



# セキュリティトレースを使用したアクセスの 確認 ONTAP 9

NetApp  
April 24, 2024

# 目次

セキュリティトレースを使用したアクセスの確認 .....	1
セキュリティトレースの仕組み .....	1
アクセスのタイプによって、セキュリティトレースモニタがチェックされます .....	1
セキュリティトレースを作成する際の考慮事項 .....	2
セキュリティトレースを実行します .....	3
セキュリティトレースの結果を解釈する .....	11
追加情報の参照先 .....	12

# セキュリティトレースを使用したアクセスの確認

## セキュリティトレースの仕組み

パーミッショントレーシングフィルタを追加すると、Storage Virtual Machine（SVM）の SMB サーバおよび NFS サーバに対するクライアントまたはユーザによる処理要求が許可または拒否された理由が ONTAP で記録されるようになります。これは、ファイルアクセスのセキュリティ形式が適切であることを確認する場合や、ファイルアクセスに関する問題のトラブルシューティングを行う場合に役立ちます。

セキュリティトレースを使用すると、SVM 上での SMB および NFS 経由のクライアント処理を検出するフィルタを設定して、フィルタに一致するすべてのアクセスチェックをトレースできます。トレース結果には、アクセスが許可または拒否された理由がわかりやすくまとめられています。

SVM のファイルやフォルダに対する SMB / NFS アクセスのセキュリティ設定を確認する場合や、アクセスに関する問題がある場合は、パーミッショントレーシングを有効にするフィルタを短時間で追加できます。

次のリストに、セキュリティトレースの仕組みに関する重要な特性を示します。

- ONTAP は、セキュリティトレースを SVM レベルで適用します。
- 各受信要求がスクリーニングされ、有効になっているセキュリティトレースのフィルタ条件に一致するかどうかを確認されます。
- トレースは、ファイルとフォルダの両方のアクセス要求に対して実行されます。
- トレースでは、次の条件に基づいてフィルタリングできます。
  - クライアント IP
  - SMB または NFS パス
  - Windows 名
  - UNIX 名
- 要求は、\_allowed\_or\_Denied\_access 応答結果でスクリーニングされます。
- 有効なトレースのフィルタ条件に一致する各要求が、トレース結果ログに記録されます。
- ストレージ管理者は、フィルタが自動的に無効になるようにタイムアウトを設定できます。
- 要求が複数のフィルタに一致する場合は、インデックス番号が最も大きいフィルタの結果が記録されます。
- ストレージ管理者は、トレース結果ログを出力し、アクセス要求が許可または拒否された理由を確認できます。

## アクセスのタイプによって、セキュリティトレースモニタがチェックされます

ファイルやフォルダに対するアクセスチェックは、複数の条件に基づいて行われます。これらすべての基準について、セキュリティトレースで操作を監視できます。

セキュリティトレースで監視されるアクセスチェックの種類は次のとおりです。

- ボリュームと qtree のセキュリティ形式
- 処理が要求されるファイルやフォルダを含むファイルシステムの効果的なセキュリティ
- ユーザマッピング
- 共有レベルの権限
- エクスポートレベルの権限
- ファイルレベルの権限
- ストレージレベルのアクセス保護セキュリティ

## セキュリティトレースを作成する際の考慮事項

Storage Virtual Machine（SVM）でセキュリティトレースを作成する場合は、以下の考慮事項に注意する必要があります。たとえば、トレースを作成できるプロトコル、サポートされるセキュリティ形式、アクティブなトレースの最大数を把握しておく必要があります。

- セキュリティトレースは SVM 上でしか作成できません。
- セキュリティトレースフィルタの各エントリは SVM 固有です。

トレースを実行する SVM を指定する必要があります。

- パーミッショントレーシングフィルタは SMB 要求と NFS 要求についてのみ追加できます。
- トレースフィルタを作成する SVM 上に SMB サーバまたは NFS サーバをセットアップする必要があります。
- NTFS、UNIX、mixed セキュリティ形式のボリュームおよび qtree 上に存在するファイルやフォルダに対してセキュリティトレースを作成できます。
- パーミッショントレーシングフィルタは SVM ごとに 10 個まで追加できます。
- フィルタを作成または変更するときは、フィルタインデックス番号を指定する必要があります。

フィルタはインデックス番号順に処理されます。インデックス番号の大きいフィルタの条件は、インデックス番号の小さい条件よりも先に処理されます。トレースされている要求が、複数の有効なフィルタの条件に一致する場合は、インデックス番号が最も大きいフィルタだけがトリガーされます。

- セキュリティトレースフィルタを作成して有効にしたあと、トレースフィルタでキャプチャしてトレース結果ログに記録できるアクティビティを生成するために、クライアントシステムでファイル要求またはフォルダ要求をいくつか実行する必要があります。
- ファイルアクセスの検証またはトラブルシューティングの目的でのみ、パーミッショントレーシングフィルタを追加してください。

パーミッショントレーシングフィルタを追加すると、コントローラのパフォーマンスが若干低下します。

検証またはトラブルシューティングが完了したら、すべてのパーミッショントレーシングフィルタを無効にするか、削除する必要があります。さらに ONTAP、ログに大量のトレース結果が送信されないように、できるだけ具体的なフィルタ条件を指定する必要があります。

# セキュリティトレースを実行します

## セキュリティトレースの概要を実行します

セキュリティトレースの実行では、セキュリティトレースフィルタの作成、フィルタ条件の確認、フィルタ条件に一致する SMB クライアントまたは NFS クライアントへのアクセス要求の生成、トレース結果の表示などを行います。

セキュリティフィルタを使用してトレース情報をキャプチャしたあと、フィルタを変更して再利用するか、不要になった場合は無効にすることができます。フィルタトレース結果を表示および分析したあと、その結果が不要になった場合は削除できます。

## セキュリティトレースフィルタを作成します

Storage Virtual Machine（SVM）で SMB および NFS のクライアント処理を検出し、フィルタに一致するすべてのアクセスチェックをトレースするセキュリティトレースフィルタを作成できます。セキュリティトレースの結果を使用して、構成の検証や、アクセスに関する問題のトラブルシューティングを行うことができます。

このタスクについて

vserver security trace filter create コマンドには 2 つの必須パラメータがあります。

必須パラメータ	説明
-vserver vserver_name	SVM 名 _  セキュリティトレースフィルタを適用するファイルやフォルダが格納されている SVM の名前。
-index index_number	フィルタインデックス番号 _  フィルタに適用するインデックス番号。トレースフィルタは SVM ごとに 10 個まで使用できます。このパラメータに指定できる値は 1~10 です。

さまざまなオプションのフィルタパラメータでセキュリティトレースフィルタをカスタマイズして、セキュリティトレースによって生成された結果を絞り込むことができます。

フィルタパラメータ	説明
-client-ip IP_Address	IP アドレスを指定します。この IP アドレスから SVM にアクセスしているユーザが対象となります。

<code>-path path</code>	<p>パーミッショントレースフィルタを適用するパスを指定します。の値 <code>-path</code> 次のいずれかの形式を使用できます。</p> <ul style="list-style-type: none"> <li>共有またはエクスポートのルートから始まる完全なパス</li> <li>共有のルートに対する相対パス</li> </ul> <p>パス値では、NFS 形式のディレクトリ UNIX 形式のディレクトリ区切り文字を使用する必要があります。</p>
<code>-windows-name win_user_name</code> または <code>-unix</code> <code>-name ``unix_user_name</code>	<p>アクセス要求をトレースする対象の Windows ユーザ名または UNIX ユーザ名を指定できます。ユーザ名変数では大文字と小文字は区別されません。同じフィルタで Windows ユーザ名と UNIX ユーザ名の両方を指定することはできません。</p> <div>  <p>トレースできるのは SMB と NFS のアクセスイベントですが、mixed セキュリティ形式または UNIX セキュリティ形式のデータに対してアクセスチェックを実行するときに、マッピングされた UNIX ユーザおよび UNIX グループが使用されることがあります。</p> </div>
<code>-trace-allow {yes</code>	<code>no}</code>
<p>セキュリティトレースフィルタでは、拒否イベントのトレースは常に有効です。必要に応じて、許可イベントをトレースすることもできます。許可イベントをトレースするには、このパラメータをに設定します <code>yes</code>。</p>	<code>-enabled {enabled</code>
<code>disabled}</code>	<p>セキュリティトレースフィルタを有効または無効にすることができます。デフォルトでは、セキュリティトレースフィルタは有効になっています。</p>
<code>-time-enabled integer</code>	<p>フィルタのタイムアウトを指定できます。指定した時間が経過すると、フィルタは無効になります。</p>

## 手順

1. セキュリティトレースフィルタを作成します。

```
vserver security trace filter create -vserver vserver_name -index
index_numberfilter_parameters
```

`filter_parameters` は、オプションのフィルタパラメータのリストです。

詳細については、コマンドのマニュアルページを参照してください。

2. セキュリティトレースフィルタのエントリを確認します。

```
vserver security trace filter show -vserver vserver_name -index index_number
```

#### 例

次のコマンドは、共有パスのファイルにアクセスするすべてのユーザを対象とするセキュリティトレースフィルタを作成します \\server\share1\dir1\dir2\file.txt IPアドレス10.10.10.7から。フィルタはに完全なパスを使用します -path オプションデータへのアクセスに使用されるクライアントの IP アドレスは 10.10.10.7 です。フィルタは 30 分後にタイムアウトします。

```
cluster1::> vserver security trace filter create -vserver vs1 -index 1
-path /dir1/dir2/file.txt -time-enabled 30 -client-ip 10.10.10.7
cluster1::> vserver security trace filter show -index 1
```

Vserver	Index	Client-IP	Path	Trace-Allow	Windows-Name
vs1	1	10.10.10.7	/dir1/dir2/file.txt	no	-

次のコマンドは、の相対パスを使用してセキュリティトレースフィルタを作成します -path オプションこのフィルタは、「joe」という名前の Windows ユーザのアクセスをトレースします。Joeは共有パスのファイルにアクセスしています \\server\share1\dir1\dir2\file.txt。許可イベントと拒否イベントをトレースします。

```
cluster1::> vserver security trace filter create -vserver vs1 -index 2
-path /dir1/dir2/file.txt -trace-allow yes -windows-name mydomain\joe

cluster1::> vserver security trace filter show -vserver vs1 -index 2
```

```

Vserver: vs1
Filter Index: 2
Client IP Address to Match: -
Path: /dir1/dir2/file.txt
Windows User Name: mydomain\joe
UNIX User Name: -
Trace Allow Events: yes
Filter Enabled: enabled
Minutes Filter is Enabled: 60
```

#### セキュリティトレースフィルタに関する情報を表示します

Storage Virtual Machine（SVM）で設定されているセキュリティトレースフィルタに関する情報を表示できます。これにより、各フィルタがトレースするアクセスイベントのタイプを確認できます。

#### ステップ

1. を使用して、セキュリティトレースフィルタエントリに関する情報を表示します vserver security

trace filter show コマンドを実行します

このコマンドの使用の詳細については、マニュアルページを参照してください。

#### 例

次のコマンドを実行すると、SVM vs1 のすべてのセキュリティトレースフィルタに関する情報が表示されます。

```
cluster1::> vserver security trace filter show -vserver vs1
Vserver  Index  Client-IP          Path                Trace-Allow
Windows-Name
-----
vs1      1      -                /dir1/dir2/file.txt    yes      -
vs1      2      -                /dir3/dir4/            no
mydomain\joe
```

## セキュリティトレースの結果を表示します

セキュリティトレースフィルタに一致するファイル操作に対して生成されたセキュリティトレースの結果を表示できます。この結果を使用して、ファイルアクセスセキュリティ設定の検証や、SMB および NFS のファイルアクセスに関する問題のトラブルシューティングを行うことができます。

#### 必要なもの

有効なセキュリティトレースフィルタが存在している必要があり、セキュリティトレースの結果が生成されるように、セキュリティトレースフィルタに一致する SMB クライアントまたは NFS クライアントから操作が実行されている必要があります。

#### このタスクについて

すべてのセキュリティトレースの結果の概要を表示することも、オプションのパラメータを指定して、出力に表示される情報をカスタマイズすることもできます。これは、多数のレコードがセキュリティトレースの結果に含まれている場合に便利です。

オプションのパラメータを何も指定しない場合、次の情報が表示されます。

- Storage Virtual Machine （SVM）名
- ノード名
- セキュリティトレースのインデックス番号
- セキュリティ形式
- パス
- 理由
- ユーザ名



トレースフィルタの設定に応じて、ユーザ名が表示されます。

フィルタの設定方法	作業
UNIX ユーザ名を使用する場合	UNIX ユーザ名が表示されます。
Windows ユーザ名を使用	Windows ユーザ名が表示されます。
ユーザ名を使用しない	Windows ユーザ名が表示されます。

オプションのパラメータを使用して、出力をカスタマイズできます。コマンド出力で返される結果を絞り込むために使用できるオプションのパラメータには、次のようなものがあります。

オプションのパラメータ	説明
<code>-fields field_name</code> はい。	選択したフィールドの出力を表示します。このパラメータは、単独で使用することも、他のオプションのパラメータと組み合わせて使用することもできます。
<code>-instance</code>	セキュリティトレースイベントに関する詳細情報を表示します。このパラメータを他のオプションのパラメータとともに使用して、特定のフィルタ結果に関する詳細情報を表示します。
<code>-node node_name</code>	指定したノード上のイベントに関する情報のみを表示します。
<code>-vserver vservice_name</code>	指定した SVM 上のイベントに関する情報のみを表示します。
<code>-index integer</code>	指定したインデックス番号に対応するフィルタの結果として発生したイベントに関する情報を表示します。
<code>-client-ip IP_address</code>	指定したクライアント IP アドレスからのファイルアクセスの結果として発生したイベントに関する情報を表示します。
<code>-path path</code>	指定したパスへのファイルアクセスの結果として発生したイベントに関する情報を表示します。
<code>-user-name user_name</code>	指定した Windows ユーザまたは UNIX ユーザによるファイルアクセスの結果として発生したイベントに関する情報を表示します。
<code>-security-style security_style</code>	指定したセキュリティ形式のファイルシステムで発生したイベントに関する情報を表示します。

コマンドで使用できる他のオプションのパラメータについては、マニュアルページを参照してください。

## ステップ

1. を使用して、セキュリティトレースフィルタの結果を表示します `vserver security trace trace-`

result show コマンドを実行します

```
vserver security trace trace-result show -user-name domain\user
```

Vserver: vs1

Node	Index	Filter Details	Reason
node1	3	User:domain\user Security Style:mixed Path:/dir1/dir2/	Access denied by explicit ACE
node1	5	User:domain\user Security Style:unix Path:/dir1/	Access denied by explicit ACE

## セキュリティトレースフィルタを変更する

トレースされたアクセスイベントを特定する際に使用するオプションのフィルタパラメータを変更するには、既存のセキュリティトレースフィルタを変更します。

このタスクについて

変更するセキュリティトレースフィルタを特定するには、フィルタを適用した Storage Virtual Machine （SVM）の名前とフィルタのインデックス番号を指定します。オプションのフィルタパラメータはすべて変更できます。

手順

1. セキュリティトレースフィルタを変更します。

```
vserver security trace filter modify -vserver vserver_name -index  
index_numberfilter_parameters
```

- ° vserver\_name は、セキュリティトレースフィルタを適用するSVMの名前です。
- ° index\_number は、フィルタに適用するインデックス番号です。このパラメータに指定できる値は 1~10 です。
- ° filter\_parameters は、オプションのフィルタパラメータのリストです。

2. セキュリティトレースフィルタのエントリを確認します。

```
vserver security trace filter show -vserver vserver_name -index index_number
```

例

次の例は、インデックス番号 1 のセキュリティトレースフィルタを変更します。このフィルタは、共有パスのファイルにアクセスしているすべてのユーザのイベントをトレースします

\\server\share1\dir1\dir2\file.txt 任意のIPアドレスから。フィルタはに完全なパスを使用します  
-path オプション許可イベントと拒否イベントをトレースします。

```
cluster1::> vsserver security trace filter modify -vsserver vs1 -index 1
-path /dir1/dir2/file.txt -trace-allow yes

cluster1::> vsserver security trace filter show -vsserver vs1 -index 1
Vserver: vs1
Filter Index: 1
Client IP Address to Match: -
Path: /dir1/dir2/file.txt
Windows User Name: -
UNIX User Name: -
Trace Allow Events: yes
Filter Enabled: enabled
Minutes Filter is Enabled: 60
```

## セキュリティトレースフィルタを削除します

セキュリティトレースフィルタエントリが不要になった場合は削除できます。セキュリティトレースフィルタは Storage Virtual Machine（SVM）ごとに 10 個までしか使用できないので、上限に達した場合は、不要なフィルタを削除すると、新しいフィルタを作成できます。

このタスクについて

削除するセキュリティトレースフィルタを一意に識別するには、次の項目を指定する必要があります。

- トレースフィルタが適用されている SVM の名前
- トレースフィルタのフィルタインデックス番号

手順

1. 削除するセキュリティトレースフィルタエントリのフィルタインデックス番号を確認します。

```
vsserver security trace filter show -vsserver vsserver_name
```

```
vsserver security trace filter show -vsserver vs1
```

Vserver	Index	Client-IP	Path	Trace-Allow	Windows-Name
-----	-----	-----	-----	-----	-----
vs1	1	-	/dir1/dir2/file.txt	yes	-
vs1	2	-	/dir3/dir4/	no	
mydomain\joe					

2. 前の手順で確認したフィルタインデックス番号を使用して、フィルタエントリを削除します。

```
vserver security trace filter delete -vserver vserver_name -index index_number
```

```
vserver security trace filter delete -vserver vs1 -index 1
```

### 3. セキュリティトレースフィルタエントリが削除されたことを確認します。

```
vserver security trace filter show -vserver vserver_name
```

```
vserver security trace filter show -vserver vs1
```

Vserver	Index	Client-IP	Path	Trace-Allow
Windows-Name				
-----	-----	-----	-----	-----
vs1	2	-	/dir3/dir4/	no
mydomain\joe				

## セキュリティトレースレコードを削除します

セキュリティトレースレコードを使用したファイルアクセスセキュリティの検証や、SMB または NFS のクライアントアクセスに関する問題のトラブルシューティングが完了したら、セキュリティトレースのログからセキュリティトレースレコードを削除できます。

このタスクについて

セキュリティトレースレコードを削除する前に、レコードのシーケンス番号を確認しておく必要があります。



各 Storage Virtual Machine (SVM) には、最大 128 件のトレースレコードを保存できます。SVM でこの上限に達した場合、最も古いトレースレコードが自動的に削除されて、新しいレコードが追加されます。したがって、SVM のトレースレコードを手動で削除しなくても、上限に達したときに、ONTAP によって自動的に最も古いトレース結果を削除して新しい結果用のスペースを確保することができます。

### 手順

#### 1. 削除するレコードのシーケンス番号を指定します。

```
vserver security trace trace-result show -vserver vserver_name -instance
```

#### 2. セキュリティトレースレコードを削除します。

```
vserver security trace trace-result delete -node node_name -vserver  
vserver_name -seqnum integer
```

```
vserver security trace trace-result delete -vserver vs1 -node node1 -seqnum  
999
```

° -node node\_name は、削除するパーミッショントレーシングイベントが発生したクラスタノードの

名前です。

これは必須パラメータです。

- ° `-vserver vservice_name` は、削除対象のパーミッショントレーシングイベントが発生したSVMの名前です。

これは必須パラメータです。

- ° `-seqnum integer` は、削除するログイベントのシーケンス番号です。

これは必須パラメータです。

## すべてのセキュリティトレースレコードを削除します

既存のセキュリティトレースレコードが不要である場合は、1つのコマンドで特定のノード上のレコードをすべて削除できます。

### ステップ

1. すべてのセキュリティトレースレコードを削除します。

```
vserver security trace trace-result delete -node node_name -vserver vservice_name *
```

- ° `-node node_name` は、削除するパーミッショントレーシングイベントが発生したクラスタノードの名前です。
- ° `-vserver vservice_name` は、削除するパーミッショントレーシングイベントが発生したStorage Virtual Machine (SVM) の名前です。

## セキュリティトレースの結果を解釈する

セキュリティトレースの結果には、要求が許可または拒否された理由が示されます。出力には、アクセスが許可または拒否された理由と、アクセスが許可または拒否されたアクセスチェック経路内の場所を組み合わせた結果が表示されます。この結果を使用して、アクションが許可された理由または許可されなかった理由を特定できます。

### 結果タイプとフィルタの詳細のリストに関する情報を検索する

セキュリティトレースの結果に表示できる結果タイプとフィルタの詳細のリストは、のマニュアルページで確認できます `vserver security trace trace-result show` コマンドを実行します

の出力例を示します Reason のフィールド Allow 結果タイプ

次に、の出力例を示します Reason のトレース結果ログに表示されるフィールド Allow 結果タイプ：

```
Access is allowed because SMB implicit permission grants requested  
access while opening existing file or directory.
```

```
Access is allowed because NFS implicit permission grants requested
access while opening existing file or directory.
```

の出力例を示します Reason のフィールド Allow 結果タイプ

次に、の出力例を示します Reason のトレース結果ログに表示されるフィールド Deny 結果タイプ：

```
Access is denied. The requested permissions are not granted by the
ACE while checking for child-delete access on the parent.
```

の出力例を示します Filter details フィールド

次に、の出力例を示します Filter details トレース結果ログのフィールド。フィルタ条件に一致するファイルやフォルダが格納されているファイルシステムの有効なセキュリティ形式が表示されます。

```
Security Style: MIXED and ACL
```

## 追加情報の参照先

SMBクライアントアクセスをテストしたあと、SMBの高度な設定を行ったり、SANアクセスを追加したりできます。NFSクライアントアクセスをテストしたあと、NFSの高度な設定を行ったり、SANアクセスを追加したりできます。プロトコルアクセスが完了したら、SVMのルートボリュームを保護する必要があります。

### SMBの設定

SMBアクセスについてさらに詳しく設定するには、次のコマンドを使用します。

- ["SMBの管理"](#)

SMBプロトコルを使用したファイルアクセスを設定および管理する方法について説明します。

- ["ネットアップテクニカルレポート 4191：『Best Practices Guide for clustered Data ONTAP 8.2 Windows File Services』"](#)

SMBの導入やその他のWindowsファイルサービスの機能の概要に加え、ONTAPに関する推奨事項や基本的なトラブルシューティング情報を紹介しています。

- ["ネットアップテクニカルレポート 3740：『SMB 2 Next-Generation CIFS Protocol in Data ONTAP』"](#)

SMB 2の機能について、設定に関する詳細やONTAPでの実装に関する情報を紹介しています。

### NFS構成

NFSアクセスについてさらに詳しく設定するには、以下を使用します。

- ["NFS の管理"](#)

NFS プロトコルを使用したファイルアクセスを設定および管理する方法について説明しています。

- ["ネットアップテクニカルレポート 4067 : 『 NFS Best Practice and Implementation Guide 』 "](#)

NFSv3 および NFSv4 の運用ガイドであり、 NFSv4 を中心に ONTAP オペレーティングシステムの概要を説明しています。

- ["ネットアップテクニカルレポート 4668 : 『 Name Services Best Practices Guide 』 "](#)

LDAP、NIS、DNS、およびローカルユーザ / グループファイルを認証用に設定する際の、ベストプラクティス、制限、推奨事項、および考慮事項をまとめています。

- ["ネットアップテクニカルレポート 4616 : 『 NFS Kerberos in ONTAP with Microsoft Active Directory 』 "](#)

- ["ネットアップテクニカルレポート 4835 : 『 How to Configure LDAP in ONTAP 』 "](#)

- ["ネットアップテクニカルレポート 3580 : 『 NFSv4 の拡張内容とベスト・プラクティス・ガイド - Data ONTAP での実装』 "](#)

ONTAP を実行するシステムに接続された AIX、Linux、または Solaris クライアントに NFSv4 のコンポーネントを実装する際のベストプラクティスを紹介しています。

## ルートボリュームの保護

SVM でプロトコルを設定したら、ルートボリュームを保護してください。

- ["データ保護"](#)

負荷共有ミラーを作成して SVM ルートボリュームを保護する方法について説明しています。これは、NAS 対応の SVM に対するネットアップのベストプラクティスです。また、SVM ルートボリュームを負荷共有ミラーから昇格させてボリュームの障害や消失からリカバリする簡単な方法についても説明しています。

## 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。