Dell Data Protection

リカバリガイド v8.13/v1.7/v1.4/v1.2

メモ、注意、警告

メモ: 製品を使いやすくするための重要な情報を説明しています。

注意: ハードウェアの損傷やデータの損失の可能性を示し、その問題を回避するための方法を説明しています。

警告: 物的損害、けが、または死亡の原因となる可能性があることを示しています。

Dell Data Protection リカバリガイド

2017 - 04

Rev. A01

目次

1

リカバリを開始する前に

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 に書き込む場合は、「リカバリ環境 ISO の CD または DVD への書き込み」で詳細を確認してください。
  - USB メディアを使用する場合は、「リムーバブルメディアへのリカバリ環境の書き込み」で詳細を確認してください。
- 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。

Dell ProSupport へのお問い合わせ

Dell Data Protection 製品向けの 24 時間 365 日対応電話サポート（877-459-7304、内線 431003）に電話をかけてください。

さらに、dell.com/support で Dell Data Protection 製品のオンラインサポートもご利用いただけます。オンラインサポートでは、ドライバ、マニュアル、テクニカルアドバイザリー、よくあるご質問（FAQ）、および緊急の問題を取り扱っています。

適切なサポート担当者に迅速におつなぎするためにも、お電話の際はお客様のサービスコードをご用意ください。

米国外の電話番号については、Dell ProSupport の国際電話番号をチェックしてください。

Policy-Based 暗号化リカバリまたはファイル / フォルダ暗号化リカバリ

Policy-Based 暗号化リカバリまたはファイル / 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復元できます。

- 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 リカバリ環境を CD または DVD に書き込むか、起動可能な USB を作成します。「付録 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。

Policy-Based 暗号化リカバリまたは FFE リカバリの実行

Policy-Based 暗号化リカバリまたは 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

<machinename_domain.com>.exe ファイルをダウンロードするには、次の手順に従います。

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 を起動したときにアクセスできる場所に **<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** という名前のリカバリファイルに移動します。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 対象コンピュータ (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** を入力して **Enter** を押し、コマンドプロンプトを表示します。

3 リカバリファイルに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、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 Policy-Based 暗号化、または 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て、**次へ** をクリックします。
リモート管理クライアントでは、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」の手順 3 で指定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。

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すると、またはファイルを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 桁の 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 **詳細とアクション** 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：サーバの完全修飾ホスト名。たとえば、次のようなホスト名です。

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

セキュリティサーバ：**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パスワード（サーバで有効化されます）

MCID：MCID フィールドをクリアします

DCID：前の手順で取得した DCID / リカバリ ID

4 Dell Administrative Utility ダイアログで、**いいえ。サーバからのダウンロードを今すぐ実行します** を選択し、**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、アンロックが失敗したことを示すメッセージが表示されます。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。**ファイルが回復されるまで、終了をクリックしないでください。**

6 ファイルの回復後、ファイルを再度ロックする準備ができたら、**終了** をクリックします。
終了 をクリックすると、暗号化済みファイルは使用不可となります。

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 リカバリ環境を CD または DVD に書き込むか、起動可能な USB を作成します。「付録 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。

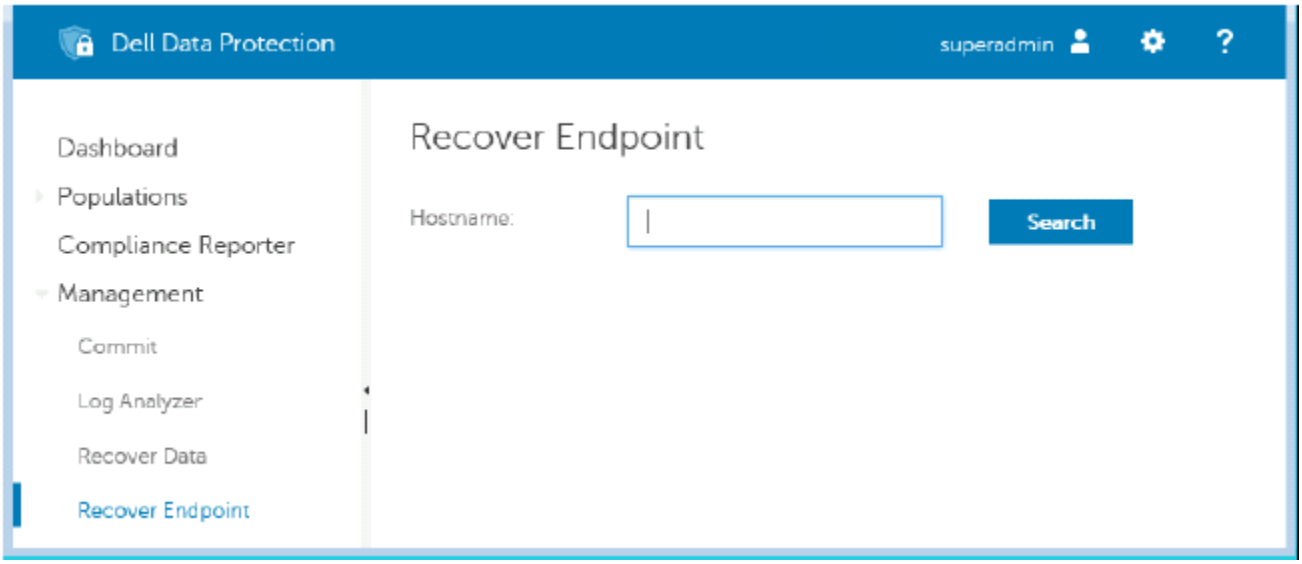
HCA リカバリの実行

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 **<machinename_domain.com>.exe** ファイルをダウンロードするには、以下の手順に従います。

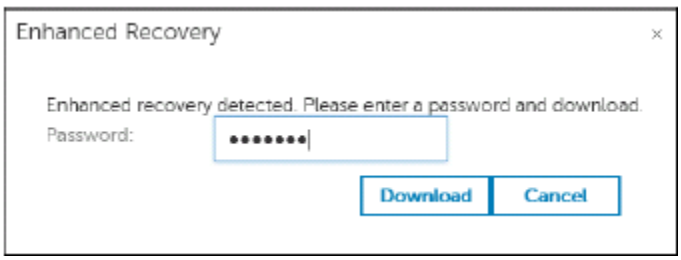
1 リモート管理コンソールを開き、左ペインから **管理** > **エンドポイントの回復** を選択します。



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。



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** という名前のリカバリファイルに移動します。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 対象コンピュータ (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** を入力して **Enter** を押し、コマンドプロンプトを表示します。

3 保存された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アセット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、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、回復は失敗します。

7 リカバリパスワードを入力して、**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」の手順 3 で指定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、保存されている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 リカバリ環境を CD または DVD に書き込むか、起動可能な USB を作成します。「付録 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

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、次の手順に従います。

a リモート管理コンソールを開き、左側のペインから、**管理、データの回復** の順に選択して **SED** タブを選択します。
b データの回復 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

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 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。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** を押します。

3 **参照** を選択してリカバリファイルを確認し、**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。

- **ドライブを一回限りアンロックする**：この方法を選択すると、PBA がバイパスされ削除されます。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。
- **ドライブをアンロックして PBA を削除する**：この方法を選択すると、ドライブがアンロックされ、ドライブから PBA が永久的に削除されます。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** 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 **<machinename_domain.com>.exe** ファイルをダウンロードするには、以下の手順に従います。

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。

<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 リカバリ環境の起動可能なメディアを作成します。手順については、「付録 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。
3 **x** を入力して **Enter** を押し、コマンドプロンプトを表示します。
4 リカバリファイルに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。
5 管理者のコマンドプロンプトで、**<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。
6 **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。
7 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。

8 プロンプトで指示された場合、再起動します。

6

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 左のペインで、**管理**、**データの回復** の順にクリックします。
3 **管理者** タブをクリックします。
4 *BitLocker* の場合：
BitLocker から受け取った**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 によるリカバリ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デルデータベースで使用することはできません。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、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。

7

パスワードリカバリ

ユーザーは自分のパスワードをよく忘れます。その場合、幸いにも、プリブート認証によりコンピュータへのアクセス権を取り戻す方法がいくつかあります。

- リカバリ質問機能は、質問と回答によって認証する機能です。
- チャレンジ / 応答コードにより、管理者の手を借りてコンピュータへのアクセス権を取り戻すことができます。この機能は、組織によって管理されているコンピュータを持つユーザーのみが使用できます。

リカバリ質問

ユーザーが初めてコンピュータにサインインすると、管理者が設定した標準質問セットに回答するように求められます。これらの質問への回答を登録すると、次回パスワードを忘れたとき、ユーザーはその回答を要求されます。質問に正しく回答すると、サインインできるようになり Windows へのアクセス権を取り戻すことができます。

前提条件

- リカバリ質問は、管理者によってセットアップされている必要があります。
- ユーザーは、質問への回答を登録しておく必要があります。
- **サインインできない場合** メニューオプションをクリックする前に、ユーザーは有効なユーザー名とドメインを入力しておく必要があります。

PBA サインイン画面からリカバリ質問にアクセスするには、次の手順に従います。

1 有効なドメイン名およびユーザー名を入力します。
2 画面の左下隅で **オプション**、**サインインできない場合** の順にクリックします。
3 Q&A ダイアログが表示されたら、初回サインイン時にリカバリ質問に登録したときに提供した回答を入力します。

チャレンジ / 応答コード

チャレンジ / 応答リカバリでは、PBA を通して認証を行い、Windows にアクセスすることができます。チャレンジ / 応答は、以下の場合に使用できます。

- ユーザーがリカバリ質問を登録する際に提供した回答を覚えてない場合。
- 管理者がリカバリ質問機能を有効にしていない場合。
- ユーザーがネットワーク接続のない離れた場所にいるため、セキュリティサーバから SED デバイスコントロールを通してアンロックコマンドを受け取れない場合。

ユーザーが **サインインできない場合** オプションをクリックした場合、またはパスワードを誤って入力し、パスワード最大入力回数に達してしまった場合は、ネットワークケーブルが接続されていないときでも チャレンジ / 応答 画面が表示されます。リカバリ質問が無効になっている場合は、**サインインできない場合** オプションを選択すると、チャレンジ / 応答 画面が直接開きます。

要件

- チャレンジ / 応答リカバリは、組織または企業がリモートに管理しているドメインコンピュータでのみ使用できます。

前提条件

- リカバリ質問に回答する前、またはチャレンジ / 応答コードを入力する前に、コンピュータをネットワークから切断します。
- サインインできない場合 をクリックする前に、有効なユーザー名とドメインを入力します。

チャレンジ / 応答リカバリを使用する方法

1 ユーザーは **オプション** リンクをクリックしてメニューを表示します。

2 ユーザーは **サインインできない場合** > **チャレンジ / 応答** の順にクリックします。

> **メモ:**
> チャレンジ / 応答 オプションは、企業が管理しているコンピュータでのみ使用できます。ドメイン外のコンピュータの場合、チャレンジ / 応答 オプションはメニューに表示されません。

3 画面が表示されたら、ユーザーはヘルプデスクに連絡し、管理者にデバイス名（ホスト名）とチャレンジコードを提供します。

4 管理者は、リモート管理コンソールを開いて **管理** > **データの回復** の順にクリックし、上部のメニューの **SED** をクリックします。

5 管理者は、SED ユーザーアクセスの回復 に、ユーザーから取得した**ホスト名**を入力して、**検索** をクリックします。

6 管理者は、該当ユーザーの名前を選択します。

7 ユーザーから取得したデバイスコードを **チャレンジ** フィールドに入力し、**応答を生成** をクリックします。

8 生成された応答コードをユーザーに提供します。

> **メモ:**
> これらのコードでは、大文字と小文字は区別されません。数字は赤で、文字は青で表示されます。

9 ユーザーは、PBA サインイン画面の **応答コード** フィールドに、応答コードを入力します。以下に、ユーザーが入力する応答コードの例を示します。

10 右矢印をクリックして続行し、PBA 画面で認証します。

11 **送信** をクリックします。

チャレンジ / 応答機能を使用して PBA で認証できるのは 1 回だけです。コンピュータを再起動すると、PBA レイヤによってコンピュータの保護が再開されます。また、PBA 画面では、ユーザーはサインインを求められます。

> **メモ:**
> チャレンジ / 応答 ダイアログを表示したユーザーは、チャレンジ / 応答シーケンスを完了して、システムへのアクセスを復元する必要があります。ユーザーがコンピュータの電源を一旦オフにして再ログインしようとした場合、使用したパスワードが正しい場合でも、PBA によってチャレンジ / 応答 ダイアログが再表示されます。

8

外付けメディアシールドのパスワードリカバリ

外付けメディアシールド (EMS) を使用して、ユーザーにユニバーサルシリアルバス (USB) フラッシュドライブや他のリムーバブルストレージメディアの暗号化を許可すると、組織内部と外部の両方のリムーバブルストレージメディアを保護することができます。ユーザーは、保護する各リムーバブルメディアデバイスにパスワードを割り当てます。このセクションでは、ユーザーがデバイスのパスワードを忘れたときに、暗号化された USB ストレージデバイスへのアクセスを復元するプロセスについて説明します。

データへのアクセスの回復

ユーザーがパスワードの試行許可回数を超えて自分のパスワードが何回も間違って入力すると、USB デバイスは手動認証モードになります。

手動認証 は、サーバにログインしている管理者に、クライアントからコードを提供するプロセスです。

手動認証モードでは、ユーザーがパスワードをリセットして自分のデータへのアクセス権を取り戻すための 2 つのオプションがあります。

管理者がアクセスコードをクライアントに提供し、ユーザーが自分のパスワードをリセットして自分の暗号化データへのアクセスを取り戻すことを許可します。

1 パスワードの入力を求められたら、**忘れた場合** ボタンをクリックします。

確認のダイアログが表示されます。

2 **はい** をクリックして確定します。確定後に、デバイスは手動認証モードになります。

3 ヘルプデスク管理者に連絡し、ダイアログに表示されるコードを伝えます。

4 ヘルプデスク管理者として、リモート管理コンソールへログインします。ヘルプデスク管理者のアカウントにはヘルプデスク権限がついていることが必要です。

5 左ペインの **データの回復** メニューオプションに進みます。

6 エンドユーザーから提供されたコードを入力します。

7 画面の右下隅にある **応答を生成** ボタンをクリックします。

8 ユーザーにアクセスコードを与えます。

> **メモ:**
> アクセスコードを提供する前に手動でユーザーを認証するようにします。たとえば、ユーザーに対して「従業員 ID 番号を教えてください」など、本人しかわからない質問をいくつかします。またはユーザーをヘルプデスクに来て ID を見せるように要請し、メディアのオーナーであることを確認します。電話でのユーザー認証に失敗したにもかかわらず、アクセスコードを提供すると、暗号化されたリムーバブルメディアへのアクセス権を攻撃者に与えてしまう可能性があります。

9 暗号化されたメディアのパスワードをリセットします。

暗号化されたメディアのパスワードをリセットするように求められます。

自己復元

自己復元は、メディアの所有者がログインしている保護マシンにドライブを挿入することで、暗号化されたリムーバブルメディアデバイスのパスワードをリセットするプロセスです。メディアの所有者が、保護された Mac または PC に認証されている限り、クライアントはキーマテリアルの消失を検知し、ユーザーにデバイスを再初期化するよう求めます。その時点で、ユーザーはパスワードをリセットし、暗号化されたデータへのアクセスを取り戻すことができます。

1 メディアの所有者として Dell Data Protection の暗号化されたワークステーションにサインインします。
2 暗号化されたリムーバブルストレージデバイスを挿入します。
3 プロンプトが表示されたら、新しいパスワードを入力し、リムーバブルストレージデバイスを再初期化します。
成功した場合、パスワードが受け入れられたことを示す小さな通知が表示されます。
4 ストレージデバイスに移動し、データにアクセスできるかを確認します。

9

Dell Data Guardian のリカバリ

リカバリツールでは、以下を実施できます。

- 保護された Office ファイルの復号化

  これにはトリプル暗号化まで含まれます。ファイルが 2 つ以上の方法で暗号化されていると、ファイルがダブルやトリプルで暗号化されている場合があります。そのようなファイルを開くと、管理者にリカバリ方法を確認するようにエラーメッセージが表示されます。
- キーマテリアルのエスクロー
- 改ざんされたファイルをチェックする機能
- 保護された Office ドキュメント (たとえばクラウドまたは Data Guardian のないデバイス上で、保護されている Office ファイルのカバーページ) のラッパーが改ざんされた場合に、そのファイルを強制的に復号化する機能

リカバリ要件

要件は次のとおりです。

- リカバリするエンドポイントで Microsoft .Net Framework 4.5.2 が実行されていること。
- リモート管理コンソールにおいて、リカバリを実行する管理者に、フォレンジック管理者役割が与えられていること。

Data Guardian のリカバリの実行

Data Guardian の保護された Office ドキュメントのリカバリを実行するには、次の手順を実行します。

Windows、USB フラッシュドライブ、またはネットワークドライブからリカバリを実行

リカバリを実行するには、次の手順に従います。

1 デルのインストールメディアから、**RecoveryTools.exe** を、次のいずれかにコピーします。

- コンピュータ - Office ドキュメントをリカバリするコンピュータに.exe をコピーします。
- USB - USB フラッシュドライブに.exe をコピーし、USB フラッシュドライブから.exe を実行します。
- ネットワークドライブ

2 **RecoveryTools.exe** をダブルクリックしてリカバリツールを起動します。

3 Data Guardian ウィンドウで、Dell サーバの URL を以下の形式で入力します。

https://<server.domain.com>:8443/cloud

> **メモ:**
> <server.domain.com> を、そのエンドポイントで Data Guardian を管理する Dell サーバの完全修飾ホスト名に交換します。Dell サーバの URL を探すには、システムトレイにある Data Guardian アイコンをクリックし、**詳細** をクリックします。詳細画面の左上隅に、サーバの URL が表示されます。

4 ユーザー名とパスワードを入力して **ログイン** をクリックします。

メモ:
管理者に指示されない限り、*SSL* トラストを有効にする チェックボックスをクリアしないでください。

メモ:
フォレンジック管理者でない者が資格情報を入力すると、ログイン権限を持っていないことを示すメッセージが表示されます。

フォレンジック管理者である場合は、リカバリツールが開きます。

5 **ソース** を選択します。

メモ:
ソースおよび宛先に移動する必要がありますが、どちらを先に選択してもかまいません。

6 **参照** をクリックして、リカバリするフォルダまたはドライブを選択します。

7 **OK** をクリックします。

8 **宛先** をクリックします。

9 **参照** をクリックして、外付けデバイス、ディレクトリの場所、デスクトップなど、宛先を選択します。

10 **OK** をクリックします。

11 リカバリする内容に基づいて、1 つ以上のチェックボックスを選択します。

オプション	説明
エスクロー	• Dell サーバにエスクローできなかったオフライン生成キーをリカバリします。 • ネットワークに接続されていないときにハードドライブが故障した場合は、スレーブドライブを使用して、データおよび非エスクローキーをコンピュータからリカバリしてください。
復号化済み	リカバリツールを保護された Office ドキュメントを含むディレクトリに向け、復号化します。 改ざんが発生した場合は、オプションとして、次のいずれか、または両方のオプションを選択します (詳細は下記参照)。 • **改ざんチェック** - 改ざんファイルがあるかどうかを確認しますが復号化しません。 • **改ざんチェック** および **改ざんされていても強制的に復号化する** - 改ざんファイルがあるかどうかを確認し、保護された Office ドキュメントのラッパーが改ざんされている場合、Data Guardian はラッパーを修復し Office ドキュメントを復号化します。
改ざんチェック	改ざんされたファイルを検知して、ログに記録するか管理者に通知します。ファイルを改ざんした作成者をログに記録します。ファイルは復号化されません。
改ざんされていても強制的に復号化する	このオプションを選択するには、**改ざんチェック** も選択する必要があります。 クラウドまたは Data Guardian のないデバイス上で、未承認者が保護された Office ドキュメント (カバーページなど) を改ざんした場合は、このオプションを選択してラッパーを修復し、保護された Office ファイルを強制的に復号化します。 **メモ :** ラッパー内の暗号化された Office .xen ファイルが改ざんされた場合、そのファイルはリカバリできません。

保護されている各 Office ドキュメントには、オリジナルのユーザーとコンピュータ名、およびファイルを変更した他のコンピュータ名の履歴を含む隠し情報があります。デフォルトでは、リカバリツールは隠し情報をチェックして情報をログに記録します。

12 選択を完了したら、**スキャン** をクリックします。

ログ領域には以下が表示されます。

- 選択したソース内で見つかり、スキャンされたフォルダ
- 復号化が成功したか失敗したかどうか

リカバリツールにより、リカバリされたファイルが選択した宛先に追加されます。ファイルを開いて表示することができます。

付録 A - リカバリ環境の書き込み

マスターインストーラをダウンロードできます。

リカバリ環境 ISO の CD または DVD への書き込み

次のリンクには、Microsoft Window 7、Windows 8、または Windows 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プロセス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