



# 外部キー管理の設定

## ONTAP 9

NetApp  
December 20, 2024

# 目次

外部キー管理の設定 .....	1
外部キー管理の概要の設定 .....	1
ONTAP 9 .2以前でネットワーク情報を収集する .....	1
クラスタへのSSL証明書のインストール .....	2
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） .....	3
ONTAP 9 .5以前で外部キー管理を有効にする（ハードウェアベース） .....	4
ONTAPでのクラスタ化された外部キーサーバの設定 .....	6
ONTAP 9 .6以降で認証キーを作成する .....	8
ONTAP 9 .5以前で認証キーを作成する .....	10
FIPSドライブまたはSEDへのデータ認証キーの割り当て（外部キー管理） .....	12

# 外部キー管理の設定

## 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ためにクラスタで使用するキーを保護できます。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。

NetApp Volume Encryption (NVE) は、ONTAP 9.1以降のオンボードキーマネージャで実装できます。ONTAP 9.3以降では、NVEを外部キー管理 (KMIP) とオンボードキーマネージャで実装できます。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 [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する

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	脚注	値
キー管理ネットワークインターフェイス名		
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は、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	

各KMIPサーバのポート番号	オプション。ポート番号はすべてのKMIPサーバで同じである必要があります。ポート番号を指定しない場合、デフォルトのポート5696が使用されます。これは、Internet Assigned Numbers Authority (IANA) がKMIPに割り当てたポートです。	
キータグ名	オプション。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

"NetAppテクニカルレポート3954：『NetApp Storage Encryption Preinstallation Requirements and Procedures for IBM Tivoli Lifetime Key Manager』 "

"NetAppテクニカルレポート4074：『NetApp Storage Encryption Preinstallation Requirements and Procedures for SafeNet KeySecure』 "

## クラスタへのSSL証明書のインストール

クラスタとKMIPサーバは、KMIP SSL証明書を使用して相互のIDを検証し、SSL接続を確立します。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サーバのルート認証局 (CA) 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。

#### タスクの内容

HAペアでは、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。

#### 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後どちらでも実行できます。

#### 手順

1. クラスタの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の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台のサーバが推奨されます。

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 クラスタ化された外部キーサーバの設定](#)。

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、両方のクラスタに同じ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、コマンドに置き換わるもの `security key-manager setup` です。外部キー管理の設定を変更するには、コマンドを実行し `security key-manager external modify` 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、パートナークラスタでこのコマンドを繰り返す必要があります `security key-manager external enable`。

次のコマンドは、3台の外部キーサーバでの外部キー管理を有効にします `cluster1`。1つ目のキーサーバはホスト名とポートを使用して指定し、2つ目のキーサーバはIPアドレスとデフォルトポートを使用して指定し、3つ目のキーサーバはIPv6アドレスとポートを使用して指定します。

```
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、コマンドに置き換わるもの `security key-manager show -status` です。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台のサーバが推奨されます。

## タスクの内容

ONTAPでは、クラスタ内のすべてのノードに対してKMIPサーバの接続が設定されます。

## 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、両方のクラスタに同じ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環境の場合は、両方のクラスタでこのコマンドを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環境の場合は、両方のクラスタでこのコマンドを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環境の場合は、両方のクラスタでこのコマンドを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。

## ONTAPでのクラスタ化された外部キーサーバの設定

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、1台のSVM上に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。キーを登録する際、ONTAPは最初にプライマリキーサーバへのアクセスを試行し、その後処理が正常に完了するまで各セカンダリサーバへのアクセスを順次試行して、キーの重複を回避します。

外部キーサーバは、NSE、NVE、NAE、SEDの各キーに使用できます。1台のSVMに最大4台の外部プライマリKMIPサーバを指定できます。各プライマリサーバには、最大3台のセカンダリキーサーバを指定できます。

### 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。"](#)です。
- このプロセスでは、KMIPを使用するキーサーバのみがサポートされます。サポートされているキーサーバのリストについては、[を参照してください"NetApp Interoperability Matrix Tool"](#)。
- 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。
- パラメータ内のserversリストの引数の順序`-secondary-key-servers`は、外部キー管理（KMIP）サーバのアクセス順序を反映しています。
- この手順で説明されているコマンドの詳細については、["ONTAPコマンドリファレンス"](#)

### クラスタ化されたキーサーバを作成する

設定手順は、プライマリキーサーバが設定されている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いずれか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の変更

外部キーサーバクラスタを変更するには、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します。

### 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、まずコマンドを使用してそのサーバをSVMから削除する必要があります `security key-manager external remove-servers`。

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 [\[mod-secondary\]](#) 既存のキーを削除するときセカンダリキーサーバをプライマリサーバに変換すると、削除と変換を完了する前に新しいサーバを追加しようとすると、キーが重複することがあります。

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には、コマンドのパラメータを ``security key-manager external modify-server`` 使用し `-secondary-key-servers`` 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。リスト内のセカンダリキーサーバの指定した順序によって、セカンダリキーサーバのアクセス順序が決まります。アクセス順序を変更するには、セカンダリキーサーバを別の順序で入力してコマンドを実行し ``security key-manager external modify-server`` ます。

セカンダリキーサーバを削除するには、 `-secondary-key-servers`` 削除するキーサーバを省略して保持するキーサーバを引数に含める必要があります。すべてのセカンダリキーサーバを削除するには、引数（なし）を使用し ``` ます。

リンク[https://docs.netapp.com/us-en/ONTAP-cli/^\[security key-manager external`](https://docs.netapp.com/us-en/ONTAP-cli/^[security key-manager external`)の詳細については、ONTAPコマンドリファレンスを参照してください。NetApp.com /us-en/ONTAP-cli/^[security key-manager external` コマンドを参照してください。

## ONTAP 9.6以降で認証キーを作成する

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サーバに格納できます `security key-manager key create`。

### タスクの内容

セキュリティの設定でデータ認証とFIPS 140-2認証に異なるキーを使用する必要がある場合は、それぞれに別々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の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せん。
- コマンドを使用すると、使用されていないキーを削除できます `security key-manager key delete`。`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、その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`

### 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
```



を設定する `prompt-for-key=true` と、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。それ以外の場合は、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、コマンドに置き換わるもの `security key-manager create-key` です。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 key query
      Vserver: cluster1
      Key Manager: external
      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: external
      Node: node2

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

```

## ONTAP 9.5以前で認証キーを作成する

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サーバに格納できます  
`security key-manager create-key`。

### タスクの内容

セキュリティの設定でデータ認証とFIPS 140-2認証に異なるキーを使用する必要がある場合は、それぞれに別々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と同じにして使用できます。

ONTAPでは、クラスタ内のすべてのノードの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になっている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てから、コマンドをもう一度実行します。

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
```

完全なコマンド構文については、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、認証キーの参照に使用する識別子です。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 `cluster1` ます。

```
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。

次の例では、の認証キーが作成されたことを確認し `cluster1` ます。

```

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へのデータ認証キーの割り当て（外部キー管理）

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 `storage encryption disk modify`。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ときに使用します。

### タスクの内容

自己暗号化ドライブは、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。SASドライブの標準のデフォルト値は、キーIDが0x0のManufacturer Secure ID (MSID；メーカーのセキュアID) です。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で表されます。このキー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。

### 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
```

完全なコマンド構文については、コマンドのマニュアルページを参照してください。



キーIDは、コマンドを使用して表示できます `security key-manager query -key -type NSE-AK`。

```
cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
```

```
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
F1CB30AFF1CB30B001010000000000A68B167F92DD54196297159B5968923C
0.0.1     data
F1CB30AFF1CB30B001010000000000A68B167F92DD54196297159B5968923C
[...]
```

## 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。