



# ネットアップのハードウェアベースの暗号化を 設定 ONTAP 9

NetApp  
April 24, 2024

# 目次

ネットアップのハードウェアベースの暗号化を設定 .....	1
ネットアップのハードウェアベースの暗号化の概要を設定 .....	1
外部キー管理を設定 .....	3
オンボードキー管理を設定 .....	15
FIPS ドライブに FIPS 140-2 認証キーを割り当てます .....	22
KMIP サーバ接続に対して、クラスタ全体の FIPS 準拠モードを有効にします .....	23

# ネットアップのハードウェアベースの暗号化を設定

## ネットアップのハードウェアベースの暗号化の概要を設定

ネットアップのハードウェアベースの暗号化は、データ書き込み時の Full Disk Encryption（FDE）をサポートします。ファームウェアに格納された暗号化キーがないとデータを読み取ることはできません。暗号化キーには認証されたノードからしかアクセスできません。

### ネットアップのハードウェアベースの暗号化について理解する

ノードは、外部キー管理サーバまたはオンボードキーマネージャから取得した認証キーを使用して自己暗号化ドライブへの認証を行います。

- 外部キー管理サーバはストレージ環境に配置されたサードパーティのシステムで、Key Management Interoperability Protocol（KMIP）を使用してノードにキーを提供します。外部キー管理サーバは、データとは別のストレージシステムで設定することを推奨します。
- オンボードキーマネージャは組み込みのツールで、データと同じストレージシステムからノードに認証キーを提供します。

NetApp Volume Encryption をハードウェアベースの暗号化とともに使用すると、自己暗号化ドライブのデータを「暗号化」できます。

自己暗号化ドライブが有効な場合は、コアダンプも暗号化されます。



HA ペアが SAS ドライブまたは NVMe ドライブ（SED、NSE、FIPS）の暗号化を使用している場合は、トピックの手順に従う必要があります **FIPS ドライブまたは SED を非保護モードに戻します** システムを初期化する前の HA ペア内のすべてのドライブ（ブートオプション 4 または 9）。そうしないと、ドライブを転用した場合にデータが失われる可能性があります。

### サポートされている自己暗号化ドライブのタイプ

2種類の自己暗号化ドライブがサポートされています。

- すべての FAS システムおよび AFF システムで、自己暗号化機能を備えた FIPS 認定の SAS ドライブまたは NVMe ドライブがサポートされます。これらのドライブは **FIPS ドライブ** と呼ばれ、Federal Information Processing Standard Publication 140-2 レベル 2 の要件に準拠しています。認定された機能により、ドライブに対する DoS 攻撃を防止するなど、暗号化に加えて保護が可能になります。FIPS ドライブは、同じノードまたは HA ペアで他のタイプのドライブと混在させることはできません。
- ONTAP 9.6以降では、AFF A800、A320、およびそれ以降のシステムで、FIPSのテストを実施していない自己暗号化NVMeドライブがサポートされます。これらのドライブは **SED** と呼ばれ、FIPSドライブと同じ暗号化機能を提供しますが、同じノードまたはHAペアで非暗号化ドライブと混在させることもできます。
- すべてのFIPS検証済みドライブは、FIPS検証に合格したファームウェア暗号化モジュールを使用します。FIPSドライブ暗号化モジュールは、ドライブの外部で生成されたキーを使用しません（ドライブに入力された認証パスフレーズは、ドライブのファームウェア暗号化モジュールでキー暗号化キーの取得に使用されます）。



非暗号化ドライブとは、SEDやFIPSドライブではないドライブです。



Flash Cacheモジュールを搭載したシステムでNSEを使用する場合は、NVEまたはNAEも有効にする必要があります。NSEは、Flash Cacheモジュール上のデータを暗号化しません。

## 外部キー管理を使用する状況

オンボードキーマネージャを使用した方がコストもかからず一般的には便利ですが、次のいずれかに当てはまる場合は外部キー管理を使用することを推奨します。

- 組織のポリシーには、FIPS 140-2レベル2以上の暗号化モジュールを使用するキー管理解決策 が必要です。
- 暗号化キーを一元管理するマルチクラスタ解決策が必要です。
- 認証キーをデータとは別のシステムや場所に格納してセキュリティを強化する必要がある場合。

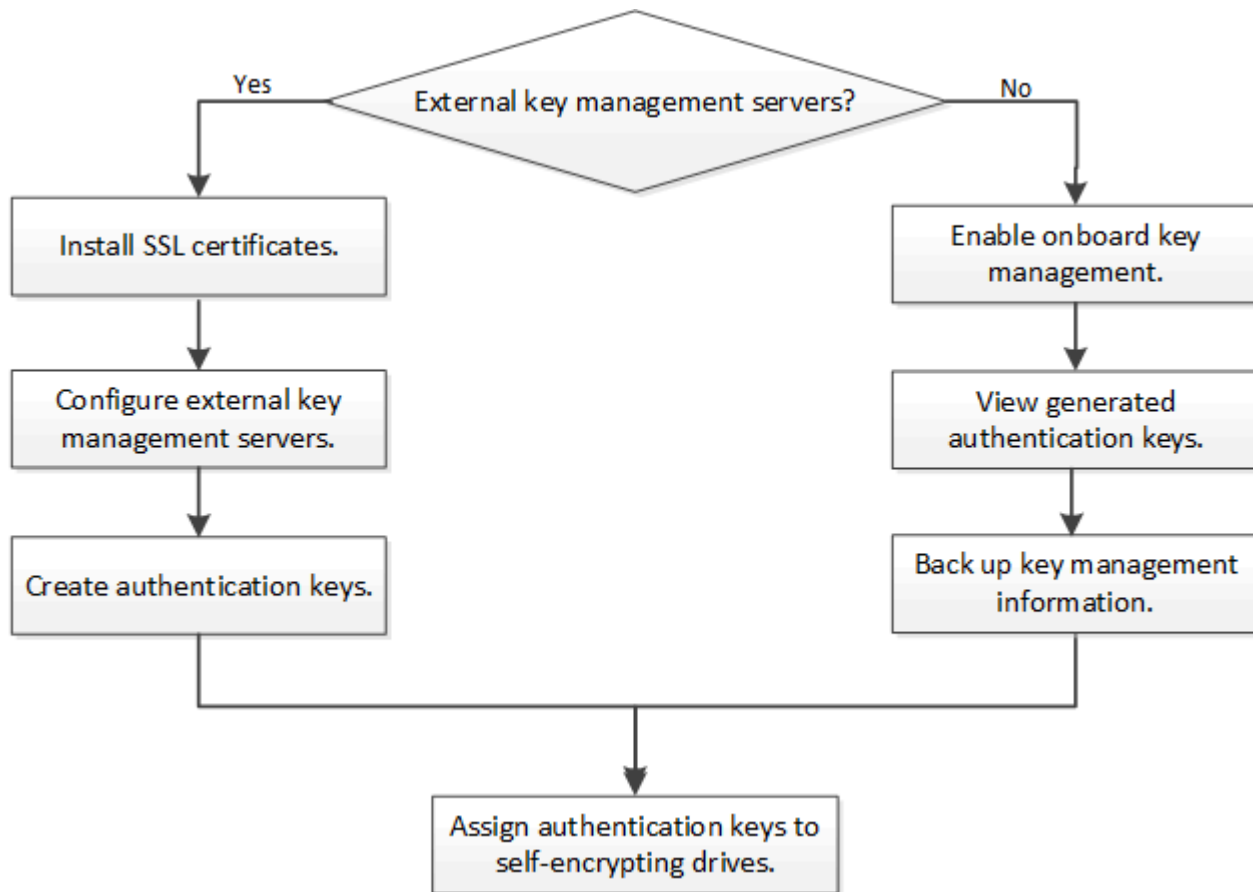
## サポートの詳細

次の表に、重要なハードウェア暗号化のサポートの詳細を示します。サポートされている KMIP サーバ、ストレージシステム、ディスクシェルフの最新情報については、Interoperability Matrix を参照してください。

リソースまたは機能	サポートの詳細
異なるタイプのディスクの混在	<ul style="list-style-type: none"> <li>• FIPS ドライブは、同じノードまたは HA ペアで他のタイプのドライブと混在させることはできません。準拠した HA ペアと準拠していない HA ペアを同じクラスタに共存させることは可能です。</li> <li>• SEDは、同じノードまたはHAペアで暗号化されていないドライブと混在させることができます。</li> </ul>
ドライブタイプ	<ul style="list-style-type: none"> <li>• FIPS ドライブには、SAS ドライブまたは NVMe ドライブを使用できます。</li> <li>• SED は NVMe ドライブである必要があります。</li> </ul>
10Gb ネットワークインターフェイス	ONTAP 9.3 以降では、KMIP を使用したキー管理の設定で外部キー管理サーバとの通信に 10Gb ネットワークインターフェイスがサポートされます。
キー管理サーバとの通信に使用するポートを指定します	ONTAP 9.3 以降では、任意のストレージコントローラポートを使用してキー管理サーバと通信できます。それ以外の場合は、キー管理サーバとの通信にポートe0mを使用する必要があります。ストレージコントローラのモデルによっては、ブートプロセス時に一部のネットワークインターフェイスをキー管理サーバとの通信に使用できない場合があります。
MetroCluster (MCC)	<ul style="list-style-type: none"> <li>• NVMe ドライブでは MCC がサポートされます。</li> <li>• SAS ドライブでは MCC がサポートされません。</li> </ul>

## ハードウェアベースの暗号化のワークフロー

自己暗号化ドライブに対してクラスタを認証するには、キー管理服务を設定する必要があります。外部キー管理サーバまたはオンボードキーマネージャを使用できます。



### 関連情報

- ["NetApp Hardware Universe の略"](#)
- ["NetApp Volume Encryption および NetApp Aggregate Encryption の略"](#)

## 外部キー管理を設定

### 外部キー管理の概要の設定

1 つ以上の外部キー管理サーバを使用して、暗号化されたデータにアクセスする際にクラスタで使用するキーを安全に保管できます。外部キー管理サーバはストレージ環境に配置されたサードパーティのシステムで、Key Management Interoperability Protocol (KMIP) を使用してノードにキーを提供します。

ONTAP 9.1 以前のバージョンでは、外部キー管理ツールを使用する前に、ノード管理ロールが設定されたポートにノード管理 LIF を割り当てる必要があります。

ONTAP 9.1 以降では、オンボードキーマネージャを使用して NetApp Volume Encryption (NVE) を実装できます。ONTAP 9.3 以降では、NVE を外部キー管理 (KMIP) およびオンボードキーマネージャとともに実装できます。ONTAP 9.11.1以降では、1つのクラスタに複数の外部キー管理ツールを設定できます。を参照し

てください [クラスタ化されたキーサーバを設定](#)

## ONTAP 9.2 以前でネットワーク情報を収集

ONTAP 9.2 以前を使用している場合は、外部キー管理を有効にする前にネットワーク設定ワークシートに情報を記入してください。



ONTAP 9.3 以降では、必要なすべてのネットワーク情報が自動的に検出されます。

項目	注：	価値
キー管理ネットワークインターフェイスの名前		
キー管理ネットワークインターフェイスの IP アドレス	ノード管理 LIF の IPv4 形式または IPv6 形式の IP アドレス	
キー管理ネットワークインターフェイスの IPv6 ネットワークプレフィックス長	IPv6 を使用している場合、IPv6 ネットワークプレフィックス長	
キー管理ネットワークインターフェイスのサブネットマスク		
キー管理ネットワークインターフェイスのゲートウェイの IP アドレス		
クラスタネットワークインターフェイスの IPv6 アドレス	キー管理ネットワークインターフェイスに IPv6 を使用している場合にのみ必要です	
各 KMIP サーバのポート番号	任意。すべての KMIP サーバで同じポート番号を使用してください。ポート番号を指定しなかった場合は、デフォルトでポート 5696 が使用されます。これは、Internet Assigned Numbers Authority（IANA）が KMIP に割り当てているポートです。	
キータグ名	任意。キータグ名は、ノードに属するすべてのキーを識別するために使用されます。デフォルトのキータグ名はノード名です。	

### 関連情報

"[ネットアップテクニカルレポート 3954](#)：『[NetApp Storage Encryption Preinstallation Requirements and Procedures for IBM Tivoli Lifetime Key Manager](#)』"

## クラスタに **SSL** 証明書をインストールします

クラスタと KMIP サーバの間では、相互の ID を検証して SSL 接続を確立するために KMIP SSL 証明書を使用します。KMIP サーバとの SSL 接続を設定する前に、クラスタの KMIP クライアント SSL 証明書、および KMIP サーバのルート Certificate Authority (CA ; 認証局) の SSL パブリック証明書をインストールする必要があります。

### このタスクについて

HA ペア構成では、両方のノードで同じ SSL KMIP パブリック証明書とプライベート証明書を使用する必要があります。複数の HA ペアを同じ KMIP サーバに接続する場合は、HA ペアのすべてのノードで同じ SSL KMIP パブリック証明書とプライベート証明書を使用する必要があります。

### 作業を開始する前に

- 証明書を作成するサーバ、KMIP サーバ、およびクラスタの時刻が同期されている必要があります。
- クラスタのパブリック SSL KMIP クライアント証明書を入手しておく必要があります。
- クラスタの SSL KMIP クライアント証明書に関連付けられた秘密鍵を入手しておく必要があります。
- SSL KMIP クライアント証明書は、パスワードで保護しないでください。
- KMIP サーバのルート認証局 (CA) の SSL パブリック証明書を入手しておく必要があります。
- MetroCluster環境では、両方のクラスタに同じKMIP SSL証明書をインストールする必要があります。



KMIP サーバへのクライアント証明書とサーバ証明書のインストールは、クラスタに証明書をインストールする前でもインストールしたあとでもかまいません。

### 手順

1. クラスタに SSL KMIP クライアント証明書をインストールします。

```
security certificate install -vserver admin_svm_name -type client
```

SSL KMIP パブリック証明書とプライベート証明書を入力するように求められます。

```
cluster1::> security certificate install -vserver cluster1 -type client
```

2. KMIP サーバのルート認証局 (CA) の SSL パブリック証明書をインストールします。

```
security certificate install -vserver admin_svm_name -type server-ca
```

```
cluster1::> security certificate install -vserver cluster1 -type server-ca
```

## ONTAP 9.6 以降で外部キー管理を有効にする (ハードウェアベース)

1 つ以上の KMIP サーバを使用して、暗号化されたデータにアクセスする際にクラスタで使用するキーを安全に保管できます。1 つのノードに最大 4 つの KMIP サーバを接続できます。冗長性とディザスタリカバリのために、少なくとも 2 台のサーバを使用する

ことを推奨します。

ONTAP 9.11.1以降では、プライマリキーサーバごとに最大3つのセカンダリキーサーバを追加して、クラスタ化されたキーサーバを作成できます。詳細については、を参照してください [クラスタ構成の外部キーサーバを構成](#)。

作業を開始する前に

- KMIP SSL クライアント証明書とサーバ証明書をインストールしておく必要があります。
- このタスクを実行するには、クラスタ管理者である必要があります。
- 外部キー管理ツールを設定する前に、MetroCluster 環境を設定する必要があります。
- MetroCluster 環境では、両方のクラスタにKMIP SSL証明書をインストールする必要があります。

手順

1. クラスタのキー管理ツールの接続を設定します。

```
security key-manager external enable -vserver admin_SVM -key-servers  
host_name|IP_address:port,... -client-cert client_certificate -server-ca-cert  
server_CA_certificates
```



- security key-manager external enable コマンドは、に置き換わるものです security key-manager setup コマンドを実行しますを実行できます security key-manager external modify コマンドを使用して、外部キー管理の設定を変更します。コマンド構文全体については、マニュアルページを参照してください。
- MetroCluster 環境で管理SVMに外部キー管理を設定する場合は、を繰り返す必要があります security key-manager external enable パートナークラスタに対して実行します。

次のコマンドは、の外部キー管理を有効にします cluster1 3つの外部キーサーバで構成されます。最初のキーサーバはホスト名とポートで指定し、2番目のキーサーバはIPアドレスとデフォルトポートで指定し、3番目のキーサーバはIPv6アドレスとポートで指定します。

```
cluster1::> security key-manager external enable -key-servers  
ks1.local:15696,10.0.0.10,[fd20:8b1e:b255:814e:32bd:f35c:832c:5a09]:1234  
-client-cert AdminVserverClientCert -server-ca-certs  
AdminVserverServerCaCert
```

2. 設定したすべての KMIP サーバが接続されていることを確認します。

```
security key-manager external show-status -node node_name -vserver SVM -key  
-server host_name|IP_address:port -key-server-status available|not-  
responding|unknown
```



- security key-manager external show-status コマンドは、に置き換わるものです security key-manager show -status コマンドを実行しますコマンド構文全体については、マニュアルページを参照してください。



```
cluster1::> security key-manager external show-status
```

Node	Vserver	Key Server	Status
-----			
-----			
node1			
	cluster1		
		10.0.0.10:5696	available
		fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234	available
		ks1.local:15696	available
node2			
	cluster1		
		10.0.0.10:5696	available
		fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234	available
		ks1.local:15696	available

```
6 entries were displayed.
```

## ONTAP 9.5 以前で外部キー管理を有効にします

1 つ以上の KMIP サーバを使用して、暗号化されたデータにアクセスする際にクラスタで使用するキーを安全に保管できます。1 つのノードに最大 4 つの KMIP サーバを接続できます。冗長性とディザスタリカバリのために、少なくとも 2 台のサーバを使用することを推奨します。

このタスクについて

ONTAP は、クラスタ内のすべてのノードについて KMIP サーバの接続を設定します。

作業を開始する前に

- KMIP SSL クライアント証明書とサーバ証明書をインストールしておく必要があります。
- このタスクを実行するには、クラスタ管理者である必要があります。
- 外部キー管理ツールを設定する前に、MetroCluster 環境を設定する必要があります。
- MetroCluster 環境では、両方のクラスタに KMIP SSL 証明書をインストールする必要があります。

手順

1. クラスタノードのキー管理ツールの接続を設定します。

```
security key-manager setup
```

キー管理ツールのセットアップが開始されます。



MetroCluster 環境では、このコマンドを両方のクラスタで実行する必要があります。

2. 各プロンプトで適切な応答を入力します。

### 3. KMIP サーバを追加します。

```
security key-manager add -address key_management_server_ipaddress
```



MetroCluster 環境では、このコマンドを両方のクラスタで実行する必要があります。

### 4. 冗長性を確保するために KMIP サーバをもう 1 つ追加します。

```
security key-manager add -address key_management_server_ipaddress
```



MetroCluster 環境では、このコマンドを両方のクラスタで実行する必要があります。

### 5. 設定したすべての KMIP サーバが接続されていることを確認します。

```
security key-manager show -status
```

コマンド構文全体については、マニュアルページを参照してください。

```
cluster1::> security key-manager show -status
```

Node	Port	Registered Key Manager	Status
-----	----	-----	-----
cluster1-01	5696	20.1.1.1	available
cluster1-01	5696	20.1.1.2	available
cluster1-02	5696	20.1.1.1	available
cluster1-02	5696	20.1.1.2	available

### 6. 必要に応じて、プレーンテキストボリュームを暗号化ボリュームに変換します。

```
volume encryption conversion start
```

ボリュームを変換する前に、外部キー管理ツールの設定をすべて完了しておく必要があります。MetroCluster環境では、両方のサイトに外部キー管理ツールを設定する必要があります。

## クラスタ構成の外部キーサーバを構成

ONTAP 9.11.1以降では、SVM上のクラスタ化された外部キー管理サーバへの接続を設定できます。クラスタ化されたキーサーバを使用すると、SVMのプライマリキーサーバとセカンダリキーサーバを指定できます。キーを登録すると、ONTAP は、処理が正常に完了するまで、プライマリキーサーバへのアクセスを順次試行する前に、キーの重複を防

止します。

外部キーサーバは、NSE、NVE、NAE、およびSEDのキーに使用できます。SVMでは、最大4つのプライマリ外部KMIPサーバをサポートできます。各プライマリサーバは、最大3つのセカンダリキーサーバをサポートできます。

作業を開始する前に

- "SVMでKMIPキー管理が有効になっている必要があります。"。
- このプロセスでサポートされるのは、KMIPを使用するキーサーバのみです。サポートされているキーサーバの一覧については、を参照してください ["NetApp Interoperability Matrix Tool で確認できます"](#)。
- クラスタ内のすべてのノードでONTAP 9.11.1以降が実行されている必要があります。
- サーバの順序は、で引数をリストします `-secondary-key-servers` パラメータには、外部キー管理 (KMIP) サーバのアクセス順序が反映されます。

クラスタ化されたキーサーバを作成します

設定手順 は、プライマリキーサーバを設定したかどうかによって異なります。

#### SVMにプライマリキーサーバとセカンダリキーサーバを追加する

1. クラスタでキー管理が有効になっていないことを確認します。  
`security key-manager external show -vserver svm_name`  
SVMですでに最大4つのプライマリキーサーバが有効になっている場合は、新しいプライマリキーサーバを追加する前に既存のプライマリキーサーバの1つを削除する必要があります。
2. プライマリキー管理ツールを有効にします。  
`security key-manager external enable -vserver svm_name -key-servers  
server_ip -client-cert client_cert_name -server-ca-certs  
server_ca_cert_names`
3. プライマリキーサーバを変更してセカンダリキーサーバを追加します。。 `-secondary-key-servers` パラメータには、最大3つのキーサーバをカンマで区切って指定できます。  
`security key-manager external modify-server -vserver svm_name -key-servers  
primary_key_server -secondary-key-servers list_of_key_servers`

#### 既存のプライマリキーサーバにセカンダリキーサーバを追加する

1. プライマリキーサーバを変更してセカンダリキーサーバを追加します。。 `-secondary-key-servers` パラメータには、最大3つのキーサーバをカンマで区切って指定できます。  
`security key-manager external modify-server -vserver svm_name -key-servers  
primary_key_server -secondary-key-servers list_of_key_servers`  
セカンダリキーサーバの詳細については、を参照してください [\[mod-secondary\]](#)。

クラスタ化されたキーサーバを変更

外部キーサーバクラスタの変更では、特定のキーサーバのステータス（プライマリまたはセカンダリ）を変更したり、セカンダリキーサーバを追加および削除したり、セカンダリキーサーバのアクセス順序を変更したりできます。

## プライマリキーサーバとセカンダリキーサーバの変換

プライマリキーサーバをセカンダリキーサーバに変換するには、まずを使用してSVMからプライマリキーサーバを削除する必要があります `security key-manager external remove-servers` コマンドを実行します

セカンダリキーサーバをプライマリキーサーバに変換するには、まず既存のプライマリキーサーバからセカンダリキーサーバを削除する必要があります。を参照してください [\[mod-secondary\]](#)。既存のキーの削除中にセカンダリキーサーバをプライマリサーバに変換する場合、削除および変換を実行する前に新しいサーバを追加しようとすると、キーが重複する可能性があります。

セカンダリキーサーバを変更します。

セカンダリキーサーバの管理はで行います `-secondary-key-servers` のパラメータ `security key-manager external modify-server` コマンドを実行します。 `-secondary-key-servers` パラメータにはカンマで区切ったリストを指定できます。リスト内で指定されたセカンダリキーサーバの順序によって、セカンダリキーサーバのアクセスシーケンスが決まります。アクセス順序は、コマンドを実行して変更できます `security key-manager external modify-server` セカンダリキーサーバを別の順序で入力します。

セカンダリキーサーバを削除するには、を実行します `-secondary-key-servers` 引数には、削除するキーサーバを省略して保持するキーサーバを指定する必要があります。すべてのセカンダリキーサーバを削除するには、引数を使用します - 「なし」を意味します。

追加情報 の場合は、を参照してください `security key-manager external` ページのを参照してください ["ONTAP コマンドリファレンス"](#)。

## ONTAP 9.6 以降で認証キーを作成します

を使用できます `security key-manager key create` コマンドを使用してノードの認証キーを作成し、設定したKMIPサーバに格納します。

このタスクについて

セキュリティの設定によりデータ認証と FIPS 140-2 認証に異なるキーを使用する必要がある場合は、それぞれの認証用のキーを作成する必要があります。そうでない場合は、FIPSへの準拠にデータアクセスと同じ認証キーを使用できます。

ONTAP では、クラスタ内のすべてのノードに対して認証キーが作成されます。

- このコマンドは、オンボードキーマネージャが有効になっている場合はサポートされません。ただし、オンボードキーマネージャを有効にすると、2つの認証キーが自動的に作成されます。キーを表示するには、次のコマンドを使用します。

```
security key-manager key query -key-type NSE-AK
```

- 設定済みのキー管理サーバにすでに 128 個を超える認証キーが格納されている場合は警告が表示されます。
- を使用できます `security key-manager key delete` 使用されていないキーを削除するコマンド。。 `security key-manager key delete` 指定したキーがONTAP で現在使用されている場合、コマンドは失敗します。(このコマンドを使用するには 'admin より大きい特権が必要です)



MetroCluster 環境でキーを削除する前に、キーがパートナークラスタで使用されていないことを確認する必要があります。パートナークラスタで次のコマンドを使用して、キーが使用されていないことを確認できます。

- ° `storage encryption disk show -data-key-id key-id`
- ° `storage encryption disk show -fips-key-id key-id`

作業を開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

手順

1. クラスタノードの認証キーを作成します。

```
security key-manager key create -key-tag passphrase_label -prompt-for-key true|false
```



設定 `prompt-for-key=true` 暗号化されたドライブを認証するときに、クラスタ管理者に使用するパスフレーズの入力を求めるプロンプトが表示されます。設定しない場合は、32 バイトのパスフレーズが自動的に生成されます。° `security key-manager key create` コマンドは、に置き換わるものです `security key-manager create-key` コマンドを実行しますコマンド構文全体については、マニュアルページを参照してください。

次の例は、の認証キーを作成します `cluster1` では、32 バイトのパスフレーズが自動的に生成されます。

```
cluster1::> security key-manager key create
Key ID:
000000000000000000002000000000001006268333f870860128fbe17d393e5083b00000000
00000000
```

2. 認証キーが作成されたことを確認します。

```
security key-manager key query -node node
```



° `security key-manager key query` コマンドは、に置き換わるものです `security key-manager query key` コマンドを実行しますコマンド構文全体については、マニュアルページを参照してください。出力に表示されるキー ID は、認証キーを参照するために使用される識別子です。実際の認証キーまたはデータ暗号化キーではありません。

次の例は、の認証キーが作成されたことを確認します `cluster1` :

```
cluster1::> security key-manager key query
      Vserver: cluster1
      Key Manager: external
      Node: node1
```

Key Tag	Key Type	Restored
-----	-----	-----
node1	NSE-AK	yes
Key ID:		
000000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e0000000000000000		
node1	NSE-AK	yes
Key ID:		
000000000000000000002000000000001006f4e2513353a674305872a4c9f3bf7970000000000000000		

```
      Vserver: cluster1
      Key Manager: external
      Node: node2
```

Key Tag	Key Type	Restored
-----	-----	-----
node2	NSE-AK	yes
Key ID:		
000000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e0000000000000000		
node2	NSE-AK	yes
Key ID:		
000000000000000000002000000000001006f4e2513353a674305872a4c9f3bf7970000000000000000		

## ONTAP 9.5 以前で認証キーを作成します

を使用できます security key-manager create-key コマンドを使用してノードの認証キーを作成し、設定したKMIPサーバに格納します。

このタスクについて

セキュリティの設定によりデータ認証と FIPS 140-2 認証に異なるキーを使用する必要がある場合は、それぞれの認証用のキーを作成する必要があります。そうでない場合は、FIPS 準拠の認証キーをデータアクセスにも使用できます。

ONTAP では、クラスタ内のすべてのノードに対して認証キーが作成されます。

- このコマンドは、オンボードキー管理が有効な場合はサポートされません。
- 設定済みのキー管理サーバにすでに 128 個を超える認証キーが格納されている場合は警告が表示されま

す。

キー管理サーバソフトウェアを使用して未使用のキーを削除し、もう一度コマンドを実行できます。

作業を開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

手順

1. クラスタノードの認証キーを作成します。

```
security key-manager create-key
```

コマンド構文全体については、コマンドのマニュアルページを参照してください。



出力に表示されるキー ID は、認証キーを参照するために使用される識別子です。実際の認証キーまたはデータ暗号化キーではありません。

次の例は、の認証キーを作成します cluster1：

```
cluster1::> security key-manager create-key
(security key-manager create-key)
Verifying requirements...

Node: cluster1-01
Creating authentication key...
Authentication key creation successful.
Key ID: F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C

Node: cluster1-01
Key manager restore operation initialized.
Successfully restored key information.

Node: cluster1-02
Key manager restore operation initialized.
Successfully restored key information.
```

2. 認証キーが作成されたことを確認します。

```
security key-manager query
```

コマンド構文全体については、マニュアルページを参照してください。

次の例は、の認証キーが作成されたことを確認します cluster1：

```
cluster1::> security key-manager query

(security key-manager query)

      Node: cluster1-01
    Key Manager: 20.1.1.1
  Server Status: available

Key Tag      Key Type  Restored
-----
cluster1-01  NSE-AK    yes
    Key ID:
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C

      Node: cluster1-02
    Key Manager: 20.1.1.1
  Server Status: available

Key Tag      Key Type  Restored
-----
cluster1-02  NSE-AK    yes
    Key ID:
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
```

## FIPS ドライブまたは SED にデータ認証キーを割り当てる（外部キー管理）

を使用できます storage encryption disk modify コマンドを使用してFIPSドライブまたはSEDにデータ認証キーを割り当てることができます。このキーは、クラスタノードでドライブ上の暗号化されたデータをロックまたはロック解除する際に使用します。

このタスクについて

自己暗号化ドライブの認証キー ID がデフォルト以外の値に設定されている場合にのみ、不正アクセスから保護されます。Manufacturer Secure ID（MSID；メーカーのセキュア ID）のキー ID が 0x0 になり、SAS ドライブの標準のデフォルト値になります。NVMe ドライブの場合、標準のデフォルト値は null キーで、空のキー ID として表されます。キー ID を自己暗号化ドライブに割り当てると、認証キー ID がデフォルト以外の値に変更されます。

この手順 はシステムの停止を伴いません。

作業を開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

手順



1. FIPS ドライブまたは SED にデータ認証キーを割り当てます。

```
storage encryption disk modify -disk disk_ID -data-key-id key_ID
```

コマンド構文全体については、コマンドのマニュアルページを参照してください。



を使用できます `security key-manager query -key-type NSE-AK` キーIDを表示するコマンド。

```
cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
```

```
Info: Starting modify on 14 disks.
      View the status of the operation by using the
      storage encryption disk show-status command.
```

2. 認証キーが割り当てられたことを確認します。

```
storage encryption disk show
```

コマンド構文全体については、マニュアルページを参照してください。

```
cluster1::> storage encryption disk show
Disk      Mode Data Key ID
-----
-----
0.0.0     data
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
0.0.1     data
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
[...]
```

## オンボードキー管理を設定

### ONTAP 9.6 以降ではオンボードキー管理を有効にしてください

オンボードキーマネージャを使用して、クラスタノードを FIPS ドライブまたは SED に対して認証できます。オンボードキーマネージャは組み込みのツールで、データと同じストレージシステムからノードに認証キーを提供します。オンボードキーマネージャは FIPS-140-2 レベル 1 に準拠しています。

オンボードキーマネージャを使用して、暗号化されたデータにアクセスする際にクラスタで使用するキーを安全に保管できます。オンボードキーマネージャは、暗号化されたボリュームや自己暗号化ディスクにアクセスする各クラスタで有効にする必要があります。

## このタスクについて

を実行する必要があります `security key-manager onboard enable` コマンドはクラスタにノードを追加するたびに実行します。MetroCluster 構成では、を実行する必要があります `security key-manager onboard enable` を実行してから、を実行します `security key-manager onboard sync` リモートクラスタで、それぞれで同じパスフレーズを使用します。

デフォルトでは、ノードのリブート時にキー管理ツールのパスフレーズを入力する必要はありません。MetroCluster 以外では、を使用できます `cc-mode-enabled=yes` リブート後にユーザにパスフレーズの入力を求めるオプション。

オンボードキーマネージャがCCモードで有効になっている場合 (`cc-mode-enabled=yes`) では、システムの動作は次のように変更されます。

- Common Criteria モードで動作している場合、クラスタパスフレーズの試行に連続して失敗したかどうか監視されます。

NetApp Storage Encryption (NSE) が有効になっている場合に、ブート時に正しいクラスタパスフレーズを入力しないと、システムはドライブを認証できず、自動的にリブートされます。これを修正するには、ブートプロンプトで正しいクラスタパスフレーズを入力する必要があります。ブート後、パラメータとしてクラスタパスフレーズを必要とするコマンドに対して、最大 5 回連続してクラスタパスフレーズを 24 時間以内に入力することができます。制限に達した場合（たとえば、クラスタのパスフレーズを 5 回連続して正しく入力できなかった場合など）は、24 時間のタイムアウトが経過するまで待つか、ノードをリブートして制限をリセットする必要があります。

- システムイメージの更新では、NetApp RSA-3072 コード署名証明書と SHA-384 コード署名ダイジェストを使用して、通常の NetApp RSA-2048 コード署名証明書および SHA-256 コード署名ダイジェストではなく、イメージの整合性をチェックします。

`upgrade` コマンドは、さまざまなデジタル署名をチェックして、イメージの内容が変更されていないか、壊れていないかを確認します。検証に成功した場合は、イメージの更新プロセスが次の手順に進みます。成功しなかった場合は、イメージの更新が失敗します。システムの更新については 'cluster image マニュアル・ページを参照してください

オンボードキーマネージャは、揮発性メモリにキーを格納します。揮発性メモリの内容は、システムのリブート時または停止時にクリアされます。通常の動作条件下では、システムが停止すると 30 秒以内に揮発性メモリの内容がクリアされます。

## 作業を開始する前に

- NSE で外部キー管理 (KMIP) サーバを使用している場合は、外部キー管理ツールのデータベースを削除しておく必要があります。

### "外部キー管理からオンボードキー管理への移行"

- このタスクを実行するには、クラスタ管理者である必要があります。
- オンボードキーマネージャを設定する前に、MetroCluster 環境を設定する必要があります。

## 手順

1. キー管理ツールの `setup` コマンドを開始します。

```
security key-manager onboard enable -cc-mode-enabled yes|no
```



設定 cc-mode-enabled=yes リブート後にユーザにキー管理ツールのパスフレーズの入力を求める場合。。 - cc-mode-enabled オプションはMetroCluster 構成ではサポートされません。。 security key-manager onboard enable コマンドは、に置き換わるものです security key-manager setup コマンドを実行します

次の例では、リブートのたびにパスフレーズの入力を求めずに、 cluster1 でキー管理ツールの setup コマンドを開始します。

```
cluster1::> security key-manager onboard enable
```

```
Enter the cluster-wide passphrase for onboard key management in Vserver
"cluster1"::      <32..256 ASCII characters long text>
Reenter the cluster-wide passphrase:      <32..256 ASCII characters long
text>
```

2. パスフレーズのプロンプトで 32 ～ 256 文字のパスフレーズを入力します。または、64 ～ 256 文字のパスフレーズを「cc-modej」に入力します。



指定された "cc-mode" パスフレーズが 64 文字未満の場合、キー管理ツールのセットアップ操作によってパスフレーズのプロンプトが再表示されるまでに 5 秒の遅延が発生します。

3. パスフレーズの確認のプロンプトでパスフレーズをもう一度入力します。
4. 認証キーが作成されたことを確認します。

```
security key-manager key query -node node
```



。 security key-manager key query コマンドは、に置き換わるものです security key-manager query key コマンドを実行しますコマンド構文全体については、マニュアルページを参照してください。

次の例は、の認証キーが作成されたことを確認します cluster1：

```
cluster1::> security key-manager key query
      Vserver: cluster1
      Key Manager: onboard
      Node: node1
```

Key Tag	Key Type	Restored
node1	NSE-AK	yes
Key ID: 000000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e00000000 00000000		
node1	NSE-AK	yes
Key ID: 000000000000000000002000000000001006f4e2513353a674305872a4c9f3bf79700000000 00000000		

```
      Vserver: cluster1
      Key Manager: onboard
      Node: node2
```

Key Tag	Key Type	Restored
node1	NSE-AK	yes
Key ID: 000000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e00000000 00000000		
node2	NSE-AK	yes
Key ID: 000000000000000000002000000000001006f4e2513353a674305872a4c9f3bf79700000000 00000000		

完了後

あとでできるように、ストレージシステムの外部の安全な場所にパスフレーズをコピーしておきます。

キー管理情報は、クラスタの Replicated Database（RDB；複製データベース）にすべて自動的にバックアップされます。災害時に備えて、情報を手動でもバックアップしておく必要があります。

## ONTAP 9.5 以前でオンボードキー管理を有効にします

オンボードキーマネージャを使用して、クラスタノードを FIPS ドライブまたは SED に対して認証できます。オンボードキーマネージャは組み込みのツールで、データと同じストレージシステムからノードに認証キーを提供します。オンボードキーマネージャは FIPS-140-2 レベル 1 に準拠しています。

オンボードキーマネージャを使用して、暗号化されたデータにアクセスする際にクラスタで使用するキーを安

全に保管できます。オンボードキーマネージャは、暗号化されたボリュームや自己暗号化ディスクにアクセスする各クラスタで有効にする必要があります。

このタスクについて

を実行する必要があります `security key-manager setup` コマンドはクラスタにノードを追加するたびに実行します。

MetroCluster 構成を使用する場合は、次のガイドラインを確認してください。

- ONTAP 9.5では、を実行する必要があります `security key-manager setup` ローカルクラスタおよび `security key-manager setup -sync-metrocluster-config yes` リモートクラスタで、それぞれで同じパスフレーズを使用します。
- ONTAP 9.5より前のバージョンでは、を実行する必要があります `security key-manager setup` ローカルクラスタで、約20秒待ってからを実行します `security key-manager setup` リモートクラスタで、それぞれで同じパスフレーズを使用します。

デフォルトでは、ノードのリブート時にキー管理ツールのパスフレーズを入力する必要はありません。ONTAP 9.4以降では、`-enable-cc-mode yes` リブート後にユーザにパスフレーズの入力を求めるオプション。

NVEの場合は、を設定します `-enable-cc-mode yes` を使用して作成したボリューム ``volume create`` および `volume move start` コマンドは自動的に暗号化されます。の場合 `volume create`` を指定する必要はありません ``-encrypt true``。の場合 `volume move start`` を指定する必要はありません ``-encrypt-destination true``。



パスフレーズの試行に失敗した場合は、ノードを再起動する必要があります。

作業を開始する前に

- NSE で外部キー管理（KMIP）サーバを使用している場合は、外部キー管理ツールのデータベースを削除しておく必要があります。

#### "外部キー管理からオンボードキー管理への移行"

- このタスクを実行するには、クラスタ管理者である必要があります。
- オンボードキーマネージャを設定する前に、MetroCluster 環境を設定する必要があります。

手順

1. キー管理ツールのセットアップを開始します。

```
security key-manager setup -enable-cc-mode yes|no
```



ONTAP 9.4以降では、`-enable-cc-mode yes` リブート後にユーザにキー管理ツールのパスフレーズの入力を求めるオプション。NVEの場合は、を設定します `-enable-cc-mode yes`` を使用して作成したボリューム ``volume create`` および `volume move start` コマンドは自動的に暗号化されます。

次の例では、リブートのたびにパスフレーズの入力を求めずに、`cluster1` でキー管理ツールをセットアップします。

• • •

- 

指定された "cc-mode" パスフレーズが 64 文字未満の場合、キー管理ツールのセットアップ操作によってパスフレーズのプロンプトが再表示されるまでに 5 秒の遅延が発生します。

- 一がすべてのノードに設定されていることを確認します。

```
security key-manager key show
```

マンド構文全体については、マニュアルページを参照してください。

Key ID	Used By
--------	---------

完了後

キー管理情報は、クラスタの Replicated Database（RDB；複製データベース）にすべて自動的にバックアップされます。

オンボードキーマネージャのパスフレーズを設定するときは、災害時に備えて、ストレージシステムの外部の安全な場所にも手動で情報をバックアップしておく必要があります。を参照してください ["オンボードキー管理情報を手動でバックアップ"](#)。

## FIPS ドライブまたは SED にデータ認証キーを割り当てる（オンボードキー管理）

を使用できます `storage encryption disk modify` コマンドを使用して FIPS ドライブまたは SED にデータ認証キーを割り当てることができます。このキーは、クラスタノードでドライブのデータにアクセスする際に使用します。

このタスクについて

自己暗号化ドライブの認証キー ID がデフォルト以外の値に設定されている場合にのみ、不正アクセスから保護されます。Manufacturer Secure ID（MSID；メーカーのセキュア ID）のキー ID が 0x0 になり、SAS ドライブの標準のデフォルト値になります。NVMe ドライブの場合、標準のデフォルト値は null キーで、空のキー ID として表されます。キー ID を自己暗号化ドライブに割り当てると、認証キー ID がデフォルト以外の値に変更されます。

作業を開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

手順

1. FIPS ドライブまたは SED にデータ認証キーを割り当てます。

```
storage encryption disk modify -disk disk_ID -data-key-id key_ID
```

コマンド構文全体については、コマンドのマニュアルページを参照してください。



を使用できます `security key-manager key query -key-type NSE-AK` キーIDを表示するコマンド。

```
cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id  
0000000000000000000020000000000010019215b9738bc7b43d4698c80246db1f4
```

```
Info: Starting modify on 14 disks.  
View the status of the operation by using the  
storage encryption disk show-status command.
```

2. 認証キーが割り当てられたことを確認します。

```
storage encryption disk show
```

コマンド構文全体については、マニュアルページを参照してください。

```
cluster1::> storage encryption disk show
Disk      Mode Data Key ID
-----
-----
0.0.0     data
00000000000000000000200000000000010019215b9738bc7b43d4698c80246db1f4
0.0.1     data
00000000000000000000200000000000010059851742AF2703FC91369B7DB47C4722
[...]
```

## FIPS ドライブに FIPS 140-2 認証キーを割り当てます

を使用できます `storage encryption disk modify` コマンドにを指定します `-fips-key-id` FIPS 140-2 認証キーを FIPS ドライブに割り当てるオプション。このキーは、ドライブに対する DoS 攻撃を防止するなど、データアクセス以外のドライブ処理に使用されます。

このタスクについて

セキュリティの設定によっては、データ認証と FIPS 140-2 認証に異なるキーを使用する必要がある場合があります。そうでない場合は、FIPS 準拠の認証キーをデータアクセスにも使用できます。

この手順 はシステムの停止を伴いません。

作業を開始する前に

ドライブファームウェアで FIPS 140-2 準拠がサポートされている必要があります。。"[NetApp Interoperability Matrix Tool](#) で確認できます" サポートされているドライブファームウェアのバージョンに関する情報が含まれます。

手順

- 最初に、データ認証キーを割り当てておく必要があります。これは、を使用して実行できます [外部キー管理ツール](#) または [オンボードキーマネージャ](#)。コマンドを使用して、キーが割り当てられていることを確認します `storage encryption disk show`。
- SED に FIPS 140-2 認証キーを割り当てます。

```
storage encryption disk modify -disk disk_id -fips-key-id
fips_authentication_key_id
```

を使用できます `security key-manager query` キーIDを表示するコマンド。



```
cluster1::> storage encryption disk modify -disk 2.10.* -fips-key-id
6A1E21D8000000000100000000000005A1FB4EE8F62FD6D8AE6754C9019F35A
```

Info: Starting modify on 14 disks.  
View the status of the operation by using the  
storage encryption disk show-status command.

### 3. 認証キーが割り当てられたことを確認します。

```
storage encryption disk show -fips
```

コマンド構文全体については、マニュアルページを参照してください。

```
cluster1::> storage encryption disk show -fips
Disk      Mode FIPS-Compliance Key ID
-----
-----
2.10.0    full
6A1E21D8000000000100000000000005A1FB4EE8F62FD6D8AE6754C9019F35A
2.10.1    full
6A1E21D8000000000100000000000005A1FB4EE8F62FD6D8AE6754C9019F35A
[...]
```

## KMIP サーバ接続に対して、クラスタ全体の FIPS 準拠モードを有効にします

使用できます security config modify コマンドにを指定します -is-fips-enabled 転送中のデータに対してクラスタ全体のFIPS準拠モードを有効にするオプション。これにより、クラスタが KMIP サーバに接続する際に FIPS モードの OpenSSL が使用されるようになります。

このタスクについて

クラスタ全体の FIPS 準拠モードを有効にすると、自動的に TLS1.2 と FIPS 認定暗号スイートのみが使用されます。クラスタ全体の FIPS 準拠モードは、デフォルトでは無効になっています。

クラスタ全体のセキュリティの設定を変更した場合は、変更後にクラスタノードを手動でリブートする必要があります。

作業を開始する前に

- ストレージコントローラは FIPS 準拠モードで設定する必要があります。
- すべての KMIP サーバで TLSv1.2 がサポートされている必要がありクラスタ全体の FIPS 準拠モードが有効になっている場合、KMIP サーバへの接続を完了するために TLSv1.2 が必要になります。

手順

1. 権限レベルを advanced に設定します。

```
set -privilege advanced
```

2. TLSv1.2 がサポートされていることを確認します。

```
security config show -supported-protocols
```

コマンド構文全体については、マニュアルページを参照してください。

```
cluster1::> security config show
```

	Cluster		Cluster
Security			
Interface	FIPS Mode	Supported Protocols	Supported Ciphers
Ready			Config
-----	-----	-----	-----
-----	-----		
SSL	false	TLSv1.2, TLSv1.1, TLSv1	ALL:!LOW: !aNULL:!EXP: !eNULL
			yes

3. クラスタ全体の FIPS 準拠モードを有効にします。

```
security config modify -is-fips-enabled true -interface SSL
```

コマンド構文全体については、マニュアルページを参照してください。

4. クラスタノードを手動でリブートします。
5. クラスタ全体の FIPS 準拠モードが有効になっていることを確認します。

```
security config show
```

```
cluster1::> security config show
```

	Cluster		Cluster
Security			
Interface	FIPS Mode	Supported Protocols	Supported Ciphers
Ready			Config
-----	-----	-----	-----
-----	-----		
SSL	true	TLSv1.2, TLSv1.1	ALL:!LOW: !aNULL:!EXP: !eNULL:!RC4
			yes

## 著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

## 商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。