ユーザー ガイド

HP Sure Recover

初版：2020 年 2 月

製品番号：L93434-291

管理者が入力する構文の例

ユーザー インターフェイスに入力する必要があるテキストは固定幅フォントで示されます。

表 -1 管理者が入力する構文の例

番号	説明
括弧や波括弧のないテキスト	示されているとおりに入力する必要がある項目
<山括弧内のテキスト>	値を入力する必要があるプレースホルダー。括弧は付けないでください
[角括弧内のテキスト]	オプションの項目。括弧は付けないでください
{波括弧内のテキスト}	1 つだけを選択する必要がある項目のセット。波括弧は入力しないでください
|	1 つだけを選択する必要がある項目の区切り文字。縦線は入力しないでください
. . .	繰り返しが可能または必要な項目。省略記号は入力しないでください

目次

1 はじめに

[HP Sure Recover]は、最小限の操作で、オペレーティング システムをネットワークから安全にインストールすることを可能にします。また、[Embedded Reimaging]（埋め込み再イメージ）機能を搭載した[HP Sure Recover]を備えるシステムでは、ローカル ストレージ デバイスからのインストールもサポートされています。

重要：[HP Sure Recover]を使用する前にデータをバックアップしてください。イメージングの過程でドライブが再フォーマットされるため、データ損失が発生します。

HP が提供するリカバリ イメージには、基本的な Windows® 10 インストーラーが含まれています。必要に応じて、[HP Sure Recover]を使用して HP デバイス用に最適化されたドライバーをインストールできます。HP のリカバリ イメージには、OneDrive のように Windows 10 に含まれているデータ リカバリ エージェントのみが含まれています。企業では独自のカスタム イメージを作成して、企業設定、アプリケーション、ドライバー、およびデータ リカバリ エージェントを追加することができます。

オペレーティング システム（OS）のリカバリ エージェントは、リカバリ イメージをインストールするために必要な手順を実行します。HP から提供されているリカバリ エージェントは、パーティション設定、フォーマット、ターゲット デバイスへのリカバリ イメージの展開などの一般的な手順を実行します。HP のリカバリ エージェントは hp.com にあるため、システムに[Embedded Reimaging]機能が搭載されていない場合は、リカバリ エージェントを入手するためにインターネットへのアクセスが必要です。また、企業はファイアウォール内で HP リカバリ エージェントをホストしたり、より複雑なリカバリ環境用のカスタム リカバリ エージェントを作成したりすることもできます。

オペレーティング システムが検出されない場合、[HP Sure Recover]を開始できます。また、マルウェアを確実に削除したい場合など、スケジュールに従って[HP Sure Recover]を実行することも可能です。これらの設定は、[HP Client Security Manager]（CSM）、[Manageability Integration Kit]（MIK）、または[HP Client Management Script Library]を使用して構成します。

ネットワーク経由の復元の実行

注記：ネットワーク復元を実行するには、有線接続を使用する必要があります。HP は、データの損失を防ぐため、[HP Sure Recover]を使用する前に、重要なファイル、データ、写真、動画などをバックアップしておくことをおすすめします。

1. HTTP または FTP の配布ポイントにアクセスできるネットワークに、クライアント システムを接続します。
2. クライアント システムを再起動し、HP のロゴが表示されたら、f11 キーを押します。
3. **[Restore from network]**（ネットワークから復元）を選択します。

ローカル ドライブからの復元の実行

クライアント システムが[Embedded Reimaging]機能をサポートしており、適用されているポリシーでスケジュールに従ってイメージをダウンロードするオプションが有効になっている場合は、スケジュールされた時刻にイメージがクライアント システムにダウンロードされます。イメージがクライアント システムにダウンロードされた後、そのイメージを再起動し、[Embedded Reimaging]ストレージ デバイスにコピーします。

[Embedded Reimaging]ストレージ デバイスのイメージを使用してローカルからの復元を実行するには、以下の操作を行います。

1. クライアント システムを再起動し、HP のロゴが表示されたら、f11 キーを押します。
2. **[Restore from local drive]**（ローカル ドライブから復元） を選択します。

[Embedded Reimaging]機能が搭載されているシステムでは、アップデートを確認するために、ダウンロード スケジュールを構成し、ダウンロード エージェントを使用する必要があります。ダウンロード エージェントは、[HP Client Security Manager]用の[HP Sure Recover]プラグインに含まれています。また、[Manageability Integration Kit]（MIK）で設定することもできます。MIK の使用手順については、HP の Web サイト、https://www.hp.com/go/clientmanagement/ （英語サイト） を参照してください。

また、スケジュールされたタスクを作成して、エージェントを SR_AED パーティションに、イメージを SR_IMAGE パーティションにコピーすることもできます。次に、[HP Client Management Script Library]を使用して、次の再起動時に内容を検証し、[Embedded Reimaging]ストレージ デバイスにコピーする必要があることを BIOS に通知するサービス イベントを送信できます。

2 企業用イメージの作成

ほとんどの企業では、[Microsoft® Deployment Tool]、[Windows 10 Assessment and Deployment Kit]、またはその両方を使用して、Windows イメージング（WIM）ファイル形式のアーカイブにイメージを含むファイルを作成しています。

要件

- [Windows 10 Assessment and Deployment Kit]（Windows ADK）の最新バージョン
- PowerShell
- OpenSSL（または RSA 秘密キー/公開キー ペアを生成するためのその他のソリューション）

  ユーザーが作成しホストする企業用イメージの整合性を確保するための RSA キー ペアを生成するために使用します。
- [Microsoft Internet Information Services]（IIS）などのサーバー ホスト ソリューション

イメージの作成

イメージの作成プロセスを開始する前に、以下の手順で示すように、イメージの処理に備えて必要なツールをインストールした作業用システムまたはビルド用システムを用意します。

1. 管理者として、`Deployment and Imaging Tools Environment` のコマンド プロンプトを開きます（[Windows ADK]の展開ツールとともにインストールされています）。
2. 以下のコマンドを使用して、イメージのステージング領域を作成します。

   ```
   mkdir C:\staging
   ```
3. 以下の例のどちらかを使用してイメージを作成します。

   3 ページの例 1：Microsoft Windows インストール イメージに基づいたイメージの作成

   6 ページの例 2：参照システムに基づくイメージの作成

例 1：Microsoft Windows インストール イメージに基づいたイメージの作成

1. Microsoft Windows インストール イメージを（Microsoft ISO、または HP OSDVD から）マウントするか、開きます。
2. 以下のコマンドを使用して、マウントされた Windows インストール イメージから install.wim ファイルをステージング領域にコピーします。

   ```
   robocopy <M:>\sources C:\staging install.wim
   ```

   注記：<M:>は、マウントされているドライブを指します。正しいドライブ レターに置き換えてください。
3. 以下のコマンドを使用して、install.wim をイメージ ファイル名（この例では「my-image」）に変更します。

   ```
   ren C:\staging\install.wim <my-image>.wim
   ```

（オプション）[HP Sure Recover]には、元々工場出荷時の HP ターゲット システム用にライセンスされていた Windows エディションに基づき、マルチインデックス イメージから特定のエディションを復元する機能が含まれています。このしくみは、インデックスが正しく名付けられている場合に機能します。お使いの Windows インストール イメージが HP OSDVD（オペレーティング システム DVD）イメージから取得されている場合、マルチエディション イメージが存在する可能性があります。マルチエディションの動作を希望せず、1 つの特定のエディションをすべてのターゲット システムで使用する場合は、インストール イメージに存在するインデックスが 1 つのみであることを確認する必要があります。

4. インストール イメージの内容を確認するには、以下のコマンドを使用します。

```
dism /Get-ImageInfo /ImageFile:C:\staging\<my-image>.wim
```

以下に、5 つのエディション（各ターゲット システムの BIOS に基づいて対応）をサポートするインストール イメージからの出力例を示します。

イメージの詳細： my-image.wim

インデックス： 1

名前： CoreSingleLanguage

説明： Windows 10 May 2019 Update - Home Single Language Edition

サイズ： 19,512,500,682 bytes

インデックス： 2

名前： Core

説明： Windows 10 May 2019 Update - Home edition

サイズ： 19,512,500,682 bytes

インデックス： 3

名前： Professional

説明： Windows 10 May 2019 Update- Professional Update

サイズ： 19.758,019,520 bytes

インデックス： 4

名前： ProfessionalEducation

説明： Windows 10 May 2019 Update - Professional Education edition

サイズ： 19,758,019,480 bytes

インデックス： 5

名前： ProfessionalWorkstation

説明： Windows 10 May 2019 Update - Professional Workstation edition

サイズ： 19,758,023,576 bytes

注記：インデックスが 1 つのみである場合、名前に関係なく、イメージが復元に使用されます。イメージ ファイルのサイズが削除前よりも大きくなる場合があります。

5. マルチエディションの動作を希望しない場合は、不要な各インデックスを削除します。

   以下の例のように、Professional エディションのみを使用する場合は（すべてのターゲット システムがライセンスされていると仮定して）、インデックス 5、4、2、および 1 を削除します。インデックスを削除するたびに、インデックス番号が再割り当てされます。したがって、最も大きいインデックス番号から最も小さいインデックス番号へと順番に削除する必要があります。それぞれの削除後に `Get-ImageInfo` を実行し、次に削除するインデックスを目で見て確認します。

   ```
   dism /Delete-Image /ImageFile:C:\staging\my-image.wim /Index:5

   dism /Delete-Image /ImageFile:C:\staging\my-image.wim /Index:4

   dism /Delete-Image /ImageFile:C:\staging\my-image.wim /Index:2

   dism /Delete-Image /ImageFile:C:\staging\my-image.wim /Index:1
   ```

   エディションのインデックスを 1 つのみ（この例では Professional）を選択します。インデックスが 1 つのみである場合、名前に関係なく、イメージが復元に使用されます。WIM メタデータの修正および内容の正規化のしくみのため、イメージ ファイルのサイズが削除前よりも大きくなることがあります。

6. （オプション）企業用のリカバリ イメージにドライバーを含めるには、以下の操作を行います。

   a. 以下のコマンドを使用して、イメージを空のフォルダーにマウントします。

      ```
      mkdir C:\staging\mount

      dism /Mount-Wim /WimFile:C:\staging\my-image.wim /MountDir:C:
      \staging\mount /Index:1
      ```

   b. サポートされているターゲット システム用の適切な HP Windows 10 Driver DVD（DRDVD）をマウントします。マウントされたドライバー メディアから、以下のコマンドを使用して、ドライバーのサブフォルダーをステージング領域にコピーします。

      ```
      robocopy /E <M:>\SWSETUP\DRV C:\staging\mount\SWSETUP\DRV
      ```

      注記：`<M:>`は、マウントされているドライブを指します。正しいドライブ レターに置き換えてください。

      C:\staging\mount\SWSETUP\DRV フォルダーの下に置くことで、他の.inf スタイルのドライバーを追加で含めることができます。[HP Sure Recover]によってこの内容が `dism /Add-Driver/Recurse` 機能でどのように処理されるかについては、以下のトピック、「オフラインの Windows イメージにドライバーを追加および削除する」を参照してください：https://docs.microsoft.com/ja-jp/windows-hardware/manufacture/desktop/add-and-remove-drivers-to-an-offline-windows-image。

      この機能では、アプリケーションの実行を必要とする.exe スタイルのドライバーはサポートされていません。

   c. 以下のコマンドを使用して、変更を保存し、イメージのアンマウントを行います。

      ```
      dism /Unmount-Wim /MountDir:C:\staging\mount /Commit
      ```

      最終的に得られるイメージ ファイルは次のとおりです：C:\staging\my-image.wim。

   d. 6 ページのイメージの分割に移動します。

例 2：参照システムに基づくイメージの作成

1. ブート可能な USB WinPE メディアを作成します。

   注記：イメージを取得するためのその他の方法については、ADK のドキュメントを参照してください。

   USB ドライブに、参照システムから取得したイメージを保持するための十分な空き領域があることを確認します。

2. 参照システムにイメージを作成します。
3. USB WinPE メディアを使用して参照システムを起動し、イメージを取得してから、DISM を使用します。

   注記：<U:>は、USB ドライブを指します。正しいドライブ レターに置き換えてください。

   ファイル名の「my-image」の部分および必要に応じて<my-image>の説明を編集します。

   ```
   dism /Capture-Image /ImageFile:<U:><\my-image>.wim /CaptureDir:C:\ /
   Name:<My Image>
   ```

4. 以下のコマンドを使用して、USB から作業用システムのステージング領域にイメージをコピーします。

   ```
   robocopy <U:>\ C:\staging <my-image>.wim
   ```

   次のイメージ ファイルが得られます：C:\staging\my-image.wim。

5. 6 ページのイメージの分割に移動します。

イメージの分割

HP では、以下のコマンドを使用して、ネットワーク ダウンロードの信頼性を向上させるために、イメージを小容量ファイルに分割することをおすすめしています。

```
dism /Split-Image /ImageFile:C:\staging\<my-image>.wim /SwmFile:C:\staging
\<my-image>.swm /FileSize:64
```

注記：FileSize（ファイルサイズ）はメガバイト単位で表示されます。必要に応じて編集します。

注記：DISM の分割アルゴリズムの性質により、生成された SWM ファイルのサイズが、指定されたファイル サイズよりも小さい、または大きい可能性があります。

マニフェストの作成

マニフェスト ファイルの形式を、バイト オーダー マーク（BOM）なしの UTF-8 にします。

以下の手順で使用されているマニフェスト ファイル名（custom.mft）は変更可能ですが、拡張子.mft および.sig を変更することはできません。また、マニフェストとシグネチャ ファイルのファイル名の部分が一致している必要があります。たとえば、custom.mft および custom.sig というペアを、myimage.mft および myimage.sig に変更することができます。

`mft_version` は、イメージ ファイルの形式を確認するために使用され、現在 1 に設定されている必要があります。

`image_version` は、新しいバージョンのイメージが使用可能かどうかを確認し、古いバージョンがインストールされないようにするために使用されます。

どちらの値も符号なし 16 ビット整数である必要があります。また、マニフェストのライン セパレーターは「`\r\n`」（`CR + LF`）であることが必須です。

マニフェストの生成

分割イメージに複数のファイルが含まれている場合があるため、PowerShell スクリプトを使用してマニフェストを生成します。

残りのすべての手順は、C:\staging フォルダーで行う必要があります。

```
CD /D C:\staging
```

1. 以下のコマンドを使用して、BOM なしの UTF-8 形式でテキスト ファイルを生成できるエディターで PowerShell スクリプトを作成します。`notepad C:\staging\generate-manifest.ps1`

   以下のスクリプトを作成します。

   ```
   $mftFilename = "custom.mft"

   $imageVersion = 1907（注意：これは、任意の 16 ビット整数にすることができます）


   $header = "mft_version=1, image_version=$imageVersion"

   Out-File -Encoding UTF8 -FilePath $mftFilename -InputObject $header

   $swmFiles = Get-ChildItem "." -Filter "*.swm"

   $ToNatural = { [regex]::Replace($_, '\d*\....
   $', { $args[0].Value.PadLeft(50) }) }


   $pathToManifest = (Resolve-Path ".").Path


   $total = $swmFiles.count

   $current = 1


   $swmFiles | Sort-Object $ToNatural | ForEach-Object {
   ```

```
    Write-Progress
        -Activity "Generating manifest" `
        -Status "$current of $total ($_)" `
        -PercentComplete ($current / $total * 100)

    $hashObject = Get-FileHash -Algorithm SHA256 -Path $_.FullName
    $fileHash = $hashObject.Hash.ToLower()
    $filePath = $hashObject.Path.Replace($pathToManifest + '\', '')
    $fileSize = (Get-Item $_.FullName).length
    $manifestContent = "$fileHash $filePath $fileSize"

    Out-File -Encoding utf8 -FilePath $mftFilename -
InputObject $manifestContent -Append
    $current = $current + 1
}
```

注記：[HP Sure Recover]のマニフェストには BOM を含めることができないため、以下のコマンドで BOM なしの UTF-8 としてファイルを書き換えます。

```
$content = Get-Content $mftFilename
$encoding = New-Object System.Text.UTF8Encoding $False
[System.IO.File]::WriteAllLines($pathToManifest + '\' + $mftFilename,
$content, $encoding)
```

2. スクリプトを保存します。
3. スクリプトを実行します。

```
powershell .\generate-manifest.ps1
```

マニフェスト シグネチャの生成

[HP Sure Recover]では、暗号化シグネチャを使用してエージェントとイメージを検証します。以下の例では、X.509 PEM 形式（.PEM 拡張子）の秘密キー/公開キー ペアを使用しています。必要に応じて、DER バイナリ証明書（.CER または.CRT 拡張子）、BASE-64 でエンコードされた PEM 証明書（.CER または.CRT 拡張子）、または PKCS1 PEM ファイル（.PEM 拡張子）を使用するようにコマンドを調整します。また、この例では、ビッグ エンディアン形式でシグネチャを生成する OpenSSL も使用しています。任意のユーティリティを使用してマニフェストに署名することもできますが、一部の BIOS バージョンではリトル エンディアン形式のシグネチャのみがサポートされています。

1. 以下のコマンドを使用して、2048 ビットの RSA 秘密キーを生成します。2048 ビットの RSA 秘密キー/公開キー ペアが PEM 形式の場合は、それらを C:\staging にコピーしてから手順 3 に進みます。

   ```
   openssl genrsa -out my-recovery-private.pem 2048
   ```

2. 以下のコマンドを使用して、秘密キーから公開キーを生成します（PEM 形式の秘密キーに対応する公開キーがある場合は C:\staging にコピーします）。

   ```
   openssl rsa -in my-recovery-private.pem -pubout -out my-recovery-public.pem
   ```

3. 以下のコマンドを使用して、手順 1 での 2048 ビットの RSA 秘密キーに基づくシグネチャ ファイル（sha256 ベースのハッシュを使用）を作成します。

   ```
   openssl dgst -sha256 -sign my-recovery-private.pem -out custom.sig custom.mft
   ```

4. 以下のコマンドを使用して、前の手順での公開キーを使用してシグネチャ ファイルを検証します。

   ```
   openssl dgst -sha256 -verify my-recovery-public.pem -signature custom.sig custom.mft
   ```

注記：

- シグネチャ ファイルのみを作成する場合、必要な手順は 1 ~ 3 です。
- [HP Sure Recover]では最小限でも手順 1、2、および 3 が必要です。ターゲット システムをプロビジョニングするには、手順 2 での公開キーを使用する必要があります。
- 手順 4 は任意ですが、シグネチャ ファイルおよびマニフェスト ファイルが正しく検証されるようにするために実行することをおすすめします。

ファイルのホスト

以下のファイルをサーバー上で C:\staging フォルダーからホストします。

- *.swm
- custom.mft（またはマニフェスト ファイル用に選択したファイル名）
- custom.sig（またはシグネチャ ファイル用に選択した一致するファイル名）

注記：IIS をホスト ソリューションとして使用している場合は、すべて「application/octet-stream:」として構成された以下の拡張子が MIME エントリに含まれるように設定する必要があります。

- .mft
- .sig
- .swm
- .wim

ターゲット システムのプロビジョニング

[HP Client Management Script Library]、[HP Client Security Manager]（CSM）/[HP Sure Recover]、または[Manageability Integration Kit]（MIK）（https://www.hp.com/go/clientmanagement/（英語サイト））を使用して、ターゲット システムをプロビジョニングできます。

このプロビジョニングのため、以下の情報を提供します。

1. 前のセクションでホストしたマニフェスト ファイルの URL アドレス（http://your_server.domain/path/custom.mft）
2. 以前に作成したシグネチャ ファイル（例：C:\staging\my-recovery-public.pem）を検証するために使用される公開キー

トラブルシューティング

カスタム復元プロセスによるセキュリティ検証の失敗に関するメッセージが表示される場合は、以下の点を確認してください。

1. マニフェストは BOM なしの UTF-8 である必要があります。
2. ファイルのハッシュを確認します。
3. システムのプロビジョニングに、マニフェストへの署名に使用された秘密キーに対応する公開キーが使用されていることを確認します。
4. IIS サーバーの MIME タイプは `application/octet-stream` である必要があります。
5. マニフェスト内のファイル パスには、クライアント システムから見たイメージを含む最上位ディレクトリへのフル パスを含める必要があります。このパスは、配布ポイントに保存されているファイルのフル パスではありません。

3 企業のファイアウォール内での[HP Sure Recover]エージェントの使用

[HP Sure Recover]エージェントは、企業のイントラネット上でホストできます。[HP Sure Recover]の SoftPaq をインストールした後、[HP Sure Recover]エージェント ディレクトリから HTTP または FTP の配布ポイントにエージェント ファイルをコピーします。次に、クライアント システムで、配布ポイントの URL と、[HP Sure Recover]エージェントの SoftPaq とともに配布された HP 公開キー `hpsr_agent_public_key.pem` をプロビジョニングします。

[HP Sure Recover]エージェントのインストール

1. [HP Sure Recover]エージェントをダウンロードし、HTTP または FTP の配布ポイントにファイルを展開します。
2. 配布ポイントに適切なファイル アクセス権を設定します。
3. Internet Information Services（IIS）を使用している場合は、MIME タイプとして以下のファイル形式に対する application/octet-stream を作成します。
   - .wim
   - .swm
   - .mft
   - .sig
   - .efi
   - .sdi

重要：以下の手順では、SCCM を使用した[HP Sure Recover]のプロビジョニングについて説明します。[HP Client Management Script Library]を使用した[HP Sure Recover]のプロビジョニング方法の例については、13 ページの「[HP Client Management Script Library]（CMSL）の使用」を参照してください。

4. SCCM を起動して**[HP Client Security Suite]**に移動し、[HP Sure Recover]ページを選択します。

注記：配布ポイントの URL には、トランスポート プロトコルとして ftp または http のどちらかが含まれています。また、クライアント システムから見た、[HP Sure Recover]エージェントのマニフェストを含む最上位ディレクトリのフル パスも含まれています。このパスは、配布ポイントに保存されているファイルのフル パスではありません。

5. 企業の配布ポイントからカスタマイズされた OS イメージを復元するには、**[Platform Image]**（プラットフォーム イメージ）セクションで**[Corporation]**（企業）オプションを選択します。IT 管理者によって提供された URL を**[Image Location URL]**（イメージの場所 URL）エントリ ボックスに入力します。公開キー `hpsr_agent_public_key.pem` を**[Image Verification]**（イメージの検証）フィールドに入力します。

注記：カスタム イメージの URL には、イメージのマニフェスト ファイル名が含まれている必要があります。

6. 企業の配布ポイントからカスタム リカバリ エージェントまたは HP リカバリ エージェントを使用するには、**[Recovery Agent]**（リカバリ エージェント）セクションで**[Corporation]**オプションを選択します。IT 管理者によって提供された URL を**[Agent Location URL]**（エージェントの場所 URL）エントリ ボックスに入力します。公開キー `hpsr_agent_public_key.pem` を**[Agent Verification Key]**（エージェント検証キー）エントリ フィールドに入力します。

   注記：BIOS では名前が recovery.mft である必要があるため、URL にエージェント マニフェストのファイル名を含めないでください。

7. ポリシーがクライアント システムに適用された後、再起動します。

8. 初期プロビジョニングの実行中に、[HP Sure Recover]のアクティベーションを完了するための 4 桁のセキュリティ コードを入力するよう求めるメッセージが表示されます。詳しくは、HP の Web サイト、https://www.hp.com/go/clientmanagement/ （英語サイト）にアクセスし、[HP Whitepapers]から「HP Manageability Integration Kit (MIK) for Microsoft System Center Manager」（英語版）を参照してください。

[HP Sure Recover]のアクティベーションが正常に完了すると、ポリシーによって適用されているカスタム URL が[HP Sure Recover]の BIOS 設定メニューに表示されます。

アクティベーションが成功したことを確認するには、コンピューターを再起動し、HP のロゴが表示されたら f10 キーを押します。**[Advanced]**（カスタム）、**[HP Sure Recover]**、**[Recovery Agent]**（リカバリ エージェント）の順に選択し、**[URL]**を選択します。

4 [HP Client Management Script Library]（CMSL）の使用

[HP Client Management Script Library]では、PowerShell を使用して[HP Sure Recover]の設定を管理できます。以下のスクリプトの例で、[HP Sure Recover]のプロビジョニング、状態の確認、設定の変更、およびプロビジョニング解除の方法を示しています。

注記：一部のコマンドはこのガイドでの行の長さを超えていますが、1 行として入力する必要があります。

```
$ErrorActionPreference = "Stop"

$path = 'C:\test_keys'
$ekpw = ""
$skpw = ""

Get-HPSecurePlatformState

try {
    Write-host 'Provisioning Endorsement Key'
    $p = New-HPSecurePlatformEndorsementKeyProvisioningPayload `
        -EndorsementKeyPassword $ekpw `
        -EndorsementKeyFile "$path\kek.pfx"
    $p | Set-HPSecurePLatformPayload

    Start-Sleep -Seconds 3

    Write-host 'Provisioning signing key'
    $p = New-HPSecurePlatformSigningKeyProvisioningPayload `
        -EndorsementKeyPassword $ekpw `
        -EndorsementKeyFile "$path\kek.pfx" `
        -SigningKeyFile "$path\sk.pfx"
    $p | Set-HPSecurePLatformPayload
```

```
    $p = New-HPSureRecoverImageConfigurationPayload `
        -SigningKeyPassword $skpw `
        -SigningKeyFile "$path\sk.pfx" `
        -Image OS `
        -ImageKeyFile "$path\os.pfx" `
        -username test -password test `
        -url "http://www.hp.com/custom/image.mft"
    $p | Set-HPSecurePLatformPayload

    $p = New-HPSureRecoverImageConfigurationPayload `
        -SigningKeyPassword $skpw `
        -SigningKeyFile "$path\sk.pfx" `
        -Image agent `
        -ImageKeyFile "$path\re.pfx" `
        -username test -password test `
        -url "http://www.hp.com/pub/pcbios/CPR"
    $p | Set-HPSecurePLatformPayload

$p = New-HPSureRecoverSchedulePayload `
        -SigningKeyPassword $skpw `
        -SigningKeyFile "$path\sk.pfx" `
        -DayOfWeek Sunday,EveryWeek -Hour 13 -Minute 27 -WindowSize 30
    $p | Set-HPSecurePlatformPayload

    $p = New-HPSureRecoverConfigurationPayload `
        -SigningKeyPassword $skpw `
        -SigningKeyFile "$path\sk.pfx" `
        -OSImageFlags NetworkBasedRecovery `
        -AgentFlags DRDVD
    $p | Set-HPSecurePlatformPayload
```

```
    Get-HPSureRecoverState -all
    Get-HPSecurePlatformState
}
finally {
    Write-Host 'Deprovisioning Sure Recover'
    Start-Sleep -Seconds 3
    $p = New-HPSureRecoverDeprovisionPayload `
        -SigningKeyPassword $skpw `
        -SigningKeyFile "$path\sk.pfx"
    $p | Set-HPSecurePlatformPayload

    Start-Sleep -Seconds 3
    Write-host 'Deprovisioning P21'

    $p = New-HPSecurePlatformDeprovisioningPayload `
        -verbose `
        -EndorsementKeyPassword $pw `
        -EndorsementKeyFile "$Path\kek.pfx"
    $p | Set-HPSecurePlatformPayload

    Write-Host 'Final secure platform state:'
    Get-HPSecurePlatformState
}
```

OpenSSL を使用したサンプル キーの生成

秘密キーは安全な場所に保管してください。公開キーは検証に使用され、プロビジョニング時に提供されている必要があります。これらのキーは 2048 ビットの長さを持ち、0x10001 の指数を使用する必要があります。例のサブジェクトを自社組織に関する情報に置き換えてください。

続行する前に、以下の環境変数を設定します。

```
set OPENSSL_CONF=<path>\openssl.cnf


# Create a self-signed root CA certificate for testing

openssl req -sha256 -nodes -x509 -newkey rsa:2048 -keyout ca.key -out
ca.crt -subj

"/C=US/ST=State/L=City/O=Company/OU=Org/CN=www.example.com “


# Create a key endorsement certificate

openssl req -sha256 -nodes -newkey rsa:2048 -keyout kek.key -out kek.csr -
subj

"/C=US/ST=State/L=City/O=Company/OU=Org/CN=www.example.com “

openssl x509 -req -sha256 -in kek.csr -CA ca.crt -CAkey ca.key -
CAcreateserial -out kek.crt

openssl pkcs12 -inkey kek.key -in kek.crt -export -out kek.pfx -CSP
"Microsoft Enhanced RSA and AES Cryptographic Provider" -passout pass:


# Create a command signing key

openssl req -sha256 -nodes -newkey rsa:2048 -keyout sk.key -out sk.csr -
subj "/C=US/ST=State/L=City/O=Company/OU=Org/CN=www.example.com “

openssl x509 -req -sha256 -in sk.csr -CA ca.crt -CAkey ca.key -
CAcreateserial -out sk.crt

openssl pkcs12 -inkey sk.key -in sk.crt -export -out sk.pfx -CSP
"Microsoft Enhanced RSA and AES Cryptographic Provider" -passout pass:

openssl pkcs12 -in sk.pfx -clcerts -nokeys -out sk_public.pem -passin
pass:


# Create an image signing key

openssl req -sha256 -nodes -newkey rsa:2048 -keyout os.key -out os.csr -
subj "/C=US/ST=State/L=City/O=Company/OU=Org/CN=www.example.com “

openssl x509 -req -sha256 -in os.csr -CA ca.crt -CAkey ca.key -
CAcreateserial -out os.crt

openssl pkcs12 -inkey os.key -in os.crt -export -out os.pfx -CSP
"Microsoft Enhanced RSA and AES Cryptographic Provider" -passout pass:
```

このコマンドを使用して、イメージ マニフェストに署名できます。

```
openssl dgst -sha256 -sign os.key -out image.sig image.mft


# Create an agent signing key

openssl req -sha256 -nodes -newkey rsa:2048 -keyout re.key -out re.csr -
subj "/C=US/ST=State/L=City/O=Company/OU=Org/CN=www.example.com “

openssl x509 -req -sha256 -in re.csr -CA ca.crt -CAkey ca.key -
CAcreateserial -out re.crt

openssl pkcs12 -inkey re.key -in re.crt -export -out re.pfx -CSP
"Microsoft Enhanced RSA and AES Cryptographic Provider" -passout pass:
```

このコマンドを使用して、エージェント マニフェストに署名できます。

```
openssl dgst -sha256 -sign re.key -out agent.sig agent.mft
```

OpenSSL ではシグネチャ ファイルがビッグ エンディアン形式で生成されますが、一部の BIOS バージョンとは互換性がありません。そのため、場合によってはエージェント シグネチャ ファイルのバイト順序を展開前に逆にする必要があります。ビッグ エンディアンのバイト順序をサポートする BIOS バージョンでは、リトル エンディアンのバイト順序もサポートされています。

A　トラブルシューティング

ドライブのパーティションの作成に失敗した

SR_AED または SR_IMAGE パーティションが Bitlocker によって暗号化されている場合、ドライブのパーティション設定に失敗することがあります。通常、これらのパーティションは gpt 属性を使用して作成され、Bitlocker による暗号化は行われませんが、ユーザーがパーティションを削除して再作成した場合、またはベア メタル ドライブ上で手動で作成した場合は、[HP Sure Recover]エージェントが削除できず、ドライブのパーティション再設定を行うときにエラーが発生して終了します。ユーザーは diskpart を実行してボリュームを選択し、`del vol override` などのコマンドを発行することによって、それらを手動で削除する必要があります。

ファームウェア監査ログ

EFI 変数の情報は以下のとおりです。

- GUID：`{0xec8feb88, 0xb1d1, 0x4f0f, {0xab, 0x9f, 0x86, 0xcd, 0xb5, 0x3e, 0xa4, 0x45}}`
- 名前：`OsRecoveryInfoLog`

Windows の下に EFI 変数を読み取る API があります。または、ユーザーが[UEFI Shell dmpstore]ユーティリティを使用して変数の内容をファイルにダンプできます。

[HP Client Management Script Library]で提供されている `HPFirmwareAuditLog` コマンドを使用して、監査ログをダンプできます。

Windows イベント ログ

[HP Sure Recover]の開始および終了イベントは BIOS 監査ログに送信されます。[HP Notifications]がインストールされている場合、Windows イベント ビューアーで[HP Sure Start]のログを確認できます。これらのイベントには、日付と時刻、ソース ID、イベント ID、およびイベント固有コードが記載されています。たとえば、`[fe 00 40 26 02 27 06 18 84 2a 02 01 00 30 f2 c3]` は、2018 年 6 月 27 日 2:26:40 にログに記録されたイベント固有コード c3f 23000 でマニフェストを認証できなかったため、リカバリに失敗したことを示しています。

注記：これらのログでは、米国の日付形式（月/日/年）が使用されています。

HP Secure Platform Management（ソース ID = 84h）

表 A-1 HP Secure Platform Management

イベント ID	デバイス数（すべて/DaaS）	イベント数（すべて/DaaS）	説明	メモ
40	256/178	943/552	プラットフォーム OS 復元プロセスは、ファームウェアによって開始されました	プラットフォームの復元が開始されました
41	221/147	588/332	プラットフォーム OS 復元プロセスが正常に完了しました	プラットフォームの復元が完了しました
42	54/42	252/156	プラットフォーム OS 復元プロセスが正常に完了しませんでした	プラットフォームの復元に失敗しました

HP の Web サイト、http://www.hp.com/go/clientmanagement/（英語サイト）から入手可能な[HP Client Management Script Library]の Get-HPFirmwareAuditLog を使用して、ファームウェアの監査ログを取得できます。[HP Secure Platform Management]のイベント ID 40、41、および 42 は、データ フィールドにイベント固有コードを返します。これは[HP Sure Recover]の操作の結果を示しています。たとえば、以下のログ エントリでは、エラーのイベント ID が 42、データが 00:30:f1:c3 となっており（dword 値 0xC3F13000 = MftOrSigDownloadFailed と解釈）、[HP Sure Recover]がマニフェストまたはシグネチャ ファイルのダウンロードに失敗したことを示しています。

```
message_number: 0

severity: Info

system_state_at_event: S0

source_id: HP Secure Platform Management

event_id: 42

timestamp_is_exact: 1

timestamp: 5/27/2019 2:44:18 PM

description: The platform OS recovery process failed to complete
successfully.

data: 00:30:f1:c3
```

復元が成功した場合、以下のように、イベント ID が 41、データが 00:00:00:00 と表示されます。

```
Event Specific Codes

Success = 0x00000000

CatalogDownloadFailed = 0xC3F11000

message_number: 0

severity: Info

system_state_at_event: S0

source_id: HP Secure Platform Management

event_id: 41
```

```
timestamp_is_exact: 1

timestamp: 5/27/2019 2:55:41 PM

description: The platform OS recovery process failed to complete
successfully.

data: 00:00:00:00
```

[HP Sure Recover]は、以下のイベント固有コードを使用します。

表 A-2 イベント固有コード

イベントの説明	イベントコード
CatalogDownloadFailed	0xC3F11000
SignatureDownloadFailed	0xC3F12000
MftOrSigDownloadFailed	0xC3F13000
FtpHttpDownloadFailed	0xC3F14000
AwsDownloadFailed	0xC3F15000
AwsDownloadUnattendedFailed	0xC3F16000
UnableToConnectToNetwork	0xC3F17000
CatalogNotAuthenticated	0xC3F21000
FtpHttpDownloadHashFailed	0xC3F22000
ManifestDoesNotAuthenticate	0xC3F23000
CatalogVersionMismatch	0xC3F31000
CatalogLoadFailed	0xC3F32000
OsDvdDidNotResolvedToOneComponent	0xC3F33000
DriversDvdDidNotResolvedToOneComponent	0xC3F34000
ManifestFileEmptyOrInvalid	0xC3F41000
ListedFileInManifestNotFound	0xC3F42000
FailedToInstallDrivers	0xC3F51000
FailedToApplyWimImage	0xC3F52000
FailedToRegisterWimCallback	0xC3F53000
FailedToCreateDismProcess	0xC3F54000
BcdbootFailed	0xC3F55000
NoSuitableDiskFound	0xC3F56000
PartitoningFailed	0xC3F57000
DiskLayoutCreationFailed	0xC3F58000
UnexpectedProblemWithConfigJson	0xC3FF1000
SureRecoverJsonParsingFailed	0xC3FF2000
RebootRequestFailed	0xC3FF3000

表 A-2 イベント固有コード(続き)

イベントの説明	イベントコード
UnableToReadConfigFile	0xC3FF4000
FailedToDetectWindowsPE	0xC3FF5000