SOPHOS
Security made simple.

SafeGuard Enterprise
ツールガイド

製品バージョン: 8.0

目次

1 このガイドについて

このガイドでは、SafeGuard Enterprise で保護されたエンドポイント用の暗号化ツールの使用方法について説明します。

ツールは、SafeGuard Enterprise ソフトウェアの Tools ディレクトリにあります。次のツールが用意されています。

- SGNState ツール - システムの状態の表示
- SGNRollback ツール - 失敗したインストールを元に戻す
- KeyRecovery ツール (RecoverKeys.exe) - POA が破損した際にアクセスを復旧
- 復旧ツール (be_restore.exe) - Windows 7 SafeGuard ディスク暗号化システム (マスターブート レコード) の復旧
- 復旧ツール (BLCRBackupRestoren.exe) - Windows 8 BitLocker システムの復旧 (ESP コンテンツのバックアップ、バックアップの復元、および NVRam の起動順序の修復)
- 無効化ツール (beinvvol.exe) - 暗号化済みボリュームの無効化
- 無効化ツール (opalinvdisk.exe) - Opal 準拠の自己暗号化ハード ドライブの無効化

対象読者

このガイドは、セキュリティ担当者として SafeGuard Enterprise を扱う管理者を対象としています。

2 SGNState: システム状態の表示

SafeGuard Enterprise には、エンドポイントにある SafeGuard Enterprise の現在の状態に関する情報 (暗号化やその他の詳細なステータス情報) を表示するためのコマンド ライン ツール `SGNState` が用意されています。

レポート

`SGNState` は、以下のようなレポート機能も提供できます。

- `SGNState` のリターンコードは、サードパーティの管理ツールを使用してサーバーで評価できます。
- `SGNState /LD` を指定すると、LANDesk 用にフォーマットされた出力結果が返され、ファイルに保存できます。

パラメータ

`SGNState` は、次のようなパラメータを指定して使用できます。

`SGNState [/?][/H/Type|Status] [/L] [/LD] [/USERLIST]`

- `/?` パラメータは、使用可能な SGNState コマンド ライン パラメータに関するヘルプ情報を表示します。
- `/H Type` パラメータは、ドライブの種類に関する追加のヘルプ情報を表示します。
- `/H Status` パラメータは、ドライブの状態に関する追加のヘルプ情報を表示します。
- `/L` パラメータは、次の情報を表示します。

  OS
  製品バージョン
  暗号化の種類 [SGN | Opal | BitLocker | BitLocker-C/R | 不明または旧バージョンの SGN]
  Power On Authentication [はい | いいえ | 該当なし]
  WOL (Wake on LAN の状態) [はい | いいえ | 該当なし]
  サーバー名
  セカンダリ サーバー名
  ログオン モード [SGN、自動ログオンなし | UID/パスワード | トークン/PIN | 指紋 | BL (BitLocker)]
  クライアント有効化の状態 [エンタープライズ | オフライン]
  前回のデータ レプリケーション [日時]
  POA での証明書ベースのトークンログオンの施行 [はい | いいえ | 該当なし]
  ユーザー証明書の種類 [0 | 1 | 2 | 3 | 該当なし | ?]
  リターンコード [リターンコード]
  ボリューム情報:

名前	種類	状態	アルゴリズム
<名前>	[HD-Part | ...]	[暗号化済み | 暗号化なし | ...]	[<アルゴリズム名> | n/a | ...]
	...	...	
	FLOPPY	アクセスできない	
	REMOV.PART	エラー発生のため停止	
	REM_PART	暗号化の開始中	
	HD-PART	暗号化の進行中	
	UNKNOWN	復号化の開始中	
		復号化の進行中	
		準備されていません	

- `/LD` パラメータは、これらの情報を LANDesk 用の形式で返します。

  `/L` の出力形式と似ていますが、各行は **Sophos SafeGuard** ではじまります。

  Sophos SafeGuard - 暗号化の状態 <名前> = [暗号化済み | 暗号化なし | 準備されていません...]

  ...

- パラメータ `/USERLIST` を使用して `SGNState` を呼び出した場合は、UMA 内のユーザーの一覧、および適用されている証明書の種類が追加で表示されます。

  証明書の種類:

0	ユーザーに証明書が割り当てられていません
1	P7 証明書 (例: P12 のあるスマートカードを使用したログオン)
2	P12 証明書
3	P7 および P12 証明書 (通常の SGN ユーザー)
該当なし	証明書の種類を特定できません
?	証明書の組み合わせが不明です

- **リターンコード**

0	暗号化されたボリュームはありません
1	少なくも 1つのボリュームが暗号化されています
-1	エラーが発生しました (例: SafeGuard Enterprise デバイス暗号化がインストールされていません)

3 SGNRollback: 失敗したインストールのロールバック

注: SGNRollback は、BitLocker のない Windows 7 環境のみで使用してください。

エンドポイントへの SafeGuard Enterprise のインストールに失敗すると、エンドポイントを起動できなくなったり、リモート管理のためにアクセスできなくなったりすることがあります。

エンドポイントへの SafeGuard Enterprise インストールに失敗した場合、次の状況で SGNRollback は復旧することができます。

- Power-on Authentication が最初の起動中にフリーズし、コンピュータが起動できなくなる。
- ハード ドライブが暗号化されていない。

SGNRollback は、SafeGuard Enterprise インストールの失敗による影響を、次のようにして自動的に元に戻します。

- 起動できなくなったコンピュータを起動できるようにする。
- SafeGuard Enterprise をアンインストールする。
- システム動作に関する他の OS コンポーネントに対する修正を元に戻す。

SGNRollback を Windows ベースの復旧システムである Windows PE または BartPE から起動します。

3.1 前提条件

SGNRollback の使用にあたり、前提条件は次のとおりです。

- SGNRollback が、復旧システム WinPE または BartPE で動作する。SGNRollback を使って復旧操作を行うには、使用する復旧システムに統合してください。詳細は、該当する復旧システムのドキュメントを参照してください。

  SGNRollback を自動起動する場合、SGNRollback を使用する管理者は、該当する設定を SGNRollback の自動起動を有効にする (Windows PE の場合) (p. 8) の説明に従って WinPE で定義するか、SGNRollback の自動起動を有効にする (BartPE の場合) (p. 8) の説明に従って BartPE で定義する必要があります。

- SafeGuard Enterprise のフルディスク暗号化がインストールされます。

注:

SafeGuard Easy から SafeGuard Enterprise に移行した場合の復旧には対応していません。

3.2 復旧システムで SGNRollback を起動する

SGNRollback は手動で起動したり、復旧システムの自動起動に追加したりすることができます。

3.2.1 SGNRollback の自動起動を有効にする (Windows PE の場合)

Windows PE で SGNRollback の自動起動を有効にするには、Microsoft の Windows 自動インストール キットをインストールします。「Windows プレインストール環境 (Windows PE) ユーザーズガイド」で説明されている、Windows PE 環境の構築方法と、アプリケーションを自動的に起動する方法を参照してください。

3.2.2 SGNRollback の自動起動を有効にする (BartPE の場合)

1. BartPEBuilder バージョン 3.1.3 以降を使用して、PE イメージを作成します。詳細は、BartPE のドキュメントを参照してください。
2. BartPE Builder で、「**Custom**」(カスタム) フィールドに復旧ツール フォルダを追加します。
3. イメージを作成します。
4. SafeGuard Enterprise メディアから、BartPE が準備した Windows 版の i386 フォルダに AutoRun0Recovery.cmd ファイルをコピーします。
5. 以下の 2行の文字列を実行して AutoRun0Recovery.cmd を作成します。

   ```
   \Recovery\recovery.exe
   exit
   ```

6. 次のようにして、コマンド ラインから PEBuilder ツールを実行します。

   ```
   Pebuilder -buildis
   ```

   新しい ISO イメージが構築され、それには自動起動ファイルが含まれます。

7. 結果イメージを復旧メディアに保存します。

このイメージを起動すると、SGNRollback が自動的に起動します。

3.3 パラメータ

SGNRollback は、次のパラメータを指定して起動できます。

`-drv WinDrive`	復旧対象である SafeGuard Enterprise がインストールされたドライブ文字を示します。このパラメータは復旧モードのみで使用できます。正しいドライブ文字を表示するためには、マルチブート システムで使用する必要があります。

3.4 失敗したインストールを元に戻す

エンドポイントで失敗した SafeGuard Enterprise のインストールを元に戻す方法は次のとおりです。

1. SGNRollback を含む復旧システムの保存された復旧メディアを使って、コンピュータを起動します。
2. 復旧システムで SGNRollback を起動します。自動起動が有効になっている場合、SGNRollback は自動的に起動します。SGNRollback は SafeGuard Enterprise をアンインストールするため、OS の準備を行います。
3. 次に、復旧メディアを取り出すように指示するメッセージが表示されます。メディアを取り出した後、コンピュータは OS のセーフ モードで再起動します。

変更された設定内容はすべて元に戻され、SafeGuard Enterprise がアンインストールされます。

4 KeyRecovery ツール: コンピュータへのアクセスの復旧

KeyRecovery ツールは、POA が破損し SafeGuard の復旧ディスクからコンピュータを起動する必要があるような複雑な状況下で、コンピュータへのアクセス復旧のために使用します。ツールはチャレンジ/レスポンスを行う際に起動されます。

注: ツールに関する詳細な説明は、**SafeGuard Enterprise の管理者ヘルプの「仮想クライアントを使用したチャレンジ/レスポンス」**を参照してください。

5 Windows BIOS の SafeGuard フルディスク暗号化システムの復元

注: ここでの説明は、SafeGuard フルディスク暗号化と SafeGuard Power-on Authentication のある Windows BIOS エンドポイントを対象にしています。

SafeGuard Enterprise は、ファイルおよびドライブを透過的に暗号化します。起動ボリュームも暗号化できます。このため、コード、暗号化アルゴリズム、暗号化鍵などの復号化機能は、起動の初期段階で使用できる必要があります。したがって、復号化に必要な SafeGuard Enterprise モジュールが使用不可能または機能しない場合は、暗号化された情報にアクセスできなくなります。

5.1 破損した MBR を復元する

SafeGuard Enterprise の Power-on Authentication は、コンピュータのハード ディスクの MBR からロードされます。インストールが完了すると SafeGuard Enterprise は、インストール前のオリジナルの状態の MBR のコピーを、自身のカーネル内に保存し、LBA 0 の PBR ローダーを変更します。変更された MBR の LBA 0 には、SafeGuard Enterprise カーネルの第 1セクタのアドレスとその合計サイズが含まれます。

MBR の問題は、SafeGuard Enterprise 復元ツール `be_restore.exe` を使用して解決できます。このツールは Win32 アプリケーションであり、DOS からではなく、Windows から実行する必要があります。

MBR ローダーが破損している場合、システムを起動できません。復元するには次の 2つの方法があります。

- バックアップから MBR を復元する
- MBR を修復する

破損した MBR を復元する前に、まず次の準備を行ってください。

1. Windows PE (プレインストール環境) CD を作成することをお勧めします。
2. 復旧ツール `be_restore.exe` を使用するには、いくつかの追加ファイルが必要になります。このツールと必要なファイルは、SafeGuard Enterprise ソフトウェア ディレクトリの `Tools\KeyRecovery and Restore` 配下にあります。このフォルダ内のすべてのファイルをメモリにコピーします。ファイルはすべて、メモリの**同じ**フォルダ内に格納してください。同じフォルダ内にない場合、復元ツールは正しく起動しません。

   注: Windows PE 環境で `be_restore.exe` を起動するには、Windows ファイルである OLEDLG.dll が必要です。このファイルは、`Tools\KeyRecovery and restore` フォルダに含まれていません。Windows インストール先から、リカバリ CD 上の復旧ツール フォルダに追加してください。
3. 必要に応じて、BIOS で起動順序を変更し、CD-ROM が最初になるようにします。

注: be_restore.exe では、ディスク 0 上の MBR のみを復元または修復できます。2台のハード ディスクを使用しており、システムが他のハード ディスクから起動する場合は、MBR を復元または修復することはできません。これは、リムーバブル ハード ディスクを使用している場合でも同じです。

5.2 以前に保存した MBR のバックアップを復元する

各 SafeGuard Enterprise エンドポイントは、**マシン固有**の SafeGuard Enterprise MBR (SafeGuard Enterprise で変更後の起動ハード ディスクの LBA 0) を SafeGuard Enterprise データベースに保存します。保存されたデータは、SafeGuard Management Center からファイルにエクスポートできます。

以前に保存した MBR のバックアップを復元する方法は次のとおりです。

1. SafeGuard Management Center で「**ユーザーとコンピュータ**」をクリックし、ナビゲーション ペインで対象のコンピュータを選択します。
2. コンピュータを右クリックしてショートカット メニューを表示し、「**プロパティ > マシンの設定 > バックアップ > エクスポート**」を選択して、MBR をエクスポートします。保存先を指定すると、.BKN という拡張子を持つ MBR を含む 512バイトのファイルが作成されます。
3. 他の SafeGuard Enterprise ファイルが配置されているメモリ上のフォルダにこのファイルをコピーします。
4. 次に Windows PE 起動 CD をドライブに挿入し、SafeGuard Enterprise ファイルを格納したメモリを差し込みます。コンピュータの電源を投入し、CD から起動します。
5. コンピュータの準備が完了したら、コマンド ボックスを起動し、メモリ上の SafeGuard Enterprise ファイルのあるディレクトリに移動し、be_restore.exe を実行します。
6. バックアップから復元するよう、「**Restore MBR**」 (MBR を復元する) を選択し、作成した .BKN ファイルを選択します。

ツールは、選択した .BKN ファイルがコンピュータと一致するかをチェックした後、保存された MBR を復元します。

5.3 バックアップを使用しないで MBR を修復する

使用できる MBR バックアップ ファイルがローカルにない場合でも、be_restore.exe を使って、破損した MBR ローダーを修復できます。be_restore.exe の「**Repair MBR**」(MBR を修復する) オプションは、ハード ディスク上の SafeGuard Enterprise カーネルを探し、そのアドレスを使用して MBR ローダーが再作成します。

この方法は、コンピュータ固有の MBR バックアップ ファイルがローカルになくても修復できるため非常に便利です。ただし、ハードディスク上の SafeGuard Enterprise カーネルを検索するため、時間がかかります。

修復するには、破損した MBR を復元する (p. 11) にある準備を行った後、be_restore.exe の実行時に「**Repair MBR**」(MBR を修復する) オプションを選択してください。

複数のカーネルが検出された場合は、be_restore.exe の「**Repair MBR**」(MBR を修復する) オプションでは、タイム スタンプが最も新しいものが使用されます。

5.4 パーティション テーブル

SafeGuard Enterprise では、新しいプライマリ パーティションまたは拡張パーティションを作成することができます。この場合、パーティションのあるハードディスク上のパーティション テーブルが変更されます。

MBR のバックアップを復元する際、ツールは、破損した MBR の LBA 0 のパーティション テーブルと、復元する MBR バックアップ ファイル (*.BKN) のパーティション テーブルが異なっていることを検出します。ユーザーは、表示されるダイアログで、使用するテーブルを指定できます。

5.4.1 パーティション テーブルが破損している MBR を修復する

パーティション テーブルが破損していると、POA へ正常にログオンした後、OS が起動できなくなることがあります。

この問題は、be_restore.exe を使って、以前保存した MBR を復元するか、バックアップがない場合は MBR を修復することで解決できます。

バックアップがある場合は、「**Restore MBR**」(MBR を復元する) オプションについて記載された手順を実行します。

バックアップがない場合は、次の手順を実行します。

1. Windows PE 起動 CD をドライブに挿入し、SafeGuard Enterprise ファイルを格納したメモリを差し込みます。コンピュータの電源を投入し、CD から起動します。
2. コンピュータの準備が完了したら、コマンドプロンプトを起動し、メモリ上の SafeGuard Enterprise ファイルのあるディレクトリに移動し、`be_restore.exe` を実行します。
3. 「**Repair MBR**」(MBR を修復する) を選択します。be_restore.exe が、現在の MBR とミラーリングされた MBR のパーティション テーブルに差異を検出した場合は、パーティション テーブルを選択するためのダイアログが表示されます。

   ミラーリングされた MBR は、SafeGuard Enterprise Client の設定中に保存されたオリジナルの Microsoft MBR で、クライアントをアンインストールした場合など、復元が可能となります。Windows でパーティションに変更が生じた場合、ミラーリングされた MBR のパーティション テーブルは SafeGuard Enterprise によって更新されます。

4. 「**From Mirrored MBR**」(ミラーリングされた MBR から) を選択します。

   重要:

   「**From Current MBR**」(現在の MBR から) を選択しないでください。選択すると、現在の MBR の破損したパーティション テーブルが使用されてしまいます。結果として、システムが起動できない状態が続くだけでなく、ミラーリングされた MBR も破損した MBR で更新されてしまいます。

5.5 Windows のディスク署名

Windows のハード ディスクにファイル システムが新規作成されると、ハード ディスクに署名が書き込まれます。この署名は、ハード ディスクの MBR 内のオフセット 0x01B～

0x01BB に保存されます。ハード ディスクの論理ドライブ文字などは、Windows のディスク署名に依存することにご注意ください。

したがって、「FDISK/MBR」などを使用してディスク署名を変更しないようにしてください。変更すると、次回の Windows 起動時に、時間のかかるハードディスクのスキャンモードが開始され、ドライブの一覧が復元されます。

SafeGuard Enterprise でドライブ文字の再構築が行われても、SafeGuard Enterprise のフィルタ ドライバ「BEFLT.sys」はロードされません。これにより、システムを起動できなくなります。コンピュータには、ブルースクリーンで「STOP 0xED “Unmountable Boot Volume”」と表示されます。

SafeGuard Enterprise でこの状態を修復するには、オリジナルの Windows のディスク署名をハード ディスクの MBR に復元する必要があります。

この操作にも `be_restore.exe` を使用します。

注: 他のツールを使用して MBR を修復しないようにしてください。たとえば、古い MS DOS FDISK.exe を使用して MBR ローダーを書き換えると (FDISK /MBR コマンド)、Windows ディスク署名のない MBR ローダーが作成されることがあります。Windows のディスク署名が削除される可能性に加え、古いツールによって作成された「新しい」MBR ローダーは、現在の一般的なハード ディスク サイズを処理できないことがあります。修復ツールは、必ず最新のバージョンを使用するようにしてください。

5.6 ブート セクタ

暗号化処理時にボリュームのブートセクタは、SafeGuard Enterprise のブートセクタと置き換えられます。SafeGuard Enterprise のブートセクタには、プライマリ/バックアップ KSA の位置およびサイズに関する情報が含まれています。位置は、パーティションの開始位置を基にした、クラスタおよびセクタで特定されます。SafeGuard Enterprise のブートセクタが破損しても、暗号化されたボリュームにはアクセスできません。破損したブートセクタは、be_restore ユーティリティを使用して復元できます。

6 Windows UEFI BitLocker チャレンジ/レスポンスの復元

ソフォスの復元ツール BLCRBackupRestoren.exe を使用して、Windows UEFI BitLocker システムを復元することができます。このツールを使用して次の操作を実行できます。

- BitLocker チャレンジ/レスポンスに関連したデータをバックアップする

  注: これは、自動バックアップに失敗した場合のみに必要です。(ログイベント 3071: 「鍵のバックアップが指定されたネットワーク共有に保存できませんでした。」)

- 以前作成したバックアップを手動で復元して、NVRAM の起動順序を修復する。

  注: これは、BitLocker チャレンジ/レスポンスに関連したデータが破損した、または削除された疑いがある場合のみに必要です。

  BLCRBackupRestoren.exe は、Windows PE 環境で起動する必要があります。このツールは、ソフォスの仮想クライアント CD に含まれています。

6.1 コマンド ライン ツールを開始する

構文

```
blcrbackuprestoren [-?][-B [-T <ファイルパス>]] [-R [-K <ファイル名>] [-S <ファイル名>]] [-I] [-D]
```

オプション

- -?

  ヘルプを表示します

- -B

  バックアップ

- -T <ファイルパス>

  既存の対象パス (任意)

- -R

  復元

- -K <ファイル名>

  鍵のパス\ファイル名 (任意)

任意の鍵ファイルは、SafeGuard Management Center からエクスポートする必要のある .BKN ファイルです。

エクスポートする方法は次のとおりです。

- SafeGuard Management Center で「**ユーザーとコンピュータ**」をクリックし、ナビゲーション ペインで対象のコンピュータを選択します。
- コンピュータを右クリックしてショートカット メニューを表示し、「**プロパティ > マシンの設定 > バックアップ > エクスポート**」を選択します。

BitLocker チャレンジ/レスポンスに関連したデータを正常にバックアップしている場合は、`-R` オプションを使用することで十分です。

- `-S` <ファイル名>

  ソースパス\ファイル名 (任意)

- `-I`

  ブートエントリをインストールします。

- `-D`

  ブートエントリを削除します。

注:

自動復旧に失敗した場合、ドライブ文字の割り当てのない復旧パーティションにあるバックアップファイルを使用するには、次の操作を実行してください。

- 復旧パーティションにドライブ文字を割り当てる
- バックアップファイルの完全修飾パス名を指定する

指定できるファイルは常に1つだけあります: <ドライブ文字>`:\SOPHOS\`<ファイル名>`.cps`

例

- **バックアップ**
  - `blcrbackuprestoren -b` (デフォルトの場所にアーカイブを作成します。)
  - `blcrbackuprestoren -b -T` <USB メモリのドライブ名>`:\Backup\` (外部ドライブにアーカイブを作成します。)
- **復元**
  - `blcrbackuprestoren -r` (デフォルトの場所からアーカイブを抽出します。)
  - `blcrbackuprestoren -r -k X:\example\example.BKN` (デフォルトの場所からアーカイブを抽出し、鍵ファイルを再構成します。)

7 暗号化ボリュームの無効化

SafeGuard Enterprise で保護されているコンピュータでは、コマンドライン ツール、`beinvvol.exe` を利用できます。このツールは、暗号化済みボリューム (ハードディスク、USB メモリなど) を安全に無効化できるツールです。このコマンド ライン ツールは DoD 標準 (5220.22-M) に準じており、鍵ストアの安全な削除に使用できます。この標準では、ランダム パターンと代替パターンによる 7回の上書きサイクルが実行されます。

このコマンド ライン ツールは、次の条件を満たすコンピュータで使用してください。

- SafeGuard Enterprise がインストールされている。
- 一部のハードディスク ボリュームが暗号化されている。

このツールは、SafeGuard Enterprise の暗号化ドライバが有効になっていないシステムで実行する必要があります。これは誤ってデータが無効化されることを防止するためです。他のシステムで使用した場合、ツールは動作せずエラーメッセージが表示されます。

注: Windows PE の CD など外部メディアからシステムを起動し、コマンドライン ヘルプの説明に従ってツールを使用することを推奨します。

無効化が完了すると、対象のボリュームを読み取ることができなくなります。

また、DoD 標準 (5220.22-M) に基づいて、各暗号化ボリュームの SafeGuard Enterprise のブートセクタ、および KSA (鍵記憶域) (元の KSA およびバックアップ) を 7回上書きして、永続的に削除します。各ボリュームのランダムなデータ暗号化鍵は SafeGuard Enterprise Client の一元化されたデータベースにバックアップされされないため、以後、ボリュームには一切アクセスできなくなります。セキュリティ担当者でも再度アクセスすることができなくなります。

また、このコマンド ライン ツールでは、利用可能なボリュームに関する情報が画面に表示されます。表示される情報は、ボリュームの名前やサイズ、およびブートセクタや KSA の情報などです。この情報は任意でファイルに保存することもできます。保存先として、無効化するボリュームは指定しないようにしてください。

注: 一度削除したデータを復旧することはできません。

7.1 コマンド ライン ツールを開始する

構文

- `xl[ボリューム]`

  対象ボリュームの情報を一覧表示します。対象ボリュームを指定しないと、すべてのボリュームの情報が一覧表示されます。

- `xi<ボリューム>`

  対象ボリュームが完全に SGN 暗号化されている場合、そのボリュームを無効にします。このコマンドでは、対象 <ボリューム> を指定する必要があります。

- <ボリューム>

  対象ボリュームを指定します (a, b, c, ..., z から指定)。<*> はすべてのボリュームを意味します。

オプション

- `-g0`

  ログ機能を無効にします。

- `-ga[ファイル]`

  ログモード: 末尾に追加。対象ログ ファイルの末尾にログ エントリを追加し、ファイルが存在しない場合は作成します。

- `-gt[ファイル]`

  ログモード: 切り捨て。対象ログ ファイルがすでに存在する場合は切り捨て、存在しない場合は作成します。

- [ファイル]

  対象ログ ファイルを指定します。指定しないと、デフォルトで、現在のパスに対象ログ ファイル BEInvVol.log が作成されます。無効化されるボリュームにあるログ ファイルは指定しないようにしてください。

- `-?、h`

  ヘルプを表示します。

例

```
> beinvvol -h
> beinvvol xld
> beinvvol xle -ga"c:\subdir\file.log"
> beinvvol xl* -gt"c:\subdir\file.log"
> beinvvol xif -gt"c:\my subdir\file.log"
> beinvvol xig -g0
> beinvvol xi*
```

8 Opal 準拠の自己暗号化ハード ドライブの無効化

自己暗号化ハード ドライブは、データがハード ディスクに書き込まれると同時にハードウェア ベースで暗号化します。Opal は Trusted Computing Group (TCG) によって策定・公開されている、特定のベンダに依存しない暗号化標準仕様です。SafeGuard Enterprise は Opal 仕様に対応しており、Opal 準拠の自己暗号化ハードドライブを実装したエンドポイントを管理できます。

Opal 準拠のハードドライブについて詳細は、**「SafeGuard Enterprise 管理者ヘルプ」の「SafeGuard Enterpriseと自己暗号化 Opal 準拠のハードドライブ**」を参照してください。

SafeGuard Enterpriseで保護されているコンピュータでは、コマンドライン ツール、`opalinvdisk.exe` を利用できます。

8.1 前提条件と推奨事項

`opalinvdisk.exe` を使用する際の前提条件および推奨事項は次のとおりです。

- `opalinvdisk.exe` を使用する前に、Opal 準拠のハードドライブを復号化する必要があります。復号化するには、エンドポイントで Windows エクスプローラの右クリックメニューから SafeGuard Enterprise の「**復号化**」コマンドを実行します。詳細については、**「SafeGuard Enterprise 管理者ヘルプ」の「Opal 準拠のハード ドライブのロック解除をユーザーに許可する」および「SafeGuard Enterprise ユーザーヘルプ」の「Opal 準拠のハード ドライブのあるエンドポイント のシステム トレイ アイコンとエクスプローラのショートカット メニュー」**を参照してください。
- 管理者権限が必要です。
- Windows PE 環境で `opalinvdisk.exe` というツールを使用することをお勧めします。
- `opalinvdisk.exe` は、`RevertSP` という任意のサービス (パラメータ名: `KeepGlobalRangeKey` 値: `False`) を起動します。実際の無効化の処理は特定のハードドライブに依存する `RevertSP` によって実行されます。詳細については、www.trustedcomputinggroup.org にある「Opal standard TCG Storage Security Subsystem Class: Opal, Specification Version 1.00, Revision 3.00」の 5.2.3項 (英語) を参照してください。

8.2 opalinvdisk.exe を実行する

1. コマンド プロンプトを開き、管理者権限で `opalinvdisk.exe` を起動します。

   ツールに関する情報と使用方法が表示されます。

2. コマンド プロンプトで、`opalinvdisk.exe` <対象デバイス名> と入力します。

   例: `opalinvdisk.exe PhysicalDrive0`

必要な前提条件が満たされていると、<対象デバイス名> で指定したハードドライブ上で RevertSP が起動します。前提条件が満たされていない場合、またはハードドライブが RevertSP に対応していない場合は、エラーメッセージが表示されます。

9 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。

- 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

10 利用条件