SOPHOS
Security made simple.

Sophos SafeGuard Native Device 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 SafeGuard Native Device Encryption for Mac について

Sophos SafeGuard Native Device Encryption for Mac は、Windows ユーザー向けの SafeGuard Enterprise と同等のデータ保護機能を Mac OS X ユーザーに提供します。

SafeGuard Native Device Encryption for Mac は、Mac OS X に搭載されている暗号化テクノロジー、FileVault 2 を利用します。FileVault 2 を使用して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が、ネットワーク全体に対してディスク暗号化を提供し、管理することもできます。

暗号化は透過的に行われます。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ユーザーに表示されません。

SafeGuard Enterprise の Management Center から、さまざまな管理操作、たとえば暗号化を実行するコンピュータ (Mac、Windows の両方) の指定、暗号化ステータスの監視、ユーザーがパスワードを忘れたときの復旧などを実行できます。

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 Native Device 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 Native Device 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
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。
POA	Power-On Authentication (「起動前認証」とも呼ばれます)
SGN	SafeGuard Enterprise
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 Native Device Encryption for Mac 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

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。

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。

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。

1. SafeGuard Enterprise のサーバー管理者から、SSL 用の SGN サーバー証明書 (**<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。そのためには、「**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、**`https://<サーバー名>/SGNSRV`** と入力して SafeGuard Enterprise サーバーが使用できることを確認します。

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 権限を使用して `sgdeadmin --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. 14) 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:

インストールの前提要件 (p. 4) にある説明に従って、サーバーを正しく設定しておくようにしてください。

1. **Sophos SafeGuard DE.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 DE.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 DE/** 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. 再起動後、Mac パスワードでログインします。
5. 「**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。

6. 「**Server**」(サーバー) タブをクリックします。
7. 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。

8. ZIP 形式の構成パッケージを選択します (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** バージョン 7.0」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)。
9. 「**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。
10. 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。
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) を参照してください)。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. 12) 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 Native Device 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。システムに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。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。

注:

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

1. **Sophos SafeGuard DE.dmg** 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て、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** バージョン 7.0」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)。
5. 対象マシンで次のコマンドを実行します。

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

    /full/path/to/file に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。

3 環境設定

Sophos SafeGuard Native Device 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。

注:

Sophos SafeGuard Native Device Encryption for Mac OS X では、「**デバイス保護**」と「**全般設定**」という種類のポリシーのみが使用され、「**ターゲット**」、「**メディアの暗号化モード**」、および「**サーバーへの接続の間隔 (分)**」以外のポリシー設定はすべて無視されます。

3.1 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 で一元的に設定されます。

ポリシー

ポリシーは SafeGuard Management Center で一元的に設定されます。フルディスク暗号化を行うには、次のような設定が必要です。

1. 「**デバイス保護**」という種類の新しいポリシーを作成します。「**デバイス保護の対象**」で、「**ローカル記憶デバイス**」、「**内部記憶装置**」または「**ブートボリューム**」を選択します。ポリシーの名前を入力し、「**OK**」をクリックします。
2. 「**メディアの暗号化モード**」で、「**ボリューム ベース**」を選択します。

これで、Mac のフルディスク暗号化用の新しいデバイス保護ポリシーが作成・設定されました。

注: 暗号化するクライアントに、このポリシーを割り当てるようにしてください。すべてのエンドポイントを暗号化する場合は、ドメインやワークグループの最上部にこのポリシーを割り当てることもできます。IT 管理者がインストールを行う場合、エンドユーザーにクライアントマシンを渡す前に、ポリシーを割り当てないようにしてください。エンドポイントの暗号化がただちに行われ、エンドユーザーの代わりに IT 管理者が FileVault 2 に登録されてしまう可能性があります。

サーバーへの接続の間隔

ポリシーやサーバーへの接続間隔の詳細は、「**SafeGuard Enterprise 管理者ヘルプ**」を参照してください。

3.2 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)**

  `sgdeadmin --synchronize` コマンドを使用して、ポリシーや鍵などのデータベース情報を SafeGuard Enterprise バックエンドと同期できます。

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

  `sgdeadmin --enable-systemmenu` コマンドを使用して、画面右上のシステムメニューを有効化します。

  `sgdeadmin --disable-systemmenu` コマンドを使用して、システムメニューを無効化します。

  注: SafeGuard Native Device Encryption のインストール後、デフォルトではこの設定は「無効」になっています。

  システムメニューの詳細は、Sophos SafeGuard Native Device Encryption システム メニュー (p. 14) 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. 14) を参照してください。

4 SafeGuard Native Device Encryption for Mac の使用

このアプリケーションに関するユーザー向けの情報は、「Sophos SafeGuard Native Device 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。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、Native Device 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。

4.1 暗号化について

FileVault 2 では、ハード ドライブ上のすべてのデータが、XTS-AES-128 アルゴリズムを使用してディスクレベルで暗号化されます。このアルゴリズムは、512 バイトブロックのために最適化されています。平文から暗号テキストへの変換は、自動的にバックグラウンドで実行され、ユーザーの作業を妨げることもありません。

これまで、フルディスク暗号化を使用した場合に問題となったのは、暗号化されたブートボリュームのロックを解除する際 (POA)、およびデスクトップにログオンする際の合計 2回、エンドユーザーが認証を行う必要があるということでした。

しかし、その必要はなくなりました。起動前のログオン時にユーザーがパスワードを入力するだけで、システムは OS 起動後にログオン情報が必要になるとパスワードを転送します。パスワードを転送することで、コールドブート後、ユーザーが 2回ログオン操作を行う必要がなくなりました。

ユーザーは、ボリュームを再暗号化することなく、いつでもパスワードをリセットできます。これは、マルチレベルの鍵システムが使用されていることによります。ユーザーに表示される鍵 (例: ログオン鍵や復旧鍵) は、派生暗号鍵なので、変更が可能です。真のボリューム暗号化鍵は、決してユーザーに渡されません。

FileVault 2 の詳細は、Apple Web サイトからダウンロード可能な「**Apple テクニカル ホワイトペーパー - FileVault 2 の導入に関するベストプラクティス (2012年 8月)**」を参照してください。

4.2 初期暗号化

システムディスクのボリュームベース暗号化がポリシーで指定されている場合、現在ログオンしているユーザーに対して、ディスク暗号化が有効化されます。クライアント側で次の手順を実行してください。

1. 暗号化を開始する前に、ログオンパスワードの入力を要求するダイアログが表示されます。Mac OS X パスワードを入力します。

   間違ったパスワードを入力すると、ダイアログが左右に揺れます。再試行してください。

   注: 空のパスワードを使用している場合は、変更してください。空のパスワードを使用して、ディスク暗号化を有効化することはできません。

2. Mac が再起動するのを待機します。

   注: 暗号化を有効化できない場合は、エラーメッセージが表示されます。詳細はログファイルを参照してください。デフォルトの保存場所は `/var/log/system.log` です。

3. ディスク暗号化が開始し、バックグラウンドで実行されます。ユーザーはそのまま作業を継続できます。

ユーザーは、このエンドポイントの最初の FileVault 2 ユーザーとして登録されます。

4.3 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 クライアントに対して、「**暗号化なし**」とポリシーで指定した場合でも、暗号化された状態が維持されます。ただし、この場合、ユーザーは復号化することを選択できます。該当するボタンが環境設定ペインに表示されます。「Disk Encryption」タブ (p. 13) を参照してください。

ローカル管理者権限のあるユーザーが、付属の FileVault 2 機能を使って、手動でハードディスクを復号化することを阻止することはできません。しかし、復号化の完了には再起動が必要となります。Mac の再起動が完了すると、ポリシーで設定済みの場合、SafeGuard Native Device Encryption for Mac によって暗号化が施行されます。

4.4 FileVault 2 ユーザーを追加する

エンドポイントですでに FileVault 2 に登録済みのユーザーのみが、再起動後、システムにログオンできます。FileVault 2 にユーザーを追加する方法は次のとおりです。

1. Mac 稼働中、FileVault 2 に登録するユーザーとしてログインします。
2. 「**Enable Your Account**」(アカウントの有効化) ダイアログにユーザーのログオン情報を入力します。Mac OS X バージョン 10.8 環境では、追加するユーザーのログオン情報のほかに、すでに FileVault 2 に登録済みのユーザーのログオン情報も入力する必要があります。Mac OS X バージョン 10.9 で、この操作は不要になりました。

したがって、ユーザーは、Mac OS X バージョン 10.8 以外の環境では、ディスク暗号化を意識することなく、通常どおりログオンすることができます。

4.5 FileVault 2 ユーザーを削除する

SafeGuard Management Center では、Mac に割り当てられているユーザーの一覧からユーザーを削除することができます。削除されたユーザーは、次回同期を行う際に、エンドポイントの FileVault 2 ユーザーの一覧からも削除されます。しかし、このユーザーは引き続き Mac にログオンすることができます。新規ユーザーと同様、稼働中の Mac にログオンするだけで再度認証されます。

特定のユーザーによる Mac の起動を禁止するには、Management Center でユーザーをブロックすることを指定してください。ユーザーは、クライアントの FileVault 2 ユーザーの一覧から削除され、新たに認証を受けることはできなくなります。

FileVault 2 ユーザーを削除する場合、少なくとも 1名の FileVault 2 ユーザーを残す必要があります。所有者を削除した場合は一覧で次に表示されているユーザーが所有者になります。SafeGuard Native Device Encryption for Mac では、所有者に指定されているユーザーに特別な権限はありません。

4.6 バックエンドとの同期

同期が行われる際、クライアントの状態が SafeGuard Enterprise バックエンドに報告され、ポリシーがアップデートされ、User Machine Assignment がチェックされます。

次の情報がクライアントから送信され、SafeGuard Management Center に表示されます。

- エンドポイントが暗号化されると、ただちに「POA」がチェックされます。他に、ドライブ名、ラベル、種類、状態、アルゴリズム、および OS も表示されます。
- FileVault 2 の新規ユーザーは、Management Center にも追加されます。

注: エンドポイントから SafeGuard Enterprise クライアントソフトウェアを削除しても、このエンドポイントとユーザーは、引き続き SafeGuard Management Center に表示されます。しかし、前回サーバーに接続した日時は更新されなくなります。

クライアント側で変更される内容は次のとおりです。

- Management Center で変更されたポリシーは、クライアントにも適用されます。
- Management Center で削除/ブロックされたユーザーは、クライアントの FileVault 2 ユーザーの一覧からも削除されます。

4.7 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 Native Device Encryption (または Sophos SafeGuard File 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。

4.7.1 「About」タブ

「**About**」(情報) タブには、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。Sophos SafeGuard File Encryption がインストールされている場合、それも表示されます。

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。

4.7.2 「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. 14) (`sgdeadmin --enable-server-verify` コマンドまたは `sgdeadmin --disable-server-verify`) 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. 5) も参照してください。

Synchronize (同期)

ポリシー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。

考えられる原因は、ログファイルを参照してください。

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

4.7.3 「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 Native Device Encryption アイコンが表示されます。詳細については Sophos SafeGuard Native Device Encryption システム メニュー (p. 14) も参照してください。

3番目のパネルには「**User Certificate**」(SafeGuard Management Center でユーザー証明書が割り当てられている場合) 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

4.7.4 「Disk Encryption」タブ

「**Disk Encryption**」(ディスク暗号化) をクリックすると、現在のポリシーおよび Mac クライアント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 クライアントの状態が表示されます。次のいずれか 1つが表示されます。

- 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、一元格納された復旧鍵があります。)
- The system disk is encrypted but there is no centrally stored recovery key available. (システムディスクが暗号化されていますが、一元格納された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) というボタンが表示されます。このボタンは、FileVault 2 が有効化されており、現在のユーザーが FileVault 2 でアクティブで、暗号化が不要であるとセキュリティ担当者がポリシーで指定したクライアントに対して有効になっています。

注: 一元格納された復旧鍵がない場合、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。この場合、次のコマンドラインツールを使って復旧鍵をインポートする必要があります:`sgdeadmin --import-recoverykey`ユーザーとセキュリティ担当者のどちらも復旧鍵にアクセスできない場合は、ディスクを復号化後、暗号化しなおして新しい復旧鍵を作成する必要があります。

4.8 Sophos SafeGuard Native Device 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が表示されます。

- 左端のアイコンには、最新の暗号化の状態が表示されます。

図 1: **システムメニュー**

	緑色のアイコン:システムディスクは暗号化されています。
	赤色のアイコン:システムディスクは暗号化されていません。

- このアイコンをクリックすると、次のメニューアイテムが表示されます。
  - **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。

注: システムメニューでこのアイコンを表示/非表示にする方法の詳細は、「User」タブ (p. 13) を参照してください。

4.9 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)
`sgdeadmin`	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`
`sgdeadmin --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。	
`sgdeadmin --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。	

コマンド名	定義	追加パラメータ (任意)
`sgdeadmin --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
`sgdeadmin --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
`sgdeadmin --synchronize`	サーバーに強制的に接続する (有効なサーバー接続が必要)。	
`sgdeadmin --import-recoverykey ["復旧鍵ファイル名"]`	FileVault 2 復旧鍵をインポートして、既存の復旧鍵を上書きする。	`--force`:確認メッセージなしで既存の復旧鍵を上書きする "復旧鍵ファイル名": ここで指定しないと、ユーザー入力が必要
`sgdeadmin --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. 5) も参照してください。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、たとえば Finder 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。	
`sgdeadmin --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。	

コマンド名	定義	追加パラメータ (任意)
`sgdeadmin --disable-server-verify`	SafeGuard Enterprise サーバーに接続するための SSL 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。	
`sgdeadmin --update-machine-info [--domain "ドメイン名"]`	現在保存されているマシンの情報を更新する。マシンの情報は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ます。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を指定する。このパラメータはコンピュータ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. 7) を参照してください。

- `sgdeadmin --enable-systemmenu`
- `sgdeadmin --disable-systemmenu`
- `sgdeadmin --synchronize`

5 復旧

復旧では、一元格納された復旧鍵を使用して、暗号化されたボリュームにアクセスできるようにします。この操作は、ユーザーが Mac OS X のログオンパスワードを忘れた場合で、他に使用できるアカウント情報がないときに必要となります。

5.1 復旧鍵について

システムで、FileVault に登録済みのユーザーすべてがパスワードを忘れ、他に使用できるアカウント情報が存在せず、使用できる復旧鍵もない場合、暗号化されたボリュームは復号化できず、データはアクセス不可能になります。このような場合、データが永続的に失われてしまう可能性もあるので、それを防ぐため、適切な復旧計画を立てることは重要です。

ディスク暗号化を有効化するたびに、新しい復旧鍵が生成されます。Sophos SafeGuard Native Device Encryption がインストールされていない状態で暗号化を有効にすると、復旧鍵はユーザーに表示されるので、ユーザーはそれを紛失せずに保管する必要があります。一方、Sophos SafeGuard Native Device Encryption がインストール済みの場合は、復旧鍵は安全に SafeGuard Enterprise バックエンドに送信され、一元的に格納されます。セキュリティ担当者は、それをいつでも取得できます。復旧処理の詳細は、Mac OS X ログオンパスワードを忘れた場合 (p. 17) を参照してください。

なお、Sophos SafeGuard Native Device Encryption がインストールされていない状態でディスクを暗号化した場合でも、復旧鍵を一元管理することはできます。その場合、インポートする必要があります。`sgdeadmin --import-recoverykey` コマンドライン オプションを使用してください。詳細は、コマンドライン オプション (p. 14) も参照してください。復旧鍵はすべて大文字として送信されます。

注:

- Mac OS X 10.8 環境: 有効な復旧鍵が入力されたかどうかは確認されません。ユーザーの責任で正しく入力する必要があります。無効な形式の場合のみエラーが表示されます。
- Mac OS X 10.9 環境: 有効な復旧鍵が入力されたかどうかが確認されます。

特定のクライアントの復旧鍵があるかを確認するには、「Disk Encryption」タブ (p. 13) を参照してください。

存在する場合は、マスター復旧鍵を使用して復旧することもできます。詳細は、「**OS X : FileVault 2 用の復旧キーを作成し導入する方法**」を参照してください。
http://support.apple.com/kb/HT5077?viewlocale=ja_JP

5.2 Mac OS X ログオンパスワードを忘れた場合

ユーザーが Mac OS X のログオンパスワードを忘れた場合で、他に使用できるアカウント情報がないときは、次の手順を実行してください。

1. ユーザーは Mac の電源を入れます。

2. ユーザーは、ログオンダイアログで「**?**」をクリックします。または、ユーザーは、間違ったログオンパスワードを 3回入力します。

   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を確認するメッセージがユーザーに表示されます。

3. ユーザーは、メッセージの横にある三角アイコンをクリックして、その次の手順 (復旧鍵の入力) に進みます。

   

4. SafeGuard Management Center で、「**ツール** > **復旧**」を選択して復旧ウィザードを開き、該当するマシンの復旧鍵を表示します。
5. Mac で入力する復旧鍵をユーザーに連絡します。

   Mac が開始し、ユーザーは、新しいパスワードとパスワードのヒントを入力できます。

Mac OS X 10.9 の場合のみ:復旧鍵は、システムを起動するために 1回使用されると、新しいものでただちに置き換えられます。新しい復旧鍵が自動的に生成され、SafeGuard Enterprise バックエンドに送信され、次回の復旧操作に備えて保管されます。

注: エンドポイントの復旧鍵は、十分注意してユーザーに提供するようにしてください。復旧鍵は、ユーザー特有ではなくマシン特有のものです。したがって、復旧鍵を使用して、同じマシン上の別のユーザーの機密情報に不正アクセスが行われていないかを確認することが必要な場合もあります。

6 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 DE** フォルダを選択します。
3. **Sophos SafeGuard DE 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。

注: ソフトウェアをアンインストールする前に、ディスクを復号化する必要はありません。

注: 管理者権限のあるユーザーによるソフトウェアのアンインストールを阻止することはできません。(この操作を Windows クライアントで阻止するポリシーは、Mac クライアントでは効果を示しません。)

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。

7 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

8 ご利用条件