NiCE

NTFSアクセスマスクフラグと、それに対応するユーザー権限は何ですか？

https://kb-ja.netapp.com/on-prem/ontap/da/NAS/NAS-KBs/What_are_NTFS_access_mask_flags_with_…
Updated: Mon, 21 Sep 2026 09:02:04 GMT

環境

- ONTAP 9以降
- Windows
- SMB / CIFS
- NTFSボリューム

回答

- ACCESS_MASKは、オブジェクトに対するユーザーの権限をエンコードするために使用される32ビットのフラグセットです。
- アクセスマスクは、プリンシパルに割り当てられたオブジェクトへの権限をエンコードするためと、オブジェクトを開く際に要求されたアクセスをエンコードするための両方に使用されます。
- 以下は、最も一般的に使用されるアクセスマスクです：
  - 読み取り権限の場合は、0x1200A9を使用してください。これは以下のフラグに対応します：
    FILE_READ_DATA（ファイル）または FILE_LIST_DIRECTORY（ディレクトリ）
    1 (0x1)
    FILE_READ_EA
    8 (0x8)
    FILE_EXECUTE（ファイル）または FILE_TRAVERSE（ディレクトリ）
    32 (0x20)
    FILE_READ_ATTRIBUTES
    128 (0x80)
    READ_CONTROL
    131072 (0x20000)
    SYNCHRONIZE
    1048576 (0x100000)
  - 変更権限には、0x1301BF を使用してください。これは、以下の追加フラグに対応します。
    FILE_WRITE_DATA（ファイル）または FILE_ADD_FILE（ディレクトリ）
    2 (0x2)
    FILE_APPEND_DATA（ファイル）または FILE_ADD_SUBDIRECTORY（ディレクトリ）
    4 (0x4)
    FILE_WRITE_EA
    16 (0x10)
    FILEget_ATTRIBUTES
    256 (0x100)
    DELETE
    65536 (0x10000)
  - フルコントロール権限を使用するには、0x1F01FF を使用してください。これは、以下の追加フラグに対応します。
    FILE_DELETE_CHILD
    64 (0x40)
    WRITE_DAC
    262144 (0x40000)

WRITE_OWNER
524288 (0x80000)

- 以下はファイル用アクセスマスクビットマップテーブルです：

Value	概要
GR GENERIC_READ 0x80000000L	**アクセス要求操作で使用する場合：**オブジェクトへの読み取りアクセスが要求されると、このビットはビットの組み合わせに**変**換されます。これらは通常、ACCESS_MASKの下位16ビットに設定されます。（個々のプロトコル仕**様**では、異なる構成が指定される場合があります。）設定されるビットは実装に依存します。この**変**換処理中に、GRビットはクリアされます。結果として得られるACCESS_MASKビットは、オブジェクトに添付されたセキュリティ記述子内のACE構造体に**対**してチェックされる実際のアクセス許可です。 **オブジェクトのセキュリティ記述子を設定する際に使用する場合：**オブジェクトにアタッチされるACEでGRビットが設定されると、それはビットの組み合わせに**変**換され、通常はACCESS_MASKの下位16ビットに設定されます。（個々のプロトコル仕**様**では、異なる構成が指定される場合があります。）設定されるビットは実装に依存します。この**変**換処理中に、GRビットはクリアされます。結果として得られるACCESS_MASKビットは、このACEによって実際に付与されるアクセス許可です。
GW GENERIC_WRITE 0x4000000L	**アクセス要求操作で使用する場合：**オブジェクトへの書き込みアクセスが要求されると、このビットはビットの組み合わせに**変**換され、通常はACCESS_MASKの下位16ビットに設定されます。（個々のプロトコル仕**様**では、異なる構成が指定されている場合があります。）設定されるビットは実装に依存します。この**変**換処理中、 GWビットはクリアされます。結果として得られるACCESS_MASKビットは、オブジェクトに添付されたセキュリティ記述子内のACE構造体に**対**してチェックされる実際のアクセス許可です。 **オブジェクトのセキュリティ記述子を設定する際に使用する場合：**オブジェクトにアタッチされるACEでGWビットが設定されると、それはビットの組み合わせに**変**換され、通常はACCESS_MASKの下位16ビットに設定されます。（個々のプロトコル仕**様**では、異なる構成が指定されている場合があります。）設定されるビットは実装に依存します。この**変**

	換処理中に、GWビットはクリアされます。結果として得られるACCESS_MASKビットは、このACEによって実際に付与されるアクセス許可です。
GX GENERIC_EXECUTE 0x20000000L	**アクセス要求操作で使用する場合：**オブジェクトへの実行アクセスが要求されると、このビットはビットの組み合わせに**変**換され、通常はACCESS_MASKの下位16ビットに設定されます。（個々のプロトコル仕**様**では、異なる構成が指定される場合があります。）設定されるビットは実装に依存します。この**変**換処理中に、GXビットはクリアされます。結果として得られるACCESS_MASKビットは、オブジェクトに添付されたセキュリティ記述子内のACE構造体に**対**してチェックされる実際のアクセス許可です。 **オブジェクトのセキュリティ記述子を設定する際に使用する場合：**オブジェクトにアタッチされるACEでGXビットが設定されると、それはビットの組み合わせに**変**換され、通常はACCESS_MASKの下位16ビットに設定されます。（個々のプロトコル仕**様**では、異なる構成が指定される場合があります。）設定されるビットは実装に依存します。この**変**換処理中に、GXビットはクリアされます。結果として得られるACCESS_MASKビットは、このACEによって実際に付与されるアクセス許可です。
GA GENERIC_ALL 0x10000000L	**アクセス要求操作で使用する場合：**オブジェクトへのすべてのアクセス**権**限が要求された場合、このビットはビットの組み合わせに**変**換され、通常はACCESS_MASKの下位16ビットに設定されます。（個々のプロトコル仕**様**では、異なる構成が指定される場合があります。）オブジェクトは、そのセマンティクスで必要とされる場合、上位16ビットのビットをその**変**換に含めることができます。設定されるビットは実装に依存します。この**変**換中に、GAビットはクリアされます。結果として得られるACCESS_MASKビットは、オブジェクトに添付されたセキュリティ記述子内のACE構造体に**対**してチェックされる実際のアクセス許可です。 **オブジェクトのセキュリティ記述子を設定する際に使用する場合：**オブジェクトにアタッチされるACEでGAビットが設定されると、それはビットの組み合わせに**変**換され、通常はACCESS_MASKの下位16ビットに設定されます。（個々のプロトコル仕**様**では、異なる構成が指定される場合があります。）オブジェクトは、必要に**応**じて、その**変**換に上位16ビ

	ットのビットを含めることができます。これはオブジェクトの セマンティクスによって決まります。設定されるビットは実装に依存します。この変換中に、GAビットはクリアされます。結果として得られるACCESS_MASKビットは、このACEによって実際に付与されるアクセス許可です。
MA MAXIMUM_ALLOWED 0x02000000L	**アクセス要求操作で使用する場合：**要求があった場合、このビットはアクセスチェックアルゴリズムを通じて、要求者にオブジェクトに対して許可される最大の権限を付与します。このビットは要求することしかできず、ACEに設定することはできません。 **オブジェクトのセキュリティ記述子を設定する際に使用する場合：**SECURITY_DESCRIPTOR で最大許容ビットを指定することに意味はありません。MA ビットは、SECURITY_DESCRIPTOR 構造体の一部である場合、設定してはならず、無視されるべきです。
AS ACCESS_SYSTEM_SECURITY 0x01000000L	**アクセス要求操作で使用する場合：**要求があった場合、このビットは要求者にオブジェクトのSACLを変更する権利を付与します。このビットは、DACLの一部であるACEに設定してはなりません。SACLの一部であるACEに設定されている場合、このビットはSACL自体へのアクセスの監査を制御します。
SY 同期する 0x00100000L	オブジェクトを同期したり、オブジェクトを待機したりするのに十分な、オブジェクトへのアクセス権を指定します。
WO WRITE_OWNER 0x00080000L	セキュリティ記述子に記載されているオブジェクトの所有者を変更する権限を指定します。
WD WRITE_DACL	オブジェクトのセキュリティ記述子の任意アクセス制御リストを変更する権限を指定します。

0x00040000L

RC

READ_CONTROL

0x00020000L

オブジェクトのセキュリティ記述子を読み取るためのアクセス権を指定します。

DE

DELETE

0x00010000L

オブジェクトを削除するためのアクセス権を指定します。

- 以下はディレクトリのアクセスマスクビットマップです：

Value	概要
FILE_LIST_DIRECTORY 0x00000001	この値は、ディレクトリの内容を列挙する権限を示します。
FILE_ADD_FILE 0x00000002	この値は、指定されたディレクトリにファイルを作成する権限を示します。
FILE_ADD_SUBDIRECTORY 0x00000004	この値は、ディレクトリの下にサブディレクトリを追加する権限を示します。
FILE_READ_EA 0x00000008	この値は、ディレクトリの拡張属性を読み取る権限を示します。
FILE_WRITE_EA 0x00000010	この値は、ディレクトリの拡張属性を書き込んだり変更したりする権限を示します。
FILE_TRAVERSE	この値は、基となるオブジェクトストアがトラバーサルチェックを強制

0x00000020	する場合に、このディレクトリを走査する権利を示します。
FILE_DELETE_CHILD 0x00000040	この値は、このディレクトリ内のファイルとディレクトリを削除する権限を示します。
FILE_READ_ATTRIBUTES 0x00000080	この値は、ディレクトリの属性を読み取る権限を示します。
FILE_WRITE_ATTRIBUTES 0x00000100	この値は、ディレクトリの属性を変更する権利を示します。
DELETE 0x00010000	この値は、ディレクトリを削除する権限を示します。
READ_CONTROL 0x00020000	この値は、ディレクトリのセキュリティ記述子を読み取る権限を示します。
WRITE_DAC 0x00040000	この値は、ディレクトリのセキュリティ記述子内のDACLを変更する権利を示します。DACL データ構造については、[MS-DTYP]セクション2.4.5の ACL を参照してください。
WRITE_OWNER 0x00080000	この値は、ディレクトリのセキュリティ記述子における所有者を変更する権利を示します。
同期する 0x00100000	このフラグはクライアントとサーバーの両方で無視しなければなりません。
ACCESS_SYSTEM_SECURITY 0x01000000	この値は、ディレクトリのセキュリティ記述子内のSACLを読み取るまたは変更する権限を示します。SACL データ構造については、[MS-DTYP] のセクション 2.4.5 の ACL を参照してください。
MAXIMUM_ALLOWED	この値は、クライアントがそのディレクトリに対して持つ最高レベルの

0x02000000	アクセス権限でディレクトリを開くことを要求していることを示します。クライアントにこのディレクトリへのアクセス権限が付与されていない場合、サーバーは STATUS_ACCESS_DENIED でオープン処理を失敗させなければなりません。
GENERIC_ALL 0x10000000	この値は、MAXIMUM_ALLOWED と ACCESS_SYSTEM_SECURITY を除く、上記にリストされているすべてのアクセスフラグに対するリクエストを示します。
GENERIC_EXECUTE 0x20000000	この値は、上記にリストされている以下のアクセスフラグ（FILE_READ_ATTRIBUTES、FILE_TRAVERSE、SYNCHRONIZE、READ_CONTROL）の要求を示します。
GENERIC_WRITE 0x40000000	この値は、上記にリストされている次のアクセスフラグの要求を示します：FILE_ADD_FILE、FILE_ADD_SUBDIRECTORY、FILE_WRITE_ATTRIBUTES、FILE_WRITE_EA、SYNCHRONIZE、およびREAD_CONTROL。
GENERIC_READ 0x80000000	この値は、上記にリストされている以下のアクセスフラグの要求を示します：FILE_LIST_DIRECTORY、FILE_READ_ATTRIBUTES、FILE_READ_EA、SYNCHRONIZE、およびREAD_CONTROL。

追加情報

Access_mask の詳細については、以下の Microsoft ドキュメントを参照してください：

- Access_Mask
- Directory_Access_Mask

NTFS アクセスマスクフラグは、vserver security file-directory show コマンドの出力に表示されます。