



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の管理
ONTAP 9

NetApp
February 12, 2026

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の管理 ..	1
UNIXセキュリティ形式のデータに対して、SMBクライアントに	
ONTAPファイルセキュリティを提供する方法について説明します。	1
UNIXセキュリティ形式のデータ用にONTAP SMBクライアントへのNTFS	
ACLのプレゼンテーションを設定する	2
ONTAP SMB FlexVolボリュームのUNIX権限の保持について学習します	2
ONTAP SMBサーバのWindowsセキュリティタブを使用して	
UNIX権限を管理する方法について学習します。	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の管理

UNIXセキュリティ形式のデータに対して、**SMB**クライアントに**ONTAP**ファイルセキュリティを提供する方法について説明します。

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によって、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選択できます。それぞれの設定の利点を理解して、ビジネス要件に適した方を選ぶようにしてください。

デフォルトでは、UNIXセキュリティ形式のボリュームに対するUNIXアクセス権がNTFS ACLとしてSMBクライアントに提供されます。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 権限を表示および編集します。

処理がUNIXシステムで許可されていない場合は、Windowsクライアントからアクセス権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を変更することはできません。これは、UNIXシステムではこうした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に格納された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にある場合。

状況に応じて、NTFS ACLとしてのUNIXアクセス権の提供を無効にすることもできます。この機能を無効にすると、UNIXセキュリティ形式のボリュームがFATボリュームとしてSMBクライアントに提供されます。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のは、次のような場合です。

- UNIXアクセス権の変更は、マウントを使用してUNIXクライアントでしか行わない場合。

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、[セキュリティ]タブで操作することはできません。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たドライブとして表示されます。

- SMBを使用するアプリケーションでアクセスするファイルやフォルダにNTFS ACLを設定しており、データがUNIXセキュリティ形式のボリュームにあると失敗する可能性がある場合。

ONTAPではボリュームがFATとして報告され、アプリケーションでACLの変更は試行されません。

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用にONTAP SMBクライアントへのNTFS ACLのプレゼンテーションを設定する

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およびUNIX有効セキュリティを使用する混在セキュリティ形式のボリューム）に対して、SMBクライアントへのNTFS ACLの表示を有効または無効にできます。

タスク概要

このオプションを有効にすると、ONTAPは、有効なUNIXセキュリティ形式のボリューム上のファイルとフォルダを、NTFS ACLを持つものとしてSMBクライアントに提示します。このオプションを無効にすると、ボリュームはSMBクライアントに対してFATボリュームとして提示されます。デフォルトでは、SMBクライアントに対してNTFS ACLが提示されます。

手順

1. 権限レベルをadvancedに設定します：`set -privilege advanced`
2. UNIX NTFS ACLオプション設定を構成します。`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 SMB FlexVolボリュームのUNIX権限の保持について学習します

現在 UNIX 権限を持つ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ると、ONTAP は UNIX 権限を保持できます。

Windows クライアント上のアプリケーションがファイルを編集して保存する場合、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、一時ファイルに元のファイル名を付けます。

Windowsクライアントがセキュリティプロパティのクエリを実行すると、UNIX権限を正確に表す構築済みACLが返されます。この構築済みACLの唯一の目的は、Windowsアプリケーションによってファイルが更新されてもファイルのUNIX権限を保持し、更新後のファイルに同じUNIX権限が付与されるようにすることです。ONTAPは、構築済みACLを使用してNTFS ACLを設定することはありません。

ONTAP SMBサーバのWindowsセキュリティタブを使用してUNIX権限を管理する方法について学習します。

SVM上の混合セキュリティ形式のボリュームまたはqtree内のファイルまたはフォルダのUNIX権限を操作する場合は、Windowsクライアントの[セキュリティ]タブを使用できます。または、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権限の変更

Windowsの「セキュリティ」タブを使用して、混合セキュリティ形式のボリュームまたはqtreeのUNIX権限を表示および変更できます。Windowsのメインの「セキュリティ」タブを使用してUNIX権限を変更する場合は、変更を加える前に、編集する既存のACEを削除する必要があります（これにより、モードビットが0に設定されます）。または、詳細エディタを使用して権限を変更することもできます。

モード権限を使用する場合、リストされているUID、GID、その他（コンピューターにアカウントを持つ他のすべてのユーザー）のモード権限を直接変更できます。例えば、表示されているUIDにr-x権限がある場合、UID権限をrwxに変更できます。

- UNIX 権限から NTFS 権限への変更

Windows セキュリティ タブを使用すると、ファイルとフォルダに UNIX 対応のセキュリティ スタイルが設定されている、混合セキュリティ スタイル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。

必要なWindowsユーザおよびグループオブジェクトに置き換える前に、まずリストされているすべてのUNIX権限エントリを削除する必要があります。その後、WindowsユーザおよびグループオブジェクトにNTFSベースのACLを設定できます。すべてのUNIXセキュリティオブジェクトを削除し、混合セキュリティ形式のボリュームまたはqtreeのファイルまたはフォルダにWindowsユーザおよびグループのみを追加することで、ファイルまたはフォルダの有効なセキュリティ形式がUNIXからNTFSに変更されます。

フォルダの権限を変更すると、Windowsのデフォルトの動作では、これらの変更がすべてのサブフォルダとファイルに反映されます。したがって、セキュリティスタイル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させたくない場合は、反映方法を適切な設定に変更する必要があります。

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。