暗号化の管理

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、ドライフ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な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 ガイド』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 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

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	<*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

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	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

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	<*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?（Disableencryption?）]** 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

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

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

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	<*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

1. 署名された証明書をアップロードします。
2. 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。

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。

例

自己署名証明書の生成

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。

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

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