



# ファイル権限を使用したファイル アクセスの保護

## ONTAP 9

NetApp  
February 12, 2026

# 目次

ファイル権限を使用したファイル アクセスの保護.....	1
ONTAP SMB SVMのWindowsセキュリティタブを使用して、高度なNTFSファイル権限を設定します。 ..	1
SMB NTFSファイル権限用のONTAPコマンド .....	4
ONTAP SMBサーバ経由でファイルにアクセスする際のアクセス制御を提供する	
UNIXファイル権限について学習します.....	4

# ファイル権限を使用したファイル アクセスの保護

## ONTAP SMB SVMのWindowsセキュリティタブを使用して、高度なNTFSファイル権限を設定します。

Windows のプロパティ ウィンドウの **Windows** セキュリティ タブを使用して、ファイルとフォルダに対する標準の NTFS ファイル権限を設定できます。

開始する前に

このタスクを実行する管理者は、選択したオブジェクトに対する権限を変更するための十分なNTFS権限を持っている必要があります。

タスク概要

NTFSファイル権限を設定するには、Windowsホストで、NTFSセキュリティ記述子に関連付けられているNTFS随意アクセス制御リスト (DACL) にエントリを追加します。その後、セキュリティ記述子をNTFSファイルおよびディレクトリに適用します。これらのタスクはWindows GUIによって自動的に処理されます。

手順

1. エクスプローラの ツール メニューから、ネットワーク ドライブの割り当て を選択します。
2. ネットワーク ドライブの割り当て ダイアログ ボックスを完了します：
  - a. \*ドライブ\*文字を選択します。
  - b. フォルダー ボックスに、権限を適用するデータが含まれている共有を含む CIFS サーバー名と共有の名前を入力します。

CIFS サーバー名が「CIFS\_SERVER」で、共有名が「share1」の場合は、「\\CIFS\_SERVER\share1」と入力する必要があります。



CIFSサーバ名の代わりに、CIFSサーバのデータ インターフェイスのIPアドレスを指定することもできます。

- c. \*完了\*をクリックします。

選択したドライブがマウントされて使用可能な状態となり、共有内に格納されているファイルやフォルダがWindowsエクスプローラ ウィンドウに表示されます。

3. NTFSファイル権限を設定するファイルまたはディレクトリを選択します。
4. ファイルまたはディレクトリを右クリックし、\*プロパティ\*を選択します。
5. \*セキュリティ\*タブを選択します。

\*Security\*タブには、NTFS権限が設定されているユーザーとグループのリストが表示されます。\*Permissions for\*ボックスには、選択したユーザーまたはグループごとに有効な「許可」と「拒否」の権限のリストが表示されます。

6. \*Advanced\*をクリックします。

Windowsの[プロパティ]ウィンドウに、ユーザおよびグループに割り当てられている既存のファイル権限

に関する情報が表示されます。

7. \*権限の変更\*をクリックします。

[アクセス許可]ウィンドウが開きます。

8. 次のうち必要な操作を実行します。

状況	操作
新しいユーザまたはグループの詳細なNTFS権限を設定する	a. *[追加]*をクリックします。 b. *選択するオブジェクト名を入力*ボックスに、追加するユーザーまたはグループの名前を入力します。 c. *OK*をクリックします。
ユーザまたはグループの詳細なNTFS権限を変更する	a. 権限エントリ： ボックスで、詳細な権限を変更するユーザーまたはグループを選択します。 b. *編集*をクリックします。
ユーザまたはグループの詳細なNTFS権限を削除する	a. [アクセス許可エントリ：] ボックスで、削除するユーザーまたはグループを選択します。 b. *削除*をクリックします。 c. 手順13に進みます。

新しいユーザーまたはグループに高度な NTFS アクセス許可を追加する場合、または既存のユーザーまたはグループの NTFS 高度なアクセス許可を変更する場合は、<Object>のアクセス許可エントリボックスが開きます。

9. 適用先 ボックスで、この NTFS ファイル権限エントリを適用する方法を選択します。

単一のファイルにNTFSファイル権限を設定する場合、\*適用先\*ボックスはアクティブになりません。\*適用先\*設定はデフォルトで\*このオブジェクトのみ\*に設定されます。

10. 権限 ボックスで、このオブジェクトに設定する詳細な権限の 許可 または 拒否 ボックスを選択します。

- 指定されたアクセスを許可するには、\*許可\*ボックスを選択します。
- 指定したアクセスを許可しない場合は、\*拒否\*ボックスを選択します。次の高度な権限に対してアクセス権を設定できます：
- フルコントロール

この詳細な権限を選択すると、他のすべての詳細な権限が自動的に選択されます（それらの権限が許可または拒否されます）。

- フォルダをトラバース / ファイルを実行
- フォルダの一覧表示 / データの読み取り
- 属性の読み取り

- 拡張属性の読み取り
- ファイルの作成 / データの書き込み
- フォルダの作成 / データの追加
- 属性を書き込む
- 拡張属性を書き込む
- サブフォルダとファイルを削除する
- 削除
- 読み取り権限
- 権限の変更
- 責任を取る



いずれかの詳細な権限ボックスが選択可能になっていない場合、その権限は親オブジェクトから継承されます。

11. このオブジェクトのサブフォルダーとファイルにこれらの権限を継承する場合は、\*これらの権限をこのコンテナ内のオブジェクトおよび/またはコンテナにのみ適用する\*ボックスを選択します。
12. \*OK\*をクリックします。
13. NTFS権限の追加、削除、または編集が完了したら、このオブジェクトの継承設定を指定します。

- \*このオブジェクトの親からの継承可能なアクセス許可を含める\*ボックスを選択します。

これがデフォルトです。

- \*すべての子オブジェクトのアクセス許可を、このオブジェクトからの継承可能なアクセス許可に置き換える\*ボックスを選択します。

単一ファイルに対してNTFSファイル権限を設定する場合、この設定は[アクセス許可]ボックスに表示されません。



この設定を選択する場合は注意が必要です。この設定を選択すると、すべての子オブジェクトの既存の権限がすべて削除され、このオブジェクトの権限の設定に置き換えられます。削除するつもりがなかった権限が誤って削除される可能性があります。これは、mixedセキュリティ形式のボリュームまたはqtreeで権限を設定する場合に特に重要です。子オブジェクトがUNIX対応のセキュリティ形式を使用している場合に、このような子オブジェクトにNTFS権限を適用すると、ONTAPによってこれらのオブジェクトがUNIXセキュリティ形式からNTFSセキュリティ形式に変更され、これらの子オブジェクトのすべてのUNIX権限がNTFS権限に置き換えられます。

- 両方のボックスを選択します。
- どちらのボックスも選択しないでください。

14. **OK** をクリックして **Permissions** ボックスを閉じます。
15. **[OK]** をクリックして、**<Object>** の高度なセキュリティ設定 ボックスを閉じます。

詳細なNTFS権限の設定方法の詳細については、Windowsのマニュアルを参照してください。

## 関連情報

- [サーバーに NTFS セキュリティ記述子を作成する](#)
- [NTFSセキュリティ形式のボリュームのファイルセキュリティに関する情報の表示](#)
- [mixedセキュリティ形式のボリュームのファイルセキュリティに関する情報の表示](#)
- [UNIXセキュリティ形式のボリュームのファイルセキュリティに関する情報の表示](#)

## SMB NTFSファイル権限用のONTAPコマンド

ONTAP CLIを使用して、ファイルおよびディレクトリに対してNTFSファイル権限を設定できます。これにより、WindowsクライアントでSMB共有を使用してデータに接続することなくNTFSファイル権限を設定できます。

NTFSファイル権限を設定するには、NTFSセキュリティ記述子に関連付けられているNTFS随意アクセス制御リスト (DACL) にエントリを追加します。その後、セキュリティ記述子をNTFSファイルおよびディレクトリに適用します。

コマンドラインで設定できるのはNTFSファイル権限だけです。CLIでNFSv4 ACLを設定することはできません。

### 手順

1. NTFSセキュリティ記述子を作成します。

```
vserver security file-directory ntfs create -vserver svm_name -ntfs-sd ntfs_security_descriptor_name -owner owner_name -group primary_group_name -control-flags-raw raw_control_flags
```

2. NTFSセキュリティ記述子にDACLを追加します。

```
vserver security file-directory ntfs dacl add -vserver svm_name -ntfs-sd ntfs_security_descriptor_name -access-type {deny|allow} -account account_name -rights {no-access|full-control|modify|read-and-execute|read|write} -apply-to {this-folder|sub-folders|files}
```

3. ファイル/ディレクトリのセキュリティ ポリシーを作成します。

```
vserver security file-directory policy create -vserver svm_name -policy-name policy_name
```

## ONTAP SMBサーバ経由でファイルにアクセスする際のアクセス制御を提供するUNIXファイル権限について学習します

FlexVol volumeには、NTFS、UNIX、または混合の3つのタイプのセキュリティスタイルがあります。セキュリティスタイルに関係なくSMB経由でデータにアクセスできますが、UNIX有効セキュリティでデータにアクセスするには適切なUNIXファイル権限が必要です。

SMB 経由でデータにアクセスする場合、要求されたアクションを実行する権限がユーザーに与えられているかどうかを判断する際に、いくつかのアクセス制御が使用されます：

- エクスポート権限

SMB アクセスのエクスポート権限の設定はオプションです。

- 共有権限
- ファイル権限

ユーザーがアクションを実行するデータには、次の種類のファイル権限が適用される場合があります：

- NTFS
- UNIX NFSv4 ACL
- UNIXモードビット

NFSv4 ACLまたはUNIXモードビットが設定されているデータの場合、データへのファイルアクセス権はUNIX形式の権限によって決定されます。SVM管理者は、ユーザーが必要なアクションを実行する権限を持つように、適切なファイル権限を設定する必要があります。



混合セキュリティ形式のボリューム内のデータは、NTFSまたはUNIX実効セキュリティ形式のいずれかになります。データがUNIX実効セキュリティ形式の場合、データへのファイルアクセス権を決定する際にNFSv4権限またはUNIXモードビットが使用されます。

## 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。