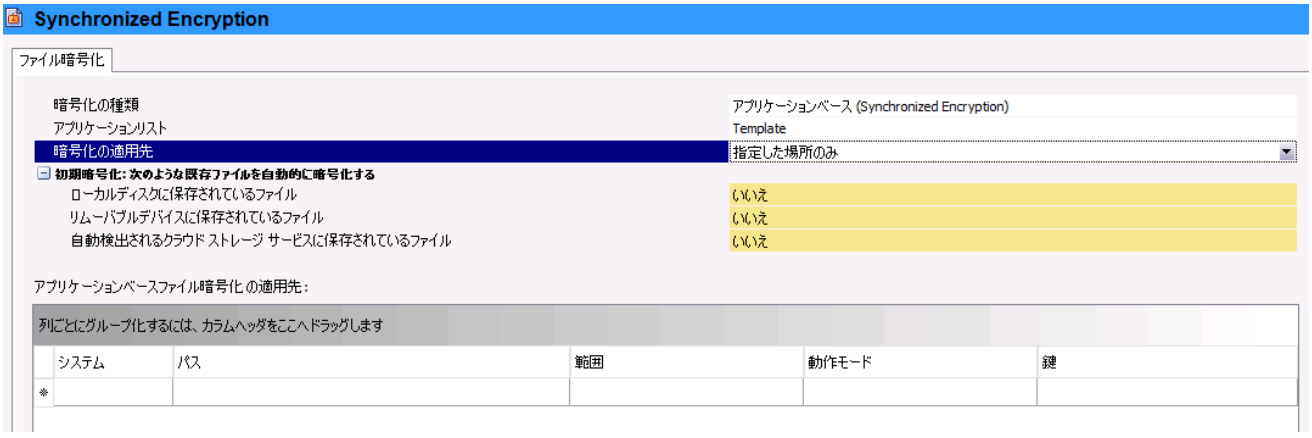
5.6 読み取り専用ポリシーの作成

Synchronized Encryption の段階的インストールを開始する際、まず、暗号化されたファイルの閲覧のみをユーザーに許可し、ファイルの暗号化は実行できないように設定します。その後、まず、特定のグループのみに対して暗号化機能を有効化し、最後に全ユーザーに対して有効化します。

インストールの最初の段階で使用するポリシーが、読み取り専用ポリシーです。

Windows

Windows ユーザーの場合、すべてのアプリケーションを含む Synchronized Encryption ポリシーを作成し、「**暗号化の適用先**」を「**指定した場所のみ**」に設定します。ただし、パスは指定しないようにしてください。



詳細については、SafeGuard Enterprise 管理者ヘルプの読み取り専用ポリシーの作成: Windows エンドポイントを参照してください。

Mac OS X

Mac OS X の場合、暗号化は Windows とは異なるかたちで動作します。Mac OS X コンピュータでは、指定された場所にある暗号化されたファイルのみを読み取ることができます。

したがって、Windows ユーザー向けの読み取り専用ポリシーを Mac OS X ユーザーに対して使用することはできません。

Mac OS X の場合、「**ファイル暗号化**」という種類のポリシーを作成して、暗号化の種類として「**ロケーションベース**」を選択する必要があります。少なくとも 1つのパスを追加し、追加したパスを暗号化の対象から「**除外**」し、それを Mac OS X ユーザーに通知してください。たとえば、<Documents>/Encrypted といったパスを指定します。暗号化されたファイルを閲覧する必要があるユーザーは、まず、閲覧するファイルをこの場所に移動またはコピーします。

詳細は、SafeGuard Enterprise 管理者ヘルプの読み取り専用ポリシーの作成: Mac エンドポイントを参照してください。

5.7 エンドユーザーへの通知

一般に、暗号化製品の使用経験のあるユーザーがあまり多くないため、暗号化の手順や規則を従業員に案内することを推奨します。特に Synchronized Encryption の場合、ユーザーが製品の動作を理解していることが重要です。たとえば、どのアプリケーションが IN アプリに指定されているかをユーザーが把握していれば、暗号化対象から漏れている主要アプリケーションがあった場合、即座に気付き、SafeGuard Enterprise のセキュリティ担当者に報告することができます。これを受け、セキュリティ担当者は、漏れているアプリケーションを暗号化の対象としてアプリケーションリストに追加することができます。

推奨する手順は次のとおりです。

- 新しく導入された暗号化規則とその結果発生する現象について簡単に説明したメールをすべてのユーザーに送信します。可能な場合は、簡単に編集できる社内 Web サイトに、新しく指定された IN アプリの情報などを都度掲載し、メールにリンクを含めます。
- メールには問い合わせ用メールアドレスを記載します。
- この時点で、すべてのエンドポイントに SafeGuard Enterprise がインストールされている場合は (読み取り専用モードなどで)、Synchronized Encryption の暗号化鍵で暗号化したファイルを添付し、ユーザーがファイルを閲覧できるかどうか確認を求めます。ユーザーが暗号化ファイルを閲覧できなかった場合は、インストールに問題があるか、またはエンドポイントと SafeGuard Enterprise のバックエンドとの通信に問題があるので、問題を修正してから全ユーザーに対して暗号化を有効化するようにしてください。

5.7.1 ユーザーへの通知文のサンプル

次にユーザーへの通知に使用するメールの文例を示します。文例には、最も重要な情報が含まれますが、「unencrypted」という名前のフォルダすべてを暗号化の対象から除外するルールを設定した場合や、文例に挙げられている以外のアプリケーションを使用している場合など、状況に応じて情報を追加してください。このメールの文例は、Synchronized Encryption の暗号化鍵で暗号化されたファイルを添付して送信することを前提に書かれています。

= =

各位

このたび、SafeGuard Enterprise の全社へのロールアウトを完了しましたので、お知らせいたします。SafeGuard Enterprise は、社内ドキュメントを保護するためにすべてのユーザーが使用するソフォスの暗号化製品です。暗号化による日々の業務への影響は特にありませんが、いくつか注意していただきたい点があります。

来週より、すべての従業員が、Synchronized Encryption というアプリケーションベースの暗号化機能を使用できるようになります。いったん、この機能が有効になると、ご使用のコンピュータで

作成したファイルは暗号化されるようになります。製品の使用開始にあたって、さまざまなガイドをイントラネット上に用意しましたので、ホームページより暗号化の項目をクリックするか、直接 https://company.internal/encryption を開いてください。

暗号化されたファイルをお使いのコンピュータで閲覧できるかどうか確認するには、添付のファイルを開いてください。

- **Windows および Mac OS X の場合:** 添付のファイルを開き、内容が閲覧できれば、設定は正しく完了しています。ファイルの内容が正しく表示されない場合は、ヘルプデスク担当者にお問い合わせください。
- **iOS および Android の場合:** お使いのデバイスで Sophos Secure Workspace アプリから添付ファイルを開きます。ファイルは暗号化されているため、システム標準のビューアで開くことはできません。お使いのモバイル端末上に Sophos Secure Workspace がインストールされていない場合は、ヘルプデスク担当者にお問い合わせください。

指定済みのアプリケーション

次のアプリケーションで作成するファイルは自動的に暗号化されます。暗号化されたファイルに異なるアプリケーションでアクセスした場合、内容を表示することはできません。

Windows:

- Adobe Reader
- MS Office 2010 (Excel、PowerPoint、Word)
- MS Office 2013 (Excel、PowerPoint、Word)
- MS Office 2016 (Excel、PowerPoint、Word)
- Office Viewer
- Foxit Reader

Mac OS X:

- Adobe Reader
- Apple 仕事効率化アプリ (Keynote、Numbers、Pages、Preview)
- MS Office 2011 (Excel、PowerPoint、Word)
- MS Office 2016 (Excel、PowerPoint、Word)

社外へファイルを送信する場合

社外にファイルを送信する際は、ファイルが暗号化された状態で送信されることに注意してください。この場合、社外の受信者はファイルを閲覧できません。機密情報が含まれていない場合は、ファイルを復号化してから送信するようにしてください。社外秘の場合や、社外秘の可能性がある場合は、ファイルをパスワード保護してください。ファイルを右クリックし、「SafeGuard ファイル暗号化」を選択します。そして、「選択したファイルの復号化」または「ファイルのパスワード保護」を選択します。

Windows 環境で **Microsoft Outlook** でファイルを送信する場合は、これらの作業を手動で行う必要はありません。暗号化されたファイルを社外に送信しようとすると、システムで検知され、ファイルの処理方法を確認するメッセージが表示されます。

Web アプリケーションにファイルをアップロードする場合

暗号化されたファイルは、常に暗号化されたままの状態でアップロードされます。つまり、SharePoint や使用しているその他の Web アプリケーションでも、暗号化された状態が保持されます。したがって、状況に応じて、ファイルを手動で復号化してからアップロードするようにしてください。暗号化されたファイルは、プレビュー機能で表示することも、検索インデックスを作成することもできないこと注意してください。

ご意見やご質問

SafeGuard Enterprise に関する問題や、暗号化機能のインストール後にコンピュータで生じた問題につきましては、ヘルプデスク担当者までお問い合わせください。

よろしくお願いいたします。

6 サポート

フルリリース

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/contact-support/support-query.aspx

7 利用条件