Dell Data Protection

ファイル / フォルダ暗号化、Hardware Crypto Accelerator、自己暗号化ドライブ、および General Purpose Key のリカバリガイド

v8.10

目次

1

はじめに

本項には、リカバリ環境を作成するための必要事項詳細が記載されています。

- リカバリ環境ソフトウェアのダウンロードコピー - Dell Data Protection インストールメディアの Windows Recovery Kit フォルダ内にあります。
- CD-R、DVD-R メディアまたはフォーマット済みの USB メディア
  - CD または DVD へ書き込む場合は、補足事項 A - リカバリ環境の書き込み で詳細を参照してください。
  - USB メディアを使用する場合は、補足事項 A - リカバリ環境の書き込み で詳細を参照してください。
- 故障したデバイスのリカバリバンドル
  - リモート管理のクライアントでは、お使いの Dell Data Protection Server からのリカバリバンドルの取得方法を説明する指示が後に記載されています。
  - ローカル管理のクライアントでは、リカバリバンドルパッケージはセットアップ中に共有ネットワークドライブまたは外部メディアのいずれかに作成されました。作業を進める前にこのパッケージを見つけてください。

2

ファイル / フォルダ暗号化リカバリ

ファイル / フォルダ暗号化（FFE）リカバリでは、以下に対するアクセスを回復できます。

- 起動せず、SDE リカバリを実行するためのプロンプトを表示するコンピュータ。
- 暗号化されたデータにアクセスできない、またはポリシーを編集できないコンピュータ。
- 前記条件のいずれかを満たす Dell Data Protection | Server Encryption が実行されているサーバー。
- Hardware Crypto Accelerator カードまたはマザーボード / TPM を交換しなければならないコンピュータ。

リカバリ要件

FFE リカバリには以下が必要です。

- 特別な起動ディスクを作成するための Windows Recovery Kit - このキットには、Windows PE（WinPE）イメージを作成し、そのイメージを Dell Data Protection ドライバとソフトウェアでカスタマイズするために使用されるファイルが含まれています。このキットは、Dell Data Protection インストールメディアの Windows Recovery Kit フォルダ内にあります。

リカバリプロセスの概要

障害が発生したシステムを回復するには、次の手順を実行します。

1. リカバリ ISO を作成して CD/DVD に書き込むか、起動可能な USB を作成します。「補足事項 A - リカバリ環境の書き込み」を参照してください。
2. リカバリファイルを入手します。
3. リカバリを実行します。

FFE リカバリの実行

FFE リカバリを実行するには、以下の手順に従います。

リカバリファイルの入手 - リモート管理のコンピュータ

LSARecovery_<machinename_domain.com>.exe ファイルをダウンロードするには、以下を行います。

1. リモート管理コンソールを開き、左ペインから **管理 > エンドポイントの回復** を選択します。
2. ホスト名 フィールドに、エンドポイントの完全修飾ドメインネームを入力して **検索** をクリックします。
3. 強化リカバリ ウィンドウでリカバリパスワードを入力し、**ダウンロード** をクリックします。

メモ： このパスワードは、リカバリキーへのアクセスのために覚えておかなければなりません。

4. WinPE から起動するときにアクセスできる場所に、**LSARecovery_<machinename_domain.com>.exe** ファイルをコピーします。

リカバリファイルの入手 - ローカル管理のコンピュータ

Personal Edition リカバリファイルを入手するには、以下を行います。

1. **LSARecovery_<systemname>.exe** ファイルという名前のリカバリファイルを見つけます。このファイルは、Personal Edition のインストール中にセットアップウィザードを実行したときにネットワークドライブまたはリムーバブルストレージに保存したものです。
2. ターゲットコンピュータ（データを回復するコンピュータ）に **LSARecovery_<systemname>.exe** をコピーします。

リカバリの実行

1. 先ほど作成した起動可能なメディアを使用して、リカバリシステム上、または回復を試みているドライブを搭載したデバイス上で、そのメディアを起動します。WinPE 環境が開きます。
2. **x** と入力し **Enter** キーを押してコマンドプロンプトを起動します。
3. リカバリファイルへ移動して起動します。
4. 次の 1 つを選択します。
   - システムが起動せず、SDE リカバリの実行を指示するメッセージを表示します。

     これにより OS へ起動する場合に、Encryption クライアントが実行するハードウェアチェックを再構築することができます。
   - システムで暗号化データへのアクセスまたはポリシーの編集を実行できないか、再インストール中です。

     Hardware Crypto Accelerator カードまたはマザーボード / TPM を交換しなければならない場合はこれを使用してください。
5. バックアップおよびリカバリ情報 ダイアログで、回復するクライアントコンピュータの情報が正しいことを確認して **次へ** をクリックします。

   デル以外のコンピュータを回復する場合は、SerialNumber および AssetTag フィールドは空白となります。
6. コンピュータのボリュームがリストされるダイアログでは、該当するすべてのドライブを選択して **次へ** をクリックします。

   複数のドライブをハイライトするには、Shift+ クリックまたは control+ クリックを行います。

   選択されたドライブが FFE 暗号化されていない場合、回復は失敗します。
7. リカバリパスワードを入力し、**次へ** をクリックします。

   リモート管理のクライアントでは、これは「リカバリファイルの入手 - リモート管理のコンピュータ」の ステップ 3 で入力したパスワードです。

   Personal Edition ではパスワードは、キーがエスクローされたときにシステムに設定された、暗号化管理者パスワードです。
8. 回復 ダイアログで、**回復** をクリックします。リカバリプロセスが開始されます。
9. リカバリが完了したら、**終了** をクリックします。

メモ： コンピュータを起動するのに使用した USB、CD / DVD メディアを必ず取り外してください。取り外すのを忘れると再度リカバリ環境で起動してしまうことがあります。

10. コンピュータの再起動後、コンピュータは完全に機能した状態になります。引き続き問題が発生する場合は、Dell ProSupport にお問い合わせください。

3

Hardware Crypto Accelerator リカバリ

Dell Data Protection Hardware Crypto Accelerator (HCA) リカバリでは、以下のアクセスを回復できます。

- HCA 暗号化ドライブ上のファイル - この方法では、提供されたキーを使用してドライブを復号化します。リカバリプロセス中に復号化する必要のある特定ドライブを選択することができます。
- ハードウェア交換後の HCA 暗号化ドライブ - この方法は、Hardware Crypto Accelerator カードまたはマザーボード / TPM の交換後に使用します。ドライブを復号化せずに暗号化されたデータへのアクセスを回復するため、リカバリを実行することができます。

リカバリ要件

HCA リカバリには以下が必要です。

- リカバリ環境 ISO へのアクセス
- 起動可能な CD / DVD または USB メディア

リカバリプロセスの概要

障害が発生したシステムを回復するには、次の手順を実行します。

1. リカバリ ISO を作成して CD/DVD に書き込むか、起動可能な USB を作成します。「補足事項 A - リカバリ環境の書き込み」を参照してください。
2. リカバリファイルを入手します。
3. リカバリを実行します。

HCA リカバリの実行

HCA リカバリを実行するには、以下の手順に従います。

リカバリファイルの入手 - リモート管理のコンピュータ

Dell Data Protection のインストール時に生成された **LSARecovery_<machinename_domain.com>.exe** ファイルをダウンロードするには、以下を行います。

1. リモート管理コンソールを開き、左ペインから **管理 > エンドポイントの回復** を選択します。
2. ホスト名 フィールドに、エンドポイントの完全修飾ドメインネームを入力して **検索** をクリックします。
3. 強化リカバリ ウィンドウでリカバリパスワードを入力し、**ダウンロード** をクリックします。

メモ： このパスワードは、リカバリキーへのアクセスのために覚えておかなければなりません。

LSARecovery_<machinename_domain.com>.exe ファイルがダウンロードされます。

リカバリファイルの入手 - ローカル管理のコンピュータ

Personal Edition リカバリファイルを入手するには、以下を行います。

1. **LSARecovery_<systemname>.exe** ファイルという名前のリカバリファイルを見つけます。このファイルは、Personal Edition のインストール中にセットアップウィザードを実行したときにネットワークドライブまたはリムーバブルストレージに保存したものです。
2. ターゲットコンピュータ（データを回復するコンピュータ）に **LSARecovery_<systemname>.exe** をコピーします。

リカバリの実行

1. 先ほど作成した起動可能なメディアを使用して、リカバリシステム上、または回復を試みているドライブを搭載したデバイス上で、そのメディアを起動します。

   WinPE 環境が開きます。
2. **x** と入力し **Enter** キーを押してコマンドプロンプトを起動します。
3. 保存されたリカバリファイルへ移動して起動します。
4. 次の 1 つを選択します。
   - HCA 暗号化済みドライブを復号化します。
   - HCA 暗号化済みドライブへのアクセスを復元します。
5. バックアップおよびリカバリ情報 ダイアログで、サービスタグまたは資産番号が正しいことを確認して、**次へ** をクリックします。
6. コンピュータのボリュームがリストされるダイアログでは、該当するすべてのドライブを選択して **次へ** をクリックします。

   複数のドライブをハイライトするには、**Shift+** クリックまたは **control+** クリックを行います。

   選択されたドライブが **HCA** 暗号化されていない場合、リカバリは失敗します。
7. リカバリパスワードを入力し、**次へ** をクリックします。

   リモート管理のコンピュータでは、これは「リカバリファイルの入手 - リモート管理のコンピュータ」の ステップ 3 で入力したパスワードです。

   ローカル管理のコンピュータでは、このパスワードは、キーがエスクローされたときに、Personal Edition のシステムに設定された、暗号化管理者パスワードです。
8. 回復 ダイアログで、**回復** をクリックします。リカバリプロセスが開始されます。
9. プロンプトで指示された場合、保存されたリカバリファイルに移動して、**OK** をクリックします。

   完全な復号化を実施する場合、以下のダイアログがステータスを表示します。このプロセスには時間がかかる場合があります。
10. リカバリが正しく完了したことを示すメッセージが表示されたら、**終了** をクリックします。コンピュータが再起動します。

コンピュータの再起動後、コンピュータは完全に機能した状態になります。引き続き問題が発生する場合は、Dell ProSupport にお問い合わせください。

4

自己暗号化ドライブ（SED）リカバリ

SED リカバリでは、以下の方法を通して SED 上のファイルへのアクセスを回復することができます。

- ドライブの一回限りのアンロックを実施して、軌道前認証（PBA）を迂回、削除します。
  - リモート管理の SED クライアントでは、PBA はリモート管理コンソールによってその後再度有効化することができます。
  - ローカル管理の SED クライアントでは、PBA はセキュリティツール管理者コンソールによって有効化することができます。
- アンロックして、ドライブから永続的に PBA を削除します。PBA が削除されると、シングルサインオンが機能しなくなります。
  - リモート管理 SED クライアントで、PBA を将来再度有効化できるようにして PBA を削除するには、リモート管理コンソールで製品を無効化する必要があります。
  - ローカル管理 SED クライアントで、PBA を将来再度有効化できるようにして PBA を削除するには、OS 内で製品を無効化する必要があります。

リカバリ要件

SED リカバリには、以下が必要です。

- リカバリ環境 ISO へのアクセス
- 起動可能な CD / DVD または USB メディア

リカバリプロセスの概要

障害が発生したシステムを回復するには、次の手順を実行します。

1. リカバリ ISO を作成して CD/DVD に書き込むか、起動可能な USB を作成します。「補足事項 A - リカバリ環境の書き込み」を参照してください。
2. リカバリファイルを入手します。
3. リカバリを実行します。

SED リカバリの実行

SED リカバリを実行するには、以下の手順に従います。

リカバリファイルの入手 - リモート管理の SED クライアント

1 リカバリファイルを入手します。

リカバリファイルは、リモート管理コンソールからダウンロードすることができます。Dell Data Protection のインストール時に生成された <hostname>-sed-recovery.dat ファイルをダウンロードするには、以下を行います。

a リモート管理コンソールを開き、左ペインから **管理 > データのリカバリ** を選択し、次に **SED** タブを選択します。

b データのリカバリ 画面のホスト名 フィールドに、エンドポイントの完全修飾ドメインネームを入力して **検索** をクリックします。

c SED フィールドでオプションを選択します。

d **リカバリファイルの作成** をクリックします。

<hostname>-sed-recovery.dat ファイルがダウンロードされます。

リカバリファイルの入手 - ローカル管理の SED クライアント

1 リカバリファイルを入手します。

ファイルが生成され、Dell Data Protection | Security Tools がコンピュータにインストールされたときに選択したバックアップロケーションからアクセスできます。ファイル名は、OpalSPkey<systemname>.dat です。

リカバリの実行

1 作成した起動可能なメディアを使用して、リカバリシステム上、またはリカバリを試みているドライブを搭載したデバイス上で、そのメディアを起動します。リカバリアプリケーションと共に WinPE 環境が開きます。

2 オプションを 1 つ選択して、**Enter** キーを押します。

3 **参照** を選択してリカバリファイルを見つけ、**開く** をクリックします。

4 1 つのオプションを選択して、**OK** をクリックします。

- **ドライブの一回限りのアンロック -** この方法は、PBA を迂回して削除します。その後、PBA はリモート管理コンソール（リモート管理 SED クライアントの場合）またはセキュリティツール管理者コンソール（ローカル管理 SED クライアントの場合）を通して再度有効化することができます。
- **ドライブの案ロックおよび PBA の削除 -** この方法はアンロックして PBA をドライブから永続的に削除します。PBA を将来再度有効化できるようにして PBA を削除するには、リモート管理コンソール（リモート管理 SED クライアントの場合）から、または OS 内（ローカル管理 SED クライアントの場合）で製品を無効化する必要があります。PBA が削除されると、シングルサインオンが機能しなくなります。

5 これでリカバリが完了しました。任意のキーを押してメニューに戻ります。

6 **r** キーを押してコンピュータを再起動します。

メモ： コンピュータを起動するのに使用した USB、CD / DVD メディアを必ず取り外してください。取り外すのを忘れると再度リカバリ環境で起動してしまうことがあります。

7 コンピュータの再起動後、コンピュータは完全に機能した状態になります。引き続き問題が発生する場合は、Dell ProSupport にお問い合わせください。

5

General Purpose Key のリカバリ

General Purpose Key (GPK) は、ドメインユーザーのレジストリの一部を暗号化するために使用されます。ただし、起動プロセス中、まれに、破損され復号化に失敗することがあります。その場合、クライアントコンピュータの CMGShield.log ファイルに以下のエラーが表示されます。

```
[12.06.13 07:56:09:622 GeneralPurposeK: 268] GPK - Failure while unsealing data [error = 0xd]
[12.06.13 07:56:09:622 GeneralPurposeK: 631] GPK - Unseal failure
[12.06.13 07:56:09:622 GeneralPurposeK: 970] GPK - Failure to get keys for the registry driver
```

GPK が復号化に失敗した場合、サーバーからダウンロードされたリカバリバンドルから GPK を解凍することで回復する必要があります。

GPK の回復

リカバリファイルの入手

Dell Data Protection のインストール時に生成された **LSARecovery_<machinename_domain.com>.exe** ファイルをダウンロードするには、以下を行います。

1. リモート管理コンソールを開き、左ペインから **管理 > エンドポイントの回復** を選択します。
2. ホスト名 フィールドに、エンドポイントの完全修飾ドメインネームを入力して **検索** をクリックします。

3 強化リカバリ ウィンドウでリカバリパスワードを入力し、**ダウンロード** をクリックします。

メモ： このパスワードは、リカバリキーへのアクセスのために覚えておかなければなりません。

LSARecovery_<machinename_domain.com>.exe ファイルがダウンロードされます。

リカバリの実行

1 補足事項 A - リカバリ環境の書き込み で作成した起動可能なメディアを使用して、リカバリシステム上、またはリカバリを試みているドライブを搭載したデバイス上で、そのメディアを起動します。

WinPE 環境が開きます。

2 **x** と入力し **Enter** キーを押してコマンドプロンプトを起動します。

3 リカバリファイルへ移動して起動します。

Encryption クライアント診断ダイアログが開き、リカバリファイルはバックグラウンドで生成されています。

4 管理コマンドプロンプトで、**LSARecovery_<machinename_domain.com>.exe –p <password> -gpk** を実行します。

GPKRCVR.txt をコンピュータに返します。

5 **GPKRCVR.txt** ファイルをコンピュータの OS ドライブのルートにコピーします。

6 コンピュータを再起動します。

GPKRCVR.txt ファイルはオペレーティングシステムに消費され、コンピュータに GPK が再生成されます。

7 プロンプトで指示された場合、再起動します。

6

暗号化済みドライブのデータ回復

対象コンピュータが起動可能でなく、ハードウェア障害がない場合、データの回復は回復環境で起動されたコンピュータで実施することができます。対象コンピュータが起動可能でなく、ハードウェアに障害がある場合、または USB デバイスの場合、データの回復はスレーブに設定されたドライブで起動することで実施することができます。ドライブをスレーブに設定した場合、ファイルシステムを表示したり、ディレクトリを参照することができます。ただし、ファイルを開こうと、またはコピーしようとすると、アクセス拒否 エラーが発生します。

暗号化されたドライブデータの回復

暗号化されたドライブデータを回復するには、以下を行います。

1 コンピュータから DCID / リカバリ ID を取得するには、以下のいずれかのオプションを選択します。

a 共有暗号化データが保存されているいずれかのフォルダで、WSScan を実行します。

「Common」の後に 8 文字の DCID / リカバリ ID が表示されます。

b リモート管理コンソールを開きエンドポイントの **詳細およびアクション** タブを選択します。

c エンドポイントの詳細画面のシールド詳細セクションにおいて、DCID / リカバリ ID を見つけます。

2 サーバーからキーをダウンロードするには、**Dell Administrative Unlock (CMGAu)** ユーティリティに移動して実行します。

Dell Administrative Unlock ユーティリティは、Dell ProSupport から入手できます。

3 Dell Administrative Utility (CMGAu) ダイアログで、以下の情報（フィールドによっては予め入力されていることがあります）を入力して **次へ** をクリックします。

サーバー： サーバーの完全修飾ホスト名、例えば：

デバイスサーバー：**https://<server.organization.com>:8081/xapi**

セキュリティサーバー：**https://<server.organization.com>:8443/xapi/**

デル管理者： フォレンジック管理者のアカウント名（サーバーで有効化されます）

デル管理者パスワード：フォレンジック管理者のアカウント名（サーバーで有効化されます）

MCID： MCID フィールドをクリアします。

DCID： 前述で取得した DCID / リカバリ ID

4 Dell Administrative Utility ダイアログで **いいえ、今すぐサーバーからのダウンロード実施** を選択して、**次へ** をクリックします。

メモ： Encryption クライアントがインストールされていない場合、メッセージは ロック解除に失敗しました を表示します。Encryption クライアントがインストールされているコンピュータに移動してください。

5 ダウンロードおよびロック解除が完了したら、ドライブから回復する必要のあるファイルをコピーします。すべてのファイルは読み出し可能です。**ファイルの回復を完了するまで 終了 をクリック しない でください。**

6 ファイルを回復してから、ファイルを再度ロックするには、**終了** をクリックします。

終了 のクリック後、暗号化されたファイルは使用不可となります。

7

BitLocker Manager リカバリ

データを回復するには、リモート管理コンソールからリカバリパスワードまたはキーパッケージを取得します。これにより、コンピュータのデータのロックを解除できるようになります。

データの回復

1 リモート管理コンソールに Dell 管理者としてログインします。

2 左ペインで、**管理 > データの回復** をクリックします。

3 マネージャ タブをクリックします。

4 BitLocker の場合：

BitLocker から取得した**リカバリ ID** を入力します。オプションとしてホスト名とボリュームを入力すると、リカバリ ID が自動入力されます。

リカバリパスワードの取得 または **キーパッケージの作成** をクリックします。

希望するリカバリ方法に応じて、データの回復にこのリカバリパスワードまたはキーパッケージを使用します。

TPM の場合：

ホスト名 を入力します。

リカバリパスワードの取得 または **キーパッケージの作成** をクリックします。

希望するリカバリ方法に応じて、データの回復にこのリカバリパスワードまたはキーパッケージを使用します。

5 リカバリを完了するには、Microsoft の回復手順 を参照してください。

メモ： BitLocker Manager が TPM を「所有」していない場合、TPM パスワードおよびキーパッケージを Dell データベースで使用できません。その場合は、キーが見つからないというエラーメッセージが表示されます。この動作は予期されたものです。

BitLocker Manager 以外のエンティティによって「所有」されている TPM を回復するには、その特定の所有者から TPM を回復するプロセスに従うか、既存の TPM リカバリのための既存プロセスに従う必要があります。

A

補足事項 A - リカバリ環境の書き込み

CD / DVD へのリカバリ環境 ISO の書き込み

次のリンクには Microsoft Window 7 / 8 / 10 でリカバリ環境のための起動可能 CD または DVD を作成するのに必要な過程が記載されています。

http://windows.microsoft.com/en-us/windows7/burn-a-cd-or-dvd-from-an-iso-file

リムーバブルメディアへのリカバリ環境の書き込み

起動可能な USB を作成するには、次の Microsoft の記事に記載されている手順に従ってください：

https://technet.microsoft.com/en-us/library/jj200124(v=ws.11).aspx


0XXXXXA0X