



## 暗号化の管理

- [SED 暗号化 \(1 ページ\)](#)
- [HyperFlex ソフトウェア暗号化 \(12 ページ\)](#)

## SED 暗号化

### 自己暗号化ドライブの概要

自己暗号化ドライブ (SED) には、着信データの暗号化と発信データの復号化をリアルタイムで行う特殊なハードウェアが備わっています。ディスク上のデータは常に暗号化された形で保存されます。この暗号化と復号化は、メディア暗号キーによって制御されます。このキーがプロセッサやメモリに保管されることは決してありません。

メディア暗号キーの暗号化には、セキュリティキー (キー暗号キーまたは認証パスフレーズとも呼ばれます) が使用されます。SED を有効にするには、セキュリティキーを提供する必要があります。ディスクがロックされていない場合、データを取得するために必要なキーはありません。

Cisco HyperFlex システムでは、セキュリティキーをローカルまたはリモートで設定できます。ローカルでキーを設定する場合は、キーを覚えておく必要があります。キーを忘れてしまった場合、そのキーを再取得することはできず、ドライブの電源再投入によってデータが失われます。キー管理サーバ (KMIP サーバとも呼ばれる) を使用すると、リモートでキーを設定できます。この方法により、ローカル管理でのキーの保管と取得に伴う問題に対処することができます。

SED の暗号化と復号化はハードウェアを介して行われます。したがって、システムの全体的なパフォーマンスには影響がありません。SED は、瞬間的な暗号化消去によってディスクの廃止コストや再配置コストを削減します。暗号化消去は、メディア暗号キーを変更することによって実行されます。ディスクのメディア暗号キーが変更されると、そのディスク上のデータは復号不能になるので、ただちにデータが使用不可になります。

SED ベースのクラスタでは、暗号化を任意に有効または無効にできます。いつでも2つの状態の間を自由に移動できます。詳細については、[HX Hardening Guide](#) を参照してください。

## HyperFlex クラスタが暗号化に対応するかどうかの確認

を使用して確認する HX データ プラットフォーム プラグイン

1. HX データ プラットフォーム プラグインから vSphere Web クライアントにログインします。
2. [Global Inventory Lists (グローバル インベントリ リスト)] > [Cisco HyperFlex Systems] > [Cisco HX Data Platform] > [Cluster\_Name] > [Summary (概要)] > の順に選択します。
3. HyperFlex クラスタに SED ドライブがあり、暗号化に対応している場合は、[サマリー (Summary)] タブの先頭に [保管中のデータの暗号化可能 (Data At Rest Encryption-Capable)] と表示されます。

HX 接続 ユーザーインターフェイスを使用して確認する

1. HX 接続 UI で、[暗号化 (Encryption)] を選択します。
2. HX クラスタに SED ドライブが含まれていて暗号化可能な場合は、[Encryption] ページに [Data At Rest Encryption-Available] が表示されます。

## ローカル暗号キーの構成

### 手順

ステップ 1 Cisco HyperFlex Connect ナビゲーション ウィンドウで、[暗号化 (Encryption)] を選択します。

ステップ 2 暗号化ページで、[暗号化の設定 (Configure encryption)] をクリックします。

ステップ 3 次の Cisco UCS Manager クレデンシアルを入力します。

UI 要素	基本的な情報
[UCS Manager のホスト名 (UCS Manager host name)] フィールド	Cisco UCS Manager クラスタ ホスト名。 IP アドレスまたは FQDN を入力します。 <eng-fi12.eng.storvisor.com>
[ユーザ名 (User name)] フィールド	<admin> ユーザ名
[パスワード (Password)] フィールド	<admin> password

[次へ (Next)] をクリックします。

**ステップ 4** ローカルに生成/保管される暗号キーを使って HyperFlex クラスタを保護するには、[ローカル キー (Local Key) ] を選択します。

[次へ (Next) ] をクリックします。

**ステップ 5** このクラスタの暗号キー (パスフレーズ) を入力します。

(注) 32 文字ちょうどの英数字を入力します。

**ステップ 6** [暗号化を有効にする (Enable Encryption) ] をクリックします。

## ローカル暗号キーの変更

### 手順

**ステップ 1** Cisco HyperFlex Connect ナビゲーション ウィンドウで、[暗号化 (Encryption) ] を選択します。

**ステップ 2** [暗号化 (Encryption) ] ページで、[鍵の再生成 (Re-key) ] をクリックします。

**ステップ 3** 次の Cisco UCS Manager クレデンシヤルを入力します。

UI 要素	基本的な情報
[UCS Manager のホスト名 (UCS Manager host name) ] フィールド	たとえば、10.193.211.120 とします。
[ユーザ名 (User name) ] フィールド	<管理者> ユーザ名。
[パスワード (Password) ] フィールド	<admin> パスワード。

[次へ (Next) ] をクリックします。

**ステップ 4** クラスタの [既存の暗号化鍵 (Existing Encryption Key) ] と、[新しい暗号化鍵 (New Encryption Key) ] を入力します。

(注) 32 文字ちょうどの英数字を入力します。

**ステップ 5** [鍵の再生成 (Re-key) ] をクリックします。

## ローカル暗号キーの無効化

### 手順

- ステップ 1** Cisco HyperFlex Connect ナビゲーション ウィンドウで、[暗号化 (Encryption)] を選択します。
- ステップ 2** [暗号化 (Encryption)] ページで、[設定の編集 (Edit configuration)] ドロップダウン メニューから [暗号化を無効にする (Disable encryption)] を選択します。
- ステップ 3** 次の Cisco UCS Manager クレデンシアルを入力します。

UI 要素	基本的な情報
[UCS Manager のホスト名 (UCS Manager host name)] フィールド	Cisco UCS Manager クラスタ ホスト名。 IP アドレスまたは FQDN を入力します。 <eng-fi12.eng.storvisor.com>
[ユーザ名 (User name)] フィールド	<admin> ユーザ名
[パスワード (Password)] フィールド	<admin> password

[次へ (Next)] をクリックします。

- ステップ 4** クラスタで暗号キーを無効にするには、クラスタに使用している暗号キーを入力します。
- ステップ 5** [暗号化を無効にする (Disable encryption)] をクリックします。
- ステップ 6** クラスタの暗号キーを無効にする操作を確定するには、[暗号化を無効にしますか? (Disable encryption?)] ダイアログボックスで、[はい、暗号化を無効にします (Yes, disable encryption)] をクリックします。

## 暗号化されたディスクの安全な消去

### 手順

- ステップ 1** Cisco HyperFlex Connect ナビゲーション ウィンドウで、[システム情報 (System Information)] を選択します。
- ステップ 2** [ディスク (Disks)] タブで、ローカル キーを安全に消去するディスクを選択します。
- ステップ 3** [安全に消去する (Secure erase)] ボタンをクリックします。
- ステップ 4** クラスタで暗号化されたディスクを安全に消去するには、クラスタで使用中の暗号化キーを入力します。
- ステップ 5** [安全に消去する (Secure erase)] をクリックします。

ステップ6 [このディスクを消去しますか? (Erase this disk?)] ダイアログボックスで、[はい、このディスクを消去します。 (Yes, erase this disk)] をクリックし、暗号化されたディスクを安全に消去します。

## リモート鍵管理

リモート KMIP 証明書の一般的な処理手順は、次のとおりです。

- 自己署名する場合は、構成でローカル認証局を指定し、ルート証明書を取得します。
- 信頼できるサードパーティ CA を使用する場合は、該当する CA を構成で指定し、そのルート証明書を使用します。
- クラスタ キーの入力を求める HX 暗号化フィールドに、ルート証明書を入力します。
- SSL サーバ証明書を作成し、証明書署名要求 (CSR) を生成します。
- CSR に、使用中のルート証明書で署名を付けます。
- クライアント証明書を使用するよう KMIP サーバ設定を更新します。
- SSL 証明書とルート CA が利用可能になったら、選択したベンダーに固有の KMIP サービス構成に進みます。

### SafeNet キー管理

SafeNet キー管理サーバを使用した暗号化キーの管理に関する詳細については、『[SafeNet Admin Guide](#)』を参照してください。

### Vormetric キー管理

Vormetric キー管理サーバを使用した暗号化キーの管理について詳しくは、『[Vormetric support portal](#)」ドキュメントのダウンロード] セクションを参照してください。

## リモート暗号キーの構成

### 手順

ステップ1 Cisco HyperFlex Connect ナビゲーション ウィンドウで、[暗号化 (Encryption)] を選択します。

ステップ2 暗号化ページで、[暗号化の設定 (Configure encryption)] をクリックします。

ステップ3 次の Cisco UCS Manager クレデンシャルを入力します。

UI 要素	基本的な情報
[UCS Manager のホスト名 (UCS Manager host name)] フィールド	Cisco UCS Manager クラスタ ホスト名。 IP アドレスまたは FQDN を入力します。 <eng-fi12.eng.storvisor.com>

UI 要素	基本的な情報
[ユーザ名 (User name) ]フィールド	<admin> ユーザ名
[パスワード (Password) ]フィールド	<root> パスワード

[次へ (Next) ] をクリックします。

**ステップ 4** キー管理 (KMIP) サーバによって生成されるリモートセキュリティキーを使って HyperFlex クラスタを保護するには、[キー管理サーバ (Key Management Server) ] を選択します。

次の証明書のいずれかを使用して、クラスタ内の自己暗号化ドライブをサーバで構成できます。

- [認証局署名証明書の使用 (Use certificate authority signed certificates) ] : 外部認証局によって署名された証明書署名要求 (CSR) を生成します。
- [自己署名証明書の使用 (Use self-signed certificates) ] : 自己署名証明書を生成します。

[次へ (Next) ] をクリックします。

## ステップ 5

### 次のタスク

新しい証明書署名要求または自己署名証明書を生成できます。

## 証明書署名要求の生成

### 手順

**ステップ 1** Cisco HyperFlex Connect ナビゲーション ウィンドウで、[暗号化 (Encryption) ] を選択します。

**ステップ 2** 暗号化ページで、[暗号化の設定 (Configure encryption) ] をクリックします。

**ステップ 3** 次の Cisco UCS Manager クレデンシャルを入力します。

UI 要素	基本的な情報
[UCS Manager のホスト名 (UCS Manager host name) ]フィールド	Cisco UCS Manager クラスタ ホスト名。 IP アドレスまたは FQDN を入力します。 <eng-fi12.eng.storvisor.com>
[ユーザ名 (User name) ]フィールド	<admin> ユーザ名

UI 要素	基本的な情報
[パスワード (Password) ] フィールド	<admin> password

[次へ (Next) ] をクリックします。

**ステップ 4** [キー管理サーバ (Key Management Server) ] > [認証局署名証明書の使用 (Use certificate authority signedcertificatess) ] を選択します。

[次へ (Next) ] をクリックします。

**ステップ 5** キー管理 (KMIP) サーバを設定するためにリモート暗号化キーを生成するには、次の詳細を入力します。

UI 要素	基本的な情報
[電子メールアドレス (Email address) ] フィールド	<管理者> 電子メールアドレス。
[組織名 (Organization name) ] フィールド	証明書を要求している組織。 32 文字以下で入力します。
[組織単位名 (Organization unit name) ] フィールド	組織ユニット 最大 64 文字まで入力できます。
[Locality] フィールド	証明書を要求している会社の本社が存在する市または町。 32 文字以下で入力します。
[状態 (State) ] フィールド	証明書を要求している会社の本社が存在する州または行政区分。 32 文字以下で入力します。
[国 (Country) ] フィールド	会社が存在する国。 2 文字のアルファベットを大文字で入力します。
[有効日数 (Valid for (days) ) ] フィールド	証明書の有効期間。

**ステップ 6** すべての HyperFlex ノードに対する証明書署名要求 (CSR) を生成してダウンロードするには、[証明書の生成 (Generate certificates) をクリックします。

**ステップ 7** 証明書をダウンロードして、認証局の署名を取得します。[閉じる (Close) ] をクリックします。

### 次のタスク

- 署名された証明書をアップロードします。
- KMIP サーバ (キー管理サーバ) を設定します。

## CSR（証明書署名要求）を使用したキー管理サーバの構成

### 始める前に

まず、生成された CSR をローカルマシンに確実にダウンロードし、その CSR に認証局の署名を付け、Cisco HX Data PlatformUI を使ってアップロードして、KMIP（キー管理）サーバを構成します。

### 手順

- ステップ 1 Cisco HyperFlex Connect ナビゲーション ウィンドウで、[暗号化（Encryption）] を選択します。
- ステップ 2 [暗号化（Encryption）] ページで、[設定の続行（Continue configuration）] をクリックします。
- ステップ 3 [設定の続行（Continue configuration）] ドロップダウンリストから、[証明書の管理（Manage certificates）] を選択して CSR をアップロードします。
- ステップ 4 次の Cisco UCS Manager クレデンシャルを入力します。

UI 要素	基本的な情報
[UCS Manager のホスト名（UCS Manager host name）] フィールド	Cisco UCS Manager クラスタ ホスト名。 IP アドレスまたは FQDN を入力します。 <eng-fi12.eng.storvisor.com>
[ユーザ名（User name）] フィールド	<admin> ユーザ名
[パスワード（Password）] フィールド	<root> パスワード

[次へ（Next）] をクリックします。

- ステップ 5 [認証局署名証明書のアップロード（Upload certificate authority signed certificates）] を選択します。[次へ（Next）] をクリックします。
- ステップ 6 [新しい証明書のアップロード（Upload new certificate）] で、CA 署名付き証明書をアップロードします。[アップロード（Upload）] をクリックします。
- ステップ 7 [設定の続行（Continue configuration）] ドロップダウンリストから、[キー管理サーバの設定（Configure key management server）] を選択して KMIP サーバを構成します。
- ステップ 8 Cisco UCS Manager クレデンシャルを入力して、プライマリ キー管理（KMIP）サーバと、必要に応じてセカンダリ KMIP サーバを設定します。

UI 要素	基本的な情報
[プライマリ キー管理サーバ（Primary key management server）] フィールド	プライマリキー管理サーバのIPアドレスを入力します。

UI 要素	基本的な情報
(オプション) [セカンダリ キー管理サーバ (Secondary key management server) ] フィールド	冗長性を確保するためにセカンダリ キー管理サーバをセットアップした場合は、ここで詳細情報を入力します。
[ポート番号 (Port number) ] フィールド	キー管理サーバに使用するポート番号を入力します。
[公開キー (Public key) ] フィールド	KMIP サーバ構成中に生成された、認証局の公開ルート証明書を入力します。

**ステップ 9** [保存 (Save) ] をクリックします。これで、リモート管理されるキーによってクラスタが暗号化されるようになります。

## 自己署名証明書の生成

### 手順

**ステップ 1** Cisco HyperFlex Connect ナビゲーション ウィンドウで、[暗号化 (Encryption) ] を選択します。

**ステップ 2** 暗号化ページで、[暗号化の設定 (Configure encryption) ] をクリックします。

**ステップ 3** 次の Cisco UCS Manager クレデンシャルを入力します。

UI 要素	基本的な情報
[UCS Manager のホスト名 (UCS Manager host name) ] フィールド	Cisco UCS Manager クラスタ ホスト名。 IP アドレスまたは FQDN を入力します。 <eng-fi12.eng.storvisor.com>
[ユーザ名 (User name) ] フィールド	<admin> ユーザ名
[パスワード (Password) ] フィールド	<root> パスワード

[次へ (Next) ] をクリックします。

**ステップ 4** [キー管理サーバ (Key Management Server) ] > [自己署名証明書を使用 (Use self-signed certificates) ] を選択します。

[次へ (Next) ] をクリックします。

**ステップ 5** キー管理 (KMIP) サーバを設定するためにリモート暗号化キーを生成するには、次の詳細を入力します。

UI 要素	基本的な情報
[電子メールアドレス (Email address) ] フィールド	<管理者> 電子メールアドレス。
[組織名 (Organization name) ] フィールド	証明書を要求している組織。 32 文字以下で入力します。
[組織単位名 (Organization unit name) ] フィールド	組織ユニット 最大 64 文字まで入力できます。
[Locality] フィールド	証明書を要求している会社の本社が存在する市または町。 32 文字以下で入力します。
[状態 (State) ] フィールド	証明書を要求している会社の本社が存在する州または行政区分。 32 文字以下で入力します。
[国 (Country) ] フィールド	会社が存在する国。 2 文字のアルファベットを大文字で入力します。
[有効日数 (Valid for (days) ) ] フィールド	証明書の有効期間。

ステップ 6 すべての HyperFlex ノードの自己署名証明書を生成してダウンロードするには、[証明書の生成 (Generate certificates) ] をクリックします。

ステップ 7 署名付き証明書をアップロードし、KMIP サーバ（キー管理サーバ）を設定します。

## SSC（自己署名証明書）を使用したキー管理サーバの構成

始める前に

KMIP（キー管理）サーバを構成するには、まず、生成された SSC をローカルマシンにダウンロードしたことを確認してください。

手順

ステップ 1 Cisco HyperFlex Connect ナビゲーション ウィンドウで、[暗号化 (Encryption) ] を選択します。

ステップ 2 [暗号化 (Encryption) ] ページで、[設定の編集 (Edit configuration) ] をクリックします。

ステップ 3 [設定の編集 (Edit configuration) ] ドロップダウンリストから、[証明書の管理 (Manage certificates) ] を選択します。

**ステップ 4** 次の Cisco UCS Manager クレデンシャルを入力して、プライマリ キー管理 (KMIP) サーバと、必要に応じてセカンダリ KMIP サーバを設定します。

UI 要素	基本的な情報
[UCS Manager のホスト名 (UCS Manager host name) ] フィールド	Cisco UCS Manager クラスタ ホスト名。 IP アドレスまたは FQDN を入力します。 <eng-fi12.eng.storvisor.com>
[ユーザ名 (User name) ] フィールド	<admin> ユーザ名
[パスワード (Password) ] フィールド	<admin> password

[次へ (Next) ] をクリックします。

**ステップ 5** プライマリおよびセカンダリ キー管理 (KMIP) サーバのクレデンシャルを入力します。

UI 要素	基本的な情報
[プライマリ キー管理サーバ (Primary key management server) ] フィールド	プライマリキー管理サーバのIPアドレスを入力します。
(オプション) [セカンダリ キー管理サーバ (Secondary key management server) ] フィールド	冗長性を確保するためにセカンダリ キー管理サーバをセットアップした場合は、ここで詳細情報を入力します。
[ポート番号 (Port number) ] フィールド	キー管理サーバに使用するポート番号を入力します。
[公開キー (Public key) ] フィールド	KMIP サーバ構成中に生成された、認証局の公開ルート証明書を入力します。

**ステップ 6** [保存 (Save) ] をクリックします。これで、リモート管理されるキーによってクラスタが暗号化されるようになります。

## 暗号化の再起動

### 手順

Cisco UCS Manager クレデンシャルを入力して、キー管理サーバまたはローカル キーの設定を再起動し、HyperFlex クラスタを安全に暗号化します。

UI 要素	基本的な情報
[UCS Manager のホスト名 (UCS Manager host name) ]フィールド	Cisco UCS Manager クラスタ ホスト名。 IP アドレスまたは FQDN を入力します。 <eng-fi12.eng.storvisor.com>
[ユーザ名 (User name) ]フィールド	<admin> ユーザ名
[パスワード (Password) ]フィールド	<admin> password

## HyperFlex ソフトウェア暗号化

### HyperFlex ソフトウェア暗号化を有効にする

以下の表は HyperFlex ソフトウェア暗号化の有効化ワークフローを要約しています。

ステップ	説明	参考資料
1.	[My Cisco Entitlements (MCE) ]から HyperFlex ソフトウェア暗号化パッケージをダウンロードします。	<a href="#">My Cisco Entitlements</a>
2.	管理 CIP にログインして、クラスタ内のすべてのコントローラー VM にパッケージをインストールします。	コマンド <code>priv install-se-core-package</code> を実行します。
3.	暗号化パッケージをインストールします。	<a href="#">HX ソフトウェア 暗号化 パッケージをインストールします : 13 個以上のノードのあるクラスタ (14 ページ)</a> を参照してください。
4.	Intersight の有効化手順に従います。	Intersight <a href="#">HyperFlex ソフトウェア暗号化</a>
5.	クラスタが暗号化されていることを確認してください。	コマンド <code>hxcli encryption info</code> を実行します。



- (注) クラスタで VMware EVC が有効になっている場合は、EVC ベースラインが Advanced Encryption Standards New Instructions (AES-NI) を備えたノードをサポートしていることを確認してください。現在の EVC ベースラインが AES-NI をサポートしていない場合は、ソフトウェア暗号化を有効にする前に EVC 設定を変更してください。

## HyperFlex ソフトウェア暗号化の注意事項と制限事項

HyperFlex ソフトウェア暗号化を有効にする前にこれらの注意事項を確認してください。

- 全ての HyperFlex クラスタ ノードが HXDP リリース 5.0(1b) 以降を実行している場合に HyperFlex ソフトウェア暗号化を有効化することができます。
- HyperFlex ソフトウェア暗号化を使用した HyperFlex ストレッチ クラスタのサポートは、HXDP リリース 5.0(2a) で導入されました。
- SED HyperFlex 構成は、HyperFlex ソフトウェア暗号化でサポートされていません。
- HyperFlex ソフトウェア暗号化は、Vmware ESXi HyperFlex 構成でのみサポートされます。
- HyperFlex ソフトウェア暗号化パッケージを HX クラスタにインストールするには、AES-NI を有効にする必要があります。
- HyperFlex ソフトウェア暗号化は、既存のデータベースで有効にできません。
- HyperFlex ソフトウェア暗号化は、新しく作成されたデータベースにのみ有効にできます。
- HyperFlex ソフトウェア暗号化がクラスタ/データストアに対して有効化されると、クラスタまたはデータストアに対して無効にできません。
- Once HyperFlex ソフトウェア暗号化がクラスタに対して有効化されると、暗号化されたデータストアまたは暗号化されていないデータストアを作成できます。

## HX ソフトウェア暗号化パッケージをインストールします : 1-12 ノードのあるクラスタ

始める前に

[My Cisco Entitlements (MCE) ] から HyperFlex ソフトウェア暗号化パッケージをダウンロードし、[My Cisco Entitlements](#) を参照してください。



- (注) HyperFlex Software Encryption パッケージは独自のソフトウェア PID でライセンスされています。これは HyperFlex Data Platform と Intersight ソフトウェアライセンスの追加です。詳細については、『[Cisco HyperFlex Systems Ordering and Licensing Guide](#)』を参照してください。

## 手順

**ステップ 1** 暗号化パッケージを HyperFlex cip ノード（クラスタ管理 IP を保持するノード）に SFTP で送信します。[ユーザー名/パスワード (**username/password**)] と winscp などのファイル 転送 アプリケーションに管理アカウントを使用します。これは、パッケージを /tmp または /home/admin directory にアップロードするはずです。

**ステップ 2** クラスタのすべての使用可能なノードのパッケージをインストールするために、cip ノードに SSH を実行し、**priv install-package --cluster** オプションを使用します。

例 :

```
priv install-se-core-package --cluster --path /tmp/storfs-se-core_<latest version>_x86_64.deb
```

(注) `--cluster` オプションを使用して暗号化パッケージをインストールするときは、すべてのノードが稼働しており、メンテナンス モードになっていないことを確認してください。

## 次のタスク

Intersight [\[HyperFlex ソフトウェア暗号化 \(HyperFlex Software Encryption\)\]](#) に移動し、クラスタの暗号化を有効にします。

## HX ソフトウェア 暗号化 パッケージをインストールします : 13 個以上のノードのあるクラスタ

## 始める前に

[My Cisco Entitlements (MCE)] から HyperFlex ソフトウェア暗号化パッケージをダウンロードし、[My Cisco Entitlements](#) を参照してください。



(注) HyperFlex Software Encryption パッケージは独自のソフトウェア PID でライセンスされています。これは HyperFlex Data Platform と Intersight ソフトウェア ライセンスの追加です。詳細については、『[Cisco HyperFlex Systems Ordering and Licensing Guide](#)』を参照してください。

## 手順

**ステップ 1** 暗号化パッケージを各 HyperFlex ノードに SFTP で送信します。[ユーザー名/パスワード (**username/password**)] と winscp などのファイル 転送 アプリケーションに管理アカウントを使用します。これは、パッケージを /tmp または /home/admin directory にアップロードするはずです。

**ステップ2** 12 個以上のノードのあるクラスタの場合、各ノードに SSH で接続し、`priv install-package -- local` オプションを使用します。

例：

```
priv install-se-core-package --local --path /home/admin/<package-filename>
```

(注) 次の手順に進む前にクラスタをシャットダウンしないでください。HyperFlex ソフトウェア暗号化が有効になります。クラスタをシャットダウンして再起動した場合は、暗号化パッケージを再インストールする必要があります。

### 次のタスク

Intersight [HyperFlex ソフトウェア暗号化](#) に移動し、クラスタの暗号化を有効にします。

## HyperFlex ソフトウェア暗号化の暗号化キーをバックアップする

暗号キーはクラスタに分散形式の複数のコピーで保管されます。クラスタ全体に影響を与える壊滅的な障害から保護するために、データ損失から保護するために暗号キーの帯域外バックアップを作成することをお勧めします。



(注) HX ソフトウェア暗号化が有効になった後で、キー変更のたびごとの DEK をバックアップすることをお勧めします。以前バックアップした DEK は、クラスタでキー変更を行った後で復元できません。

以前保存したバックアップから失ったり、破損したりした場合、クラスタに暗号化された DEK 構成を復元するには、TAC にお問い合わせください。

### 手順

**ステップ1** `hxcli encryption backup-keys -f <path to file name>` コマンドを実行します。

(注) ファイル名の先頭は `/home/admin/` でなければなりません。

**ステップ2** コマンドが実行されたときにプロンプトされた後で、パスフレーズを入力します。

すべてのパスワードルールに合格した後で、コマンドは暗号化形式でファイルを正常に保存します。

(注) パスフレーズの長さは最低 8 文字で、少なくとも 1 個の小文字、少なくとも 1 個の大文字、少なくとも 1 個の数字、少なくとも 1 個の特殊文字 (`!@#%^&*()_+{}?` のいずれか) を含む必要があります。

## HyperFlex ソフトウェア暗号化の安全なディスク消去

ディスクのベーシック（モード '0'）および標準（モード '1' / モード '2'）サニタイズを行うためのオプションを備えたソフトウェアベースのディスク消去ユーティリティです。分類は主に、サニタイズされるディスクの領域、データ消去の一部としてのドライブ上の上書きサイクルとパターンの数に基づいています。

安全な消去の操作を実施する前に、以下のことを考慮してください。

- 安全なディスク消去 (secure disk erase) は破壊的で不可逆的であり、不適切な使用はデータの損失につながる可能性があります。
- 安全なディスク消去 (secure disk erase) ユーティリティはデフォルトで、選択したディスクにデータの最後のコピーが含まれているかどうかをチェックします。このチェックはバイパスしてはなりません。
- 安全なディスク消去 (secure disk erase) は、サニタイズのモードとドライブのサイズに応じて、時間のかかる操作になる場合があります。
- 管理者モードから安全な消去操作をトリガーできます。
- 複数のディスクを並行してサニタイズできます。

### 制限事項

- ブート ディスク / ハウスキーピング ディスクは、安全な消去が許可されていません。
- ディスクが安全に消去されると、ディスクを同じクラスタに再展開することはできません。
- 安全なディスク消去 (secure disk erase) は、SED ドライブでサポートされていません。
- 安全なディスク消去 (secure disk erase) が進行中のときに、完了するまで同じディスクで消去を実行できません。

### 手順

---

**ステップ 1** `secure_disk_erase` コマンドを実行して、ターゲットディスクの絶対パスを指定します。

例 :

```
-d DISK_PATH, --disk-path DISK_PATH
```

**ステップ 2** 以下のさまざまな消去のモードから選択します。

ベーシック（デフォルト）モードの消去（例 モード '0'） :

例 :

```
admin:~$ secure_disk_erase -d /dev/sdh -m 1
```

```
THIS UTILITY WILL IRRECOVERABLY ERASE DATA FROM DRIVE.PROCEED WITH CAUTION.  
All data (including storfs) from the disk /dev/sdh will be destroyed, proceed [Y/N]:y
```

```
Successfully removed the disk from the system: '/dev/sdh'  
Starting erase operation for disk '/dev/sdh'  
SEAGATE ST1200MM0009 CN03 peripheral_type: disk [0x0]  
<< supports protection information>>  
Unit serial number: WFK25FY70000C917H4GQ  
LU name: 5000c500a762ca2b  
  
Successfully triggered secure erase operation for the disk: '/dev/sdh'  
Please use following command to track the erase progress:  
secure_disk_erase -d /dev/sdh --progress
```

**ステップ 3** 以下のコマンドを使用して消去の進捗をチェックします。

例 :

```
admin:~$ secure_disk_erase -d /dev/sdh --progress  
Fetching the secure erase progress:  
Progress indication: 80.15% don
```

**ステップ 4** 消去プロセスが完了した後で、ノードから消去したドライブを物理的に取り外してください。

---



## 翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。