



ネットワークの保護 ONTAP 9

NetApp
February 12, 2026

目次

| | |
|--|----|
| ネットワークの保護 | 1 |
| すべてのSSL接続に対してFIPSを使用してONTAPネットワークセキュリティを構成する | 1 |
| FIPS を有効にする | 2 |
| FIPSの無効化 | 3 |
| FIPS準拠ステータスの表示 | 3 |
| IPSecの転送中暗号化の設定 | 4 |
| ONTAPネットワークでIPセキュリティを使用するための準備 | 4 |
| ONTAPネットワークのIPセキュリティを構成する | 8 |
| ONTAPバックエンド クラスター ネットワーク暗号化を設定する | 13 |
| クラスター ネットワーク通信の暗号化を有効または無効にする | 14 |
| クラスター ネットワーク暗号化証明書を管理する | 14 |
| ONTAPネットワーク内のLIFのファイアウォールポリシーを設定する | 15 |
| ファイアウォール ポリシーとLIF | 16 |
| portmapサービスの設定 | 17 |
| ファイアウォール ポリシーの作成とLIFへの割り当て | 18 |
| ファイアウォール サービスとポリシーを管理するための ONTAP コマンド | 22 |

ネットワークの保護

すべてのSSL接続に対してFIPSを使用してONTAPネットワークセキュリティを構成する

ONTAPは、すべてのSSL接続において連邦情報処理標準（FIPS）140-2に準拠しています。SSL FIPSモードのオン/オフを切り替えたり、SSLプロトコルをグローバルに設定したり、ONTAP内の脆弱な暗号を無効にしたりできます。

デフォルトでは、ONTAP の SSL は FIPS 準拠が無効に設定され、次の TLS プロトコルが有効になっています：

- TLSv1.3（ONTAP 9.11.1以降）
- TLSv1.2

以前のONTAPリリースでは、次のTLSプロトコルがデフォルトで有効になっていました：

- TLSv1.1（ONTAP 9.12.1以降ではデフォルトで無効）
- TLSv1（ONTAP 9.8以降ではデフォルトで無効）

SSL FIPSモードが有効な場合は、ONTAPからONTAP外部のクライアントまたはサーバ コンポーネントへのSSL通信に、FIPSに準拠したSSL用の暗号が使用されます。

管理者アカウントがSSH公開鍵を使用してSVMにアクセスできるようにする場合は、SSL FIPSモードを有効にする前に、ホスト キー アルゴリズムがサポートされていることを確認する必要があります。

注： ONTAP 9.11.1 以降のリリースでは、ホスト キー アルゴリズムのサポートが変更されました。

| ONTAPリリース | サポートされているキーのタイプ | サポートされていないキー タイプ |
|-----------|-----------------------------------|---|
| 9.11.1以降 | ecdsa-sha2-nistp256 | rsa-sha2-512 + rsa-sha2-256 + ssh-ed25519 + ssh-dss + ssh-rsa |
| 9.10.1以前 | ecdsa-sha2-nistp256 + ssh-ed25519 | ssh-dss + ssh-rsa |

サポートされるキー アルゴリズムを使用していない既存のSSH公開鍵アカウントは、FIPSを有効にする前に、サポートされるキー アルゴリズムで再設定する必要があります。この処理を実行しないと管理者認証は失敗します。

詳細については、"[SSH公開鍵アカウントの有効化](#)"を参照してください。

ONTAP 9.18.1では、SSLでML-KEM、ML-DSA、SLH-DSAといった量子コンピュータ耐性暗号アルゴリズムのサポートが導入され、将来起こり得る量子コンピュータ攻撃に対するセキュリティがさらに強化されます。これらのアルゴリズムはFIPSは無効ですの場合にのみ利用可能です。量子コンピュータ耐性暗号アルゴリズムは、FIPSが無効で、ピアがそれらをサポートしている場合にネゴシエートされます。

FIPS を有効にする

システムのインストールまたはアップグレードの直後に、すべてのセキュアなユーザがセキュリティ設定を調整することを推奨します。SSL FIPSモードが有効な場合は、ONTAPからONTAP外部のクライアントまたはサーバ コンポーネントへのSSL通信に、FIPSに準拠したSSL用の暗号が使用されます。



FIPSが有効な場合、4096ビットのRSAキーを使用する証明書をインストールまたは作成することはできません。

手順

1. advanced権限レベルに切り替えます。

```
set -privilege advanced
```

2. FIPSを有効にします。

```
security config modify * -is-fips-enabled true
```

3. 続行するように求められたら、`y`を入力してください

4. ONTAP 9.9.1以降では、再起動は不要です。ONTAP 9.8以前を実行している場合は、クラスタ内の各ノードを1つずつ手動で再起動してください。

例

ONTAP 9.9.1以降を実行している場合、警告メッセージは表示されません。

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

Warning: This command will enable FIPS compliance and can potentially cause some non-compliant components to fail. MetroCluster and Vserver DR require FIPS to be enabled on both sites in order to be compatible.

Do you want to continue? {y|n}: y

Warning: When this command completes, reboot all nodes in the cluster. This is necessary to prevent components from failing due to an inconsistent security configuration state in the cluster. To avoid a service outage, reboot one node at a time and wait for it to completely initialize before rebooting the next node. Run "security config status show" command to monitor the reboot status.

Do you want to continue? {y|n}: y

`security config modify`および SSL FIPS

モード構成の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/security-config-modify.html](https://docs.netapp.com/us-en/ontap-cli/security-config-modify.html)["ONTAPコマンド リファレンス"]を参照してください。

FIPSの無効化

ONTAP 9.18.1以降、ONTAPのSSLはML-KEM、ML-DSA、およびSLH-DSAのポスト量子コンピューティング暗号化アルゴリズムをサポートします。これらのアルゴリズムは、FIPSが無効で、ピアがこれらのアルゴリズムをサポートしている場合にのみ使用できます。

手順

1. advanced権限レベルに切り替えます。

```
set -privilege advanced
```

2. 次のように入力してFIPSを無効にします。

```
security config modify -is-fips-enabled false
```

3. 続行するように求められたら、`y`と入力します。
4. ONTAP 9.9.1以降では、再起動は不要です。ONTAP 9.8以前を実行している場合は、クラスタ内の各ノードを手動で再起動してください。

SSLv3 プロトコルを使用する必要がある場合は、上記の手順で FIPS を無効にする必要があります。SSLv3 は、FIPS が無効になっている場合にのみ有効にできます。

次のコマンドでSSLv3を有効にできます。ONTAP 9.9.1以降を実行している場合は、警告メッセージは表示されません。

```
security config modify -supported-protocols SSLv3
```

```
Warning: Enabling the SSLv3 protocol may reduce the security of the  
interface, and is not recommended.
```

```
Do you want to continue? {y|n}: y
```

```
Warning: When this command completes, reboot all nodes in the cluster.  
This is necessary to prevent components from failing due to an  
inconsistent security configuration state in the cluster. To avoid a  
service outage, reboot one node at a time and wait for it to completely  
initialize before rebooting the next node. Run "security config status  
show" command to monitor the reboot status.
```

```
Do you want to continue? {y|n}: y
```

FIPS準拠ステータスの表示

クラスタ全体が現在のセキュリティ設定を実行しているかどうかを確認できます。

手順

1. ONTAP 9.8 以前を実行している場合は、クラスタ内の各ノードを 1 つずつ手動で再起動します。
2. 現在の準拠ステータスを表示します。

security config show

```
cluster1::> security config show
Cluster      Supported
FIPS Mode    Protocols Supported Cipher Suites
-----
false        TLSv1.3,   TLS_RSA_WITH_AES_128_CCM,
TLS_RSA_WITH_AES_128_CCM_8,
              TLSv1.2   TLS_RSA_WITH_AES_128_GCM_SHA256,
              TLS_RSA_WITH_AES_128_CBC_SHA,
              TLS_RSA_WITH_AES_128_CBC_SHA256,
TLS_RSA_WITH_AES_256_CCM,
              TLS_RSA_WITH_AES_256_CCM_8,
              ...
```

`security config show`の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/security-config-show.html>["ONTAPコマンド リファレンス"]を参照してください。

関連情報

- ["FIPS 203 : Module-Lattice-Based Key-Encapsulation Mechanism Standard \(ML-KEM\) "](#)
- ["FIPS 204 : Module-Lattice-Based Digital Signature Standard \(ML-DSA\) "](#)
- ["FIPS 205 : ステートレス ハッシュベース デジタル署名標準 \(SLH-DSA\) "](#)

IPSecの転送中暗号化の設定

ONTAPネットワークでIPセキュリティを使用するための準備

ONTAP 9.8以降では、必要に応じてIPセキュリティ (IPsec) を使用してネットワークトラフィックを保護できます。IPSecは、ONTAPで使えるいくつかの移動中 / 転送中データ暗号化オプションの1つです。本番環境でIPSecを使用する前に、IPSecを設定する準備をしておく必要があります。

ONTAPでのIPセキュリティの実装

IPsecは、IETFによって管理されるインターネット標準です。ネットワーク エンドポイント間を流れるトラフィックの、IPレベルでのデータ暗号化、データ整合性、認証を実現します。

ONTAPでは、ONTAPとさまざまなクライアントの間のあらゆるIPトラフィック (NFS、SMB、iSCSIプロトコルなど) が、IPsecによって保護されます。プライバシーとデータ整合性を確保するだけでなく、リプレイ攻撃や中間者攻撃などの各種攻撃からネットワークトラフィックを守ります。ONTAPでは、トランスポートモードのIPsec実装を使用します。IPv4がIPv6を使用してONTAPとクライアントの間でキー マテリアルをネ

ゴシエートするために、Internet Key Exchange (IKE) プロトコル バージョン2を利用します。

クラスタでIPSec機能を有効にすると、さまざまなトラフィック特性に一致するONTAPセキュリティ ポリシー データベース (SPD) のエントリが、ネットワークに1つ以上必要になります。これらのエントリは、データの処理と送信に必要な特定の保護の詳細 (暗号スイートや認証方式など) にマッピングされます。各クライアントにも、対応するSPDエントリが必要です。

トラフィックの種類によっては、別の移動中データ暗号化オプションが望ましいものもあります。たとえば、NetApp SnapMirrorとクラスタ ピアリング トラフィックの暗号化については、IPsecではなくTransport Layer Security (TLS) プロトコルが一般的に推奨されます。これは、ほとんどの状況でTLSの方が高いパフォーマンスが得られるためです。

関連情報

- ["Internet Engineering Task Force"](#)
- ["RFC 4301：インターネット プロトコルのセキュリティ アーキテクチャ"](#)

ONTAP IPsec実装の進化

IPsecはONTAP 9.8で初めて導入されました。その実装は、以下に説明するように、その後のONTAPリリースで進化を続けています。

ONTAP 9.18.1

IPsec ハードウェア オフロードのサポートがIPv6 トラフィックに拡張されました。

ONTAP 9.17.1

IPsec ハードウェア オフロードのサポートが["リンク アグリゲーション グループ"](#)に拡張されました。["耐量子 事前共有鍵 \(PPK\)"](#)はIPsec 事前共有キー (PSK) 認証でサポートされています。

ONTAP 9.16.1

暗号化や整合性チェックなどの暗号化操作の一部は、サポートされているNICカードにオフロードできます。詳細については、[IPSecのハードウェア オフロード機能](#)を参照してください。

ONTAP 9.12.1

MetroCluster IP構成とファブリック接続MetroCluster構成で、フロントエンドのホスト プロトコルとしてIPsecがサポートされました。MetroClusterクラスタでのIPsecのサポートはフロントエンドのホスト トラフィックに限定され、MetroClusterのクラスタ間LIFではサポートされません。

ONTAP 9.10.1

IPsec認証には、PSKに加えて証明書も使用できます。ONTAP 9.10.1より前のバージョンでは、認証にはPSKのみがサポートされています。

ONTAP 9.9.1

IPsecで使用する暗号化アルゴリズムが、FIPS 140-2準拠になりました。これらのアルゴリズムは、FIPS 140-2認定を受けたONTAPのNetApp Cryptographic Moduleで処理されています。

ONTAP 9.8

IPsecのサポートが、トランスポート モードの実装に基づいて初めて利用可能になりました。

IPSecのハードウェア オフロード機能

ONTAP 9.16.1以降を使用している場合、暗号化や整合性チェックなど、計算負荷の高い特定の処理を、ストレージ ノードにインストールされたネットワーク インターフェイス コントローラー (NIC) カードにオフロードするオプションがあります。NICカードにオフロードされた処理のスループットは約5%以下です。これにより、IPsecで保護されたネットワーク トラフィックのパフォーマンスとスループットが大幅に向上します。

要件と推奨事項

IPsecのハードウェア オフロード機能を使用する前に、考慮しておくべき要件がいくつかあります。

サポートされるイーサネット カード

サポートされているイーサネット カードのみをインストールして使用する必要があります。ONTAP 9.16.1 以降では、次のイーサネット カードがサポートされています：

- X50131A (2p、40G/100G/200G/400G Ethernetコントローラ)
- X60132A (4p、10G/25G Ethernet Controller)

ONTAP 9.17.1 では、次のイーサネット カードのサポートが追加されました。

- X50135A (2p、40G/100G Ethernet Controller)
- X60135A (2p、40G/100G Ethernet Controller)

X50131A および X50135A カードは、次のプラットフォームでサポートされています：

- ASAA1K
- ASAA90
- ASAA70
- AFF A1K用
- AFF A90
- AFF A70

X60132A および X60135A カードは、次のプラットフォームでサポートされています：

- ASAA50
- ASAA30
- ASAA20
- AFF A50
- AFF A30
- AFF A20用

サポートされているプラットフォームとカードの詳細については、"[NetApp Hardware Universe](#)"を参照してください。

クラスタ スコープ

IPsecハードウェアオフロード機能はクラスタ全体でグローバルに設定されます。そのため、例えば `security

ipsec config` コマンドはクラスタ内のすべてのノードに適用されます。

構成の一貫性

サポートされているNICカードが、クラスタ内のすべてのノードに取り付けられている必要があります。サポートされているNICカードが一部のノードでしか使用できない場合、一部のLIFがオフロード対応のNICにホストされていないと、フェイルオーバー後にパフォーマンスが大幅に低下することがあります。

アンチリプレイの無効化

ONTAP（デフォルト設定）およびIPsecクライアントでIPsecアンチリプレイ保護を無効にする必要があります。無効にしない場合、フラグメンテーションとマルチパス（冗長ルート）はサポートされません。

ONTAP IPsec 設定がデフォルトから変更され、アンチリプレイ保護が有効になっている場合は、次のコマンドを使用して無効にします：

```
security ipsec config modify -replay-window 0
```

クライアントでIPsecアンチリプレイ保護が無効になっていることを確認する必要があります。アンチリプレイ保護を無効にするには、クライアントのIPsecドキュメントを参照してください。

制限事項

IPsecのハードウェア オフロード機能を使用する前に、考慮しておくべき制限事項がいくつかあります。

IPv6

ONTAP 9.18.1以降では、IPsecハードウェアオフロード機能でIPv6がサポートされます。ONTAP 9.18.1以前のバージョンでは、IPsecハードウェアオフロードはIPv6をサポートしていません。

拡張シーケンス番号

IPSecの拡張シーケンス番号は、ハードウェア オフロード機能ではサポートされていません。通常の32ビットシーケンス番号のみが使用されます。

リンク アグリゲーション

ONTAP 9.17.1 以降では、IPsec ハードウェア オフロード機能を["リンク アグリゲーション グループ"](#)で使用できます。

9.17.1以前のバージョンでは、IPsecハードウェアオフロード機能はリンクアグリゲーションをサポートしていません。ONTAP CLIの`network port ifgrp` コマンドで管理されるインターフェースまたはリンクアグリゲーショングループでは使用できません。

ONTAP CLIでの設定のサポート

ONTAP 9.16.1では、既存の3つのCLIコマンドが更新され、以下に説明するIPsecハードウェアオフロード機能がサポートされます。詳細については、["ONTAPでのIPセキュリティの設定"](#)も参照してください。

| ONTAP コマンド | 更新 |
|----------------------------|--|
| security ipsec config show | ブール型パラメータ `Offload Enabled` は、現在の NIC オフロード ステータスを表示します。 |

| ONTAP コマンド | 更新 |
|--|--|
| <code>security ipsec config modify</code> | このパラメータ `is-offload-enabled` を使用して、NIC オフロード機能を有効または無効にすることができます。 |
| <code>security ipsec config show-ipseca</code> | インバウンド トラフィックとアウトバウンド トラフィックをバイト数とパケット数で表示するために、4つの新しいカウンタが追加されています。 |

ONTAP REST APIでの設定のサポート

ONTAP 9.16.1では、以下に説明するように、IPSecのハードウェア オフロード機能をサポートするために、既存の2つのREST APIエンドポイントが更新されています。

| REST エンドポイント | 更新 |
|---|---|
| <code>/api/security/ipsec</code> | パラメータ `offload_enabled` が追加され、PATCH メソッドで使用できるようになりました。 |
| <code>/api/security/ipsec/security_association</code> | オフロード機能で処理された総バイト数とパケット数を追跡するために、2つの新しいカウンタ値が追加されています。 |

ONTAP REST APIの詳細（["ONTAP REST APIの新機能"](#)を含む）については、ONTAP自動化ドキュメントを参照してください。["IPsec エンドポイント"](#)の詳細については、ONTAP自動化ドキュメントも参照してください。

関連情報

- ["セキュリティ IPsec"](#)

ONTAP ネットワークのIPセキュリティを構成する

ONTAP クラスタでIPSecの転送中暗号化を設定してアクティブ化するためには、いくつかのタスクを実行する必要があります。



IPsec を設定する前に、必ず["IPセキュリティを使用する準備"](#)を確認してください。たとえば、ONTAP 9.16.1以降で使用可能なIPsecハードウェア オフロード機能を使用するかどうかを決定する必要がある場合があります。

クラスタでのIPsecの有効化

IPsecをクラスタで有効にすることで、転送中もデータの安全性と暗号化を維持できます。

手順

1. IPsecがすでに有効になっているかどうかを確認します。

```
security ipsec config show
```

結果に `IPsec Enabled: false` が含まれる場合は、次の手順に進みます。

2. IPsecを有効にします。

```
security ipsec config modify -is-enabled true
```

ブール型パラメータ `is-offload-enabled` を使用して、IPsec ハードウェア オフロード機能を有効にできます。

3. 検出コマンドをもう一度実行します。

```
security ipsec config show
```

結果には `IPsec Enabled: true` が含まれるようになりました。

証明書認証用のIPsecポリシーの作成準備

この手順は、認証に事前共有キー（PSK）のみを使用しており、証明書認証を使用しない場合は省略できます。

認証に証明書を使用するIPsecポリシーを作成する前に、次の前提条件を満たしていることを確認する必要があります。

- ONTAPとクライアントの両方がエンド エンティティ（ONTAPまたはクライアント）の証明書を検証できるように、両方に相手側のCA証明書がインストールされている。
- ポリシーの対象になるONTAP LIFの証明書がインストールされている。



証明書はONTAP LIF間で共有できます。証明書とLIFが1対1で対応している必要はありません。

手順

1. すでにインストールされている場合（ONTAPの自己署名ルートCAの場合）を除き、相互認証で使用するすべてのCA証明書（ONTAP側とクライアント側の両方のCAを含む）をONTAP証明書管理にインストールします。

サンプル コマンド

```
cluster::> security certificate install -vserver svm_name -type server-ca  
-cert-name my_ca_cert
```

2. 認証中にインストールされている CA が IPsec CA 検索パス内にあることを確認するには、`security ipsec ca-certificate add` コマンドを使用して ONTAP 証明書管理 CA を IPsec モジュールに追加します。

サンプル コマンド

```
cluster::> security ipsec ca-certificate add -vserver svm_name -ca-certs  
my_ca_cert
```

3. ONTAP LIFで使用する証明書を作成してインストールします。この証明書の発行元CAがすでにONTAPにインストールされ、IPsecに追加されている必要があります。

サンプル コマンド

```
cluster::> security certificate install -vserver svm_name -type server -cert  
-name my_nfs_server_cert
```

ONTAPの証明書の詳細については、ONTAP 9のドキュメントのsecurity certificateコマンドを参照してください。

セキュリティ ポリシー データベース (SPD) の定義

IPsecでトラフィックをネットワーク上で転送するためにはSPDエントリが必要です。これは、認証にPSKと証明書のどちらを使用する場合にも当てはまります。

手順

1. `security ipsec policy create` コマンドを使用して次の操作を実行します：

- a. IPsec転送に参加するONTAPのIPアドレスまたはIPアドレスのサブネットを選択します。
- b. ONTAPのIPアドレスに接続するクライアントのIPアドレスを選択します。



クライアントでInternet Key Exchangeバージョン2 (IKEv2) と事前共有キー (PSK) がサポートされている必要があります。

- c. 必要に応じて、トラフィックを保護するための上位層プロトコル (UDP、TCP、ICMPなど)、ローカルポート番号、リモートポート番号などの詳細なトラフィックパラメータを選択します。対応するパラメータは、protocols、local-ports、`remote-ports`です。

この手順は、ONTAPのIPアドレスとクライアントのIPアドレスの間のすべてのトラフィックを保護する場合は省略します。デフォルトでは、すべてのトラフィックが保護されます。

- d. 希望する認証方法の `auth-method` パラメータとして、PSK または公開鍵インフラストラクチャ (PKI) を入力します。
 - i. PSK を入力する場合は、パラメータを含めて、<enter> を押して事前共有キーを入力して検証します。



ホストとクライアントの両方がstrongSwanを使用し、ホストまたはクライアントに対してワイルドカード ポリシーが選択されていない場合、`local-identity` および `remote-identity` パラメータはオプションです。

- ii. PKIを入力する場合は、cert-name、local-identity、`remote-identity` パラメータも入力する必要があります。リモート側の証明書IDが不明な場合、または複数のクライアントIDが想定される場合は、特別なID `ANYTHING` を入力してください。
- e. ONTAP 9.17.1以降では、`ppk-identity` パラメータを使用して、オプションでポスト量子事前共有鍵 (PPK) IDを入力できます。PPKは、将来起こりうる量子コンピュータ攻撃に対するセキュリティをさらに強化します。PPK IDを入力すると、PPKシークレットの入力を求められます。PPKはPSK認証でのみサポートされます。

```
`security ipsec policy create`
```

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

```
security ipsec policy create -vserver vs1 -name test34 -local-ip-subnets
192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32
Enter the preshared key for IPsec Policy _test34_ on Vserver _vs1_:
```

```
security ipsec policy create -vserver vs1 -name test34 -local-ip-subnets
192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32 -local-ports 2049
-protocols tcp -auth-method PKI -cert-name my_nfs_server_cert -local
-identity CN=netapp.ipsec.lif1.vs0 -remote-identity ANYTHING
```

ONTAPとクライアントの両方で一致するIPsecポリシーが設定され、両方に認証クレデンシャル（PSKまたは証明書）がインストールされるまで、クライアントとサーバの間でIPトラフィックを転送することはできません。

IPsec IDの使用

事前共有キー認証方式では、ホストとクライアントの両方でstrongSwanを使用しており、ホストまたはクライアントに対してワイルドカード ポリシーが選択されていない場合、ローカルIDとリモートIDは任意です。

PKI/証明書認証方式では、ローカルIDとリモートIDの両方が必須です。これらのIDは、それぞれの証明書内で認証されるIDを指定し、検証プロセスで使用されます。リモートIDが不明な場合、または複数の異なるIDが使用される可能性がある場合は、特別なID `ANYTHING` を使用してください。

タスク概要

ONTAPでは、SPDエントリを変更するかSPDポリシーの作成時にIDを指定します。SPDには、IPアドレスまたは文字列形式のID名を使用できます。

手順

1. 次のコマンドを使用して、既存のSPD ID設定を変更します。

```
security ipsec policy modify
```

コマンド例

```
security ipsec policy modify -vserver vs1 -name test34 -local-identity
192.168.134.34 -remote-identity client.fooboo.com
```

IPsecの複数クライアント設定

IPsecを利用するクライアントの数が少ない場合は、クライアントごとにSPDエントリを1つ使用するだけで十分です。ただし、数百、数千のクライアントがIPsecを利用する必要がある場合は、IPsecの複数クライアント設定を使用することを推奨します。

タスク概要

ONTAPでは、IPsecを有効にした状態で、単一のSVM IPアドレスに複数のクライアントを多数のネットワーク経由で接続できます。そのためには、次のいずれかの方法を使用します。

- サブネット構成

特定のサブネット（例：192.168.134.0/24）上のすべてのクライアントが単一のSPDポリシーエントリを使用して単一のSVM IPアドレスに接続できるようにするには、`remote-ip-subnets`をサブネット形式で指定する必要があります。さらに、`remote-identity`フィールドに正しいクライアント側IDを指定する必要があります。



サブネット設定で単一のポリシー エントリを使用する場合、そのサブネット内のIPsecクライアントはIPsec IDと事前共有キー（PSK）を共有します。ただし、これは証明書認証には当てはまりません。証明書を使用する場合は、各クライアントはそれぞれ固有の証明書か共有の証明書のいずれかを認証に使用できます。ONTAPのIPsecは、証明書の有効性をローカルの信頼ストアにインストールされているCAに基づいてチェックします。証明書失効リスト（CRL）のチェックもサポートされています。

- すべてのクライアント構成を許可する

送信元 IP アドレスに関係なく、すべてのクライアントが SVM IPsec 対応 IP アドレスに接続できるようにするには、`remote-ip-subnets` フィールドを指定するときに `0.0.0.0/0` ワイルドカードを使用します。

さらに、正しいクライアント側IDを `remote-identity` フィールドに指定する必要があります。証明書認証の場合は、`ANYTHING` と入力できます。

また、`0.0.0.0/0` ワイルドカードを使用する場合は、使用するローカルまたはリモートのポート番号を具体的に設定する必要があります。例：`NFS port 2049`

手順

- 次のいずれかのコマンドを使用して、複数クライアント向けのIPsecを設定します。

- 複数の IPsec クライアントをサポートするために サブネット構成 を使用している場合：

```
security ipsec policy create -vserver vs1 -name policy_name
-local-ip-subnets IPsec_IP_address/32 -remote-ip-subnets
IP_address/subnet -local-identity local_id -remote-identity remote_id
```

コマンド例

```
security ipsec policy create -vserver vs1 -name subnet134 -local-ip-subnets
192.168.134.34/32 -remote-ip-subnets 192.168.134.0/24 -local-identity
ontap_side_identity -remote-identity client_side_identity
```

- 複数の IPsec クライアントをサポートするために すべてのクライアントを許可する構成 を使用している場合：

```
security ipsec policy create -vserver vs1 -name policy_name
-local-ip-subnets IPsec_IP_address/32 -remote-ip-subnets 0.0.0.0/0 -local
-ports port_number -local-identity local_id -remote-identity remote_id
```

コマンド例

```
security ipsec policy create -vserver vs1 -name test35 -local-ip-subnets
IPsec_IP_address/32 -remote-ip-subnets 0.0.0.0/0 -local-ports 2049 -local
-identity ontap_side_identity -remote-identity client_side_identity
```

IPSecの統計の表示

ネゴシエーションを通じて、ONTAP SVMのIPアドレスとクライアントのIPアドレスの間に、IKEセキュリティ アソシエーション（SA）と呼ばれるセキュリティ チャネルが確立されます。実際のデータの暗号化と復号化を実行するために、両方のエンドポイントにIPsec SAがインストールされます。統計コマンドを使用して、IPsec SAとIKE SAの両方のステータスを確認できます。



IPsec ハードウェア オフロード機能を使用している場合は、コマンド `security ipsec config show-ipsecsa` でいくつかの新しいカウンターが表示されます。

コマンド例

IKE SAのコマンドの例：

```
security ipsec show-ikesa -node hosting_node_name_for_svm_ip
```

IPsec SAのコマンドと出力の例：

```
security ipsec show-ipsecsa -node hosting_node_name_for_svm_ip
```

```
cluster1::> security ipsec show-ikesa -node cluster1-node1
```

| Vserver | Policy Name | Local Address | Remote Address | Initiator-SPI | State |
|---------|-------------|----------------|----------------|------------------|-------------|
| vs1 | test34 | 192.168.134.34 | 192.168.134.44 | c764f9ee020cec69 | ESTABLISHED |

IPsec SAのコマンドと出力の例：

```
security ipsec show-ipsecsa -node hosting_node_name_for_svm_ip
```

```
cluster1::> security ipsec show-ipsecsa -node cluster1-node1
```

| Vserver | Policy Name | Local Address | Remote Address | Inbound SPI | Outbound SPI | State |
|---------|-------------|----------------|----------------|-------------|--------------|-----------|
| vs1 | test34 | 192.168.134.34 | 192.168.134.44 | c4c5b3d6 | c2515559 | INSTALLED |

関連情報

- ["security certificate install"](#)
- ["セキュリティ IPsec"](#)

ONTAPバックエンド クラスタ ネットワーク暗号化を設定する

ONTAP 9.18.1以降では、バックエンドクラスタネットワーク上の転送データにトランスポート層セキュリティ（TLS）暗号化を設定できます。この暗号化により、バックエンドクラスタネットワーク上のONTAPノード間で転送されるONTAPに保存されている顧

客データが保護されます。

タスク概要

- バックエンド クラスタ ネットワークの暗号化は、デフォルトで無効になっています。
- バックエンド クラスタ ネットワークの暗号化を有効にすると、ONTAPに保存されているすべての顧客データは、バックエンド クラスタ ネットワーク上のONTAPノード間で送信される際に暗号化されます。制御パス データなど、一部のクラスタ ネットワーク トラフィックは暗号化されません。
- デフォルトでは、バックエンド クラスタのネットワーク暗号化では、クラスタ内の各ノードに対して自動生成された証明書が使用されます。[クラスター ネットワーク暗号化証明書を管理する](#)各ノードでカスタムインストールされた証明書を使用することもできます。

開始する前に

- 次のタスクを実行するには、`admin`権限レベルの ONTAP 管理者である必要があります。
- バックエンド クラスタ ネットワークの暗号化を有効にするには、クラスタ内のすべてのノードでONTAP 9.18.1以降が実行されている必要があります。

クラスター ネットワーク通信の暗号化を有効または無効にする

手順

1. 現在のクラスター ネットワーク暗号化ステータスを表示します：

```
security cluster-network show
```

このコマンドは、クラスター ネットワーク暗号化の現在のステータスを表示します：

```
Cluster-1::*> security cluster-network show

Enabled: true

Mode: tls

Status: READY
```

2. TLS バックエンド クラスタ ネットワーク暗号化を有効または無効にします：

```
security cluster-network modify -enabled <true|false>
```

このコマンドは、バックエンド クラスタ ネットワーク上の顧客転送中データの暗号化通信を有効または無効にします。

クラスター ネットワーク暗号化証明書を管理する

1. 現在のクラスター ネットワーク暗号化証明書情報を表示します：

```
security cluster-network certificate show
```

このコマンドは、現在のクラスター ネットワーク暗号化証明書情報を表示します：

```
security cluster-network certificate show
Node                                Certificate Name                                CA
-----
node1                               -                                                  Cluster-
1_Root_CA
node2                               -                                                  Cluster-
1_Root_CA
node3                               google_issued_cert1                             Google_CA1
node4                               google_issued_cert2                             Google_CA1
```

クラスター内の各ノードの証明書と認証局（CA）の名前が表示されます。

2. ノードのクラスター ネットワーク暗号化証明書を変更します：

```
security cluster-network certificate modify -node <node_name> -name
<certificate_name>
```

このコマンドは、特定のノードのクラスター ネットワーク暗号化証明書を変更します。このコマンドを実行する前に、証明書がインストールされ、インストール済みのCAによって署名されている必要があります。証明書管理の詳細については、"[System ManagerでONTAP証明書を管理する](#)"を参照してください。
'-name'が指定されていない場合は、自動生成されたデフォルトの証明書が使用されます。

ONTAPネットワーク内のLIFのファイアウォールポリシーを設定する

ファイアウォールの設定は、クラスターのセキュリティを強化し、ストレージシステムへの不正アクセスを防止するのに役立ちます。デフォルトでは、オンボード ファイアウォールは、データLIF、管理LIF、クラスター間LIFの特定のIPサービスに対するリモート アクセスを許可するように設定されています。

ONTAP 9.10.1以降：

- ファイアウォール ポリシーは廃止され、LIFサービス ポリシーに置き換えられました。以前は、オンボード ファイアウォールはファイアウォール ポリシーを使用して管理していました。今後はLIFサービス ポリシーを使用します。
- ファイアウォール ポリシーはすべて空であり、基盤となるファイアウォールでいずれのポートも開きません。代わりに、LIFのサービス ポリシーを使用してすべてのポートを開く必要があります。

- 9.10.1以降にアップグレードしたあとに、ファイアウォール ポリシーからLIFサービス ポリシーに移行するための操作は必要ありません。以前のリリースのONTAPで使用されていたファイアウォール ポリシーと整合性のあるLIFサービス ポリシーが自動的に構築されます。カスタム ファイアウォール ポリシーを作成および管理するスクリプトやその他のツールを使用している場合は、代わりにカスタム サービス ポリシーを作成するようにスクリプトのアップグレードが必要になることがあります。

詳細については、"[LIFとサービス ポリシー \(ONTAP 9.6以降\)](#)"を参照してください。

ファイアウォール ポリシーは、SSH、HTTP、HTTPS、Telnet、NTP、NDMP、NDMPS、RSH、DNS、SNMPなどの管理サービス プロトコルへのアクセスを制御するのに使用できます。NFSやSMBなどのデータ プロトコル用にファイアウォール ポリシーを設定することはできません。

ファイアウォール サービスとポリシーの管理には、次のような操作があります。

- ファイアウォール サービスを有効または無効にする
- 現在のファイアウォール サービスの設定を表示する
- ポリシー名とネットワーク サービスを指定して新しいファイアウォール ポリシーを作成する
- ファイアウォール ポリシーを論理インターフェイスに適用する
- 既存のファイアウォール ポリシーとまったく同一の新しいポリシーを作成する

この機能は、同じSVM内でよく似たポリシーを作成するときや、別のSVMにポリシーをコピーするときに使用できます。

- ファイアウォール ポリシーについての情報を表示する
- ファイアウォール ポリシーで使用するIPアドレスおよびネットマスクを変更する
- LIFで使用していないファイアウォール ポリシーを削除する

ファイアウォール ポリシーとLIF

LIFのファイアウォール ポリシーは、各LIFを介したクラスタへのアクセスを制限するために使用します。デフォルトのファイアウォール ポリシーが、各タイプのLIFを介したシステムへのアクセスにどのように影響し、LIFのセキュリティを調節するためにファイアウォール ポリシーをどのようにカスタマイズできるかを理解する必要があります。

```
`network interface create`または `network interface modify`  
コマンドを使用してLIFを設定する場合、`-firewall-  
policy`パラメータに指定された値によって、LIFへのアクセスが許可されるサービスプロトコル  
とIPアドレスが決まります。`network interface`  
の詳細については、link:https://docs.netapp.com/us-en/ontap-  
cli/search.html?q=network+interface["ONTAPコマンド リファレンス  
"]を参照してください。
```

ほとんどの場合、デフォルトのファイアウォール ポリシーの値をそのまま使用できますが、特定のIPアドレスや管理サービス プロトコルへのアクセスを制限しなければならない場合もあります。設定可能な管理サービス プロトコルは、SSH、HTTP、HTTPS、Telnet、NTP、NDMP、NDMPS、RSH、DNS、およびSNMPです。

すべてのクラスタ LIF のファイアウォール ポリシーはデフォルトで `""` に設定されており、変更できません。

次の表に、LIFの作成時にそのロール（ONTAP 9.5以前）またはサービス ポリシー（ONTAP 9.6以降）に基づいてLIFに割り当てられるデフォルトのファイアウォール ポリシーを示します。

| ファイアウォール ポリシー | デフォルトのサービス プロトコル | デフォルトのアクセス | 割り当て対象のLIF |
|---------------|--|---------------------|------------------------|
| mgmt | dns、http、https、ndmp、ndmps、ntp、snmp、ssh | 任意のアドレス (0.0.0.0/0) | クラスタ管理、SVM管理、ノード管理LIF |
| mgmt-nfs | dns、http、https、ndmp、ndmps、ntp、portmap、snmp、ssh | 任意のアドレス (0.0.0.0/0) | SVM管理アクセスもサポートするデータLIF |
| intercluster | https、ndmp、ndmps | 任意のアドレス (0.0.0.0/0) | すべてのインタークラスタLIF |
| data | dns、ndmp、ndmps、portmap | 任意のアドレス (0.0.0.0/0) | すべてのデータLIF |

portmapサービスの設定

portmapサービスは、RPCサービスをRPCサービスがリスンするポートにマップします。

portmapサービスはONTAP 9.3までは常にアクセス可能でしたが、ONTAP 9.4から設定対象となり、ONTAP 9.7からは自動で管理されるようになりました。

- ONTAP 9.3までは、サードパーティのファイアウォールではなく組み込みのONTAPファイアウォールを使用するネットワーク構成では、ポート111でportmapサービス（rpcbind）へのアクセスが常に許可されていました。
- ONTAP 9.4～ONTAP 9.6では、ファイアウォール ポリシーを変更してportmapサービスへのアクセスを許可するかどうかをLIFごとに制御できます。
- ONTAP 9.7以降ではportmapファイアウォール サービスは廃止され、代わりに、NFSサービスをサポートするすべてのLIFに対してportmapポートが自動的に開かれます。

Portmap サービスは、**ONTAP 9.4** から **ONTAP 9.6** のファイアウォールで設定できます。

ここからは、ONTAP 9.4～ONTAP 9.6リリースでportmapファイアウォール サービスを設定する方法について説明します。

構成に応じて、特定のタイプのLIF（管理LIFとクラスタ間LIFなど）にサービスへのアクセスを禁止することができます。状況によっては、データLIFからのアクセスも禁止できます。

想定される動作

ONTAP 9.4～ONTAP 9.6の動作は、アップグレード時にシームレスに移行できるように設計されています。portmapサービスにすでに特定のタイプのLIFからアクセスしている場合、それらのタイプのLIFからは引き続きサービスにアクセスできます。ONTAP 9.3以前と同様に、ファイアウォール内でアクセスを許可するサ

ービスをLIFのタイプ別のファイアウォール ポリシーで指定できます。

この動作を有効にするには、クラスタ内のすべてのノードでONTAP 9.4～ONTAP 9.6が実行されている必要があります。影響するのはインバウンド トラフィックのみです。

新しいルールは次のとおりです。

- リリース9.4～9.6にアップグレードすると、既存のすべてのファイアウォール ポリシー（デフォルトまたはカスタム）にportmapサービスが追加されます。
- 新しいクラスタやIPspaceを作成した場合、portmapサービスはデフォルトのデータ ポリシーにのみ追加され、デフォルトの管理ポリシーまたはクラスタ間ポリシーには追加されません。
- 必要に応じて、デフォルトまたはカスタムのポリシーにportmapサービスを追加したり削除したりできます。

portmapサービスを追加または削除する方法

SVMまたはクラスタのファイアウォール ポリシーにportmapサービスを追加する（ファイアウォール内でのアクセスを許可する）には、次のように入力します。

```
system services firewall policy create -vserver SVM -policy  
mgmt|intercluster|data|custom -service portmap
```

SVMまたはクラスタのファイアウォール ポリシーからportmapサービスを削除する（ファイアウォール内でのアクセスを禁止する）には、次のように入力します。

```
system services firewall policy delete -vserver SVM -policy  
mgmt|intercluster|data|custom -service portmap
```

network interface modifyコマンドを使用して、既存のLIFにファイアウォールポリシーを適用できます。この手順で説明するコマンドの詳細については、["ONTAPコマンド リファレンス"](#)を参照してください。

ファイアウォール ポリシーの作成とLIFへの割り当て

LIFを作成するときに、デフォルトのファイアウォール ポリシーが割り当てられます。多くの場合、ファイアウォールのデフォルト設定をそのまま使用でき、変更する必要はありません。ただし、LIFにアクセスできるネットワーク サービスやIPアドレスを変更したい場合は、カスタム ファイアウォール ポリシーを作成してLIFに割り当てます。

タスク概要

- policy`名前` `data intercluster cluster、または`mgmt`でファイアウォールポリシーを作成することはできません。

これらの値は、システム定義のファイアウォール ポリシー用に予約されています。

- クラスタLIFのファイアウォール ポリシーを設定したり変更したりすることはできません。

クラスタLIFのファイアウォール ポリシーは、どのサービス タイプでも0.0.0.0/0に設定されます。

- ポリシーからサービスを削除する必要がある場合は、既存のファイアウォール ポリシーを削除してから、新しいポリシーを作成する必要があります。
- クラスタでIPv6が有効になっている場合は、IPv6アドレスを指定してファイアウォール ポリシーを作成できます。

IPv6 を有効にすると、data、intercluster、および `mgmt` ファイアウォール ポリシーの受け入れ可能なアドレスのリストに IPv6 ワイルドカードである `::/0` が含まれるようになります。

- System Managerを使用してクラスタ全体のデータ保護機能を設定するときは、必ず、許可されるアドレスのリストにクラスタ間LIFのIPアドレスを含め、クラスタ間LIFと会社所有のファイアウォールの両方でHTTPSサービスを許可してください。

デフォルトでは、`intercluster` ファイアウォールポリシーはすべてのIPアドレス (0.0.0.0/0、またはIPv6の場合は`::/0`) からのアクセスを許可し、HTTPS、NDMP、およびNDMPサービスを実効にします。このデフォルトポリシーを変更する場合、またはクラスタ間LIF用に独自のファイアウォールポリシーを作成する場合は、各クラスタ間LIFのIPアドレスを許可リストに追加し、HTTPSサービスを有効にする必要があります。

- ONTAP 9.6以降では、HTTPSおよびSSHのファイアウォール サービスはサポートされていません。

ONTAP 9.6では、`management-https` および `management-ssh` LIFサービスは、HTTPSおよびSSH管理アクセスに使用できます。

手順

1. 特定のSVMのLIFで使用可能なファイアウォール ポリシーを作成します。

```
system services firewall policy create -vserver vservice_name -policy
policy_name -service network_service -allow-list ip_address/mask
```

ファイアウォール ポリシーに追加するネットワーク サービスごとに上記のコマンドを繰り返して、各サービスで許可されるIPアドレスを指定できます。

2. `system services firewall policy show` コマンドを使用して、ポリシーが正しく追加されたことを確認します。
3. ファイアウォール ポリシーをLIFに適用します。

```
network interface modify -vserver vservice_name -lif lif_name -firewall-policy
policy_name
```

4. `network interface show -fields firewall-policy` コマンドを使用して、ポリシーがLIFに正しく追加されたことを確認します。

`network interface show`の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/network-interface-show.html](https://docs.netapp.com/us-en/ontap-cli/network-interface-show.html)["ONTAPコマンド リファレンス"]を参照してください。

ファイアウォール ポリシーを作成してLIFに割り当てる例

次のコマンドは、10.10サブネットのIPアドレスからのHTTPおよびHTTPSプロトコルによるアクセスを許可するdata_httpというファイアウォール ポリシーを作成し、SVM vs1のdata1というLIFに適用してから、クラスタのすべてのファイアウォール ポリシーを表示します。

```
system services firewall policy create -vserver vs1 -policy data_http  
-service http - allow-list 10.10.0.0/16
```

```
system services firewall policy show
```

| Vserver | Policy | Service | Allowed |
|-----------|--------------|---------|--------------|
| ----- | ----- | ----- | ----- |
| cluster-1 | | | |
| | data | | |
| | | dns | 0.0.0.0/0 |
| | | ndmp | 0.0.0.0/0 |
| | | ndmps | 0.0.0.0/0 |
| cluster-1 | | | |
| | intercluster | | |
| | | https | 0.0.0.0/0 |
| | | ndmp | 0.0.0.0/0 |
| | | ndmps | 0.0.0.0/0 |
| cluster-1 | | | |
| | mgmt | | |
| | | dns | 0.0.0.0/0 |
| | | http | 0.0.0.0/0 |
| | | https | 0.0.0.0/0 |
| | | ndmp | 0.0.0.0/0 |
| | | ndmps | 0.0.0.0/0 |
| | | ntp | 0.0.0.0/0 |
| | | snmp | 0.0.0.0/0 |
| | | ssh | 0.0.0.0/0 |
| vs1 | | | |
| | data_http | | |
| | | http | 10.10.0.0/16 |
| | | https | 10.10.0.0/16 |

```
network interface modify -vserver vs1 -lif data1 -firewall-policy
data_http
```

```
network interface show -fields firewall-policy
```

| vserver | lif | firewall-policy |
|-----------|--------------|-----------------|
| ----- | ----- | ----- |
| Cluster | node1_clus_1 | |
| Cluster | node1_clus_2 | |
| Cluster | node2_clus_1 | |
| Cluster | node2_clus_2 | |
| cluster-1 | cluster_mgmt | mgmt |
| cluster-1 | node1_mgmt1 | mgmt |
| cluster-1 | node2_mgmt1 | mgmt |
| vs1 | data1 | data_http |
| vs3 | data2 | data |

ファイアウォール サービスとポリシーを管理するための ONTAP コマンド

`system services firewall` コマンドを使用してファイアウォール サービスを管理し、
`system services firewall policy` コマンドを使用してファイアウォール
ポリシーを管理し、`network interface modify` コマンドを使用して
LIFのファイアウォール設定を管理できます。

ONTAP 9.10.1以降：

- ファイアウォール ポリシーは廃止され、LIFサービス ポリシーに置き換えられました。以前は、オンボード ファイアウォールはファイアウォール ポリシーを使用して管理していました。今後はLIFサービス ポリシーを使用します。
- ファイアウォール ポリシーはすべて空であり、基盤となるファイアウォールでいずれのポートも開きません。代わりに、LIFのサービス ポリシーを使用してすべてのポートを開く必要があります。
- 9.10.1以降にアップグレードしたあとに、ファイアウォール ポリシーからLIFサービス ポリシーに移行するための操作は必要ありません。以前のリリースのONTAPで使用されていたファイアウォール ポリシーと整合性のあるLIFサービス ポリシーが自動的に構築されます。カスタム ファイアウォール ポリシーを作成および管理するスクリプトやその他のツールを使用している場合は、代わりにカスタム サービス ポリシーを作成するようにスクリプトのアップグレードが必要になることがあります。

詳細については、"[LIFとサービス ポリシー（ONTAP 9.6以降）](#)"を参照してください。

| 状況 | 使用するコマンド |
|--|---|
| ファイアウォール サービスを有効または無効にする | <code>system services firewall modify</code> |
| ファイアウォール サービスの現在の設定を表示する | <code>system services firewall show</code> |
| ファイアウォール ポリシーを作成する、または既存のファイアウォール ポリシーにサービスを追加する | <code>system services firewall policy create</code> |
| LIFにファイアウォール ポリシーを適用する | <code>network interface modify -lif lifname -firewall-policy</code> |
| ファイアウォール ポリシーに関連付けられたIPアドレスとネットマスクを変更する | <code>system services firewall policy modify</code> |
| ファイアウォール ポリシーに関する情報を表示する | <code>system services firewall policy show</code> |
| 既存のファイアウォール ポリシーとまったく同じ新しいポリシーを作成する | <code>system services firewall policy clone</code> |
| LIFで使用していないファイアウォール ポリシーを削除する | <code>system services firewall policy delete</code> |

関連情報

- ["システム サービス ファイアウォール"](#)
- ["network interface modify"](#)

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。