SOPHOS
Security made simple.

Sophos SafeGuard File Encryption for Mac 管理者ヘルプ

製品バージョン: 7
ドキュメント作成日: 2014年 12月

目次

1 Sophos SafeGuard File Encryption for Mac について

Sophos SafeGuard File Encryption for Mac は、Sophos SafeGuard Enterprise によって Windows 環境に提供されるデータ保護機能を Mac 環境に拡張したものです。ローカルドライブ、ネットワーク共有、リムーバブルドライブ、およびクラウドストレージにあるファイルを暗号化します。

SafeGuard File Encryption for Mac を使用して暗号化・復号化したファイルは、他の Mac ユーザーや Windows PC ユーザーと安全に交換することができます。

SafeGuard Enterprise で暗号化されたファイルをモバイルデバイスで読む場合は、Sophos Mobile Encryption for iOS または Android を使用してください。

SafeGuard Management Center にある「File Encryption」ポリシーで、ファイル ベースの暗号化のルールを定義します。File Encryption ポリシーでは、File Encryption で暗号化するフォルダ、暗号化モード、および暗号化に使用する鍵を指定します。この集中管理機能により、複数のプラットフォームで、常に同じフォルダや暗号化鍵を使用することができます。

1.1 このドキュメントについて

このドキュメンでは、Sophos SafeGuard File Encryption for Mac のインストール、設定、および管理方法について説明します。

SafeGuard Management Center の操作方法とポリシーの設定方法に関する詳細は、「**SafeGuard Enterprise 管理者ヘルプ**」を参照してください。

ユーザー向け情報の詳細は、「**Sophos SafeGuard File Encryption for Mac クイック スタートアップガイド**」を参照してください。

1.2 用語と略語

このドキュメントで使用している用語と略語は次のとおりです。

用語、略語	意味、説明
FUSE	Filesystem in user space (http://osxfuse.github.io/ (英語) を参照)
GUID	Globally Unique Identifier: コンピュータのソフトウェアを識別するための一意の参照番号。
保護されたフォルダ	保護されたフォルダは、SafeGuard Management Center で作成されたルールが適用されるフォルダ

用語、略語	意味、説明
	です。このルールによって、フォルダのコンテンツの暗号化が指定されます。
SSL	Secure Sockets Layer: インターネット通信にセキュリティを提供する暗号化プロトコル。

2 インストール

ここでは、Sophos SafeGuard File Encryption を Mac OS X クライアントにインストールする方法について説明しています。管理環境 (バックエンド) へのインストール方法の詳細は、「**SafeGuard Enterprise インストールガイド**」を参照してください。

Mac OS X クライアントへは、次の 2とおりの方法でインストールできます。

- 手動 (有人) インストール
- 自動 (無人) インストール

注: SafeGuard Disk Encryption 6.01 以前をインストール済みの場合は、それをアンインストールしてから、SafeGuard File Encryption for Mac バージョン 7 をインストールする必要があります。

SafeGuard File Encryption と SafeGuard Native Device Encryption (バージョン 6.10 までの名称は SafeGuard Disk Encryption です) の両方を使用する場合は、共にバージョン 7 である必要があります。1台の Mac で、この 2つの製品の異なるバージョンを使用することはできません。

インストーラパッケージは署名付きで、OS X はこの署名を検証しようとします。インターネット接続が遅かったり、設定に問題があると、インストール操作中に最高 20分の待機時間が発生する場合もあります。

2.1 インストールの前提要件

インストールを開始する前に、次のようにして SafeGuard Enterprise-SSL サーバー証明書をシステムのキーチェーンにインポートし、SSL に対して「**常に信頼**」オプションを設定してください。

注: ログイン キーチェーンには保存しないでください。

1. SafeGuard のサーバー管理者から、SSL 用の証明書 (**<証明書名>.cer** ファイル) を取得します。
2. キーチェーンに **<証明書名>.cer** ファイルをインポートします。それには、「**アプリケーション**-**ユーティリティ**」で、「**キーチェーンアクセス.app**」をダブルクリックします。
3. 左側のペインで、「**システム**」を選択します。
4. Finder ウィンドウを開き、上記の **<証明書名>.cer** ファイルを選択します。
5. この証明書ファイルを、「システム」の「キーチェーンアクセス」ウィンドウにドラッグ&ドロップします。
6. Mac OS X パスワードを入力するようメッセージが表示されます。
7. パスワードの入力後、「**キーチェーンを変更**」をクリックして操作を確認します。
8. 次に、**<証明書名>.cer** ファイルをダブルクリックします。「**信頼**」の横にある矢印をクリックして、信頼の設定を表示します。
9. 「**SSL (Secure Sockets Layer)**」に対して、「**常に信頼**」オプションを選択します。
10. ダイアログを閉じます。Mac OS X パスワードを入力するようメッセージが再表示されます。

11. パスワードを入力し、「**設定をアップデート**」をクリックして確定します。証明書アイコンの右下隅に、すべてのユーザーに対してこの証明書が信頼されていることを示す青い「+」記号が表示されます。

12. Web ブラウザを開き、次のように入力して SafeGuard Enterprise サーバーを使用できることを確認します。**`https://<サーバー名>/SGNSRV`**

これでインストールを行う準備ができました。

注:

証明書のインポートは、`sudo /usr/bin/security add-trusted-cert -d -k /Library/Keychains/System.keychain -r trustAsRoot -p ssl "/<フォルダ名>/<証明書名>.cer"` というコマンドでも実行できます。このコマンドはスクリプトによる自動インストールにも使用できます。お使いの設定に応じてフォルダ名と証明書名を変更してください。

注:

ここで説明している手順を飛ばす場合は、`sudo sgfsadmin --disable-server-verify` コマンドを実行してください。詳細は、コマンドラインオプション (p. 21) を参照してください。このコマンドは、セキュリティの脆弱性につながる恐れがあるので推奨されません。

2.2 手動 (有人) インストール

手動 (有人) インストールでは、各操作段階でインストールを管理・テストすることができます。インストールは、1台の Mac に対して実行します。

注:

FUSE for OS X (OSXFUSE) バージョン 2.7.0 以降がインストール済みであることを確認してください。FUSE for OS X、およびダウンロードオプションの詳細は、http://osxfuse.github.io/ (英語) を参照してください。

インストールの前提要件 (p. 5) にある説明に従って、サーバーの接続を正しく設定しておくようにしてください。

1. **Sophos SafeGuard FE.dmg** を開きます。
2. 提供されるリリースノートを参照後、**Sophos SafeGuard FE.pkg** をダブルクリックして、インストールウィザードの指示に従います。ソフトウェアを新規インストールするため、パスワードの入力が求められます。製品は、**/Library/Sophos SafeGuard FS/** フォルダにインストールされます。
3. 「**Close**」(閉じる) をクリックして、インストールを完了します。
4. 「**システム環境設定**」を開き、Sophos Encryption アイコンをクリックして製品の設定画面を表示します。

5. 「**Server**」(サーバー) タブをクリックします。

6. サーバーと証明書の詳細が表示されている場合は、以下の手順を飛ばしてステップ 11 に進み、「**Synchronize**」(同期) をクリックしてください。何も表示されていない場合は、以下の手順を実行してください。
7. ZIP 形式の構成パッケージを選択します (Mac エンドポイント用の構成パッケージの作成方法の詳細は、「**SafeGuard Enterprise 管理者ヘルプ**」の「**構成パッケージについて** > **Mac 用の構成パッケージの作成**)」を参照)。
8. 「**Server**」(サーバー) ダイアログ内の指定されたエリアに、ZIP ファイルをドラッグ & ドロップします。
9. Mac の管理者パスワードを入力するようメッセージが表示されます。パスワードを入力し、「**OK**」をクリックして確認します。
10. Mac パスワードを入力して、SafeGuard ユーザー証明書を要求します。
11. 次のようにして、SafeGuard Enterprise サーバーへの接続を確認します。企業証明書の詳細が、「**Server**」(サーバー) ダイアログの下部に表示されます。「**Synchronize**」(同期) をクリックします。接続に成功すると、「Last Contacted」(前回の接続日時) のタイムスタンプが更新されます。(「**Server**」(サーバー) タブの「**Server Info**」(サーバー情報) エリアの「**Last Contacted**」(前回の接続日時) を参照)。接続に失敗した場合、次のアイコンが表示されます。

    

    詳細は、システム ログ ファイルを参照してください。

    同期とサーバーへの接続の詳細は、「Server」タブ (p. 16) を参照してください。

2.3 リモート管理ソフトウェアを使用した自動 (無人) インストール

自動 (無人) インストールでは、インストール操作中、ユーザーの介入は必要ありません。

このセクションでは、SafeGuard File Encryption for Mac の自動 (無人) インストールの基本的な手順について説明します。実際に行う手順は、使用する管理ソフトウェアによって異なる場合があります。インストール済みの管理ソフトウェアを使用してください。

注:

パッケージは、以下の説明にある順にインストールするようにしてください。

クライアントコンピュータに SafeGuard File Encryption for Mac をインストールする手順は次のとおりです。

1. **Sophos SafeGuardFS.pkg** インストーラファイルをダウンロードします。
2. ファイルを対象マシンにコピーします。
3. ファイルを対象マシンにインストールします。Apple Remote Desktop を使用している場合、ステップ 2 と 3 は 1つの手順になります。
4. ZIP 形式の構成パッケージを選択し、対象マシンにコピーします (Mac 用の構成パッケージの作成方法の詳細は、「**SafeGuard Enterprise 管理者ヘルプ**」の「**構成パッケージについて** > **Mac 用の構成パッケージを作成する**」を参照)。

5. 対象マシンで次のコマンドを実行します。

   ```
   /usr/bin/sgfsadmin --import-config /full/path/to/file.zip
   ```

   /full/path/to/file には、適切なパスを指定します。このコマンドは、管理者権限で実行する必要があります。Apple Remote Desktop を使用している場合は、「**ユーザー名**」フィールドに「**`root`**」を入力して、コマンドを実行したユーザーを指定します。

6. 使用している管理ソフトウェア特有の設定に従って、随時、対象マシンのシャットダウンなど、追加の手順を実行してください。

3 推奨事項、制限事項

3.1 推奨事項

管理負荷を抑える

- マウントポイント (つまり、保護されたフォルダ) の数を最小限に抑えてください。
- **「モバイルアカウントを作成する前に確認を要求」オプションを無効にする**

  Mac エンドポイント用のモバイルアカウントを作成/使用する場合、「**モバイルアカウントを作成する前に確認を要求**」を無効にするようにしてください。このオプションが有効になっていると、ユーザーは、「Don't Create」（作成しない） を選択することができます。これによって、ローカル ホーム ディレクトリのないユーザーなど、不完全な OS X ユーザーが作成されてしまいます。

  このオプションを無効にするには、次の手順を実行してください。

  1. 「**システム環境設定**」を開いて、「**ユーザとグループ**」をクリックします。
  2. ロックアイコンをクリックして、パスワードを入力します。
  3. ユーザーを選択します。
  4. 「**ログインオプション**」をクリックします。
  5. 「**ネットワークアカウントサーバ**」で、「**編集...**」をクリックします。
  6. Active Directory ドメインを選択します。
  7. 「**ディレクトリユーティリティを開く...**」をクリックします。
  8. ロックアイコンをクリックして、パスワードを入力し、「**設定を変更**」をクリックします。
  9. Active Directory を選択して、編集アイコンをクリックします。
  10. 「**詳細オプションを表示**」の左側にある矢印をクリックします。
  11. 「**ログイン時にモバイルアカウントを作成**」を選択し、「**モバイルアカウントを作成する前に確認を要求する**」を選択から外します。
  12. 「**OK**」をクリックして確定します。

3.2 制限事項

- **クライアントで設定できる保護されたフォルダ (マウントポイント) の最大数**

  各 Mac OS X クライアントで指定できる保護されたフォルダ (マウントポイント) の数は、最大 24個です。1台のマシンに複数のユーザーがログインしている場合は、ログインしているユーザーすべてのマウントポイントを加算する必要があります。FUSE for OS X を使用する他の製品が Mac にある場合、これらのマウントポイントの数も、最大数 24個に含める必要があります。

- **保護されたフォルダで、バージョン履歴を保存できない**

(これまで変更したことのある) ファイルを保護されたフォルダで開くと、標準機能の「**すべてのバージョンをブラウズ...**」が表示されません。

- **除外するフォルダ**

  暗号化から除外されるフォルダは次のとおりです。

  - **除外されるフォルダ (サブフォルダは除外されない):**
    - <ルート>
    - <ルート>/Volumes/
    - <ユーザープロファイル>/
  - **除外されるフォルダ (サブフォルダも除外される):**
    - <デスクトップ>/
    - <ルート>/bin/
    - <ルート>/sbin/
    - <ルート>/usr/
    - <ルート>/private/
    - <ルート>/dev/
    - <ルート>/Applications/
    - <ルート>/System/
    - <ルート>/Library/
    - <ユーザープロファイル>/Library/
    - /<リムーバブル>/SGPortable/
    - /<リムーバブル>/System Volume Information/

  たとえば、追加パーティションのルート (<ルート>/Volmues) に暗号化ルールを適用した場合、受信したポリシーとして表示されるものの、効果はありません。

  また、<ルート>/abc に適用した暗号化ルールは有効ですが、<ルート>/private/abc に適用した暗号化ルールは無効になります。

- **ファイルを検索する**
  - **Spotlight 検索**

    暗号化されたファイルに対して Spotlight 検索を使用することはできません。したがって、保護されたフォルダで検索を行っても、一致する文字列は返されません。

  - **ラベルの付いたファイル**

    保護されたフォルダで、ラベルの付いたファイルを検索することはできません。

- **CD への書き込み**

  暗号化されたデータを CD に書き込むことはできません。

- **保護されたフォルダの共有**

  保護されたフォルダをネットワークを介して共有することはできません。たとえば、<ドキュメント> フォルダにルールが適用されている場合、このフォルダは共有できなくなります。

- **ファイルを削除する**

  保護されたフォルダ (マウントポイント) からファイルを削除する場合、削除を確認するメッセージが表示されます。削除されたファイルはゴミ箱フォルダに移動されないため、復元することはできません。

- **SafeGuard Portable**

  SafeGuard Portable は Mac OS X では使用できません。

- **Time Machine の使用**

  暗号化されたフォルダに対して Time Machine を使用しても、旧バージョンは表示されません。しかし、Time Machine が有効になっている限り、バックアップは存在します。隠れているだけです。次の手順を実行します。

  - Time Machine を開きます (例: Spotlight 検索で「Time Machine」と入力します)。ルートフォルダのコンテンツが表示されます。
  - 「**Shift - Command - G**」キー (「フォルダへ移動」オプション) を押して、復元対象の暗号化されているフォルダへの隠しパスを入力します。例:通常使用している暗号化フォルダが /Users/admin/Documents の場合
    は、/Users/admin/.sophos_safeguard_Documents/ と入力します。
  - 復元するフォルダを参照し、Time Machine メニューバーの矢印アイコンをクリックして、「**<ファイル名> を復元...**」を選択します。Time Machine からデスクトップに戻ると、ファイルは復元されているので復号化することができます。

    注: 隠しパスにあるファイルのコンテンツを読むことはできません。したがって、バックアップには暗号化されたデータのみが含まれ、ファイルの内容は安全に保護されます。

- **AirDrop の使用**

  AirDrop を使用して、暗号化されたファイルを転送できます。転送先ドライブが、暗号化されたファイルを処理できることを確認してください。できない場合、予期しない動作が発生することがあります。

- **Handoff**

  暗号化したファイルに対して Handoff を使用することはできません。

- **`autofs` でマウントされるネットワークファイル共有**

  ポリシーが適用済みで、起動時に自動的にマウントされるネットワークファイル共有は、Sophos SafeGuard File Encryption によって検出されません。元のマウントポイントを置き換えることができないため、このようなマウントポイントを処理することはできません。

4 環境設定

Sophos SafeGuard File Encryption for Mac OS X は、SafeGuard Management Center で管理されます。以下のセクションでは、Mac 特有の環境設定について説明しています。Management Center の一般的な機能の詳細は、「**SafeGuard Enterprise 管理者ヘルプ**」を参照してください。File Encryption ポリシーの詳細については、「**SafeGuard Enterprise 管理者ヘルプ**」の「ポリシーの設定」セクション、およびその後の各セクションを参照してください。

注:

SafeGuard File Encryption for Mac では、「**File Encryption**」および「**General Settings**」という種類のポリシーのみが使用されます。つまり、ローカルファイルシステム、リムーバブルメディア、ネットワーク共有、およびクラウドストレージにあるデータの暗号化の管理には、「**File Encryption**」ポリシーのみが必要です。「**Device Protection**」ポリシー(「**Cloud Storage**」ポリシーおよび「**Removable Media Encryption**」ポリシーを含む)は、SafeGuard File Encryption for Mac OS X では無視されます。「**File Encryption**」ポリシーは、必ずユーザーオブジェクトに割り当てるようにしてください。エンドポイントに割り当てられた「**File Encryption**」ポリシーは、OS X エンドポイントで無視されます。

注:

SafeGuard Management Center では、バックスラッシュを使用してパスを入力する必要があります。バックスラッシュは、Mac クライアント側でスラッシュに自動変換されます。

4.1 一元管理される環境設定オプション

以下のオプションは、Management Center で一元設定されます。

- **ポリシー**
- **鍵**
- **証明書**

  SafeGuard Enterprise バックエンドは、X.509 証明書をユーザーに提供します。初回ログイン後、証明書が生成されます。証明書は、ユーザーの鍵リングを保護します。ログイン後、証明書を要求する方法の詳細は、「**クイックスタートアップガイド**」を参照してください。

- **サーバーへの接続の間隔**

注: これらのオプションの詳細は、「**SafeGuard Enterprise 管理者ヘルプ**」を参照してください。

4.2 ローカル管理される環境設定オプション

以下のオプションは、Mac クライアントでローカル設定されます。

- **Synchronize database information (データベース情報を同期する)**

`sgfsadmin --synchronize` コマンドを使用して、ポリシー、鍵、証明書などのデータベース情報を Management Center と同期できます。

- **Enable or disable the system menu (システムメニューを有効化/無効化する)**

  `sgfsadmin --enable-systemmenu` コマンドを使用して、右上隅のシステムメニューを有効化できます。

  `sgfsadmin --disable-systemmenu` コマンドを使用して、システムメニューを無効化できます。

  このオプションについての詳細は、Sophos SafeGuard File Encryption システム メニュー (p. 20) を参照してください。

コマンドラインオプションの全容は、コマンドラインオプション (p. 21) を参照してください。

5 File Encryption for Mac の使用

このアプリケーションのユーザー向け情報は、「File Encryption クイック スタートアップ ガイド」を参照してください。最新版の製品ドキュメントは、次の「ドキュメント」ページから入手可能です。http://www.sophos.com/ja-jp/support/documentation.aspx

以下のセクションでは、File Encryption for Mac の使用に関する管理者向け情報について説明しています。

5.1 暗号化について

各暗号化ファイルは、ランダムに生成された DEK (データ暗号化鍵) という鍵で、アルゴリズム AES-256 を使って暗号化されています。このランダムに生成された一意の DEK は暗号化され、ファイルヘッダとして、暗号化されたファイルとともに保存されるため、ファイルサイズは 4KB 大きくなります。

DEK は、KEK (鍵暗号化鍵) によって暗号化されます。この KEK は、中央 SafeGuard Enterprise データベースに保存されます。そして、セキュリティ担当者によって、1人のユーザー、グループ、または組織単位に割り当てられます。

この暗号化ファイルを復号化するには、ファイルに特有の KEK が、ユーザーの鍵リングに存在する必要があります。

5.2 初期暗号化

クライアント側で次の手順を実行してください。

1. 「**システム環境設定**」を開きます。
2. Sophos Encryption 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. まだ開いていない場合は、「**Locally Translated Path**」(ローカル変換されたパス) ビューに切り替えます。これで次の操作を実行できます。
   a) すべてのポリシーを適用します。これには、ウィンドウの下部で「 **Enforce all policies**」(すべてのポリシーの適用) ボタンをクリックします。
   または
   b) ポリシーを 1つ選択して、「**Enforce policy**」(ポリシーの適用) ボタンをクリックします。

注: 初期暗号化の実行中は、デバイスを切断しないようにしてください。

注: ローカル変換されたパスの詳細やコンテンツを表示するには、一覧から該当するパスを選択して、「**Finder に表示**」をクリックします。Finder ウインドウが開き、選択したパスと、該当する場合そのコンテンツが表示されます。

5.3 パスワードについて

Sophos SafeGuard 鍵リングは、ユーザー証明書で保護されています。対応する秘密鍵は、OS X パスワードによって保護されます。

SafeGuard Enterprise でユーザーが作成されていない場合、このパスワードは証明書を生成するために必要です。

ローカルでパスワードを変更する

ユーザーは、「**システム環境設定 > ユーザとグループ**」で、パスワードをローカルで変更することができます。これ以外の手順は不要です。

パスワードが別のエンドポイントで変更された場合

注: パスワードは、Windows エンドポイントおよび Mac エンドポイントで変更できます。

このエンドポイントでは変更されたパスワードが不明なため、次の手順を実行する必要があります。

1. 新しいパスワードで OS X にログオンします。
2. 「**The system was unable to unlock your keychain**」(キーチェーンのロックを解除できませんでした) が表示されます。
3. 「**Update Keychain Password**」(キーチェーン パスワードの変更) を選択します。
4. 古いパスワードを入力します。

忘れたパスワードをリセットする方法の詳細は、Mac OS X ログインパスワードを忘れた場合 (p. 25) を参照してください。

5.4 ユーザーの簡易切り替え

ユーザーの簡易切り替えは、SafeGuard File Encryption for Mac でも有効です。これによって、アプリケーションを閉じたり、マシンからログアウトしたりせずに、1台のエンドポイントでユーザーアカウントを切り替えることができます。

注: OS X FUSE では、最大 24個のマウントポイント (保護されたフォルダ) を指定できます。推奨事項、制限事項 (p. 9) も参照してください。

5.5 環境設定ペイン

環境設定ペインでは、特定のアプリケーションやシステムに対する設定を指定できます。Sophos SafeGuard File Encryption (または Sophos SafeGuard Native Device Encryption) を Mac クライアントにインストールすると、「**システム環境設定**」に、次の環境設定ペインアイコンが表示されます。

アイコンをクリックすると、Sophos Encryption 環境設定ペインが開きます。「**About**」(情報) 画面が表示されます。

メニューバーから、次のタブを開くことができます。

5.5.1 「About」タブ

「**About**」(情報) タブには、Mac OS X クライアントにインストールされている製品のバージョン、および著作権や登録商標に関する情報が表示されます。インストールされている場合は、Sophos SafeGuard Disk Encryption や Native Device Encryption も表示されます。

ウィンドウ下部のリンクをクリックすると、ソフォス Web サイトが開きます。

5.5.2 「Server」タブ

「**Server**」(サーバー) をクリックすると、次の情報と機能が表示されます。

Server Info (サーバー情報)

- **Contact interval:** サーバーとの同期頻度。同期頻度の設定方法の詳細は、「**SafeGuard Enterprise 管理者ヘルプ**」の「ポリシーの設定 > 全般設定」を参照してください。
- **Last Contacted:** クライアントが、前回サーバーに接続した日時。
- **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:** SafeGuard Enterprise サーバーに接続するための SSL サーバー検証が有効または無効であることが表示されます。このオプションの変更方法の詳細は、コマンドライン オプション (p. 21) を参照してください。

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 Management Center から Mac クライアントに構成内容を適用します。詳細は、手動 (有人) インストール (p. 6) を参照してください。

Synchronize (同期)

ポリシーや鍵などのデータベース情報を手動で同期するには、このボタンをクリックします。この操作は、SafeGuard Management Center で設定を変更した後などに必要になることがあります。

同期に失敗すると、次のアイコンが表示されます。

問題が解決しない場合は、プライマリサーバーの URL とセカンダリサーバーの URL を使用して、サーバーへの接続を確認してください。一般的な前提条件については、インストール (p. 5) を参照してください。以前同期に成功した場合は、SSL 証明書の有効期限が切れていることが原因であることも考えられます。考えられる原因に関する情報は、システム ログ ファイルも参照してください。

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

5.5.3 「User」タブ

「**User**」(ユーザー) をクリックすると、次の情報が表示されます。

- **Username**: 現在ログオンしているユーザーのユーザー名。
- **Domain**: クライアントが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**: 初回ログオン後、ユーザーに対して生成された GUID。

2つ目のパネルでは、次のオプションを選択/選択解除できます。

- **Show System Menu for File Encryption**: 選択すると、メニューバーに Sophos SafeGuard アイコンが表示されます。詳細は、Sophos SafeGuard File Encryption システム メニュー (p. 20) を参照してください。

3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。

- **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

5.5.4 「Keys」タブ

「**Keys**」(鍵) をクリックすると、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、各鍵の 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。

5.5.5 「Policies」タブ

「**Policies**」(ポリシー) タブをクリックすると、ポリシーのビューが表示されます。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) には、その時点で特定の 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。
  - @ マーク: 初期暗号化や、容量の大きなファイルの暗号化処理中に、「@」と表示される一番左側の列に、暗号化処理が終わるまで丸い回転マークが表示されます。
  - **Mode** (モード): 「**encrypt**」(暗号化) または「**exclude**」(除外) のどちらかが表示されます。

    注:

    モードの詳細については、「**SafeGuard Enterprise 管理者ヘルプ**」を参照してください。

  - **Scope** (範囲): サブフォルダが暗号化の対象であるかが表示されます。
  - **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。

    青字で表示される鍵は、ユーザーの個人鍵です。

    オレンジ色の文字で表示される鍵は、ユーザーに割り当て済みのポリシーで設定されたことを意味します。しかし、この鍵は、ユーザーの鍵リンクに割り当てられていないため、ユーザーが所有する鍵ではありません。これが原因で、データアクセス時に問題が発生する場合があります。詳細は、データアクセス時に問題が発生する (p. 25) を参照してください。

  「Received Policies」(受信したポリシー) ビューに切り替えるには、タブの右下の「**Policy**」(ポリシー) ビューの右端に表示される以下のアイコンをクリックします。

  

- 「**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。このビューは、SafeGuard Management Center のビューと同じです。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。

保護対象のフォルダを表示し、「Locally Translated Path」ビューでポリシーを適用する

「**Locally Translated Path**」(ローカル変換されたパス) の表でポリシーが選択されている場合 ① は、次の操作を行えます。

- 「**Show in Finder** 」(Finder で表示) ボタン ② をクリックし、保護されたフォルダ (マウントポイント) を Finder ウィンドウで開き、内容を表示する。
- 「**Enforce Policy**」(ポリシーを適用) ③ をクリックし、選択したポリシーを、指定した場所にあるすべてのファイルに適用する。プログレスバーが表示されます。システムで

ポリシーの適用処理が完了するまで待ちます。または、プログレスバーの横にある×マークをクリックして処理をキャンセルします。

注:

ポリシー1つを選択から外す場合は、「**コマンド**」キーを押しながら、該当するポリシーをマウスでクリックします。

注:

書き込み禁止ファイル、または権限がないためアクセスできないファイルは、暗号化の対象から除外されます。

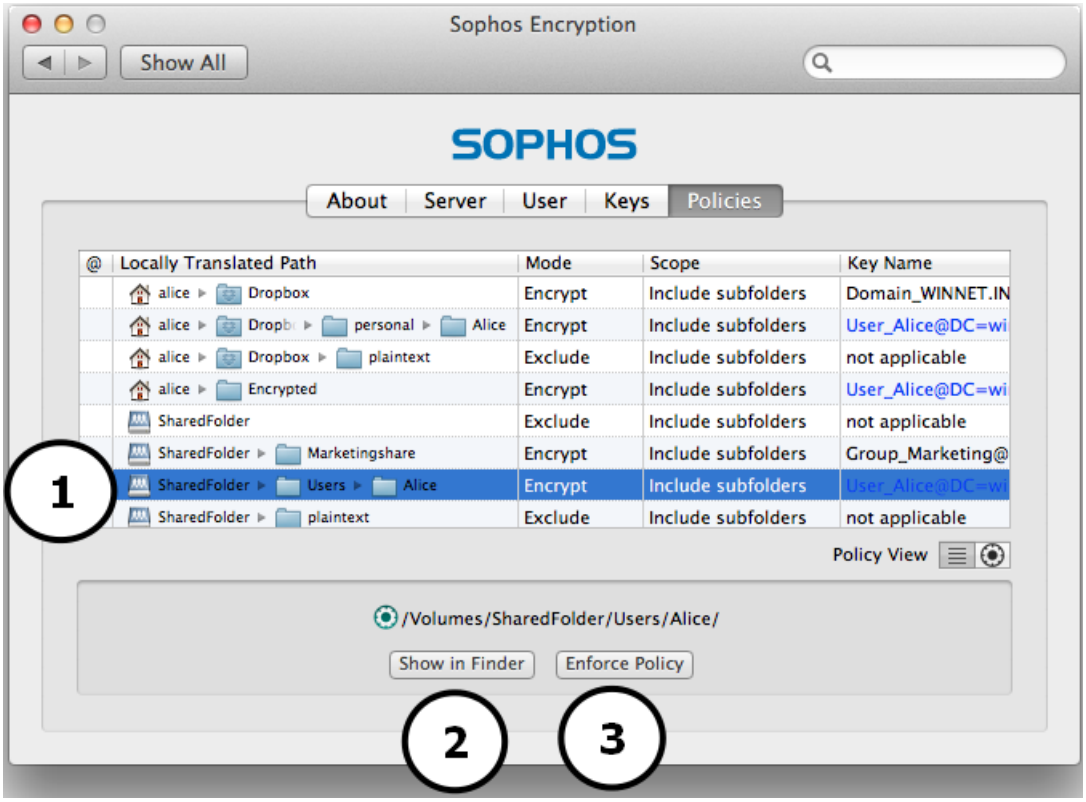

図 1: 「Policies」**タブ画面** - 「Locally Translated Path」**ビュー**

ポリシーを適用後のファイルの処理

ポリシーの適用後、ファイルは次のように処理されます。

- 平文のファイルは、ポリシーで適用された暗号化鍵で暗号化されます。
- ポリシーで指定された暗号化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。
- 別の暗号化鍵で暗号化済みのファイルは、次のように処理されます。
  - ユーザーの鍵リングに対応する暗号化鍵がない場合は、変更されず同じ状態が維持されます。
  - 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、その暗号化鍵で再暗号化されます。

- 複数回暗号化されているファイルは、ポリシーで割り当てられた暗号化鍵で、暗号化が1回行われます。必要な暗号化鍵のいずれか1つを利用できない場合、このようなファイルは可能な限り復号化されます。

5.6 Sophos SafeGuard File Encryption システム メニュー

システムメニューには次のような情報と機能が表示されます。

1. ファイルを選択すると、その暗号化状態と鍵名が自動的にアイコンで表示されます。

	緑色のアイコン:ファイルは暗号化されており、対応する鍵があります。
	赤色のアイコン:ファイルは暗号化されていますが、対応する鍵がありません。
	グレーのアイコン:ファイルは暗号化の対象になっていますが、まだ暗号化されていません。(*)
	黒色のアイコン:ファイルは暗号化から無視または除外されています。

(*) このアイコンが表示される場合の例: 暗号化ポリシーが適用済みのディレクトリにある、暗号化されていないファイルを選択すると、アイコンはグレー表示されます。このファイルを暗号化するには、「**Policies**」(ポリシー) タブを開き、このディレクトリに適用済みのポリシーを選択して、「**Enforce Policy**」(ポリシーの適用) を選択してください。詳細は、「Policies」タブ (p. 17) を参照してください。

2. ファイルの暗号化中、アイコンの外側の輪が回転します。この動作は、ファイルの現在の暗号化状態に依存しません。
3. 選択したファイルやボリュームに応じて、以下のようなメニューアイテムが表示されます。
   - 現在の暗号化や鍵の状態:

     ファイル、ディレクトリ、またはボリュームを選択すると、現在の暗号化の状態に関するメッセージ、必要な鍵の鍵名、およびユーザーがこの鍵を所有するかどうかに関する情報が表示されます。

     注:

     ファイルやディレクトリの現在の暗号化状態や鍵名を表示するには、一度フォーカスをデスクトップなどに移動した後、再びファイルやディスクトリにフォーカスを移動することが必要な場合もあります。

   - 使用可能な SafeGuard の保護されたフォルダ (マウントポイント) の一覧

     注:

     保護されたフォルダのアイコンにカーソルを移動すると、そのフォルダへのフルパスが表示されます。

   - **Open Sophos Encryption Preferences...**

Sophos Encryption 環境設定ペインを表示するためのオプションです。詳細は、環境設定ペイン (p. 15) を参照してください。

5.7 コマンドライン オプション

「ターミナル」アプリケーションを使用して、コマンドやコマンドライン オプションを入力することができます。使用できるコマンドライン オプションは次のとおりです。

コマンド名	定義	追加パラメータ (任意)
`sgfsadmin`	簡単なヘルプ情報の他、使用可能なコマンドの一覧を表示する。	`--help`
`sgfsadmin --version`	インストール済み製品のバージョンおよび著作権情報を表示する。	
`sgfsadmin --status`	バージョン、サーバー、証明書情報などのシステムの状態に関する情報を表示する。	
`sgfsadmin --list-user-details`	現在ログオンしているユーザーに関する情報を表示する。	`--all`: すべてのユーザーに関する情報を表示する (sudo 権限が必要) `--xml`: xml 形式で出力結果を表示する
`sgfsadmin --list-keys`	鍵ストアにある、既存の鍵の GUID と名前の一覧を表示する。	`--all`: すべてのユーザーに関する情報を表示する (sudo 権限が必要) `--xml`: xml 形式で出力結果を表示する
`sgfsadmin --list-policies`	ポリシーに関連した情報を表示する。可能な場合、鍵 GUID は鍵名に解決される。太字は個人鍵を指します。	`--all`: すべてのユーザーに関する情報を表示する (sudo 権限が必要) `--xml`: xml 形式で出力結果を表示する `--raw`: SafeGuard Management Center サーバー側で設定した状態のポリシーを表示する。

コマンド名	定義	追加パラメータ (任意)
`sgfsadmin --enforce-policies`	暗号化ポリシーを適用する。	`--all`: 適用可能なすべてのディレクトリにポリシーを適用する "ディレクトリ名": ポリシーを適用するディレクトリを指定する。
`sgfsadmin --file-status "ファイル名1" ["ファイル名2"..."ファイル名N"]`	ファイルや複数のファイルに関する暗号化情報を表示する。ワイルドカードを使用できます。	`--xml`: xml 形式で出力結果を表示する
`sgfsadmin --import-config "/対象/ファイル/への/パス"`	指定した構成 ZIP ファイルをインポートする。詳細は、手動 (有人) インストール (p. 6) を参照してください。このコマンドの実行には管理者権限 (sudo) が必要です。 **注:** ドラッグ & ドロップ機能を使用して、完全なパスを、Finder などから「ターミナル」アプリケーションにドラッグ & ドロップできます。	
`sgfsadmin --enable-server-verify`	SafeGuard Enterprise サーバーに接続するための SSL サーバー検証を有効にする。インストール後、SSL サーバー検証が有効になります。このコマンドの実行には管理者権限 (sudo) が必要です。	
`sgfsadmin --disable-server-verify`	SafeGuard Enterprise サーバーに接続するためのサーバー検証を無効にする。このコマンドの実行には管理者権限 (sudo) が必要です。 **注:** このコマンドは、セキュリティの脆弱性につながる恐れがあるので推奨されません。	

コマンド名	定義	追加パラメータ (任意)
`sgdeadmin --update-machine-info [--domain "ドメイン名"]`	対象のクライアントを SafeGuard Enterprise サーバーに登録する際に使用される、現在保存されているマシンの情報を更新する。このコマンドの実行には管理者権限 (sudo) が必要です。 **注:** このコマンドは、コンピュータが所属するドメインまたはワークグループが変更された後のみに使用してください。コンピュータが複数のドメインまたはワークグループに所属している場合、このコマンドを実行すると、ドメインの登録が変更されたり、個人鍵や FileVault 2 ユーザーが削除されたりする場合があります。	`--domain "ドメイン名"` SafeGuard Enterprise サーバーへの登録にクライアントが使用するドメイン。このパラメータはマシンが複数のドメインに参加している場合のみに必要です。必ずコンピュータが所属しているドメインを指定してください。そうでない場合、コマンドの実行に失敗します。

以下のコマンドに関する詳細な説明は、ローカル管理される環境設定オプション (p. 12) を参照してください。

- `sgfsadmin --enable-systemmenu`
- `sgfsadmin --disable-systemmenu`
- `sgfsadmin --synchronize`

5.8 リムーバブルデバイスの使用

注:

リムーバブルメディアを使用する前に、リムーバブルメディアにあるファイルの暗号化を許可するポリシーおよび鍵が割り当てられていることを確認してください。

1. リムーバブルデバイスを接続します。
2. デバイス上の平文のファイルを暗号化するかどうかを確認するダイアログが表示されます。「**Yes**」(はい) をクリックすると、暗号化が開始されます。「**NO**」(いいえ) をクリックすると、ファイルは平文のままで残りますが、デバイス上のすでに暗号化されているファイルにアクセスすることができます。どちらを選択しても、デバイス上の新しいファイルは、ポリシーに準じて常に暗号化されます。
3. デバイス上のファイルが自動的に暗号化されます。これは、システムメニューアイコンの外側の輪が回転することで示されます。
4. デバイス上のすべてのファイルの暗号化が完了すると、アイコンの外側の輪の回転が停止します。

5. リムーバブルデバイスを取り出します。対応する保護されたフォルダのアイコンは自動的に消えます。

   注:

   リムーバブルデバイスにあるデータを他のユーザーと交換・変更するには、両ユーザーに適切なポリシーおよび鍵が割り当てられている必要があります。Windows クライアントと Mac OS X クライアント間でデータ交換を行うには、FAT32 形式でデバイスをフォーマットする必要があります。また、個人鍵を使用することはできません。Windows クライアントの場合、データ交換ポリシーが必要です。メディア パスフレーズ機能は、Windows のみで使用できます。Mac OS X クライアントの場合、ポリシーの種類が「**File Encryption**」のポリシーが定義されている場合のみデータにアクセスできます。

6 トラブルシューティング

6.1 Mac OS X ログインパスワードを忘れた場合

ユーザーが Mac OS X ログインパスワードを忘れた場合は、次の手順を実行します。

1. ユーザーによって、新しいユーザーパスワードの作成が要求されます。
2. ユーザーの管理環境で既存のパスワードをリセットし、新しいパスワードを生成します。次回ログオンする際、ユーザーによるパスワード変更が必要となるよう、該当するオプションを指定します。
3. SafeGuard Management Center アプリケーションに切り替えて、ユーザーの証明書を削除します。
4. ユーザーに新しいパスワードを渡します。
5. この新しいパスワードを使ってログインするようユーザーに伝えます。
6. ログイン後、「**Reset Password**」(パスワードのリセット) ダイアログが表示されます。
7. 新しいパスワードを選択し、それを入力・確認入力し、さらにパスワードのヒントを指定する必要があることをユーザーに伝えます。最後にユーザーは「**Reset Password**」(パスワードのリセット) をクリックして、変更を確定します。
8. パスワードのリセット後、ユーザーに対して次のメッセージが表示されます。

   The system was unable to unlock your login keychain (ログイン キーチェーンのロックを解除できませんでした)
9. 「**Create New Keychain**」(キーチェーンの新規作成) オプションを選択するようユーザーに伝えます。
10. このユーザー用の新しいキーチェーンが作成されます。
11. その後、ユーザーは、ステップ 7 で選択した新しい OS X パスワードを入力して、SafeGuard ユーザー証明書を作成する必要があります。

ユーザーの鍵は、新しいキーチェーンに自動的に取り込まれるため、すべてのドキュメントにこれまで通りにアクセスできます。

6.2 データアクセス時に問題が発生する

データアクセス時に問題が発生する場合は、ユーザーの鍵リングに対応する鍵がないことが原因であることが考えられます。

- Management Center 環境を確認して、必要に応じて修正してください。現在ログオンしているユーザーが、対応する鍵を所有しているかを確認する方法の詳細は、Sophos SafeGuard File Encryption システム メニュー (p. 20) を参照してください。

  ユーザーのキーチェーンにない鍵を使用して暗号化したファイルを復号化することはできません。このような保護されたフォルダへのファイルコピーをユーザーが続行しようとし (これによって対象ファイルの暗号化が開始されます)、対応する鍵がない場合、管理者のユーザー名とパスワードの入力を求める Mac OS X ダイアログが表示されます。

この場合、ユーザーは「**Cancel**」(キャンセル) をクリックするようにしてください (パスワードを入力しても暗号化ファイルにアクセスすることはできません)。

7 クライアントからのアンインストール

このソフトウェアをクライアントからアンインストールする必要がある場合は、次の手順を実行してください。

1. Mac クライアントで **/Library** に移動します。
2. **Sophos SafeGuard FS** フォルダを開きます。
3. **Sophos SafeGuard FS Uninstaller.pkg** ファイルを選択してダブルクリックします。
4. ウィザードの指示に従ってアンインストールを行います。
5. Mac で作業を続行する前に、システムを再起動してください。

   注: アンインストーラパッケージは署名付きで、OS X はこの署名を検証しようとします。インターネット接続が遅かったり、設定に問題があると、アンインストール操作中に最高 20分の待機時間が発生する場合もあります。

8 テクニカルサポート

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。

- 「SophosTalk」ユーザーフォーラム (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/
- オンラインでのお問い合せ。
  https://secure2.sophos.com/ja-jp/support/contact-support/support-query.aspx

9 ご利用条件