# 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

## 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。<br>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。<br>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。<br>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。<br>b. *削除*をクリックします。<br>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ー内のオブジェクトおよび/またはコンテナーにのみ適用する*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。削除するつもりの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



## 商標に関する情報