SOPHOS

Cybersecurity made simple.

SafeGuard Enterprise for Mac

ユーザーヘルプ

製品バージョン: 8.3

目次

1 SafeGuard Enterprise for Mac について

Sophos SafeGuard は、Mac で実行されるセキュリティ対策ソリューションです。次の 2つのコンポーネントから構成されています。

- SafeGuard Native Device Encryption (p. 1) は、FileVault 暗号化テクノロジーを使用して、コンピュータを保護します。
- SafeGuard File Encryption (p. 2) では、鍵やパスワードを使用して、ファイルを暗号化できます。

お使いの製品によっては、このヘルプで説明するすべての機能が含まれていない場合もあります。これは、使用しているライセンス、およびセキュリティ担当者が適用したポリシーに依存します。

Sophos SafeGuard は、Sophos SafeGuard Management Center コンソールから一元的に設定・管理されます。Sophos Safeguard Enterprise の管理方法の詳細は、製品ドキュメントページを参照してください。

Sophos SafeGuard に関する全般的な情報を表示するには、システムメニューの SafeGuard アイコンをクリックして、Sophos SafeGuard 環境設定ペイン (p. 5)を開きます。

ファイルの暗号化/復号化に関する最も重要なオプションは、Finder の右クリックメニューからアクセスできます。

重要
OS をアップデートする前に、まず、使用している Sophos SafeGuard のバージョンが、最新の OS に対応していることを確認してください。詳細は、SafeGuard Enterprise リリースノートを参照してください。OS を先にアップデートすると、データにアクセスできなくなる場合があることにご注意ください。

1.1 SafeGuard Native Device Encryption

Sophos SafeGuard Native Device Encryption は、OS に搭載されている FileVault ディスク暗号化テクノロジーを利用します。ハードディスク全体を暗号化し、コンピュータの盗難や紛失によるデータ漏えいを防止します。

SafeGuard Native Device Encryption は、バックグラウンドで動作します。ファイルを開くとき、編集するとき、または保存するときに、暗号化や復号化の指示は表示されません。

インストールの詳細は、Sophos SafeGuard 環境設定ペインの「Disk Encryption」タブ (p. 7)で参照できます。

SafeGuard Native Device Encryption では、次の操作を実行できます。

- コンピュータの暗号化 (p. 9)
- コンピュータの復号化 (p. 9)
- SafeGuard Native Device Encryption および SafeGuard File Encryption (p. 10)
- SafeGuard Enterprise サーバーへの接続の確認 (p. 16)

1.2 SafeGuard File Encryption

SafeGuard File Encryption では、コンピュータで暗号化するファイル、およびファイルの内容を読むことができるユーザーを、セキュリティ担当者が定義することができます。暗号化するファイルを定義する方法には、次の 2種類があります。

- ロケーションベースのファイル暗号化 (p. 3)
- アプリケーションベースのファイル暗号化 (p. 3)

File Encryption ポリシーは、コンピュータではなく、ユーザーに対して適用されます。通常、File Encryption ポリシーでは、「**書類**」などのユーザーのフォルダにあるファイルは暗号化するように指定されています。しかし、ファイルの暗号化対象から除外するフォルダを、セキュリティ担当者が指定している場合もあります。コンピュータ上で暗号化の対象に指定されている場所は、環境設定ペインの「Policies」タブ (p. 6)で参照できます。

Finder で、暗号化されているファイルは緑色の鍵マーク付きで表示されます。暗号化されていないファイルには、通常、何もマークが付きません。

注
バンドルやパッケージとして保存されているファイルの場合、暗号化されていても鍵マーク付きで表示されないことがあります。たとえば、テキストエディットで、暗号化されている画像ファイルを暗号化されているテキストファイルに挿入し、添付書類付きリッチテキストとして保存した場合、ファイルのアイコンは暗号化されていないように見えます。しかし、実際は暗号化されています。

暗号化ソフトウェアがインストールされ、SafeGuard Enterprise サーバーとの通信が確立されると、macOS のパスワードの入力が促されます。さらに、個人証明書も必要となります。この証明書は、パスワードを入力すると SafeGuard Enterprise サーバー上に生成されます。これは、製品インストール後、初回ログイン後、またはパスワードのリセット後のみに必要です。

SafeGuard File Encryption をインストールした後は、セキュリティ担当者によって適用されたすべてのポリシーを施行する必要があります。詳細は、ポリシーに基づいたファイルの暗号化 (p. 11)を参照してください。

SafeGuard File Encryption では、次の操作を実行できます。

- ポリシーに基づいたファイルの暗号化 (p. 11)
- ファイルの手動暗号化/復号化 (p. 11)
- 暗号化されたファイルのメール送信 (p. 12)
- ファイルのパスワード保護 (p. 12)
- リムーバブルデバイス上のファイルの暗号化 (p. 14)
- 暗号化ファイルの復旧 (p. 15)

macOS 10.14 におけるユーザーの同意

macOS 10.14 以降では、アプリケーションが他のアプリケーションを制御する場合、ユーザーの同意が必要となります。インストール後、macOS に「**"Sophos SafeGuard" が "Finder" を制御するアクセスを要求しています**」というメッセージが表示され、許可または拒否するよう促されます。Finder は、SafeGuard File Encryption が正常に機能するうえで必要な機能であるため、「**OK**」をクリックします。

「**オートメーション**」セクションの「**プライバシー**」の設定に項目が追加され、SafeGuard File Encryption に Finder の制御が許可されます。

「**許可しない**」をクリックすると、このダイアログは今後表示されなくなり、SafeGuard File Encryption で Finder の機能を使用することはできなくなります。

この設定を後から変更する場合は、「**オートメーション**」セクションの「**プライバシー**」設定を開き、「**Sophos SafeGuard**」の下の「**Finder**」を選択して、SafeGuard File Encryption に Finder の制御を許可します。

1.2.1 ロケーションベースのファイル暗号化

ロケーションベースのファイル暗号化では、暗号化対象の場所をセキュリティ担当者が定義することができます。このような場所は、暗号化対象フォルダ (p. 4)と呼ばれます。暗号化の対象となるコンピュータの場所は、環境設定ペインの「Policies」タブ (p. 6)で参照できます。

- 暗号化対象に指定されている場所に新規ファイルを作成すると、ファイルは自動的に暗号化されます。
- 暗号化対象に指定されている場所に暗号化されていないファイルを移動すると、ファイルは暗号化されます。
- 暗号化対象から除外されている場所に暗号化されているファイルを移動すると、ファイルは復号化されます。
- 暗号化されたファイルに対する鍵がある場合、ファイルの読み取りおよび変更が可能です。
- 暗号化されたファイルに対する鍵がない場合、ファイルの内容を読んだり、別の場所に移動したりすることはできません。
- 暗号化されたファイルに、File Encryption がインストールされていないコンピュータからアクセスしても、ファイルの内容を読むことはできません。

1.2.2 アプリケーションベースのファイル暗号化

アプリケーションベースのファイル暗号化では、指定されたアプリケーション (例: Microsoft Word など) で作成/変更したファイルが暗号化されます。ファイル暗号化を自動的に実行するアプリケーションのリストは、ポリシーで指定されます。アプリケーションベースのファイル暗号化は、すべての暗号化対象フォルダ (p. 4)に適用されます。さらに、セキュリティ担当者は、暗号化の対象から除外する場所を指定できます。コンピュータで暗号化の対象に指定されている場所は、環境設定ペインの「Policies」タブ (p. 6)で参照できます。

- 指定したアプリで作成した新規ファイルは、自動的に暗号化されます。
- 指定したアプリで変更したファイルは、自動的に暗号化されます。
- 暗号化されたファイルに対する鍵がある場合、ファイルの読み取りおよび変更が可能です。
- 暗号化されたファイルに対する鍵がない場合、ファイルの内容を読むことはできません。
- 暗号化されたファイルに、File Encryption がインストールされていないコンピュータからアクセスしても、ファイルの内容を読むことはできません。
- 暗号化されたファイルに、ポリシーで定義されていないアプリケーションでアクセスしても、ファイルの内容を読むことはできません。

1.2.3 暗号化対象フォルダ

暗号化対象フォルダは、Mac、ネットワーク共有、またはリムーバブルデバイスにある、ファイル暗号化対象の場所です。セキュリティ担当者は、暗号化対象の場所をポリシーで定義します。通常、Microsoft Outlook または Apple Mail がメールの添付ファイルを保存する、Documents や一時フォルダなどが指定されます。

macOS Catalina 環境で SafeGuard Enterprise は、Documents、Desktop、Pictures、Apple Mail などのフォルダにアクセスするためにユーザーのパーミッションを必要とします。

次の手順を実行して、SafeGuard Enterprise がこれらのフォルダにアクセスできるようにしてください。

1. 「**セキュリティとプライバシー**」を開きます。
2. ロックを解除して変更します。
3. 「**フルディスクアクセス**」を選択します。
4. 「+」ボタンをクリックして、次の 2つの SafeGuard アプリを「**フルディスクアクセス**」パネルに追加します。
   - sgd: /usr/local/bin/ フォルダから追加
   - Sophos SafeGuard: /Library/Sophos SafeGuard FS フォルダから追加

制限事項

- **暗号化対象フォルダにある場合のみ、暗号化されたファイルにアクセスできる**

  暗号化対象フォルダ以外のフォルダにある、暗号化されたファイルにアクセスすることはできません。暗号化されたファイルを、まず、暗号化対象フォルダに移動してから復号化するか、手動で復号化してから、暗号化対象フォルダ以外のフォルダに移動する必要があります。
- **暗号化対象フォルダで、バージョン履歴を保存できない**

  暗号化対象フォルダでは、標準機能の「**すべてのバージョンをブラウズ...**」が利用できません。
- **ファイルの検索**
  - デフォルトでは、暗号化対象フォルダにあるファイルを Spotlight を使って検索することはできません。Spotlight の使用を有効化する方法は、暗号化されたファイルの検索 (p. 15)を参照してください。
  - 暗号化対象フォルダで、ラベルの付いたファイルを検索することはできません。
- **暗号化対象フォルダの共有**

  暗号化対象フォルダをネットワーク上で共有することはできません。

2 Sophos SafeGuard 環境設定ペイン

Sophos SafeGuard Enterprise for Mac をインストールすると、「**システム環境設定**」に Sophos SafeGuard アイコンが表示されます。

アイコンをクリックすると、Sophos SafeGuard 環境設定ペインが開きます。

「**バージョン情報**」タブが表示されます。お使いの Mac にインストールされている製品バージョンに関する情報が表示されます。

2.1 「Server」タブ

「**Server**」(サーバー) タブには、SafeGuard Enterprise サーバーに関連した次の情報や機能が表示されます。

Server Info (サーバー情報)

- **Contact interval:** サーバーとの同期間隔。
- **Last Contacted:** 前回サーバーと同期した日時。
- **Primary Server URL:** プライマリサーバーの URL。
- **Secondary Server URL:** セカンダリサーバーの URL。
- **Server Verification:** サーバーに接続するための SSL サーバー検証が有効であるかどうかを表示。

Drag configuration zip file here (構成 ZIP ファイルをここにドラッグ＆ドロップする)

このドロップゾーンに構成 ZIP ファイルをドラッグ＆ドロップして、SafeGuard Enterprise サーバーから Mac に構成内容を適用します。

Synchronize (同期)

SafeGuard Enterprise サーバーと手動で同期するには、このボタンをクリックします。

Check Connection (接続のチェック)

SafeGuard Enterprise サーバーとの接続を確認するには、このボタンをクリックします。

Company Certificate (企業証明書)

- **Valid from:** 証明書の有効期限の開始日時
- **Valid to:** 証明書の有効期限の終了日時
- **Issuer:** 証明書の発行元インスタンス
- **Serial:** 企業証明書のシリアル番号

2.2 「User」タブ

「**User**」(ユーザー) タブには次の情報が表示されます。

- **Username**: ユーザー名。
- **Domain**: Mac の所属するドメインディレクトリ。ローカルユーザーに対しては、ローカルコンピュータ名が表示されます。

- **SafeGuard User GUID**: 初回ログイン時に生成されるユーザー GUID。
- **SafeGuard User State**: ユーザーの状態 (**SGN user** (SGN ユーザー) または **Unconfirmed user** (認証されていないユーザー)) を表示。認証されていないユーザーは、暗号化されているファイルを開いたり、作成したりすることはできません。このような場合は、セキュリティ担当者にアカウントを認証するよう依頼してください。

2つ目のパネルには、「**User Certificate**」(ユーザー証明書) に関する情報が表示されます。これは、File Encryption のみで使用できます。

- **Valid from:** 証明書の有効期限の開始日時
- **Valid to:** 証明書の有効期限の終了日時
- **Issuer:** 証明書の発行元インスタンス
- **Serial:** 証明書のシリアル番号

3つ目のパネルでは、各コンポーネントに対するアイコンをシステムメニューに表示するかどうかを選択できます。各オプションは、該当するコンポーネントがインストールされている場合のみに表示されます。

- **Show System Menu for Native Device Encryption** (Native Device Encryption のシステムメニューを表示する)
- **Show System Menu for File Encryption** (File Encryption のシステムメニューを表示する)

2.3 「Keys」タブ

このタブは、SafeGuard File Encryption がインストールされている場合のみに表示されます。

「**Keys**」(鍵) タブには、すべての鍵の名前が一覧表示されます。

画面右下の「**Number of Keys**」(鍵の数) の横にあるリストアイコンをクリックすると、鍵の GUID 情報の表示/非表示を切り替えられます。

「**Key Name**」(鍵名) または「**Key GUID**」(鍵 GUID) というヘッダを使って鍵を一覧表示したり、ソートしたりできます。

青字で表示される鍵は、ユーザーの個人鍵です。ローカル鍵は緑色で表示されます (詳細は、ローカル鍵の使用 (p. 15)を参照してください)。それ以外の (標準の) 鍵は、黒で表示されます。

2.4 「Policies」タブ

このタブは、SafeGuard File Encryption がインストールされている場合のみに表示されます。

「**Policies**」(ポリシー) タブの右下に表示される各アイコンをクリックすると、「**Locally Translated Path**」(ローカル変換されたパス) ビューや、「**Received Policies**」(受信したポリシー) ビューに切り替わります。

- 「**Locally Translated Path**」(ローカル変換されたパス) ビューには、この時点で特定の Mac にログインしているユーザーに適用されるポリシーのみが表示されます。表の各列には次の情報が表示されます。
  - **@**: 初期暗号化や容量の大きなファイルの暗号化を行う際、暗号化処理が終わるまで、一番左側の列に丸い回転マークが表示されます。
  - **Locally Translated Path** (ローカル変換されたパス): Mac での場所が表示されます。
  - **Mode** (モード): 暗号化対象の場所、または対象から除外する場所であるかが表示されます。
  - **Scope** (範囲): サブフォルダの暗号化を実行するかどうかが表示されます。

  - **Key Name** (鍵名): 対象の場所に割り当てられた鍵の名前が表示されます。

    ユーザーの個人鍵は、青色で表示されます。

    オレンジ色で表示される鍵は、ユーザーに適用されているポリシーで設定されたものです。しかし、鍵リングに割り当てられていないため、ユーザーはこの鍵を所有していません。このため、データにアクセスする際、問題が発生することがあります。この場合は、セキュリティ担当者までお問い合わせください。

- 「**Received Policies**」(受信したポリシー) ビューには、サーバーから受信したポリシーすべてが表示されます。表には次の情報が含まれます。
  - **Received Policies** (受信したポリシー): 暗号化対象のファイルやフォルダが表示されます。
  - これ以外の列には、前述の「**Locally Translated Path**」(ローカル変換されたパス) ビューと同じ情報が表示されます。

「Locally Translated Path」ビューでのポリシーの適用

- 何もポリシーが選択されていない場合は、「**Enforce all Policies**」(すべてのポリシーの適用) ボタンをクリックして初期暗号化を開始できます。詳細は、ポリシーに基づいたファイルの暗号化 (p. 11)を参照してください。
- ポリシーを選択する際、「**Enforce Policy**」(ポリシーを適用) ボタンをクリックして、選択したポリシーのみを適用することができます。
- ポリシーを選択する際、「**Show in Finder**」(Finder で表示) ボタンをクリックして、選択した暗号化対象フォルダを Finder で開くことができます。

ポリシーの適用によるファイルへの変更

- 平文のファイルは、ポリシーで適用された鍵で暗号化されます。
- ポリシーで指定された鍵で暗号化済みのファイルは、暗号化された状態が維持されます。
- 別の鍵で暗号化済みのファイルは、次のいずれかの方法で処理されます。
  - 対応する鍵がユーザーの鍵リングにない場合は変更されません。または
  - ユーザーの鍵リングにポリシーで割り当てられた暗号化鍵がある場合は、その鍵で再暗号化されます。
- 暗号化対象から除外されているフォルダにあるファイルは復号化されます。
- 権限がないためアクセスできないファイル (読み取り専用ファイル) は変更されません。

2.5 「Disk Encryption」タブ

このタブは、SafeGuard Native Device Encryption がインストールされている場合のみに表示されます。

「**Disk Encryption**」(ディスク暗号化) には、現在のポリシーおよび Mac の暗号化の状態が表示されます。

1つ目のパネルには、システムディスクの暗号化が、セキュリティ担当者によってポリシーで指定されているかが表示されます。

2つ目のパネルには、Mac の状態が表示されます。次のいずれかが表示されます。

- The system disk is encrypted and a centrally stored recovery key is available. (システムディスクが暗号化されており、集中管理されている復旧鍵があります。)
- The system disk is encrypted but there is no centrally stored recovery key available. (システムディスクは暗号化されていますが、集中管理されている復旧鍵がありません。)
- The system disk is not encrypted. (システムディスクは暗号化されていません。)

画面の下に「**Decrypt System Disk**」(システムディスクの復号化) ボタンが表示されます。このボタンは、セキュリティ担当者が、暗号化が不要であるとポリシーで指定したエンドポイントで使用できます。

3 操作方法

3.1 コンピュータの暗号化

セキュリティ担当者によって Synchronized Encryption ポリシーが適用されると、macOS パスワードの入力を促すダイアログが表示されます。入力すると、コンピュータの暗号化が開始します。

1. macOS のパスワードを入力します。
2. 「**Enable**」(有効化) または「**Enable and Restart**」(有効化して再起動) をクリックします。
   Apple File System (APFS) フォーマットを使用している Mac では再起動の必要がないため、「**Enable**」(有効化) オプションのみが表示されます。

ディスク暗号化はバックグラウンドで処理されるので、ユーザーは通常の作業を続行することができます。詳細は、SafeGuard Native Device Encryption (p. 1)を参照してください。

暗号化が有効にならない場合は、管理者にお問い合わせください。

3.2 コンピュータの復号化

通常、復号化の操作は必要はありません。暗号化済みの Mac に対して、暗号化を行わないというポリシーをセキュリティ担当者が適用した場合でも、暗号化された状態が維持されます。ただし、この場合、復号化することを選択できます。環境設定ペインの該当するボタンを使用します。詳細は、「Disk Encryption」タブ (p. 7)を参照してください。

3.3 パスワードを忘れた場合のリセット

パスワードを忘れたときのリセット手順は、Mac にインストールされている暗号化の種類によって異なります。

- SafeGuard Native Device Encryption (p. 9)
- SafeGuard Native Device Encryption および SafeGuard File Encryption (p. 10)

3.3.1 SafeGuard Native Device Encryption

macOS パスワードを忘れた場合は、次の手順を実行します。

1. Mac の電源を入れます。
2. 「**パスワード**」フィールドの疑問符マークをクリックします。
   パスワードのヒントが表示され、復旧鍵を使用してパスワードをリセットするかどうかを確認するメッセージが表示されます。
3. メッセージの横の矢印アイコンをクリックして復旧鍵フィールドを表示します。
4. セキュリティ担当者に復旧鍵を要求します。
5. 該当するフィールドに復旧鍵を入力して、右側の矢印アイコンをクリックします。
   Mac が起動して、「**Reset Password**」(パスワードのリセット) ダイアログが表示されます。

6. Active Directory ユーザーの場合、管理者にパスワードのリセットを依頼して、新しいパスワードを入手します。
   a) コンピュータが、Active Directory ドメインサービスに接続していることを確認します。
   b) 「**Reset Password**」(パスワードのリセット) ダイアログで、「**Cancel**」(キャンセル) をクリックして新しいパスワードを入力します。
   c) 必要に応じて、パスワードを再設定します。
7. macOS のローカルユーザーの場合は、新しいパスワードとパスワードのヒントを入力し、「**Reset Password**」(パスワードのリセット) をクリックします。
8. システムでログインキーチェーンをロック解除できない場合は、「**Create New Keychain**」(キーチェーンの新規作成) をクリックします。
9. APFS フォーマットのシステムディスクを使用する macOS 10.13 搭載の Mac では、新しい復旧パスワードを作成するのに新しいパスワードが必要となる場合があります。メッセージが表示されたら、パスワードを入力します。

   このメッセージは、SafeGuard Enterprise Server に接続しているときのみに表示されます。接続していない場合は、次回接続した際にメッセージが表示されます。

3.3.2 SafeGuard Native Device Encryption および SafeGuard File Encryption

ここで説明する手順は、SafeGuard Native Device Encryption と SafeGuard File Encryption の両方がインストールされていることを前提に書かれています。上記のいずれか 1つのみを使用している場合は、手順が異なることがあります。

macOS パスワードを忘れた場合は、次の手順を実行します。

1. Mac の電源を入れます。
2. 「**パスワード**」フィールドの疑問符マークをクリックします。
   パスワードのヒントが表示され、復旧鍵を使用してパスワードをリセットするかどうかを確認するメッセージが表示されます。
3. メッセージの横の矢印アイコンをクリックして復旧鍵フィールドを表示します。
4. セキュリティ担当者に復旧鍵を要求します。セキュリティ担当者は、SafeGuard Management Center で、該当するユーザー証明書も削除する必要があります。
5. 該当するフィールドに復旧鍵を入力して、右側の矢印アイコンをクリックします。
   Mac が起動して、「**Reset Password**」(パスワードのリセット) ダイアログが表示されます。
6. Active Directory ユーザーの場合、管理者にパスワードのリセットを依頼して、新しいパスワードを入手します。
   a) コンピュータが、Active Directory ドメインサービスに接続していることを確認します。
   b) 「**Reset Password**」(パスワードのリセット) ダイアログで、「**Cancel**」(キャンセル) をクリックして新しいパスワードを入力します。
   c) 必要に応じて、パスワードを再設定します。
7. macOS のローカルユーザーの場合は、新しいパスワードとパスワードのヒントを入力し、「**Reset Password**」(パスワードのリセット) をクリックします。
8. 「**Create New Keychain**」(新しいキーチェーンを作成) をクリックします。
   新しいログインキーチェーンが作成されます。キーチェーンの既存のエントリは、有効のまま残ります。
9. APFS フォーマットのシステムディスクを使用している macOS 10.13 搭載の Mac では、復旧パスワードを新規作成する際に新しいパスワードが必要となる場合があります。メッセージが表示されたら、パスワードを入力します。

このメッセージは、SafeGuard Enterprise Server に接続しているときのみに表示されます。接続していない場合は、次回接続した際にメッセージが表示されます。

10. 新しいパスワードを入力して、SafeGuard ユーザー証明書を作成します。
Active Directory のユーザーの場合、ユーザーの鍵は SafeGuard Enterprise の鍵リングに自動的に取り込まれます。ドキュメントにはこれまでと同様にアクセスできます。
11. ローカルユーザーの場合は、ユーザー登録を確認するよう、セキュリティ担当者に依頼します。
12. 環境設定ペインの「**Server**」(サーバー) タブを開き、「**Synchronize**」(同期) をクリックします。

鍵が復元され、暗号化されたドキュメントに再びアクセスできるようになります。

3.4 Device Encryption の復旧鍵の集中管理

集中管理されている復旧鍵がない場合、ヘルプデスク担当者はパスワードの復旧を支援できません。集中管理されている復旧鍵を利用するには、次のコマンドラインで復旧鍵をインポートします: sgdeadmin --import-recoverykey。この操作を行うと、必要なときにセキュリティ担当者から復旧鍵を入手できるようになります。

復旧鍵が不明な場合は、セキュリティ担当者に問い合わせてください。ログオンパスワードを忘れた場合、使用できる復旧鍵がないと、暗号化されたディスク上のデータはすべて失われてしまうのでご注意ください。

3.5 ポリシーに基づいたファイルの暗号化

セキュリティ担当者は、暗号化するファイルおよび使用する鍵を、ポリシーを使用して定義します。コンピュータにある機密ファイルが暗号化されるようにするには、初期暗号化を実行することを推奨します。この場合、セキュリティ担当者によって適用されたポリシーすべてが施行されます。初期暗号化を開始する方法は次のとおりです。

1. 「**システム環境設定**」を開きます。
2. Sophos SafeGuard アイコンをクリックします。
3. 「**Policies**」(ポリシー) タブを選択します。
4. 「**Locally Translated Path**」(ローカル変換されたパス) ビューに切り替え、「**Enforce all policies**」(すべてのポリシーの適用) をクリックします。

暗号化対象フォルダ (p. 4)にあるファイルすべては、ポリシーで指定されている鍵を使用して、暗号化または再暗号化されます。

1つのポリシーを適用する場合は、該当するポリシーを選択して「**Enforce Policy**」(ポリシーの適用) をクリックします。

特定のファイルやフォルダをポリシーに従って暗号化する場合は、ファイルやフォルダを右クリックして、「**Encrypt According to Policy**」(ポリシーに基づいて暗号化) をクリックします。

3.6 ファイルの手動暗号化/復号化

SafeGuard File Encryption では、個々のファイルを手動で暗号化/復号化できます。ファイルを右クリックして、次のいずれかを実行してください。

- **暗号化の状態の表示**: ファイルが暗号化されているかどうか、および使用された鍵が表示されます。

- **ポリシーに基づいて暗号化**: ポリシーで指定されている鍵を使用して、選択したファイルを暗号化または再暗号化できます。
- **選択したファイルの復号化** (アプリケーションベースのファイル暗号化のみ): ファイルを復号化して、平文で保存できます。ファイルの復号化は、機密データが含まれていない場合のみに実行することを推奨します。
- **選択したファイルの暗号化** (アプリケーションベースのファイル暗号化のみ): ポリシーで指定されている鍵を使用して、ファイルを手動で暗号化できます。
- **ファイルのパスワード保護**: 個々のファイルに手動でパスワードを設定して暗号化できます。これは、社外のユーザーとファイルを安全に共有する際に便利です。詳細は、ファイルのパスワード保護 (p. 12)を参照してください。このオプションは、暗号化されていないファイル、またはファイルの送信者の鍵リングにある鍵を使用して暗号化されたファイルに対してのみ実行できます。

3.7 ファイル暗号化の対象の場所の表示

セキュリティ担当者は、暗号化する/暗号化しないファイルの場所をポリシーで定義します。ポリシーの詳細は次のようにして参照できます。

1. 「**システム環境設定**」を開きます。
2. Sophos SafeGuard アイコンをクリックします。
3. 「**Policies**」(ポリシー) タブを選択します。詳細は、「Policies」タブ (p. 6)を参照してください。

3.8 暗号化されたファイルのメール送信

暗号化されたファイルを社内のユーザーに送信する際、暗号化や復号化を手動で行う必要はありません。適切な鍵がある受信者は、ファイルの内容を読むことができます。

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。詳細は、ファイルのパスワード保護 (p. 12)を参照してください。

パスワード保護を使用せずに社外のユーザーにメールを送信する場合は、送信前にファイルを復号化するようにしてください。復号化しないと、受信者は暗号化されたファイルにアクセスできなくなることにご注意ください。

3.9 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。
   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。
2. 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。

3. 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
4. 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。

3.10 クラウドにあるファイルの暗号化

Sophos SafeGuard は、次の条件が満たされている場合、クラウドにあるファイルを自動的に暗号化します。

- クラウドストレージのフォルダにあるファイルの暗号化を管理者が指定している。
- クラウドストレージのフォルダが、暗号化対象フォルダ外にある (詳細は、暗号化対象フォルダ (p. 4)を参照してください)。
- 対応している、次のクラウド ストレージ サービスのいずれかを使用している:
  - Box
  - Dropbox
  - Google ドライブ
  - Microsoft OneDrive
  - Microsoft OneDrive for Business

クラウドストレージのフォルダが、暗号化対象のフォルダであるかどうかは、環境設定ペインの「**Policies**」タブで確認できます。詳細は、「Policies」タブ (p. 6)を参照してください。

注

- 暗号化されたファイルには、クラウド ストレージ サービスのオーバーレイアイコンでなく、Sophos SafeGuard のオーバーレイアイコンが表示されます。
- クラウドにある暗号化されたファイルを、複数のユーザーが同時に表示/編集することはできません。

3.11 リムーバブルデバイス上のファイルの暗号化

リムーバブルデバイスをコンピュータに挿入すると、デバイス上のファイルの処理方法を確認するダイアログが表示されます。選択できるオプションは次のとおりです。

1. 「**Remember setting and do not show this dialog again**」(この設定を保存し、次回からこのダイアログを表示しない) を選択して、「**No**」をクリックする。
   このデバイス上のファイルは、常時、暗号化されなくなります。
2. 「**Remember setting and do not show this dialog again**」(この設定を保存し、次回からこのダイアログを表示しない) を選択して、「**Yes**」をクリックする。
   このデバイスに新しいファイルを保存すると、そのファイルは暗号化されるようになります。
3. 「**Encrypt existing files**」(既存のファイルを暗号化する) を選択して、「**Yes**」をクリックする。
   デバイスがコンピュータに接続している限り、既存のファイルが保存され、またデバイスに新しいファイルを保存した場合にもファイルは暗号化されるようになります。
4. 「**Remember setting and do not show this dialog again**」(この設定を保存し、次回からこのダイアログを表示しない) および「**Encrypt existing files**」(既存のファイルを暗号化する) を選択して、「**Yes**」をクリックする。
   デバイス上の既存のファイルと新規ファイルの両方が、常に自動で暗号化されるようになります。

3.12 リムーバブルデバイスを使用した、暗号化されたファイルの交換

USB メモリや外付けハードディスクなどのリムーバブルデバイスを使用して、暗号化されたファイルを交換することができます。

リムーバブルデバイス上のデータを他のユーザーと交換・変更するには、両方のユーザーに適切なポリシーと鍵が割り当てられている必要があります。

macOS エンドポイントと Windows エンドポイントとの間でデータ交換を行うには、デバイスが FAT32 形式でフォーマットされている必要があります。他のファイル形式でフォーマットされている場合でも、限定された機能で動作する場合があります。Finder にはファイル形式が表示されないため、ファイルシステムをチェックするにはディスクユーティリティを使用してください。

リムーバルデバイスを使用してサイズの大きいファイルを交換する場合は、交換するファイルの容量の 2倍以上の空き容量がデバイスにあることを確認してください。

Time Machine バックアップにも使用されるリムーバブルデバイスの場合、Backups.backupdb ディレクトリは暗号化から自動的に除外されます。

3.13 ローカル鍵の使用

ローカル鍵は、ロケーションベースのファイル暗号化 (p. 3)のみで使用できます。

ローカル鍵は、リムーバブルデバイスやクラウド ストレージ サービス上の指定されているフォルダ内のファイルを暗号化する際に使用します。このようなフォルダは、暗号化ポリシーで事前に指定しておく必要があります。

ローカル鍵を作成する方法は次のとおりです。

1. エンドポイントが SafeGuard Enterprise サーバーに接続していることを確認します。詳細は、「Server」タブ (p. 5)を参照してください。
2. 1つまたは複数のファイルを右クリックして、「**新しい鍵の作成**」を選択します。
3. 鍵の名前とパスフレーズを入力して、「**OK**」をクリックします。
   鍵名には、「Local_」という文字が先頭に、日時が末尾にそれぞれ追加されます。

ローカル鍵が作成され、鍵リングに追加されます。これで、ローカル鍵をリムーバブルデバイスやクラウドのフォルダに適用できるようになりました。

3.14 暗号化されたファイルの検索

暗号化されたファイルを検索する場合は、手動で Spotlight を有効に設定する必要があります。

1. Spotlight の検索を有効にするには、次のターミナルコマンドを実行します。
   sgfsadmin --enable-spotlight
2. Spotlight の検索を無効にするには、次のターミナルコマンドを実行します。
   sgfsadmin --disable-spotlight

注
Spotlight を Sophos SafeGuard と併用すると、検索速度が遅くなる可能性があります。

3.15 暗号化ファイルの復旧

ファイルの暗号化に使用された鍵が鍵リングに含まれていない場合、そのファイルを開くことはできません。鍵がない理由として、ファイルへのアクセスが社内ポリシーで許可されていないことが考えられます。また、許可されてはいるものの、何らかの理由で必要な鍵を持っていない可能性もあります。この場合、使用された鍵を特定した後、それを鍵リングに割り当てるよう、セキュリティ担当者に依頼する必要があります。次の手順を実行します。

1. ファイルを右クリックして、ショートカット メニューから「**暗号化の状態の表示**」を選択します。
   このファイルの暗号化に使用された鍵が表示されます。
2. セキュリティ担当者にその鍵名を伝えます。
3. この鍵を鍵リングに割り当てるようにセキュリティ担当者に依頼します。
4. セキュリティ担当者がユーザーポリシーを更新したことが確認できたら、「**システム環境設定 > Sophos SafeGuard > Server**」を開きます。
5. 「**Synchronize**」(同期) ボタンをクリックします。
6. 「**Keys**」(鍵) タブを開き、リストに必要な鍵があるかどうかを確認します。

ファイルの暗号化に使用された鍵が「**Keys**」(鍵) タブのリストにある場合は、そのファイルを開くことができます。

3.16 SafeGuard Enterprise サーバーへの接続の確認

エンドポイントと SafeGuard Enterprise サーバーの同期に問題が発生している場合は、次の手順を実行してください。

1. 「Sophos SafeGuard 環境設定ペイン (p. 5)」を開き、「「Server」タブ (p. 5)」をクリックします。
2. 「**Check Connection**」(接続の確認) ボタンをクリックします。
   「**Check SafeGuard Enterprise Client-Server Connectivity**」(SafeGuard Enterprise クライアント/サーバー間の接続の確認) ウィンドウが開きます。
3. 「**Run**」(実行) をクリックします。
   SafeGuard Enterprise サーバーへの接続が、システムによって確認されます。
4. ウィンドウ下部の「**Export**」(エクスポート) ボタンをクリックすると、結果をテキストファイルとして保存できます。
5. SafeGuard Enterprise サーバーへの接続に失敗した場合は、管理者に問い合わせてください。

4 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

5 利用条件