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、リアルタイムで着信データを暗号化し、発信データを復号化する特別なハードウェアが含まれています。ディスク上のデータは常に暗号化された形式で格納されます。メディアの暗号化キーは、データの暗号化と復号化を制御します。このキーは、プロセッサやメモリに格納されることはありません。

セキュリティ キー（キー暗号化キーまたは認証パスフレーズとも呼ばれます）を使用して、メディア暗号化キーを暗号化します。SED を有効にするには、セキュリティ キーを入力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、データをフェッチするのにキーは必要ありません。

Cisco HyperFlex Systems を使用して、ローカルまたはリモートのセキュリティ キーを構成できます。ローカル キーを構成するときは、キーを忘れないでください。キーを忘れた場合、回復できず、ドライブの電源が再投入されるとデータは失われます。キーは、キー管理サーバ（KMIP サーバとも呼ばれます）を使用してリモートで構成できます。この方法は、ローカル管理のキーの保管および回復に関連する問題に対処します。

SED の復号化と暗号化はハードウェアを介して行われます。したがって、システム全体のパフォーマンスに影響しません。SED は、瞬時暗号化消去によりディスクのリタイアメントと再デプロイメントコストを削減します。暗号化消去はメディア暗号化キーを変更することによって行われます。ディスクのメディア暗号化キーを変更すると、ディスク上のデータは復号化できず、すぐに使用できなくなります。

HyperFlex クラスタが暗号化できることの確認

HX Data Platform プラグイン を使用して確認します

1. HX Data Platform プラグイン から vSphere Web クライアント にログインします。
2. **[Cisco HX Data Platform]** > **[hx_cluster]** > **[概要（Summary）]** を選択します。
3. HyperFlex 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、[概要（Summary）] タブの上部に [保管中のデータの暗号化可能（Data At Rest Encryption-Capable）] が表示されます。

HX Connect ユーザ インターフェイスを使用していることを確認します

1. HX Connect UI から、[暗号化（Encryption）] を選択します。
2. HX HyperFlex 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、[暗号化（Encryption）] ページに [保管中のデータの暗号化対応可（Data At Rest Encryption-Available）] が表示されます。

ローカル暗号化キーの構成

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（Encryption）] 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	基本情報
[UCS Manager のホスト名（UCS Manager host name）] フィールド	Cisco UCS Manager のクラスタ ホスト名です。 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

[Next] をクリックします。

ステップ 4 ローカルで生成され、保存された暗号化キーを使用して 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。

[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）**を入力してください。

（注） ちょうど 32 文字の英数字で入力します。

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

ローカル暗号化キーの変更

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、[再キー（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	**基本情報**
[UCS Manager のホスト名（UCS Manager host name）] フィールド	例：*10.193.211.120*。
[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。

[Next] をクリックします。

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

（注） ちょうど 32 文字の英数字で入力します。

ステップ 5 [再キー（Re-key）] をクリックします。

ローカルの暗号化キーの無効化

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）] ページの [構成の編集（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	基本情報
[UCS Manager のホスト名（UCS Manager host name）] フィールド	Cisco UCS Manager のクラスタ ホスト名です。 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

[Next] をクリックします。

ステップ 4 クラスタで暗号化キーを無効にするには、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 [暗号化を無効にする（Disable encryption）] をクリックします。

ステップ 6 クラスタで暗号化キーを無効にすることを確認するために [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（Yes）] をクリックします。

暗号化されたディスクを安全に消去する

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 **disk** 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 クラスタ上の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）] をクリックして暗号化されたディスクを安全に消去します。

リモート キー管理

リモート KMIP 証明書の処理の一般的な手順は次のとおりです。

- 自己署名する場合は、設定でローカルの証明機関を指定し、ルート証明書を取得します。
- 信頼されたサードパーティの CA を使用する場合は、設定でそれを指定し、そのルート証明書を使用します。
- クラスタ キーを尋ねる 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。
- 使用しているルート証明書で CSR に署名します。
- クライアント証明書を使用する KMIP サーバ設定を更新します。
- SSL 証明書とルート CA が利用可能な状態で、選択したベンダーに固有の KMIP サービス設定で続行します。

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は、『HyperFlex Encryption and SafeNet Key Management TechNote』と『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関する詳細は、Vormetric サポート ポータルのマニュアル ダウンロード セクションを参照してください。

リモート暗号化キーの構成

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（Encryption）] 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	基本情報
[UCS Manager のホスト名（UCS Manager host name）] フィールド	Cisco UCS Manager のクラスタ ホスト名です。 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

[Next] をクリックします。

ステップ 4 キー管理（KMIP）サーバよって生成されたリモート セキュリティ キーを使用して 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 1 つを使用するためにクラスタ内の自己暗号化ドライブを持つサーバを構成できます。

- [証明機関署名付きの証明書を使用する（Use certificate authority signed certificates）]：外部証明機関によって署名された証明書署名要求（CSR）を生成します。
- [自己署名の証明書を使用する（Use self-signed certificates）]：自己署名の証明書を生成します。

[Next] をクリックします。

ステップ 5

次のタスク

証明書署名要求または自己署名の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（Encryption）] 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	基本情報
[UCS Manager のホスト名（UCS Manager host name）] フィールド	Cisco UCS Manager のクラスタ ホスト名です。 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

[Next] をクリックします。

ステップ 4 [キー管理サーバ（Key Management Server）] > [証明機関署名の証明書を使用する（Use certificate authority signed certificates）] を選択します。

[Next] をクリックします。

ステップ 5 キー管理（KMIP）サーバを構成するリモート暗号化キーを生成するには、次の詳細を完了します。

UI 要素	基本情報
[電子メール アドレス（Email address）] フィールド	<*admin*> 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 文字以内で入力します。
[組織ユニット名（Organization unit name）] フィールド	組織ユニット。 64 文字以内で入力します。
[地域（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 文字以内で入力します。
[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 文字以内で入力します。
[国（Country）] フィールド	会社が存在する国。 2 つの英字を大文字で入力します。
[有効な日数（Valid for (days)）] フィールド	証明書の有効期間。

ステップ 6 HyperFlex のすべてのノードのための証明書署名要求（CSR）を生成してそれらを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、証明機関によって署名された証明書を取得します。[閉じる（Close）] をクリックします。

次のタスク

1. 署名付き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

KMIP（キーマネージメント）サーバを構成するために、ローカルマシン上で生成されたCSRをダウンロードし、それが証明機関によって署名され、Cisco HX Data Platform UI 経由でアップロードされている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、[構成の続行（Continue configuration）] をクリックします。

ステップ 3 [構成の続行（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	基本情報
[UCS Manager のホスト名（UCS Manager host name）] フィールド	Cisco UCS Manager のクラスタ ホスト名です。 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

[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。[Next] をクリックします。

ステップ 6 [新規証明書のアップロード（Upload new certificate）] で CA 署名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 [構成の続行（Continue configuration）] ドロップダウン リストから [キー管理サーバ の構成（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 のクレデンシャルを入力して、プライマリ キー管理サーバ（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。
（省略可能）[セカンダリ キー管理サーバ（Secondary key management server）] フィールド	冗長化のためのセカンダリ キー管理サーバを設定した場合は、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証明書機関の公開ルート証明書を入力します。

ステップ 9 [保存（Save）] をクリックしてクラスタをリモート管理キーで暗号化します。

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（Encryption）] 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	基本情報
[UCS Manager のホスト名（UCS Manager host name）] フィールド	Cisco UCS Manager のクラスタ ホスト名です。 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

[Next] をクリックします。

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

[Next] をクリックします。

ステップ 5 キー管理（KMIP）サーバを構成するリモート暗号化キーを生成するには、次の詳細を完了します。

UI 要素	基本情報
[電子メール アドレス（Email address）] フィールド	<*admin*> 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 文字以内で入力します。
[組織ユニット名（Organization unit name）] フィールド	組織ユニット。 64 文字以内で入力します。
[地域（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 文字以内で入力します。

UI 要素	基本情報
[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 文字以内で入力します。
[国（Country）] フィールド	会社が存在する国。 2 つの英字を大文字で入力します。
[有効な日数（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それらを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、証明機関によって署名された証明書を取得します。[閉じる（Close）] をクリックします。

次のタスク

1. 署名付き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。

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 マネージメント）サーバを構成するためにローカル マシン上で生成された SSC がダウンロードされている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、[構成の編集（Edit configuration）] をクリックします。

ステップ 3 [構成の編集（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 の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	基本情報
[UCS Manager のホスト名（UCS Manager host name）] フィールド	Cisco UCS Manager のクラスタ ホスト名です。 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

[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。
（省略可能）[セカンダリ キー管理サーバ（Secondary key management server）] フィールド	冗長化のためのセカンダリ キー管理サーバを設定した場合は、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証明書機関の公開ルート証明書を入力します。

ステップ 6 [保存（Save）] をクリックしてクラスタをリモート管理キーで暗号化します。

暗号化のやり直し

Cisco UCS Manager のクレデンシャルを入力して、HyperFlex クラスタを安全に暗号化するための、キー管理サーバまたは ローカル キーの構成を再起動します。

UI 要素	基本情報
[UCS Manager のホスト名（UCS Manager host name）] フィールド	Cisco UCS Manager のクラスタ ホスト名です。 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