



# クラスタとKMIPサーバの相互認証

## ONTAP 9

NetApp  
February 12, 2026

# 目次

クラスタとKMIPサーバの相互認証 .....	1
ONTAPクラスタとKMIPサーバの相互認証の概要 .....	1
ONTAP でクラスタの証明書署名要求を生成する .....	1
ONTAPクラスタ用のCA署名サーバ証明書をインストールする .....	2
ONTAPにKMIPサーバー用のCA署名付きクライアント証明書をインストールする .....	3

# クラスタとKMIPサーバの相互認証

## ONTAPクラスタとKMIPサーバの相互認証の概要

クラスタと外部キーマネージャ（Key Management Interoperability Protocol (KMIP) サーバなど）を相互認証することで、キーマネージャはSSL経由のKMIPを使用してクラスタと通信できるようになります。これは、アプリケーションまたは特定の機能（ストレージ暗号化機能など）が、安全なデータアクセスを提供するために安全なキーを必要とする場合に行います。

## ONTAP でクラスタの証明書署名要求を生成する

セキュリティ証明書 `generate-csr` コマンドを使用して、証明書署名要求（CSR）を生成できます。要求が処理されると、証明機関（CA）が署名されたデジタル証明書を送信します。

開始する前に

このタスクを実行するには、クラスタ管理者またはSVM管理者である必要があります。

手順

1. CSRを生成します。

```
security certificate generate-csr -common-name <FQDN_or_common_name>
-size 512|1024|1536|2048 -country <country> -state <state> -locality
<locality> -organization <organization> -unit <unit> -email-addr
<email_of_contact> -hash-function SHA1|SHA256|MD5
```

```
`security certificate generate-csr`
```

の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/security-certificate-generate-csr.html](https://docs.netapp.com/us-en/ontap-cli/security-certificate-generate-csr.html) ["ONTAPコマンド リファレンス"] をご覧ください。

次のコマンドは、SHA256ハッシュ関数で生成される2,048ビット秘密鍵を使用して、CSRを作成します。この証明書は、米国カリフォルニア州のサンバールにある企業（カスタム共通名server1.companyname.com）のIT部門のソフトウェアグループが使用します。SVM担当管理者のEメールアドレスはweb@example.comです。出力にはCSRと秘密鍵が表示されます。

```
cluster1::>security certificate generate-csr -common-name
server1.companyname.com -size 2048 -country US -state California -
locality Sunnyvale -organization IT -unit Software -email-addr
web@example.com -hash-function SHA256
Certificate Signing Request :
-----BEGIN CERTIFICATE REQUEST-----
<certificate_value>
-----END CERTIFICATE REQUEST-----
Private Key :
24 | Administrator Authentication and RBAC
-----BEGIN RSA PRIVATE KEY-----
<key_value>
-----END RSA PRIVATE KEY-----
Note: Please keep a copy of your certificate request and private key
for future reference.
```

2. CSR出力の証明書要求をデジタル形式（Eメールなど）で信頼できるサードパーティのCAに送信し、署名を求めます。

要求が処理されると、署名済みのデジタル証明書がCAから送信されます。秘密鍵とCA署名デジタル証明書のコピーを保管する必要があります。

## ONTAPクラスタ用のCA署名サーバ証明書をインストールする

SSLサーバがクラスタまたはStorage Virtual Machine（SVM）をSSLクライアントとして認証できるようにするには、クラスタまたはSVMにクライアントタイプのデジタル証明書をインストールします。次に、SSLサーバ管理者にclient-ca証明書を提供し、サーバにインストールしてもらいます。

開始する前に

```
`server-ca`証明書タイプを使用して、クラスタまたはSVMに
SSLサーバのルート証明書がすでにインストールされている必要があります。
```

手順

1. クライアント認証に自己署名デジタル証明書を使用するには、`type client`パラメータを指定して`security certificate create`コマンドを使用します。

```
`security certificate create`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/security-certificate-create.html["ONTAPコマンド リファレンス"]をご覧ください。
```

2. クライアント認証にCA署名デジタル証明書を使用するには、次の手順を実行します：

- a. `security certificate generate-csr` コマンドを使用して、デジタル証明書署名要求 (CSR) を生成します。

ONTAP は、証明書要求と秘密キーを含む CSR 出力を表示し、将来の参照用に出力をファイルにコピーするように通知します。

- b. CSR 出力からの証明書要求を電子形式 (電子メールなど) で信頼できる CA に送信し、署名を依頼します。

将来の参照用に、秘密キーと CA 署名証明書のコピーを保管しておく必要があります。

要求が処理されると、署名済みのデジタル証明書が CA から送信されます。

- a. `-type client` パラメータを指定した `security certificate install` コマンドを使用して、CA 署名証明書をインストールします。
- b. プロンプトが表示されたら証明書と秘密キーを入力し、\*Enter\* キーを押します。
- c. プロンプトが表示されたら追加のルート証明書または中間証明書を入力し、\*Enter\* キーを押します。

信頼されたルート CA から始まり、お客様に発行された SSL 証明書で終わる証明書チェーンに中間証明書がない場合は、クラスタまたは SVM に中間証明書をインストールします。中間証明書は、エンドエンティティサーバ証明書を発行するために信頼されたルート CA によって発行される従属証明書です。その結果、信頼されたルート CA から始まり、中間証明書を經由して、お客様に発行された SSL 証明書で終わる証明書チェーンが作成されます。

3. クラスタまたは SVM の `client-ca` 証明書を SSL サーバーの管理者に提供し、サーバーにインストールしてもらいます。

```
`-instance` および -type client-ca パラメータを指定した security certificate show コマンドは、client-ca 証明書情報を表示します。
```

#### 関連情報

- ["security certificate install"](#)
- ["セキュリティ証明書の表示"](#)

## ONTAP に KMIP サーバー用の CA 署名付きクライアント証明書をインストールする

Key Management Interoperability Protocol (KMIP) の証明書サブタイプ (`-subtype kmip-cert` パラメータ) は、`client` および `server-ca` タイプとともに、証明書がクラスタと KMIP サーバなどの外部キー マネージャとの相互認証に使用されることを指定します。

#### タスク概要

KMIP 証明書をインストールして、KMIP サーバーをクラスタの SSL サーバーとして認証します。

#### 手順

1. `-type server-ca` および `-subtype kmip-cert` パラメータを指定した `security certificate install` コマンドを使

用して、KMIPサーバーのKMIP証明書をインストールします。

2. プロンプトが表示されたら、証明書を入力し、Enterキーを押します。

ONTAP は、将来の参照用に証明書のコピーを保管しておくように通知します。

```
cluster1::> security certificate install -type server-ca -subtype kmip-  
cert  
-vserver cluster1  
  
Please enter Certificate: Press <Enter> when done  
-----BEGIN CERTIFICATE-----  
<certificate_value>  
-----END CERTIFICATE-----  
  
You should keep a copy of the CA-signed digital certificate for future  
reference.  
  
cluster1::>
```

#### 関連情報

- ["security certificate install"](#)

## 著作権に関する情報

Copyright © 2026 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。