



## 外部キー管理を設定 ONTAP 9

NetApp  
September 12, 2024

# 目次

外部キー管理を設定 .....	1
外部キー管理の概要の設定 .....	1
System Managerを使用して外部キー管理ツールを管理します。 .....	1
クラスタに SSL 証明書をインストールします .....	3
ONTAP 9.6 以降で外部キー管理を有効にする（NVE） .....	4
ONTAP 9.5 以前で外部キー管理を有効にします .....	7
クラウドプロバイダを使用してキーを管理します .....	9

# 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、NetApp Volume Encryption (NVE) によってオンボードキーマネージャがサポートされます。ONTAP 9.3以降では、NVEで外部キー管理 (KMIP) とオンボードキーマネージャがサポートされます。ONTAP 9.10.1 以降では、を使用できます [Azure Key Vaultサービス](#)または[Google Cloud Key Managerサービス](#) NVEキーを保護するため。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](#)

## System Managerを使用して外部キー管理ツールを管理します。

ONTAP 9.7以降では、オンボードキーマネージャを使用して認証キーと暗号化キーを格納および管理できます。ONTAP 9.13.1以降では、外部キー管理ツールを使用してこれらのキーを格納および管理することもできます。

オンボードキーマネージャは、クラスタ内のセキュアなデータベースにキーを格納および管理します。スコープはクラスタです。外部キー管理ツールは、クラスタの外部にキーを格納および管理します。スコープには、クラスタまたはStorage VMを指定できます。1つ以上の外部キー管理ツールを使用できます。次の条件が適用されます。

- ・ オンボードキーマネージャが有効になっている場合、外部キー管理ツールをクラスタレベルで有効にすることはできませんが、Storage VMレベルで有効にすることはできます。
- ・ 外部キー管理ツールがクラスタレベルで有効になっている場合、オンボードキーマネージャを有効にすることはできません。

外部キー管理ツールを使用する場合は、Storage VMおよびクラスタごとに最大4つのプライマリキーサーバを登録できます。各プライマリキーサーバは、最大3台のセカンダリキーサーバでクラスタ化できます。

## 外部キー管理ツールを設定する




Storage VMに外部キー管理ツールを追加するには、Storage VMのネットワークインターフェイスの設定時にオプションのゲートウェイを追加する必要があります。Storage VMをネットワークルートなしで作成した場合は、外部キー管理ツール用のルートを明示的に作成する必要があります。を参照してください "[LIFを作成する \(ネットワークインターフェイス\)](#)"。

### 手順

外部キー管理ツールは、System Managerの別の場所から設定できます。

1. 外部キー管理ツールを設定するには、次のいずれかの開始手順を実行します。

ワークフロー	ナビゲーション	開始ステップ
キーマネージャを設定します	[クラスタ]>*[設定]*	[セキュリティ]*セクションまでスクロールします。[暗号化]*で、を選択します  。[外部キーマネージャ]*を選択します。
ローカル階層を追加してください	ストレージ>*階層*	[+ローカル階層の追加]*を選択します。[Configure Key Manager]チェックボックスをオンにします。[外部キーマネージャ]*を選択します。
ストレージを準備	ダッシュボード	セクションで、[ストレージの準備]*を選択します。次に、[Configure Key Manager]を選択します。[外部キーマネージャ]*を選択します。
暗号化を設定（キー管理ツールをStorage VMスコープでのみ使用）	ストレージ>* Storage VM *	Storage VMを選択します。[設定]タブを選択します。の[暗号化]*セクションで、を選択します  。


2. プライマリキーサーバを追加するには、を選択し  Add、[IPアドレス]または[ホスト名]\*および[ポート]\*フィールドに入力します。
3. インストールされている既存の証明書は、[KMIP Server CA Certificates]\*フィールドと[KMIP Client Certificate]\*フィールドに表示されます。 次のいずれかの操作を実行できます。
  - を選択し  て、キー管理ツールにマッピングするインストール済み証明書を選択します。（複数のサービスCA証明書を選択できますが、選択できるクライアント証明書は1つだけです）。
  - まだインストールされていない証明書を追加して外部キー管理ツールにマッピングする場合は、\*[新しい証明書の追加]\*を選択します。
  - 外部キー管理ツールにマッピングしないインストール済みの証明書を削除するには、証明書名の横にあるを選択し  ます。
4. セカンダリキーサーバを追加するには、[セカンダリキーサーバ]\*列で[追加]\*を選択し、詳細を指定します。
5. [保存]\*を選択して設定を完了します。

## 既存の外部キー管理ツールを編集します

すでに外部キー管理ツールを設定している場合は、その設定を変更できます。

### 手順

1. 外部キー管理ツールの設定を編集するには、次のいずれかの開始手順を実行します。

適用範囲	ナビゲーション	開始ステップ
クラスタスコープの外部キー管理ツール	[クラスタ]>*[設定]*	セクションまでスクロールします。[暗号化]*でを選択し  、[外部キーマネージャの編集]*を選択します。

Storage VMスコープの外部キー管理ツール	ストレージ>* Storage VM *	Storage VMを選択します。[設定]タブを選択します。セクションの[セキュリティ]で、を選択し ⋮、[外部キーマネージャの編集]*を選択します。
--------------------------	----------------------	---

2. 既存のキーサーバは\*[キーサーバ]\*の表に表示されます。次の操作を実行できます。

- を選択して新しいキーサーバを追加し **+ Add** ます。
- キーサーバを削除するには、テーブルセルの末尾にあるキーサーバの名前を選択します ⋮。そのプライマリキーサーバに関連付けられているセカンダリキーサーバも設定から削除されます。

## 外部キー管理ツールを削除します

ボリュームが暗号化されていない場合は、外部キー管理ツールを削除できます。

### 手順

1. 外部キー管理ツールを削除するには、次のいずれかの手順を実行します。

適用範囲	ナビゲーション	開始ステップ
クラスタスコープの外部キー管理ツール	[クラスタ]>*[設定]*	セクションまでスクロールします。[暗号化]*で、を選択し ⋮、[外部キーマネージャの削除]*を選択します。
Storage VMスコープの外部キー管理ツール	ストレージ>* Storage VM *	Storage VMを選択します。[設定]タブを選択します。セクションの[セキュリティ]で、を選択し ⋮、[外部キーマネージャの削除]*を選択します。

## キー管理ツール間でキーを移行する

クラスタで複数のキー管理ツールを有効にしている場合は、キー管理ツール間でキーを移行する必要があります。このプロセスはSystem Managerで自動的に完了します。

- オンボードキーマネージャまたは外部キーマネージャがクラスタレベルで有効になっていて、一部のボリュームが暗号化されている場合は、その後、Storage VMレベルで外部キー管理ツールを設定する際には、それらのキーをクラスタレベルのオンボードキーマネージャまたは外部キー管理ツールからStorage VMレベルの外部キー管理ツールに移行する必要があります。このプロセスは、System Managerによって自動的に実行されます。
- Storage VMで暗号化なしでボリュームを作成した場合は、キーを移行する必要はありません。

## 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（NVE）

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。ONTAP 9.6以降では、データSVMが暗号化されたデータにアクセスする際に使用するキーを保護するための独立した外部キー管理ツールを設定できます。

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](#)。

このタスクについて

1 つのクラスタまたは SVM 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。

外部キー管理のスコープによって、キー管理サーバの保護対象がクラスタ内のすべての SVM になるか、選択

した SVM のみになるかが決まります。

- クラスタ内のすべての SVM に対して外部キー管理を設定するには、*cluster scop* を使用します。クラスタ管理者は、サーバに格納されているすべてのキーにアクセスできます。
- ONTAP 9.6 以降では、*svm scop* を使用して、クラスタ内のデータ SVM に外部キー管理を設定できます。各テナントが異なる SVM（または SVM のセット）を使用してデータを提供するマルチテナント環境には、この方法が最適です。特定のテナントの SVM 管理者だけが、そのテナントのキーにアクセスできます。
- マルチテナント環境の場合は、次のコマンドを使用して、*MT\_EK\_MGMT* のライセンスをインストールします。

```
system license add -license-code <MT_EK_MGMT license code>
```

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。

同じクラスタで両方のスコープを使用できます。1 つの SVM に対してキー管理サーバが設定されている場合、ONTAP はそれらのサーバのみを使用してキーを保護します。それ以外 ONTAP の場合は、クラスタに対して設定されたキー管理サーバでキーが保護されます。

オンボードキー管理はクラスタスコープで設定でき、外部キー管理は SVM スコープで設定できます。を使用できます `security key-manager key migrate` コマンドを使用して、クラスタスコープのオンボードキー管理から SVM スコープの外部キー管理ツールにキーを移行します。

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、クラスタ管理者または SVM の管理者である必要があります。
- MetroCluster 環境で外部キー管理を有効にする場合は、外部キー管理を有効にする前に MetroCluster が完全に設定されている必要があります。
- 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クラスタのログインプロンプトでコマンドを実行すると、*admin\_SVM* デフォルトでは、現在のクラスタの管理 SVM が使用されます。クラスタスコープを設定するには、クラスタ管理者である必要があります。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。
- ° 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 -vserver cluster1 -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. キー管理ツールとして SVM を設定します。

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



- SVM のログインプロンプトでコマンドを実行すると、SVM デフォルトは現在の SVM です。SVM スコープを設定するには、クラスタ管理者または SVM 管理者である必要があります。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。
- MetroCluster 環境でデータ SVM に外部キー管理を設定する場合は、の手順を繰り返す必要はありません `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 `svm1` 単一のキーサーバがデフォルトポート 5696 でリスンしている場合：

```
svm11::> security key-manager external enable -vserver svm1 -key-servers
keyserver.svm1.com -client-cert SVM1ClientCert -server-ca-certs
SVM1ServerCaCert
```

## 3. 最後の手順をその他の SVM に対して繰り返します。



を使用することもできます `security key-manager external add-servers` コマンドを使用して追加の SVM を設定します。。 `security key-manager external add-servers` コマンドは、に置き換わるものです `security key-manager add` 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。

## 4. 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
```



。 `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			
	svm1	keyserver.svm1.com:5696	available
	cluster1	10.0.0.10:5696	available
		fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234	available
		ks1.local:15696	available
node2			
	svm1	keyserver.svm1.com:5696	available
	cluster1	10.0.0.10:5696	available
		fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234	available
		ks1.local:15696	available

8 entries were displayed.

5. 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。

## 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ー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、クラスター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、クラスター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、両方のクラスターに 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
```

```
cluster1::> security key-manager add -address 20.1.1.1
```



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
```

```
cluster1::> security key-manager add -address 20.1.1.2
```



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。

## クラウドプロバイダを使用してキーを管理します

ONTAP 9.10.1 以降では、を使用できます ["Azure キーボールド \(AKV\)"](#) および ["Google Cloud Platform のキー管理サービス \(Cloud KMS\)"](#) クラウドでホストされるアプリケーションでONTAP暗号化キーを保護する。ONTAP 9.12.0以降では、を使用してNVEキーを保護することもできます ["AWS KMS"](#)。

AWS KMS、AKV、Cloud KMSを使用して保護できます ["NetApp Volume Encryption \(NVE\) キー"](#) データSVMの場合のみ。

このタスクについて

クラウドプロバイダを使用したキー管理は、CLIまたはONTAP REST APIを使用して有効にできます。

クラウドプロバイダを使用してキーを保護する場合は、デフォルトではデータSVM LIFがクラウドキー管理エンドポイントとの通信に使用されることに注意してください。ノード管理ネットワークは、クラウドプロバイダの認証サービス (login.microsoftonline.com for Azure ; oauth2.googleapis.com for Cloud KMS) との通信に使用されます。クラスタネットワークが正しく設定されていないと、クラスタでキー管理サービスが適切に利用されません。

クラウドプロバイダのキー管理サービスを利用する場合は、次の制限事項に注意してください。

- クラウドプロバイダのキー管理は、NetApp Storage Encryption (NSE) およびNetApp Aggregate Encryption (NAE) では使用できません。 ["外部 KMIP"](#) 代わりに使用できます。
- クラウドプロバイダのキー管理はMetroCluster構成では使用できません。
- クラウドプロバイダのキー管理は、データSVMでのみ設定できます。

作業を開始する前に

- 適切なクラウドプロバイダでKMSを設定しておく必要があります。
- ONTAPクラスタのノードでNVEがサポートされている必要があります。
- ["Volume Encryption \(VE\) ライセンスとマルチテナントEncryption Key Management \(MTEKM\) ライセンスをインストールしておく必要があります。"](#)です。これらのライセンスはに含まれてい ["ONTAP One"](#) ます。
- クラスタ管理者またはSVM管理者である必要があります。
- データSVMに暗号化されたボリュームが含まれていないか、キー管理ツールを使用していないことを確認してください。データSVMに暗号化されたボリュームが含まれている場合は、KMSを設定する前にそれらのボリュームを移行する必要があります。

## 外部キー管理を有効にします

外部キー管理を有効にする方法は、使用するキー管理ツールによって異なります。該当するキー管理ツールと環境のタブを選択します。

## AWS

作業を開始する前に

- 暗号化を管理するIAMロールで使用されるAWS KMSキーの付与を作成する必要があります。IAMロールには、次の処理を許可するポリシーが含まれている必要があります。

- DescribeKey
  - Encrypt
  - Decrypt
- [+]

詳細については、AWSのドキュメントを参照してください "[助成金](#)"。

### ONTAP SVMでAWS KMSを有効にします

1. 作業を開始する前に、AWS KMSからアクセスキーIDとシークレットキーの両方を取得します。

2. 権限レベルを `advanced` に設定します。

```
set -priv advanced
```

3. AWS KMSを有効にします。

```
security key-manager external aws enable -vserver svm_name -region  
AWS_region -key-id key_ID -encryption-context encryption_context
```

4. プロンプトが表示されたら、シークレットキーを入力します。

5. AWS KMSが正しく設定されたことを確認します。

```
security key-manager external aws show -vserver svm_name
```

## Azure

### ONTAP SVMでAzure Key Vaultを有効にします

1. 作業を開始する前に、クライアントシークレットまたは証明書のいずれかで、Azure アカウントから適切な認証クレデンシャルを取得する必要があります。  
また、クラスタ内のすべてのノードが正常であることを確認する必要があります。これを確認するには、コマンドを使用します `cluster show`。

2. 特権レベルを `advanced` に設定します

```
set -priv advanced
```

3. SVMでAKVを有効にします

```
security key-manager external azure enable -client-id client_id -tenant-id  
tenant_id -name -key-id key_id -authentication-method {certificate|client-  
secret}
```

プロンプトが表示されたら、Azure アカウントからクライアント証明書またはクライアントシークレットを入力します。

4. AKVが正しく有効になっていることを確認します。

```
security key-manager external azure show vserver svm_name
```

サービスの到達可能性がOKでない場合は、データSVM LIFを介したAKVキー管理サービスへの接続を確立します。

## Google Cloud

### ONTAP SVMでCloud KMSを有効にします

1. 開始する前に、Google Cloud KMSアカウントキーファイルの秘密鍵をJSON形式で取得します。これは GCP アカウントにあります。

また、クラスタ内のすべてのノードが正常であることを確認する必要があります。これを確認するには、コマンドを使用します `cluster show`。

2. 特権レベルをadvancedに設定します。

```
set -priv advanced
```

3. SVMでCloud KMSを有効にします

```
security key-manager external gcp enable -vserver svm_name -project-id  
project_id-key-ring-name key_ring_name -key-ring-location key_ring_location  
-key-name key_name
```

プロンプトが表示されたら、サービスアカウントの秘密鍵を使用して JSON ファイルの内容を入力します

4. Cloud KMSが正しいパラメータで構成されていることを確認します。

```
security key-manager external gcp show vsriver svm_name
```

のステータス `kms_wrapped_key_status` になります “UNKNOWN” 暗号化されたボリュームが作成されていない場合。

サービスへの到達可能性がOKでない場合は、データSVM LIFを介してGCPキー管理サービスへの接続を確立します。

データSVM用にすでに暗号化されたボリュームが1つ以上設定され、管理SVMのオンボードキーマネージャで対応するNVEキーが管理されている場合は、それらのキーを外部キー管理サービスに移行する必要があります。CLIでこれを行うには、次のコマンドを実行します。

```
security key-manager key migrate -from-Vserver admin_SVM -to-Vserver data_SVM
```

データSVMのすべてのNVEキーが正常に移行されるまで、テナントのデータSVM用に暗号化された新しいボリュームを作成することはできません。

#### 関連情報

- ["ネットアップのCloud Volumes ONTAP向け暗号化ソリューションを使用したボリュームの暗号化"](#)

## 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。