



# UNIXセキュリティ形式のデータに対するファイルセキュリティのSMBクライアントへの提供方法を管理します。

ONTAP 9

NetApp  
December 20, 2024

# 目次

UNIXセキュリティ形式のデータに対するファイルセキュリティの SMBクライアントへの提供方法を管理します。 .....	1
UNIXセキュリティ形式のデータに関してファイルセキュリティを SMBクライアントに提供する方法の概要を管理します。 .....	1
UNIXセキュリティ形式のデータに対するNTFS ACLの提供を有効または無効にする .....	2
ONTAPによるUNIXアクセス権の維持方法 .....	2
Windowsの[セキュリティ]タブを使用したUNIXアクセス権の管理 .....	2

# UNIXセキュリティ形式のデータに対するファイルセキュリティのSMBクライアントへの提供方法を管理します。

## UNIXセキュリティ形式のデータに関してファイルセキュリティをSMBクライアントに提供する方法の概要を管理します。

SMBクライアントへのNTFS ACLの提供を有効または無効にすることで、UNIXセキュリティ形式のデータに関するファイルセキュリティをSMBクライアントに提供する方法を選択できます。それぞれの設定には利点があり、ビジネス要件に最適な設定を選択するために理解しておく必要があります。

デフォルトでは、ONTAPはUNIXセキュリティ形式のボリュームに対するUNIXアクセス権をNTFS ACLとしてSMBクライアントに提供します。これは次のような場合に適しています。

- Windows の [ プロパティ ] ボックスの [ セキュリティ \* ] タブを使用して、UNIX アクセス権を表示および編集する。

処理がUNIXシステムで許可されていない場合、Windowsクライアントから権限を変更することはできません。たとえば、所有していないファイルの所有権は変更できません。これは、UNIXシステムではこの処理が許可されていないためです。この制限により、SMBクライアントはファイルやフォルダに対して設定されたUNIXアクセス権をバイパスできないようになっています。

- UNIXセキュリティ形式のボリューム上のファイルの編集や保存に特定のWindowsアプリケーション（Microsoft Officeなど）を使用しており、ONTAPでの保存時にUNIXアクセス権を維持する必要がある場合。
- 使用するファイルのNTFS ACLを読み取ることを想定した特定のWindowsアプリケーションが環境内にあります。

状況によっては、NTFS ACLとしてのUNIXアクセス権の提供を無効にすることができます。この機能を無効にすると、ONTAPはUNIXセキュリティ形式のボリュームをFATボリュームとしてSMBクライアントに提供します。UNIXセキュリティ形式のボリュームをFATボリュームとしてSMBクライアントに提供する理由はいくつかあります。

- UNIXアクセス権を変更するには、UNIXクライアントでマウントを使用する必要があります。

UNIXセキュリティ形式のボリュームがSMBクライアントでマッピングされている場合は、[セキュリティ] タブは使用できません。マッピングされたドライブは、ファイル権限がないFATファイルシステムでフォーマットされているように見えます。

- SMBを介したアプリケーションを使用している場合、アクセスするファイルやフォルダにNTFS ACLを設定していますが、データがUNIXセキュリティ形式のボリューム上にあると失敗する可能性があります。

ONTAPでボリュームがFATと報告された場合、アプリケーションはACLの変更を試行しません。

### 関連情報

[FlexVolでのセキュリティ形式の設定](#)

## UNIXセキュリティ形式のデータに対するNTFS ACLの提供を有効または無効にする

UNIX セキュリティ形式のデータ（UNIX セキュリティ形式のボリュームと UNIX 対応のセキュリティを使用する mixed セキュリティ形式のボリューム）に対する NTFS ACL の SMB クライアントへの提供を有効または無効にできます。

### タスクの内容

このオプションを有効にすると、ONTAP は、UNIX 対応のセキュリティ形式を使用するボリュームのファイルおよびフォルダを NTFS ACL を使用するように SMB クライアントに提供します。このオプションを無効にした場合は、ボリュームが SMB クライアントに FAT ボリュームとして提供されます。デフォルトでは、NTFS ACL が SMB クライアントに提供されます。

### 手順

1. 権限レベルをadvancedに設定します。 `set -privilege advanced`
2. UNIX NTFS ACL オプションを設定します。 `vserver cifs options modify -vserver vserver_name -is-unix-nt-acl-enabled {true|false}`
3. オプションが目的の値に設定されていることを確認します。 `vserver cifs options show -vserver vserver_name`
4. admin権限レベルに戻ります。 `set -privilege admin`

## ONTAPによるUNIXアクセス権の維持方法

UNIX アクセス権を現在持っている FlexVol ボリューム内のファイルが Windows アプリケーションによって編集および保存されても、ONTAP は UNIX アクセス権を維持できます。

Windows クライアントのアプリケーションは、ファイルを編集して保存するときに、ファイルのセキュリティプロパティを読み取り、新しい一時ファイルを作成し、それらのプロパティを一時ファイルに適用してから、一時ファイルに元のファイル名を付けます。

セキュリティプロパティのクエリを実行すると、Windows クライアントは、UNIX アクセス権を正確に表す構築済み ACL を受け取ります。この構築済み ACL は、Windows アプリケーションによってファイルが更新されるたびにファイルの UNIX アクセス権を維持し、生成されたファイルが同じ UNIX アクセス権を持つようにするためだけに使用されます。ONTAP は、構築済み ACL を使用して NTFS ACL を設定しません。

## Windowsの[セキュリティ]タブを使用したUNIXアクセス権の管理

SVM 上の mixed セキュリティ形式のボリュームまたは qtree に含まれるファイルまたはフォルダの UNIX アクセス権を操作する場合は、Windows クライアントのセキュリティタブを使用できます。また、Windows ACL を照会および設定できるアプリケーションを使用することもできます。

- UNIX アクセス権の変更

Windows のセキュリティタブを使用して、mixed セキュリティ形式のボリュームまたは qtree の UNIX アクセス権を表示および変更できます。メインの [Windows Security] タブを使用して UNIX アクセス権を変更する場合は、編集する既存の ACE を削除してから（モードビットを 0 に設定）、変更を行う必要があります。または、高度なエディタを使用して権限を変更することもできます。

モードのアクセス権を使用している場合は、リストされた UID、GID、およびその他（コンピュータにアカウントを持つその他すべてのユーザ）のモードアクセス権を直接変更できます。たとえば、表示された UID に r-x のアクセス権が設定されている場合、この UID のアクセス権を rwx に変更できます。

- UNIX アクセス権を NTFS アクセス権に変更しています

Windows のセキュリティタブを使用して、ファイルおよびフォルダのセキュリティ形式が UNIX 対応である mixed 型セキュリティ形式のボリュームまたは qtree 上で、UNIX セキュリティオブジェクトを Windows セキュリティオブジェクトに置き換えることができます。

適切な Windows のユーザおよびグループのオブジェクトに置き換える前に、リストされている UNIX アクセス権のエントリをすべて削除しておく必要があります。次に、Windows のユーザおよびグループのオブジェクトに NTFS ベースの ACL を設定します。すべての UNIX セキュリティオブジェクトを削除し、Windows のユーザおよびグループのみを mixed セキュリティ形式のボリュームまたは qtree 上のファイルまたはフォルダに追加すると、ファイルまたはフォルダのセキュリティ形式が UNIX から NTFS へ変換されます。

フォルダの権限を変更する場合、Windows のデフォルトの動作では、すべてのサブフォルダとファイルにこれらの変更が反映されます。したがって、セキュリティ形式の変更をすべての子フォルダ、サブフォルダ、およびファイルに反映したくない場合は、反映する範囲を希望の範囲に変更する必要があります。

## 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。