iStorage

NEC

iStorage M シリーズ
NAS オプション ソフトウェア

Virtual File Platform

ファイルアクセス（CIFS/NFS）ユーザーズガイド

IF306-11

対象製品

Virtual File Platform
6.4.3-15 以降

輸出時の注意

本製品（ソフトウェアを含む）は、外国為替及び外国貿易法で規定される規制貨物（または役務）に該当することがあります。
その場合、日本国外へ輸出する場合には日本国政府の輸出許可が必要です。
なお、輸出許可申請手続にあたり資料等が必要な場合には、お買い上げの販売店またはお近くの当社営業拠点にご相談ください。

商標類

マイクロソフト製品のスクリーンショットの使用について

Microsoft Corporation のガイドラインに従って画面写真を使用しています。

発行

2022 年 5 月（第 11 版）

目次

図目次

表目次

はじめに

このマニュアルは，CIFS または NFS クライアントから Virtual File Platform（HVFP）の CIFS サービスまたは NFS サービスを利用するに当たって，事前に知っておいていただきたいことや，注意する必要があることについて説明したものです。

HVFP の CIFS サービスまたは NFS サービスを利用する場合は，必ずこのマニュアルを読み，設定方法および指示事項をよく理解してから操作してください。

また，このマニュアルをいつでも利用できるよう，HVFP の CIFS サービスまたは NFS サービスを利用するコンピュータの近くに保管してください。

このマニュアルでは，主に次のプログラムを対象として説明しています。

・File Services Manager

なお，最新のサポート対象製品情報は，NEC サポートポータルの以下のページに掲載のサポートマトリクスを参照してください。

・「お知らせ／技術情報」－「技術情報」－「【iStorage M シリーズ】【NAS オプション】接続サポートマトリクス」　　コンテンツ ID：3140101655

対象読者

このマニュアルは，CIFS サービスまたは NFS サービスの管理に携わるシステム管理者にお読みいただくことを前提に説明しています。

また，「システム構成ガイド」（IF302）などの HVFP のマニュアルを通読していて，次の知識をお持ちであることを前提に説明しています。

- ストレージシステムに関する基本的な知識
- ネットワークに関する基本的な知識
- ファイル共有サービスに関する基本的な知識
- SAN に関する基本的な知識
- CIFS に関する基本的な知識
- NFS に関する基本的な知識
- UNIX に関する基本的な知識
- Windows に関する基本的な知識
- WWW ブラウザーに関する基本的な知識

マニュアルの構成

このマニュアルは，次に示す章と付録から構成されています。

章	内容
1. CIFS サービスの概要	HVFP の CIFS サービスを利用したアクセスの概要について説明しています。
2. CIFS サービス利用時のシステムの構成	HVFP の CIFS サービスを利用するための動作環境とネットワーク構成について説明しています。
3. File Services Manager での CIFS サービスの運用	HVFP を利用するためにシステム管理者が行う運用管理操作の中から，CIFS サービスを利用する場合に注意が必要な操作について説明しています。
4. CIFS クライアントのユーザー管理	CIFS クライアントのユーザー管理について説明しています。
5. CIFS クライアントのユーザー認証	CIFS クライアントのユーザー認証に関する注意事項について説明しています。
6. Windows ドメイン環境のユーザー資源移行手順	Windows ドメイン環境で作成されたユーザー資源を移行する際の注意事項と，バックアップユーティリティを用いて HVFP 上にユーザー資源を移行する手順について説明しています。
7. 共有ディレクトリへの CIFS アクセス	CIFS クライアントから共有ディレクトリにアクセスする場合の手順と注意事項について説明しています。
8. CIFS 共有内のファイル・フォルダ	CIFS 共有ディレクトリ内に作成するファイル・フォルダに関する注意事項について説明しています。
9. MMC 連携	MMC による CIFS 共有管理に関する注意事項について説明しています。
10. Volume Shadow Copy Service を使用した差分スナップショットの公開	ファイルスナップショット機能で作成された差分スナップショットを，Volume Shadow Copy Service を使用して CIFS クライアントに公開する方法について説明しています。

章	内容
11. CIFS クライアントとして使用するプラットフォームについて	CIFS クライアントとして使用するプラットフォームの違いによる注意事項を説明しています。
12. Virtual Server 運用上の注意事項	Virtual Server を使用する場合の CIFS 共有に関する注意事項を説明しています。
13. NFS サービスの概要	HVFP の NFS サービスを利用したアクセスの概要について説明しています。
14. NFS サービス利用時のシステムの構成	HVFP の NFS サービスを利用するための動作環境とネットワーク構成について説明しています。
15. File Services Manager での NFS サービスの運用	HVFP を利用するためにシステム管理者が行う運用管理操作の中から，NFS サービスを利用する場合に注意が必要な操作について説明しています。
16. NFS クライアントのユーザー管理	NFS クライアントのユーザー管理について説明しています。
17. NFS クライアントのユーザー認証	NFS クライアントのユーザー認証の方法および注意事項について説明しています。
18. 共有ディレクトリへの NFS アクセス	NFS クライアントから共有ディレクトリにアクセスする場合の手順と注意事項について説明しています。
19. NFS 共有内のファイル・ディレクトリ	NFS 共有ディレクトリ内に作成するファイル・ディレクトリに関する注意事項について説明しています。
20. ファイル共有を利用するときの注意事項	CIFS クライアントと NFS クライアントで共有しているファイルシステムやファイル共有を利用するときの注意事項について説明しています。
A. CIFS サービス利用時のトラブルシュート	CIFS サービス利用時のエラーによって syslog または CIFS ログに出力されるメッセージとその対処，および MMC 操作時のエラーと対処について説明しています。また，CIFS サービスおよびファイル共有の設定についてよくある質問および回答を，FAQ の形式で説明しています。
B. NFS サービス利用時のトラブルシュート	NFS サービス利用時のエラーと対処について説明しています。
C. Kerberos 認証を利用するときの NFS 環境の構築手順	Kerberos 認証を利用するときの NFS 環境の構築手順について，実行例を基に説明しています。
D. Kerberos 認証を利用するときの NFS 共有ディレクトリへのアクセス手順	Kerberos 認証を利用するときの NFS 共有ディレクトリへのアクセス手順について，実行例を基に説明しています。
E. セカンダリー KDC サーバの追加手順	セカンダリー KDC サーバを構築して追加する手順について，実行例を基に説明しています。
F. WORM 運用のための API	WORM 運用に使用するカスタムアプリケーションを作成するための API について説明しています。
G. 参考資料	参考資料として，関連する Web サイトの URL について説明しています。
H. 略語一覧	HVFP のマニュアルで使用している略語を示しています。

このマニュアルでは，製品の GUI 項目と操作はクラスタ構成の場合を想定して記載しています。

マニュアル体系

HVFP のマニュアル体系を次に示します。

マニュアル名	内容
Virtual File Platform ファーストステップガイド（IF301）	HVFP をセットアップする前に検討しておくべきこと，および，セットアップの手順について説明しています。
Virtual File Platform システム構成ガイド（IF302）	HVFP を運用するために，最初にお読みいただくマニュアルです。 HVFP の運用を開始する前に理解または検討しておいていただきたいことや，外部サーバの環境設定などについて説明しています。
Virtual File Platform セットアップガイド（IF303）	HVFP のセットアップ方法について説明しています。 仮想サーバで HVFP を運用する場合は，「仮想サーバ環境セットアップガイド」（IF304）をお読みください。
Virtual File Platform 仮想サーバ環境セットアップガイド（IF304）	HVFP での Virtual Server のセットアップ方法について説明しています。
Virtual File Platform 仮想サーバ環境セットアップガイド別紙（IF318）	HVFP における Virtual Server の性能に関する説明をしています。
Virtual File Platform ユーザーズガイド（IF305）	HVFP を運用するために必要な手順や GUI リファレンスなどを説明しています。
Virtual File Platform ファイルアクセス（CIFS/NFS）ユーザーズガイド（IF306）（このマニュアル）	CIFS または NFS クライアントから，HVFP の CIFS サービスまたは NFS サービスを利用するに当たって，事前に知っておいていただきたいことや，注意する必要があることについて説明しています。
Virtual File Platform ファイルアクセス（Quota）ユーザーズガイド（IF307）	ファイルシステムやディレクトリに Quota を設定する際に，事前に知っておいていただきたいことや，注意する必要があることについて説明しています。
Virtual File Platform トラブルシューティングガイド（IF308）	HVFP の障害対策を説明しています。
Virtual File Platform トラブルシューティングガイド別紙（IF309）	HVFP のソフトウェア障害の回復手順について説明しています。
Virtual File Platform インストールガイド（IF310）	HVFP のインストール方法について説明しています。
Virtual File Platform コマンドリファレンス（IF311）	HVFP で使用できるコマンドの文法について説明しています。
Virtual File Platform API リファレンス（IF312）	HVFP の API の使用方法について説明しています。
Virtual File Platform メッセージリファレンス（IF313）	HVFP のメッセージについて説明しています。
Virtual File Platform メッセージリファレンス別紙（IF314）	HVFP の SNMP Trap にて通知されるメッセージについて説明しています。
Virtual File Platform ESMPRO 通報設定（IF315）	ESMPRO と連携して通報を行うための設定方法について説明しています。
Virtual File Platform BackupRestore 機能補足資料（NetBackup）（IF316）	NetBackup のマニュアルの理解を補助するためのものです。
Virtual File Platform システム動作情報のグラフ化手順書（IF317）	HVFP のシステム動作情報をグラフ化する手順について説明しています。

このマニュアルでの表記

このマニュアルでは，製品の名称を省略して表記しています。このマニュアルでの表記と，製品の正式名称または意味を次の表に示します。

このマニュアルでの表記	製品名称または意味
Active Directory	Active Directory(R)
HVFP	Virtual File Platform
Mac OS X	次の製品を区別する必要がない場合の表記です。 ・ Mac OS(R) X v10.5 ・ Mac OS(R) X v10.7 ・ OS X v10.8 ・ OS X v10.9 ・ OS X v10.10 ・ OS X v10.11 ・ mac OS v10.12
Mac OS X v10.8	OS X v10.8
Mac OS X v10.9	OS X v10.9
Mac OS X v10.10	OS X v10.10
Mac OS X v10.11	OS X v10.11
OpenLDAP	OpenLDAP 2.x
Solaris	次の製品を区別する必要がない場合の表記です。 ・ Solaris 9 オペレーティングシステム SPARC プラットフォーム版 ・ Solaris 10 オペレーティングシステム SPARC プラットフォーム版
Solaris 10	Solaris 10 オペレーティングシステム SPARC プラットフォーム版
Windows	Microsoft(R) Windows(R) Operating System
Windows 8.1	次の製品を区別する必要がない場合の表記です。 ・ Microsoft(R) Windows(R) 8.1 32-bit ・ Microsoft(R) Windows(R) 8.1 64-bit ・ Microsoft(R) Windows(R) 8.1 Enterprise 32-bit ・ Microsoft(R) Windows(R) 8.1 Enterprise 64-bit ・ Microsoft(R) Windows(R) 8.1 Pro 32-bit ・ Microsoft(R) Windows(R) 8.1 Pro 64-bit
Windows 10	次の製品を区別する必要がない場合の表記です。 ・ Microsoft(R) Windows(R) 10 Education 32-bit ・ Microsoft(R) Windows(R) 10 Education 64-bit ・ Microsoft(R) Windows(R) 10 Enterprise 32-bit ・ Microsoft(R) Windows(R) 10 Enterprise 64-bit ・ Microsoft(R) Windows(R) 10 Home 32-bit ・ Microsoft(R) Windows(R) 10 Home 64-bit ・ Microsoft(R) Windows(R) 10 Pro 32-bit ・ Microsoft(R) Windows(R) 10 Pro 64-bit

このマニュアルでの表記	製品名称または意味
Windows Server 2012	次の製品を区別する必要がない場合の表記です。 ・ Microsoft(R) Windows Server(R) 2012 Datacenter ・ Microsoft(R) Windows Server(R) 2012 Essentials ・ Microsoft(R) Windows Server(R) 2012 Foundation ・ Microsoft(R) Windows Server(R) 2012 Standard ・ Microsoft(R) Windows Server(R) 2012 R2 Datacenter ・ Microsoft(R) Windows Server(R) 2012 R2 Essentials ・ Microsoft(R) Windows Server(R) 2012 R2 Foundation ・ Microsoft(R) Windows Server(R) 2012 R2 Standard
Windows Server 2012 R2	次の製品を区別する必要がない場合の表記です。 ・ Microsoft(R) Windows Server(R) 2012 R2 Datacenter ・ Microsoft(R) Windows Server(R) 2012 R2 Essentials ・ Microsoft(R) Windows Server(R) 2012 R2 Foundation ・ Microsoft(R) Windows Server(R) 2012 R2 Standard
Windows Server 2016	次の製品を区別する必要がない場合の表記です。 ・ Microsoft(R) Windows Server(R) 2016 Datacenter ・ Microsoft(R) Windows Server(R) 2016 Standard
Windows Server 2019	次の製品を区別する必要がない場合の表記です。 ・ Microsoft(R) Windows Server(R) 2019 Datacenter ・ Microsoft(R) Windows Server(R) 2019 Standard

このマニュアルでは Windows での操作について特に断っていない場合，Windows 7 までのユーザーインターフェースを想定して記載しています。Windows Server 2012 以降の新しいユーザーインターフェースの Windows を使用されている場合は，新しいユーザーインターフェースでの操作についてのドキュメントを参照して，読み替えてください。

このマニュアルで使用する記号

このマニュアルでは，次に示す記号を使用しています。

記号	意味
[ ]	画面，メニュー，ボタン，キーボードのキーなどを示します。 （例） ［ファイルシステム］サブウィンドウ ［OK］ボタン ［Enter］キー
＜ ＞	可変値であることを示します。 （例）＜ホスト名＞.＜ポート番号＞ 実際のホスト名が「host0」，ポート番号が「1024」の場合，「host0.1024」と指定することを示します。

コマンドの書式で使用する記号

このマニュアルでは，次に示す記号を使用してコマンドを説明しています。

記号	意味
[]	この記号で囲まれている項目は省略してもよいことを示します。複数の項目がこの記号で囲まれている場合は，すべてを省略するか，どれか 1 つを指定することを示します。 （例 1）[A] 「何も指定しない」か「A を指定する」ことを示します。 （例 2）[B|C] 「何も指定しない」か「B または C を指定する」ことを示します。

KB（キロバイト）などの単位表記について

1KB（キロバイト），1MB（メガバイト），1GB（ギガバイト），1TB（テラバイト），1PB（ペタバイト）はそれぞれ 1,024 バイト，$1{,}024^2$ バイト，$1{,}024^3$ バイト，$1{,}024^4$ バイト，$1{,}024^5$ バイトです。

1Block（ブロック）は 512 バイトです。

1

CIFS サービスの概要

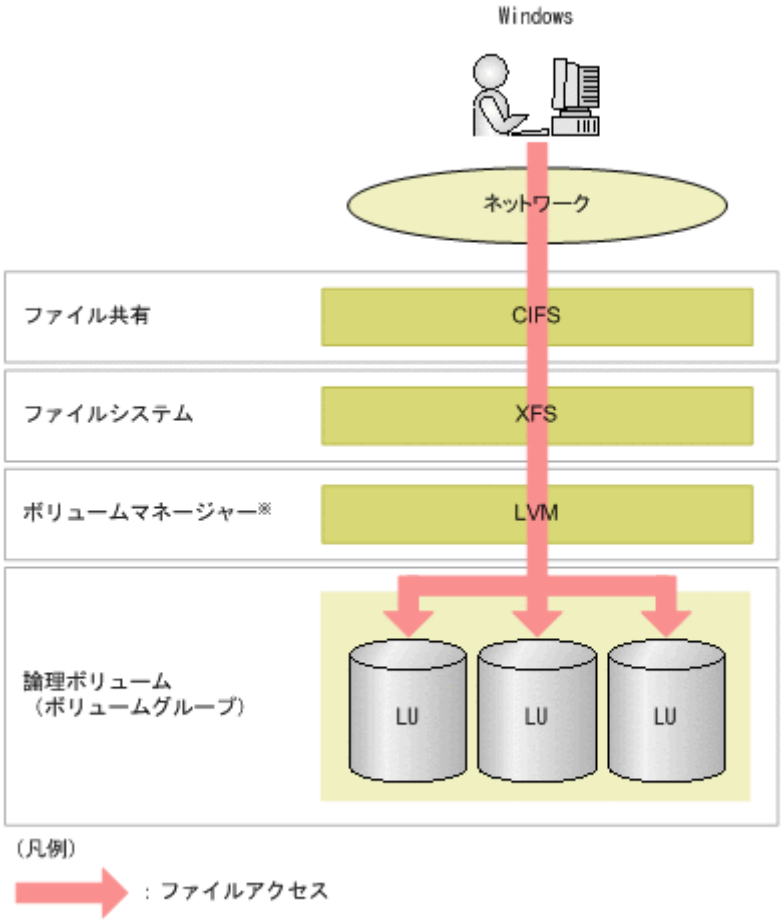
CIFS クライアントは Virtual File Platform（HVFP）の CIFS サービスを利用してデータにアクセスできます。この章では，CIFS サービス利用の概要について説明します。

1.1 CIFS サービス利用の概要

システム管理者がファイルシステムやディレクトリに CIFS 共有を作成することで，CIFS クライアントはネットワークを介してストレージシステム内のデータにアクセスできます。

CIFS クライアントがファイルシステム内のデータにアクセスする流れを次の図に示します。

図 1-1： CIFS クライアントがファイルシステム内のデータにアクセスする流れ



注※ LUを一つだけ利用する場合は，論理ボリュームを構成しないでファイルシステムを構築できます。このとき，ボリュームマネージャーは利用しません。

2

CIFS サービス利用時のシステムの構成

この章では，HVFP の CIFS サービスを利用するための動作環境とネットワーク構成について説明します。

2.1 CIFS サービスでサポートする製品

CIFS サービスでサポートする製品を次に示します。

- 最新のサポート対象製品情報は，NEC サポートポータルの以下のページに掲載のサポートマトリクスを参照してください。
  「お知らせ／技術情報」－「技術情報」－「【iStorage M シリーズ】【NAS オプション】接続サポートマトリクス」　　コンテンツ ID：3140101655
- 製造元のサポートが停止している OS については，NAS オプションにおけるサポートを停止しています。

2.1.1 CIFS クライアント

最新のサポート対象製品情報は，NEC サポートポータルの以下のページに掲載のサポートマトリクスを参照してください。

「お知らせ／技術情報」－「技術情報」－「【iStorage M シリーズ】【NAS オプション】接続サポートマトリクス」　　コンテンツ ID：3140101655

CIFS クライアントからのアクセスに SMB2.0 を使用するよう HVFP で設定していると，Windows8.1 以降または Widnows Server 2012 以降の CIFS クライアントから HVFP にアクセスできないことがあります。この場合の対処方法については，「A.4 ファイル操作時のエラーと対処」を参照してください。

2.1.2 Active Directory ドメインコントローラー

Active Directory ドメインコントローラーとしてサポートする製品を次に示します。

最新のサポート対象製品情報は，NEC サポートポータルの以下のページに掲載のサポートマトリクスを参照してください。

「お知らせ／技術情報」－「技術情報」－「【iStorage M シリーズ】【NAS オプション】接続サポートマトリクス」　　コンテンツ ID：3140101655

Active Directory ドメインコントローラーのプラットフォームによってサポートする SMB プロトコルのバージョンが異なります。そのため，CIFS サービスがドメインコントローラーとの通信で使用する SMB プロトコルのバージョンが，使用する Active Directory ドメインコントローラーでサポートされていることを確認してください。サポートされていない場合は，cifsoptset コマンドの client_ipc_max_protocol および client_ipc_min_protocol オプションで，CIFS サービスがドメインコントローラーとの通信で使用する SMB プロトコルのバージョンの設定を変更してください。

2.2 ネットワークの構成

CIFS 共有を利用する場合，同一クラスタのノードは，同じワークグループ，または同じ Active Directory ドメインに参加する必要があります。

Virtual File Platform（HVFP）では次の表に示す CIFS プロトコルをサポートしており，CIFS クライアントは HVFP のノードまたは Virtual Server の仮想 IP アドレス（IPv4 または IPv6），ホスト名または NetBIOS 名を使用して CIFS サービスを利用できます。

表 2-1：HVFP でサポートしている CIFS プロトコル

#	プロトコル
1	NetBIOS over TCP/IP
2	Direct Hosting of SMB

ただし，HVFP を新規インストールした場合は，データ通信に掛かる負荷やセキュリティ面でのリスクを軽減するために，NetBIOS over TCP/IP プロトコルは使用しない設定になっています。このため，次の場合には，CIFS サービスの構成定義で，NetBIOS over TCP/IP プロトコルを使用するように設定してください。

- ブラウジング機能を利用する場合
  IPv4 接続をするクライアントだけがブラウジング機能を利用できます。
- HVFP のノードまたは Virtual Server の NetBIOS 名を解決するために，CIFS クライアントから WINS，lmhosts またはブロードキャストを利用する場合

また，ブラウジング機能を利用するネットワークでは，次の点に注意してください。

- 同一クラスタのノードは，同じワークグループ，または同じ Active Directory ドメインに参加させてください。
- CIFS クライアントから HVFP のノードまたは Virtual Server の NetBIOS 名を指定する場合，アクセスするノードまたは Virtual Server のホスト名を指定してください。
- HVFP は，接続されているネットワークの設定および状況によって，マニュアルに記載されている事項と異なった挙動を示すことがあります。記述されている事項と異なった挙動を示す場合は，ネットワークアドレスの重複やサーバ設定，ルーターの設定を見直すことによって，ネットワーク全体が正常に動作していることを確認してください。
- ブラウジング機能を利用できるのは IPv4 接続をするクライアントだけです。

HVFP でノードまたは Virtual Server の NetBIOS 名称を使用して CIFS サービスを利用する場合，ネットワーク内のすべてのマシンが WINS，DNS，lmhosts などのサービスを利用して名前解決ができることを前提として構成されるネットワークを例に，各構成での注意点について説明します。ここで説明するネットワーク構成は次に示す 3 つの場合です。なお，これらのネットワーク構成の具体的な説明は，「システム構成ガイド」（IF302）を参照してください。

- CIFS クライアントと HVFP のノードまたは Virtual Server が同じサブネットに接続されている場合
- CIFS クライアントが HVFP のノードまたは Virtual Server と異なるサブネットに接続されている場合
- 複数のポートで CIFS サービスを利用する場合

2.2.1 CIFS クライアントと HVFP のノードまたは Virtual Server が同じサブネットに接続されている場合

CIFS クライアントと HVFP のノードまたは Virtual Server が同じサブネットに接続されている場合にブラウジング機能を利用するときの注意事項を次に示します。

- CIFS クライアント側では，WINS サーバを利用して名前解決することを推奨します。
- ドメインコントローラーが同じサブネットにない場合，HVFP が提供する CIFS サービスがローカルマスターブラウザーとして動作することがあります。このとき，フェールオーバーが発生すると，ローカルマスターブラウザーとして動作していた CIFS サービスが一時的に停止するため，CIFS クライアントがコンピューター一覧を取得するのに時間が掛かります。CIFS

クライアントは，CIFS サービスがローカルマスターブラウザーとして動作してから CIFS 共有にアクセスしてください。

2.2.2 CIFS クライアントが HVFP のノードまたは Virtual Server と異なるサブネットに接続されている場合

CIFS クライアントが HVFP のノードまたは Virtual Server と異なるサブネットに接続されている場合にブラウジング機能を利用するときの注意事項を次に示します。

- 必ず Active Directory 構成にしてください。
- HVFP のノードまたは Virtual Server が接続されているサブネットには，ドメインコントローラーを用意する必要があります。
- CIFS クライアントに対するネームサーバとして WINS サーバを利用する場合は，ネットワーク内のすべての CIFS クライアントを WINS クライアントに設定することを推奨します。
- WINS サーバを利用しない場合，lmhosts ファイルを次のとおり修正する必要があります。
  - CIFS クライアントと同じサブネットにあるドメインコントローラーの lmhosts ファイルに，次の記述を追加してください。ドメインコントローラーが接続されていないサブネットでは，すべての CIFS クライアントの lmhosts ファイルに，次の記述を追加してください。
    ＜HVFPのノードまたはVirtual Serverと同じサブネットにあるドメインコントローラーのIPアドレス＞ ＜ドメイン名＞#1B

2.2.3 複数のポートで CIFS サービスを利用する場合

複数のポートで CIFS サービスを利用する場合にブラウジング機能を利用するとき，ポートが接続するサブネットごとに別の WINS サーバが必要になります。ネットワークに接続しているすべての CIFS クライアントは，使用する WINS サーバに応じて，HVFP のノードまたは Virtual Server にアクセスする経路を選択できます。

2.2.4 DNS を利用する場合

CIFS サービスの認証モードを設定するときに指定するドメインコントローラーのサーバ名に複数の IP アドレスが割り当てられている場合に，HVFP からアクセスできない IP アドレスが含まれていると，運用中にドメインコントローラーにアクセスできなくなることがあります。原因として，DNS のラウンドロビン機能によって，割り当てられたすべての IP アドレスに対して処理が分散され，HVFP からアクセスできない IP アドレスがドメインコントローラーのアドレスとして引き当てられたことが考えられます。なお，Windows の nslookup コマンドでラウンドロビン機能を使用しているかどうかを確認できます。このような問題が発生している場合は，/etc/hosts ファイルにドメインコントローラーを登録することで対処できます。［Network & System Configuration］ダイアログの［Edit System File］ページで /etc/hosts ファイルに次の情報を追記してください。

＜HVFPからアクセスできるIPアドレス＞ ＜ドメインコントローラーのホスト名＞ ＜ドメインコントローラーのホスト名（FQDN）＞

追記例を次に示します。

```
10.213.89.113 dc-host dc-host.sample.domain.local
```

3

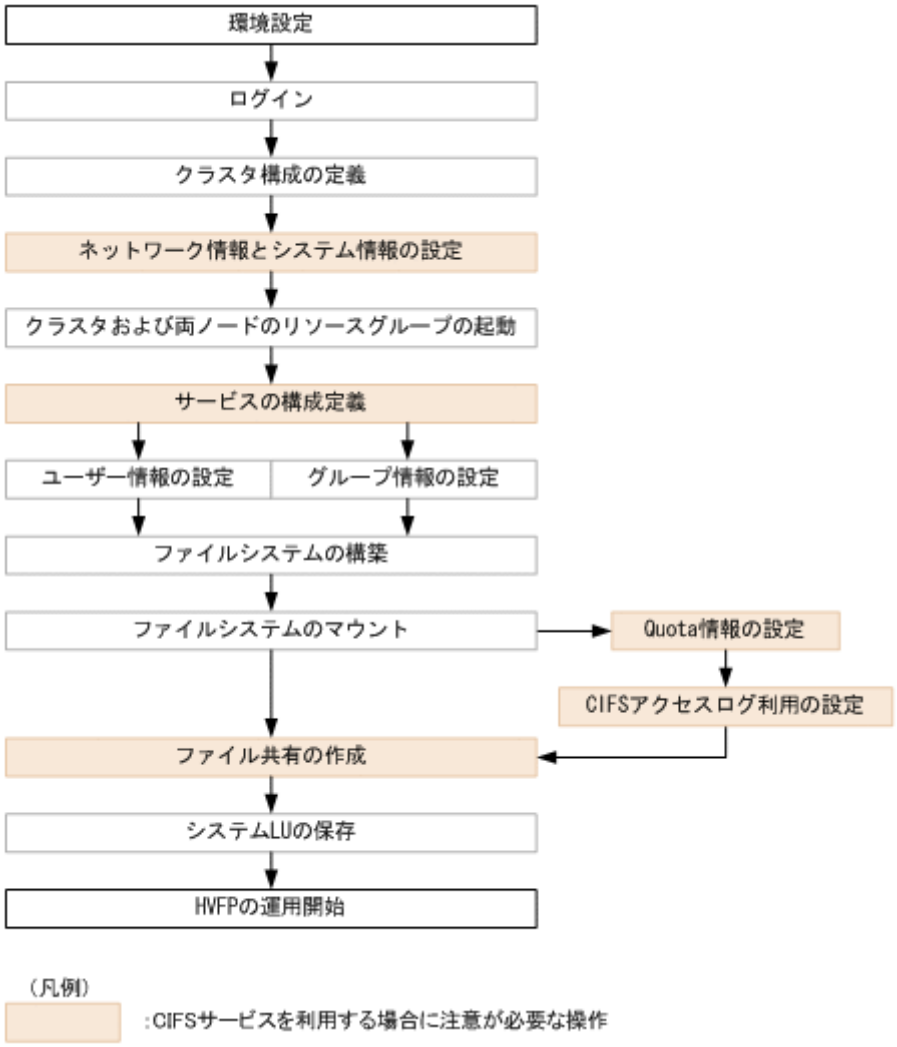
File Services Manager での CIFS サービスの運用

この章では，HVFP を利用するためにシステム管理者が行う運用管理操作の中から，CIFS サービスを利用する場合に注意が必要な操作について説明します。なお，ここでは，File Services Manager の GUI を使用することを前提とします。

3.1 File Services Manager での設定の流れ

システム管理者は，HVFP の運用を開始するために必要な情報を，File Services Manager で設定します。File Services Manager での設定手順を次の図に示します。図で示した操作のうち，このマニュアルでは，CIFS サービスを利用する場合に注意が必要な操作について主に説明します。それ以外の操作については，「ユーザーズガイド」（IF305）を参照してください。

図 3-1： File Services Manager の設定手順



3.2 ネットワーク情報とシステム情報の設定

システム管理者は，［Network & System Configuration］ダイアログの［System Setup Menu］ページから，必要に応じて HVFP の各ノードまたは Virtual Server のインターフェース情報，ネットワーク情報，連携する外部サーバの情報などを設定・変更できます。ここでは，システムファイルを直接編集する際の注意事項を説明します。［System Setup Menu］ページからのそれ以外の設定については，「ユーザーズガイド」（IF305）を参照してください。

3.2.1 システムファイルを直接編集する

システム管理者は，［Network & System Configuration］ダイアログの［Edit System File］ページで HVFP のシステムファイルを直接編集できます。システムファイルを直接編集する方法と設

定内容については，「ユーザーズガイド」（IF305）を参照してください。システムファイルは，クラスタ内のノード間で同じ設定になるよう，ノードごとに設定してください。

ここでは，CIFS サービスを利用する場合に編集するシステムファイルと編集契機を次に示します。

- /etc/hosts
  ノードまたは Virtual Server，および CIFS 共有にアクセスする CIFS クライアントを限定するのにホスト名で指定する場合に編集します。
- /etc/cifs/lmhosts
  CIFS サービスの認証モードが Active Directory 認証で，信頼関係を結んでいるドメインのドメインコントローラーを検索する必要がある場合に編集します。

3.3 サービスの構成定義

システム管理者が管理できる CIFS サービスの内容を次の表に示します。このサービスの管理の詳細については，「ユーザーズガイド」（IF305）を参照してください。

表 3-1： CIFS サービスの管理内容

サービスの種類	サービス名	構成定義の変更	サービスのメンテナンス	起動・停止・再起動
CIFS サービス	CIFS	○	○	○

（凡例）○：できる

3.3.1 CIFS サービスの構成定義の変更

CIFS サービスの構成定義の変更について補足します。

3.3.1.1 CIFS サービスの構成定義の変更

CIFS サービスの構成定義を変更する方法と注意事項については，「ユーザーズガイド」（IF305）を参照してください。ここでは，［Access Protocol Configuration］ダイアログの［CIFS Service Management］ページで CIFS サービスの構成定義を変更する場合の注意事項について補足します。

表 3-2：［CIFS Service Management］ページ（Setting Type：Security）の［CIFS service setup］での注意事項

#	項目	説明および注意事項
1	［Host access restrictions］	ネットワークを指定する場合，次の形式としてください。 IPv4 の場合 ネットワークアドレスを指定する場合 IP アドレスを指定します （例：「10.203.15.0」）。 ネットマスクに従ってネットワークの範囲を指定する場合 ＜ネットワークアドレス＞ / ＜ネットマスク＞ （例：「10.203.15.0/255.255.255.0」） IPv6 の場合 アドレスプレフィックスを指定する場合 IP アドレスを指定します （例：「fe80::223:7dff:0:0」）。 プレフィックス長に従ってネットワークの範囲を指定する場合 ＜アドレスプレフィックス＞ / ＜プレフィックス長＞ （例：「fe80::223:7dff:0:0/64」）

3.3.1.2 認証モードの設定

CIFS サービスでは 3 つの認証モードを選択できます。認証モードの設定方法および注意事項については，「ユーザーズガイド」（IF305）を参照してください。ここでは，認証モードを設定する場合の注意事項について補足します。

表 3-3：CIFS サービスで選択できる認証モードと注意事項

#	認証モード	説明および注意事項
1	Local authentication	［Local Authentication］ページで指定する情報について示します。 ・ ノードまたは Virtual Server が所属するワークグループ名を指定します。 ・ ノードまたは Virtual Server のホスト名と異なる名称を指定してください。ノードまたは Virtual Server のホスト名と同じ名称を指定した場合，ACL を設定したときにグループ名が正しく表示されないおそれがあります。

#	認証モード	説明および注意事項
2	Active Directory authentication	［Active Directory Authentication］ページで指定する情報について示します。 ・［Domain name］には，Active Directory ドメインの DNS 名を指定します。入力した英小文字はすべて英大文字として認識されます。 ドメインコントローラーのポリシーで［ドメインコントローラ：LDAP サーバー署名必須］が［署名を必要とする］になっている場合は，LDAP 通信を署名付きにするように設定していないと，ドメインの参加に失敗します。事前に，cifsoptset コマンドで LDAP 通信を署名付きにするように設定しておいてください。 ・［Domain user name］には，パーセント（%）および単価記号（@）は指定できません。 ユーザー名にこれらの文字を含まないドメインのユーザーを指定してください。 ここで指定したユーザーは，ノードまたは Virtual Server を，Active Directory ドメインに参加，離脱させる際のユーザーアカウントとして使用されます。 指定したユーザーがドメインの管理者権限を持たない一般的なドメインユーザーの場合，以下の制限があります。 ◦ 10 台を超えるサーバ（ここでは HVFP のノードまたは Virtual Server）を Active Directory ドメインに参加させることはできません。ただし，そのユーザーをドメインの Account Operators グループに所属させることによって，10 台を超えるサーバを Active Directory ドメインに参加させることができるようになります。このため，指定したユーザーがすでに 10 台のサーバをドメインに参加させていて，さらにサーバをドメインに参加させる場合は，ドメインの Account Operators グループに所属させていることを事前に確認してください。 ◦ Active Directory ドメインから離脱した際に，ノードまたは Virtual Server のコンピュータアカウントを Active Directory ドメインから削除できません。離脱時に削除するためには，指定してユーザーを以下のいずれかのグループに所属させるか，削除するために必要な権限を設定する必要があります。 ・Domain Admins ・Account Operators ・Enterprise Admins また，設定済みのユーザーをほかのユーザーに変更する場合は，事前に次のどちらかの操作をしてください。 ◦ ドメインコントローラー上で，変更前のユーザーが参加させたノードまたは Virtual Server のコンピュータアカウントを削除する。 ◦ ドメインコントローラー上で，対象のノードまたは Virtual Server のコンピュータアカウントに対して，新たに指定するユーザーの ACL を追加し，次の操作に対する許可を与える。 ・読み取り ・DNS ホスト名への検証された書き込み ・サービスプリンシパル名への検証された書き込み ・パスワードのリセット ・パスワードの変更 ・アカウントの制限の書き込み 注意：次のような設定変更を実施した際に，参加していた Active Directory ドメインから離脱します。 ◦ . 参加する Active Directory のドメインの変更 ◦ . ユーザ認証を Active Directory 認証以外の認証に変更

#	認証モード	説明および注意事項
		・［Domain name (NetBIOS)］に誤った値を入力しても，［Domain name］の値が正しい場合，CIFS サービスの起動・再起動に成功します。この時，ユーザーマッピングを使用する設定で CIFS 共有へアクセスした場合，共有上のファイルに対して ACL の操作を行った時にドメインコントローラーと通信できないなどの問題が発生することがあります。入力する値に注意してください。 ・ HVFP の参加先ドメインのコンピュータアカウントに設定された情報によっては，ドメインへの参加が失敗することがあります。HVFP と同じホスト名のコンピュータアカウントが参加先ドメインに登録されている場合は，次のどちらかの方法で対処したあと，ドメインに参加してください。 ◦ HVFP と同じホスト名のコンピュータアカウントの情報を上書きしないように，HVFP のホスト名を変更してください。 ◦ HVFP と同じホスト名のコンピュータアカウントが存在しないときは，そのコンピュータアカウントをドメインから手動で削除してください。 このほか， Active Directory 認証に関する注意事項については，「5.2 」を参照してください。

3.3.1.3 ユーザーマッピングの設定

ユーザーマッピングを使用するための設定および注意事項については，「ユーザーズガイド」（IF305）を参照してください。

ここでは，ユーザーマッピング方式として［Use user mapping using LDAP.］を選択する際の注意事項について補足します。

この場合，ユーザーマッピング機能では，トランスポート・レイヤー・セキュリティ（TLS）を利用する OpenLDAP サーバは使用できません。

TLS とは，インターネット上で情報を暗号化して送受信するプロトコルです。

3.3.1.4 SMB プロトコルの設定

CIFS アクセスでは，クライアントは SMB というファイル共有プロトコルを使用して HVFP のノードまたは Virtual Server にアクセスします。HVFP では CIFS サービスの構成定義で，使用する SMB プロトコルを選択できます。

クライアントがどの SMB プロトコルでアクセスするかは，CIFS クライアントのプラットフォームと CIFS サービスの構成定義の内容によって，接続時の HVFP とクライアント間のネゴシエーションで決まります。CIFS アクセスでの SMB プロトコルを次に示します。

表 3-4： CIFS アクセスでの SMB プロトコル

CIFS クライアントのプラットフォーム	CIFS サービスの構成定義			
	SMB1.0	SMB2.0	SMB2.1	SMB3.0
Mac OS X v10.5 Mac OS X v10.7 Mac OS X v10.8	SMB1.0	SMB1.0	SMB1.0	SMB1.0
Mac OS X v10.9[*1]	SMB1.0	SMB1.0	SMB1.0	SMB1.0
Mac OS X v10.10[*2] Mac OS X v10.11[*2] macOS v10.12[*2]	－	SMB2.0	－	－
Windows 8.1 Windows Server 2012	SMB1.0	SMB2.0	SMB2.1	SMB3.0

CIFS クライアントのプラットフォーム	CIFS サービスの構成定義			
	SMB1.0	SMB2.0	SMB2.1	SMB3.0
Windows 10[*3] Windows Server 2016 Windows Server 2019	SMB1.0[*4]	SMB2.0	SMB2.1	SMB3.0

（凡例） －：サポートしていない

注＊ 1

SMB1.0 を使用して CIFS アクセスするように，HVFP またはクライアントで事前に設定する必要があります。HVFP または Mac OS X v10.9 クライアントでの設定方法については，「(1) Mac OS X v10.9 の場合」を参照してください。

注＊ 2

SMB2.0 を使用して CIFS アクセスするように，HVFP で事前に設定する必要があります。Mac OS X v10.10，v10.11，および macOS v10.12 クライアントから CIFS アクセスする場合の設定方法については，「(2)Mac OS X v10.10 ，v10.11，または macOS v10.12 の場合」を参照してください。

注＊ 3

Windows 10 を含む SMB3.0 クライアントをご利用になる環境（Windows 10 と，Windows 10 でないクライアントの混在環境を含む）では，本装置の CIFS サービスの設定で SMB3.0 を有効にしてください。

注＊ 4

SMB1.0 を使用して CIFS アクセスする場合は，HVFP またはクライアントで事前に設定うる必要があります。HVFP またはクライアントでの設定方法については，「11.3.4 SMB1.0 で接続する場合」を参照してください。

CIFS サービスの構成定義で使用する SMB プロトコルの設定を変更した場合，変更前から CIFS サービスに接続していた CIFS クライアントはいったんログオフし，ログインし直してください。

なお，SMB 2.0，SMB 2.1 および SMB 3.0 でサポートされる項目のうち，HVFP では次に示す項目をサポートしています。

SMB 2.0

- 1 パケットでの複数コマンドの要求
- バッファーサイズの拡大
- SMB プロトコルが扱えるファイル数や共有数の増加

SMB 2.1

1MB のラージ MTU
なお，CIFS クライアントで 1MB のラージ MTU を有効にする方法については，Microsoft のサポートに問い合わせてください。

SMB 3.0

SMB の暗号化
なお，SMB の暗号化を使用して CIFS クライアントとの通信を暗号化すると，暗号化しない場合と比べて，アクセス性能が低下します。

注意：

SMB の暗号化を有効にした CIFS 共有では，CIFS サービスおよび CIFS 共有の設定に関わらず，クライアントキャッシュは無効になります。

3.3.1.5 自動リロードの設定

CIFS サービスでは，CIFS 共有の設定を変更する際に，設定内容を自動的にリロードするかどうかを設定できます。自動リロードの設定方法および注意事項については，「ユーザーズガイド」を参照してください。ここでは，自動リロードを有効に設定した場合に自動的にリロードする CIFS 共有の設定について補足します。

表 3-5： 自動的にリロードする CIFS 共有の設定

#	設定	備考
1	読み取り専用の設定	設定を変更する場合は，GUI を使用してください。 GUI の詳細については，「ユーザーズガイド」を参照してください。
2	特別に権限設定されたユーザー / グループの設定	
3	ホスト / ネットワークによるアクセス制限の設定	
4	閲覧可能共有の設定	
5	ゲストアカウントアクセスを許可する設定	
6	オーナーだけにアクセス権限を設定する設定	
7	新規ファイルのアクセス権限の設定	
8	新規ディレクトリのアクセス権限の設定	
9	CIFS 共有名の設定	
10	CIFS クライアント向けコメントの設定	
11	ホームディレクトリ自動作成を有効にする設定	
12	ファイルタイムスタンプ変更許可ユーザーの設定	
13	同期書き込みポリシーの設定	
14	Windows クライアントのアクセスポリシーの設定	
15	クライアント側での書き込みバッファリング許可の設定	
16	アクセス競合時に読み取り専用のクライアントキャッシュを使用する設定	
17	アクセスベースの列挙を有効にする設定	
18	Volume Shadow Copy Service を使用する設定	
19	SMB 暗号化の設定	
20	オフライン属性の設定	設定を変更する場合は，cifsedit コマンドを使 用してください。 cifsedit コマンドの詳細については，「コマン ドリファレンス」を参照してください。
21	case_sensitive オプションの設定＊	設定を変更する場合は，cifsoptset コマンドを使用してください。 cifsoptset コマンドの詳細については，「コマンドリファレンス」を参照してください。
22	hide_system_files オプションの設定＊	
23	logging_unsupported_access オプションの設定＊	
24	check_strict_allocate オプションの設定＊	

注＊

-x オプションとともに default を指定した場合は，コマンド実行後，CIFS クライアントでいったんログオフしたあと，ログインし直してください。または，CIFS サービスを再起動してください。

3.4 CIFS 共有管理

ここでは，システム管理者が File Services Manager で CIFS 共有を作成する場合や属性を編集する場合の注意事項について説明します。

3.4.1 CIFS 共有の作成

システム管理者は［共有追加］ダイアログまたは［ファイルシステム構築と共有作成］ダイアログで CIFS 共有を作成できます。CIFS 共有を作成する方法は，「ユーザーズガイド」（IF305）を参照してください。ここでは，CIFS 共有を作成する場合の注意事項について補足します。

CIFS サービスだけでファイルやディレクトリを共有する場合，次のように設定してください。

- 次の GUI の［最終アクセス時刻記録］で［はい］を選択してください。なお，［はい］を選択していない場合でも，Microsoft Excel などのアプリケーションの動作仕様によってファイルを更新した場合にアクセス日時が更新されることがあります。
  ・［ファイルシステム構築と共有作成］ダイアログの［アドバンスド］タブ
  ・［ファイルシステム構築］ダイアログの［アドバンスド］タブ
  ・［ファイルシステムのマウント］ダイアログ
- Classic ACL タイプのファイルシステムの場合，CIFS サービスでファイル所有者以外のユーザーによるファイル更新日時の変更ができるように，次の GUI の［ファイルタイムスタンプ変更許可ユーザー］で［書き込み許可ユーザー］を選択してください。
  ・［ファイルシステム構築と共有作成］ダイアログの［アドバンスド］タブ
  ・［共有追加］ダイアログの［アドバンスド］タブ
  ・［共有編集］ダイアログの［アドバンスド］タブ
  Advanced ACL タイプのファイルシステムの場合，ファイル更新日時の変更は ACL の「属性の書き込み」の権限に依存します。
  なお，Advanced ACL タイプのファイルシステムの場合，常に ACL を操作できます。

CIFS と NFS でファイルやディレクトリを共有する場合，次のことに注意してください。

CIFS サービスで，ファイル所有者以外でのファイル更新日時の変更を許可すると，該当ファイルに書き込み権限のあるすべてのユーザーが CIFS クライアントを経由することでファイル更新日時を変更できます。このファイルの所有者以外のユーザーによるファイル更新日時の変更は，NFS クライアントでは許可されていないため，同一のファイルを CIFS クライアントと NFS クライアントで共有する場合には十分注意してください。

CIFS 共有上のファイルを Microsoft Word ／ Excel ／ PowerPoint で参照・更新する場合は ACL を使用する設定にしてください。

ノードのメモリー量が 64GB 以上の場合，自動リロードを有効にしたときに作成できる CIFS 共有数の上限は 1 クラスタ当たり 1,024 です。CIFS サービスの構成定義で CIFS 共有の設定を自動リロードする設定にしている場合，CIFS 共有を作成したり編集したりすると，CIFS 共有の設定をリロードして，接続中の CIFS クライアントに反映します。CIFS クライアントの接続数が多いときには，リロードによる負荷が高くなり，ファイルアクセスの応答が一時的に遅くなるため，推奨値に従って運用してください。なお，リロード直後のファイルアクセスの応答に最大で 20 秒程度掛かることがあります。

CIFS クライアントの接続数と CIFS 共有数の推奨値を次の表に示します。

表 3-6： CIFS クライアントの接続数と CIFS 共有数の推奨値

CIFS クライアントの接続数	CIFS 共有数
4,800 以下	1,024 以下
4,801 ～ 6,000	768 以下
6,001 ～ 7,200	512 以下
7,201 ～ 9,600	256 以下

注：この推奨値は，ノードのメモリー量が 64GB 以上で CPU 数が 2（12 コア）の場合に，1 つのテキストファイルの読み取りおよび書き込みを，各 CIFS クライアントから 5 分間隔で実施したときの性能を基に算出しています。

3.4.2 CIFS 共有の属性編集

システム管理者は，［共有編集］ダイアログで CIFS 共有の属性を編集できます。CIFS 共有の属性を編集する方法および注意事項は，「ユーザーズガイド」（IF305）を参照してください。ここでは，CIFS 共有の属性を編集する場合の注意事項について説明します。

- 情報を変更しなかった項目については，現在設定されている情報が適用されます。
- CIFS 共有を作成したファイルシステムに差分スナップショットの自動作成スケジュールを設定し，差分スナップショットに自動的にファイル共有を作成して運用する場合，編集した CIFS 共有の情報を基に，差分スナップショットに CIFS 共有が作成されます。

上記に加え，「3.4.1 CIFS 共有の作成」に示す CIFS 共有を作成する際の注意事項もあわせて参照してください。

3.4.3 自動リロード有効時の自動リロード対象項目

自動リロードの対象は，以下となります。

- 共有追加（FSM、cifscreate）
- 共有削除（FSM，cifsdelete）
- FSM の共有編集での［ベーシック］タブ
  - プロトコル（ただし，CIFS 設定が変更されていない場合を除く）
- FSM の共有編集での［アクセス制御］タブ
  - 読み取り専用
  - 権限設定ユーザー / グループ
  - ホスト / ネットワークによるアクセス制御
  - 閲覧可能共有
  - ゲストアクセス許可
  - オーナーだけのアクセス権限
  - 新規ファイル・ディレクトリのアクセス制限
- FSM の共有編集での［アドバンス］タブ
  - 共有名
  - コメント
  - ホームディレクトリ自動作成
  - タイムスタンプ変更許可ユーザー
  - 同期ポリシー
  - アクセスポリシー
  - oplock level1

- oplock level2
- アクセスベースの列挙
- VSS の使用
- SMB 暗号化

・ cifsedit
- オフライン属性

・ cifsoptset（共有単位）
- case_sensitive
- change_notify
- notify_delay_time
- hide_system_files

3.5 Quota 情報の設定

システム管理者は，ファイルシステムごとまたはディレクトリごとに Quota を設定できます。ディレクトリごとに設定する Quota をサブツリー Quota といいます。ファイルシステムごとの Quota は GUI かコマンドで，ディレクトリごとの Quota はコマンドで設定できます。Quota の設定方法については，「ユーザーズガイド」（IF305），「コマンドリファレンス」（IF311）を参照してください。

ここでは，Quota に関する注意事項を説明します。

・ CIFS クライアントは，Windows のプロパティで Quota 情報の詳細を参照できません。Quota 情報の詳細を参照したい場合は，File Services Manager を使用してください。

・ CIFS クライアントでのディスク容量の表示については，「8.6 ディスク容量表示」を参照してください。

・ グループに対してデフォルト Quota を設定できません。

3.6 CIFS アクセスログを利用する

システム管理者や CIFS 管理者は，採取された CIFS アクセスログを参照することで CIFS 共有へのアクセス履歴を確認できます。システム管理者は，CIFS アクセスログを採取するかどうかや採取する契機などを事前に設定する必要があります。

CIFS アクセスログ（`/var/log/cifs/log.CIFSaccess`）は，［Check for Errors］ダイアログの［List of RAS Information］ページ（［List of other log files］表示）で参照できます。［Check for Errors］ダイアログの［List of RAS Information］ページ（［List of other log files］表示）を参照する方法については，「ユーザーズガイド」（IF305）を参照してください。また，ファイルシステム上のディレクトリに最新の CIFS アクセスログを退避することもできます。CIFS アクセスログの退避については，「3.6.4 最新の CIFS アクセスログの退避」を参照してください。

3.6.1 CIFS アクセスログの採取を開始する前に確認しておくこと

CIFS アクセスログの採取を開始する前に次のことを確認してください。

・ CIFS アクセスログを採取する契機は，システム管理者が事前に設定します。CIFS クライアントが CIFS 共有にアクセスしたときの履歴がすべて採取されるわけではなく，CIFS サービスや CIFS 共有ごとの設定によって，CIFS アクセスログが採取される契機が変わります。

- CIFS アクセスログを採取する契機は，CIFS サービスまたは CIFS 共有ごとに設定できます。CIFS サービスと CIFS 共有のどちらにも設定している場合は，CIFS 共有に対して設定した内容が有効となります。
- CIFS アクセスログは，ノード単位で同じファイルに出力され，事前に設定した容量を超えるとローテーションされます。ログファイルの容量と数は変更できます。詳細は，「ユーザーズガイド」（IF305）を参照してください。
- CIFS アクセスログを採取する契機を設定していても，CIFS クライアントからのアクセス方法や，アクセスの成功および失敗の要因によっては，CIFS アクセスログが採取されなかったり，設定とは異なる契機で採取されたりします。
- OS ディスクに保存されたログファイルの容量が上限に達したときに欠落するアクセス履歴は次のとおりです。
  - ログファイルの容量が上限に達した時点で CIFS アクセスログの採取を中止するよう設定していない場合は，古いログファイルが上書きされるため，上書きされたログファイルのアクセス履歴が欠落します。
  - ログファイルの容量が上限に達した時点で CIFS アクセスログの採取を中止するよう設定している場合は，CIFS アクセスログの採取が中止され，以降のアクセス履歴が欠落します。

  ログファイルをファイルシステム上に退避するよう設定することで，アクセス履歴の欠落を防ぐことができます。ファイルシステム上に退避されるログファイルの名称は次のとおりです。
  `cifsaccesslog_` ＜ノードのホスト名＞ `_` ＜ YYYYMMDD ＞ `_` ＜ hhmmss ＞ `.log`
- ファイルシステム上に退避したログファイルを CIFS クライアントから参照する場合，退避先のディレクトリに CIFS 共有を設定し，CIFS 管理者の権限で参照してください。退避したログファイルへの不正なアクセスを防ぐため，CIFS 共有を作成するとき，ユーザーに対して書き込みおよび読み取りを許可しないよう設定することを推奨します。
- OS ディスクまたは Virtual Server OS LU に保存されたログファイルが上書きされる場合，SNMP トラップまたは E-mail で通知されます。CIFS 共有の利用状況によっては，数分に 1 回の間隔で通知されることもあります。ログファイルが上書きされる際に通知される SNMP トラップまたは E-mail を抑止する場合は，上書きされるログファイルがファイルシステムに退避されるよう設定してください。
- 退避先として指定したファイルシステムの容量不足でログファイルを退避できなかった場合，SNMP トラップまたは E-mail で通知されます。CIFS 共有へのアクセス状況によっては，数分に 1 回の間隔で通知されることもあります。ログファイルを退避できなかった際に通知される SNMP トラップまたは E-mail を抑止する場合は，ファイルシステムの使用量が閾値を超えた際に警告を通知するよう設定し，ファイルシステムの使用量を監視してください。

3.6.2 ログファイル容量の見積もり

CIFS アクセスログのログファイルを退避する際，退避先として指定したファイルシステムの容量が不足すると，ログファイルを保存できなくなります。システム管理者は，出力されるログファイルの容量を見積もってから，退避先のファイルシステムの容量を設定してください。また，退避先のファイルシステムから不要となったログファイルを定期的に削除したり移動したりして，計画的に運用してください。

1,000 クライアントが CIFS 共有にアクセスしたときに 1 日に出力されるログファイルの容量を次の表に示します。なお，Virtual Server を利用しないで HVFP を運用している場合を想定しています。出力されるログファイルの容量は，ネットワーク環境や CIFS クライアントのアクセス状況によって異なります。表に示すログファイルの容量を目安として，余裕を持って見積もってください。

表 3-7： 1,000 クライアントがアクセスしたときの CIFS アクセスログのログファイル容量

CIFS アクセスログの設定例	CIFS アクセスログが採取される契機	ログファイル容量（MB/ 日）
CIFS 共有への接続または切断したときの CIFS アクセスログを採取する	CIFS 共有への接続または切断に成功または失敗したとき	20
データの書き込みを伴う操作を実行したときの CIFS アクセスログを採取する	• ファイルの作成またはデータの書き込みに成功または失敗したとき • フォルダの作成に成功または失敗したとき • ファイルまたはフォルダの削除に成功または失敗したとき • ファイルまたはフォルダのアクセス許可の変更に成功または失敗したとき • ファイルまたはフォルダの所有権の変更に成功または失敗したとき • CIFS 共有への接続または切断に成功または失敗したとき	60
すべての CIFS アクセスログを採取する	• フォルダ一覧の表示に成功または失敗したとき • データの読み取りに成功または失敗したとき • ファイルの作成またはデータの書き込みに成功または失敗したとき • フォルダの作成に成功または失敗したとき • ファイルまたはフォルダの削除に成功または失敗したとき • ファイルまたはフォルダのアクセス許可の読み取りに成功または失敗したとき • ファイルまたはフォルダのアクセス許可の変更に成功または失敗したとき • ファイルまたはフォルダの所有権の変更に成功または失敗したとき • CIFS 共有への接続または切断に成功または失敗したとき	410

なお，これらのログファイル容量は，1,000 クライアントが次の操作を実行したときの値です。

1. CIFS 共有内の 1,000 ファイルを dir コマンドで表示します。
   この操作を実行したあと，5 分間休止します。
2. CIFS 共有内の 1 ファイルを同じ CIFS 共有内にコピーします。
   この操作を実行したあと，5 分間休止します。
3. 手順 1. と手順 2. の操作を繰り返します。

3.6.3 CIFS アクセスログに出力される情報

CIFS アクセスログは次の形式で出力されます。

```
＜日付＞,＜時刻＞,＜プロセスID＞,＜ユーザー名＞,＜クライアントホストのIPアドレス＞,［＜CIFS共有名＞］,［＜判定＞］,［＜メッセージテキスト＞］,＜契機＞,［＜詳細＞］,"［＜オブジェクト名＞］"
```

CIFS アクセスログに出力される情報を次に示します。

表 3-8： CIFS アクセスログに出力される情報

項目	説明
日付	イベントが実行された日付が「YYYY/MM/DD」の形式で出力されます。

項目	説明
時刻	イベントが実行された時刻が「hh:mm:ss」の形式で出力されます。
プロセス ID	イベントが実行されたプロセスの ID が出力されます。
ユーザー名	アクセスした CIFS クライアントのユーザー名が出力されます。
クライアントホストの IP アドレス	CIFS クライアントホストの IP アドレスが出力されます。
CIFS 共有名	CIFS 共有名が出力されます。 CIFS 共有が削除されていた場合は出力されません。
判定	アクセスに成功したかどうかが出力されます。 OK アクセスに成功した場合に出力されます。 NG アクセスに失敗した場合に出力されます。
メッセージテキスト	メッセージが出力されます。

項目	説明
契機	CIFS アクセスログが採取された契機が出力されます。 opendir または closedir フォルダ一覧を表示した場合に出力されます。 open または close 次の場合に出力されます。 ◦ データの読み取りを実施した場合 ◦ ファイルの作成およびデータの書き込みを実施した場合 ◦ フォルダを作成した場合 ◦ ファイルまたはフォルダを削除した場合 ◦ ファイルまたはフォルダのアクセス許可の読み取りを実施した場合 ◦ ファイルまたはフォルダのアクセス許可を変更した場合 ◦ ファイルまたはフォルダの所有権を変更した場合 ◦ ファイルまたはフォルダの名称を変更した場合 mkdir フォルダを作成した場合に出力されます。 unlink または rmdir ファイルまたはフォルダを削除した場合に出力されます。 sys_acl_get_file ファイルまたはフォルダのアクセス許可の読み取りを実施した場合に出力されます。 sys_acl_set_file ファイルまたはフォルダのアクセス許可を変更した場合に出力されます。 chown ファイルまたはフォルダの所有権の変更した場合に出力されます。 connect または disconnect CIFS 共有への接続または切断を実施した場合に出力されます。 rename ファイルまたはフォルダの名称を変更した場合に出力されます。 set_owner ファイルまたはフォルダの所有者の設定で，次のどちらかを指定した場合に出力されます。 ◦ BUILTIN/Well-known SID アカウント ◦ SID 解決不可アカウント set_group ファイルまたはフォルダのグループの設定で，次のどちらかを指定した場合に出力されます。次の場合に出力されます。 ◦ BUILTIN/Well-known SID アカウント ◦ SID 解決不可アカウント set_dacl ファイルまたはフォルダの DACL の設定で，次のどちらかを指定した場合に出力されます。 ◦ BUILTIN/Well-known SID アカウント ◦ SID 解決不可アカウント set_sacl ファイルまたはフォルダに SACL を設定しようとした場合に出力されます。アクセスしたユーザーに特権がなく，ファイルまたはフォルダのオープンがエラーになった場合は出力されません。 set_attrib ファイルまたはフォルダのファイル属性の設定で，未サポートの属性が含まれていた場合に出力されます。

項目	説明
詳細	CIFS アクセスログが採取された契機の詳細が出力されます。 O_RDONLY データの読み取りを実施する際に，読み取り専用の属性でファイルを開いた場合に出力されます。 O_WRONLY ファイルの作成およびデータの書き込みを実施する際に，書き込み専用の属性でファイルを開いた場合に出力されます。 O_RDWR ファイルの作成およびデータの書き込みを実施する際に，読み書き用の属性でファイルを開いた場合に出力されます。 E ファイルまたはフォルダにファイル属性を設定する際に，暗号化属性（Encrypted）を指定した場合に出力されます。 C ファイルまたはフォルダにファイル属性を設定する際に，圧縮属性（Compressed）を指定した場合に出力されます。 O ファイルまたはフォルダにファイル属性を設定する際に，オフライン属性（Offline）を指定した場合に出力されます。 T ファイルまたはフォルダにファイル属性を設定する際に，一時ファイル属性（Temporary）を指定した場合に出力されます。 P ファイルまたはフォルダにファイル属性を設定する際に，スパースファイル属性（SparseFile）を指定した場合に出力されます。 L ファイルまたはフォルダにファイル属性を設定する際に，リパースポイント属性（ReparsePoint）を指定した場合に出力されます。 I ファイルまたはフォルダにファイル属性を設定する際に，非インデックス対象ファイル属性（NotContentIndexed）を指定した場合に出力されます。
オブジェクト名	アクセスしたファイル，フォルダ，接続または切断した CIFS 共有，名称変更前後のファイル，フォルダの絶対パスなど，操作対象のオブジェクト名が出力されます。名称変更前後のファイル，フォルダの絶対パスは，＜変更前の絶対パス＞＞＜変更後の絶対パス＞の形式で出力されます。 操作対象のオブジェクトが削除されていた場合は出力されません。

3.6.4 最新の CIFS アクセスログの退避

ここでは，最新の CIFS アクセスログの退避について説明します。

通常，CIFS アクセスログは，OS ディスクに保存されたログファイルの容量が上限に達したときに，事前に設定したファイルシステム上のディレクトリに，自動的に退避されます。ただし，`--save` オプションを指定して `cifslogctl` コマンドを実行すると，ログファイルの容量が上限に達したかどうかに関係なく，最新の CIFS アクセスログを退避できます。

CIFS アクセスログを採取する契機の設定方法については，「ユーザーズガイド」（IF305）および「コマンドリファレンス」（IF311）を参照してください。CIFS アクセスログの退避先を設定する方法および CIFS アクセスログを退避する方法については，「コマンドリファレンス」（IF311）を参照してください。

4

CIFS クライアントのユーザー管理

この章では CIFS クライアントのユーザー管理について説明します。

4.1 ユーザー管理方法

HVFP では，ファイルシステムを利用するユーザーの UID，GID およびパスワードなどのユーザー情報を次の表に示す方法で管理できます。

表 4-1：HVFP でサポートするユーザー管理方法

#	項目	説明
1	File Services Manager	ファイルシステムを利用するユーザーを File Services Manager で管理する場合に，ユーザー情報を登録します。
2	NIS サーバ	ファイルシステムを利用するユーザーを NIS サーバで管理する場合に，ユーザー情報を登録します。*
3	ユーザー認証用 LDAP サーバ	ファイルシステムを利用するユーザーをユーザー認証用 LDAP サーバで管理する場合に，ユーザー情報を登録します。*
4	Active Directory	Active Directory を使用してファイルシステムを利用するユーザーを管理する場合に，次のどちらかの作業を実施します。 ・ File Services Manager，NIS サーバ，ユーザー認証用 LDAP サーバのどれかにユーザー情報を登録する ・ ユーザーマッピングを設定する

注 *

NIS サーバおよびユーザー認証用 LDAP サーバの登録情報を File Services Manager に登録する方法については「4.2.1 NIS サーバまたはユーザー認証用 LDAP サーバの情報の登録」を参照してください。

4.2 ローカルでのユーザー管理

ここでは，NIS サーバまたはユーザー認証用 LDAP サーバに登録されたユーザー・グループを File Services Manager に登録する際に必要な手順について説明します。File Services Manager へのローカルユーザー・グループの登録に関する一般的な方法については，「ユーザーズガイド」（IF305）を参照してください。

4.2.1 NIS サーバまたはユーザー認証用 LDAP サーバの情報の登録

NIS サーバまたはユーザー認証用 LDAP サーバで管理しているユーザーが，ローカル認証を利用して HVFP の CIFS 共有にアクセスする場合，または HVFP の CIFS 共有で ACL 機能を使用する場合は，NIS サーバまたはユーザー認証用 LDAP サーバに登録したユーザーを File Services Manager にも登録する必要があります。

File Services Manager には，NIS サーバまたはユーザー認証用 LDAP サーバに登録されたユーザーを認証する機能がありません。そのため，NIS サーバまたはユーザー認証用 LDAP サーバに登録されたユーザーを認証できるように，File Services Manager に NIS サーバまたはユーザー認証用 LDAP サーバのユーザーを登録するためのスクリプトを準備しています。

また，NIS サーバまたはユーザー認証用 LDAP サーバで管理しているグループを HVFP の CIFS 共有へのアクセスで使用する場合，NIS サーバまたはユーザー認証用 LDAP サーバに登録したグループを File Services Manager に登録したグループとマッピングする必要があります。

File Services Manager には，NIS サーバまたはユーザー認証用 LDAP サーバに登録されたグループを，HVFP で扱う機能がありません。そのため，NIS サーバまたはユーザー認証用 LDAP サーバに登録されたグループを HVFP の CIFS 共有へのアクセスで使用できるように，File Services

Manager に登録したグループと NIS サーバまたはユーザー認証用 LDAP サーバに登録されたグループをマッピングするためのスクリプトを準備しています。

4.2.1.1 機能概要

ユーザー追加・削除の実行手順，およびグループマッピング登録・解除の実行手順を示します。ユーザー追加・削除時は，ユーザー情報を記録した CSV ファイルを使用します。同様に，グループマッピング登録・解除時は，マッピング情報を記録した CSV ファイルを使用します。これらの CSV ファイルのフォーマットに関しては，「4.2.1.2 CSV ファイルフォーマット」を参照してください。

(a) ユーザー追加・削除時の実行手順

NIS サーバまたはユーザー認証用 LDAP サーバで管理しているユーザーが HVFP の CIFS 共有にアクセスする場合，NIS サーバまたはユーザー認証用 LDAP サーバに登録したユーザーを File Services Manager に登録する必要があります。NIS サーバまたはユーザー認証用 LDAP サーバに登録したユーザーを File Services Manager に登録する手順を次に示します。

- ここで登録するユーザーは，CIFS 共有へのアクセス時に使用されます。
- パスワードは，CIFS 共有へのアクセス時にローカル認証で使用されます。

1. CIFS 共有を作成します（アクセスできるクライアントを制限します）。
   手順 2 で，暗号化されていないパスワードを，ファイルに保存する必要があります。そのため，ほかのユーザーから参照されないように，作成する CIFS 共有へのアクセスを制限することを強く推奨します。
2. CSV ファイルを手順 1 で作成したディレクトリに保存します。
   保存する CSV ファイルに対してはウイルスチェックを実施し，問題ないことを確認してください。
3. SSH で HVFP のノードまたは Virtual Server にログインします。
4. スクリプトを実行（`sudo cifsusredit`）して，ユーザーの登録・削除・参照を行います。
5. HVFP のノードまたは Virtual Server からログアウトします。
6. CSV ファイル（手順 2 で保存したファイル）を削除し，共有ディレクトリ（手順 1 で作成したディレクトリ）を削除します。
7. クラスタを構成しているほかのノードに対して同様に手順 1 ～手順 6 を実行します。

(b) グループマッピング登録・解除の実行手順

NIS サーバまたはユーザー認証用 LDAP サーバで管理しているグループを HVFP の CIFS 共有へのアクセスで使用する場合，NIS サーバまたはユーザー認証用 LDAP サーバに登録したグループを File Services Manager に登録したグループとマッピングする必要があります。NIS サーバまたはユーザー認証用 LDAP サーバに登録したグループを File Services Manager にマッピングする手順を次に示します。なお，ここで登録するマッピングは，CIFS 共有資源の ACL で使用されます。

1. CIFS 共有を作成します。
   作成する CIFS 共有へのアクセスを制限することを強く推奨します。
2. CSV ファイルを手順 1 で作成したディレクトリに保存します。
   保存する CSV ファイルは，ウイルスチェックを実施してください。
3. SSH で HVFP のノードまたは Virtual Server にログインします。

4. スクリプトを実行（sudo cifsgrpedit）して，グループマッピングの登録・削除・参照を行います。
5. HVFP のノードまたは Virtual Server からログアウトします。
6. CSV ファイル（手順 2 で保存したファイル）を削除します。
7. クラスタを構成しているほかのノードに対して同様に手順 1 ～手順 6 を実行します。

4.2.1.2 CSV ファイルフォーマット

データファイルは，コンマ（,）区切りの CSV ファイル形式で記述します。CSV ファイルフォーマットを次のとおりとします。

- フィールドをコンマ（,）で区切り，各フィールドの前後に空白を空けてはいけません。空白を使用した場合は，空白はフィールドの値と解釈されます。
  例：CSV ファイルにエントリーを記述する場合

```
フィールド1-1,フィールド1-2
フィールド2-1,フィールド2-2
フィールド3-1,フィールド3-2
```

- フィールドの値に引用符（"）を含む場合は，引用符（"）の前に引用符（"）を記述し，さらにフィールド全体を引用符（"）で囲みます。
  例：「フィールド 1, フィールド "2"」を記述する場合

```
フィールド1,"フィールド""2"""
```

- フィールドの値にコンマ（,）を含む場合は，フィールド全体を引用符（"）で囲みます。
  例：「フィールド 1, フィールド ,2」を記述する場合

```
フィールド1,"フィールド,2"
```

- 行の終端には，改行を入れます。

(a) ユーザー登録ファイルのフォーマット

ユーザー登録ファイルのフォーマットを次に示します。1 行には 1 ユーザーの情報だけを記述します。複数ユーザーを指定する場合は，複数行にわたって記述します。

```
ユーザー名,パスワード
ユーザー名,パスワード
ユーザー名,パスワード
```

(b) グループマッピングのフォーマット

グループマッピングファイルのフォーマットを次に示します。1 行には 1 グループのマッピング情報だけを記述します。複数グループを指定する場合は，複数行にわたって記述します。

```
NISサーバなどの外部グループ名,File Services Managerに登録するグループ名
NISサーバなどの外部グループ名,File Services Managerに登録するグループ名
NISサーバなどの外部グループ名,File Services Managerに登録するグループ名
```

- グループマッピングで使用できない文字
  次に示す文字を使用した場合，正常に動作しません。
  ¥/[]:|<>+=;,?*"

4.2.1.3 CIFS ユーザー登録・削除・参照用スクリプトの仕様

ユーザー登録・削除・参照用のスクリプトについて説明します。

名称

```
cifsusredit
```

構文

```
sudo cifsusredit option [csv-file]
```

機能説明

CIFS ユーザーの登録，削除または参照を行います。

引数

option

次のどれかを指定します。それぞれの動作について次に示します。この引数は指定必須です。

・add

指定された csv-file に記述されたユーザーを，File Services Manager に登録します。option が add の場合，csv-file 引数は指定必須です。実行結果を，標準出力に出力します。

・delete

指定された csv-file に記述されたユーザーを，File Services Manager から削除します。option が delete の場合，csv-file 引数は指定必須です。実行結果を，標準出力に出力します。

・list

File Services Manager に登録されたユーザー名を，標準出力に出力します。

csv-file

ユーザーの情報が記述された CSV ファイルを指定します。

戻り値

CSV ファイルに指定されたユーザーの登録・削除がすべて正常終了した場合は 0，異常終了した場合は 0 以外の値が返却されます。

注意事項：

- 「csv-file」は CIFS 共有ディレクトリに保存した CSV ファイルの名前です。「Shared Directory」のディレクトリ：「/mnt/test1/test1」に，CSV ファイル：「file.csv」を保存した場合，コマンドの引数には `/mnt/test1/test1/file.csv` と指定します。この引数は，option 引数に add または delete を指定した場合に指定しなければなりません。
- ユーザー名とパスワードを記述した CSV ファイルを CIFS 共有ディレクトリに保存する際は，ほかのクライアントマシンからアクセスできないように，共有ディレクトリにアクセス制限をしてください。
- このコマンド実行後は，ユーザー名とパスワードを記述した CSV ファイルを速やかに削除してください。
- CSV ファイルに指定するユーザー名は，NIS サーバまたはユーザー認証用 LDAP サーバに登録されたユーザー名を指定してください。
- すでに File Services Manager に登録されているユーザー名を CSV ファイルに指定した場合，CSV ファイルに指定されたパスワードで上書きされます。
- 使用できる改行コードは，LF または CR+LF です。
- 2 バイトコードは指定しないでください。2 バイトコードが指定された場合の動作は保証できません。

4.2.1.4 CIFS グループマッピングスクリプトの仕様

グループマッピング用のスクリプトについて説明します。

名称

```
cifsgrpedit
```

構文

```
sudo cifsgrpedit option [csv-file]
```

機能説明

NIS サーバまたはユーザー認証用 LDAP サーバに登録されたグループを，HVFP のグループとして使用するためのコマンドです。

引数

option

次のどれかを指定します。それぞれの動作について次に示します。この引数は指定必須です。

・add

指定された csv-file に記述されたグループのマッピング情報を，File Services Manager に登録します。option が add の場合，csv-file 引数は指定必須です。実行結果を，標準出力に出力します。

・delete

指定された csv-file に記述されたグループのマッピング情報を，File Services Manager から削除します。option が delete の場合，csv-file 引数は指定必須です。実行結果を，標準出力に出力します。

・list

File Services Manager に登録されたグループ名を，標準出力に出力します。

csv-file

グループマッピングの情報が記述された CSV ファイルを指定します。

戻り値

CSV ファイルに指定されたグループのマッピングがすべて正常終了した場合は 0，異常終了した場合は 0 以外の値が返却されます。

注意事項：

- 「csv-file」は CIFS 共有ディレクトリに保存した CSV ファイルの名前です。「Shared Directory」のディレクトリ：「/mnt/test1/test1」に，CSV ファイル：「file.csv」を保存した場合，コマンドの引数には `/mnt/test1/test1/file.csv` と指定します。この引数は，option 引数に add または delete を指定した場合に指定しなければなりません。
- CSV ファイルに指定するグループ名は，NIS サーバまたはユーザー認証用 LDAP サーバに登録されたグループ名を指定してください。
- すでに File Services Manager に登録されているグループ名を CSV ファイルに指定した場合，グループマッピングが失敗します。
- 使用できる改行コードは，LF または CR+LF です。
- 2 バイトコードは指定しないでください。2 バイトコードが指定された場合の動作は保証できません。

4.2.1.5 NIS サーバまたはユーザー認証用 LDAP サーバで管理しているユーザーに関する注意事項

NIS サーバまたはユーザー認証用 LDAP サーバで管理しているユーザーが HVFP の CIFS 共有にアクセスしたり，HVFP の CIFS 共有で ACL 機能を使用したりする場合，ユーザー登録時に設定したコメントが ACL の表示に使用されます。

4.2.2 ローカルユーザー・グループ登録時の注意事項

ローカルユーザー・グループ登録時の注意事項を次に示します。

- CIFS アクセスをするユーザーで，1 人のユーザーが所属することのできるグループ数は主グループを含めて最大で 1,023 グループになります。1,023 を超えるグループにユーザーを所属させる場合は，ユーザーマッピングを使用する設定にしてください。
- Windows ビルトインユーザー・グループと同名のローカルユーザー・グループを File Services Manager に登録した場合，Windows ビルトインユーザー・グループと見なされることで，これらのローカルユーザー・グループを CIFS クライアントから ACL や所有者として設定できないことがあります。
- HVFP のホスト名を変更した場合，または Virtual Server 運用で Virtual Server 名を変更した場合，CIFS クライアントからのアクセス時にローカルユーザーの認証に時間がかかることがあります。この場合，ローカルユーザー・グループを削除して，削除前と同じユーザー・グループの情報を指定してローカルユーザー・グループを再作成してください。
- 設定ウィザードで作成した運用テスト用のユーザーでアクセスした場合，CIFS クライアントからの認証に時間がかかることがあります。そのため，新しく作成したローカルユーザー・グループでアクセスしてください。

4.3 ドメインでのユーザー管理

ユーザーマッピングを利用する場合，次の点に注意してください。

- Windows ビルトイン ユーザー・グループは HVFP では認識されません。
- Windows のネストしたグループは，Active Directory ドメインが Native mode である場合には，HVFP 上で有効となります。

ユーザーマッピングを利用しない場合，次の点に注意してください。

- ユーザーに対するグループは，File Services Manager や NIS などに登録されたグループが有効になります。ドメインコントローラー上のグループは有効になりません。

4.4 ユーザーマッピング用 LDAP サーバの構築

［Use user mapping using LDAP.］方式のユーザーマッピングを利用する場合，ユーザーマッピング用の LDAP サーバを構築する必要があります。HVFP でのユーザーマッピング用 LDAP サーバのサポート状況を表 4-2： HVFP でのユーザーマッピング用 LDAP サーバのサポート状況に示します。

ここでは，OpenLDAP を使用してユーザーマッピング用 LDAP サーバを構築するときの注意事項と設定例について説明します。

表 4-2：HVFP でのユーザーマッピング用 LDAP サーバのサポート状況

LDAP サーバ		サポート状況
Open LDAP	Linux	○
	Solaris	○

（凡例）○：サポートしている

4.4.1 LDAP サーバを構築するときの注意事項

LDAP サーバを初期化した場合，または LDAP サーバを再構築した場合は，CIFS サービスの再起動が必要となります。CIFS 共有にアクセスしているユーザーがいないことを確認してから，CIFS サービスを再起動してください。

また，再起動後，CIFS サービス環境にキャッシュされているユーザーマッピング情報を削除してください。

4.4.2 OpenLDAP を使用して LDAP サーバを構築するときの注意事項

ここでは，OpenLDAP を使用して LDAP サーバを構築するときの注意事項を説明します。

なお，ユーザーマッピング機能では，トランスポート・レイヤー・セキュリティ（TLS）を利用する OpenLDAP サーバは使用できません。TLS とは，インターネット上で情報を暗号化して送受信するプロトコルです。

OpenLDAP の LDAP サーバでは，検索する最大数（LDAP クライアントからの検索要求に対して返すエントリー数）が指定できます。

- デフォルトは 500 エントリーです。
- LDAP サーバに格納されたユーザー情報やユーザーマッピング情報のエントリー数が最大数を超えると，［Check for Errors］ダイアログの［List of RAS Information］ページ（［Batch-download］表示）でユーザーマッピング情報のダウンロードに失敗したり，［Edit Quota］ダイアログの［List of Quota Information］ページなどで一覧を表示できなかったりします。また，［ファイルシステム構築と共有作成］ダイアログ，［共有追加］ダイアログまたは［共有編集］ダイアログの［アクセス制御］タブで，［特別に権限設定されたユーザー / グループ］の［全ユーザー］や［全グループ］が正しく表示されません。そのため，LDAP サーバの定義に次の sizelimit ディレクティブを追加してください。

  ```
  sizelimit -1
  ```

4.4.3 OpenLDAP を使用して LDAP サーバを構築するときの設定例

ここでは，OpenLDAP を使用して LDAP サーバを構築するときの設定例を示します。

4.4.3.1 スキーマファイルの作成

LDAP 方式のユーザーマッピングを利用する場合に，OpenLDAP で構築した LDAP サーバで認識する属性，オブジェクトクラスを定義したスキーマファイルを作成します。LDAP サーバでは，ユーザーマッピングで変換したユーザー ID およびグループ ID を格納するために，属性とオブジェクトクラスを定義する必要があります。

HVFP では，ユーザーマッピングを利用するために必要なスキーマファイル（samba.schema）を提供しています。リモートホストから scp コマンドを使用して次のディレクトリから取得してください。

```
/usr/share/doc/cifs/examples/samba.schema
```

なお，OpenLDAP を使用して構築した LDAP サーバのスキーマファイルを作成する場合は，次に示す属性，オブジェクトクラスを定義してください。

```
attributetype ( 1.3.6.1.4.1.7165.2.1.20 NAME 'sambaSID'
        DESC 'Security ID'
        EQUALITY caseIgnoreIA5Match
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.26{64} SINGLE-VALUE )
objectclass ( 1.3.6.1.4.1.7165.2.2.7 NAME 'sambaUnixIdPool' SUP top AUXILIARY
        DESC 'Pool for allocating UNIX uids/gids'
        MUST ( uidNumber $ gidNumber ) )
objectclass ( 1.3.6.1.4.1.7165.2.2.8 NAME 'sambaIdmapEntry' SUP top AUXILIARY
        DESC 'Mapping from a SID to an ID'
        MUST ( sambaSID )
        MAY ( uidNumber $ gidNumber ) )
objectclass ( 1.3.6.1.4.1.7165.2.2.9 NAME 'sambaSidEntry' SUP top STRUCTURAL
        DESC 'Structural Class for a SID'
        MUST ( sambaSID ) )
```

スキーマファイルを作成，または取得したあと，このユーザーマッピングを利用するためのスキーマファイルを読み込むためには，LDAP サーバの定義に include ディレクティブを追加してください。

/etc/ldap/schema の下にスキーマファイルを格納した場合の include ディレクティブの記述例を次に示します。

```
include /etc/ldap/schema/samba.schema
```

4.4.3.2 index ディレクティブの設定

OpenLDAP を使用して構築した LDAP サーバに格納するユーザー ID，グループ ID の数が多くなると，LDAP サーバの検索の性能が低くなるおそれがあるので，index ディレクティブを設定してください。ユーザーマッピングを利用する場合，LDAP サーバの定義で index ディレクティブを次のように設定することを推奨します。

```
index uidNumber,gidNumber,objectClass,sambaSID eq
```

- index ディレクティブを変更した場合，LDAP サーバのデータベースの現在の内容を基に索引を再作成する必要があります。OpenLDAP が提供する slapindex コマンドを使用して索引を再作成してください。
- slapindex コマンドを実行する場合，いったん LDAP サーバを停止し，slapindex コマンドを実行したあとに LDAP サーバを再起動してください。

4.5 ユーザー ID・グループ ID の手動登録

ここでは，ユーザーマッピング使用時に任意のユーザー ID・グループ ID を手動で登録する際の手順について説明します。

4.5.1 Active Directory に登録するときの手順

ユーザーマッピング方式として［Use user mapping using Active Directory schema.］を選択している場合，Active Directory のユーザー管理画面から，任意のユーザー ID・グループ ID を手動登録する必要があります。

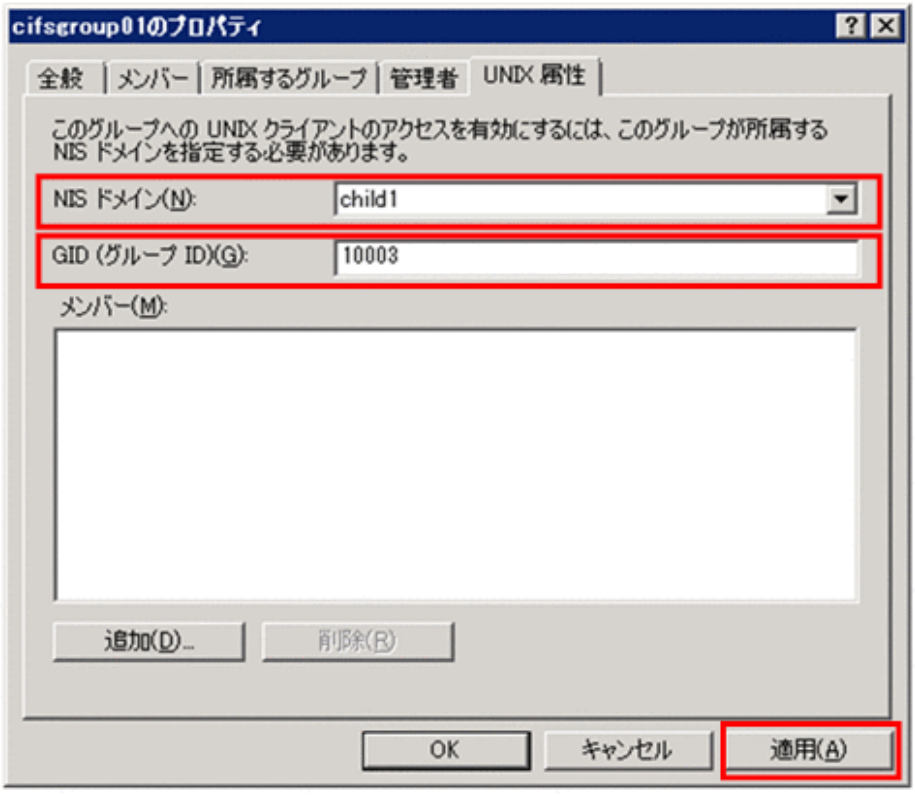
ここでは，その手順について説明します。

4.5.1.1 グループ ID を登録する

グループ ID を手動登録する手順を次に示します。

1. ドメインコントローラーの［Active Directory ユーザーとコンピュータ］画面で，対象のグループの［プロパティ］画面を開きます。
2. ［UNIX 属性］タブを選択します。
3. ［NIS ドメイン］のプルダウンメニューから該当するものを選択します。
4. ［GID (グループ ID)］のテキストボックスの内容を任意のグループ ID に変更します。
5. ［適用］ボタンをクリックします。

図 4-1： グループの［プロパティ］画面の［UNIX 属性］タブの表示例



4.5.1.2 ユーザー ID を登録する

ユーザー ID を手動登録する手順を次に示します。

1. ドメインコントローラーの［Active Directory ユーザーとコンピュータ］画面で，対象のユーザーの［プロパティ］画面を開きます。
2. ［所属するグループ］タブで，プライマリーグループが UNIX 属性の GID を持つグループであること確認してください。

3. ［UNIX 属性］タブを選択します。
4. ［NIS ドメイン］のプルダウンメニューから該当するものを選択します。
5. ［UID］のテキストボックスの内容を任意のユーザー ID に変更します。
6. ［プライマリ グループ名 /GID］のプルダウンメニューから，該当するプライマリーグループを選択します。
7. ［適用］ボタンをクリックします。

図 4-2：ユーザーの［プロパティ］画面の［所属するグループ］タブの表示例

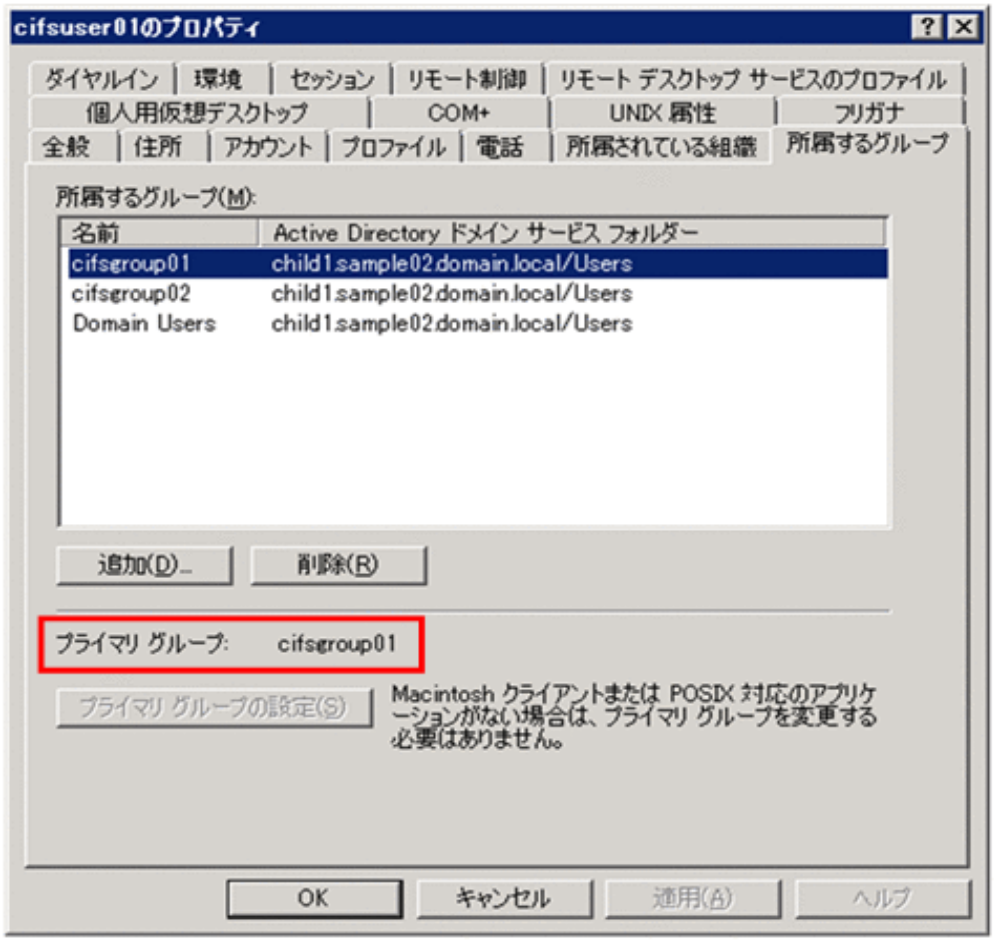
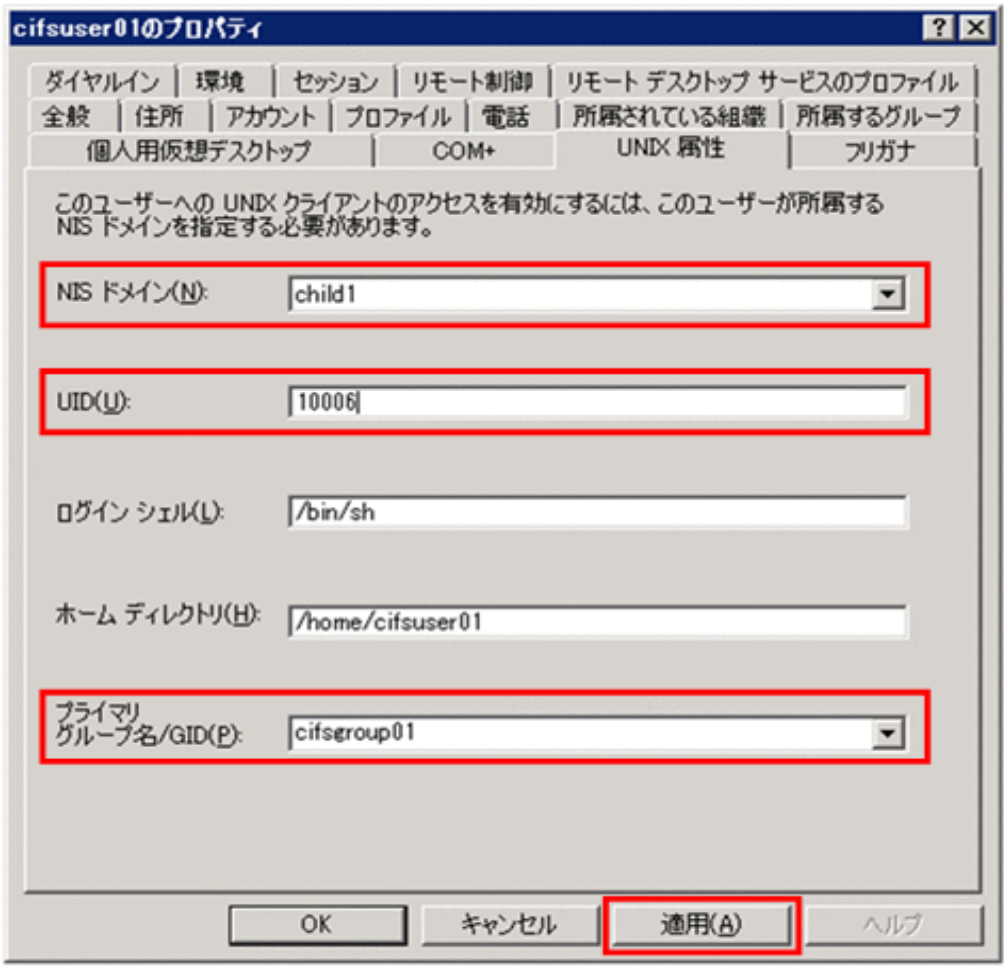


図 4-3：ユーザーの［プロパティ］画面の［UNIX 属性］タブの表示例



4.5.2 LDAP サーバに登録するときの手順

ユーザーマッピング方式として［CIFS Service Management］ページ（Setting Type：User mapping）の［Use user mapping using LDAP.］を選択しており，かつ，［Allocate manually］を選択している場合，LDAP サーバに任意のユーザー ID・グループ ID を手動登録する必要があります。

ここでは，その手順について説明します。

注意：

LDAP サーバに ID を手動登録後，ID の割り当て方式を［Allocate manually］から［Allocate automatically］に変更すると，自動割り当てによってユーザーマッピング情報が重複するおそれがあるため，変更しないでください。

4.5.2.1 グループ ID を登録する

グループ ID を手動登録する手順を次に示します。

1. LDAP サーバ上に，対象のグループの情報を次の形式で記したファイルを用意します。

```
dn: sambaSID=<Active DirectoryのグループのSID>,<ユーザーマッピング用LDAPのDN>
objectClass: sambaIdmapEntry
objectClass: sambaSidEntry
gidNumber: <グループに割り当てるUNIX属性のGID>
sambaSID: <Active DirectoryのグループのSID>
```

（例）

```
dn: sambaSID=S-1-5-21-848980995-581375927-1041525310-53490,dc=test,dc=local
objectClass: sambaIdmapEntry
objectClass: sambaSidEntry
gidNumber: 200000
sambaSID: S-1-5-21-848980995-581375927-1041525310-53490
```

2. 次の形式で ldapadd コマンドを実行します。

```
ldapadd -f <グループ情報を記したファイル名> -x -D "<LDAP管理者の共通名>,<ユーザーマッピング用LDAPのDN>" -w <LDAP管理者のパスワード>
```

（例）

```
ldapadd -f entries.ldif -x -D "cn=Manager,dc=test,dc=local" -w adminpass
```

4.5.2.2 ユーザー ID を登録する

ユーザー ID を登録する手順を次に示します。

1. LDAP サーバ上に，対象のユーザーの情報を次の形式で記したファイルを用意します。

```
dn: sambaSID=<Active Directoryのユーザーの SID>,<ユーザーマッピング用LDAPのDN>
objectClass: sambaIdmapEntry
objectClass: sambaSidEntry
uidNumber: <ユーザーに割り当てるUNIX属性のUID>
sambaSID: <Active Directoryのユーザーの SID>
```

（例）

```
dn: sambaSID=S-1-5-21-848980995-581375927-1041525310-53491,dc=test,dc=local
objectClass: sambaIdmapEntry
objectClass: sambaSidEntry
uidNumber: 200001
sambaSID: S-1-5-21-848980995-581375927-1041525310-53491
```

2. 次の形式で ldapadd コマンドを実行します。

```
ldapadd -f <ユーザー情報を記したファイル名> -x -D "<LDAP管理者の共通名>,<ユーザーマッピング用LDAPのDN>" -w <LDAP管理者のパスワード>
```

（例）

```
ldapadd -f entries.ldif -x -D "cn=Manager,dc=test,dc=local" -w adminpass
```

4.5.3 LDAP サーバに登録した ID を削除するときの手順

ここでは，LDAP サーバに登録したユーザー ID・グループ ID を削除する手順を示します。

1. LDAP サーバ上で，次の形式で ldapdelete コマンドを実行します。

```
ldapdelete -x -D "<LDAP管理者の共通名>,<ユーザーマッピング用LDAPのDN>"
"sambaSID=<Active Directoryのユーザーの SID>,<ユーザーマッピング用LDAPの組織単位名>,<ユーザーマッピング用LDAPのDN>" -w <LDAP管理者のパスワード>
```

（例）

```
ldapdelete -x -D "cn=Manager,dc=test,dc=local" "sambaSID=S-1-5-21-848980995-581375927-1041525310-53491,ou=idmap,dc=test,dc=local" -w adminpass
```

2. File Services Manager の［Access Protocol Configuration］ダイアログの［CIFS Service Maintenance］ページで［Clear User Map Cache File］ボタンをクリックして，キャッシュファイルを削除します。

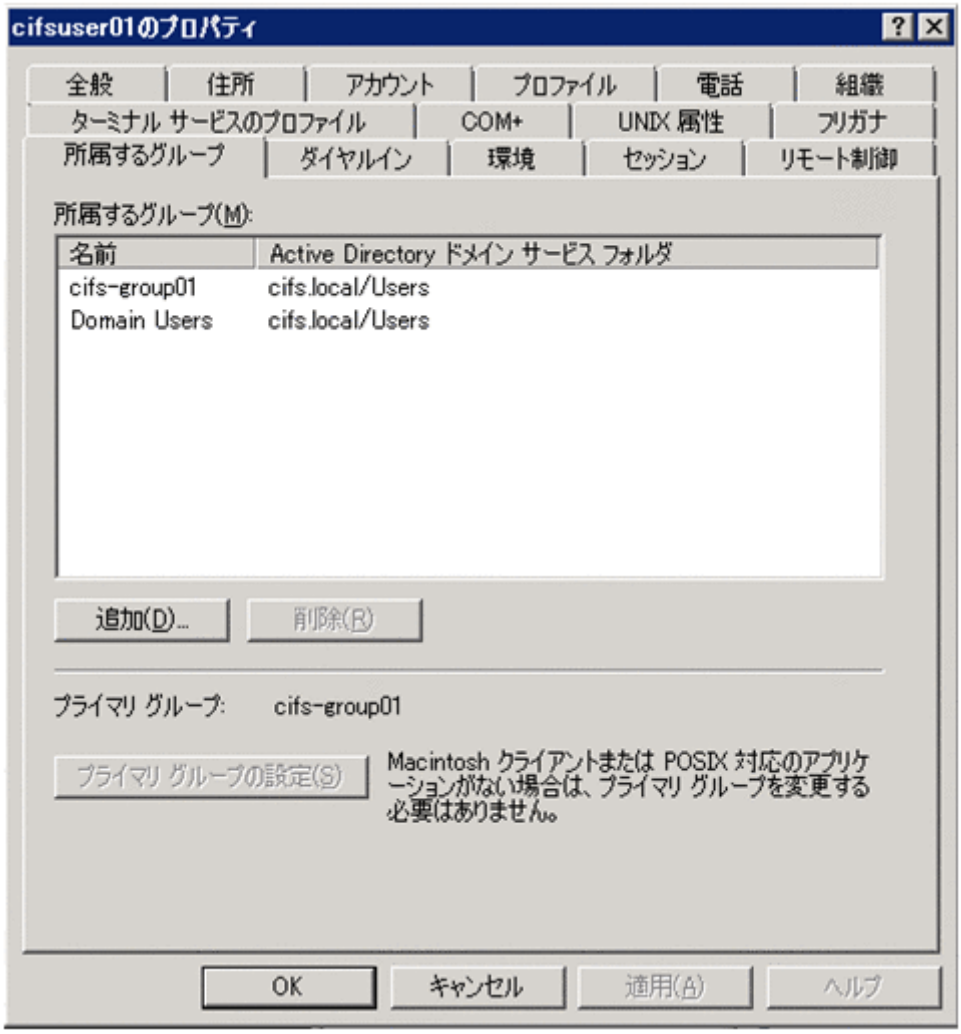
4.6 RFC2307 スキーマを使用する場合のユーザー管理について

ここでは，ユーザーマッピングの方式が Active Directory スキーマ方式で，かつ［CIFS Service Management］ページ（Setting Type：User mapping）の［User mapping setup］で［Name service switch］に［Using LDAP as a network information service (RFC2307)］を指定してユーザーを管理する場合について補足説明します。

HVFP では，CIFS クライアントが CIFS 共有にアクセスする際に使用するドメインユーザーの UNIX 属性のうち，プライマリーグループのグループ ID として使用する UNIX 属性値を，次の 2 つから選択することができます。

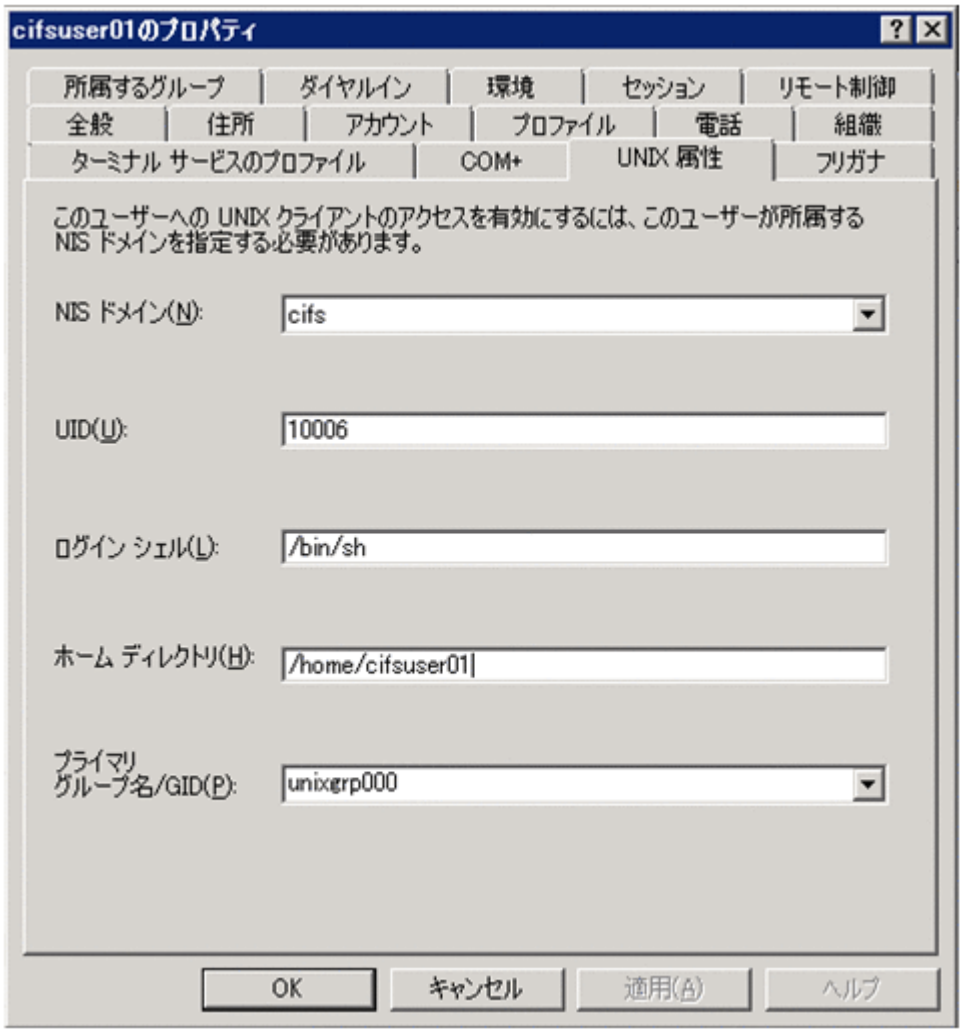
- ユーザーが属するグループ（UNIX 属性の `primaryGroupID` が示すグループ）の `gidNumber` の値
  Active Directory のユーザーのプロパティ画面の［所属するグループ］タブ下部の［プライマリ グループ］に表示されるグループ（次の図に示す例では cifs-group01）に対応するものです。

図 4-4：［所属するグループ］タブの表示例



- ユーザー自身の gidNumber の値
  Active Directory のユーザーのプロパティ画面の［UNIX 属性］タブの［プライマリグループ名 /GID］に表示されるグループ（次の図に示す例では unixgrp000）に対応するものです。

図 4-5：［UNIX 属性］タブの表示例



HVFP は，CIFS クライアントが CIFS 共有にアクセスする際のグループとして，デフォルトでは前者の「ユーザーが属するグループの gidNumber の値」を使用して動作しますが，後者の「ユーザー自身の gidNumber の値」を使用して動作させるには，use_gidnumber オプションを指定して cifsoptset コマンドを実行し，CIFS サービスの設定を変更する必要があります。

4.7 複数ドメインから HVFP を利用している場合のアクセス

ノードまたは Virtual Server が参加しているドメインと信頼関係を結んだドメインに所属しているユーザーも HVFP の CIFS 共有にアクセスできます。HVFP を利用できるドメインの範囲については，「システム構成ガイド」（IF302）を参照してください。ドメインの構成を変更すると，CIFS 共有へのアクセスに時間が掛かることがあります。システム管理者は，ドメイン管理者からドメインの構成変更について連絡を受けたあと，変更されたドメイン構成に合わせて CIFS サービスの構成定義を変更してください。CIFS サービスの構成定義の変更については，「ユーザーズガイド」（IF305）を参照してください。

5

CIFS クライアントのユーザー認証

この章では，CIFS クライアントのユーザー認証に関する注意事項について説明します。

5.1 Local authentication

Windows に共通の注意事項だけです。詳細は，「11.1 Windows に共通すること」を参照してください。

5.2 Active Directory authentication

ここでは，Windows に共通すること以外の注意事項について説明します。Windows に共通の注意事項については，「11.1 Windows に共通すること」を参照してください。

ユーザーマッピングを使用しないで Active Directory 認証をする場合は，File Services Manager，NIS サーバまたはユーザー認証用の LDAP サーバで，ドメインコントローラーに登録されているユーザーと同じユーザーを登録しておく必要があります。グループについては，ドメインコントローラーに登録されているグループ名称と異なる名称を登録しても問題ありません。ただし，異なる名称を登録すると，ACL を参照または設定する場合に，ドメインコントローラーに登録されているグループ名称と File Services Manager，NIS サーバまたはユーザー認証用の LDAP サーバで登録してあるグループ名称を対応付ける必要があるため，同じ名称で登録することを推奨します。

逆にユーザーマッピングを使用する場合は，ドメインコントローラーに登録されているユーザーおよびグループと同じ名称のユーザーおよびグループを File Services Manager，NIS サーバまたはユーザー認証用の LDAP サーバで登録しないでください。ドメインコントローラーと同じユーザーおよびグループ名称を，ユーザーマッピングで割り当てられたユーザー ID およびグループ ID と異なる ID を使用して File Services Manager，NIS サーバまたはユーザー認証用の LDAP サーバで登録した場合，CIFS クライアントから CIFS 共有にアクセスしたときに，ユーザーマッピングで割り当てられたユーザー ID およびグループ ID ではなく，File Services Manager，NIS サーバまたはユーザー認証用の LDAP サーバ上のユーザー ID またはグループ ID でフォルダおよびファイルが作成されることがあります。File Services Manager，NIS サーバまたはユーザー認証用の LDAP サーバ上のユーザー ID もしくはグループ ID でフォルダおよびファイルが作成されるのは，ユーザー ID またはグループ ID が設定された範囲を超えた場合や，ユーザーマッピング用の LDAP サーバの障害などで，ユーザー ID またはグループ ID の割り当てができなかった場合です。

ユーザーマッピングを使用しないで Active Directory 認証をする場合は，File Services Manager で作成された共有ディレクトリへのアクセス時に複数の Active Directory ドメインと信頼関係があっても，CIFS クライアントは，ノードまたは Virtual Server が参加しているドメインに対してログオンする必要があります。

認証時に指定するユーザー名，File Services Manager の GUI やコマンドで指定するユーザー名またはグループ名に，Active Directory のアカウントを指定する場合は，Active Directory のアカウントのプロパティで［Windows2000 より前］に表示されている名称を指定してください。なお，使用している Windows のバージョンによっては項目名が異なることがあります。

Active Directory 認証でユーザーマッピングを使用した場合に，CIFS クライアントからの共有アクセス時に認証に失敗したときは，表 5-1 に示す内容を確認してください。

Active Directory 認証をする場合で次のときには，ドメイン側のノードまたは Virtual Server の情報と，ノードまたは Virtual Server 側のドメイン構成の情報が不一致になって，認証に失敗することがあります。この場合，CIFS クライアントが CIFS 共有に接続できない状態を回復するためには，ノードまたは Virtual Server を Active Directory ドメインに再度参加させてください。

- ドメインコントローラーで障害が発生した
- ドメイン構成を変更した

- ノードまたは Virtual Server の構成を変更した（ノード上の OS の新規インストールや障害発生時の CIFS 設定の復元など）
- ドメインコントローラーで HVFP のコンピュータアカウントを変更または削除した

また、システム設定情報を保存してから次の操作を実施した場合も，システム LU または Virtual Server OS LU を回復したあと，ノードまたは Virtual Server を Active Directory ドメインに再度参加させてください。

- HVFP でドメインへの再参加
- HVFP のホスト名変更

システム設定情報を保存したあとに CIFS サービスの認証を変更した場合は，システム LU または Virtual Server OS LU を回復したあとに CIFS サービスの認証を変更して，ノードまたは Virtual Server を Active Directroy ドメインに再度参加させる必要があります。CIFS サービスの認証を変更した場合は，システム設定情報を保存してください。

CIFS クライアントから CIFS 共有へのアクセスで Active Directory 認証に失敗した場合は，CIFS クライアントの認証チケットの確認で失敗しているおそれがあります。CIFS クライアントマシンに再度ログインするか，Windows を再起動してください。

Active Directory 認証を設定した場合，ドメインコントローラー，HVFP および CIFS クライアントの間で時刻がずれないように運用してください。時刻が 5 分以上ずれると，CIFS クライアントが HVFP にアクセスする際，認証に失敗することがあります。

ユーザーマッピングを使用すると，ノードまたは Virtual Server が参加しているドメインと信頼関係を結んだドメインに所属しているユーザーも，HVFP の CIFS 共有にアクセスできます。ただし，ノードまたは Virtual Server が Active Directory ドメインに参加している場合，HVFP を利用するユーザーは次に示すドメインのどちらかに所属している必要があります。

- ノードまたは Virtual Server が参加しているドメインと親子関係にあるドメイン
- ノードまたは Virtual Server が参加しているドメインと明示的に 1 対 1 の信頼関係を結んだドメイン

Active Directory 認証時，ノードまたは Virtual Server が参加しているドメインのユーザーおよび信頼関係を結んだドメインに所属しているユーザーのどちらを指定する場合も，ドメイン名，ユーザー名およびパスワードを正しく指定してください。

HVFP のノードまたは Virtual Server が参加している Active Directory ドメインを変更する際に，そのノードまたは Virtual Server のコンピュータアカウントを変更前の Active Directory ドメインで削除できなくてメッセージ KAQM16168-W が出力されることがあります。この場合，CIFS クライアントが HVFP にアクセスする際の認証に失敗することがあるので，不要になったノードまたは Virtual Server のコンピュータアカウントを変更前の Active Directory ドメインで削除してください。

Active Directory 認証をする場合 , ドメインコントローラーのイベントログに「Kerberos チケットを生成するための適切なキーがありませんでした」というメッセージが記録されることがあります。これは，Kerberos の暗号化アルゴリズムを決定する際に記録されるもので，HVFP の運用には問題ありません。なお，メッセージおよびイベント ID については，ドメインコントローラーのプラットフォームによって異なることがあります。

Active Directory 認証時， HVFP のドメインへの参加またはクライアントの共有アクセスができなくなるため， Active Directory のポリシー（コンピューターの構成 ¥ ポリシー ¥Windows の設定 ¥ セキュリティの設定 ¥ ローカル ポリシー ¥ セキュリティ ポリシーの設定）の「ネットワーク セキュリティ：Kerberos で許可する暗号化の種類を構成する」で，「RC4_HMAC_MD5」のチェ

ックを外さないでください。なお，Windows のバージョンによっては項目名が異なることがあります。

CIFS サービスがドメインコントローラーとの通信で使用する SMB プロトコルのバージョンが，ドメインコントローラーでサポートされていることを確認してください。サポートされていない場合は，HVFP のドメインへの参加またはクライアントの共有アクセスができなくなるため，cifsoptset コマンドの client_ipc_max_protocol および client_ipc_min_protocol オプションで，CIFS サービスがドメインコントローラーとの通信で使用する SMB プロトコルのバージョンの設定を変更してください。

6.4.2-00 より前のシステムバージョンで Active Directory 認証を使用している場合，HVFP はフェールオーバー後にドメインコントローラーに匿名で接続します。そのため，ドメインコントローラーの設定で匿名接続を許可していない場合はフェールオーバー後にアクセスできなくなります。この場合は，ドメインコントローラーで匿名接続を許可するように設定してください。

ドメインコントローラー上でユーザーやグループの UNIX 属性を変更した場合は，HVFP 上のフォルダやファイルの ACL を手動で付け替えるとともに，File Services Manager の［Access Protocol Configuration］ダイアログの［CIFS Service Maintenance］ページで［Clear User Map Cache File］ボタンをクリックして，ユーザーマッピングのキャッシュファイルを削除してください。

クラスタ構成の場合は，ユーザーマッピングの設定を両ノードで一致させてください。

OU（組織単位）には，HVFP のコンピュータアカウントや，HVFP で指定したドメインユーザーのアクセス権を設定するようにしてください。

WORM 対応ファイルシステムを運用する場合，Active Directory の更改などによってドメインに属するユーザーの UID および GID が変わると，ACL の設定によっては WORM ファイルにアクセスできなくなります。また，更改の前後で UID および GID を合わせることができません。このため，RID 方式のユーザーマッピングを使用する際は，ファイルが WORM 化する前に Everyone に許可を設定するなどして対処してください。なお，Active Directory スキーマ方式の場合は，ActiveDirectory の設定によって UID および GID を合わせることができます。これは，LDAP によるユーザーマッピングでも同様です。

Read Only Domain Controller（RODC）を認証サーバとして設定すると，Kerberos チケットが発行されず，CIFS アクセスできないことがあります。

HVFP のリプレース中などの状況で，2 つ以上の HVFP のノードが同一のホスト名で存在している場合は，同一の名称で Active Directory に参加させないでください。

ファイアウォールなどで，HVFP と，信頼関係先を含む Active Directory との間の通信を遮断しないでください。

NTLM 認証を使用しているときは，Active Directory で NTLM 認証を遮断しないでください。

Active Directory の LDAP 署名の設定は，HVFP の設定と一致させてください。

5.3 ユーザーマッピングを使用している場合の認証

ユーザーマッピングを使用したときに，CIFS クライアントからの共有アクセス時に認証に失敗した場合，次の表に示す内容を確認してください。

表 5-1： CIFS クライアントからの共有アクセス時に認証が失敗した場合の対策

#	確認項目	確認内容	対策
1	［Access Protocol Configuration］ダイアログの［CIFS Service Maintenance］ページの［Range of UIDs］および［Range of GIDs］*1*4*6	ユーザー ID・グループ ID の範囲がすべて使用されている。	ユーザー ID・グループ ID の範囲を拡張してください。
		ユーザー ID・グループ ID の範囲に使用されていない部分がある。	#2 の項目を確認してください。
2	［Access Protocol Configuration］ダイアログの［List of Services］ページに表示される CIFS サービスの稼働状態 *2	サービスが正しく稼働している。	#3 の項目を確認してください。
		CIFS サービスが正しく稼働していない。	サービスを再起動してください。
3	CIFS サービス構成定義で設定した LDAP サーバ *4	LDAP サーバが正しく稼働しているか。	LDAP の稼働状況に応じて対処をしてください。
		認証が失敗したユーザーにユーザー ID・グループ ID が登録されていない。*7	ユーザー ID・グループ ID を登録してください
4	CIFS ログを参照 *3（/var/log/cifs/log.winbindd）	障害情報が出力されていないか。	出力されるログに従って調査・対処をしてください。
5	`umapidget` コマンド実行 *5	認証が失敗したユーザーのユーザー ID・グループ ID が範囲外である。	ユーザー ID・グループ ID の範囲を拡張してください。
		認証が失敗したユーザーのユーザー ID・グループ ID が範囲内である。	#2 の項目を確認してください。
6	認証が失敗したユーザーの Active Directory の管理画面 *8	認証が失敗したユーザーに UNIX 属性のユーザー ID・グループ ID が登録されていない。	UNIX 属性のユーザー ID・グループ ID を登録してください。

注 *1

ユーザーマッピングするユーザー ID・グループ ID の割り当て状況を確認します。

注 *2

ユーザーマッピングしたユーザー ID・グループ ID の参照，割り当てに失敗していないかを確認します。CIFS サービスの稼働状況を確認する方法については，「ユーザーズガイド」（IF305）を参照してください。

注 *3

CIFS ログなどのログファイルを参照する方法については，「ユーザーズガイド」（IF305）を参照してください。

注 *4

ユーザーマッピング方式として［Use user mapping using LDAP.］を選択している場合だけです。

注 *5

ユーザーマッピング方式として［Use user mapping using RIDs.］を選択している場合だけです。

注 *6

ID の割り当て方式として［Allocate automatically］を選択している場合だけです。

注 *7

ID の割り当て方式として［Allocate manually］を選択している場合だけです。

注 *8

ユーザーマッピング方式として［Use user mapping using Active Directory schema.］を選択している場合だけです。

LDAP 方式のユーザーマッピング使用時，LDAP サーバへの接続ができない場合は，CIFS サービスへのアクセスに失敗するおそれがあります。この場合，LDAP サーバへ接続できなくなる障害を取り除き，2 分後 * または cifscachectl コマンドで unresolved_negative_cache を破棄したあとに CIFS サービスへアクセスしてください。unresolved_negative_cache を破棄する方法については，「コマンドリファレンス」を参照してください。

注 *

cifsoptset コマンドで unresolved_negative_cache の有効期間を変更している場合は，設定されている unresolved_negative_cache の有効期間が経過したあとになります。
unresolved_negative_cache の有効期間は，cifsoptlist コマンドで確認できます。

ドメインコントローラーとのネットワークに障害が発生している状態で SNMP または E-mail 通知を利用して CIFS サービスに関連する障害情報を確認した場合，接続の失敗を検知してから 5 分間はそれ以降のドメインコントローラーからのユーザー・グループ情報は取得できません。そのため，その間は CIFS クライアントからのユーザー認証が失敗します。この場合，ドメインコントローラーへ接続できない障害を取り除き，SNMP または E-mail 通知を利用してドメインコントローラーとの接続が回復したことを確認したあと，5 分後 * または cifscachectl コマンドで unresolved_negative_cache を破棄したあとに CIFS サービスへアクセスしてください。unresolved_negative_cache を破棄する方法については，「コマンドリファレンス」を参照してください。

注 *

cifsoptset コマンドで unresolved_negative_cache の有効期間とドメインコントローラーへの問い合わせ結果に関するキャッシュの有効期間を変更している場合は，設定されている有効期間のうち，長い方の時間が経過したあとになります。これらの有効期間は，cifsoptlist コマンドで確認できます。

CIFS クライアントから短時間・大量接続をする際，HVFP に掛かっている負荷や CIFS クライアント・DC サーバなどの処理能力やネットワーク環境によっては，CIFS クライアントが HVFP への接続に失敗する場合があります。その場合には次の例に挙げるような回避策を実施していただくことを推奨します。

- HVFP への CIFS アクセスをする前に，事前に接続してください。
  CIFS クライアントがタイミングをずらしながら事前に接続することで，DC サーバやネットワークの負荷を分散できます。事前の接続には，Windows API の `WNetAddConnection2()` 関数や，`net` コマンドなどを使用してください（`net` コマンドで事前接続をした場合，CIFS アクセスをする際に，再度，認証が発生する場合があります）。また，HVFP 側のタイムアウトによって接続が切断されるのを防ぐためには，HVFP 側のタイムアウト値を 0（0 は，タイムアウトなしを表します）に設定してください。タイムアウト値は，File Services Manager の［Access Protocol Configuration］ダイアログの［CIFS Service Management］ページ（Setting Type：Performance）にある［Client time-out］で設定できます。

・ HVFP への接続に失敗した場合，CIFS クライアント側で再度接続してください。再接続するには，DC サーバやネットワークの負荷を分散するために，30 秒～ 60 秒程度の間隔をあけることを推奨いたします。

参考までに HVFP を含めたドメイン環境での DC サーバやネットワークなどが正常な状態であれば，1 秒当たりに処理できる接続数は，NTLM 認証を使用した場合には約 100 で，Kerberos 認証を使用した場合には約 10 ～ 12 となります（Kerberos 認証の場合，リプライ攻撃防止などのために認証処理に時間が掛かります)。

6

Windows ドメイン環境のユーザー資源移行手順

この章では，Windows ドメイン環境で作成されたユーザー資源を移行する際の注意事項と，バックアップユーティリティを使用して HVFP 上にユーザー資源を移行する手順について説明します。

6.1 資源を移行する前に

HVFP 上の CIFS 共有で提供するアクセス制御リスト（ACL）は，ファイルシステム（Classic ACL タイプファイルシステムまたは Advanced ACL タイプファイルシステム）によって違いがあります。Classic ACL タイプファイルシステムは，POSIX に準拠した UNIX ACL を Windows ACL にマッピングしたものになります。UNIX ACL は，概念としては Windows ACL と類似していますが，UNIX 上のファイルパーミッションに基づいたものであるため，機能面で大きく異なる部分があります。そのため，Windows ACL とまったく同じ機能を使用できません。Advanced ACL タイプファイルシステムは，Windows ACL と同様に詳細なアクセス許可を設定でき，より Windows に近い ACL でのアクセス制御ができます。ACL に関する説明については「8.3 ACL」を参照してください。

Windows 環境からの移行

ファイルシステムタイプの違いによる Windows 環境からの移行に関する仕様の差異を次の表に示します。

表 6-1： ファイルシステムタイプの違いによる Windows 環境からの移行の仕様差異

#	項目		Classic ACL タイプ	Advanced ACL タイプ	備考
1	操作ユーザー		File Services Manager で登録された CIFS 管理者	File Services Manager で登録された CIFS 管理者	一般ユーザーの場合，移行先フォルダの ACL，移行対象ファイル，フォルダの ACL によってデータ移行，所有者の変更，ACL の設定に影響があります。
2	所有者の移行	ユーザー	可	可	SID および UID を解決できることが前提です。*1
		グループ	不可	可	SID および GID を解決できることが前提です。*1
		BUILTIN/Well-known SID アカウント	不可	不可	－
		SID 解決不可アカウント	不可	不可	SID および GID を解決できることが前提です。*1
3	ACL の移行 *2*3	ファイル所有者	可	可	－
		プライマリーグループ	可	可	－
		DACL（随意 ACL）	一部不可 *4*5（POSIX ACL にマッピング）	可	SID，UID および GID を解決できることが前提です。*1
		SACL（監査 ACL）	不可 *6	不可 *6	－

#	項目		Classic ACL タイプ	Advanced ACL タイプ	備考
4	ファイル属性の移行	読み取り専用属性	可	可	－
		アーカイブ属性	可 *6	可	Windows バックアップユーティリティでは，移行元の属性を移行できるが，XCOPY コマンドではすべてのファイルにアーカイブ属性が付けられます。
		システム属性	可 *6	可	－
		隠し属性	可 *6	可	－
		ディレクトリ属性	可	可	－
		暗号化属性	不可 *6	不可 *6	XCOPY コマンドの場合は非暗号化ファイルとなり，Windows バックアップユーティリティの場合は暗号化ファイルの復元がエラーとなります。
		圧縮属性	不可 *6	不可 *6	圧縮ファイル属性が解除され，非圧縮のデータが保存されます。
		オフライン属性	不可	不可	－
		ノーマルファイル属性	可	可	－
		一時ファイル属性	不可	不可	－
		スパースファイル属性	不可	不可	－
		リパースポイント属性	不可	不可	－
		非インデックス対象ファイル属性	不可	不可	－
5	タイムスタンプの移行	アクセス日時	不可	不可	コピー（移行）した日時となります。
		更新日時	可	可	－
		作成日時	不可 *7	不可 *7	－

（凡例）可：移行できる　不可：移行できない　－：備考なし

注 *1

例えば，Windows の Active Directory 移行ツール（ADMT）などを使用して Active Directory ドメインでアカウントを移行した場合，移行元のファイルサーバで使用していたアカウント（SID）は HVFP で解決できないため，ほかのファイルサーバから HVFP にファイルやフォルダのアクセス権を移行できないことがあります。ファイルやフォルダのアクセス権を移行する場合は，移行前のアカウントの情報を移行後のアカウントに割り当て直してから移行してください。

なお，HVFP では，ほかのファイルサーバからデータをインポートする際に，インポート元のアカウントの情報をマッピングする手順を提供しています。ほかのファイルサーバから CIFS プロトコルを使用してデータをインポートする手順については，「ユーザーズガイド」（IF305）を参照してください。

また，cifsoptset コマンドで，Windows ドメインのビルトインアカウントの Authenticated Users および Network に対する ACL 設定を有効にした場合は，

Authenticated Users および Network を認識できます。このとき，ほかのファイルサーバからデータをインポートしても，Authenticated Users および Network に対する ACL 設定はインポートされません。ほかのアカウントと同様に移行元のアカウントのマッピング機能を使用してください。Windows ドメインのビルトインアカウントの Authenticated Users および Network に対する ACL 設定を有効にするかどうかを設定する方法については，「コマンドリファレンス」を参照してください。

注 *2

指定できる ACL リビジョンは ACL_REVISION(0x2) です。ACL_REVISION_DS(0x4) の ACL リビジョンは指定できません。

注 *3

指定できる ACE タイプはアクセス許可 ACE（0x0）とアクセス拒否 ACE（0x1）です。そのほかの ACE タイプは指定できません。

注 *4

Classic ACL タイプファイルシステムでは，ACE が 63（所有者，グループを含む）を超えた場合，移行できないことがあります。Advanced ACL タイプファイルシステムでは，ACE が 700 を超えた場合，移行できないことがあります。

注 *5

DACL に，HVFP で認識できないユーザー／グループ，または Everyone，CREATOR OWNER，CREATOR GROUP を除く BUILTIN/Well-known SID アカウントが含まれている場合，その ACE は除外して移行されます。

注 *6

HVFP では未サポートです。SACL（監査 ACL）が未サポートなので Windows 標準の監査機能と同じことはできませんが，監査機能については CIFS アクセスログでの代替を検討してください。

注 *7

移行先のファイルシステムが，ファイル作成日時を記録するよう設定されている場合だけ移行できます。ファイル作成日時を記録しない設定の場合，ファイル更新日時，アクセス日時またはファイル属性変更日時の中からいちばん古い日時が作成日時となります。

Windows に標準装備されているコマンドまたはアプリケーションプログラムによるユーザー資源移行について，次の表に示します。ユーザー資源の属性移行可否を考慮し，HVFP ではバックアップユーティリティを推奨します。

表 6-2：コマンド／アプリケーションによるユーザー資源移行

#	コマンド／アプリケーション	移行に関する留意事項
1	エクスプローラによるコピー	ACL 情報を復元できません。ACL 情報にはファイル所有者，プライマリーグループが含まれ，資源の所有者はファイル移行を実行したユーザーとなります。このためファイル移行後，ACL の再設定が必要です。
2	XCOPY	File Services Manager で登録された CIFS 管理者が，XCOPY コマンドのオプションを指定して実行することで，所有者および ACL 情報を移行できます。HVFP で認識できるユーザー *1 が所有者ではない場合，ファイルを移行できません。
3	バックアップユーティリティ（Windows 標準）*2	File Services Manager で登録された CIFS 管理者が，バックアップユーティリティを操作することで，所有者および ACL 情報を移行できます。バックアップしたファイルの情報がレポートに出力されます。

注 *1

HVFP で認識できるユーザーとは，HVFP 上で SID をユーザー名にマッピングできるユーザーのことです。したがって，参加しているドメインに登録されているユーザー・グループは

HVFP で認識できるユーザー・グループとなり，Everyone，CREATOR OWNER，CREATOR GROUP を除く Windows クライアント独自のユーザー・グループ（ビルトイン ユーザーも含む）は HVFP で認識できないユーザー・グループとなります。また，参加しているドメインのユーザー・グループであっても，移行時にすでにドメインから削除されている場合は，HVFP で認識できないユーザー・グループとなります。

補足：

cifsopsset コマンドで，Windows ドメインのビルトインアカウントの Authenticated Users および Network に対して ACL 設定を有効にした場合は，Authenticated Users および Network を認識できます。Windows ドメインのビルトインアカウントの Authenticated Users および Network に対する ACL 設定を有効にするかどうかを設定する方法については，「コマンドリファレンス」（IF311）を参照してください。

注 *2

Windows に標準装備されているバックアップツールのことです。

XCOPY コマンド，バックアップユーティリティを使用してファイルを移行する場合の注意事項

- ユーザー資源に設定されている ACL の移行は，移行元の Windows マシン，コマンド・アプリケーションを実行する Windows マシン，移行先の HVFP のノードまたは Virtual Server が同一の Windows ドメインに参加し，かつ File Services Manager の CIFS サービス構成定義でユーザーマッピングを使用している場合だけできます。
- バックアップしたファイルの HVFP への移行は，File Services Manager で登録された CIFS 管理者で行う必要があります。CIFS 管理者の登録方法については，「ユーザーズガイド」（IF305）を参照してください。
- CIFS サービス構成定義の認証方法が Active Directory 認証以外の場合，もしくは Active Directory 認証でもユーザーマッピングを使用しない場合，ユーザー資源に設定されている ACL の移行はできません。移行を実施した場合，移行されたユーザー資源のオーナーは root，グループはユーザー資源移行を実施したユーザーが属するグループになります。
- Windows マシンでの ACL と HVFP でのファイル属性，ACL，タイムスタンプの移行の可否については，表 6-1： ファイルシステムタイプの違いによる Windows 環境からの移行の仕様差異を参照してください。

64 以上の ACE を保持するファイル・フォルダを移行する場合の注意事項（Classic ACL タイプ）

ファイル・フォルダのオーナー，グループを含めて 64 以上の ACE を保持するファイル・フォルダの場合，Windows サーバから HVFP へすべての ACE が移行できない場合があります。この場合の回避策としては，同一の ACL を設定されているユーザーが同一のグループに属するように設定し，該当グループに対して ACL を設定してください。これによって ACE 数が 63 以内になるようにしてください。

701 以上の ACE を保持するファイル・フォルダを移行する場合の注意事項（Advanced ACL タイプ）

ファイル・フォルダのオーナー，グループを含めて 701 以上の ACE を保持するファイル・フォルダの場合，Windows サーバから HVFP へ，すべての ACE を移行できない場合があります。この場合の回避策としては，ACL 内に同一のアクセス権を設定されているユーザーが複数存在する場合，それらのユーザーを 1 つのグループに属するようにし，複数のユーザーの代わりにそのグループを ACL に設定するようにして，ACE 数が 700 以内になるようにしてください。

移行時に付加される ACE についての注意事項（Classic ACL タイプ）

ユーザー資源の移行時にファイル，フォルダそれぞれに次の ACE が自動的に付加されます。

- ファイル移行
  該当ファイルのオーナーとグループが ACL として設定され，表示されます。
- フォルダ移行
  サブフォルダおよびファイルに適用する ACL を持つフォルダの場合は 「CREATOR OWNER」，「CREATOR GROUP」という ACL が追加設定され，表示されます。

ファイル所有者が HVFP で認識できるドメインユーザーではない場合のファイル移行についての注意事項

バックアップユーティリティを利用した場合，移行先ファイルの所有者は，次のどちらかになります。

- CIFS 管理者（root ユーザー）
- 移行元の ACL にユーザーと主グループの組み合わせが存在する場合，移行元の ACL に含まれるユーザー

XCOPY コマンドを利用した場合，そのファイルの移行がエラーとなり，移行先には空ファイルが作成されます。

ファイル所有者以外の ACL に HVFP で 認識できない SID を持つユーザー・グループが含まれる場合のファイル移行についての注意事項

移行時に HVFP で認識できない SID を持つユーザー・グループの ACE がある場合，その ACE を除いた ACL が移行されます。

ファイル所有者が CIFS 管理者（root ユーザー）となる場合の注意事項

CIFS 管理者は、ユーザー，グループまたはディレクトリに対する Quota やデフォルト Quota による制限はありません。Quota 管理を行う場合は、資源移行後にファイル所有者を適切なユーザに変更し Quota 設定してください。詳細は，「ファイルアクセス（Quota）ユーザーズガイド」（IF307）を参照してください。

6.2 バックアップユーティリティによる移行

Windows ドメイン環境のユーザー資源を，HVFP 上に移行する手順を次に示します。

1. 移行対象ファイルのファイル属性，ACL 情報の取得
   Windows ドメイン環境から HVFP に移行する場合，ファイル属性，ACL に仕様差異が存在するため，移行後にファイル属性，ACL の再設定をする必要がある場合があります。そのため，CACLS コマンドや ATTRIB コマンドなどで移行前に移行対象ファイルのファイル属性，ACL 情報を取得しておいてください。

2. バックアップファイルの作成
   バックアップユーティリティを使用して移行対象ファイルのデータをバックアップし，バックアップファイルを作成します。バックアップ操作については，バックアップユーティリティのヘルプやドキュメントを参照してください。
   バックアップが完了したら，移行対象のフォルダ，ファイルが正しくバックアップファイルに含まれていることを確認してください。

3. File Services Manager への CIFS 管理者の登録
   バックアップしたファイルの HVFP への移行は CIFS 管理者で実施してください。CIFS 管理者以外のユーザーの場合，ファイル所有者であってもファイル属性が正しく移行できない場合があります。
   File Services Manager の［Access Protocol Configuration］ダイアログの［CIFS Service Management］ページ（Setting Type : Administration）で，Windows サーバからのファイ

ル移行を実施するユーザーまたはそのユーザーが属するグループを CIFS 管理者として登録します。詳細は，「ユーザーズガイド」（IF305）を参照してください。

4. ファイルシステムと CIFS 共有の作成

   HVFP 上に移行先のファイルシステムと CIFS 共有を作成します。

   File Services Manager の［ファイルシステム構築と共有作成］ダイアログでファイルシステムの構築と CIFS 共有の作成を一括して行うか，［ファイルシステム構築］ダイアログでファイルシステムを構築したあと［共有追加］ダイアログで CIFS 共有を追加します。詳細は，「ユーザーズガイド」（IF305）を参照してください。

   参考

   HVFP の CIFS サービス構成定義は，Windows サーバの挙動に合わせ，デフォルトで「ファイル名に含まれる大文字と小文字を区別しない」という設定になっています。

   HVFP のノードまたは Virtual Server で `cifsoptlist` コマンド，`cifsoptset` コマンドを実行することで，ノードまたは Virtual Server 内の CIFS サービスや各 CIFS 共有での設定内容を参照，変更できます。

   「ファイル名に含まれる大文字と小文字を区別する」という設定に一時的に変更して HVFP への移行（バックアップファイルの復元）操作をすると，移行処理の性能向上を期待できます。ただし，設定を変更して移行した場合は移行完了後，必ず「ファイル名に含まれる大文字と小文字を区別しない」という設定に戻してから HVFP を運用してください。「ファイル名に含まれる大文字と小文字を区別する」という設定で運用し，HVFP の共有ディレクトリ内に大文字と小文字だけが異なる同名のファイルが存在すると，CIFS クライアントでは大文字と小文字を区別しないため，意図しないファイルを操作してしまうおそれがあります。

5. バックアップファイルの復元

   バックアップユーティリティを使用して手順 2 で作成したバックアップファイルのデータを，手順 4 で作成したファイル共有に復元します。

   手順 3 で登録した CIFS 管理者がバックアップファイルが存在する Windows にログインして実行してください。復元操作については，バックアップユーティリティのヘルプやドキュメントを参照してください。

6. CIFS ログの確認

   ファイル移行時にユーザーマッピング機能が正しく動作していない場合，ファイル所有者や ACL が正しく移行されないことがあります。そのため，ファイル移行作業完了後，CIFS ログ（/var/log/cifs/log.winbindd）によって，ユーザーマッピング機能のエラーが発生していないことを確認してください。エラーが発生している場合には，原因を取り除いた後，再度移行作業をしてください。

   なお，CIFS ログなどのログファイルを参照する方法については「ユーザーズガイド」（IF305）を，CIFS ログ（/var/log/cifs/log.winbindd）のメッセージについては，「A.2.2 log.winbindd」を参照してください。

7. 移行先のファイルの ACL 再設定

   Windows ドメイン環境から HVFP に移行する場合，ファイル属性，ACL に仕様差異が存在するため，ACL が正しく復元されていない場合があります。この場合，HVFP での ACL 仕様に基づき，ACL の再設定をしてください。

   ACL の再設定は File Services Manager で登録した CIFS 管理者で行う必要があります。手順 3 で登録した CIFS 管理者で CIFS 共有にアクセスして実施してください。

7

共有ディレクトリへの CIFS アクセス

この章では，CIFS クライアントから共有ディレクトリにアクセスする場合の手順と注意事項について説明します。

7.1 アクセス方法

CIFS クライアントから共有ディレクトリにアクセスする場合，次のとおり指定してください。なお，このアクセス方法は，ユーザーまたはシステムごとにどちらかの指定方式で統一してください。

- ¥¥＜Physical Node ホスト名または Virtual Server 名*＞¥＜CIFS 共有名＞¥＜使用するディレクトリのパス＞
- ¥¥＜仮想 IP アドレス＞¥＜CIFS 共有名＞¥＜使用するディレクトリのパス＞

注 *

指定パス中の Physical Node ホスト名または Virtual Server 名は，HVFP のノードまたは Virtual Server のホスト名または NetBIOS 名に相当します。また，Physical Node ホスト名または Virtual Server 名には，DNS の CNAME レコードに登録した別名を指定できません。なお，IPv6 接続で CIFS 共有にアクセスする場合，Physical Node ホスト名，Virtual Server 名，仮想 IP アドレスには，ホスト名または ipv6-literal.net 名を指定する必要があります。ipv6-literal.net 名は，次に示すような，IPv6 アドレスの区切り文字のコロン（:）をハイフン（-）に置き換え，末尾に .ipv6-literal.net を付加した形式の IP アドレスです。

IPv6 アドレスが fd00::5:50 の場合の ipv6-literal.net 名

```
fd00--5-50.ipv6-literal.net
```

クライアントからの接続方法

Windows は，クライアントからの接続方法として NetBIOS over TCP/IP が有効に設定されている場合，CIFS 接続をする際に NetBIOS over TCP/IP（ポート 139）と Direct Hosting of SMB（ポート 445）の両方同時に（パラレルに）接続を試し，先に応答した方の接続を使用して CIFS アクセスします。この動作は Microsoft の次のページでも説明されています。

http://support.microsoft.com/kb/204279/ja

これによって，応答が遅かった方の接続は，クライアントからすぐに切断されますが，この切断のタイミングによっては，すでに smbd の子プロセスが最初のリクエストに対する応答を返そうとしているため，クライアントからコネクションが切断されたことを示すメッセージがログに記録されることがあります（メッセージ内容については「A.2 CIFS ログ」および「A.2.1 log.smbd」を参照してください）。CIFS アクセス自体は，先に接続した方のコネクションでクライアントと通信をするため，特に問題はありません。

名前解決サービス

CIFS クライアントで利用できる名前解決サービスは，WINS，DNS，lmhosts などです。これらの名前解決サービスを利用する場合の注意事項を次の表に示します。

表 7-1：名前解決サービス利用に関する注意事項

名前解決サービス	注意事項
WINS	ネットワーク上のほかの CIFS クライアントをすべて WINS クライアントに設定してください。なお，HVFP のノードまたは Virtual Server の仮想 IP アドレスと，ホスト名または NetBIOS 名は，WINS サーバに手動で登録してください。
DNS	HVFP のノードまたは Virtual Server の仮想 IP アドレスと，ホスト名または NetBIOS 名は，DNS サーバに手動で登録してください。
lmhosts	すべての CIFS クライアントの lmhosts に HVFP のノードまたは Virtual Server の仮想 IP アドレスと，ホスト名または NetBIOS 名を登録してください。

7.2 CIFS クライアントからアクセスしているときの注意事項

CIFS クライアントからアクセスしているときの注意事項を次に示します。

- 接続に関しての注意事項です。
  CIFS サービスに接続できる CIFS クライアントの数（最大接続数）は，24,000 です（詳細は表 7-2： CIFS クライアントの最大接続数および CIFS 共有数の上限値を参照してください）。
  フェールオーバーの発生によって，1 つのノードで複数のリソースグループが稼働しているときも，最大接続数は変わりません。CIFS クライアントが CIFS サービスへ接続したとき，最大接続数を上回っていた場合は，接続に失敗した旨を表すメッセージがクライアントに表示されます。
  CIFS 共有へのアクセスを中止しても，CIFS サービスへの接続は即座に切断されません。
  CIFS サービスへの接続を切断する方法は，次のとおりです。
  - CIFS クライアントに再ログインする。
  - HVFP 上の CIFS 共有への接続をすべて切断する。

  また，CIFS クライアントが，ファイルをオープンしていない状態で［Client time-out］に指定した時間の間 HVFP にアクセスしなかった場合，HVFP は CIFS クライアントとの接続を自動的に切断します。［Client time-out］時間については，「ユーザーズガイド」（IF305）を参照してください。
  ユーザーが，HVFP によって接続が切断された CIFS 共有にアクセスしようとした場合，CIFS クライアントは CIFS サービスへの再接続を自動的に試みます。そのため，再接続時にユーザーが認証情報を再入力する必要はありません。ただし，CIFS サービスに再接続したとき，接続できる CIFS クライアント数の上限値を上回っていた場合は，通常の接続と同様，CIFS 共有にアクセスできません。
  なお，エクスプローラで CIFS 共有の内容を表示している場合は，エクスプローラが定期的に CIFS サービスにアクセスするため，HVFP が接続を自動的に切断することはありません。

表 7-2： CIFS クライアントの最大接続数および CIFS 共有数の上限値

モデル	メモリー量	自動リロード	CIFS クライアントの最大接続数（1 クラスタ当たり）	CIFS 共有数の上限（1 クラスタ当たり）
Nh4b/Nh4c	32GB	×	6,000	7,500
		○	2,000	256
	64GB	×	12,000	7,500
		○	4,800	256
Nh8b/Nh8c	64GB	×	24,000	7,500
		○	9,600	1,024
	96GB	×	24,000	7,500
		○	9,600	1,024

（凡例）○：自動リロードする　×：自動リロードしない

- 書き込み要求が CIFS クライアントにキャッシュされている場合に，CIFS クライアントまたはネットワークで障害やディスク容量不足が発生すると，データを保証できないこと（例えば，ファイルの書き込みが成功したように見えるが，データが正しく書き込まれていないなど）があります。CIFS 共有内のファイルの更新データをクライアントにキャッシュする設定の場合には，注意してください。

- ファイルの更新データをクライアントにキャッシュする設定を有効にしている場合，あるCIFS クライアントで書き込み要求をキャッシュしている状態で別の CIFS クライアントが同じファイルをオープンしようとすると，先に最初のクライアントからキャッシュのフラッシュが実行されます。これに加え，書き込み要求およびクローズ要求に同期して書き込むように設定している場合，異なる CIFS クライアントから同じファイルをオープンしようとすると，最初のクライアントからの書き込みとディスクドライブへのフラッシュが完了するまで，別のCIFS クライアントでファイルのオープンが完了しません。このため，あとからアクセスしたCIFS クライアントからファイルを開くときに時間が掛かることがあります。
- 複数のクライアントから CIFS 共有内の同一ファイルに対して更新を行う場合，ファイルの更新データをクライアントにキャッシュするように設定すると，アクセス遅延や，データの信頼性低下が発生するおそれがあります。そのため，複数クライアントから同時に更新されるおそれがあるファイルは，クライアントにキャッシュしないように設定した CIFS 共有内に保存することを推奨します。
- CIFS クライアントから CIFS 共有内でフォルダを移動した場合，移動したフォルダの更新日時は，移動した時刻に変更されます。
- クライアントが CIFS 共有にファイル・フォルダを作成する場合，作成先の同一フォルダ内に格納されるファイル・フォルダの数が多くなるほど時間が掛かります。これは，作成対象のファイル・フォルダの名称に対して大文字と小文字を判定したうえで，名称の重複をチェックしていることが理由です。
  HVFP では，CIFS サービスの構成定義の初期設定として，Windows サーバの動作に従い「ファイル名に含まれる大文字と小文字を区別しない」が設定されています。例えば，ABC.txt と abc.txt は同じファイルと判定され，同一フォルダ内に作成できません。
  同一フォルダ内のファイル・フォルダ数が 1,000 を超えると，重複チェックにさらに時間が掛かるようになります。同一フォルダ内のファイル・フォルダの数が多くなるほど，HVFP に負荷が掛かったり，ファイル・フォルダの表示に時間が掛かったりするため，大量のファイル・フォルダが同一フォルダ内に格納されることのないように運用してください。
  `cifsoptset` コマンドを使用して，CIFS サービスの構成定義を「ファイル名に含まれる大文字と小文字を区別する」に変更することで処理時間は短縮が期待できます。このとき，同一フォルダ内のファイル・フォルダ名称が，大文字と小文字を区別しなくても重複していないことを確認してください。重複していると，CIFS クライアントが意図しないファイルを操作するおそれがあります。
- CIFS クライアントとの通信に SMB 署名を使用すると，転送中の SMB パケットを改ざんする中間者攻撃を防止できます。ただし，セキュリティが向上する反面，ファイルアクセス性能が低下します。SMB 署名を使用するためには，クライアントと HVFP のそれぞれで設定が必要です。HVFP では，SMB 2.0，SMB 2.1 および SMB 3.0 の通信に対して，クライアントから SMB 署名を要求された場合，常に SMB 署名を使用するように動作します。また，SMB1.0 の通信に対して SMB 署名を使用するかどうかを，cifsoptset コマンドで変更できます。初期設定では，SMB 1.0 の通信に対して SMB 署名は使用されません。
- CIFS クライアントからファイルシステムを利用しているときに，システム管理者が CIFS サービスの構成定義を変更すると，CIFS クライアントの操作が正常に完了しないおそれがあります。操作が完了できなかった場合は，CIFS サービスの構成定義が変更されたあとで，再度操作してください。
- CIFS クライアントがファイルシステムを利用しているときに，システム管理者が CIFS 共有の情報を変更すると，変更内容が有効にならないおそれがあります。CIFS クライアントは，変更内容を有効にするため，CIFS 共有に接続し直したり，Windows を再起動したりしてください。

- フェールオーバーが発生した場合，フェールオーバーやフェールバックによって移動したリソースグループのサービスを利用していた CIFS クライアントの操作は強制的に中断されます。
- CIFS クライアントからアクセスしているノードまたは Virtual Server で，CIFS クライアントからのアクセスとデータの書き込みを抑止しているときに CIFS サービスを再起動した場合，CIFS サービスが不完全な状態となります。この場合，［Access Protocol Configuration］ダイアログの［List of Services］ページの［Status］に「Running」，［Information］に「The service is incomplete. Restart the service.」が表示され，CIFS 共有に接続できなくなることがあります。
- 次の表に示す操作を実行すると，CIFS クライアントからのアクセスとデータの書き込みが抑止されるおそれがあります。CIFS 共有に接続できなくなった場合，表に示す操作がすべて完了してから CIFS サービスを再起動してください。CIFS サービスを再起動する前に確認する内容もあわせて表に示します。

表 7-3：アクセスと書き込みが抑止されるおそれのある操作と確認事項

操作	確認事項
差分スナップショットの作成	次のことを確認してください。 ・［差分スナップショットの作成または置換］ダイアログでの差分スナップショットの作成が実行中でない。 ・ syncadd コマンドでの差分スナップショットの作成が実行中でない。 ・ 現在の時刻に差分スナップショットが自動作成されるようにスケジュールが設定されている場合は，システムメッセージまたは SNMP トラップを取得して，差分スナップショットの自動作成が終了している。 自動作成を実行したときに出力されるシステムメッセージおよび通知される SNMP トラップについては，「メッセージリファレンス」（IF313）を参照してください。
差分格納デバイスの拡張	次のことを確認してください。 ・［File Snapshots 編集］ダイアログの［ストレージ］タブでの差分格納デバイスの拡張が実行中でない。 ・ syncexpand コマンドでの差分格納デバイスの拡張が実行中でない。
horcfreeze コマンドの実行	horcfreeze コマンドで書き込みを抑止したファイルシステムに対して，horcunfreeze コマンドを実行して書き込みの抑止を解除したかどうかを確認してください。
オンラインバックアップの実行	次のことを確認してください。 ・ オンラインバックアップが実行中でない。 ・［NDMP Server Control］ページに「Stopped」が表示されている。または，「Running」が表示されていて［Stop］ボタンが表示されている。 ・ ndmpcontrol コマンドに -l オプションを指定して実行したときに表示される NDMPsvrstatus と connectstatus の値は，それぞれ「stopped」と「disconnected」である。

注

GUI とコマンドの詳細については，「ユーザーズガイド」（IF305）および「コマンドリファレンス」（IF311）を参照してください。

- 同一ファイルを複数ユーザーで共有する場合，Windows アプリケーションによるアクセスの競合が発生した際に，Windows アプリケーションの仕様によって，ファイルに個別に設定されている ACL が欠落する場合があります。
- 障害発生中のファイルシステム上にある CIFS 共有を参照したとき，CIFS 共有にファイルやディレクトリがまったく表示されない場合があります。なお，ファイルシステムの障害回復後は，CIFS 共有の内容が正常に表示されます。

- CIFS クライアントがスタブファイルにアクセスした場合，ファイルの処理に時間が掛かり，タイムアウトとなることがあります。CIFS サービスの構成定義または CIFS 共有の属性として［Windows クライアントのアクセスポリシー］に［パラレル］を設定していると，CIFS クライアントがスタブファイルにアクセスしたとき，タイムアウトするまでの時間が最大で 15 分まで延長されます。なお，スタブファイルについては，「システム構成ガイド」（IF302）を参照してください。
- ノードの OS が高負荷状態の場合，CIFS クライアントが CIFS 共有にアクセスした際，ファイルシステムの使用率が 100% に達する前にデバイス空き領域不足エラーになることがあります。
- CIFS クライアントに，次の表に示す，システムが使用するファイルまたはフォルダが表示されることがあります。システムが使用するファイルまたはフォルダに関する注意事項を表に示します。

表 7-4： システムが使用するファイルまたはフォルダに関する注意事項

ファイル名または フォルダ名	注意事項
.arc	このフォルダは，次の契機で作成されます。 ・ ほかのファイルサーバからデータをインポートする場合 ・ 重複排除機能を使用する場合 このフォルダ以下のデータを編集または削除すると，システム情報の不整合が発生するおそれがあります。そのため，このフォルダ以下のデータは編集および削除しないでください。
.backupdates	NDMP 機能を使用する場合に作成されるファイルです。このファイルは編集および削除できません。
.conflict	このフォルダ以下のデータは編集および削除できません。
.conflict_longpath	このフォルダ以下のデータは編集および削除できません。
.history	このフォルダ以下のデータは編集および削除できません。
lost+found	ファイルシステムの整合性チェックを実施する場合に作成されるフォルダです。このフォルダ以下のデータは編集および削除できません。
.lost+found	このフォルダ以下のデータは編集および削除できません。
.snaps	ファイルシステムの共有内に差分スナップショットを公開する場合に作成されるフォルダです。このフォルダ以下のデータは編集および削除できません。
.system_gi	重複排除機能を使用する場合に使用されるフォルダです。このフォルダ以下のデータは編集および削除できません。
.system_reorganize	一時的にデータを退避して inode 領域の空き容量を確保するために使用されるフォルダです。このフォルダはシステム導入時に必ず作成され，フォルダ以下のデータは編集および削除できません。
.temp_backupdates	NDMP 機能を使用する場合に作成されるファイルです。このファイルは編集および削除できません。

- フォルダ内のオブジェクトに一括で ACL を設定する際に，「表 7-4： システムが使用するファイルまたはフォルダに関する注意事項」に示すファイルおよびフォルダが存在すると，ACL 設定が失敗し，処理が中断します。この場合，cifsoptset コマンドで，システムが使用するファイルおよびフォルダを一覧から除外するよう設定することで，ACL 設定の失敗による処理の中断を防ぐことができます。ACL の設定が完了したら，システムが使用するファイルおよびフォルダを一覧に含めるよう，再度設定を変更してください。
  または，対象のフォルダに対して別名で CIFS 共有を作成し，その共有に対して，cifsoptset コマンドでシステムが使用するファイルおよびフォルダを一覧から除外するよう設定してから，ACL を設定してください。

システムが使用するファイルおよびフォルダを一覧から除外するかどうかを設定する方法については，「コマンドリファレンス」（IF311）を参照してください。

- システムが使用するファイルおよびフォルダを一覧から除外するよう設定した場合，またはABE（Access Based Enumeration：アクセスベースの列挙）を有効にした場合，表示されないファイルまたはフォルダが格納されているフォルダを削除しようとすると，削除に失敗します。
  このとき，エラーは表示されず，CIFS クライアントからはフォルダが削除されたように見えますが，再表示すると，対象のフォルダが表示されます。
- ファイルの所有者がエクスプローラを使用して，アクセスが許可されていないファイルのアクセス権限を変更すると，エラーが発生してプロパティ画面を操作できなくなるおそれがあります。アクセスが許可されていないファイルのアクセス権限は変更しないでください。ファイルにアクセスできなくなった場合は，CIFS 管理者またはアクセスが許可されているユーザーがアクセス権限を変更してください。
- robocopy でファイルやフォルダを移行する場合，robocopy のエラー有無に関わらずSACL（監査 ACL）は移行されません。
- Windows の API を使用して CIFS 共有のファイルにアクセスする場合，クライアントから CreateFile() でファイルをオープンするときは，FILE_READ_DATA を含むアクセスマスクを指定してファイルをオープンしてください。アクセスマスクに FILE_WRITE_DATA を指定し，かつ FILE_READ_DATA を指定していないファイルをオープンし，ファイルのハンドルに LockFileEx() で LOCKFILE_EXCLUSIVE_LOCK を指定しないでファイルをロックすると，LockFileEx() が ERROR_INVALID_HANDLE でエラーとなります。なお，FILE_READ_DATA や FILE_WRITE_DATA のほか，GENERIC_READ や GENERIC_WRITE を指定する場合も同様です。
- プリンターなどの機能を持った複合機からのアクセスはサポートしていません。
- UPN(ユーザープリンシパル名：” ユーザー名 @ ドット付きのドメイン名 ” の形式) でユーザー名を指定し，CIFS アクセスする場合，下記のすべての条件を満たしている必要があります。
  - HVFP の認証方式が Active Directory 認証である。
  - CIFS クライアントが HVFP と同じドメインに参加している。
  - HVFP のホスト名 (ノードのホスト名，または，Virtual Server 名) が DNS に登録されている。
    例)
    HVFP のホスト名 ：host1
    DNA(A レコード) ：host1 ←→ 192.168.10.30
  - CIFS クライアントが HVFP のホスト名を使用してアクセスする。
    例) 共有ディレクトリ "share" へアクセスする場合，下記のどちらの指定方法でも UPN 指定でのアクセスが可能です。
    \\host1.sample.local\share (FQDN 指定)
    \\host1\share
- システムが使用するファイルおよびフォルダの所有者，ACL 設定，名称を変更しないでください。システム情報の不整合やユーザデータの消失を引き起こす可能性があります。

7.3 Anti-Virus Enabler を適用した環境での CIFS アクセスの留意事項

CIFS 共有のファイルを操作しようとしたときに，対象のファイルがウイルスに感染していたり，リアルタイムスキャン処理中にエラーが発生したりすると，意図した操作結果と異なることがあります。例えば，CIFS 共有内に格納しようとしたファイルがウイルスに感染していた場合は，ファイルを格納できません。

Anti-Virus Enabler を使用した環境で，CIFS クライアントの使用状況によっては，CIFS クライアントのタイムアウトによるセッション切断が発生し，アプリケーションプログラムが異常終了することがあります。この現象が発生した場合には，次のメッセージが CIFS クライアント側に出力されます。

メッセージ

```
Anti-Virus Enabler環境でのCIFSクライアント異常内容は，次のとおりです。
エラー番号：6     ハンドルが無効です。
エラー番号：64    指定されたネットワーク名は利用できません。
エラー番号：121   セマフォがタイムアウトしました。
```

Anti-Virus Enabler 環境での CIFS クライアント要求が上記エラーとなった場合にクライアント側でのタイムアウトによるセッション切断を検知した CIFS ログでの異常内容は，次のとおりとなる場合があります。

/var/log/cifs/log.smbd での出力例

```
[2004/04/27 19:25:18, 0, pid=26428] lib/util_sock.c:write_socket_data(407)
write_socket_data: write failure. Error = Connection reset by peer
```

この現象が発生する条件は次のとおりです。

同一の CIFS クライアントから多重にファイルアクセスした場合

1 つの CIFS クライアントが多重にファイルアクセスした場合，各ファイルの open/close でウイルスチェックのために時間を要し，後続の CIFS アクセス要求が長時間待たされるので，CIFS クライアントでタイムアウトによるセッション切断となります。

CIFS クライアントから大容量のファイルをアクセスした場合

大容量のファイルをアクセスした場合，ファイルの open/close でウイルスチェックのために時間を要し，CIFS アクセス要求が長時間完了しないため，CIFS クライアントでタイムアウトによるセッション切断となります。

この現象が発生する場合の処置は次のとおりです。

同一の CIFS クライアントから多重にファイルアクセスする場合

CIFS クライアント側の運用によって，シーケンシャルにアクセスするなど，多重アクセスを抑えてウイルススキャンに掛かる待ち時間を短縮してください。

CIFS クライアントから大容量のファイルをアクセスした場合

アクセスしたファイルのウイルススキャンは最後まで実行されます。このため，そのファイルに再度アクセスすることによって，ウイルススキャン無しでファイルにアクセスできます。

複数の CIFS クライアントから同時に CIFS アクセスした場合でも，スキャンサーバの処理性能，台数，ネットワーク環境によって，CIFS クライアントでタイムアウトによるセッション切断とな

ることがあります。この場合は，スキャンサーバを複数使用することでスキャン処理による待ち時間を短縮できます。

トレンドマイクロ社のスキャンソフトを使用する場合で，かつ CIFS サービスの構成定義として［Host access restrictions］でノードまたは Virtual Server にアクセスするクライアントホストを制限している場合は，スキャンサーバのホスト名またネットワークアドレスについてはアクセスを許可する設定にしてください。

フェールオーバーが原因でウイルススキャンに失敗することがあります。この場合は，再度そのファイルにアクセスすればスキャンが実行されます。

トレンドマイクロ社のスキャンソフトを使用する場合，［Access Protocol Configuration］ダイアログの［CIFS Service Maintenance］ページの［Current number of CIFS login clients］に表示されるログイン中の CIFS クライアント数，および MIB 情報の現在のセッション数には，登録したスキャンサーバの台数が含まれています。

7.4 ホームドライブを設定するとき

HVFP で提供する CIFS 共有内のディレクトリは，CIFS クライアントのホームドライブに割り当てることができます。

設定方法によっては，ホームドライブを設定するときにホームディレクトリが自動的に作成されます。ホームディレクトリが自動的に作成されない場合は，手動で作成するか，HVFP が提供するホームディレクトリの自動作成機能を利用してください。ホームドライブの設定例を次に示します。

Windows のプロパティ画面でユーザーごとに設定する

管理対象のユーザーのプロパティ画面から，ホームドライブ（接続ドライブ）およびホームディレクトリ（ホームフォルダ）のパスを設定できます。この操作は，CIFS 管理者として設定されたユーザーまたは CIFS 管理者として設定されたグループに属するユーザーが実施する必要があります。ユーザーマッピングを使用している環境で運用してください。
Windows のプロパティ画面でホームドライブを設定した場合，ホームディレクトリが自動的に作成されます。

Windows が提供するユーザー登録コマンドで一括して設定する

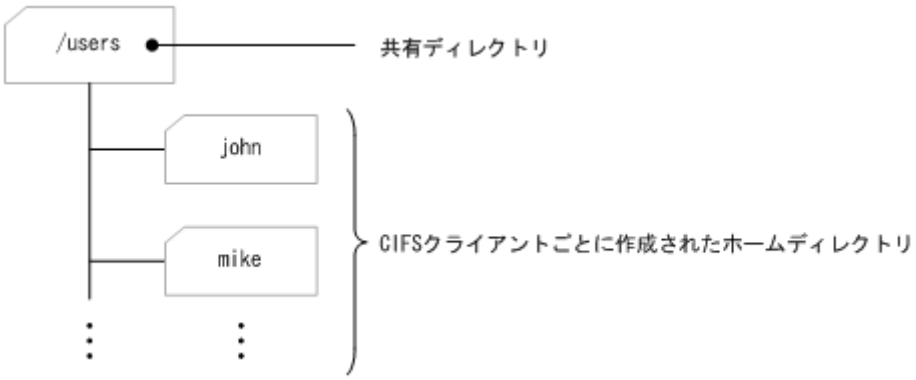
コマンドを利用して複数ユーザーを登録する際に，ホームドライブおよびホームディレクトリのパスを設定できます。コマンドを利用してホームドライブを設定しても，ホームディレクトリは自動的に作成されません。

7.4.1 ホームディレクトリの自動作成機能とは

HVFP では，共有ディレクトリを作成するときにホームディレクトリの自動作成機能を有効にすることで，CIFS クライアントが CIFS 共有にアクセスした際に自動的にホームディレクトリが作成されます。CIFS クライアントのユーザー名をすべて小文字に変換した文字列が，自動作成されたディレクトリの名称となります。

自動作成されるホームディレクトリの構成を次の図に示します。

図 7-1： 自動作成されるホームディレクトリの構成



Advanced ACL タイプのファイルシステムで自動作成されるディレクトリのアクセス権は，親ディレクトリの ACL に依存します。親ディレクトリから継承する ACL がない場合，ホームディレクトリを利用する CIFS クライアントには，フルコントロールのアクセス許可（このフォルダ，サブフォルダおよびファイルにも ACL を適用）のアクセス権が与えられます。親ディレクトリから継承する ACL がある場合，自動作成されるディレクトリには継承する ACL だけが与えられ，ホームディレクトリを利用する CIFS クライアントのアクセス権が自動で個別に与えられることはありません。

Classic ACL タイプのファイルシステムで自動作成されるディレクトリのアクセス権は，次のとおりです。

- ホームディレクトリを利用する CIFS クライアント：`rwx`
- ホームディレクトリを利用する CIFS クライアントが属するグループ：`--x`
- その他のユーザー：`--x`

7.4.2 ホームディレクトリの自動作成機能を利用する前に

ホームディレクトリの自動作成機能を利用するかどうかは，CIFS 共有を作成する際に設定する必要があります。システム管理者は，ホームディレクトリの自動作成機能を利用する前に次のことを確認してください。

- CIFS クライアントがゲストアカウント（nobody）でファイルシステムにアクセスした場合，ホームディレクトリは作成されません。
- ホームディレクトリの自動作成機能を有効にすると，ホームドライブを設定していない CIFS クライアントがファイルシステムにアクセスしても，ディレクトリが作成されます。不要なディレクトリは，CIFS 管理者が削除してください。
- ホームディレクトリの自動作成機能を有効にすると，コンピュータアカウントでファイルシステムにアクセスしてもディレクトリが作成されます。不要なディレクトリは CIFS 管理者が削除するか，ディレクトリが作成されないようにコンピュータアカウントのアクセスを ACL や共有レベル ACL で制限するなどの対処を検討してください。
- ホームディレクトリの自動作成に失敗しても，CIFS クライアントには通知されません。コマンドプロンプトを起動してホームドライブが正しく設定されていることを確認するよう，CIFS クライアントに通知してください。
- CIFS クライアントのユーザー名に，次に示す文字以外の文字が使用されている場合は，手動でディレクトリを作成してください。
  - 英数字
  - マルチバイト文字

- 感嘆符（!），番号記号（#），ドル記号（$），パーセント（%），アンパサンド（&），アポストロフィ（'），始め丸括弧（(），終わり丸括弧（)），ハイフン（-），ピリオド（.），アクサンシルコンフレックス（^），アンダーライン（_），アクサングラーブ（ ` ），始め波括弧（{），終わり波括弧（}），波ダッシュ（~）およびスペース

- ユーザー名がドメイン間で重複している場合は，ディレクトリの自動作成が失敗します。自動作成されるディレクトリ名が重複しないよう，ドメインごとに CIFS 共有を分けて運用することを推奨します。
- CIFS クライアントのユーザー名として，HVFP システムの予約語となっているユーザー名に加えて，次に示すものも使用しないでください。ユーザー名の予約語については，「ユーザーズガイド」（IF305）を参照してください。
  - .arc
  - .backupdates
  - .history
  - .lost+found
  - .snaps
  - .system_gi
  - .system_reorganize
  - .temp_backupdates
  - lost+found
  - schedule_syslu_backup.tgz
- UNC 形式のパス名（\\ サーバ名 \ 共有名 \・・・）でホームディレクトリにアクセスする場合，共有名を省略できません。

7.4.3 ホームドライブの運用を開始する

ホームドライブの運用を開始するには，HVFP で必要な設定をしたあと，CIFS クライアント環境でホームドライブを設定します。HVFP で必要な設定手順の一例と推奨値を次に示します。

1. CIFS 管理者を設定します。
   ［Access Protocol Configuration］ダイアログの［CIFS Service Management］ページ（Setting Type：Administration）で，Windows のプロパティ画面を利用してホームドライブを設定するユーザーまたはそのユーザーが属するグループを CIFS 管理者に設定してください。
2. ファイルシステムを構築・マウントします。
   ［ファイルシステム構築］ダイアログで，ファイルシステムを構築・マウントしてください。
3. CIFS 共有を作成します。
   ［共有追加］ダイアログで必要な項目を指定し，ホームディレクトリの親ディレクトリとなる CIFS 共有を作成してください。なお，ほかの CIFS クライアントからホームディレクトリへの不正なアクセスを防ぐため，次の値を設定することを推奨します。

表 7-5：［共有追加］ダイアログで指定する推奨値

タブ	項目	推奨値
［ベーシック］	［プロトコル］	CIFS プロトコルを使用するよう［CIFS(Windows(R) クライアント用)］を指定します。
	［共有ディレクトリの所有者］	［ディレクトリ生成 / ディレクトリ権限変更］ ホームディレクトリの親ディレクトリとなる共有ディレクトリを作成するために指定します。 また，作成する共有ディレクトリの所有ユーザーと所有グループを次のとおり指定します。 所有ユーザー：root 所有グループ：root
［アクセス制御］	［閲覧可能共有］	CIFS クライアント環境で CIFS 共有名を一覧に表示しないようにするためにチェックボックスのチェックを外します。
	［ACL 登録ユーザー / グループ］（Advanced ACL タイプのファイルシステムの場合）	作成する CIFS 共有の ACL を次のとおり指定します。 ［ユーザー名 / グループ名］ Windows ドメインのビルトインアカウントの Everyone をグループとして指定します。 ［権限］ ［フルコントロール権限］でアクセス許可を指定します。
	［新規ディレクトリのアクセス権限］（Classic ACL タイプのファイルシステムの場合）	作成する CIFS 共有のアクセス権を次のとおり指定します。 所有者：RW（読み取りおよび書き込みを許可） グループ：RO（読み取りだけを許可） その他：RO（読み取りだけを許可）
［アドバンスド］	［ホームディレクトリ自動作成を有効にする］	ホームディレクトリの自動作成機能を有効にするためにチェックボックスをチェックします。

注

［ファイルシステム構築と共有作成］ダイアログで CIFS 共有を作成する場合は，このほか，［これらの ACL を，このフォルダ，サブフォルダおよびファイルに適用する］のチェックボックスのチェックが外れていることを確認してください。

4. 必要に応じて，デフォルト ACL を設定します。
   Classic ACL タイプのファイルシステムで自動的に作成されたホームディレクトリのアクセス権を変更する場合は，dirsetacl コマンドでデフォルト ACL を設定してください。

7.5 Windows の移動ユーザープロファイル機能を利用する場合の注意事項

Windows の移動ユーザープロファイル機能を利用して，CIFS クライアントのユーザープロファイル保存先として HVFP の CIFS 共有を指定する場合の注意事項を示します。。

- ユーザー名称にパーセント（%）を含むユーザーは移動ユーザープロファイル機能を利用できません。
- 移動ユーザープロファイル機能を利用すると，ユーザープロファイルのデータは，Windows へのログオン時に HVFP の CIFS 共有からダウンロードされて CIFS クライアントに適用されます。このため，ユーザープロファイルのデータ容量が大きい場合には，Windows へのログオン処理に時間が掛かります。この場合は，Windows のフォルダリダイレクト機能を使用し，ユーザープロファイルの一部のフォルダ（例えば，多くのデータが保存されおそれがある

「ドキュメント」フォルダなど）は，ユーザープロファイル保存先配下のフォルダなどにリダイレクトされるように設定してください。

8

CIFS 共有内のファイル・フォルダ

この章では，CIFS 共有のディレクトリ内に作成するファイル・フォルダに関する注意事項について説明します。

8.1 ファイル・ディレクトリ名称

ファイル名およびディレクトリ名の注意事項について説明します。

8.1.1 サポート文字

HVFP では，各国語サポートのため UTF-8 でエンコードしたファイル名およびディレクトリ名を使用しています。CIFS 共有上のファイル名およびディレクトリ名の最大長は次の表のようになります。

表 8-1： ファイルおよびディレクトリ名の最大長

対象	名称の最大長*
	Windows・HVFP
ファイル名	255 文字
ディレクトリ名	244 文字
ファイルパス名	259 文字
ディレクトリパス名	247 文字

注＊

CIFS クライアントからエクスプローラを使用してアクセスするときの最大長です。使用するアプリケーションによっては，最大長が異なることがあります。

注意：

- マルチバイト文字は 1 文字として換算します。
- サロゲートペア文字は 2 文字として換算します。
- Variation Selector（異体字選択子）と呼ばれるコードを付加した文字は 3 文字として換算します。ただし，HVFP の GUI やコマンドでは 2 文字として換算します。

また，Volume Shadow Copy Service を使用して差分スナップショットにアクセスする場合は，名称の最大長よりが 25 文字短くなります。なお，クライアントからアクセスできるファイル名，ディレクトリ名およびパス名の最大長は，クライアントによって異なることがあります。

上記の最大長を超えた名称を指定してファイル・ディレクトリの作成や名称の変更をした場合，その操作がエラーとなることがあります。最大長に近い名称のファイル名およびディレクトリ名は使用しないでください。

ファイル名およびディレクトリ名として，次に示す文字やパス名は使用しないでください。

- ファイル名およびディレクトリ名末尾のスペース
- ファイル名およびディレクトリ名末尾のピリオド (.)
- ファイル名およびディレクトリ名の引用符（"），アステリスク（*），斜線（/），コロン（:），始め山括弧（<），終わり山括弧（>），疑問符（?），円記号（\）および縦線（|）

8.1.2 ファイル名およびディレクトリ名の最大長に関する注意事項

8.1.2.1 CIFS クライアントからアクセスする場合

HVFP で使用する機能によっては，自動的にパスが付与されるため，元のファイルやディレクトリのパス長より長くなることがあります。このとき，パス長が上限を超えると，CIFS クライアントからファイルやディレクトリにアクセスできなくなります。ファイルやディレクトリのパス長は，ホスト名または IP アドレス，および CIFS 共有名を含むほか，次に示す注意事項を考慮し

て上限を超えないようにしてください。ファイルパス名およびディレクトリパス名の最大長については，「8.1.1 サポート文字」を参照してください。

差分スナップショットを使用する場合：

- 差分スナップショットをファイルシステムの共有内に公開する場合，差分スナップショットのパス長が「\.snaps\all\YYYY_MM_DD_hhmm」分の 27 文字長くなります。
- 差分スナップショットにファイル共有を作成する場合，差分スナップショットの CIFS 共有名の文字数が，ファイルシステムの CIFS 共有名の文字数より大きいと，その差分だけ差分スナップショットのパス長が長くなります。

Backup Restore を使用する場合：

- Backup Restore のボリュームレプリケーション連携機能を使用する場合，コピー先のホスト名または IP アドレス，および CIFS 共有名の文字数の合計がコピー元の値より大きいと，その差分だけパス長が長くなります。

File Remote Replicator を使用する場合：

- File Remote Replicator を使用する場合に，プライマリーサイトとセカンダリーサイトを切り替える運用で，切り替え前のセカンダリーに相当するサイトのファイルシステムに CIFS 共有を作成する際は，切り替え前のセカンダリーサイトのホスト名または IP アドレス，および CIFS 共有名の文字数の合計が切り替え前のプライマリーサイトの値より大きいと，その差分だけ切り替え後のプライマリ ― サイトでのパス長が長くなります。
- File Remote Replicator で最新差分スナップショットを公開している場合，セカンダリーサイトでの最新差分スナップショットのパス長は「\.snaps\all\YYYY_MM_DD_hhmm」でアクセスすると 27 文字長くなります。また，「\.snaps\latest」でアクセスすると 14 文字長くなります。この時 , セカンダリーサイトのホスト名または IP アドレス，および CIFS 共有名の文字数の合計がプライマリーサイトの値より大きいと，その差分も含めて最新差分スナップショットのパス長は長くなります。

ほかのファイルサーバからデータをインポートする場合：

- ほかのファイルサーバからデータをインポートする場合，移行先のホスト名または IP アドレス，および CIFS 共有名の文字数の合計が移行元の値より大きいと，その差分だけパス長が長くなります。

NDMP 機能を使用する場合：

- NDMP 機能を使用している場合，元のパス名より文字数の大きいパス名のディレクトリを指定してリストアすると，その差分だけパス長が長くなります。

8.1.2.2 連携している機能から CIFS クライアントとしてアクセスする場合

CIFS クライアントからアクセスするファイルやディレクトリのパス長が長くなると，連携している機能が正常に動作しなくなるおそれがあります。ファイルやディレクトリのパス長は，ホスト名または IP アドレス，および CIFS 共有名を含むほか，次に示す注意事項を考慮して上限を超えないようにしてください。ファイルパス名およびディレクトリパス名の最大長については，「8.1.1 サポート文字」を参照してください。

- トレンドマイクロ社のスキャンサーバを使用する場合，スキャンサーバはスキャン対象のファイルに CIFS クライアントとして次の形式でアクセスします。
  \\ ＜ホスト名または IP アドレス＞ \C$\ ＜ファイルシステム名＞ \ ＜ファイルパス＞

8.1.3 8.3 形式の MS-DOS ファイル名

HVFP では，一部のアプリケーションなどで表示される 8.3 形式の MS-DOS ファイル名が，Windows とは異なる規則によって生成されます。HVFP での長いファイル名に対する 8.3 形式の名前を確認するためには，コマンドプロンプトで次のコマンドを実行してください。

```
dir /x 対象のファイルまたはフォルダ名
```

フォルダ名やファイル名にマルチバイトの文字を含む場合，8.3 形式の名前が，実際の名前より長くなることがあります。そのため，実際のフォルダ名やディレクトリ名ではパスの最大長に達していなくても，8.3 形式の名前でパスの最大に達することがあります。8.3 形式の名前を使用するアプリケーションを使用する場合，実際の名前だけでなく，8.3 形式の名前でもパスの最大を超えないようにしてください。

8.1.4 CIFS 共有名の表示に関する注意事項

CIFS 共有名がすべて大文字の共有を，CIFS クライアントで表示すると，クライアントによっては CIFS 共有名が小文字で表示されることがあります。

CIFS 共有名に使用できる文字は，「ユーザーズガイド」（IF305）の CIFS 共有の作成および編集の共有名の項目を確認してください。

8.2 ファイル・ディレクトリの所有者および所有グループ

HVFP では，`Everyone`，`CREATOR GROUP` および `CREATOR OWNER` 以外の Windows ビルトインユーザー・グループが認識されません *。CIFS 共有内のファイル・ディレクトリの所有者および所有グループには，これらのユーザー・グループを指定しないでください。このほか，ユーザー名が単価記号（@）で始まるユーザー，およびドメイン名が単価記号（@）で始まるドメインに所属するユーザーも指定できません。

注 *

`cifsoptset` コマンドで，Windows ドメインのビルトインアカウントの `Authenticated Users` および `Network` に対して ACL 設定を有効にした場合は，`Authenticated Users` および `Network` を認識できます。Windows ドメインのビルトインアカウントの `Authenticated Users` および `Network` に対する ACL 設定を有効にするかどうかを設定する方法については，「コマンドリファレンス」（IF311）を参照してください。

8.3 ACL

任意のユーザーやグループに対して利用の許可（または拒否）を定義したものをアクセス制御エントリー（ACE : Access Control Entry）といい，これを集めたものを随意アクセス制御リスト（DACL : Discretionary Access Control List）といいます。Windows の NTFS でサポートされているアクセス制御リスト（ACL : Access Control List）とは，DACL，リソースへの成功または失敗したアクセス試行を記録するシステムアクセス制御リスト（SACL : System Access Control List）および所有者に関する ACE を総称したものを指します。なお，DACL は ACL と表現されることがあります。

HVFP で提供する ACL 機能には，POSIX ACL に準拠した ACL を設定できる Classic ACL タイプと，Windows の NTFS ACL に準拠した ACL を設定できる Advanced ACL タイプの 2 種類があります。ただし，Advanced ACL タイプでも，Windows の NTFS ACL との差異は一部存在します。

この節では，CIFS クライアントからの ACL の設定方法，Windows での ACL の仕様と HVFP での仕様，そして，ACL を利用する場合の注意事項について説明します。

なお，HVFP では，次に示すユーザー・グループに対する ACL を設定できません。

- ユーザー名が単価記号（@）で始まるユーザー
- ドメイン名が単価記号（@）で始まるドメインに所属するユーザー
- Everyone，CREATOR GROUP および CREATOR OWNER 以外の Windows ビルトインユーザー・グループ *

  注 *

  cifsoptset コマンドで，Windows ドメインのビルトインアカウントの Authenticated Users および Network に対して ACL 設定を有効にした場合は，Authenticated Users および Network を認識できます。Windows ドメインのビルトインアカウントの Authenticated Users および Network に対する ACL 設定を有効にするかどうかを設定する方法については，「コマンドリファレンス」（IF311）を参照してください。

8.3.1 Classic ACL タイプと Advanced ACL タイプの差異

HVFP での NTFS ACL 項目の適用範囲を，ファイルシステムの種類ごとに次の表に示します。

表 8-2： HVFP での NTFS ACL 項目の適用範囲

大項目	小項目 *	Classic ACL タイプ	Advanced ACL タイプ
DACL	アクセス権限	rwx パーミッションで実施（3 種類）	詳細設定可（14 種類）
	設定エントリー数	ファイル：63 フォルダ：126	ファイル：700 フォルダ：700
	参照権限	すべてのユーザー	ファイル所有者および READ_DAC 権限を持つユーザー
	更新権限	所有者，書き込み権限のあるユーザー	ファイル所有者および WRITE_DAC 権限を持つユーザー
SACL		未サポート	未サポート
所有者	ユーザー	可	可
	グループ	不可	可
	所有者変更	未サポート	可
	特権	ACL 設定・タイムスタンプ更新（POSIX 準拠）	ACL 設定・取得，所有者参照
	参照権限	すべてのユーザー	ファイル所有者および，READ_DAC 権限を持つユーザー
	更新権限	－	WRITE_OWNER 権限を持つユーザー

大項目	小項目 *	Classic ACL タイプ	Advanced ACL タイプ
ファイル属性	読み取り専用属性	可	可
	アーカイブ属性	未サポート	可
	システム属性	未サポート	可
	隠し属性	未サポート	可
	ディレクトリ属性	可	可
	暗号化属性	不可	不可
	圧縮属性	不可	不可
	オフライン属性	可	可
	ノーマルファイル属性	可	可
	一時ファイル属性	不可	不可
	スパースファイル属性	不可	不可
	リパースポイント属性	不可	不可
	非インデックス対象ファイル属性	不可	不可
拡張属性		不可	不可
ファイル時刻	精度	秒	秒
	更新権限	所有者および書き込み権限のあるユーザー	WRITE_ATTRIBUTES 権限のあるユーザー

（凡例）可：設定できる　不可：設定できない　－：該当しない

注 *

File Services Manager で登録した CIFS 管理者（root ユーザー）はアクセス権限の影響を受けません。

8.3.2 Classic ACL タイプ

Classic ACL タイプのファイルシステムを使用する際の注意事項を説明します。

なお，`dirsetacl` コマンドで Classic ACL タイプの ACL を設定した場合，設定した ACL の種別および設定対象によって，CIFS クライアントで［名前］と［適用先］に表示される情報が変わります。

設定した ACL の種別および設定対象と CIFS クライアントでアクセス制御に表示される内容の関係を次の表に示します。

表 8-3：設定した ACL と CIFS クライアントでアクセス制御に表示される内容の関係

HVFP での設定内容		CIFS クライアントで表示される内容	
ACL の種別	設定の対象	［名前］に 表示される内容	［適用先］に 表示される内容
アクセス ACL	オーナー	＜オーナー名＞	「このフォルダのみ」
	所有グループ	＜所有グループ名＞	
	その他	Everyone	
	特定のユーザー	＜ユーザー名＞または＜ユーザー登録時に設定したコメント＞	
	特定のグループ	＜グループ名＞	
	マスク	-	-
デフォルト ACL	オーナー	CREATOR OWNER	「サブフォルダとファイルのみ」
	所有グループ	CREATOR GROUP	
	その他	Everyone	
	特定のユーザー	＜ユーザー名＞または＜ユーザー登録時に設定したコメント＞	
	特定のグループ	＜グループ名＞	
	マスク	-	-

（凡例）-：何も表示されない

注

その他，特定のユーザー，特定のグループのアクセス ACL とデフォルト ACL に同じパーミッションを設定した場合，「適用先」には「このフォルダ，サブフォルダおよびファイル」が表示されます。

また，dirsetacl コマンドで設定した ACL は，指定したパーミッションによって，CIFS クライアントでアクセス権として表示される情報が変わります。設定したパーミッションと CIFS クライアントでアクセス権として表示される内容の関係を次の表に示します。

表 8-4：設定したパーミッションと CIFS クライアントでアクセス権として表示される内容の関係

CIFS クライアントで 表示される アクセス権の詳細	設定したパーミッション							
	7 (rwx)	6 (rw-)	5 (r-x)	4 (r--)	3 (-wx)	2 (-w-)	1 (--x)	0 (---)
フォルダのスキャン / ファイルの実行	○	×	○	×	○	×	○	×
フォルダの一覧 / 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	○	○	×	×	○	○	×	×
属性の書き込み	○	○	×	×	○	○	×	×
拡張属性の書き込み	○	○	×	×	○	○	×	×

CIFS クライアントで表示されるアクセス権の詳細	設定したパーミッション							
	7 (rwx)	6 (rw-)	5 (r-x)	4 (r--)	3 (-wx)	2 (-w-)	1 (--x)	0 (---)
サブフォルダとファイルの削除	○	×	×	×	×	×	×	×
削除	○	×	×	×	×	×	×	×
アクセス許可の読み取り	○	○	○	○	○	○	○	×
アクセス許可の変更	○	×	×	×	×	×	×	×
所有権の取得	○	×	×	×	×	×	×	×

（凡例）○：許可されている　×：許可されていない

8.3.2.1 CIFS クライアントからの ACL の設定方法

ここでは，CIFS クライアントからの ACL の設定方法について説明します。

CIFS クライアントからの ACL 設定

Windows では，NTFS でフォーマットされたディスク内のファイル・フォルダのプロパティを参照した場合「セキュリティ」の項目が表示されます。ここで該当ファイルに対して，システム内やドメイン内に存在するユーザーやグループ単位でアクセス権を指定できます。HVFP ではこのファイル・フォルダのプロパティ画面からの変更だけとなります。CACLS コマンドからの ACL の設定はサポートしていません。

ACL を設定できるユーザー

HVFP では，ファイル所有者，または File Services Manager で登録した CIFS 管理者だけがアクセス権限を設定できます。

ACL の設定でアクセスを許可する対象

ACL の設定でアクセスを許可する対象が，HVFP と Windows で異なります。Windows ではグループや Everyone の権限がオーナーの権限にも影響しますが，HVFP では影響しません。例えば，ファイルのオーナーがファイルにアクセスする場合，Windows では Everyone に許可を設定していれば，オーナーに許可を設定していなくてもアクセスできますが，HVFP では Everyone に許可を設定していても，オーナーに許可を設定していなければアクセスできません。これは，グループに関しても同様です。

すべてのアクセス権限を「なし」にした ACL エントリー

Windows では，すべてのアクセス権限を「なし」にした場合，そのエントリー自体が削除されます。このため，HVFP 上ですべてのアクセス権限を「なし」に設定した場合，次のような現象が発生することがあります。

- ファイルを Microsoft Word ／ Excel ／ PowerPoint で更新した際にそのエントリーが削除される，またはその他のユーザーの権限が付与される。
- 所有者または所有グループのアクセス権限を「なし」にした場合，ファイルの［プロパティ］－［セキュリティ］で ACL を設定した際に，所有者が変更される。

したがって，その他のユーザー（Everyone）以外は，すべてのアクセス権限を「なし」に設定しないでください。

アクセス許可の［拒否］設定

CIFS 共有上のファイル・フォルダに対しては，［拒否］のアクセス許可用チェックボックスは利用できません。アクセス制御（ACL）の設定は，［許可］のアクセス許可用チェックボックスを利用してください。

すべてのアクセスを制限する ACL 設定をする場合

アクセス制御（ACL）の設定は［許可］のアクセス許可用チェックボックスを利用する必要があるため，ACL を使用して特定のフォルダ・ファイルに対してすべてのアクセスを制限するよう設定する場合は，Everyone を「なし」にして特定ユーザー，グループに許可を与える運用としてください。

すべてのアクセス権限を削除する主な ACL 操作

設定されたすべての ACL エントリーまたはすべてのアクセス権限を削除することはできません。この削除要求は無効となります。この場合は，アクセス権限を「なし」にしてください。次に，すべてのアクセス権限を「なし」にする主な ACL 操作を示します。

- ACL 設定をしたファイル・フォルダのすべてのアクセス権限を「なし」にする場合，設定済みの ACL の［許可］チェックボックスのチェックをすべて外して，適用してください。
- ACL 設定をしたフォルダの配下にあるファイル・フォルダのすべてのアクセス権限を「なし」にする場合，次のどちらかを実行してください。
  ・デフォルト ACL が設定されていないフォルダで［子オブジェクトのアクセス許可すべてを，このオブジェクトからの継承可能なアクセス許可で置き換える］をチェックして適用する。
  ・すべてのアクセス権限を親フォルダから継承しているフォルダの親フォルダか，または親フォルダから継承しない ACL エントリーのアクセス権限がすべて「なし」になっているフォルダの親フォルダで，デフォルト ACL の［許可］チェックボックスのチェックをすべて外して，適用する。

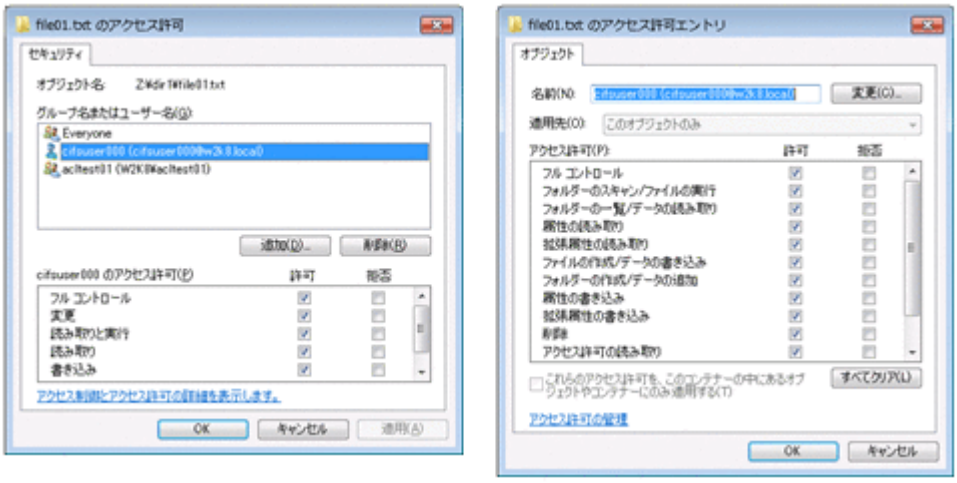
8.3.2.2 ファイルの ACL の設定・表示方法

ここでは，ファイルの ACL の設定と表示について説明します。

ファイルの ACL 設定・表示画面

ファイルのアクセス権限の設定には，次の図に示す，ファイルの［プロパティ］－［セキュリティ］－［編集］をクリックすると表示される基本設定画面と，ファイルの［プロパティ］－［セキュリティ］－［詳細設定］－［アクセス許可の変更］をクリックし対象のアクセス許可エントリーをダブルクリックすると表示される詳細設定画面を使用します。

図 8-1： ファイルの ACL 設定画面（左：基本設定画面，右：詳細設定画面）



ファイルの ACL 設定・表示での注意事項

- プロパティ画面の［グループ名またはユーザー名］には，システム管理者がユーザー登録するときに入力したコメントが表示されます。
- ファイルに対して ACL を設定できる数は，所有者（owner），グループ（group），その他（other），CIFS 環境用に登録されているユーザーおよびグループを合わせて最大 63 件となります。
- ファイルの所有者は変更できません。
- ファイルを作成したユーザーやグループは ACL から削除できません。
- オーナーの ACL から読み取り権限を削除することはできません。
- ファイルの［プロパティ］－［セキュリティ］でファイルに ACL を設定するときに設定内容の ACL にユーザーと主グループの組み合わせが存在しない場合は，設定要求のあった ACL に設定対象ファイルの所有者および所有グループの ACE が追加されて設定されます。
- CIFS 共有上のファイルに実行権限を設定しても，設定内容は無効です。
- 対象のファイルを CIFS 共有で作成したユーザー，または CIFS 管理者だけが ACL を設定できます。

ファイル所有者についての注意事項

- Microsoft Excel ／ Word ／ PowerPoint のファイル更新時に次の条件と一致した場合，ファイル更新後のファイル所有者が更新前の所有者およびファイル更新者以外のユーザーになる場合があります。
  ・更新前ファイル ACL に，ユーザーと主グループが含まれる組み合わせが複数存在する。
- ファイルの［プロパティ］－［セキュリティ］から ACL を設定するときに次の条件が重なった場合，ファイル所有者が ACL に存在するユーザーに変更されます。
  ・ファイル所有者と所有グループのどちらも存在しない
  ・ファイル所有者以外のユーザーと主グループの組み合わせが存在する

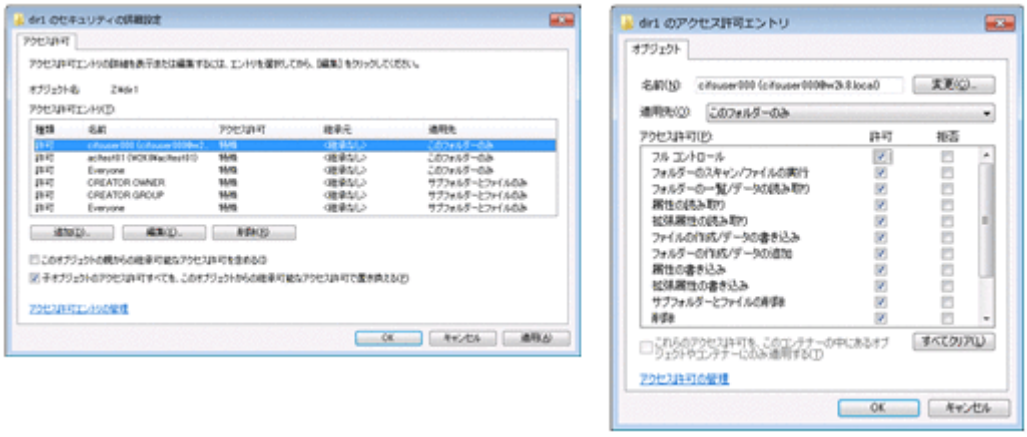
8.3.2.3 フォルダの ACL の設定・表示方法

ここでは，フォルダの ACL の設定と表示について説明します。

フォルダの ACL 設定・表示画面

フォルダのアクセス権限の設定には，プロパティを参照した場合の「セキュリティ」の基本設定画面ではなく，フォルダの［プロパティ］－［セキュリティ］－［詳細設定］－［アクセス許可の変更］をクリックし対象のアクセス許可エントリーをダブルクリックすると表示される詳細設定画面を使用してください。フォルダの ACL 設定画面を次の図に示します。

図 8-2： フォルダの ACL 設定画面



アクセス ACL とデフォルト ACL

フォルダに対する ACL にはデフォルト ACL とアクセス ACL が存在します。
設定したフォルダに作成されるサブフォルダとファイルへも反映される ACL をデフォルト ACL といい，設定したフォルダにだけ反映される ACL をアクセス ACL といいます。
HVFP でのオーナー，グループのデフォルト ACL はそれぞれ，Windows 上の CREATOR OWNER，CREATOR GROUP にマッピングされて表示されますが，これらの ACE は次の操作をした場合に生成されます。

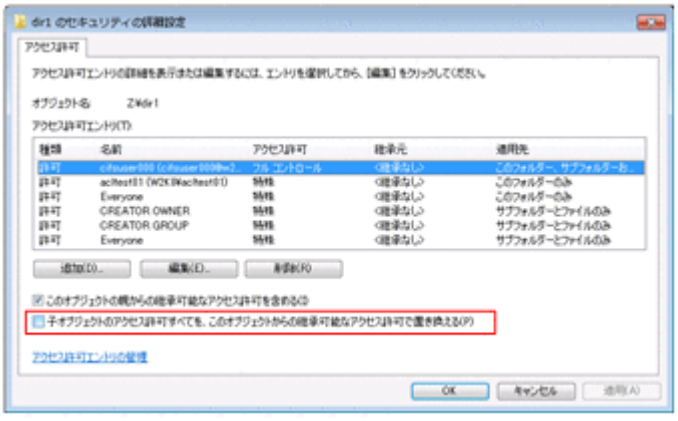
- デフォルト ACL がないフォルダ内でのフォルダの新規作成後，ユーザー ACL，グループ ACL の追加
- デフォルト ACL があるフォルダ内でのフォルダの新規作成

ACL の変更方法

図 8-3： フォルダに対するアクセス許可エントリーの例にフォルダに対するアクセス許可エントリーの例を示します。
アクセス ACL だけを変更する場合，詳細設定画面で表示される適用先に「このフォルダのみ」と表示される ACL を変更してください。
デフォルト ACL を変更する場合，変更対象がそのファイルのオーナーまたはオーナーが属するグループか，それ以外かによって変更方法が異なります。次にそれぞれの変更方法を示します。

- オーナーまたはオーナーが属するグループの場合
  オーナーまたはオーナーが属するグループのデフォルト ACL を設定する場合，CREATOR OWNER または CREATOR GROUP をそれぞれ変更してください。
- 上記以外のユーザー，グループの場合
  詳細設定画面で表示される適用先が「サブフォルダとファイルのみ」と表示される名前とマッピングされるのがデフォルト ACL になります。これらの適用先を「このフォルダ，サブフォルダおよびファイル」に変更すると，デフォルト ACL とアクセス ACL の両方に同じ権限を設定できます。
  CREATOR OWNER または CREATOR GROUP，オーナー以外のユーザーおよびオーナーが属するグループ以外のグループで，適用先が「サブフォルダとファイルのみ」または「このフォルダ，サブフォルダおよびファイル」のアクセス許可エントリーを変更すると，継承によって下位のフォルダとファイルにアクセス権限が継承されます。親フォルダからのアクセス権限の継承については，「8.3.2.4 親フォルダからのアクセス権限の継承」を参照してください。

図 8-3： フォルダに対するアクセス許可エントリーの例



ACL の適用先

詳細設定画面（図 8-2： フォルダの ACL 設定画面）では上記以外の適用先を選択することができますが，適用先によってアクセス ACL またはデフォルト ACL が変更されるか，どちら

の ACL も変更されない場合があります。適用先とアクセス ACL，デフォルト ACL のマッピングについては次の表を参照してください。

表 8-5：適用先とアクセス ACL，デフォルト ACL のマッピング

Windows で選択できる適用先	設定対象フォルダで変更される ACL		
	対象がオーナー，オーナーが属するグループの場合	対象が CREATOR OWNER，CREATOR GROUP の場合	対象がオーナー以外のユーザーとグループ，Everyone の場合
このフォルダのみ	アクセス ACL	適用されない	アクセス ACL
このフォルダ，サブフォルダおよびファイル	― *	適用されない	アクセス ACL デフォルト ACL
このフォルダとサブフォルダ	アクセス ACL	適用されない	アクセス ACL
このフォルダとファイル	アクセス ACL	適用されない	アクセス ACL
サブフォルダとファイルのみ	― *	デフォルト ACL	デフォルト ACL
サブフォルダのみ	適用されない	適用されない	適用されない
ファイルのみ	適用されない	適用されない	適用されない

（凡例）―：該当しない

注 *

対象がオーナーまたはオーナーが属するグループの場合には，適用先を「このフォルダ，サブフォルダおよびファイル」または「サブフォルダとファイルのみ」に変更しないでください。変更した場合，下位フォルダとファイルの権限変更が不正に行われるおそれがあります。オーナーとオーナーが属するグループのデフォルト ACL は，それぞれ CREATOR OWNER と CREATOR GROUP の ACL で変更してください。

また，適用先によって下位フォルダとファイルに対するアクセス権限の継承動作が異なります。適用先とアクセス権限の継承先については次の表を参照してください。

表 8-6：適用先と下位フォルダとファイルに対するアクセス権限の継承

Windows で選択できる適用先	アクセス権限の継承先（下位フォルダとファイルの内，変更される ACL[*1]）	
	対象がオーナー，オーナーが属するグループの場合	対象がオーナー，オーナーが属するグループ以外の場合
このフォルダのみ	なし	なし
このフォルダ，サブフォルダおよびファイル	なし[*2]	フォルダのアクセス ACL とデフォルト ACL，ファイルの ACL
このフォルダとサブフォルダ	なし	フォルダのアクセス ACL
このフォルダとファイル	なし	ファイルの ACL
サブフォルダとファイルのみ	なし[*2]	フォルダのアクセス ACL とデフォルト ACL，ファイルの ACL
サブフォルダのみ	なし	フォルダのアクセス ACL
ファイルのみ	なし	ファイルの ACL

注 *1

表中で変更対象であっても，［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］チェックボックスがチェックされていないフォルダとファイルの ACL は変更されません。このチェックボックスの詳細は「8.3.2.4 親フォルダからのアクセス権限の継承」を参照してください。

注 *2

対象がオーナーまたはオーナーが属するグループの場合には，適用先を「このフォルダ，サブフォルダおよびファイル」または「サブフォルダとファイルのみ」へ変更しないでください。変更した場合，下位フォルダとファイルの権限変更が不正に行われるおそれがあります。オーナーとオーナーが属するグループの権限を継承させる場合には，それぞれ CREATOR OWNER と CREATOR GROUP の ACL を変更してください。

フォルダの ACL 設定・表示での注意事項

- プロパティ画面の［グループ名またはユーザー名］には，システム管理者がユーザー登録するときに入力したコメントが表示されます。
- フォルダの ACL には，デフォルト ACL とアクセス ACL が存在するため，CREATOR OWNER，CREATOR GROUP が画面に表示されます。このため，設定できる ACL 数は，ファイルに対して ACL を設定できる数 63 件に，CREATOR OWNER，CREATOR GROUP を含むデフォルト ACL 63 件を合わせた，最大 126 件となります。
- フォルダの所有者は変更できません。
- フォルダを作成したユーザーやグループは ACL から削除できません。
- オーナーのアクセス ACL とデフォルト ACL（CREATOR OWNER）は，常にフルコントロールであり，変更できません。フォルダ作成時にオーナーに対する書き込み権限がない場合，最初の ACL 設定の際にオーナーの ACL にフルコントロールが設定されます。
- フォルダのセキュリティの詳細設定画面には，［子オブジェクトのアクセス許可すべてを，このオブジェクトからの継承可能なアクセス許可で置き換える］チェックボックス（図 8-3： フォルダに対するアクセス許可エントリーの例）が存在します。チェックすると，そのフォルダ配下のフォルダやファイルに個別に設定した権限が，継承できる親ディレクトリの権限（親ディレクトリのデフォルト ACL）に置き換えられ，上位フォルダからのアクセス許可の継承が有効になります。ただし，親ディレクトリのデフォルト ACL が設定されていない場合，継承する ACL が存在しないため，そのフォルダ配下のフォルダやファイルの ACL に変更はありません。
- フォルダのプロパティ画面から ACL を設定した場合，設定したアクセス権に関係なく，マスクにはフルコントロール（rwx）が設定されます。
- 対象のフォルダを CIFS 共有で作成したユーザー，または CIFS 管理者だけが ACL を設定できます。

8.3.2.4 親フォルダからのアクセス権限の継承

ここでは，親フォルダからのアクセス権限の継承について説明します。

新規ファイル・フォルダへのアクセス権限の継承

詳細設定画面（図 8-2： フォルダの ACL 設定画面）で適用先に「サブフォルダとファイルのみ」または「このフォルダ，サブフォルダおよびファイル」を選択した ACL が存在する場合，フォルダ下に新規にファイル・フォルダを作成した場合，親のフォルダのデフォルト ACL が継承され，「オーナーのアクセス ACL，オーナーが属するグループのアクセス ACL，Everyone のアクセス ACL」以外のアクセス ACL に反映されます。
HVFP の CIFS 共有にファイル・フォルダを新規に作成した場合に設定されるアクセス ACL の値を次の表に示します。

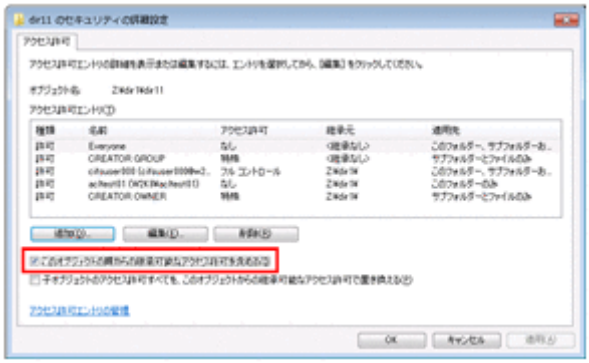
表 8-7：HVFP の CIFS 共有にファイル・フォルダを新規に作成したときに設定されるアクセス ACL の値

デフォルト ACL 設定有無	権限付与対象エントリー	設定されるアクセス ACL
なし	所有者	［新規ファイルのアクセス権限］/［新規ディレクトリのアクセス権限］指定値
	所有グループ	［新規ファイルのアクセス権限］/［新規ディレクトリのアクセス権限］指定値
	Everyone	［新規ファイルのアクセス権限］/［新規ディレクトリのアクセス権限］指定値
	追加した ACE	存在しない
所有者 所有グループ Everyone	所有者	デフォルト ACL と［新規ファイルのアクセス権限］/［新規ディレクトリのアクセス権限］指定値との論理積
	所有グループ	デフォルト ACL と［新規ファイルのアクセス権限］/［新規ディレクトリのアクセス権限］指定値との論理積
	Everyone	デフォルト ACL と［新規ファイルのアクセス権限］/［新規ディレクトリのアクセス権限］指定値との論理積
	追加した ACE	存在しない
所有者 所有グループ Everyone 追加した ACE	所有者	［新規ファイルのアクセス権限］/［新規ディレクトリのアクセス権限］指定値
	所有グループ	［新規ファイルのアクセス権限］/［新規ディレクトリのアクセス権限］指定値
	Everyone	［新規ファイルのアクセス権限］/［新規ディレクトリのアクセス権限］指定値
	追加した ACE	デフォルト ACL

既存ファイル・フォルダへのアクセス権限の継承

ファイル・フォルダのセキュリティの詳細設定画面には，［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］チェックボックスがあります（次の図）。このチェックボックスをチェックしている場合，親ディレクトリの権限の設定が変更された場合，該当するフォルダ下に存在するフォルダおよびファイルはその情報を継承し，アクセス権が自動的に変更されます。ファイルまたはフォルダの権限を個別に設定する場合には，このチェックボックスのチェックを外す必要があります。

図 8-4：アクセス許可の継承チェックボックス



既存ファイル・フォルダへのアクセス権限の継承有無

フォルダやファイルのプロパティで表示される［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］チェックボックスは，次の場合だけチェックしてください。

- 親フォルダにデフォルト ACL がない場合
- 親フォルダにデフォルト ACL があり，対象のフォルダやファイルの ACL とその親のデフォルト ACL が同じ場合

明示的にこのチェックを外すためには，このチェックボックスのチェックを外し，設定を適用してください。なお，このチェックボックスを外せるのは，そのファイルまたはフォルダの所有者，もしくは File Services Manager で登録した CIFS 管理者だけです。

XCOPY コマンドやバックアップユーティリティを用いて Windows ドメイン環境から資源を移行した場合には，［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］チェックボックスのチェック有無も ACL 情報とともに移行されます。

次に，フォルダの ACL を変更する時，ACL を親から継承させるためのユーザー操作について，Windows と HVFP での差異を次の表に示します。

表 8-8：ACL を親から継承させるためのユーザー操作の差異

サーバ	クライアント
	Windows
Windows	サブフォルダおよびファイルに対し，［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］にチェックを入れる。
File Services Manager	ACL を親フォルダのデフォルト ACL と同一にする。*

注 *

HVFP でも，親フォルダのデフォルト ACL が，対象のアクセス ACL よりも多くの権限を持っている場合には，［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］にチェックを入れることで，ACL を親から継承させることができます。それ以外の場合には，手動でアクセス ACL を親フォルダのデフォルト ACL と同一に設定する必要があります。

既存ファイル・フォルダへのアクセス権限を継承する場合の注意事項

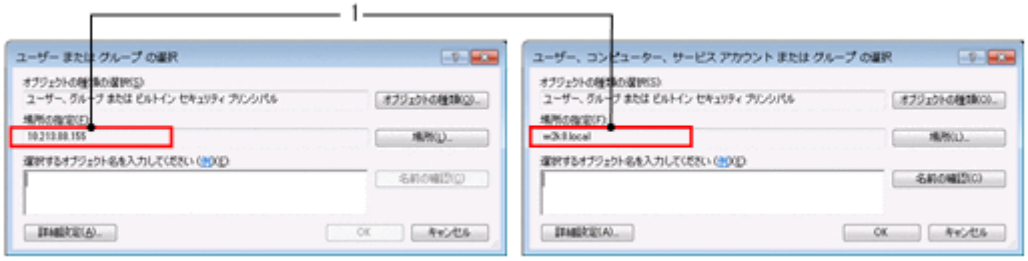
- ［このオブジェクトの親からの継承可能なアクセス許可を含める］チェックボックスがチェックされている場合でも，親フォルダのアクセス権限変更操作をしたユーザーと所有者が異なるフォルダとファイルについては，権限は変更されません。このようなフォルダとファイルの権限を変更する必要がある場合には，File Services Manager で登録した CIFS 管理者が ACL 設定をするか，各フォルダとファイルの所有者が直接，対象のフォルダまたはファイルの ACL 設定をするようにしてください。
- 親フォルダからの継承を有効にし，フォルダにデフォルト ACL を設定した状態で，ファイル所有者と更新ユーザーがそれぞれ異なる主グループに属している場合，Microsoft Excel ／ Word ／ PowerPoint によるファイル更新によって更新前の所有者，所有者の主グループに対する ACL は，それぞれファイル更新後の所有者，所有者の主グループに対する権限へと置き変わる場合があります。これによって，更新前の所有者および所有者の主グループに属するユーザーがアクセス不可となることがあります。

8.3.2.5 ユーザーおよびグループ ACL の追加

ここでは，ユーザーおよびグループの ACL の追加について説明します。

ユーザーおよびグループ ACL の追加は，ファイルまたはフォルダのアクセス許可画面の［追加］から行います。［追加］をクリックすると表示される［ユーザーまたはグループの選択］画面を次の図に示します。

図 8-5：ユーザーまたはグループ選択画面（左：ユーザーマッピングを使用しない場合，右：ユーザーマッピングを使用する場合）



CIFS 共有で作成したフォルダに対して，ファイルまたはフォルダのプロパティ画面で ACL を設定する場合，CIFS サービスの認証方式によって選択するユーザーまたはグループが属する［場所の指定］（上記の図の 1 で示す個所）が異なります。

ローカル認証，Active Directory 認証でユーザーマッピングを使用しない場合

［ユーザーまたはグループの選択］画面の［場所の指定］に HVFP のノードまたは Virtual Server のホスト名が表示されているユーザーまたはグループを選択する必要があります。

注意事項：

- Active Directory 認証を選択した場合，［ユーザーまたはグループの選択］画面の［場所の指定］にドメインコントローラーが表示されていることがありますが，このとき，ユーザーやグループに ACL を設定しても有効になりません。
- 図 8-5： ユーザーまたはグループ選択画面（左：ユーザーマッピングを使用しない場合，右：ユーザーマッピングを使用する場合）の左に示す［ユーザーまたはグループの選択］画面の［場所の指定］に HVFP のノードまたは Virtual Server のホスト名が表示されているユーザーを表示するためには，File Services Manager の［Local Users］ダイアログの［Add User］ページで CIFS ユーザーを登録する必要があります。
- グループを表示するためには，File Services Manager の［Local Users］ダイアログの［Add Group］ページでグループを追加する時に，［Apply to CIFS ACL environment］チェックボックスをチェックしてグループを登録する必要があります。
- 環境によって，ファイルまたはフォルダのアクセス許可画面からユーザーおよびグループ ACL を追加できないことがあります。その場合は，`dirsetacl` コマンドで設定してください。なお，ファイルに対して ACL を追加したい場合は，`dirsetacl` コマンドで対象のファイルに ACE が継承されるように，該当するディレクトリに対して ACE の継承範囲を設定してください。

Active Directory 認証でユーザーマッピングを使用する場合

［ユーザーまたはグループの選択］画面の［場所の指定］にドメインコントローラーが表示されているユーザーまたはグループを選択する必要があります。

［ユーザーまたはグループの選択］画面の［場所の指定］にドメインコントローラーが表示されない場合，次の原因によってドメインコントローラーと通信できていないおそれがあります。

- ［Access Protocol Configuration］ダイアログの［Active Directory Authentication］ページの［Domain name (NetBIOS)］に指定した値が誤っている。
- CIFS クライアントで，DNS によるドメインコントローラーの IP アドレスを解決できない。
- CIFS 操作をしているユーザーが，ドメインユーザーではない。

なお，［ユーザーまたはグループの選択］画面の［場所の指定］に HVFP のノードまたは Virtual Server のホスト名が表示されているユーザーまたはグループを選択することで，HVFP のローカルユーザーおよびローカルグループの ACL を設定できます。

注意事項：

・この場合は，図 8-5： ユーザーまたはグループ選択画面（左：ユーザーマッピングを使用しない場合，右：ユーザーマッピングを使用する場合）の左に示す［ユーザーまたはグループの選択］画面を使用します。その［場所の指定］に HVFP のノードまたは Virtual Server のホスト名が表示されているユーザーを表示するためには，File Services Manager の［Local Users］ダイアログの［Add User］ページで CIFS ユーザーを登録する必要があります。
・グループを表示するためには，File Services Manager の［Local Users］ダイアログの［Add Group］ページでグループを追加する時に，［Apply to CIFS ACL environment］チェックボックスをチェックしてグループを登録する必要があります。
・CIFS クライアントは，ドメインに参加している必要があります。参加していない場合，［ユーザーまたはグループの選択］画面の［場所の指定］に HVFP のノードまたは Virtual Server のホスト名を表示しても，HVFP のローカルユーザーおよびローカルグループは表示されません。
・環境によって，ファイルまたはフォルダのアクセス許可画面からユーザーおよびグループ ACL を追加できないことがあります。その場合は，`dirsetacl` コマンドで設定してください。なお，ファイルに対して ACL を追加したい場合は，`dirsetacl` コマンドで対象のファイルに ACE が継承されるように，該当するディレクトリに対して ACE の継承範囲を設定してください。

なお，CIFS サービスの認証方式に関わらず，ファイルまたはフォルダのアクセス許可画面からユーザーおよびグループ ACL を追加できない場合は，次のどれかの方法で追加できることがあります。

- 管理者（Administrators グループに所属するユーザー）で Windows クライアントにログオンする。
- Administrator でないユーザー（Windows クライアントに個別に追加したユーザー）で Windows クライアントにログオンする。
- ユーザーおよびグループ ACL の追加で認証ダイアログが表示された際に，HVFP に接続するときのユーザー名およびパスワードを入力する。
- HVFP に接続するときに指定するユーザー名およびパスワードと，Windows クライアントにログオンするときのユーザー名およびパスワードを同じにする。
- Windows クライアントからホスト名を指定して HVFP に接続する。
- Windows クライアントを Active Directory ドメインに参加させる。この場合，HVFP の認証方式や HVFP が参加するドメインと関係がなくても問題ありません。

8.3.2.6 ファイル作成時の ACL

HVFP では POSIX 準拠であり，ファイル作成時に ACL としてオーナー・グループが表示されます。設定される ACL については表 8-7： HVFP の CIFS 共有にファイル・フォルダを新規に作成したときに設定されるアクセス ACL の値を参照してください。

8.3.2.7 フォルダ作成時の ACL

フォルダもファイルと同様，フォルダ作成時に ACL としてオーナー・グループが表示されます。

フォルダ作成時に設定される ACL についても，ファイルと同様に表 8-7： HVFP の CIFS 共有にファイル・フォルダを新規に作成したときに設定されるアクセス ACL の値を参照してください。オーナーに対する ACL は，プロパティによる ACL 設定では常にフルコントロールが設定されます。

8.3.2.8 SACL

CIFS クライアントからの SACL 設定要求は無効です。設定要求が行われた場合，設定は無視されます（操作できるが，変更されません）。

8.3.2.9 無効な ACE

BUILTIN/Well-known SID アカウントの ACE，または UID，GID 解決不可の ACE は無視され，それ以外の ACE だけが設定されます。また，Active Directory や LDAP サーバに登録された UID，GID がマッピングされていない場合も同様です。

8.3.2.10 Windows での ACL 設定値の HVFP のファイルパーミッションへのマッピング

HVFP では POSIX 準拠の ACL を提供するため，Linux でのファイルパーミッション（rwx）を，基本設定および詳細設定で示される項目にマッピングします。CIFS クライアントで表示される Windows アクセス許可の項目と HVFP でのファイルパーミッションの関係を次の表に示します。

表 8-9： Windows アクセス許可の項目と HVFP でのファイルパーミッションの関係

#	Windows アクセス許可の項目		HVFP でのファイルパーミッション
	基本設定	詳細設定	
1	読み取り	フォルダの一覧 / データの読み取り	r - -
2		属性の読み取り	
3		拡張属性の読み取り	
4	読み取りと実行	項番 1 ～ 3 および項番 11	r - x
5	書き込み	ファイルの作成 / データの書き込み	- w -
6		フォルダの作成 / データの追加	
7		属性の書き込み	
8		拡張属性の書き込み	
9	変更	すべての許可チェックボックスがチェック	r w x
10	フルコントロール	すべての許可チェックボックスがチェック	r w x
11	―	フォルダのスキャン / ファイルの実行	- - x[*1]
12		サブフォルダとファイルの削除 [*2]	- - -
13		削除	
14		アクセス許可の読み取り	
15		アクセス許可の変更	

（凡例）―：該当する基本設定がないことを示します。

注 *1

HVFP の CIFS 共有に格納した実行ファイルの場合，「ファイルの実行」権限がない場合もそのファイルに対する「読み取り」権限があればファイルの実行ができます。

注 *2

HVFP では，「サブフォルダとファイルの削除」権限は「書き込み」権限に含まれます。したがって，削除するファイル・フォルダの親フォルダに「書き込み」権限がある場合に，削除ができます。

8.3.3 Advanced ACL タイプ

Advanced ACL タイプのファイルシステムを使用する際の注意事項を説明します。

8.3.3.1 CIFS クライアントからの ACL の設定・表示

ここでは，CIFS クライアントからの ACL の設定および表示について説明します。

なお，Advanced ACL タイプのファイルシステムでは，対象となるファイルまたはフォルダのプロパティ画面で，アクセス許可の読み取りおよびアクセス許可の変更の権限を許可されたアカウント，または CIFS サービスに登録されている CIFS 管理者だけが，ACL を設定できます。

ファイル・ディレクトリに設定できるアクセス権限

Advanced ACL タイプファイルシステムに対して CIFS クライアントから設定できるアクセス権限と対応する NTFS ACE マスクを次の表に示します。各アクセス権限について許可・拒否が選択できます。
許可・拒否が同時に指定された場合には，拒否が優先されます。

表 8-10：アクセス制御リストで指定するアクセス権限と NTFS ACE マスク

#	アクセス権限	許可または拒否される操作	NTFS ACE マスク
1	フォルダのスキャン *1	ユーザーがそのフォルダへのアクセス許可を持っていない状態での，そのフォルダ下のファイルまたはフォルダにアクセスするためのフォルダ間の移動	FILE_TRAVERSE
	ファイルの実行 *2	プログラム，ファイルの実行	FILE_EXECUTE
2	フォルダの一覧 *1	そのフォルダ内のファイル名とサブフォルダ名の表示	FILE_LIST_DIRECTORY
	データの読み取り *2	ファイルデータの読み取り	FILE_READ_DATA
3	属性の読み取り	読み取り専用属性および隠しファイル属性など，ファイルまたはフォルダの属性の表示	FILE_READ_ATTRIBUTES
4	拡張属性の読み取り	ファイルまたはフォルダの拡張属性の表示	FILE_READ_EA
5	ファイルの作成 *1	そのフォルダ内でのファイル作成	FILE_ADD_FILE
	データの書き込み *2	ファイルの変更および既存の内容の上書き	FILE_WRITE_DATA
6	フォルダの作成 *1	フォルダ内でのフォルダの作成	FILE_ADD_SUBDIRECTORY
	データの追加 *2	既存のデータの変更，削除，または上書きを伴わない，ファイルの末尾に対する変更	FILE_APPEND_DATA
7	属性の書き込み	読み取り専用属性または隠しファイル属性など，ファイルまたはフォルダの属性の変更	FILE_WRITE_ATTRIBUTES
8	拡張属性の書き込み	ファイルまたはフォルダの拡張属性の変更	FILE_WRITE_EA
9	サブフォルダとファイルの削除 *1	サブフォルダおよびファイルの削除（サブフォルダまたはファイルに削除アクセス許可が付与されていない場合を含む）	FILE_DELETE_CHILD
10	削除	ファイルまたはフォルダの削除（ただし，この削除アクセス許可がなくても，親フォルダに対する「サブフォルダとファイルの削除」が許可されていれば削除できます）	DELETE
11	アクセス許可の読み取り	ファイルまたはフォルダのアクセス許可の表示	READ_CONTROL
12	アクセス許可の変更	ファイルまたはフォルダのアクセス許可の変更	WRITE_DAC
13	所有権の取得	ファイルまたはフォルダの所有権の取得	WRITE_OWNER

注 *1

フォルダだけに適用される属性

注 *2

ファイルだけに適用される属性

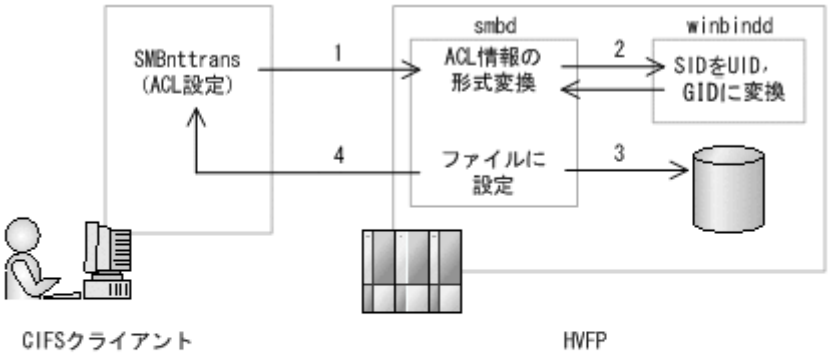
ファイル・ディレクトリへのアクセス権限設定

Advanced ACL タイプでは，CIFS クライアントから送信されたアクセス権限を HVFP 独自の形式に変換し，ファイルシステムに設定します。ACE の順序は CIFS クライアントから送信したものをそのまま引き継ぎます。

このとき，BUILTIN/Well-known SID アカウントまたは UID，GID 解決不可の ACE があった場合，そのエントリーはスキップして設定されます。

次の図に ACL 設定処理の概要を示します。

図 8-6：ACL 設定処理概要



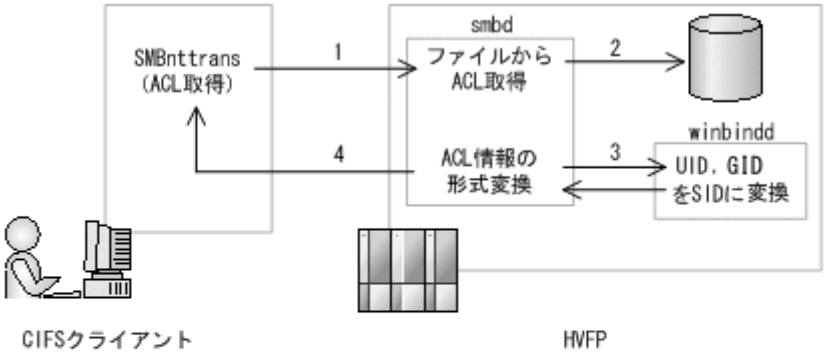
1 ACL設定要求
2 ACL情報の形式変換
主にSIDをUID，GIDに変換する。
ユーザーマッピングを使用しない場合，smbdで解決する。
3 ACLをファイルに設定
4 ACL設定結果を返却

ファイル・ディレクトリのアクセス権限取得

ファイル・ディレクトリから取得したアクセス権限を Windows での形式に変換し，CIFS クライアントに返却します。

次の図に ACL 取得処理の概要を示します。

図 8-7：ACL 取得処理概要



1 ACL取得要求
2 ファイルからACLを取得
3 Windowsでの形式に変換
主にUID，GIDをSIDに変換する。
ユーザーマッピングを使用しない場合，ユーザーマッピングで解決できない場合は，smbdで解決する。
4 ACLを返却

8.3.3.2 ファイルシステムルート ACL

Advanced ACL タイプファイルシステム作成直後のファイルシステムルート ACL のデフォルト値は次の表のとおりです。

表 8-11： ファイルシステムルート ACL のデフォルト値

名前	アクセス許可	適用先	Windows Server	Advanced ACL タイプ
Administrators	フルコントロール	このフォルダ，サブフォルダおよびファイル	○	－
SYSTEM	フルコントロール	このフォルダ，サブフォルダおよびファイル	○	－
CREATOR_OWNER	フルコントロール	サブフォルダとファイルのみ	○	－
Users	読み取りと実行	このフォルダ，サブフォルダおよびファイル	○	－
Users	フォルダの作成 / データの追加	このフォルダとサブフォルダ	○	－
Users	ファイルの作成 / データの書き込み	サブフォルダ	○	－
Everyone	フルコントロール	このフォルダ，サブフォルダおよびファイル	○ *	○

（凡例）○：存在する　－：存在しない

注 *

「アクセス許可」は「読み取りと実行」で，「適用先」は「このフォルダのみ」です。

8.3.3.3 ACL に関連する値

ACL は各ユーザーまたは各グループに対するアクセス権限を規定する ACE の集合から成ります。各 ACE は次の 4 要素から成ります。

- ユーザー名またはグループ名（に相当する ID）
- ACE エントリーが許可を意味するのか，拒否を意味するのかなどのエントリーの意味を規定する ACE タイプ
- どういったオペレーションに対してアクセス許可するのか，拒否するのかを規定する ACE マスク
- ACL の継承などを規定する ACE フラグ

また，NTFS ACL で使用される ACE タイプ，ACE マスク，ACE フラグの値と HVFP の Advanced ACL での対応を次の表に示します。

表 8-12： Advanced ACL タイプの ACE タイプ一覧

#	ACE タイプ	説明	対応
1	ACCESS_ALLOWED_ACE_TYPE	この ACE は許可エントリーである。	○
2	ACCESS_ALLOWED_CALLBACK_ACE_TYPE	アクセス許可時にアプリケーションが指定したコールバック関数を起動する。	×
3	ACCESS_ALLOWED_CALLBACK_OBJECT_ACE_TYPE	#2 の OBJECT に特化した ACE タイプ。	×

#	ACE タイプ	説明	対応
4	ACCESS_ALLOWED_COMPOUND_ACE_TYPE	(予約済み)	×
5	ACCESS_ALLOWED_OBJECT_ACE_TYPE	Active Directory のオブジェクトに対する許可エントリーである。	×
6	ACCESS_DENIED_ACE_TYPE	この ACE は拒否エントリーである。	○
7	ACCESS_DENIED_CALLBACK_ACE_TYPE	アクセス拒否時にアプリケーションが指定したコールバック関数を起動する。	×
8	ACCESS_DENIED_CALLBACK_OBJECT_ACE_TYPE	#7 の OBJECT に特化した ACE タイプ。	×
9	ACCESS_DENIED_OBJECT_ACE_TYPE	Active Directory のオブジェクトに対する拒否エントリーである。	×
10	ACCESS_MAX_MS_ACE_TYPE	(予約済み)	×
11	ACCESS_MAX_MS_V2_ACE_TYPE	(予約済み)	×
12	ACCESS_MAX_MS_V3_ACE_TYPE	(予約済み)	×
13	ACCESS_MAX_MS_V4_ACE_TYPE	(予約済み)	×
14	ACCESS_MAX_MS_OBJECT_ACE_TYPE	(予約済み)	×
15	ACCESS_MIN_MS_ACE_TYPE	ACCESS_ALLOWED_ACE_TYPE と同じ。	×
16	ACCESS_MIN_MS_OBJECT_ACE_TYPE	ACCESS_ALLOWED_OBJECT_ACE_TYPE と同じ。	×
17	SYSTEM_AUDIT_ACE_TYPE	監査関連	×
18	SYSTEM_ALARM_ACE_TYPE	(予約済み)	×
19	SYSTEM_ALARM_CALLBACK_ACE_TYPE	(予約済み)	×
20	SYSTEM_ALARM_CALLBACK_OBJECT_ACE_TYPE	(予約済み)	×
21	SYSTEM_ALARM_OBJECT_ACE_TYPE	(予約済み)	×
22	SYSTEM_AUDIT_CALLBACK_ACE_TYPE	監査関連	×
23	SYSTEM_AUDIT_CALLBACK_OBJECT_ACE_TYPE	監査関連	×
24	SYSTEM_AUDIT_OBJECT_ACE_TYPE	監査関連	×

(凡例) ○ : 対応している　× : 対応していない

表 8-13 : NTFS ACE マスク一覧と対応の有無

Bit	アクセス権	Windows GUI 上の表記	説明	対応
31	GENERIC_READ	—	次のフラグの組み合わせ FILE_READ_ATTRIBUTES FILE_READ_DATA FILE_READ_EA READ_CONTROL SYNCHRONIZE	○ *1
30	GENERIC_WRITE	—	次のフラグの組み合わせ FILE_APPEND_DATA FILE_WRITE_ATTRIBUTES FILE_WRITE_DATA FILE_WRITE_EA READ_CONTROL SYNCHRONIZE	○ *1

Bit	アクセス権	Windows GUI 上の表記	説明	対応
29	GENERIC_EXECUTE	－	次のフラグの組み合わせ FILE_READ_ATTRIBUTES READ_CONTROL SYNCHRONIZE FILE_EXECUTE	○ *1
28	GENERIC_ALL	－	次のフラグの組み合わせ DELETE_ACCESS READ_CONTROL_ACCESS WRITE_DAC_ACCESS WRITE_OWNER_ACCESS SYNCHRONIZE_ACCESS FILE_ALL_ACCESS（0 ～ 8 ビットすべて）	○ *1
27	（予約済み）	－	－	× *2
26	（予約済み）	－	－	× *2
25	（予約済み）	－	－	× *2
24	RIGHT_TO_ACCESS_SACL	－	－	× *3
23	（未割り当て）	－	－	× *2
22	（未割り当て）	－	－	× *2
21	（未割り当て）	－	－	× *2
20	SYNCHRONIZE	同期	そのファイルまたはディレクトリのハンドルで異なるスレッドが待機し，シグナルを発生させるほかのスレッドと同期することを許可する。	○
19	WRITE_OWNER	所有権の取得	所有権の取得	○
18	WRITE_DAC	アクセス許可の変更	DACL を変更できる。	○
17	READ_CONTROL	アクセス許可の読み取り	DACL を読める。	○
16	DELETE	削除	ファイルまたはディレクトリを削除できる。親ディレクトリに FILE_DELETE_CHILD 拒否エントリーが設定されていても，削除できる。	○
15	（未割り当て）	－	－	× *2
14	（未割り当て）	－	－	× *2
13	（未割り当て）	－	－	× *2
12	（未割り当て）	－	－	× *2
11	（未割り当て）	－	－	× *2
10	（未割り当て）	－	－	× *2
9	（未割り当て）	－	－	× *2
8	FILE_WRITE_ATTRIBUTES	属性の書き込み	NTFS 属性を書き込める。	○
7	FILE_READ_ATTRIBUTES	属性の読み取り	NTFS 属性を読み出せる。	○

Bit	アクセス権	Windows GUI 上の表記	説明	対応
6	FILE_DELETE_CHILD	サブディレクトリとファイルの削除	ディレクトリ内のファイルとサブディレクトリを削除できる。ただし，サブディレクトリ内のファイルやディレクトリに「読み取り専用属性」が設定されている場合は削除に失敗する。	○
5	FILE_EXECUTE	ファイルの実行	ファイルを実行できる。	○
	FILE_TRAVERSE	フォルダのスキャン	フォルダを走査できる。（UNIX との互換性のためにある）	○
4	FILE_WRITE_EA	拡張属性の書き込み	拡張属性を書き込める。	○ *4
3	FILE_READ_EA	拡張属性の読み取り	拡張属性を読み出せる。	○ *4
2	FILE_APPEND_DATA	データの追加	ファイルにデータを追加できる。	○
	FILE_ADD_SUBDIRECTORY	ディレクトリの作成	ディレクトリ内にサブディレクトリを作成できる。	○
1	FILE_WRITE_DATA	データの書き込み	ファイルにデータを書ける。	○
	FILE_ADD_FILE	ファイルの作成	ディレクトリ内にファイルを作成できる。	○
0	FILE_READ_DATA	データの読み取り	ファイルのデータを読める。	○
	FILE_LIST_DIRECTORY	ディレクトリの一覧	ディレクトリの内容をリスティングできる。	○

（凡例）○：対応している　×：対応していない　－：該当するものがない

注 *1

GENERIC_READ/GENERIC_WRITE/GENERIC_EXECUTE/GENERIC_ALL は，それ自体が固有のアクセス権を持つのではなく，ACL を設定するオブジェクト（ファイル，ディレクトリ，Active Directory のオブジェクトなど）に依存しないアクセス権を設定するために用意されているフラグです。ファイル・ディレクトリに対してこのフラグを指定した場合は，複数のアクセス権がまとめて設定されます。

注 *2

現状は未割り当て部分であるため，これらのビットが設定されている ACE を受け取った場合，そのビットを 0 にして処理します。

注 *3

このマスクは，ファイルやディレクトリに対して付加するものではなく，また HVFP では SACL には対応しないため，このビットが設定されている ACE を受け取った場合，クライアントにエラーを返します。

注 *4

拡張属性は OS/2 のファイルシステム HPFS 固有の属性であり XFS では対応していません。したがって，HVFP としてこれらのマスクに対して何らかの処理をする必要はないが，クライアントのファイルを HVFP にコピーしても情報が失われないように，ビットとしてはファイルシステム内にも確保・維持しています。

表 8-14： NTFS ACL の ACE フラグ一覧

bit	ACE フラグ	説明	対応
7	FAILED_ACCESS_ACE_FLAG	「アクセス失敗」の監査メッセージを残す。	×
6	SUCCESSFUL_ACCESS_ACE_FLAG	「アクセス成功」の監査メッセージを残す。	×
5	−	未使用（グループを表すビットとして流用予定）	−
4	INHERITED_ACE	ACE が祖先から継承されたものであることを示す。	○
3	INHERIT_ONLY_ACE	自分自身にはこの ACE は適用されないが，子孫のファイル・サブディレクトリにはこの ACE を継承する。	○
2	NO_PROPAGATE_INHERIT_ACE	OBJECT_INHERIT_ACE と CONTAINER_INHERIT_ACE の各フラグは継承しない。「これらのアクセス許可を，このコンテナの中にあるオブジェクトやコンテナにのみ適用する」に対応する。	○
1	CONTAINER_INHERIT_ACE	ディレクトリがこの ACE を継承する。	○
0	OBJECT_INHERIT_ACE	ファイルがこの ACE を継承する。	○

（凡例）○：対応している　×：対応していない　−：該当するものがない

表 8-15： Windows GUI 上の表記と ACE フラグの組み合わせ

Windows GUI 上の表記	表 8-14 での ACE フラグの組み合わせ *		
	#3	#1	#0
このディレクトリのみ	×	×	×
このディレクトリ，サブディレクトリおよびファイル	×	○	○
このディレクトリとサブディレクトリ	×	○	×
このディレクトリとファイル	×	×	○
サブディレクトリとファイルのみ	○	○	○
サブディレクトリのみ	○	○	×
ファイルのみ	○	×	○

（凡例）○：ビットが 1　×：ビットが 0

注 *

ACE フラグの組み合わせは，表 8-14： NTFS ACL の ACE フラグ一覧のビット位置を参照してください。#3，#1，#0 がビット位置を指しています。

8.3.3.4 ACL の評価

ファイルやディレクトリへのアクセス要求に対して，次の規則に従ってアクセス許可またはアクセス拒否を決定します。

- ACL が設定されていない場合（NULL ACL）は，すべてのアクセスを許可する。
- ACE が 0 個の場合（Empty ACL）は，すべてのアクセスを拒否する。ただし，ファイル所有者に限り，アクセス権の変更要求を許可する（”READ_CONTROL” と ”WRITE_DAC” の許可エントリーが設定されているものと見なす）。
- パーミッションに基づくファイル所有者 ACE，ファイル所有グループ ACE，Everyone の ACE を評価する。

ファイル所有者とファイル所有グループは，そのファイルおよびディレクトリの拒否の位置で評価し，Everyone は，その他の ACE を ACL のリストに並んでいる順に評価したあと評価します。

- ACL のリストに並んでいる順に ACE を評価する。
- 評価の結果が確定したら，その後に続く ACE は評価しない。
- アクセスを拒否するエントリーが見つかった場合は，「アクセス拒否」として評価を確定する。
- アクセスを許可するエントリーが見つかった場合は，「アクセス許可」として評価を確定する。
- すべての ACE に対して評価を確定できなかった場合は，「アクセス拒否」として評価を確定する。

Windows の CIFS クライアントは ACE の順序に責任を持ち，自身の持っている ACE の拒否，自身の持っている ACE の許可，親から継承した ACE の拒否，親から継承した ACE の許可，親の親から継承した ACE の拒否，親の親から継承した ACE の許可，の順に並べ替えて CIFS サーバに ACL の格納要求をします。HVFP はこの並びでクライアントが格納することを期待しており，並びが正しいかどうかのチェックはしません。

なお，Windows プロパティのセキュリティタブの詳細設定を開いた直後の並びは，ACE の評価順（ACL のリストに並んでいる順）と同じです。

上記の規則で評価するため，Everyone の拒否 ACE がある場合には，ユーザー ACE でいくら許可されていてもアクセスが拒否されることがあります。つまりパーミッションではユーザーが許可されているように見えてもアクセスできないことがあるので注意が必要です。

8.3.3.5 ACL の初期値と継承と伝播

新規に作成されたファイル・ディレクトリの ACL の初期値は，親ディレクトリの継承設定に従って継承されます。この ACE の継承は切ることができます。その際これまで継承していた ACE の内容をまったく破棄するか，継承していた ACE と同等の内容をそのファイル・ディレクトリそのものの ACE として取り込むかを選択できます。

ACE の継承をいったん切ったあと，継承を再び復活させることもできます。ただし，ACE の継承を切った際に同様の ACE を自身の ACE として取り込んだ場合，継承を復活させると同内容の ACE が重複して設定されることになるので注意が必要です。

なお，継承属性の ACE を変更した場合，子や孫にその変更を伝播させるのは CIFS クライアント側で行われます。NFS やその他のプロトコルからアクセスした場合には，継承属性の ACE 変更を伝播させることはできません。CIFS クライアント以外からアクセスしているときに継承属性の ACE を変更する場合は，アプリケーションの責任で伝播を行ってください。

8.3.3.6 ACE の重複チェック

CIFS クライアントから同一ユーザーや同一グループに対する ACE を 2 エントリー以上登録しても，HVFP 側では特にチェックしません。

8.3.3.7 SACL

CIFS クライアントからの SACL 設定要求は無効です。設定要求が行われた場合，設定は無視されます（操作できるが，変更されません）。

8.3.3.8 無効な ACE

BUILTIN/Well-known SID アカウントの ACE，または UID，GID 解決不可の ACE は無視され，それ以外の ACE だけが設定されます。また，Active Directory や LDAP サーバに登録された UID，GID がマッピングされていない場合も同様です。

8.3.3.9 ファイル所有者と UNIX パーミッション

Advanced ACL タイプのファイルシステムの「ファイル所有者」には，ユーザー，グループのどちらでも登録できます。HVFP の内部では，次の表に示すとおり，「ファイル所有者」と UNIX パーミッションの「ファイル所有ユーザー」と「ファイル所有グループ」を対応させています。このため，NFS から該当のファイルの情報を参照したり，パーミッション変更を行ったりする場合には注意が必要です。

表 8-16： UNIX パーミッションでのファイル所有者の扱い

ファイル所有者	UNIX パーミッションでの扱い	
	ファイル所有ユーザー	ファイル所有グループ
ユーザー	ファイル所有者の UID	ファイル所有者が属するプライマリーグループの GID
グループ	“groupowner” （システム用途の UID を割り当て）	ファイル所有者の GID

所有者として設定できるアカウント

Advanced ACL タイプファイルシステムでは，アクセス許可の読み取りおよび所有権の取得の権限を許可されたアカウント，または CIFS サービスに登録されている CIFS 管理者だけが，CIFS 共有で作成したファイルまたはフォルダの所有者を変更できます。
所有者として指定されるアカウントごとの設定可否を次の表に示します。

表 8-17： 所有者設定可否

アカウント	設定可否	所有者特権	備考
ユーザー	可	そのユーザー	－
グループ	可	そのグループに所属するすべてのユーザー	－
BUILTIN/Well-known SID アカウント	不可	－	XCOPY コマンドでの移行失敗を回避するため，エラーとはしないで，処理をスキップします。
SID 解決不可アカウント （ドメイン外ユーザー，削除済みのアカウントなど）	不可	－	

（凡例）－：該当しない

ファイル・ディレクトリへの所有者設定

CIFS クライアントから送信された所有者情報（SID）を HVFP 内部で UID，GID に変換し，設定ファイルシステムに設定します。
要求されたアカウントが BUILTIN/Well-known SID アカウントまたは UID，GID を解決できないアカウントであった場合，何もしないで正常終了します。

ファイル・ディレクトリの所有者取得

HVFP 内部でファイル・ディレクトリから取得した所有者情報（UID，GID）を SID に変換し，CIFS クライアントに返却します。

このとき，SID 変換できなかったエントリー（NFS アクセスユーザーなど，CIFS 管理外アカウント）が存在した場合，HVFP が独自の SID を生成します（Classic ACL タイプでも同様です）。この場合，CIFS クライアントでの表示では，ユーザー名ではなく SID が表示されます。

所有グループ設定可否

Advanced ACL タイプファイルシステムでも POSIX 互換として所有グループの設定・取得ができます。
ただし，所有者と異なり，ファイル作成だけでは設定されません。また，プロパティ画面など通常操作では設定・参照できなくて，Windows のコマンドでだけ操作できます。
Advanced ACL タイプファイルシステムでは，この所有グループはアクセス権限チェックでは使用しないで，Quota 管理でだけ使用します。また，Advanced ACL タイプファイルシステムでは，所有者にグループが設定されている場合には，所有グループは設定できません。
所有者の違いによる所有グループの設定可否を次の表に示します。

表 8-18：所有グループ設定可否

所有者	アカウント	設定可否	備考
ユーザーの場合	グループ	可	－
	BUILTIN/Well-known SID アカウント	不可	－
	SID 解決不可アカウント（ドメイン外ユーザー，削除済みのアカウントなど）	不可	XCOPY コマンドでの移行失敗を回避するため，エラーとはしないで，処理をスキップします。
グループの場合	－	不可	

（凡例）－：該当しない

ファイル・ディレクトリへの所有グループ設定

BUILTIN/Well-known SID アカウントおよび SID から GID 解決できないアカウント（ドメイン外グループ，ユーザーなど）が指定された場合，所有者グループ変更処理をスキップし，正常終了します。
また，所有者がグループとして設定されているファイル，ディレクトリに対するプライマリーグループの変更については，所有者グループの変更処理をスキップし，正常終了します。

8.3.3.10 ACL 最大設定数

Advanced ACL タイプファイルシステムのファイル・フォルダに対して設定できる ACL のエントリー数は，アクセス ACL とデフォルト ACL の総和となり，最大 700 件となります。

8.3.3.11 Advanced ACL タイプファイルシステムへの移行

HVFP では，既存の共有情報が格納されている Classic ACL タイプファイルシステムを Advanced ACL タイプファイルシステムで再マウントするか，fsctl コマンドでファイルシステム内の ACL タイプを Classic ACL から Advanced ACL のタイプに変換することで自動的に移行できます。

HVFP では，既存の共有情報が格納されている Classic ACL タイプファイルシステムを Advanced ACL タイプファイルシステムに移行できますが，次の点に注意してください。

- XCOPY コマンドやバックアップユーティリティなどでの移行
  Classic ACL タイプファイルシステムでは，ACL をプロパティ表示したときの内容と実際のアクセス評価の内容が異なることがあります。そのため，XCOPY コマンドなどで Classic ACL タイプファイルシステムから Advanced ACL タイプファイルシステムに移行する場合に

は，ACL をプロパティ表示したときのアクセス許可内容が移行されるので注意願います。つまり，移行後は移行以前のアクセス評価内容と異なることがあります。

8.3.3.12 継承 ACL がない場合のデフォルト設定 ACL

Advanced ACL タイプファイルシステムでは，フォルダおよびファイルが作成されると，親フォルダに設定された ACL の中から継承できる ACE を検索し，そのフォルダおよびファイルに設定します。親フォルダから継承できる ACL を取得できない場合，次の表に示す ACL をデフォルトとして設定します。

フォルダ作成の場合

表 8-19： フォルダのデフォルト継承 ACL

項目	内容
DOS 属性	DOS_ATTR_DIR
ACE 継承フラグ	なし
所有者	作成ユーザー
所有者グループ	作成したユーザーが属するグループ
ACE	CIFS 共有内に新規に作成するフォルダのアクセス権設定を省略するかオーナーだけにフルコントロールのアクセス権を与える設定にした場合 種類：許可 名前：作成ユーザー アクセス許可：フルコントロール 適用先：このフォルダのみ CIFS 共有内に新規に作成するフォルダのアクセス権を設定している場合* 種類：許可または拒否（指定したモードによる） 名前：作成ユーザー，作成ユーザーが属するグループ，その他のユーザー アクセス許可：設定されている許可 適用先：このフォルダのみ

注 *

この場合の注意事項については，「8.3.3.15 CIFS 共有内に新規に作成するフォルダやファイルにデフォルトで設定される ACL についての注意事項」を参照してください。

ファイル作成の場合

表 8-20： ファイルのデフォルト継承 ACL

項目	内容
DOS 属性	アーカイブ
ACE 継承フラグ	なし
所有者	作成ユーザー
所有者グループ	作成したユーザーが属するグループ

項目	内容
ACE	CIFS 共有内に新規に作成するフォルダのアクセス権設定を省略するかオーナーだけにフルコントロールのアクセス権を与える設定にした場合 種類：許可 名前：作成ユーザー アクセス許可：フルコントロール CIFS 共有内に新規に作成するフォルダのアクセス権を設定している場合* 種類：許可または拒否（指定したモードによる） 名前：作成ユーザー，作成ユーザーが属するグループ，その他のユーザー アクセス許可：設定されている許可

注 *

この場合の注意事項については，「8.3.3.15 CIFS 共有内に新規に作成するフォルダやファイルにデフォルトで設定される ACL についての注意事項」を参照してください。

8.3.3.13 Windows からの移行での注意点

Windows システムでは，デフォルトのセキュリティポリシー設定によって，すべてのユーザーに対して「走査チェックのバイパス」の特権が与えられています。そのため，Windows の NTFS ACL では，ほとんどの場合，フォルダの ACL で「フォルダのスキャン」権限が許可されていなくても，そのフォルダ配下のオブジェクト（フォルダ，ファイル）にアクセス権限があれば，オブジェクトの絶対パスを指定することで操作できます。

HVFP のファイルシステムでも，CIFS 走査チェックのバイパス機能によって，CIFS アクセスでは，上位のディレクトリにアクセス権限がなくても，目的のオブジェクト（フォルダ，ファイル）にアクセス権限があれば，そのオブジェクトの絶対パスを指定することで操作できます。

なお，バージョン 4.2.0-00 より前の HVFP から引き継いだファイルシステムは，CIFS 走査チェックのバイパス機能が無効に設定されています。CIFS 走査チェックのバイパス機能が無効な場合，目的のオブジェクトを操作するためには，そこに至るすべての上位ディレクトリに，ACL で「フォルダのスキャン」権限が許可されている必要があります。

CIFS 走査チェックのバイパス機能の詳細については，「システム構成ガイド」（IF302）を参照してください。

8.3.3.14 ファイル属性の変更について

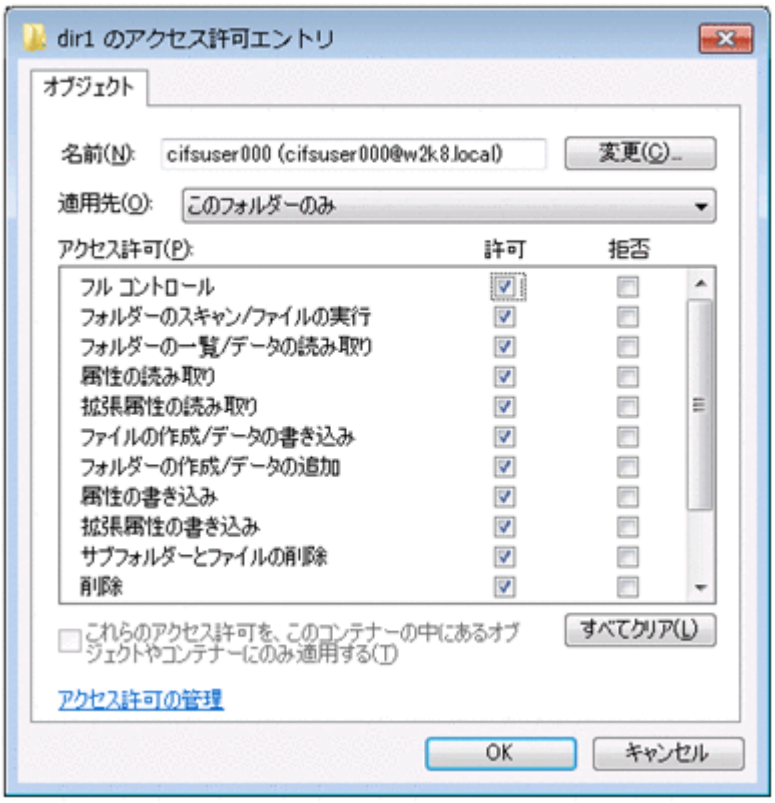
Advanced ACL タイプファイルシステムでファイル属性を変更した場合に，変更結果がエクスプローラの表示に即座に反映されないことがあります。その場合は，エクスプローラの［表示］メニューから［最新の情報に更新］を実行してください。

8.3.3.15 CIFS 共有内に新規に作成するフォルダやファイルにデフォルトで設定される ACL についての注意事項

CIFS 共有内に新規に作成するフォルダやファイルのアクセス権を設定した場合に，デフォルトで設定される ACL についての注意事項を示します。

- CIFS 共有内に新規に作成するフォルダやファイルに対して，HVFP で指定したアクセス権（rw，ro または none）が CIFS クライアントで表示される際，アクセス許可エントリーの項目（次の図を参照）によっては，Advanced ACL タイプと Classic ACL タイプのファイルシステムとで「許可」の内容が異なることがあります。

図 8-8：アクセス許可エントリーの例



「許可」の内容が異なる点を次の表に示します。なお，表に記載していないエントリー項目については，デフォルトで設定される ACL の内容に差異はありません。また，表中の「設定される」は CIFS クライアントで表示されるアクセス許可エントリー項目の「許可」がチェックされるという意味，「設定されない」は「許可」がチェックされないという意味です。

表 8-21：アクセス許可エントリーの表示項目と指定するアクセス権（rw，ro または none）の対応（フォルダの場合）

CIFS クライアントで表示されるアクセス許可エントリーの項目	Classic ACL タイプのファイルシステムの CIFS 共有に指定するアクセス権と NTFS ACL 設定有無	Advanced ACL タイプのファイルシステムの CIFS 共有に指定するアクセス権と NTFS ACL 設定有無
属性の読み取り	rw：設定される ro：設定される none：設定されない	rw：設定される ro：設定される none：設定される
削除	rw：設定される ro：設定されない none：設定されない	rw：設定されない ro：設定されない none：設定されない
アクセス許可の変更	rw：設定される ro：設定されない none：設定されない	アクセス権の設定対象がオーナーの場合 rw：設定される ro：設定される none：設定される アクセス権の設定対象がグループまたはその他の場合 rw：設定されない ro：設定されない none：設定されない

CIFS クライアントで表示されるアクセス許可エントリーの項目	Classic ACL タイプのファイルシステムの CIFS 共有に指定するアクセス権と NTFS ACL 設定有無	Advanced ACL タイプのファイルシステムの CIFS 共有に指定するアクセス権と NTFS ACL 設定有無
所有権の取得	rw：設定される ro：設定されない none：設定されない	アクセス権の設定対象がオーナーの場合 rw：設定される ro：設定される none：設定される アクセス権の設定対象がグループまたはその他の場合 rw：設定されない ro：設定されない none：設定されない

表 8-22：アクセス許可エントリーの表示項目と指定するアクセス権（rw，ro または none）の対応（ファイルの場合）

CIFS クライアントで表示されるアクセス許可エントリーの項目	Classic ACL タイプのファイルシステムの CIFS 共有に指定するアクセス権と NTFS ACL 設定有無	Advanced ACL タイプのファイルシステムの CIFS 共有に指定するアクセス権と NTFS ACL 設定有無
属性の読み取り	rw：設定される ro：設定される none：設定されない	rw：設定される ro：設定される none：設定される
アクセス許可の読み取り	rw：設定される ro：設定される none：設定されない	rw：設定される ro：設定される none：設定される
アクセス許可の変更	rw：設定されない ro：設定されない none：設定されない	アクセス権の設定対象がオーナーの場合 rw：設定される ro：設定される none：設定される アクセス権の設定対象がグループまたはその他の場合 rw：設定されない ro：設定されない none：設定されない
所有権の取得	rw：設定されない ro：設定されない none：設定されない	アクセス権の設定対象がオーナーの場合 rw：設定される ro：設定される none：設定される アクセス権の設定対象がグループまたはその他の場合 rw：設定されない ro：設定されない none：設定されない

- Advanced ACL タイプファイルシステムの CIFS 共有には，アクセス許可として「許可」と「拒否」があり，HVFP でのアクセス権の設定内容によっては次に示すように，CIFS クライアントで表示されるアクセス許可エントリーの項目が「拒否」になることがあります。
  - 「オーナー」または「グループ」に「許可」を設定しないで，「その他」に「許可」を設定した場合
    「オーナー」または「グループ」には「拒否」が設定されます。
  - 「オーナー」に「許可」を設定しないで，「グループ」に「許可」を設定した場合
    「オーナー」には「拒否」が設定されます。

このため，HVFP で CIFS 共有に同じ内容のアクセス権を指定しても（「オーナー」，「グループ」，「その他」に指定する rw，ro，none の組み合わせが同じでも），Advanced ACL タイプと Classic ACL タイプのファイルシステムとでデフォルトで設定される ACL に差異が生じます。Advanced ACL タイプファイルシステムの CIFS 共有に Classic ACL タイプファイルシステムの CIFS 共有と同様の「拒否」が設定されないようにするには，次に示す手順でアクセス権（rw，ro または none）の組み合わせを考慮して設定してください。
なお，換算表に記載された値は，アクセス権の関係を数値化したものであり，rwx を 8 進数で表現した値とは異なります。

a. アクセス権の指定値（rw，ro，none）を次に示す換算表に従って数値化します。

表 8-23： フォルダの場合の換算表

アクセス権の指定値	アクセス権の設定対象		
	オーナー	グループ	その他
rw	7	7	7
ro	5	5	5
none	1	1	1

表 8-24： ファイルの場合の換算表

アクセス権の指定値	アクセス権の設定対象		
	オーナー	グループ	その他
rw	7	6	6
ro	4	4	4
none	0	0	0

b. オーナー，グループ，その他に対して指定するアクセス権の指定値が，次に示す大小関係になるようにします。
所有者 ≧ グループ ≧ その他

指定値の大小関係が成立する場合と成立しない場合の例を次に示します。

指定値の大小関係が成立する場合

CIFS 共有内に新規に作成するファイルのアクセス権を，「オーナー：rw，グループ：ro，その他：none」にした場合，数値に換算した指定値は「オーナー：7，グループ：4，その他：0」となり，指定値の大小関係が成立します。この場合，デフォルトで設定される ACL にファイルシステムの ACL タイプの違いによる差異は生じません。

指定値の大小関係が成立しない場合

CIFS 共有内に新規に作成するファイルのアクセス権を，「オーナー：rw，グループ：ro，その他：rw」にした場合，数値に換算した指定値は「オーナー：7，グループ：4，その他：6」で，グループよりもその他のアクセス権の値が大きくなり，指定値の大小関係が成立しません。この場合，CIFS クライアントで表示されるグループのアクセス許可エントリーの項目は CIFS 共有内に新規に作成したファイルへの書き込みが「拒否」となり，そのグループに属するオーナーも新規に作成したファイルを更新できなくなります。

- CIFS 共有内に新規に作成するフォルダまたはファイルのアクセス権としてオーナーに ro（換算値は，フォルダ：5，ファイル：4）または none（換算値は，フォルダ：1，ファイル：0）を設定しないでください。設定した場合，オーナーであっても，CIFS 共有内に新規に作成したフォルダでのファイル作成や CIFS 共有内に新規に作成したファイルへの書き込みができなくなります。
- CIFS 共有のアクセス権を設定しているかどうかに関係なく，Advanced ACL タイプファイルシステムの CIFS 共有を CIFS クライアントで表示したときに CREATOR OWNER，CREATOR GROUP の ACE があると，そのフォルダ下に新規に作成するフォルダまたはファ

イルには，同じユーザーまたは同じグループに対して，2 種類の ACE が設定されることがあります。その条件を次に示します。

同じユーザーに 2 種類の ACE が設定される場合

新規にフォルダまたはファイルを作成する操作者の ACE が継承される設定になっていて，かつ，その操作者の ACE と CREATOR OWNER のアクセス許可の内容または適用先が異なっている CIFS 共有の場合，そのフォルダ下に新規に作成したフォルダまたはファイルには，作成した操作者と CREATOR OWNER の ACE が設定されます。

同じグループに 2 種類の ACE が設定される場合

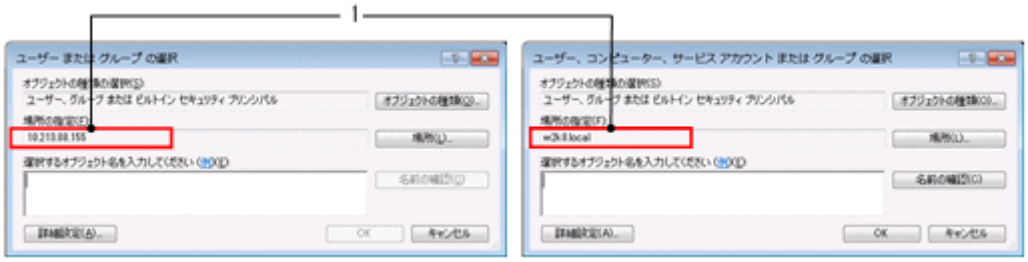
新規にフォルダまたはファイルを作成する操作者が属しているグループの ACE が継承される設定になっていて，かつ，そのグループの ACE と CREATOR GROUP のアクセス許可の内容または適用先が異なっている CIFS 共有の場合，そのフォルダ下に新規に作成したフォルダまたはファイルには，作成した操作者が属しているグループと CREATOR GROUP の ACE が設定されます。

8.3.3.16 ユーザーおよびグループ ACL の追加

ここでは，ユーザーおよびグループの ACL の追加について説明します。

ユーザーおよびグループ ACL の追加は，ファイルまたはフォルダのアクセス許可画面の［追加］から行います。［追加］をクリックすると表示される［ユーザーまたはグループの選択］画面を次の図に示します。

図 8-9：ユーザーまたはグループ選択画面（左：ユーザーマッピングを使用しない場合，右：ユーザーマッピングを使用する場合）



CIFS 共有で作成したフォルダに対して，ファイルまたはフォルダのプロパティ画面で ACL を設定する場合，CIFS サービスの認証方式によって選択するユーザーまたはグループが属する［場所の指定］（上記の図の 1 で示す個所）が異なります。

ローカル認証，Active Directory 認証でユーザーマッピングを使用しない場合

［ユーザーまたはグループの選択］画面の［場所の指定］に HVFP のノードまたは Virtual Server のホスト名が表示されているユーザーまたはグループを選択する必要があります。

注意事項：

・Active Directory 認証を選択した場合，［ユーザーまたはグループの選択］画面の［場所の指定］にドメインコントローラーが表示されていることがありますが，このとき，ユーザーやグループに ACL を設定しても有効になりません。

・図 8-9： ユーザーまたはグループ選択画面（左：ユーザーマッピングを使用しない場合，右：ユーザーマッピングを使用する場合）の左に示す［ユーザーまたはグループの選択］画面の［場所の指定］に HVFP のノードまたは Virtual Server のホスト名が表示されているユーザーを表示するためには，File Services Manager の［Local Users］ダイアログの［Add User］ページで CIFS ユーザーを登録する必要があります。

・グループを表示するためには，File Services Manager の［Local Users］ダイアログの［Add Group］ページでグループを追加する時に，［Apply to CIFS ACL environment］チェックボックスをチェックしてグループを登録する必要があります。

・環境によって，ファイルまたはフォルダのアクセス許可画面からユーザーおよびグループ ACL を追加できないことがあります。その場合は，dirsetacl コマンドで設定してください。なお，ファイルに対して ACL を追加したい場合は，dirsetacl コマンドで対象のファイルに ACE が継承されるように，該当するディレクトリに対して ACE の継承範囲を設定してください。

Active Directory 認証でユーザーマッピングを使用する場合

［ユーザーまたはグループの選択］画面の［場所の指定］にドメインコントローラーが表示されているユーザーまたはグループを選択する必要があります。
［ユーザーまたはグループの選択］画面の［場所の指定］にドメインコントローラーが表示されない場合，次の原因によってドメインコントローラーと通信できていないおそれがあります。

- ［Access Protocol Configuration］ダイアログの［Active Directory Authentication］ページの［Domain name (NetBIOS)］に指定した値が誤っている。
- CIFS クライアントで，DNS によるドメインコントローラーの IP アドレスを解決できない。
- CIFS 操作をしているユーザーが，ドメインユーザーではない。

なお，［ユーザーまたはグループの選択］画面の［場所の指定］に HVFP のノードまたは Virtual Server のホスト名が表示されているユーザーまたはグループを選択することで，HVFP のローカルユーザーおよびローカルグループの ACL を設定できます。
注意事項：

・この場合は，図 8-9： ユーザーまたはグループ選択画面（左：ユーザーマッピングを使用しない場合，右：ユーザーマッピングを使用する場合）の左に示す［ユーザーまたはグループの選択］画面を使用します。その［場所の指定］に HVFP のノードまたは Virtual Server のホスト名が表示されているユーザーを表示するためには，File Services Manager の［Local Users］ダイアログの［Add User］ページで CIFS ユーザーを登録する必要があります。
・グループを表示するためには，File Services Manager の［Local Users］ダイアログの［Add Group］ページでグループを追加する時に，［Apply to CIFS ACL environment］チェックボックスをチェックしてグループを登録する必要があります。
・CIFS クライアントは，ドメインに参加している必要があります。参加していない場合，［ユーザーまたはグループの選択］画面の［場所の指定］に HVFP のノードまたは Virtual Server のホスト名を表示しても，HVFP のローカルユーザーおよびローカルグループは表示されません。
・環境によって，ファイルまたはフォルダのアクセス許可画面からユーザーおよびグループ ACL を追加できないことがあります。その場合は，dirsetacl コマンドで設定してください。なお，ファイルに対して ACL を追加したい場合は，dirsetacl コマンドで対象のファイルに ACE が継承されるように，該当するディレクトリに対して ACE の継承範囲を設定してください。

なお，CIFS サービスの認証方式に関わらず，ファイルまたはフォルダのアクセス許可画面からユーザーおよびグループ ACL を追加できない場合は，次のどれかの方法で追加できることがあります。

- 管理者（Administrators グループに所属するユーザー）で Windows クライアントにログオンする。
- Administrator でないユーザー（Windows クライアントに個別に追加したユーザー）で Windows クライアントにログオンする。
- ユーザーおよびグループ ACL の追加で認証ダイアログが表示された際に，HVFP に接続するときのユーザー名およびパスワードを入力する。
- HVFP に接続するときに指定するユーザー名およびパスワードと，Windows クライアントにログオンするときのユーザー名およびパスワードを同じにする。

- Windows クライアントからホスト名を指定して HVFP に接続する。
- Windows クライアントを Active Directory ドメインに参加させる。この場合，HVFP の認証方式や HVFP が参加するドメインと関係がなくても問題ありません。

8.4 ファイル属性

CIFS クライアントからの CIFS 共有のファイル属性の操作について説明します。

8.4.1 CIFS クライアントからのファイル属性の設定および表示

ここでは，CIFS クライアントからの CIFS 共有のファイル属性の設定と表示について説明します。

ファイル属性の設定ができるユーザー

HVFP では，ファイルおよびディレクトリに対する書き込み権限を持つユーザー，または File Services Manager で登録した CIFS 管理者だけが，ファイル属性を設定できます。書き込み権限を持たないファイル所有者はファイル属性の設定はできません。

8.4.1.1 ファイル属性の適用可否

CIFS クライアントから設定したファイル属性の HVFP での適用可否は，ファイルシステムの ACL タイプによって次の表に示すように異なります。

表 8-25： ファイル属性の HVFP での適用可否

ファイル属性	内容	Classic ACL タイプでの適用可否	Advanced ACL タイプでの適用可否
読み取り専用属性（Read Only）	書き込みや移動などを禁止することを示す属性。書き込み禁止属性とも呼ばれる。	可	可
システムファイル属性（System）	システムの動作に必要で，重要なファイルであることを示す属性。通常，これらのファイルを移動したり書き換えたりしてはいけない。	不可	可
隠しファイル属性（Hidden）	シェルからは通常見えないようになっているファイル。ただし，エクスプローラでも設定によっては見ることができる。	不可	可
アーカイブ属性（Archive）	最後にバックアップを取ったあとにファイル内容が変更されたことを示す。	不可	可 *
圧縮属性（Compressed）	ファイルシステムが NTFS である場合だけ利用できる属性。この属性を持つファイルはファイルシステムレベルで圧縮されていることを示す。	不可	不可
暗号化属性（Encrypted）	ファイルシステムが NTFS の場合だけ利用できる属性。ファイルを暗号化して機密性を高める。圧縮属性と同時には設定できない。暗号化属性のあるファイルは暗号化属性に非対応のバックアップツールなどでバックアップしないほうがよい（バックアップ時に暗号化が解除されてしまうため）。	不可	不可
ディレクトリ属性（Directory）	ファイルがディレクトリであるか通常のファイルであるかを示す。	可	可
オフライン属性（Offline）	ファイルがスタブファイルであることを示す。	可	可

注 *

「8.4.1.3 アーカイブ属性に関する注意事項」を参照してください。

8.4.1.2 NFS との共有に関する注意事項

同一ファイルおよびディレクトリを CIFS サービスと NFS サービスとで共有する場合の注意事項を次に示します。

- NFS クライアントがパーミッションを操作してオーナー，グループおよびその他のユーザーの書き込み権限を削除した場合，CIFS クライアントから見ると読み取り専用属性となります。
- CIFS クライアントが読み取り専用属性を設定した場合は注意が必要です。CIFS クライアントが読み取り専用属性を設定しても，NFS クライアントではその設定が有効となりません。
- NFS クライアントで作成したファイルやディレクトリの名称の先頭文字がピリオド（.）の場合，CIFS 共有では隠しファイル属性が付与されます。

8.4.1.3 アーカイブ属性に関する注意事項

Advanced ACL タイプファイルシステムの場合，通常ファイルとシンボリックリンクファイル以外の名前の変更や移動では，アーカイブ属性は ON になりません。

8.4.1.4 読み取り専用属性に関する注意事項

読み取り専用属性が設定されているファイル，フォルダの場合，［Access Protocol Configuration］ダイアログの［CIFS Service Management］ページ（Setting Type：Administration）で［CIFS administrator name(s)］に指定した CIFS 管理者であっても，Windows API を使用してファイルを削除することはできません。

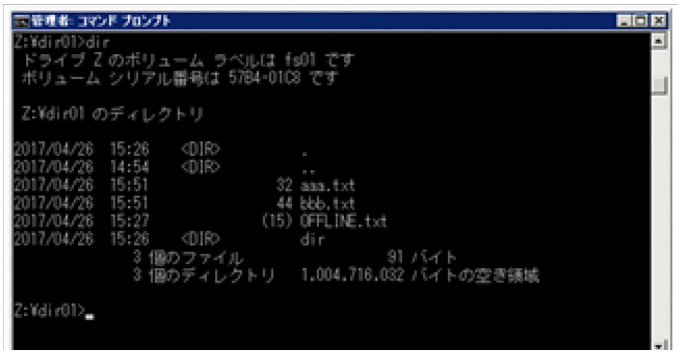
8.4.1.5 オフライン属性について

HVFP は，ほかのファイルサーバからオンデマンドでインポートされたりしてスタブファイルとなったファイルを，オフライン属性を持つファイルとして管理します。オンデマンドでのインポートについては，「システム構成ガイド」（IF302）を参照してください。なお，オフライン属性は CIFS クライアントから設定できる属性ではありません。

CIFS クライアントがオフライン属性のファイルをエクスプローラで表示した場合，アイコンの左下に，CIFS クライアントによっては×印が付きます。エクスプローラの属性列には，オフライン属性を示す文字「O」が表示されます。ただし，オフライン属性のショートカットファイルの場合は，アイコンが表示されなくなることがあります。ショートカットファイルかどうかは，エクスプローラの種類列の表示で判別できます。コマンドプロンプトでファイルの一覧を表示した場合，オフライン属性のファイルはファイルサイズが括弧で囲まれます。

図 8-10： エクスプローラでのオフライン属性の表示例

図 8-11： コマンドプロンプトでのオフライン属性の表示例



8.4.2 Windows の拡張属性

Windows の拡張属性は，［プロパティ］－［概要］タブに表示される内容を管理する場合に使用されていますが，HVFP への移行は，一部不可の場合があります。これは，アプリケーションによって拡張属性を名前付きストリームと呼ばれる NTFS 固有の領域に格納しているためであり，このストリームのデータは NTFS ボリューム以外へのコピーはできないため，HVFP への移行時には無効となります。

参考として主なアプリケーションでの拡張属性の格納場所について次の表に示します。

表 8-26： 拡張属性の格納場所

アプリケーション	格納場所	HVFP への移行可否
Microsoft Word	メインデータストリーム	可
Microsoft Excel	メインデータストリーム	可
Microsoft PowerPoint	メインデータストリーム	可

アプリケーション	格納場所	HVFP への移行可否
メモ帳	SummaryInformation データストリーム *	不可
ワードパッド	SummaryInformation データストリーム *	不可
Zip ファイル	SummaryInformation データストリーム *	不可

注 *

NTFS では，1 つのファイルが複数のデータストリームと呼ばれるもので構成されています。このうち，実際のファイルデータが格納されているのは「メインデータストリーム」または「名前無しデータストリーム」と呼ばれます。非 NTFS の場合は，このメインデータストリームしかアクセスできません。
メインデータストリーム以外のストリームを「名前付きデータストリーム」と呼び，SummaryInformation データストリームは，この「名前付きデータストリーム」の 1 つです。

以上のように HVFP では拡張属性の設定・参照・移行はサポートしませんが，拡張属性関連のアクセス権限設定および，アクセス権限チェックはします。

8.5 タイムスタンプ

ここでは，CIFS 共有アクセス時のファイルタイムスタンプについて説明します。

8.5.1 ファイルアクセス日時

ファイルアクセス日時の更新の有無は，File Services Manager の［ファイルシステムのマウント］ダイアログで設定を行います。ファイルアクセス日時の更新についての詳しい設定方法は，「ユーザーズガイド」（IF305）を参照してください。なお，アクセス日時はファイルのプロパティを開いた場合も更新されます。

8.5.2 ファイル更新日時

ファイル更新日時についての注意事項を示します。

- CIFS クライアントから CIFS 共有内でフォルダの移動を行った場合，フォルダの更新日時は移動操作を行った時刻に変更されます。
- ［ファイルシステムのマウント］ダイアログの［最終アクセス時刻記録］を［はい］としていない場合でも，Microsoft Excel などのアプリケーションの動作仕様によっては，ファイルを更新した場合にアクセス日時が更新される場合があります。

8.5.3 ファイル作成日時

ファイルが存在するファイルシステムでファイル作成日時を記録しない設定になっている場合，ファイルを更新したときや，ファイルサイズやファイルの権限などファイル属性を更新したときにファイルの作成日時が更新されることがあります。これは，HVFP では，ファイル作成日時を記録しない設定の場合，ファイル更新日時，アクセス日時またはファイル属性変更日時の中のいちばん古い日時を，ファイルの作成日時として CIFS クライアントに返却しているからです。

8.5.4 ファイルタイムスタンプ精度

ファイルタイムスタンプの精度について説明します。

8.5.4.1 ファイルタイムスタンプの管理方式

HVFP と Windows（NTFS）でのファイルタイムスタンプの管理方式の比較表を次の表に示します。

表 8-27： ファイルタイムスタンプ管理方式

項目	Windows	HVFP
時刻の起点	1601 年	1970 年
記憶領域	8 バイト	4 バイト *1
精度	100 ナノ秒	100 ナノ秒 *2

注 *1

WORM 対応ファイルシステムの場合，ファイルアクセス日時の記憶領域は 8 バイトです。

注 *2

WORM 対応ファイルシステムの場合，ファイルアクセス日時の精度は秒です。

8.5.4.2 ファイルタイムスタンプの更新精度

HVFP と Windows でのファイルタイムスタンプの更新精度の比較表を次の表に示します。

表 8-28： ファイルタイムスタンプ更新精度

タイムスタンプ種別	Windows	HVFP
ファイルアクセス日時	1 時間	100 ナノ秒
ファイル更新日時	100 ナノ秒	100 ナノ秒
ファイル作成日時	100 ナノ秒	100 ナノ秒

8.5.5 ファイルタイムスタンプ更新権限

ファイルタイムスタンプ設定対象のファイルに読み取り専用属性が設定されている場合，［Access Protocol Configuration］ダイアログの［CIFS Service Management］ページ（Setting Type : Security）で［File timestamp changeable users］に指定したユーザーであっても，ファイルタイムスタンプを更新することはできません。

8.6 ディスク容量表示

CIFS クライアントでは，対象の共有で使用できるディスク容量を表示でき，共有が存在するファイルシステムやディレクトリに Quota が設定されている場合，この値を加味したディスク容量が表示されます。ただし，File Services Manager で登録した CIFS 管理者でディスク容量を表示した場合は，ファイルシステムやディレクトリに設定された Quota 値を加味した値ではなく，ファイルシステムの容量が表示されます。

ここでは，Quota 設定有無とディスク容量の表示についてまとめます。

Quota 機能は，ユーザーが使用できるブロック容量や inode 数を監視・制限するための機能です。CIFS 共有を使用する場合には，共有サイズの表示にも影響を与えます。

HVFP と Windows の Quota 機能を比較すると，次に示す差異があります。

Quota 機能で監視・制限できるセキュリティ情報

セキュリティ情報とは，ファイルの所有者や所有グループなどのことです。HVFP では，所有者と所有グループを Quota 機能の適用対象としており，どちらか片方（あるいは両方）が Quota 設定の上限値に抵触しているとファイル操作をすることができません。これに対して Windows では，所有者だけを Quota 機能の適用対象としています。所有グループは，Quota 機能の適用対象にできません。

デフォルト Quota 機能で作成できる Quota 設定の種類

デフォルト Quota 機能は，Quota 設定がなされていないファイルの所有者に対し，自動的に Quota 設定を適用する機能です。HVFP では，所有者がユーザーである場合だけ，デフォルト Quota 機能によって Quota 設定が適用されます。所有者がグループである場合は，適用されません。一方 Windows では，所有者がユーザー，グループのどちらであっても，デフォルト Quota 機能によって Quota 設定が適用されます。

HVFP と Windows の Quota 機能に関する仕様の比較を次の表に示します。

表 8-29： HVFP と Windows の Quota 機能に関する仕様比較

セキュリティ情報		Quota 機能による監視・制限		デフォルト Quota 機能による Quota 設定	
		HVFP	Windows	HVFP	Windows
所有者	ユーザー	○	○	○	○
	グループ	○	○	×	○
所有者グループ		○	×	×	×

（凡例）○：できる　×：できない

Quota 機能で監視・制限できるセキュリティ情報に関する仕様差異の例を次の表に示します。表は，所有者に対してユーザー Quota を設定した場合，所有グループに対してグループ Quota を設定した場合，および最上位ディレクトリに対してディレクトリ Quota（HVFP でのサブツリーディレクトリ Quota）を設定した場合の，Quota 設定の適用有無と CIFS 共有のプロパティに表示される共有サイズについて示しています。

表 8-30： Quota 機能で監視・制限できるセキュリティ情報に関する仕様差異の例

セキュリティ情報	Quota 機能の適用範囲		共有サイズ	
	HVFP	Windows	HVFP	Windows
所有者に対してユーザー Quota を設定	適用される	適用される	Quota 設定の上限値	Quota 設定の上限値
所有グループに対してグループ Quota を設定	適用される	適用されない	Quota 設定の上限値	ファイルシステムの総容量
共有の最上位ディレクトリに対してディレクトリ Quota を設定	適用される	適用される	Quota 設定の上限値	Quota 設定の上限値

なお，HVFP では，ファイルシステムごとの Quota を設定した場合は，ユーザー Quota，デフォルト Quota およびグループ Quota の設定からディスク容量を算出します。ディレクトリごとの Quota を設定した場合は，サブツリーユーザー Quota，サブツリーデフォルト Quota，サブツリーグループ Quota およびサブツリーディレクトリ Quota の設定を加味して算出します。

Advanced ACL タイプファイルシステムでは，所有者がグループの Quota についてはサポートしていません。デフォルト Quota についても同様です。グループ Quota は，あるグループが所有者となっているファイルの容量と，あるグループがファイルの所有グループとなっているファイルの容量の合計値で評価されます。

CIFS クライアントから参照したディスク容量にデータを書き込むための空き容量がある場合でも，容量不足でエラーになることがあります。この場合，fslist コマンドでファイルシステムのブロックの残容量を確認するほか，quotaget および stquota コマンドでユーザーや所属グループのブロック使用量や inode 使用量を確認してください。

8.6.1 Quota 設定内容の CIFS クライアントでの確認可否

HVFP で設定した Quota を，CIFS クライアントからディスク容量を参照することで確認できます。Quota 設定内容の CIFS クライアントでの確認可否を次の表に示します。

表 8-31： HVFP で設定した Quota 値の CIFS クライアントでの確認可否

Quota 設定			CIFS クライアントからの確認可否
サブツリーユーザー Quota	ブロック容量	ソフトリミット	可
		ハードリミット	可
		猶予期間	不可
	inode	ソフトリミット	不可
		ハードリミット	不可
		猶予期間	不可
サブツリーデフォルト Quota	ブロック容量	ソフトリミット	可
		ハードリミット	可
	inode	ソフトリミット	不可
		ハードリミット	不可
サブツリーグループ Quota	ブロック容量	ソフトリミット	可
		ハードリミット	可
		猶予期間	不可
	inode	ソフトリミット	不可
		ハードリミット	不可
		猶予期間	不可
サブツリーディレクトリ Quota	ブロック容量	ソフトリミット	可
		ハードリミット	可
		猶予期間	不可
	inode	ソフトリミット	不可
		ハードリミット	不可
		猶予期間	不可
ユーザー Quota	ブロック容量	ソフトリミット	可
		ハードリミット	可
		猶予期間	不可
	inode	ソフトリミット	不可
		ハードリミット	不可
		猶予期間	不可
デフォルト Quota	ブロック容量	ソフトリミット	可
		ハードリミット	可
	inode	ソフトリミット	不可
		ハードリミット	不可

Quota 設定			CIFS クライアントからの確認可否
グループ Quota	ブロック容量	ソフトリミット	可
		ハードリミット	可
		猶予期間	不可
	inode	ソフトリミット	不可
		ハードリミット	不可
		猶予期間	不可

上記の表に示したように，CIFS クライアントで表示できる Quota 設定は，ブロック容量に関する値だけです。また，表示されているディスク容量がソフトリミットであるかハードリミットであるかを確認することはできません。

ディスク容量に表示される Quota 設定は，ドライブの割り当て先ディレクトリで有効な Quota 設定です。ディスク容量に表示される Quota 設定は，Quota の設定値やディスクの使用状況によって変化します。この詳細については，「8.6.2 ディスク使用量に応じたディスク容量表示」および「8.6.3 複数の Quota を設定した場合のディスク容量表示」を参照してください。

また，複数のディレクトリにそれぞれドライブを割り当ててディスク容量を表示した場合，ディスク容量が正しく表示されないことがあります。応答遅延などのクライアントへの影響をご考慮のうえ，`cifsoptset` コマンドで `dfree_cache_time` に 0 を指定してディスクの空き容量の情報をキャッシュしないように設定してください。`cifsoptset` コマンドでディスク容量をキャッシュしないように設定する方法については，「コマンドリファレンス」（IF311）を参照してください。

CIFS クライアントでのディスク容量の表示例を，次の図に示します。図中の太枠で囲った個所が，Quota 設定およびディスク使用量に応じて変化します。

図 8-12： Quota 設定なしの時のディスク容量表示

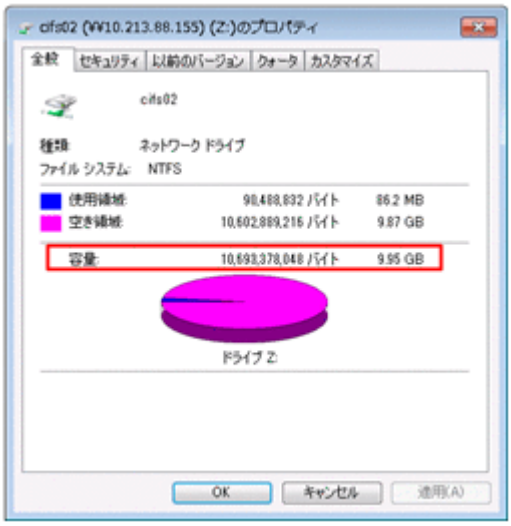
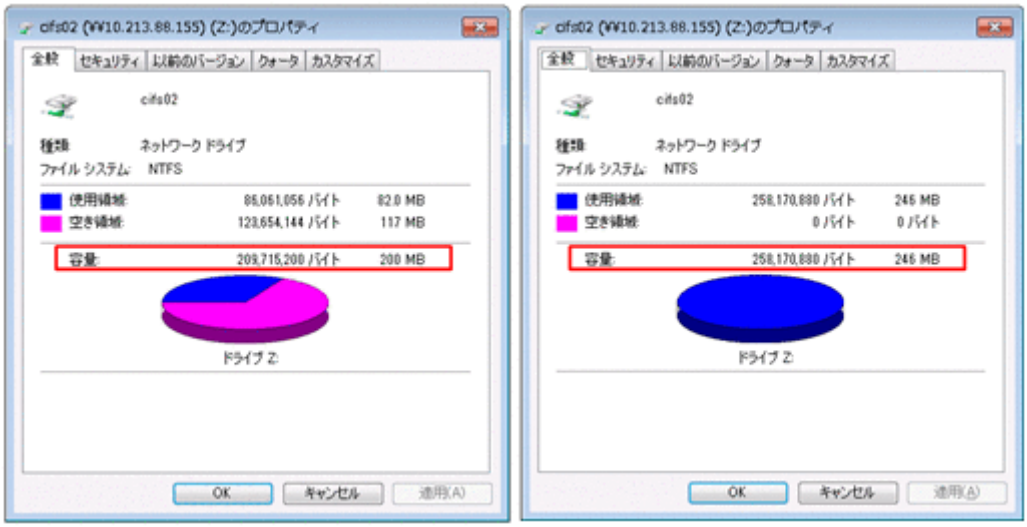


図 8-13：Quota 設定ありの時のディスク容量表示（左は使用量が Quota 制限内の場合，右は使用量が Quota 制限を超過した場合）



8.6.2 ディスク使用量に応じたディスク容量表示

HVFP で Quota としてブロック容量と inode 数を設定した場合の CIFS クライアントでのディスク容量表示について説明します。

Quota（ブロック容量）設定時

HVFP でブロック容量の Quota を設定した場合，ディスク使用量に応じて CIFS クライアントでは次の表のように表示されます。

表 8-32：HVFP で Quota（ブロック容量）を設定して CIFS クライアントで表示した場合

Quota 値		使用量	ディスク容量
ソフトリミット	ハードリミット		
設定なし	設定なし	－	ファイルシステムの容量
設定なし	設定あり	ハードリミット以上	ブロックの使用量
		ハードリミット未満	ブロック容量のハードリミット
設定あり	設定なし	ソフトリミット以上	ブロックの使用量
		ソフトリミット未満	ブロック容量のソフトリミット
設定あり	設定あり	ハードリミット以上	ブロックの使用量
		ソフトリミット以上 ハードリミット未満	ブロックの使用量
		ソフトリミット未満	ブロック容量のソフトリミット

（凡例）－：該当しない

Quota（inode 数）設定時

HVFP で inode 数の Quota を設定した場合，ディスク使用量に応じて CIFS クライアントでは次の表のように表示されます。ただし，設定された inode 数を，クライアントから確認することはできません。

表 8-33：HVFP で Quota（inode 数）を設定して CIFS クライアントで表示した場合

Quota 値		使用量	ディスク容量
ソフトリミット	ハードリミット		
設定なし	設定なし	－	ファイルシステムの容量
設定なし	設定あり	ハードリミット以上	ブロックの使用量
		ハードリミット未満	ファイルシステムの容量
設定あり	設定なし	ソフトリミット以上	ブロックの使用量
		ソフトリミット未満	ファイルシステムの容量
設定あり	設定あり	ハードリミット以上	ブロックの使用量
		ソフトリミット以上 ハードリミット未満	ブロックの使用量
		ソフトリミット未満	ファイルシステムの容量

（凡例）－：該当しない

8.6.3 複数の Quota を設定した場合のディスク容量表示

複数の Quota 設定が適用される CIFS クライアントからディスク容量を表示した場合に，表示されるディスク容量の値について説明します。

8.6.3.1 HVFP の場合

HVFP では，ディスク使用量が Quota 制限に達しているかどうかによって，CIFS クライアント上で表示されるディスク容量が異なります。

ディスク使用量が Quota 制限に達していない場合

CIFS クライアントの使用するブロック容量および inode 数が，適用されるすべての Quota に対して，その制限に達していない場合，次の表に示す規則に基づいてディスク容量が表示されます。

表 8-34：複数の Quota を設定した場合のディスク容量（Quota 制限に達していない場合）

ディレクトリごとの Quota（サブツリー Quota）				ファイルシステムごとの Quota			ディスク容量
ユーザー	デフォルト	グループ	ディレクトリ	ユーザー	デフォルト	グループ	
ブロック容量制限あり	－						サブツリーユーザー Quota のブロック容量リミット値
Quota の設定なし	ブロック容量制限あり	－					サブツリーデフォルト Quota のブロック容量リミット値
ブロック容量制限なし		ブロック容量制限あり	－				サブツリーグループ Quota のブロック容量リミット値
ブロック容量制限なし			ブロック容量制限あり	－			サブツリーディレクトリ Quota のブロック容量リミット値
ブロック容量制限なし				ブロック容量制限あり	－		ユーザー Quota のブロック容量リミット値

ディレクトリごとの Quota（サブツリー Quota）				ファイルシステムごとの Quota			ディスク容量
ユーザー	デフォルト	グループ	ディレクトリ	ユーザー	デフォルト	グループ	
ブロック容量制限なし				Quota の設定なし	ブロック容量制限あり	－	デフォルト Quota のブロック容量リミット値
ブロック容量制限なし						ブロック容量制限あり	グループ Quota のブロック容量リミット値
ブロック容量制限なし							ファイルシステムのサイズ

（凡例）－：Quota 設定の有無に依存しないことを示します。

注

「リミット値」は，ソフトリミットが設定されている場合はソフトリミットの値を，そうでない場合はハードリミットの値を指します。

ディスク使用量が Quota 制限に達している場合

CIFS クライアントの使用するブロック容量または inode 数が，適用される Quota のどれかで，その制限に達している場合，次の表に示す規則に基づいてディスク容量が表示されます。

表 8-35：複数の Quota を設定した場合のディスク容量（Quota 制限に達している場合）

ディレクトリごとの Quota（サブツリー Quota）				ファイルシステムごとの Quota			ディスク容量
ユーザー	デフォルト	グループ	ディレクトリ	ユーザー	デフォルト	グループ	
使用量が制限を超過	－						サブツリーユーザー Quota のブロック使用量
使用量は制限内	使用量が，少なくとも 1 つの制限を超過						サブツリーユーザー Quota のブロック容量リミット値
ブロック容量制限なし		使用量が制限を超過	－				サブツリーグループ Quota のブロック使用量
ブロック容量制限なし		使用量は制限内	使用量が，少なくとも 1 つの制限を超過				サブツリーグループ Quota のブロック容量リミット値
ブロック容量制限なし			使用量が制限を超過	－			サブツリーディレクトリ Quota のブロック使用量
ブロック容量制限なし			使用量は制限内	使用量が，少なくとも 1 つの制限を超過			サブツリーディレクトリ Quota のブロック容量リミット値
ブロック容量制限なし				使用量が制限を超過	－		ユーザー Quota のブロック使用量
ブロック容量制限なし				使用量は制限内	使用量が，少なくとも 1 つの制限を超過		ユーザー Quota のブロック容量リミット値

ディレクトリごとの Quota（サブツリー Quota）				ファイルシステムごとの Quota			ディスク容量
ユーザー	デフォルト	グループ	ディレクトリ	ユーザー	デフォルト	グループ	
ブロック容量制限なし						使用量が制限を超過	グループ Quota のブロック使用量
ブロック容量制限なし						使用量は制限内	グループ Quota のブロック容量リミット値

（凡例）－：Quota 設定の有無に依存しないことを示します。

注

「リミット値」は，ソフトリミットが設定されている場合はソフトリミットの値を，そうでない場合はハードリミットの値を指します。

8.6.3.2 Windows サーバの場合

Windows サーバでブロック容量の Quota を設定した場合，CIFS クライアントでは次の表のように表示されます。

表 8-36：Windows サーバで設定した Quota を CIFS クライアントで表示した場合

ディレクトリ Quota		ディスク Quota		使用量	ディスク容量
ソフトリミット	ハードリミット	警告レベルの設定	ディスク領域の制限		
設定なし	設定なし	設定なし	設定なし	－	ボリュームの容量
		設定あり	設定あり	「ディスク領域を制限する」に指定した値以上	「ディスク領域を制限する」に指定した値
				「ディスク領域を制限する」に指定した値未満	「ディスク領域を制限する」に指定した値*
				「警告レベルの設定」に指定した値未満	「ディスク領域を制限する」に指定した値*
設定なし	設定あり	設定なし	設定なし	「ハードリミット」に指定した値以上	「ハードリミット」に指定した値*
				「ハードリミット」に指定した値未満	「ハードリミット」に指定した値
		設定あり	設定あり	「ディスク領域を制限する」に指定した値以上	「ディスク領域を制限する」と「ハードリミット」のうち小さい方の値*
				「ハードリミット」に指定した値以上「ディスク領域を制限する」に指定した値未満	「ディスク領域を制限する」と「ハードリミット」のうち小さい方の値*
				「警告レベルの設定」に指定した値以上「ハードリミット」に指定した値未満	「ディスク領域を制限する」と「ハードリミット」のうち小さい方の値*
				「警告レベルの設定」に指定した値未満	「ディスク領域を制限する」と「ハードリミット」のうち小さい方の値*

ディレクトリ Quota		ディスク Quota		使用量	ディスク容量
ソフトリミット	ハードリミット	警告レベルの設定	ディスク領域の制限		
設定あり	設定なし	設定なし	設定なし	「ソフトリミット」に指定した値以上	「ソフトリミット」に指定した値*
				「ソフトリミット」に指定した値未満	「ソフトリミット」に指定した値
		設定あり	設定あり	「ディスク領域を制限する」に指定した値以上	「ディスク領域を制限する」と「ソフトリミット」のうち小さい方の値*
				「ソフトリミット」に指定した値以上「ディスク領域を制限する」に指定した値未満	「ディスク領域を制限する」と「ソフトリミット」のうち小さい方の値*
				「警告レベルの設定」に指定した値以上「ソフトリミット」に指定した値未満	「ディスク領域を制限する」と「ソフトリミット」のうち小さい方の値*
				「警告レベルの設定」に指定した値未満	「ディスク領域を制限する」と「ソフトリミット」のうち小さい方の値*
設定あり	設定なし	設定なし	設定なし	「ソフトリミット」に指定した値以上	「ソフトリミット」に指定した値*
				「ソフトリミット」に指定した値未満	「ソフトリミット」に指定した値
		設定あり	設定あり	「ディスク領域を制限する」に指定した値以上	「ディスク領域を制限する」と「ソフトリミット」のうち小さい方の値*
				「ソフトリミット」に指定した値以上「ディスク領域を制限する」に指定した値未満	「ディスク領域を制限する」と「ソフトリミット」のうち小さい方の値*
				「警告レベルの設定」に指定した値以上「ソフトリミット」に指定した値未満	「ディスク領域を制限する」と「ソフトリミット」のうち小さい方の値*
				「警告レベルの設定」に指定した値未満	「ディスク領域を制限する」と「ソフトリミット」のうち小さい方の値*

（凡例）－：Quota 設定の有無に依存しないことを示します。

注 *

HVFP ではディスク使用量に応じてディスク容量表示が変わりますが，Windows サーバでは常に［ディスク領域を制限する］で設定した値が表示されます。

8.7 WORM ファイル

WORM とは，特定のファイルシステム（これを WORM 対応ファイルシステムと呼ぶ）内にあるファイルを読み取り専用にして，一定期間または無期限にデータの変更および削除をできなくする機能です。ファイルをこの状態にすることを WORM 化と呼び，WORM 化したファイルを WORM ファイルと呼びます。

WORM ファイルには次に示す特徴があります。なお，WORM 対応ファイルシステムについては，「システム構成ガイド」（IF302）を参照してください。

ファイルのリテンション期間を設定したり，延長したりするには，ユーザーが独自に作成するカスタムアプリケーションを使用します。カスタムアプリケーションを作成するための API については，「F WORM 運用のための API」を参照してください。

- 書き込みができない
  ファイルの ACL でアクセス許可の「書き込み」が「許可」になっていても，書き込むことはできません。
  なお，WORM ファイルには読み取り専用属性の付与と解除ができます。
- WORM 化は ACL ではなくファイル属性の設定を契機としている
  WORM 化されるのは，ファイル属性として「読み取り専用」を設定した場合です。ファイルの ACL で「読み取り」だけを許可しても WORM 化されません。
- WORM ファイルの有限リテンションと無限リテンション
  WORM 化されたファイルでは，ファイルに設定したリテンション期間（ファイルを保存する期間）が atime として扱われます。
  一定期間データの変更および削除ができないことを有限リテンションと呼び，この場合はリテンション期間として，現在時刻よりも未来の日時をファイルに設定します。有限リテンションの WORM ファイルは，atime が未来の時刻になります。
  無期限にデータの変更および削除ができないことを無限リテンションと呼び，この場合はリテンション期間として，現在時刻よりも 24 時間以上過去の日時をファイルに設定します。無限リテンションの WORM ファイルは，atime が 24 時間以上過去の時刻になります。
- WORM ファイルのリテンション期間は延長だけができる
  有限リテンションの場合，設定したリテンション期間を延長できますが，短縮できません。
  無限リテンションの場合，設定したリテンション期間を変更できません。また，有限リテンションを無限リテンションに変更できません。
- atime は秒単位になる
  WORM 対応ファイルシステムでは atime は秒単位になります。
- WORM ファイルの atime は更新されない
  WORM 化されていないファイルの場合，アクセスすると atime は更新されます。しかし，リテンション期間を設定した WORM ファイルの場合，アクセスしても atime は更新されません。
- WORM ファイルの削除は「読み取り専用」属性の解除が必要
  設定したリテンション期間を過ぎた WORM ファイルは，読み取り専用属性を解除することで，削除できるようになります。ただし，データの変更はできません。

8.8 ABE によるアクセス制御

ABE（Access Based Enumeration：アクセスベースの列挙）は，CIFS クライアントがファイルやフォルダの一覧を表示する場合に，読み取り権限があるかどうかでファイル名やフォルダ名を表示するかどうかを制御する機能です。ABE を有効にすると，読み取り権限がないファイルやフォルダは CIFS クライアントに表示されなくなります。また，ABE を有効にすると，CIFS クライアントでのファイルやフォルダの一覧表示が遅くなる場合があります。

8.8.1 ABE によるファイルやフォルダの表示／非表示

ABE によるファイルやフォルダの表示／非表示について，例を基に説明します。ABE の設定方法については，「ユーザーズガイド」（IF305）を参照してください。

フォルダ，ファイルの読み取り権限の有無と ABE が有効か無効かによるクライアントでの表示の関係を次の表に示します。

表 8-37： フォルダ，ファイルの読み取り権限の有無と ABE が有効か無効かによるクライアントでの表示の関係

フォルダ名／ファイル名	フォルダ，ファイルの読み取り権限の有無	クライアントでの表示	
		ABE 有効の場合	ABE 無効の場合
dir1	有る	表示される	表示される
file11	有る	表示される	表示される
file12	無い	表示されない	表示される
dir2	無い	表示されない	表示される
file21	有る	表示されない	表示されない *
file22	無い	表示されない	表示されない *

注 *

dir2 に読み取り権限がないため，配下のファイルの一覧を取得できなくて表示されません。

CIFS クライアントでの表示例を，次の図に示します。ABE を有効にした場合，読み取り権限がない file12 と dir2 は表示されません（図 8-14： ABE が有効な場合）。ABE を無効にした場合，dir1，dir1 配下の file11 および file12，dir2 はアクセス権に関係なく表示されますが，dir2 の読み取り権限がないためその配下のファイルの一覧は表示されません（図 8-15： ABE が無効の場合）。なお，ABE はファイルやフォルダを表示するかどうかを制御するだけです。このため，ファイルのパスを知っていれば，アクセス権のあるファイルにはアクセスできます。例えば，表 8-37： フォルダ，ファイルの読み取り権限の有無と ABE が有効か無効かによるクライアントでの表示の関係の dir2 に対して ACL で「フォルダのスキャン」権限が許可されていれば，ファイルのパスを指定することで file21 にアクセスできます。

図 8-14： ABE が有効な場合

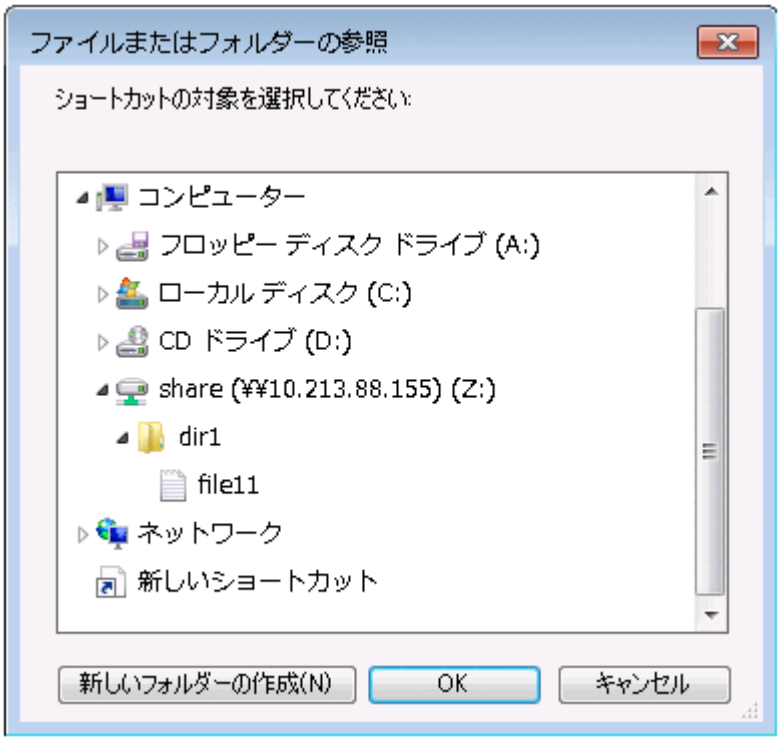
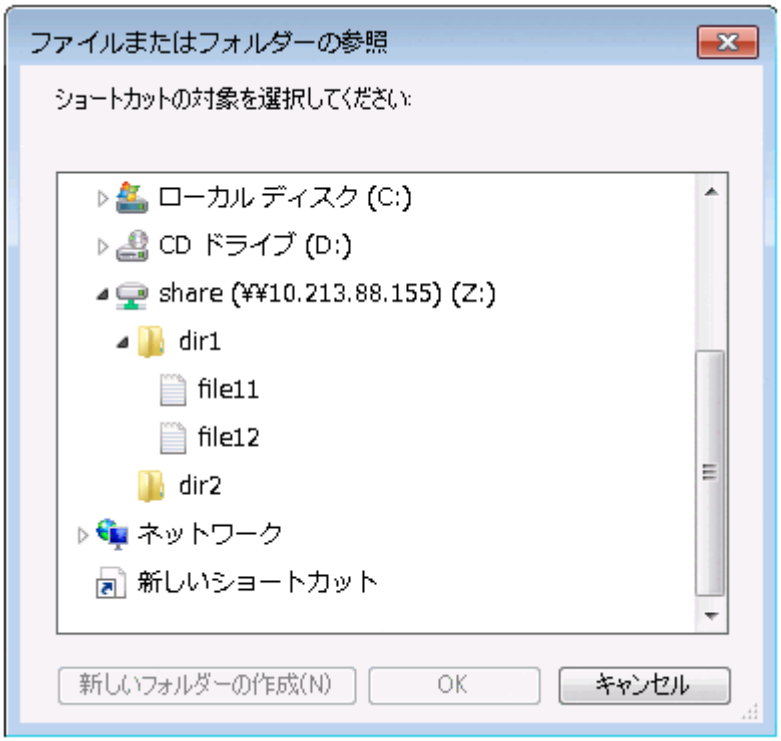


図 8-15： ABE が無効の場合

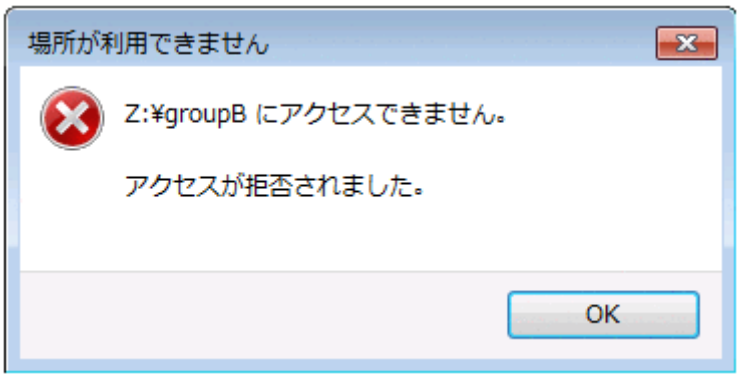


ショートカットファイルも ABE による表示／非表示の対象になります。したがって，ABE を有効にすると，読み取り権限のないショートカットファイルは表示されません。ショートカットファイルの読み取り権限があり，ファイル本体に読み取り権限がない場合，ショートカットファイルは表示されますが，ファイル本体は表示されません。

なお，File Services Manager で登録した CIFS 管理者は root ユーザーであるため，ABE による影響を受けません。

ABE を無効にすると，アクセス権のないフォルダやファイルも表示されます。この場合にアクセス権のないフォルダやファイルにアクセスすると，アクセスが拒否され，次に示すような画面が表示されます。

図 8-16：アクセス権がないフォルダやファイルへのアクセス結果の例



8.8.2 ABE によるファイルやフォルダの表示に必要な読み取り権限

ABE によるファイルやフォルダの表示に必要な権限は，ファイルやフォルダの ACL でアクセス許可の「読み取り」が「許可」になっていることですが，この読み取り権限は次の 5 つの権限をあわせたもので，どれか 1 つが欠けてもファイルやフォルダは表示されません。

- フォルダの一覧 / データの読み取り
- 属性の読み取り
- 拡張属性の読み取り
- アクセス許可の読み取り
- 同期 *

注 *

「同期」の権限は，ファイルおよびフォルダ作成時に自動的に付与されます。GUI からは設定できません。

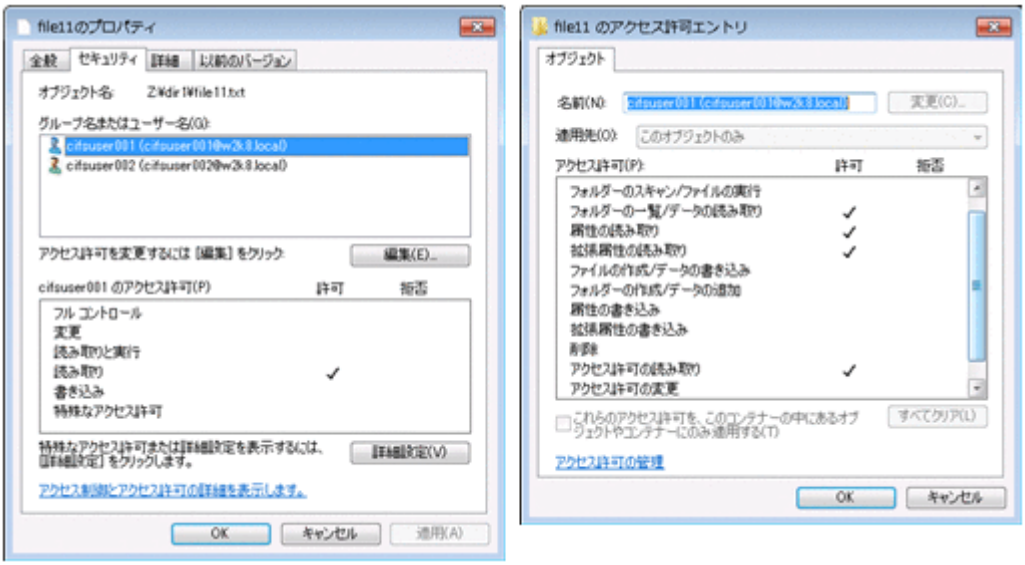
ファイルやフォルダの表示に必要な読み取り権限の有無は，この 5 つの権限の論理和で判定されます。例えば，「フォルダの一覧 / データの読み取り」だけを許可されているユーザーが，「属性の読み取り」，「拡張属性の読み取り」，「アクセス許可の読み取り」および「同期」を許可されているグループに所属して操作した場合，ファイルやフォルダは表示されます。

なお，ファイルの所有者は，そのファイルのアクセス権を操作する権限を持っています。このため，所有者が操作した場合，「フォルダの一覧 / データの読み取り」，「属性の読み取り」，「拡張属性の読み取り」および「同期」が許可されていれば，「アクセス許可の読み取り」が許可されていなくてもファイルやフォルダは表示されます。

HVFP の Classic ACL タイプのファイルシステムの場合，POSIX 準拠の ACL であるため，このような詳細な ACL は設定できません。

ABE によるファイルやフォルダの表示に必要な読み取り権限の表示例を次の図に示します。

図 8-17： ABE によるファイルやフォルダの表示に必要な読み取り権限の表示例（左：読み取り権限，右：詳細な読み取り権限）



8.9 CIFS 共有上のファイル・フォルダの制限

ここでは，CIFS 共有上のファイル・フォルダの制限について示します。

HVFP では CIFS 共有上に，Windows のバックアップイメージ用や，Hyper-V での仮想ハードディスク用として使われている VHD（Virtual Hard Disk）および VHDX 形式のファイルを作成し，それを利用した運用をすることはできません。

9

MMC 連携

Windows の管理ツールの 1 つである「コンピュータの管理」の「共有フォルダー」機能を MMC（Microsoft Management Console）から利用して，CIFS 共有を管理できます。MMC に「共有フォルダー」スナップインを追加することで，CIFS 管理者が HVFP の CIFS 共有を管理したり，CIFS 共有への CIFS クライアントの接続を管理したり，CIFS クライアントが開いている CIFS 共有上のファイルを管理したりできます。

9.1 HVFP の MMC 連携

HVFP では次のバージョンの MMC と連携できます。

- MMC 1.2
- MMC 2.0
- MMC 3.0

HVFP では，Windows が提供する「共有フォルダー」機能を利用できます。「共有フォルダー」機能の一覧を次に示します。

表 9-1： Windows が提供する「共有フォルダー」機能の一覧

「共有フォルダー」機能	
共有	CIFS 共有の作成
	CIFS 共有の削除
	CIFS 共有のコメント変更
	CIFS 共有のユーザー数制限
	CIFS 共有のキャッシュ要否
	CIFS 共有の一覧表示 *1*2
	共有レベル ACL 設定
	共有フォルダーの ACL 設定 *1
セッション	セッションの一覧表示 *1*2
	セッションの切断
開いているファイル	開いているファイルの一覧表示 *1*2
	開いているファイルを閉じる

注 *1

HVFP では，CIFS 管理者だけでなく，エンドユーザーも利用できます。

注 *2

HVFP では，情報の一部が正しく表示されません。詳細については，表 9-2： CIFS 共有一覧で参照できる項目と HVFP での利用可否，表 9-5： セッション一覧で参照できる項目と HVFP での利用可否および表 9-6： 開いているファイル一覧で参照できる項目と HVFP での利用可否を参照してください。

9.2 MMC と連携するために必要な作業（システム管理者の作業）

HVFP が MMC と連携するには，システム管理者が事前に File Services Manager で次の作業を実施しておく必要があります。各作業の詳細については，「ユーザーズガイド」（IF305）を参照してください。

- ファイルシステムの作成とマウント
  MMC で管理するファイルシステムを作成し，マウントします。
- CIFS サービスの起動確認
  CIFS サービスが起動していることを［List of Services］ページで確認します。
- CIFS 管理者の設定確認

CIFS 管理者が設定されていることを［CIFS Service Management］ページ（Setting Type : Administration）で確認します。

9.3 MMC と連携するために必要な作業（CIFS 管理者の作業）

HVFP が MMC と連携するには，CIFS 管理者が MMC に「共有フォルダー」スナップインを追加して，HVFP に接続する必要があります。

CIFS 管理者は，次のどちらかの方法で MMC を開いてください。

- ［スタート］－［アクセサリ］－［ファイル名を指定して実行］をクリックし，mmc と入力して［OK］ボタンをクリックする。
- コマンドプロンプトから mmc と入力して［Enter］キーを押す。

MMC に「共有フォルダー」スナップインを追加して，HVFP に接続する手順の一例を次に示します。

1. メインツールバーの［ファイル］－［スナップインの追加と削除］をクリックします。
2. ［スナップインの追加と削除］ダイアログボックスで［利用できるスナップイン］から［共有フォルダー］スナップインを選択して［追加］ボタンをクリックします。
3. ［共有フォルダー］ダイアログボックスで［別のコンピュータ］ラジオボタンを選択し，ノードまたは Virtual Server の仮想 IP アドレスまたはホスト名を指定して［完了］ボタンをクリックします。
4. ［スナップインの追加と削除］ダイアログボックスの［OK］ボタンをクリックします。
   手順 3. で指定したノードまたは Virtual Server に対する［共有フォルダー］スナップインが，コンソールツリーに組み込まれます。
5. コンソールを保存します。
   保存したコンソールは，［スタート］－［すべてのプログラム］－［管理ツール］から使用できます。

9.4 管理共有を利用する前に

CIFS 管理者が MMC から HVFP の CIFS 共有を管理する際に，次の管理共有（デフォルト共有）を利用して CIFS 共有にアクセスします。なお，CIFS クライアントが CIFS 共有を参照する場合も利用できます。

- 共有名：C$
- 共有パス：/mnt

管理共有を利用する際は，次のことに注意してください。

- File Services Manager からは利用できません。
- 管理共有の直下のファイルシステムを作成，削除または更新できません。
- 管理共有の直下のファイルシステムがアンマウント中または閉塞中の場合，ファイルシステムに属するフォルダの一覧を表示したり，フォルダを作成，削除または更新したりできません。
- もう一方のノードのリソースグループに所属しているファイルシステムに対して，CIFS 共有を作成，削除または管理できません。

9.5 MMC からの CIFS 共有管理

CIFS 管理者は，MMC を使用して，接続先のファイルシステムで CIFS 共有を作成，削除または更新できます。

MMC で HVFP の CIFS 共有を管理する場合，表示内容が無効な項目があったり，HVFP での制限に従って指定する項目があったりします。

CIFS 管理者は，MMC から CIFS 共有を管理する前に次のことに注意してください。

- CIFS 共有の一覧には，IPC$ や ADMIN$ などの Windows の特殊なフォルダも表示されますが，CIFS 管理者は操作できません。
- CIFS 共有を削除すると，共有レベル ACL の設定も削除されます。

9.5.1 CIFS 共有一覧の参照

MMC で HVFP の CIFS 共有一覧を参照する場合に，利用できない項目があります。表示される項目と HVFP での利用可否を次に示します。

表 9-2： CIFS 共有一覧で参照できる項目と HVFP での利用可否

項目名	利用可否	説明
共有名	○	CIFS 共有名が表示されます。 例：share1
フォルダー パス	○	CIFS 共有のパスが表示されます。 例：C:¥mnt¥fs01¥share1
タイプ	×	ネットワーク接続の種類として次のどれかが表示されます。ただし，正しい値ではありません。 ・ Windows ・ Macintosh ・ NetWare
クライアント接続数	○	CIFS 共有へのクライアントの接続数が表示されます。
説明	○	CIFS 共有を作成する際に指定した，CIFS 共有の説明が表示されます。 例：share1

（凡例）○：利用できる　×：利用できない

9.5.2 CIFS 共有の作成

MMC で CIFS 共有を作成するときに指定できる文字は，HVFP での制限に従います。MMC の項目名と指定する内容について次に示します。

表 9-3： CIFS 共有作成時に MMC で指定する項目

項目名	説明
フォルダー パス	作成する CIFS 共有の絶対パスを，先頭に「C:」を付けて指定します。 先頭の「C:」を除き，249 文字以内（差分スナップショットの自動作成スケジュールを運用する場合は 234 文字以内）で指定してください。 「C:」のあとに指定できる文字は英数字，感嘆符（!），番号記号（#），ドル記号（$），パーセント（%），アンパサンド（&），アポストロフィ（'），始め丸括弧（(），終わり丸括弧（)），正符号（+），コンマ（,），ハイフン（-），ピリオド（.），セミコロン（;），等号（=），単価記号（@），始め角括弧（[），終わり角括弧（]），アクサンシルコンフレックス（^），アンダーライン（_），アクサングラーブ（`），始め波括弧（{），終わり波括弧（}），波ダッシュ（~）およびスペースです。このほか，マルチバイト文字も指定できます。なお，末尾に指定したスペースおよび斜線は削除されます。 パーセント（%）は次の組み合わせで絶対パスに指定しないでください。 %D，%G，%H，%I，%L，%M，%N，%P，%R，%S，%T，%U，%V，%a，%d，%g，%h，%i，%m，%p，%u，%v，%w，%$ シンボリックリンクを含むパスは指定できません。また，「.snaps」，「.history」および「.lost+found」というディレクトリ名は指定できません。加えて，「.arc」，「.system_gi」，「.system_reorganize」および「lost+found」は，ファイルシステム直下のディレクトリの名称として指定できません。
共有名	作成する CIFS 共有の共有名を指定します。 80 文字以内（差分スナップショットの自動作成スケジュールを運用する場合は 69 文字以内）で指定してください。 指定できる文字は英数字，感嘆符（!），番号記号（#），ドル記号（$），パーセント（%），アンパサンド（&），アポストロフィ（'），始め丸括弧（(），終わり丸括弧（)），正符号（+），コンマ（,），ハイフン（-），ピリオド（.），セミコロン（;），等号（=），単価記号（@），始め角括弧（[），終わり角括弧（]），アクサンシルコンフレックス（^），アンダーライン（_），アクサングラーブ（`），始め波括弧（{），終わり波括弧（}），波ダッシュ（~）およびスペースです。このほか，マルチバイト文字も指定できます。ただし，「$」，「.」や「..」のようにドル記号（$）またはピリオド（.）だけを指定したり，「Abc.」や「Abc.$」のようにピリオド（.）を文字列の末尾やドル記号（$）を除いた末尾に指定したりできません。また，末尾に指定したスペースは削除されます。 パーセント（%）は次の組み合わせで共有名に指定しないでください。 %D，%G，%H，%I，%L，%M，%N，%P，%R，%S，%T，%U，%V，%a，%d，%g，%h，%i，%m，%p，%u，%v，%w，%$ なお，global，homes，printers，admin$，c$，global$，homes$，ipc$ および printers$ は，CIFS 共有名として指定できません。 英大文字と英小文字に関係なく，ノードまたは Virtual Server で一意な名称を指定してください。
説明	作成する CIFS 共有の説明を指定します。 256 文字以内で指定してください。 指定できる文字は英数字，感嘆符（!），番号記号（#），ドル記号（$），アンパサンド（&），アポストロフィ（'），始め丸括弧（(），終わり丸括弧（)），アステリスク（*），正符号（+），コンマ（,），ハイフン（-），ピリオド（.），斜線（/），コロン（:），始め山括弧（<），終わり山括弧（>），疑問符（?），単価記号（@），始め角括弧（[），円記号（¥），終わり角括弧（]），アクサンシルコンフレックス（^），アンダーライン（_），アクサングラーブ（`），始め波括弧（{），縦線（|），終わり波括弧（}）および波ダッシュ（~）です。スペースも指定できますが，文字列の先頭および末尾には指定できません。また，円記号（¥）は文字列の末尾に指定できません。 このほか，マルチバイト文字も指定できます。

9.5.3 CIFS 共有の情報の変更

MMC で CIFS 共有の情報を変更する際，一部の項目に指定する値は HVFP の制限に従います。MMC の項目名と指定する内容について次に示します。

表 9-4： CIFS 共有の情報変更時に指定する項目

項目名	説明
説明	CIFS 共有の説明を指定します。256 文字以内で指定してください。 指定できる文字は英数字，感嘆符（!），番号記号（#），ドル記号（$），アンパサンド（&），アポストロフィ（'），始め丸括弧（(），終わり丸括弧（)），アステリスク（*），正符号（+），コンマ（,），ハイフン（-），ピリオド（.），斜線（/），コロン（:），始め山括弧（<），終わり山括弧（>），疑問符（?），単価記号（@），始め角括弧（[），円記号（¥），終わり角括弧（]），アクサンシルコンフレックス（^），アンダーライン（_），アクサングラーブ（`），始め波括弧（{），縦線（|），終わり波括弧（}）および波ダッシュ（~）です。スペースも指定できますが，文字列の先頭および末尾には指定できません。また，円記号（¥）は文字列の末尾に指定できません。 このほか，マルチバイト文字も指定できます。
ユーザー数制限	CIFS 共有に接続するユーザー数の上限を指定します。 ただし，HVFP の CIFS クライアントの最大接続数を超える接続はできません。 HVFP の CIFS クライアントの最大接続数については，表 7-2： を参照してください。
オフラインの設定	オフラインで利用できるファイルとプログラムがある場合，どの項目をオフラインのユーザーが利用できるようにするかを，次のどれかを選択して指定します。 • ユーザーが指定したファイルおよびプログラムのみオフラインで利用可能にする • 共有フォルダーにあるファイルやプログラムはオフラインで利用可能にしない • 共有フォルダーからユーザーが開いたファイルとプログラムは，すべて自動的にオフラインで利用可能にする

9.6 MMC からのセッション管理

CIFS 管理者は MMC を使用して，CIFS 共有にアクセスしているユーザーのセッションの一覧を参照したり，セッションを切断したりできます。

HVFP の CIFS 共有にアクセスしているユーザーのセッションを，MMC から管理する場合の注意事項について示します。

9.6.1 セッション一覧の参照

HVFP の CIFS 共有にアクセスしているユーザーのセッション一覧を参照する場合に，利用できない項目があります。表示される項目と HVFP での利用可否を次に示します。

表 9-5： セッション一覧で参照できる項目と HVFP での利用可否

項目名	利用可否	説明
ユーザー	○	CIFS 共有に接続しているユーザーの名称が表示されます。 例：group01¥administrator
コンピュータ	○	CIFS 共有に接続しているユーザーのコンピュータ名が表示されます。 例：adam

項目名	利用可否	説明
タイプ	×	ネットワーク接続の種類として次のどれかが表示されます。ただし，正しい値ではありません。 ・ Windows ・ Macintosh ・ NetWare
開いているファイルの数	○	CIFS クライアントが開いている CIFS 共有上のファイルの数が表示されます。
接続時間	×	正しい値が表示されず，常に 0 が表示されます。
アイドル時間	×	正しい値が表示されず，常に 0 が表示されます。
ゲスト	×	正しい値が表示されず，常に「いいえ」が表示されます。

（凡例）○：利用できる　×：利用できない

なお，トレンドマイクロ社のスキャンソフトを使用するように設定している場合，スキャンサーバからのアクセスによるセッションも表示されます。

9.6.2 セッションの切断

MMC からセッションを切断する場合，次のことに注意してください。

- セッションを個別に指定して切断する際に，ユーザー名とコンピュータ名が同一のセッションが複数存在すると，該当するすべてのセッションが切断されます。
- セッションを切断すると，操作中のデータが失われるおそれがあります。切断する前に，接続しているユーザーに連絡してください。
- MMC から CIFS 共有を作成または更新すると，セッションが自動的に切断されます。このため，MMC を操作していたクライアントマシンから同じセッションでファイルにアクセスすると，エラーになることがあります。この場合は，いったんセッションを切断してから，再度ファイルにアクセスしてください。
- スキャンサーバからのアクセスによるセッションをウイルススキャン中に切断した場合，スキャンエラーとなることがあります。

9.7 開いているファイルの MMC からの管理

MMC を使用して CIFS クライアントが開いている CIFS 共有上のファイルの一覧を参照することができます。なお，CIFS 管理者であれば，CIFS クライアントが開いているファイルを閉じることができます。

CIFS クライアントが開いている HVFP の CIFS 共有ファイルを，MMC から管理する場合の注意事項について示します。

9.7.1 開いているファイルの一覧表示

CIFS クライアントが開いている CIFS 共有上のファイルの一覧を表示したとき，利用できない項目があります。表示される項目と HVFP での利用可否を次に示します。

表 9-6： 開いているファイル一覧で参照できる項目と HVFP での利用可否

項目名	利用可否	説明
開いているファイル	○	CIFS クライアントが開いている CIFS 共有上のファイルの名前が表示されます。名前付きパイプも含まれます。なお，表示される文字数は 260 文字までです。 例：C:¥mnt¥share¥file.txt
アクセス	○	ファイルを開いているユーザーの名称が表示されます。 例：group01¥user01
タイプ	×	ネットワーク接続の種類として次のどれかが表示されます。正しい値ではありません。 ・ Windows ・ Macintosh ・ NetWare
ロック数	○	開いているファイルに対するロックの数が表示されます。
オープンモード	○	CIFS クライアントがファイルを開いたときに与えられたアクセス権が次のどれかで表示されます。 ・ 読み取り ・ 書き込み ・ 書き込みと読み取り ・ アクセスなし

（凡例）

○：利用できる　×：利用できない

9.7.2 開いているファイルを閉じる

開いているファイルを MMC から閉じる場合，次のことに注意してください。

- ファイルは強制的に閉じられます。また，ファイルを閉じることは，CIFS クライアントに対して通知されません。このため，ファイルを閉じると，操作中のデータが失われるおそれがあります。閉じる前に，ファイルを操作しているユーザーに連絡してください。
- 名前付きパイプを閉じることはできません。
- ディレクトリを閉じても，ディレクトリ下にあるファイルは閉じられません。
- 大量のファイルが開かれている状態で MMC からすべてのファイルを閉じた場合，HVFP に負荷が掛かります。

9.8 共有レベル ACL

CIFS 管理者は，MMC で共有レベル ACL を設定できます。設定した共有レベル ACL は，共有フォルダー内のすべてのファイルとサブフォルダに適用されます。

共有レベル ACL は，HVFP で設定できる Advanced ACL や Classic ACL のように個々のディレクトリやファイルに設定される ACL ではなく，CIFS 共有に設定される ACL です。共有レベル ACL に対して，Advanced ACL や Classic ACL のことをファイルレベル ACL と呼びます。

ファイルレベル ACL と共有レベル ACL のどちらも設定されている場合，共有レベル ACL を評価したあとで，ファイルレベル ACL を評価します。例えば，共有レベル ACL で読み取りだけを許可していて，ファイルレベル ACL でフルコントロールが設定されているファイルに対しては，読み取りだけが許可されます。

CIFS 管理者が設定できる共有レベル ACL について次の表に示します。

表 9-7： 共有レベル ACL

項目	説明
設定するアクセス権	・ フルコントロール ・ 変更 ・ 読み取り
ACE の種別	許可または拒否
ACE の上限	1 共有当たり 1,820 エントリーまで

共有レベル ACL を設定する場合，指定できる ACE 数と CIFS 共有数にリソースグループごとの上限があります。次の条件を満たす値を指定してください。

図 9-1： 指定できる ACE 数と CIFS 共有数の上限算出

65,536 ＞（↑((36 x ACE数 + 320) x 10)↑ × ↑(共有数 / 10)↑) / 1024

（凡例）

↑((36 x ACE数 + 320) x 10)↑ ：((36 x ACE数 + 320) x 10)の計算結果を 8,192バイト単位に切り上げた値

↑(共有数 / 10)↑ ：(共有数 / 10)の計算結果を整数値に切り上げた値

CIFS 共有数と，共有ディレクトリに対して指定できる ACE 数の目安を次に示します。

表 9-8： CIFS 共有数に対して指定できる ACE 数の目安

CIFS 共有数	共有ディレクトリに対する ACE 数
1,000	1,820
7,500	210

共有レベル ACL ではアクセス権として「フルコントロール」,「変更」または「読み取り」を設定できます。各アクセス権と CIFS 共有での操作との対応を次の表に示します。

表 9-9： CIFS 共有での操作と共有レベル ACL で設定するアクセス権との対応

CIFS 共有での操作	共有レベル ACL のアクセス権		
	フルコントロール	変更	読み取り
ファイル名とサブフォルダ名の表示	○	○	○
サブフォルダへの移動	○	○	○
ファイル内容の表示とプログラムの実行	○	○	○
共有フォルダーへのファイルとサブフォルダの追加	○	○	×
ファイルのデータの変更	○	○	×
サブフォルダとファイルの削除	○	○	×
アクセス許可の変更	○	×	×
所有権の取得	○	×	×

（凡例）

○：操作できる　×：操作できない

共有レベル ACL を設定する場合，次のことに注意してください。

・ 共有レベル ACL は，File Services Manager から設定できません。

- 共有レベル ACL は CIFS 共有だけで有効な ACL です。NFS サービスからのアクセスに対しては共有レベル ACL のアクセス制限が適用されません。
- 操作しているユーザーに対して，複数のアクセス許可が該当する場合，各アクセス許可の論理和が適用されます。例えば，「読み取り」のアクセス許可を持つユーザー A が「変更」のアクセス許可を持つグループ B に属している場合，「変更」のアクセス許可がユーザー A に適用されます。
- 許可エントリーと拒否エントリーを同時に設定した場合は，拒否エントリーが優先されます。
- 共有レベル ACL を変更するときに，対象の CIFS 共有に接続しているユーザーには変更後の ACL が適用されません。CIFS 管理者は，対象の CIFS 共有に接続しているユーザーがいないことを確認してから共有レベル ACL を変更してください。
- CIFS 共有に対して，共有レベル ACL のほかにアクセス制御（read only，read list または write list）が設定されている場合，どちらか厳しい方のアクセス制限が適用されます。例えば，共有レベル ACL で「フルコントロール」が設定されていても，「read only」のアクセス制御が設定されていた場合は，対象の CIFS 共有に対して読み取りだけが許可されます。
  CIFS 共有に対して共有レベル ACL とアクセス制御が設定されている場合に適用されるアクセス権について次の表に示します。

表 9-10： 共有レベル ACL とアクセス制御が設定されている場合に適用されるアクセス権

共有レベル ACL	アクセス制御			
	read only		read list	write list
	yes	no		
フルコントロール	RO	RW	RO	RW
変更	RO	RW	RO	RW
読み取り	RO	RO	RO	RO

（凡例）
RO：読み取りだけができる　RW：読み取りと書き込みができる

- 共有レベル ACL に「読み取り」だけを設定すると，対象の CIFS 共有は読み取り専用で公開されます。CIFS 管理者からのアクセスに対しても読み取りだけが許可されます。

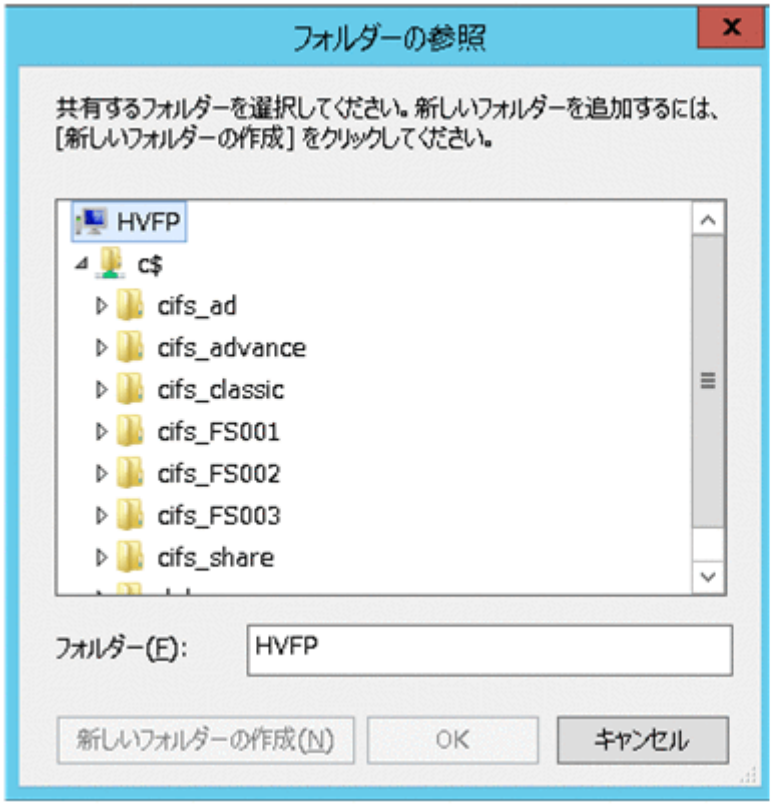
9.9 MMC 操作上の注意事項

MMC を操作する上での注意事項を挙げます。なお，操作画面の図は，Windows Server 2012 R2, MMC 3.0 を使用した場合の例です。

- フォルダの参照画面について
  共有を追加する際，共有するフォルダへのパスを［フォルダの参照］画面（図 9-2： フォルダの参照画面例参照）から選択できます。
  フォルダの参照画面で，C$ フォルダの直下には，ファイルシステムがフォルダとして表示されます。このとき，マウントされているファイルシステムだけが表示されます。
  また，Physical Node 使用時で，フェールオーバー状態の場合（稼働中のノードで両リソースグループを運用している場合），もう一方のノードに所属するファイルシステムも表示されます。この場合，もう一方のノードのファイルシステムに共有を作成できませんが，画面上でもう一方のノードのファイルシステムを選択したり，その配下にフォルダを作成したりできるので注意してください。

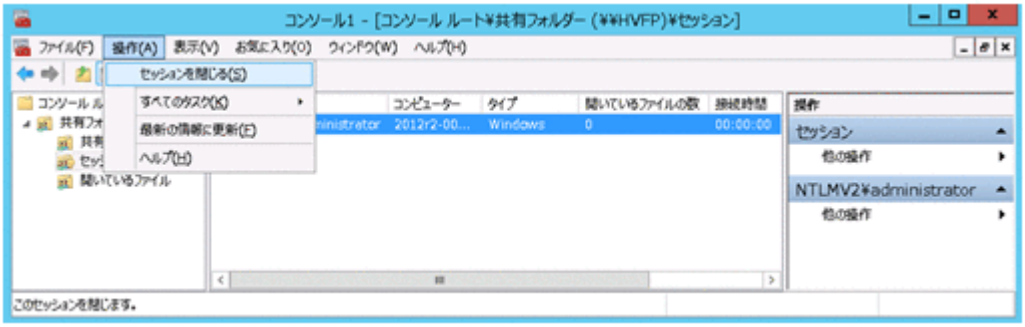
なお，もう一方のノードのファイルシステム，およびその配下のフォルダを選択した場合，共有を作成する際にエラーとなります（エラーの詳細は，「A.3.1 共有の追加操作でのエラー」を参照してください）。

図 9-2： フォルダの参照画面例



- 任意のユーザーのセッションを切断する操作について
  任意のユーザーを選択し，［操作］メニューから［セッションを閉じる］を選択すると，対象ユーザーのセッションだけを閉じることができます（図 9-3： セッションの操作画面例 1 参照）。この時，操作対象としているユーザーと，ユーザー名およびコンピュータ名が同一のセッションが複数存在すると，それらのセッションは，まとめて切断されるので注意してください。

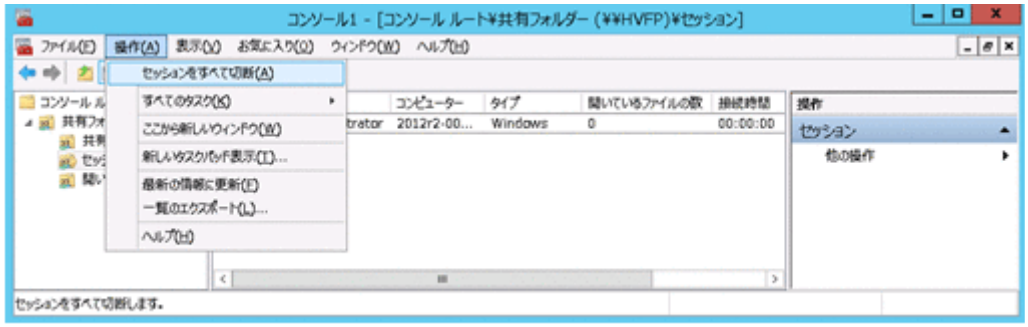
図 9-3： セッションの操作画面例 1



- すべてのセッションを切断する操作について
  ツリーの「セッション」を選択し，［操作］メニューから［セッションをすべて切断］を選択すると，接続している全セッションを一度に閉じることができます（図 9-4： セッションの操作画面例 2 参照）。この時，ユーザー名およびコンピュータ名が同一のユーザーが複数接続されていると，セッションは正常に切断されますが，図 A-4： セッションの切断に失敗した際の画面例に示すエラー画面が複数表示されます。

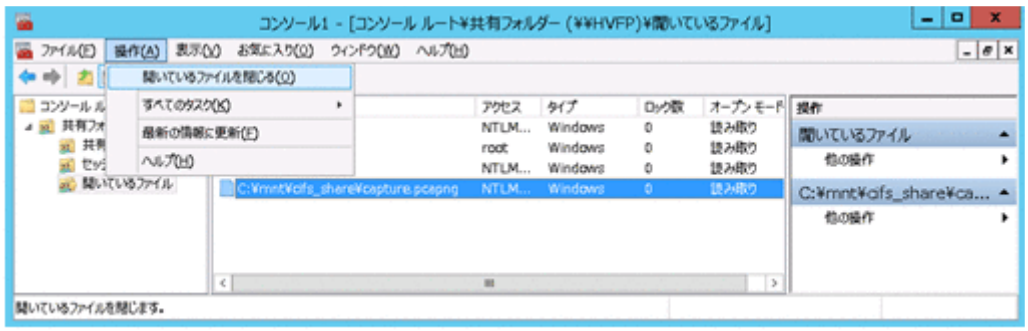
なお，このエラー画面が表示されても，セッションが切断されていない場合は，「A.3.3 共有の停止時のエラー」の (2) を参照してください。

図 9-4：セッションの操作画面例 2



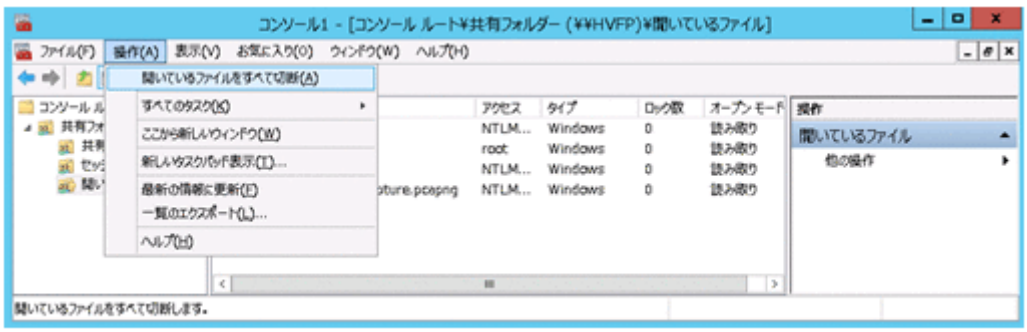
- 任意のファイルを閉じる操作について
  任意のファイルを選択し，［操作］メニューから［開いているファイルを閉じる］を選択すると，選択したファイルだけを閉じることができます（図 9-5： 任意のファイルを閉じる操作の画面例参照）。この時，CIFS クライアントに対して通知されることなく，選択したファイルが閉じられるので注意してください。

図 9-5：任意のファイルを閉じる操作の画面例



- すべてのファイルを閉じる操作について
  ツリーの「開いているファイル」を選択し，［操作］メニューから［開いているファイルをすべて切断］を選択すると，CIFS クライアントが開いている CIFS 共有上のすべてのファイルを一度に閉じることができます（図 9-6： すべてのファイルを閉じる操作の画面例）。この時，CIFS クライアントに対して通知されることなく，すべてのファイルが閉じられるので注意してください。

図 9-6：すべてのファイルを閉じる操作の画面例



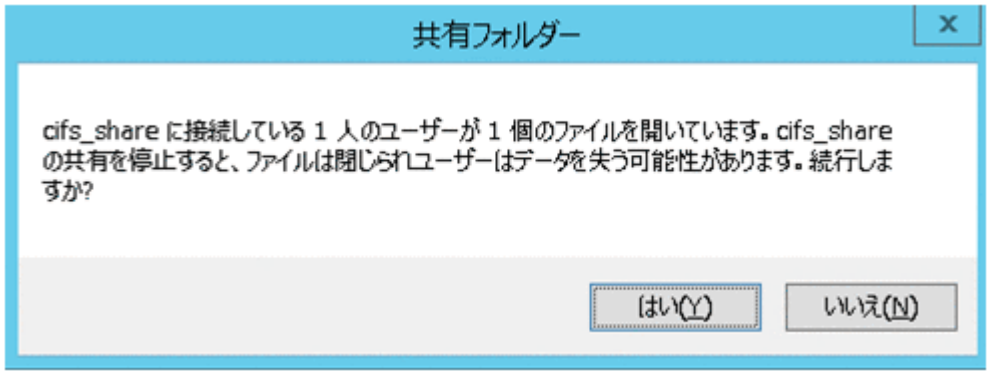
- MMC のバージョンによる違いについて
  MMC から CIFS 共有を作成する際に設定するアクセス許可のデフォルト値は，次に示すように MMC のバージョンによって異なります。

表 9-11： MMC のバージョンによるアクセス許可のデフォルト値の違い

MMC のバージョン	アクセス許可のデフォルト値
1.2	すべてのユーザーがフルコントロールを持つ
2.0 または 3.0	すべてのユーザーが読み取り専用のアクセスを持つ

このため，MMC 2.0 または MMC 3.0 を使用する場合に CIFS 共有への書き込みができるようにするには，ウィザードのアクセス許可を設定する画面で［アクセス許可のカスタマイズ］ラジオボタンを選択して［カスタマイズ］ボタンをクリックし，書き込みを許可するユーザーに対して「フルコントロール」または「変更」を設定する必要があります。
また，MMC 3.0 を使用して CIFS 共有を削除すると，次の図に示すメッセージが表示されます。CIFS 共有の削除は，［はい］をクリックしたあと実行されます。

図 9-7： MMC 3.0 で CIFS 共有を削除するときの表示メッセージ



なお，CIFS 共有を削除すると，操作中のデータが失われるおそれがあります。削除する前に，接続しているユーザーに連絡してください。

10

Volume Shadow Copy Service を使用した差分スナップショットの公開

この章では，ファイルスナップショット機能で作成された差分スナップショットを，Volume Shadow Copy Service を使用して CIFS クライアントに公開する方法を説明します。

ファイルスナップショット機能の概要，運用方法および運用上の注意事項については，「システム構成ガイド」（IF302）および「ユーザーズガイド」（IF305）を参照してください。

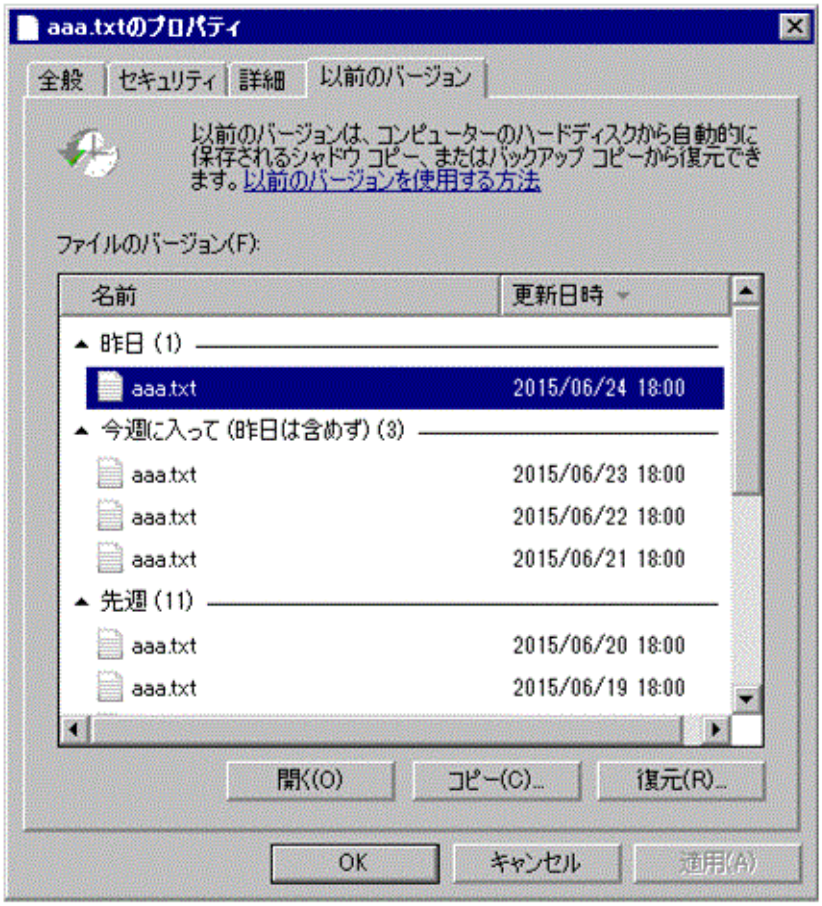
10.1 Volume Shadow Copy Service の概要

差分スナップショットを Volume Shadow Copy Service を使用して CIFS クライアントに公開できます。差分スナップショットをファイルシステムの共有内に公開したり，差分スナップショットに対して共有を作成したりする必要はありません。

CIFS クライアントに公開しているファイルシステムに対して作成された差分スナップショットを 1 つ以上マウントしている場合，または，クライアントからアクセスされた際に差分スナップショットをマウントする場合，CIFS クライアントがファイルシステム内のファイルまたはフォルダのプロパティダイアログを参照すると，［以前のバージョン］タブ内に差分スナップショットの対象ファイルまたはフォルダの一覧が表示されます。CIFS クライアントは，このタブから差分スナップショットのファイルやフォルダの内容を表示したり，ほかのフォルダにコピーしたり，作成元のファイルシステムに復元したりできます。

［以前のバージョン］タブの表示例を次に示します。

図 10-1： ファイルまたはフォルダのプロパティダイアログの［以前のバージョン］タブ



［以前のバージョン］タブ内で公開する差分スナップショットに対して，ファイルの更新があったかどうかを確認するかどうかによって，［以前のバージョン］タブに表示される情報が変わります。

［以前のバージョン］タブに表示される情報の差異を次に示します。

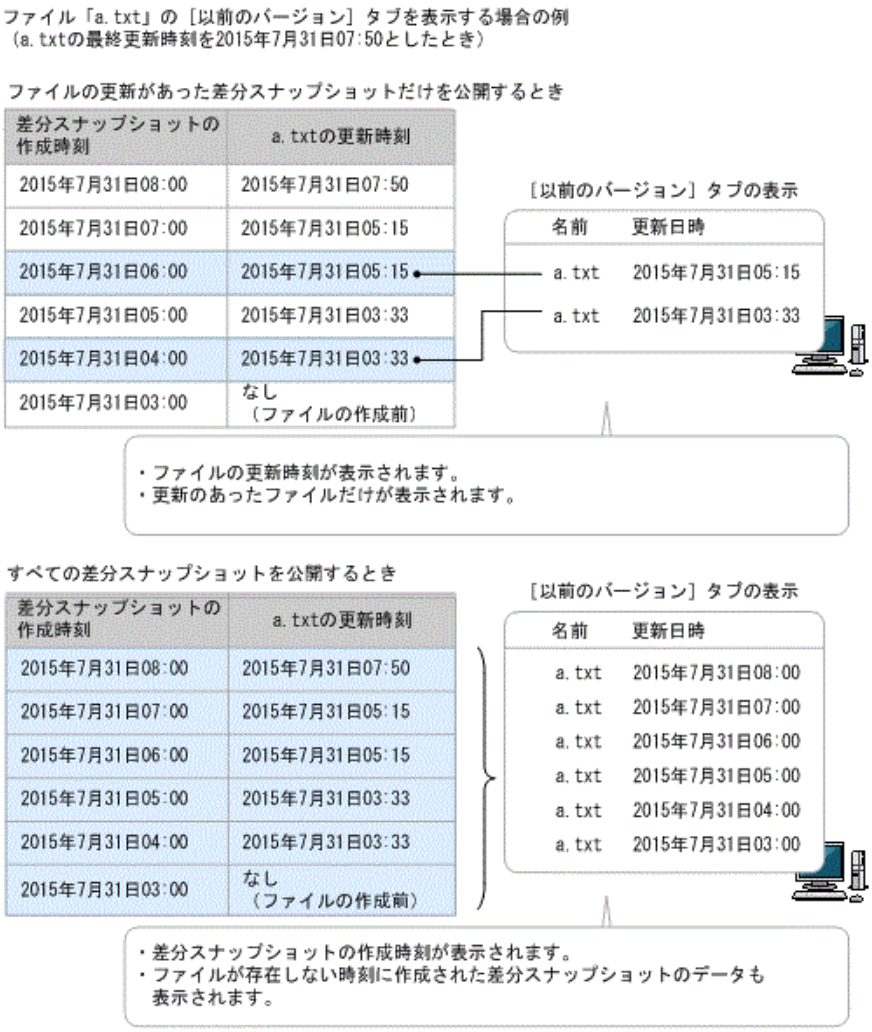
表 10-1：［以前のバージョン］タブに表示される情報

［以前のバージョン］タブ内で公開する差分スナップショット	［以前のバージョン］タブに表示される情報
ファイルの更新があった差分スナップショットだけを公開する（クライアントからアクセスされた際に一時的に差分スナップショットをマウントしない設定の場合を含む）	参照対象がファイルの場合，更新のあったファイルだけが表示されます。［更新日時］にはファイルの更新時刻が表示されます。参照対象がフォルダの場合，フォルダが存在しない時刻に作成された差分スナップショットのデータ * が表示されることがあります。［更新日時］には差分スナップショットの作成時刻が表示されます。
自動作成されたすべての差分スナップショットを公開する	参照対象のファイルまたはフォルダが存在しない時刻に作成された差分スナップショットのデータ * が表示されることがあります。［更新日時］には差分スナップショットの作成時刻が表示されます。

注 *

ファイルまたはフォルダが存在しない時刻に作成された差分スナップショットのデータにアクセスしようとするとエラーになります。

図 10-2：［以前のバージョン］タブに表示される情報の表示例



10.2 Volume Shadow Copy Service に対応する CIFS クライアントのプラットフォーム

HVFP でサポートされている CIFS クライアントのプラットフォームのうち，Volume Shadow Copy Service に対応していないプラットフォームは次のとおりです。

- Mac OS X

10.3 Volume Shadow Copy Service を使用した差分スナップショットの公開方法

ここでは，Volume Shadow Copy Service を使用して差分スナップショットを CIFS クライアントに公開する方法を説明します。

操作手順は，すでに差分スナップショットを運用していることを前提としています。

Volume Shadow Copy Service を使用した差分スナップショットの公開を開始する手順を次に示します。

1. CIFS サービスの構成定義で，ファイル共有にデフォルトで Volume Shadow Copy Service を使用するよう設定します。
   ［CIFS Service Management］ページ（Setting Type：Basic）の［CIFS default setup］で，［Volume Shadow Copy Service］に「Use」を指定します。
2. Volume Shadow Copy Service で差分スナップショットを公開しないファイル共有がある場合は，それらのファイル共有に対して Volume Shadow Copy Service を使用しないよう設定します。
   既存のファイル共有で差分スナップショットを公開しない場合は，［共有編集］ダイアログの［アドバンスド］タブの［CIFS］サブタブで，［Volume Shadow Copy Service を使用］に「いいえ」を指定します。今後追加するファイル共有で差分スナップショットを公開しない場合は，追加する際に［ファイルシステム構築と共有作成］ダイアログまたは［共有追加］ダイアログで同様に設定してください。
3. CIFS サービスを再起動します。
   ［Access Protocol Configuration］ダイアログの［List of Services］ページで CIFS サービスを再起動します。

なお，上記の手順を完了した時点で，CIFS クライアントが対象のファイル共有にすでにアクセスしていた場合は，ファイル共有内のファイルまたはフォルダのプロパティダイアログに以前のバージョンが表示されません。エンドユーザーに，一度ログオフしたあと，ログオンしてから再度ファイル共有にアクセスするよう連絡してください。

10.4 CIFS クライアントが Volume Shadow Copy Service を使用する際の注意事項

CIFS クライアントが差分スナップショットを参照するために Volume Shadow Copy Service を使用する際の注意事項は次のとおりです。

- Volume Shadow Copy Service を使用した差分スナップショットにアクセスする場合は，ファイルまたはフォルダのプロパティダイアログの［以前のバージョン］タブから操作してください。
- ［以前のバージョン］タブに表示される差分スナップショットは，CIFS クライアントのプラットフォームによって異なる場合があります。
- CIFS クライアントが［以前のバージョン］タブから差分スナップショットのファイルまたはフォルダをコピーまたは復元したあと，再度コピーまたは復元する場合は，対象のプロパティダイアログを閉じてから操作してください。プロパティダイアログを閉じずに操作してもコピーまたは復元できません。
- CIFS クライアントが［以前のバージョン］タブから差分スナップショットのファイルまたはフォルダをコピーまたは復元しても，次の属性はコピーまたは復元されません。
  - 作成日時
  - アクセス日時
  - ACL
  - 所有者
- 作成直後の差分スナップショットについて，次のことを確認してください。
  ファイルの更新があった差分スナップショットだけを公開するとき
  ［以前のバージョン］タブに作成直後の差分スナップショットが表示されないことがありますが，しばらくすると表示されるようになります。

すべての差分スナップショットを公開するとき
作成直後の差分スナップショットのデータにアクセスしようとするとエラーになることがありますが，しばらくするとデータにアクセスできるようになります。

- 次の形式の名称をファイル共有内のファイルまたはフォルダに指定しないでください。
@GMT-nnnn.nn.nn-nn.nn.nn（「n」は 0 ～ 9 の数字）
その名称のファイルまたはフォルダ，および差分スナップショットにアクセスできなくなるおそれがあります。
- 差分スナップショットの数が多い場合に，［以前のバージョン］タブでファイルの更新があった差分スナップショットだけを公開すると，すべての差分スナップショットを公開するときに比べて，［以前のバージョン］タブの表示に時間が掛かります。
- 差分スナップショットに存在するファイルの種別によって，次の表に示すように CIFS クライアントからの操作が制限されます。

表 10-2：CIFS クライアントからの操作の制限

操作	WORM 化されていないファイル	WORM ファイル*	スタブファイル
［以前のバージョン］タブでの対象ファイルの一覧表示	○	○	×
［開く］ボタン	○	○	×
［コピー］ボタン	○	○	×
［復元］ボタン	○	×	×

（凡例）○：実行できる　×：実行できない
注 *
リテンション期間が過ぎた WORM ファイルも含まれます。

- Volume Shadow Copy Service を使用して差分スナップショットにアクセスする場合は , 差分スナップショットにアクセスするための情報（付加情報）がパス名に付加されます。そのため，アクセス可能なファイルやフォルダのパス名の最大長が，クライアントからアクセスできる最大長より 25 文字短くなります。差分スナップショットにアクセスしようとする際，付加情報を加えたパス長が，クライアントからアクセスできるパス名の最大長を超えた場合，差分スナップショットにアクセスできなくなります。なお，クライアントからアクセスできるパス名の最大長は，クライアントの動作に依存するため，環境によって異なることがあります。
- 一度存在したあとに存在しない期間があったファイルまたはディレクトリは，［以前のバージョン］タブ内に差分スナップショットが表示されないことがあります。
- ファイルやフォルダのパス長の制限によって，Volume Shadow Copy Service を使用して差分スナップショットにアクセスできない場合は，差分スナップショットにファイル共有を作成してアクセスしてください。作成する CIFS 共有名は，作成元の CIFS 共有名の長さを超えないようにしてください。

すべての差分スナップショットを公開する際の注意事項

すべての差分スナップショットを公開すると [以前のバージョン] タブの表示時間は，ファイルの更新があった差分スナップショットだけを公開する場合に比べて早くなります。

すべての差分スナップショットを公開する場合の注意事項は次のとおりです。

- ファイルまたはフォルダが存在しない時刻に作成された差分スナップショットのデータにアクセスしようとするとエラーになります。

- Windows 8.1 または Windows Server 2012 以降のクライアント OS を使用する必要があります。
  なお，Windows 8.1 または Windows Server 2012 以降のクライアント OS で［以前のバージョン］タブから差分スナップショットのファイルまたはフォルダをコピーする場合は，ファイルまたはフォルダを開いて，データが存在していることを確認してからコピーしてください。ファイルまたはフォルダが存在していないと，Windows のコピー処理が完了しないため，エクスプローラまたはクライアント OS がハングアップするおそれがあります。
- 次の問題が発生するため，Windows 8.1 または Windows Server 2012 より古いクライアント OS は使用しないでください。
  - ファイルまたはフォルダが存在しない時刻に作成された差分スナップショットのデータにアクセスしようとしたときに，エラーが表示されないおそれがあります。
  - ［以前のバージョン］タブで差分スナップショットのファイルまたはフォルダをコピーまたは復元しても，ファイル属性がコピーまたは復元されません。
- SMB 1.0 を使用し，かつ差分スナップショットの数が 20 を超える場合，差分スナップショットのファイルまたはフォルダを復元したときに，［以前のバージョン］タブで差分スナップショットの一覧を再表示する時間は，ファイルの更新があった差分スナップショットだけを公開するときと比べても変わりません。
- 次に示すファイルまたはフォルダを［以前のバージョン］タブで表示する時間は，ファイルの更新があった差分スナップショットだけを公開する場合と比べても変わりません。
  - システム属性が付与されたフォルダ
  - 次に示す特定の拡張子のファイル
    `ani，appref-ms，cur，exe，lnk，mfp，pif，scf，scr，searchConnector-ms` など

11

CIFS クライアントとして使用するプラットフォームについて

この章では，CIFS クライアントとして使用するプラットフォームの違いによる注意事項について説明します。

11.1 Windows に共通すること

CIFS クライアントで，Windows へログオンしたあと，初めて CIFS 共有にアクセスするときには，Windows へログオンする際に使用したユーザー名とパスワードで HVFP のノードまたは Virtual Server に認証要求が送信されます。そのため，ゲストアカウントでのアクセスを許可している場合に，Windows にログオンしているユーザーが［Access Protocol Configuration］ダイアログの［CIFS Service Management］ページ（Setting Type：Security）の［Mapping to guest account］で指定したユーザーに該当すると，ユーザー名とパスワードの入力が要求されないで，ゲストアカウントとして CIFS 共有にアクセスすることがあります。ゲストアカウントでのアクセスを許可する場合には，注意してください。

また，CIFS サービスの認証モードが Active Directory Authentication の場合には，Windows にログオンしたユーザー名とパスワードで認証に失敗すると，ユーザー名とパスワードの入力を求められます。ゲストアカウントでのアクセスを許可している場合に，入力したユーザー名とパスワードでの認証に失敗した場合にはゲストアカウントでアクセスされますので，注意してください。

11.2 Windows 8.1 の場合

CIFS クライアントが Windows 8.1 の場合の注意事項を次に示します。

11.2.1 共有内のファイル・フォルダ

クライアントから共有ディレクトリ内に作成するファイル・フォルダに関しての注意事項を次に説明します。

11.2.1.1 ACL を追加する場合

HVFP の共有上のファイル・ディレクトリに ACL を追加しようとする際に次の条件が重なると，ローカルユーザー／グループを参照できなくて，ACL を追加できません。

- クライアントにログオンする方法が次のどちらかである
  - ユーザーアカウント制御（UAC）を有効に設定した状態で，次のどちらかのローカルアカウントでログオンする
    - Administrator（ビルトインアカウント）
    - 一般ユーザーアカウント（クライアントマシン上のローカルアカウント）
  - ユーザーアカウント制御（UAC）を無効に設定した状態で，クライアントにローカルアカウントでログオンする
- 認証方式が次のどちらかである
  - ローカル認証
  - Active Directory 認証かつ，ユーザーマッピングを使用しない

11.2.1.2 Quota を使用する場合

クライアントがエクスプローラを使用して共有にファイルを移動または貼り付ける際に，ブロック使用量または inode 数が HVFP で設定したソフトリミットを超過すると，ハードリミットを超過していない状態でも，クライアントの操作に失敗します。なお，COPY コマンドや XCOPY コマンドを使用すると，ハードリミットを超過していない状態であれば，共有にファイルを移動または貼り付けることができます。

11.2.1.3 オフラインファイルを有効にする場合

クライアント側でオフラインファイルを有効にした共有に Microsoft Office のファイルを作成した際に，ファイルが正しく保存されないことがあります。そのため，Windows 8.1 で Microsoft Office を使用する場合には，共有のオフラインファイルを無効にしてください。

11.2.2 MMC を使用する場合

Windows 8.1 から MMC を使用して CIFS 共有を管理する場合の注意事項を次に説明します。

11.2.2.1 Windows へのログオン

次のどれかの方法で Windows にログオンしてください。それ以外の場合には，HVFP へのアクセスが拒否されます。

- ドメインアカウントを使用してログオンする
- Administrator アカウントを使用してログオンする
- クライアントのユーザーアカウント制御（UAC）を無効に設定した状態で，Administrator 以外の管理者アカウントでログオンする

11.2.2.2 共有レベル ACL

共有レベル ACL にエントリーを追加しようとする際に，次の条件が重なると，ローカルユーザー／グループを参照できないため，共有レベル ACL の追加ができません。

- クライアントにログオンする方法が次のどちらかである
  - ユーザーアカウント制御（UAC）を有効に設定した状態で，次のどちらかのローカルアカウントでログオンする
    ・Administrator（ビルトインアカウント）
    ・一般ユーザー アカウント（クライアントマシン上のローカルアカウント）
  - ユーザーアカウント制御（UAC）を無効に設定した状態で，クライアントにローカルアカウントでログオンする
- 認証方式が次のどちらかである
  - ローカル認証
  - Active Directory 認証かつ，ユーザーマッピングを使用しない

11.3 Windows 10，Windows Server 2016，または Windows Server 2019 の場合

CIFS クライアントが Windows 10，Windows Server 2016，または Windows Server 2019 の場合の注意事項を次に示します。

11.3.1 共有内のファイル・フォルダ

クライアントから共有ディレクトリ内に作成するファイル・フォルダに関しての注意事項を次に説明します。

11.3.1.1 ACL を追加する場合

HVFP の共有上のファイル・ディレクトリに ACL を追加しようとする際に次の条件が重なると，ローカルユーザー／グループを参照できなくて，ACL を追加できません。

- クライアントにログオンする方法が次のどちらかである
  - ユーザーアカウント制御（UAC）を有効に設定した状態で，次のどちらかのローカルアカウントでログオンする
    - Administrator（ビルトインアカウント）
    - 一般ユーザーアカウント（クライアントマシン上のローカルアカウント）
  - ユーザーアカウント制御（UAC）を無効に設定した状態で，クライアントにローカルアカウントでログオンする
- 認証方式が次のどちらかである
  - ローカル認証
  - Active Directory 認証かつ，ユーザーマッピングを使用しない

11.3.1.2 Quota を使用する場合

クライアントがエクスプローラを使用して共有にファイルを移動または貼り付ける際に，ブロック使用量または inode 数が HVFP で設定したソフトリミットを超過すると，ハードリミットを超過していない状態でも，クライアントの操作に失敗します。なお，COPY コマンドや XCOPY コマンドを使用すると，ハードリミットを超過していない状態であれば，共有にファイルを移動または貼り付けることができます。

11.3.1.3 オフラインファイルを有効にする場合

クライアント側でオフラインファイルを有効にした共有に Microsoft Office のファイルを作成した際に，ファイルが正しく保存されないことがあります。そのため，Microsoft Office を使用する場合には，共有のオフラインファイルを無効にしてください。

11.3.2 MMC を使用する場合

MMC を使用して CIFS 共有を管理する場合の注意事項を次に説明します。

11.3.2.1 Windows へのログオン

次のどれかの方法で Windows にログオンしてください。それ以外の場合には，HVFP へのアクセスが拒否されます。

- ドメインアカウントを使用してログオンする
- Administrator アカウントを使用してログオンする
- クライアントのユーザーアカウント制御（UAC）を無効に設定した状態で，Administrator 以外の管理者アカウントでログオンする

11.3.2.2 共有レベル ACL

共有レベル ACL にエントリーを追加しようとする際に，次の条件が重なると，ローカルユーザー／グループを参照できないため，共有レベル ACL の追加ができません。

- クライアントにログオンする方法が次のどちらかである
  - ユーザーアカウント制御（UAC）を有効に設定した状態で，次のどちらかのローカルアカウントでログオンする
    - Administrator（ビルトインアカウント）
    - 一般ユーザー アカウント（クライアントマシン上のローカルアカウント）
  - ユーザーアカウント制御（UAC）を無効に設定した状態で，クライアントにローカルアカウントでログオンする
- 認証方式が次のどちらかである
  - ローカル認証

- Active Directory 認証かつ，ユーザーマッピングを使用しない

11.3.3 アクセスしているときの注意事項

クライアントが CIFS サービスにアクセスしているときにフェールオーバーやフェールバックが発生すると，フェールオーバーやフェールバック後の最初の CIFS アクセスがエラーになることがあります。この場合は，アクセスし直してください。

11.3.4 SMB1.0 で接続する場合

デフォルトでは CIFS 接続時に SMB 署名が必要です。HVFP で SMB 1.0 を使用するように設定している場合，デフォルトでは SMB 署名を使用しない設定であるため，CIFS アクセスがエラーとなります。この場合，次のどちらかの設定を変更してください。

CIFS クライアントの設定

CIFS クライアントで，SMB 署名を使用した CIFS アクセスの設定を変更します。クライアント上で，「ローカルセキュリティポリシー」から 「セキュリティの設定」－「ローカルポリシー」－「セキュリティオプション」の「Microsoft ネットワーク クライアント：常に通信にデジタル署名を行う」の設定を確認し，有効である場合は，無効にしてください。

HVFP の設定（CIFS クライアントの設定を変更できない場合）

cifsoptset コマンドを実行して， HVFP へのすべての CIFS アクセスに対して SMB 1.0 の通信で SMB 署名を使用するようにしてください。 SMB 署名を使用するように設定する方法については，「コマンドリファレンス」を参照してください

11.4 Windows Server 2012 の場合

CIFS クライアントが Windows Server 2012 の場合の注意事項を次に示します。

11.4.1 共有内のファイル・フォルダ

クライアントから共有ディレクトリ内に作成するファイル・フォルダに関しての注意事項を次に説明します。

11.4.1.1 ACL を追加する場合

HVFP の共有上のファイル・ディレクトリに ACL を追加しようとする際に次の条件が重なると，ローカルユーザー／グループを参照できなくて，ACL を追加できません。

- クライアントにログオンする方法が次のどちらかである
  - ユーザーアカウント制御（UAC）を有効に設定した状態で，次のどちらかのローカルアカウントでログオンする
    - Administrator（ビルトインアカウント）
    - 一般ユーザーアカウント（クライアントマシン上のローカルアカウント）
  - ユーザーアカウント制御（UAC）を無効に設定した状態で，クライアントにローカルアカウントでログオンする
- 認証方式が次のどちらかである
  - ローカル認証
  - Active Directory 認証かつ，ユーザーマッピングを使用しない

11.4.1.2 Quota を使用する場合

クライアントがエクスプローラを使用して共有にファイルを移動または貼り付ける際に，ブロック使用量または inode 数が HVFP で設定したソフトリミットを超過すると，ハードリミットを超過していない状態でも，クライアントの操作に失敗します。なお，COPY コマンドや XCOPY コマンドを使用すると，ハードリミットを超過していない状態であれば，共有にファイルを移動または貼り付けることができます。

11.4.2 MMC を使用する場合

Windows Server 2012 から MMC を使用して CIFS 共有を管理する場合の注意事項を次に説明します。

11.4.2.1 Windows へのログオン

次のどれかの方法で Windows にログオンしてください。それ以外の場合には，HVFP へのアクセスが拒否されます。

- ドメインアカウントを使用してログオンする
- Administrator アカウントを使用してログオンする
- クライアントのユーザーアカウント制御（UAC）を無効に設定した状態で，Administrator 以外の管理者アカウントでログオンする

11.4.2.2 共有レベル ACL

共有レベル ACL にエントリーを追加しようとする際に，次の条件が重なると，ローカルユーザー／グループを参照できないため，共有レベル ACL の追加ができません。

- クライアントにログオンする方法が次のどちらかである
  - ユーザーアカウント制御（UAC）を有効に設定した状態で，次のどちらかのローカルアカウントでログオンする
    - Administrator（ビルトインアカウント）
    - 一般ユーザー アカウント（クライアントマシン上のローカルアカウント）
  - ユーザーアカウント制御（UAC）を無効に設定した状態で，クライアントにローカルアカウントでログオンする
- 認証方式が次のどちらかである
  - ローカル認証
  - Active Directory 認証かつ，ユーザーマッピングを使用しない

11.4.3 アクセスしているときの注意事項

クライアントが CIFS サービスにアクセスしているときにフェールオーバーやフェールバックが発生すると，フェールオーバーやフェールバック後の最初の CIFS アクセスがエラーになることがあります。この場合は，アクセスし直してください。

11.5 Mac OS X の場合

CIFS クライアントが Mac OS X の場合の注意事項を次に示します。

11.5.1 サポート範囲について

CIFS クライアントが Mac OS X の場合，次に示すことはできません。

- MMC 連携
- Volume Shadow Copy Service を使用した差分スナップショットの公開
- 分散ファイルシステム（DFS：Distributed File System）
- CIFS 共有の更新データのクライアント側でのキャッシュ

11.5.2 ファイル名・ディレクトリ名について

ファイル名・ディレクトリ名に指定できる文字の種類とパス名の長さは，Windows で使用できる範囲に限ってサポートします。このため，ファイル名・ディレクトリ名として，次に示す文字やパス名は使用しないでください。

- ファイル名末尾のスペース
- ファイル名およびディレクトリ名の引用符（"），アステリスク（*），斜線（/），コロン（:），始め山括弧（<），終わり山括弧（>），疑問符（?），円記号（¥）および縦線（|）
- 256 文字以上のファイルのパス名
- 260 文字以上のディレクトリのパス名
- アプリケーションが制限している文字数を超えるパス名
  例：Excel 2004 の半角 219 文字以上のファイルのパス名

11.5.3 操作上の注意

CIFS クライアントが Mac OS X の場合の，操作上の注意を次に示します。

また，このほかの注意事項として，Mac OS X v10.9 の場合は「11.5.3.1 Mac OS X v10.9 の場合」，Mac OS X v10.10，v10.11，または macOS v10.12 の場合は「11.5.3.2 Mac OS X v10.10，v10.11，または macOS v10.12 の場合」を参照してください。

- クライアントが共有にファイルをドロップまたはペーストする際に，ブロック使用量または inode 数が HVFP で設定したソフトリミットを超過すると，ハードリミットを超過していない状態でも，クライアントの操作に失敗します。
- CIFS 共有にアクセスおよびファイルの操作をした場合，隠しファイルが作成されることがあります。この隠しファイルもファイルシステムのユーザー領域を使用し，ブロック使用量および inode 使用量が増加します。このため，HVFP でのファイルシステムの容量や Quota の設定では，隠しファイル分も考慮してください。
- マルチバイト文字のユーザーアカウントでアクセスすると，最上位の共有名が，Finder に文字コードで表示されることがあります。
- クライアントで使用するアプリケーションによっては，CIFS 共有のファイルを更新した場合，ファイルの ACL が新規作成時の設定に戻ることがあります。これを回避するには，ファイル単位の ACL でアクセス制御するのではなく，上位のディレクトリに ACL を設定するなどしてアクセス制御してください。
- クライアントで使用するアプリケーションによっては，CIFS 共有のファイルを更新した場合，ファイルの所有者がファイルを操作したユーザーに変更されることがあります。このため，所有者に依存したアクセス制御とならないよう，上位のディレクトリに ACL を設定するなどしてアクセス制御してください。
  なお，Classic ACL タイプのファイルシステムの場合は，ファイルの操作者および操作者が所属するグループに対して ACL を設定してください。

- ファイルまたはフォルダに 128 件以上の ACL が設定されていても，表示できるのは 128 件までです。また，128 件を超える ACL を設定する操作は失敗します。このような場合も，ファイルまたはフォルダに設定済みの ACL によるアクセス制御は有効です。
- ACL を操作するには，HVFP のノードまたは Virtual Server，および Mac OS X の CIFS クライアントを Active Directory ドメインに参加させ，ドメインのユーザーアカウントで CIFS クライアントにログインする必要があります。
- UNIX をベースとする Mac OS X から CIFS 共有を操作する場合，CIFS サービスの UNIX クライアント向け専用の拡張機能を利用するかどうかで，ACL 操作などでクライアントからの CIFS 共有に対するリクエストの処理方法に次の違いがあります。

  CIFS サービスの UNIX クライアント向け専用の拡張機能を利用する場合

  CIFS クライアントからのリクエストは UNIX クライアント向け専用の拡張機能を利用して処理されるため，POSIX ACL に準拠した ACL を設定できる Classic ACL タイプのファイルシステムに適しています。NTFS ACL に準拠した ACL を設定できる Advanced ACL タイプのファイルシステムの場合は，UNIX クライアント向け専用の拡張機能で処理しきれないリクエストがあるため，これらのリクエストはクライアント側で Windows クライアントからのようなリクエストに切り替えられます。

  CIFS サービスの UNIX クライアント向け専用の拡張機能を利用しない場合

  ファイルシステムが Classic ACL タイプか Advanced ACL タイプかに関係なく，リクエストはクライアント側で Windows クライアントからのようなリクエストに切り替えられます。

  CIFS サービスの UNIX クライアント向け専用の拡張機能を利用するかどうかは `cifsoptset` コマンドで設定し，`cifsoptlist` コマンドで確認できます。
- Mac OS X v10.7 以降の書類の「バージョン」機能は利用できません。
  書類を操作した際に「書類 " *ファイル名* " があるボリュームは，バージョン履歴の保存には対応していません。」と表示されることがありますが，無視してください。
- ローカル認証でユーザーマッピングを使用しない場合に，ユーザーおよびグループ ACL を追加したいときは，`dirsetacl` コマンドで設定してください。なお，ファイルに対して ACL を追加したい場合は，`dirsetacl` コマンドで対象のファイルに ACE が継承されるように，該当するディレクトリに対して ACE の継承範囲を設定してください。
- Mac OS X ではファイルへの書き込み権限を持っていても，Mac OS X 上のアプリケーションの動作によって，ファイルの書き込みが失敗することがあります。
  そのため，Mac OS X でファイルの更新を伴う作業を実施する際には，次のとおり設定しておくことを奨励します。
  a. CIFS 共有直下の .TemporaryItems フォルダ，そのフォルダ内のすべてのファイルおよびフォルダに対して，操作するユーザまたはそのユーザが属するグループにフルコントロールの権限を与えてください。
  b. 操作対象のファイルに「削除」権限を設定するか，その親フォルダに「サブフォルダとファイルの削除」権限を設定してください。
  c. 操作するユーザおよびそのユーザが所属するグループの両方にアクセス権を設定して，上位のフォルダからそのアクセス権が継承されるようにしてください。

11.5.3.1 Mac OS X v10.9 の場合

Mac OS X v10.9 クライアントから SMB2.0，SMB2.1 および SMB3.0 を使用した CIFS アクセスはできません。SMB1.0 を使用して CIFS アクセスするように，HVFP または Mac OS X v10.9 クライアントで設定を変更する必要があります。

HVFP で設定を変更する場合

[CIFS Service Management] ページ (Setting Type：Basic）で，CIFS クライアントからのアクセスに対して SMB1.0 を使用するように設定します。設定方法については「ユーザーズガイド」を参照してください。

Mac OS X v10.9 クライアントで設定を変更する場合

次のどちらかの方法で設定を変更します。

- Finder の [サーバへ接続] で [smb://」ではなく「cifs://」を使用して接続します。

- ～ /Library/Preferences/nsmb.conf ファイルに次の記述を追加したあと，Finder の [サーバへ接続] で「smb://」を使用して接続します。

```
[default]
smb_neg=smb1_only
```

11.5.3.2 Mac OS X v10.10，v10.11，または macOS v10.12 の場合

Mac OS X v10.10，v10.11，または macOS v10.12 の場合は次の注意事項も確認してください。

- Mac OS X v10.10，v10.11，および macOS v10.12 クライアントから CIFS アクセスする場合は，SMB2.0 だけをサポートしているため，HVFP で設定を変更する必要があります。
  [CIFS Service Management] ページ（Setting Type：Basic）で，CIFS クライアントからのアクセスに対して SMB2.0 を使用するように設定します。設定方法については，「ユーザーズガイド」（IF305）を参照してください。
  なお，Mac OS X v10.10，v10.11，および macOS v10.12 のクライアント上では，SMB2.x などのマイナーバージョン（x 部分）を指定できません。
- Mac OS X v10.9 以前のバージョンでは，SMB1.0 の CIFS アクセスだけをサポートしています。そのため，Mac OS X v10.9 以前のバージョンと，v10.10，v10.11，または mac OS v10.12 のバージョンを共存させる場合に，v10.9 以前のバージョンの CIFS クライアントは，各クライアント上の SMB のバージョンを 1.0 に制限するよう設定を変更する必要があります。設定を変更する方法については，「(1)Mac OS X v10.9 の場合」を参照してください。
  また，Mac OS X v10.9 以前のバージョンから，v10.10，v10.11，または macOS v10.12 にアップグレードした場合は，[CIFS Service Management] ページ（Setting Type：Basic）で CIFS クライアントからのアクセスに対して SMB2.0 を使用するように設定したあと，各クライアント上の SMB のバージョンを 1.0 に制限する設定を解除してください。
- Mac OS X v10.11 で，CIFS 共有名に半濁点または濁点文字を使用した場合は，Mac クライアント上の問題により，Mac クライアントから CIFS 接続ができなくなります。共有名への半濁点または濁点の使用は避けてください。

12

Virtual Server 運用上の注意事項

この章では，Virtual Server を使用する場合の CIFS 共有に関する注意事項を説明します。

12.1 CIFS 共有への接続数と CIFS 共有数の上限

CIFS サービスに接続できる Virtual Server 当たりの CIFS クライアントの数（最大接続数）および CIFS 共有数の上限値を次に示します。

表 12-1： CIFS サービスに接続できる Virtual Server 当たりの CIFS クライアントの最大接続数および CIFS 共有数の上限値

モデル	ノードのメモリー量	Virtual Server に割り当てたメモリー量（GB 単位）	自動リロード	CIFS クライアントの最大接続数	CIFS 共有数の上限
Nh4b/ Nh4c	32GB	2 ～ 3 未満	×	500	7,500
			○	300	256
		3 ～ 16 未満	×	392× 割り当てたメモリー量* － 284	7,500
			○	121× 割り当てたメモリー量* ＋ 58	256
		16 ～ 26	×	375× 割り当てたメモリー量*	7,500
			○	175× 割り当てたメモリー量* － 800	256
	64GB	2 ～ 3 未満	×	500	7,500
			○	300	256
		3 ～ 16 未満	×	392× 割り当てたメモリー量* － 284	7,500
			○	121× 割り当てたメモリー量* ＋ 58	256
		16 ～ 33 未満	×	1,125× 割り当てたメモリー量* － 12,000	7,500
			○	475× 割り当てたメモリー量* － 5,600	256
		33 ～ 56	×	24,000	7,500
			○	9,600	256

モデル	ノードのメモリー量	Virtual Server に割り当てたメモリー量（GB 単位）	自動リロード	CIFS クライアントの最大接続数	CIFS 共有数の上限
Nh8b/ Nh8c	64GB	2 ～ 3 未満	×	500	7,500
			○	300	256
		3 ～ 16 未満	×	392× 割り当てたメモリー量* － 284	7,500
			○	121× 割り当てたメモリー量* ＋ 58	256
		16 ～ 33 未満	×	1,125× 割り当てたメモリー量* － 12,000	7,500
			○	475× 割り当てたメモリー量* － 5,600	256
		33 ～ 56	×	24,000	7,500
			○	9,600	256
	96GB	2 ～ 3 未満	×	500	7,500
			○	300	256
		3 ～ 16 未満	×	392× 割り当てたメモリー量* － 284	7,500
			○	121× 割り当てたメモリー量* ＋ 58	256
		16 ～ 33 未満	×	1,125× 割り当てたメモリー量* － 12,000	7,500
			○	475× 割り当てたメモリー量* － 5,600	256
		33 ～ 85	×	24,000	7,500
			○	9,600	256

（凡例）○：自動リロードする　×：自動リロードしない

測定条件

CIFS クライアントの最大接続数の測定条件は次のとおりです。

- 上限値まで CIFS 共有が作成されている。
- 各クライアントが次の条件でファイルを操作している。
  －各クライアントからのファイル操作が 1 回 / 分である。
  －各クライアントが操作するファイルが 1 ファイル / セッションである。
- 各クライアントからのファイル操作と同時に，ほかの処理が実行されていない。

注 *

端数を切り捨てた GB 単位の整数値

13

NFS サービスの概要

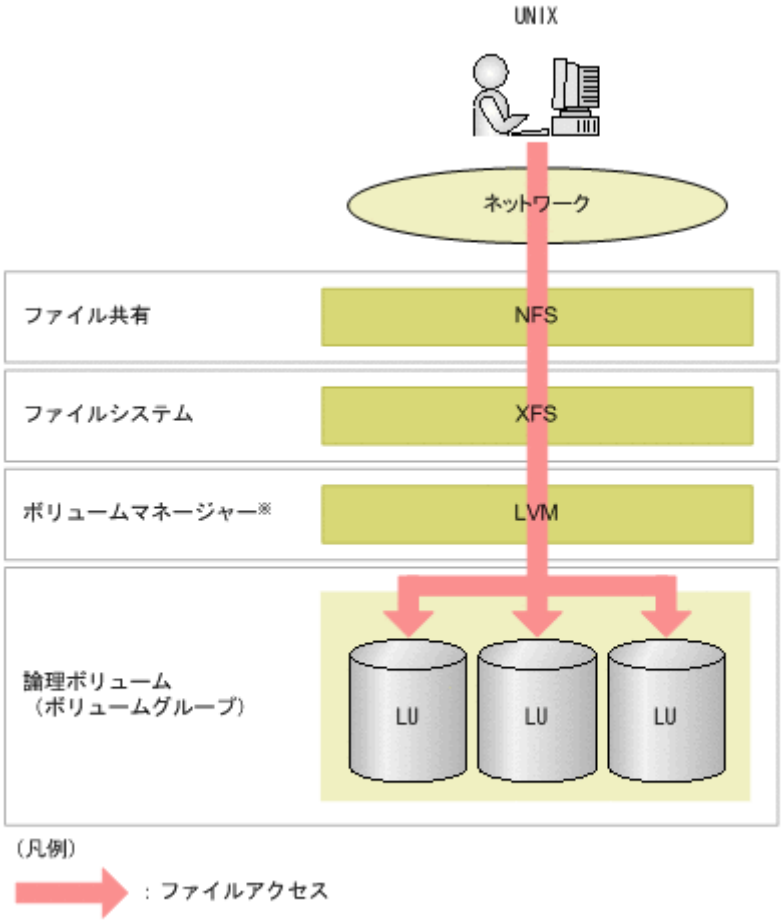
NFS クライアントは HVFP の NFS サービスを利用してデータにアクセスできます。この章では，NFS サービス利用の概要について説明します。

13.1 NFS サービス利用の概要

システム管理者がファイルシステムやディレクトリに NFS 共有を作成することで，NFS クライアントはネットワークを介してストレージシステム内のデータにアクセスできます。

NFS クライアントがファイルシステム内のデータにアクセスする流れを次の図に示します。

図 13-1： NFS クライアントがファイルシステム内のデータにアクセスする流れ



注※ LUを一つだけ利用する場合は，論理ボリュームを構成しないでファイルシステムを構築できます。このとき，ボリュームマネージャーは利用しません。

HVFP で提供するファイルシステムでは，NFSv2，NFSv3 または NFSv4 プロトコルを利用できます。NFS プロトコルの各バージョンの利用可否は，NFS サービスの構成定義で指定できます。NFS サービスの構成定義の参照または変更については，「ユーザーズガイド」（IF305）を参照してください。

NFS クライアントは，マウント時に設定されたバージョンの NFS プロトコルでファイルシステムにアクセスします。

また，HVFP では，NFS クライアントを UNIX（AUTH_SYS）または Kerberos 認証方式でユーザー認証できます。NFS クライアントのユーザー認証については，「17. NFS クライアントのユーザー認証」を参照してください。

NFSv4 プロトコルを利用する場合には，NFS クライアントに前提パッチの適用が必要となるなど，運用に当たっての制約があります。

NFSv4 プロトコルで提供されている機能を使用しない場合には，安定稼働のため，NFSv2 または NFSv3 プロトコルを利用する運用を推奨します。

14

NFS サービス利用時のシステムの構成

この章では，HVFP の NFS サービスを利用するための動作環境とネットワーク構成について説明します。

14.1 NFS サービスでサポートする製品

NFS サービスでサポートする製品を次に示します。

- 最新のサポート対象製品情報は，NEC サポートポータルの以下のページに掲載のサポートマトリクスを参照してください。
  「お知らせ／技術情報」－「技術情報」－「【iStorage M シリーズ】【NAS オプション】接続サポートマトリクス」　　コンテンツ ID：3140101655
- 製造元のサポートが停止している OS については，NAS オプションにおけるサポートを停止しています。

14.1.1 NFS クライアント

NFS クライアントとしてサポートする製品を次に示します。

最新のサポート対象製品情報は，NEC サポートポータルの以下のページに掲載のサポートマトリクスを参照してください。

「お知らせ／技術情報」－「技術情報」－「【iStorage M シリーズ】【NAS オプション】接続サポートマトリクス」　　コンテンツ ID：3140101655

14.1.2 KDC サーバ

Kerberos 認証を利用してユーザーを認証する場合は，KDC サーバとして，UNIX マシンまたは Active Directory ドメインコントローラーが必要です。

UNIX マシン

KDC サーバとして UNIX マシンを利用する場合にサポートする製品を次に示します。

- HP-UX 11i v3
- Red Hat Enterprise Linux Advanced Platform v5.2
- Solaris 10 オペレーティングシステム（SunOS 5.10）SPARC プラットフォーム版

Active Directory ドメインコントローラー

KDC サーバとして Active Directory ドメインコントローラーを利用する場合にサポートする製品を次に示します。

- Microsoft(R) Windows Server(R) 2019 Datacenter
- Microsoft(R) Windows Server(R) 2019 Standard

14.1.3 ID マッピング用サーバ

NFSv4 ドメイン構成で運用する場合，NFS クライアントのユーザー名，グループ名を UID，GID に変換する（ID マッピングを行う）ための外部サーバを使用するときには，ID マッピング用の外部サーバとしてユーザー認証用の LDAP サーバまたは NIS サーバが必要です。

ユーザー認証用の LDAP サーバ

ID マッピング用サーバとしてユーザー認証用の LDAP サーバを利用する場合にサポートする製品を次に示します。

- OpenLDAP 2.2.23

NIS サーバ

HVFP では，UNIX マシンを NIS サーバとして利用できます。

NIS サーバとして利用する UNIX マシンについては，NIS 機能を持った製品がインストールされたマシンであれば，製品のバージョンに制限はありません。

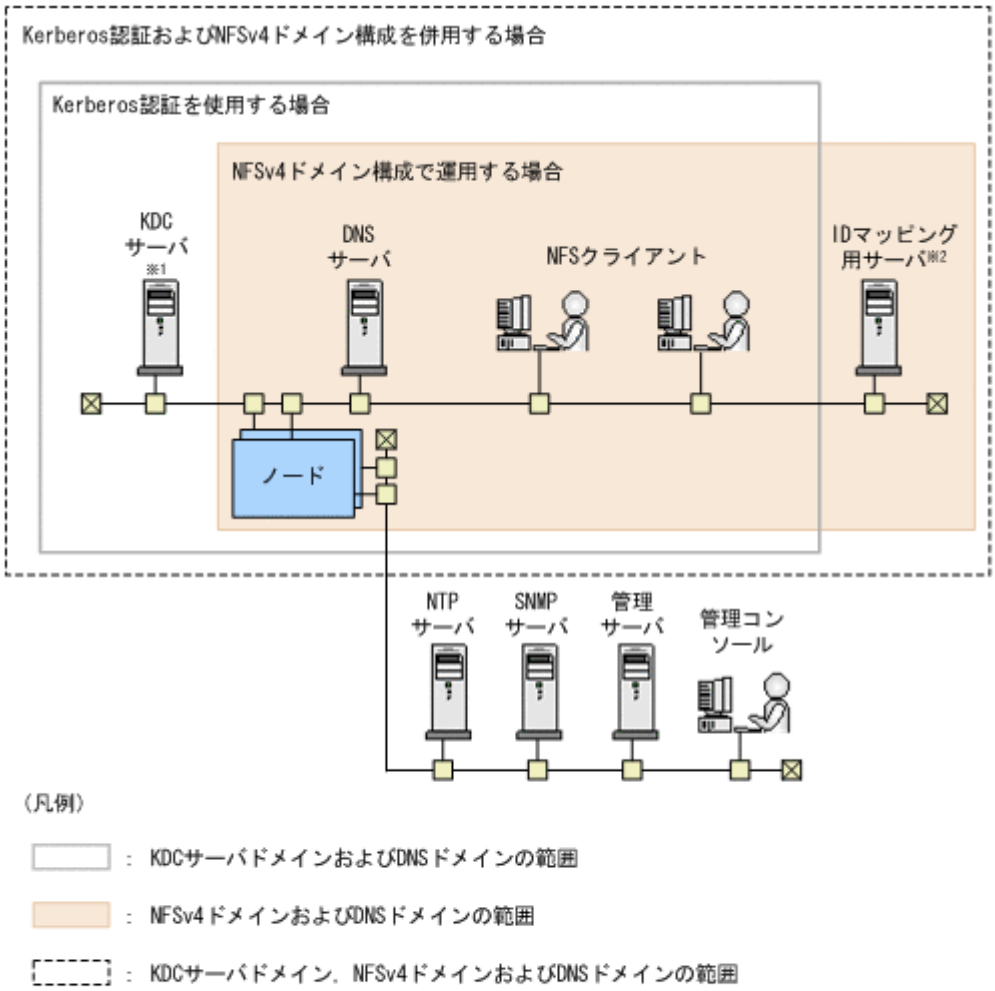
14.2 ネットワークの構成

ここでは，NFS 運用時のネットワークの構成について，NFS サービスだけを運用する場合と，CIFS サービスと NFS サービスを同時に運用する場合に分けて説明します。

14.2.1 NFS サービスを運用する場合のネットワークの構成

NFS サービスだけを運用する場合のネットワークの構成例を次の図に示します。

図 14-1： NFS サービスを運用する場合のネットワーク構成例



注※1　UNIXマシンまたはActive Directoryドメインコントローラーを KDCサーバとして利用できます。

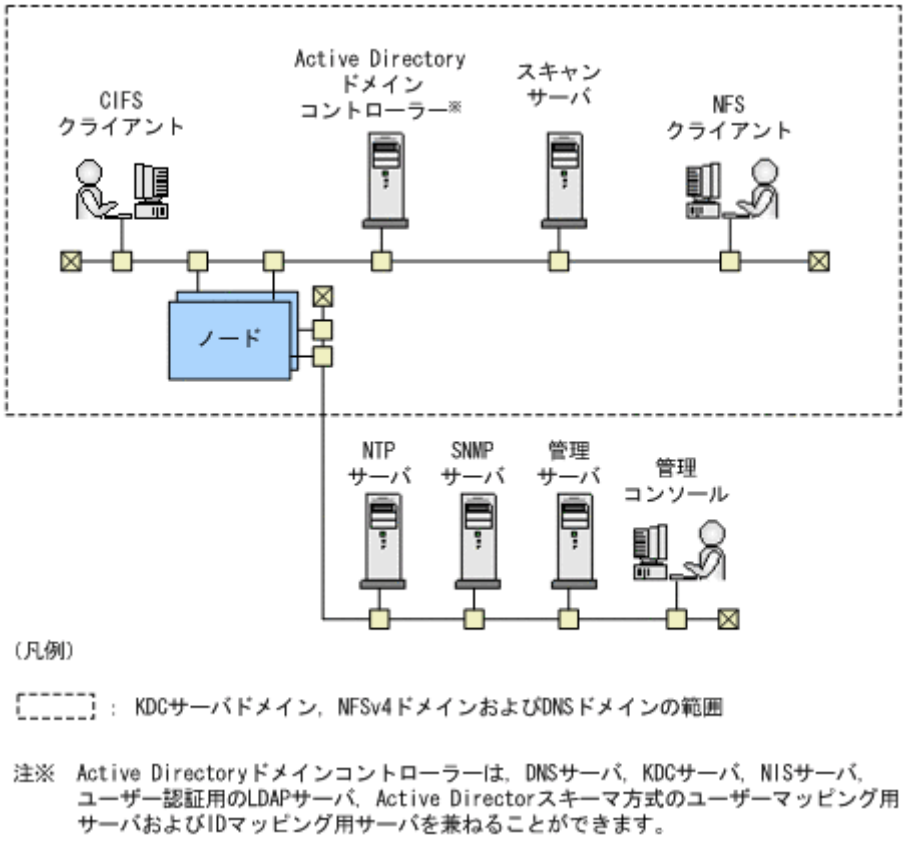
注※2　IDマッピング用サーバとして，ユーザー認証用のLDAPサーバ，NISサーバまたはActive Directoryドメインコントローラーを利用できます。

KDC サーバドメインや NFSv4 ドメインは，HVFP のノードまたは Virtual Server ごとに 1 つずつ設定できます。Kerberos 認証と NFSv4 ドメイン構成を併用して HVFP を運用する場合は，KDC サーバドメイン，NFSv4 ドメインおよび NFS クライアントが属する DNS ドメインの範囲がすべて一致している必要があります。

14.2.2 CIFS および NFS サービスを同時に運用する場合のネットワークの構成

CIFS および NFS サービスを同時に運用する場合に，NFS サービスで Kerberos 認証を利用する際は，CIFS および NFS サービスで KDC サーバを共有するために Active Directory ドメインコントローラーを使用する必要があります。また，NFS サービスで NFSv4 ドメイン構成を利用する際に，CIFS サービスでも Active Directory スキーマ方式のユーザーマッピングを利用することで，ID マッピング用サーバやユーザー認証用の LDAP サーバを Active Directory ドメインコントローラーに集約できます。CIFS および NFS サービスを同時に運用する場合に外部サーバを共有するときのネットワークの構成例を次の図に示します。

図 14-2： CIFS および NFS サービスを同時に運用する場合に外部サーバを共有するときのネットワークの構成例



CIFS および NFS サービスを同時に運用する場合で，Kerberos 認証と NFSv4 ドメイン構成を併用するときは，Active Directory のドメイン，KDC サーバドメインおよび NFSv4 ドメインの範囲がすべて一致している必要があります。

14.3 Kerberos 認証および NFSv4 ドメイン構成を利用するときの NFS 環境の構築

Kerberos 認証および NFSv4 ドメイン構成を利用して，NFS サービスだけを運用する場合，または CIFS および NFS サービスを同時に運用する場合の NFS 環境の構築について説明します。

Kerberos 認証を利用する際に必要となる KDC サーバは，HVFP の運用に応じて使用できるマシンが異なります。

NFS サービスだけを運用している場合は，UNIX マシンまたは Active Directory をインストールしたドメインコントローラーのどちらかを KDC サーバとして使用できます。CIFS および NFS サービスを同時に運用している場合は，Active Directory をインストールしたドメインコントローラーを使用する必要があります。

この節では，HVFP の運用に応じた NFS 環境の構築手順を説明します。なお，構築手順を説明する際には，Kerberos 認証に関する次の用語を使用します。

KDC サーバドメイン

KDC サーバと，KDC サーバで認証されるユーザー，および認証情報を利用するサーバから成る集合のことです。KDC サーバドメインのことをレルムとも呼びます。Active Directory ドメインコントローラーを KDC サーバとして利用する場合には，CIFS クライアントおよび NFS クライアントを KDC サーバで認証します。

プリンシパル

KDC サーバで認証されるユーザーを識別するための名称です。プリンシパルの形式は，＜ユーザー名＞@＜KDC サーバドメイン名＞です。

キータブファイル

KDC サーバで認証されるホスト情報が格納されているファイルです。KDC サーバで作成したキータブファイルは，HVFP のノードまたは Virtual Server，および各 NFS クライアントマシンへ転送します。
NFS サービスのプリンシパルおよび NFS クライアントの各ユーザーに対するプリンシパルを作成して，事前にキータブファイルに登録しておく必要があります。

14.3.1 NFS サービスだけを運用する場合の NFS 環境の構築

ここでは，NFS サービスだけを運用する場合の NFS 環境構築の流れを説明します。

1. KDC サーバの構築とキータブファイルの作成
   Kerberos 認証のために KDC サーバを構築します。また，Kerberos 認証で必要となるキータブファイルを KDC サーバで作成します。
2. キータブファイルの転送と組み込み
   手順 1 で作成したキータブファイルを，HVFP のノードまたは Virtual Server，および各クライアントマシンへ転送します。
   転送されたキータブファイルの内容を HVFP のノードまたは Virtual Server で管理するキータブファイルにマージします。また，それぞれのクライアントマシンで，転送されたキータブファイルを組み込みます。
3. HVFP のノードまたは Virtual Server でのサービスの構成定義と NFS 共有の作成
   ［Access Protocol Configuration］ダイアログで，Kerberos 認証のための設定および NFSv4 ドメインの設定を行います。また，［ファイルシステム構築と共有作成］または［共有追加］ダイアログで NFS 共有を作成します。
4. NFS クライアントのマシンでのマウント
   NFS 共有が設定されているファイルシステムまたはディレクトリをマウントし，NFS 共有にアクセスできるようにします。

キータブファイルの作成方法，および NFS クライアントのマシンでキータブファイルを組み込む方法の詳細については，使用するそれぞれの製品のドキュメントを参照してください。

次に，この手順を詳しく説明します。なお，ID マッピング用サーバはすでに設定されていることを想定しています。

14.3.1.1 KDC サーバの構築とキータブファイルの作成

KDC サーバを構築し，キータブファイルを作成する手順を示します。

1. UNIX マシンまたは Active Directory ドメインコントローラーで KDC サーバを構築します。
2. KDC サーバでキータブファイルを作成します。
   この操作にはプラットフォームのコマンドを使用します。まず，root ユーザーに対する初期チケットを取得し，次に必要なプリンシパルの作成を行ったあと，適当なファイル名（例えば，/tmp/nfs.keytab）でキータブファイルを作成します。

14.3.1.2 キータブファイルの転送と組み込み

HVFP のノードまたは Virtual Server および各クライアントマシンへキータブファイルを転送し，組み込む手順を示します。

1. キータブファイルを作成した UNIX マシンまたは Active Directory ドメインコントローラーから，HVFP の SSH 用アカウントのホームディレクトリ（/home/nasroot）へキータブファイルを転送します。
   キータブファイルを UNIX マシンから転送する場合には，scp コマンドを使用してください。Active Directory ドメインコントローラーから転送する場合には，安全に複写できるソフトウェアを利用してください。
2. HVFP のノードまたは Virtual Server で nfskeytabadd コマンドを実行して，転送されたキータブファイルをマージします。
   転送したキータブファイルの内容が，HVFP のノードまたは Virtual Server で管理するキータブファイルにマージされます。
3. nfskeytablist コマンドを実行して，マージされたキータブファイルを確認します。
4. キータブファイルを作成した UNIX マシンまたは Active Directory ドメインコントローラーから，各クライアントマシンの適当なディレクトリ（例えば，/tmp）へキータブファイルを転送します。
   キータブファイルを UNIX マシンから転送する場合には，scp コマンドを使用してください。Active Directory ドメインコントローラーから転送する場合には，安全に複写できるソフトウェアを利用してください。
5. 各クライアントマシンで，転送されたキータブファイルをマシンに組み込みます。

14.3.1.3 HVFP のノードまたは Virtual Server でのサービスの構成定義と NFS 共有の作成

HVFP のノードまたは Virtual Server で行う作業の手順を示します。

1. ［Access Protocol Configuration］ダイアログの［NFS Service Management］ページで，Kerberos 認証のための設定，NFSv4 ドメインの設定などの情報を指定します。
   次の情報を指定します。
   - NFS サービスで使用できる NFS プロトコルのバージョン
   - セキュリティフレーバー
   - NFSv4 ドメインのドメイン名
   - KDC サーバ名および KDC サーバドメイン名
     サーバ名は，半角英数字，ハイフン (-) またはアンダーライン (_) で構成された英字から始まるサーバ名か IP アドレスを指定してください。Active Directory ドメインコントローラーを KDC サーバとして使う場合には，Active Directory ドメインコントローラーの名称を指定してください。
2. NFS サービスを再起動します。

3. ［ファイルシステム構築と共有作成］または［共有追加］ダイアログで，NFS 共有の作成と Kerberos 認証のための設定を行います。
［アクセス制御］タブの［NFS］サブタブで設定するセキュリティフレーバーについては，NFS サービスの構成定義で指定した内容をそのまま使用することも，作成する NFS 共有で独自に設定することもできます。

14.3.1.4 NFS クライアントのマシンでのマウント

NFS クライアントで mount コマンドを実行して，クライアントのマシンから NFS 共有にアクセスできるようにします。

mount コマンドでは，次のオプションを指定します。

- アクセスに使用する NFS プロトコルのバージョン（クライアントが Solaris の場合，デフォルトで NFSv4 が使用されます）
- セキュリティフレーバー（sys，krb5，krb5i または krb5p）

オプションの指定方法の詳細については，クライアントのドキュメントを参照してください。

14.3.2 CIFS および NFS サービスを同時に運用する場合の NFS 環境の構築

ここでは，CIFS および NFS サービスを同時に運用する場合の NFS 環境構築の流れを説明します。なお，安全にキータブファイルの転送ができる複写用のソフトウェアを，Active Directory ドメインコントローラーに準備しておく必要があります。

1. キータブファイルの作成
Active Directory ドメインコントローラーで，キータブファイルを作成します。
2. キータブファイルの転送と組み込み
手順 1 で作成したキータブファイルを，HVFP のノードまたは Virtual Server，および各クライアントマシンへ転送します。
転送されたキータブファイルの内容を HVFP のノードまたは Virtual Server で管理するキータブファイルにマージします。また，それぞれのクライアントマシンで，転送されたキータブファイルを組み込みます。
3. HVFP のノードまたは Virtual Server でのサービスの構成定義と NFS 共有の作成
［Access Protocol Configuration］ダイアログで，Kerberos 認証のための設定および NFSv4 ドメインの設定を行います。また，［ファイルシステム構築と共有作成］または［共有追加］ダイアログで NFS 共有を作成します。
4. NFS クライアントのマシンでのマウント
NFS 共有が設定されているファイルシステムまたはディレクトリをマウントし，NFS 共有にアクセスできるようにします。

キータブファイルの作成方法，および NFS クライアントのマシンでキータブファイルを組み込む方法の詳細については，使用するそれぞれの製品のドキュメントを参照してください。

次に，この手順を詳しく説明します。なお，ID マッピング用サーバはすでに設定されていることを想定しています。

14.3.2.1 キータブファイルの作成

Active Directory ドメインコントローラーで，キータブファイルを作成します。

この操作では，まず，root ユーザーに対する初期チケットを取得し，次に必要なプリンシパルの作成を行ったあと，適当なファイル名（例えば，nfs.keytab）でキータブファイルを作成します。

14.3.2.2 キータブファイルの転送と組み込み

キータブファイルを作成した Active Directory ドメインコントローラーから，HVFP のノードまたは Virtual Server および各クライアントマシンへキータブファイルを転送し，組み込む作業の手順を示します。

1. キータブファイルを作成した Active Directory ドメインコントローラーで，安全に複写できるソフトウェアを利用して，HVFP の SSH 用アカウントのホームディレクトリ（/home/nasroot）へキータブファイルを転送します。
2. HVFP のノードまたは Virtual Server で nfskeytabadd コマンドを実行して，転送されたキータブファイルをマージします。
   転送されたキータブファイルが，HVFP のノードまたは Virtual Server で管理するキータブファイル（/etc/krb5.keytab）にマージされます。
3. nfskeytablist コマンドを実行して，マージされたキータブファイルを確認します。
4. キータブファイルを作成した Active Directory ドメインコントローラーで，安全に複写できるソフトウェアを利用して，各クライアントマシンの適当なディレクトリ（例えば，/tmp）へキータブファイルを転送します。
5. 各クライアントマシンで，転送されたキータブファイルをマシンに組み込みます。

14.3.2.3 HVFP のノードまたは Virtual Server でのサービスの構成定義と NFS 共有の作成

HVFP のノードまたは Virtual Server で行う作業の手順を示します。

1. ［Access Protocol Configuration］ダイアログの［NFS Service Management］ページで，Kerberos 認証のための設定，NFSv4 ドメインの設定などの情報を指定します。
   次の情報を指定します。
   - NFS サービスで使用できる NFS プロトコルのバージョン
   - セキュリティフレーバー
   - NFSv4 ドメインのドメイン名
   - KDC サーバ名および KDC サーバドメイン名
     KDC サーバ名には，Active Directory ドメインコントローラーの名称を指定してください。
2. NFS サービスを再起動します。
3. ［ファイルシステム構築と共有作成］または［共有追加］ダイアログで，NFS 共有の作成と Kerberos 認証のための設定を行います。
   ［アクセス制御］タブの［NFS］サブタブで設定するセキュリティフレーバーについては，NFS サービスの構成定義で指定した内容をそのまま使用することも，作成する NFS 共有で独自に設定することもできます。

14.3.2.4 NFS クライアントのマシンでのマウント

NFS クライアントで mount コマンドを実行して，クライアントのマシンから NFS 共有にアクセスできるようにします。

mount コマンドでは，次のオプションを指定します。

- アクセスに使用する NFS プロトコルのバージョン（クライアントが Solaris の場合，デフォルトで NFSv4 が使用されます）
- セキュリティフレーバー（sys，krb5，krb5i または krb5p）

オプションの指定方法の詳細については，クライアントのドキュメントを参照してください。

15

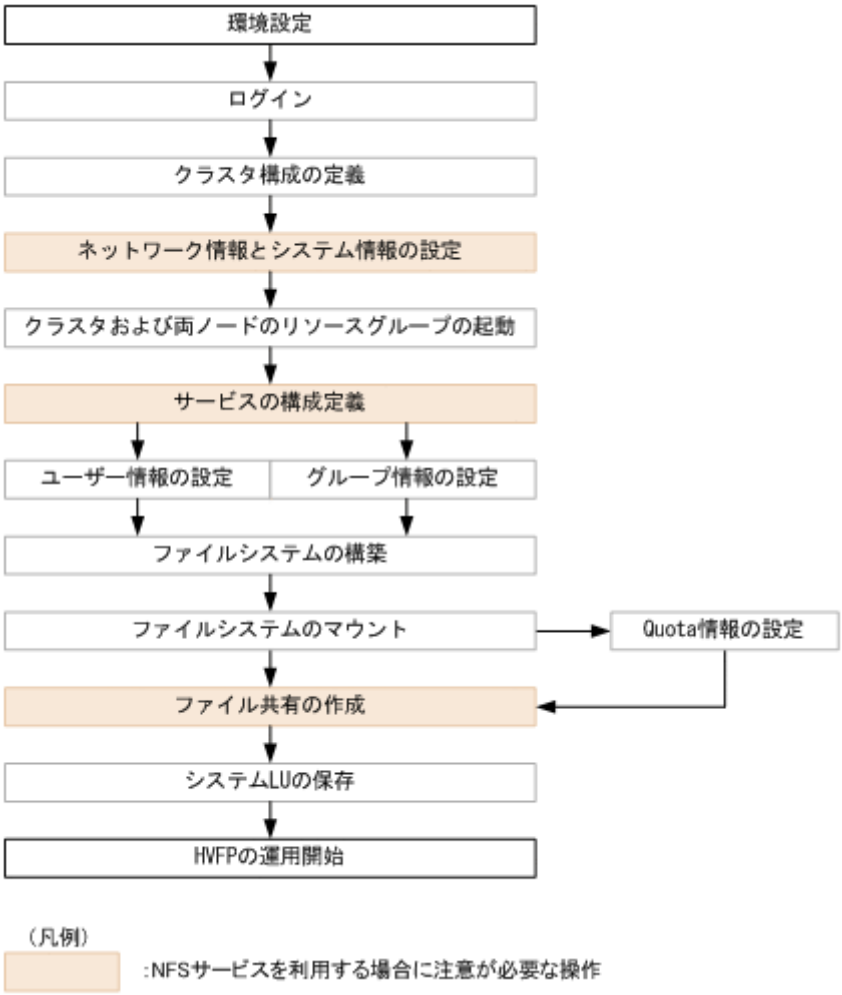
File Services Manager での NFS サービスの運用

この章では，HVFP を利用するためにシステム管理者が行う運用管理操作の中から，NFS サービスを利用する場合に注意が必要な操作について説明します。なお，ここでは，File Services Manager の GUI を使用することを前提とします。

15.1 File Services Manager での設定の流れ

システム管理者は，HVFP の運用を開始するために必要な情報を，File Services Manager で設定します。File Services Manager での設定手順を次の図に示します。図で示した操作のうち，このマニュアルでは，NFS サービスを利用する場合に注意が必要な操作について主に説明します。それ以外の操作については，「ユーザーズガイド」（IF305）を参照してください。

図 15-1： File Services Manager の設定手順



15.2 ネットワーク情報とシステム情報の設定

システム管理者は，［Network & System Configuration］ダイアログの［System Setup Menu］ページから，HVFP の各ノードまたは Virtual Server のインターフェース情報，ネットワーク情報および連携する外部サーバの情報などを設定できます。

NFS サービスを利用する場合は，次の設定を確認してください。

- NIS サーバの設定
  NFS 共有の公開先としてネットグループの指定ができる運用にする場合には，NIS サーバを設定する必要があります。
- ID マッピング用サーバの設定
  NFSv4 ドメイン構成で運用する場合，ID マッピング用サーバとしてユーザー認証用の LDAP サーバまたは NIS サーバを設定する必要があります。

- DNS サーバの設定
  HVFP のノードまたは Virtual Server のホスト名，NFS クライアントのホスト名に加えて，Kerberos 認証を利用する場合には，KDC サーバのホスト名を DNS サーバに登録することによって，一元的にホスト名の名前解決をすることができます。

［System Setup Menu］ページでの設定方法については，「ユーザーズガイド」（IF305）を参照してください。

15.2.1 システムファイルを直接編集する

システム管理者は，［Network & System Configuration］ダイアログの［Edit System File］ページで HVFP のシステムファイルを直接編集できます。システムファイルを直接編集する方法と設定内容については，「ユーザーズガイド」（IF305）を参照してください。

ここでは，NFS サービスを利用する場合に編集するシステムファイルと編集契機を次に示します。

/etc/hosts

NFS 共有の公開先ホストから NFS ファイルロックを使用する場合に編集します。

15.3 サービスの構成定義

システム管理者が管理できる NFS サービスの内容を次の表に示します。サービス管理の詳細については，「ユーザーズガイド」（IF305）を参照してください。

表 15-1： NFS サービスの管理内容

サービスの種類	サービス名	構成定義の変更	サービスのメンテナンス	起動・停止・再起動
NFS サービス	NFS	○	×	○

（凡例）○：できる　×：できない

システム管理者は，NFS サービスの構成定義で設定した，NFS サービスで利用できる NFS プロトコルのバージョン，セキュリティフレーバーなどについての設定内容をエンドユーザー（NFS クライアントのユーザー）に通知する必要があります。

システム管理者は，NFS サービスの構成定義を変更する前に次のことに注意してください。

- Physical Node 上で操作する場合は，クラスタ内で設定内容が同じになるよう HVFP のノードごとにサービスの構成定義を変更してください。
- NFS サービスの構成定義で，NFS プロトコルのバージョンやセキュリティフレーバーなどの設定を解除する場合，または最大転送長を変更する場合，事前に NFS クライアント側からファイルシステムをアンマウントするよう，NFS クライアントホストの管理者に依頼する必要があります。アンマウントしないでこれらの設定を変更すると，NFS サービスの再起動後に NFS クライアントからファイルシステムにアクセスできなくなります。システム管理者は，構成定義を変更し，NFS サービスを再起動したあとで，NFS クライアント側でアンマウントしたファイルシステムを再度マウントするよう，NFS クライアントホストの管理者に連絡してください。

15.3.1 NFS サービスの構成定義の変更

NFS サービスの構成定義を変更する方法と注意事項については，「ユーザーズガイド」（IF305）を参照してください。ここでは，［Access Protocol Configuration］ダイアログの［NFS Service

Management］ページで NFS サービスの構成定義を変更する場合の注意事項について補足します。

表 15-2：［NFS Service Management］ページの［NFS service setup］での注意事項

#	項目	説明および注意事項
1	［Number of nfsd processes］	運用中に起動する nfsd プロセスの数は，指定した上限値を超えない範囲で，システムの状態に応じて自動的に変更されます。
2	［nfsd buffer size］	最大転送長を変更する前に，NFS クライアント側からファイルシステムをアンマウントするよう，NFS クライアントホストの管理者に依頼する必要があります。 また，UDP プロトコルを使用して NFS マウントする場合，56 より大きな値を指定しても，最大転送長は 56KB に制限されます。
3	［KDC server domain name］	KDC サーバと Active Directory ドメインコントローラーを兼用する場合は，ここで指定した名称は Active Directory ドメインの名称としても使用されます。 CIFS サービスで使用していた Active Directory ドメインまたはドメインコントローラーと異なる名称を設定した場合，CIFS サービスを再起動する必要があります。
4	［KDC server name(s)］	KDC サーバと Active Directory ドメインコントローラーを兼用する場合は，ここで指定した名称は Active Directory ドメインコントローラーの名称としても使用されます。 CIFS サービスで使用していた Active Directory ドメインまたはドメインコントローラーと異なる名称を設定した場合，CIFS サービスを再起動する必要があります。

15.4 NFS 共有管理

ここでは，システム管理者が File Services Manager で NFS 共有を作成する場合や属性を編集する場合の注意事項について説明します。

15.4.1 NFS 共有の作成と設定変更

システム管理者は［共有追加］ダイアログまたは［ファイルシステム構築と共有作成］ダイアログで NFS 共有を作成できます。NFS 共有を作成する方法は，「ユーザーズガイド」（IF305）を参照してください。ここでは，［アクセス制御］タブの［NFS］サブタブで指定する，NFS 共有を作成する場合の設定の注意事項について説明します。なお，同じ情報は［共有編集］ダイアログの［アクセス制御］タブの［NFS］サブタブでも指定できます。

NFS 共有の作成，属性の編集を行う場合には，次の情報を指定できます。

- NFS 共有の公開先（ホストまたはネットワーク）
  公開先のホストまたはネットワークの指定には，次の方法があります。
  特定のホスト
  　ホスト名または IP アドレスで指定する。
  サブネットワークやグループに属するすべてのホスト
  　NFS クライアントが属する DNS ドメインの DNS ドメイン名，NIS のネットグループまたはサブネットワークの IP アドレスで指定する。
  すべてのホスト
  　ワイルドカード（*）で指定する。
- 公開先に対するセキュリティフレーバー

公開先ごとに，許可する認証方式（UNIX（AUTH_SYS）認証，Kerberos 認証）として，sys，krb5，krb5i，krb5p のうちの少なくとも 1 つを選択します。
サービス単位で許可されている認証方式をそのまま引き継ぐ場合には，［デフォルトの設定を使用］を選択します。
NFS クライアントが NFS 共有にアクセスするとき，セキュリティフレーバーのどれを使用するかは，NFS クライアントのマシンでファイルシステムをマウント（NFS マウント）するときの mount コマンド（sec オプション）の指定，またはオプションのデフォルト値で決まります。

- 公開先に対するアクセス権
  公開先ごとに，NFS 共有を読み取りと書き込みを許可して公開するか，読み取りだけを許可して公開するかを指定します。
- 匿名ユーザーへのマッピング
  公開先ごとに，匿名ユーザーへのマッピングを行わない（［非適用］）か，匿名ユーザーへマッピングするユーザーを root ユーザーだけとする（［root ユーザー用］）か，またはすべてのユーザーをマッピングする（［全ユーザー用］）かのどれかを指定します。
- 匿名ユーザーに対して使用する UID，GID
  ユーザーが匿名ユーザーとしてアクセスするときに使用するユーザー ID（UID）およびグループ ID（GID）を指定します。
  なお，NFSv4 ドメインを設定した環境では，［非適用］を指定した場合でも，NFS サービスの構成定義で設定されている［Anonymous user name］の UID，［Anonymous group name］の GID で匿名ユーザーのマッピングが行われます。また，［root ユーザー用］を指定した場合は，NFS サービスでの匿名ユーザーのマッピングの結果に対して，root ユーザーだけに［匿名マッピング用 UID］および［匿名マッピング用 GID］で指定する UID，GID が適用されます。［全ユーザー用］を指定した場合は，NFS サービスでの設定よりも，［匿名マッピング用 UID］および［匿名マッピング用 GID］で指定する UID，GID が優先されます。

15.4.2 NFS 共有の属性編集

システム管理者は，［共有編集］ダイアログで NFS 共有の属性を編集できます。NFS 共有の属性を編集する方法および注意事項は，「ユーザーズガイド」（IF305）を参照してください。ここでは，NFS 共有の属性を編集する場合の注意事項について説明します。

- 情報を変更しなかった項目については，現在設定されている情報が適用されます。
- NFS 共有を作成したファイルシステムに差分スナップショットの自動作成スケジュールを設定し，差分スナップショットに自動的にファイル共有を作成して運用する場合，編集した NFS 共有の情報を基に，差分スナップショットに NFS 共有が作成されます。

上記に加え，「15.4.1 NFS 共有の作成と設定変更」に示す NFS 共有を作成する際の注意事項もあわせて参照してください。

16

NFS クライアントのユーザー管理

この章では，NFS クライアントのユーザー管理について説明します。

16.1 ユーザー管理方法

HVFP では，ファイルシステムを利用する NFS クライアントのユーザー名，グループ名，UID，GID などのユーザー情報を次の表に示す方法で管理できます。

表 16-1： NFS クライアントのユーザー情報の管理方法

#	項目	説明
1	File Services Manager*	ファイルシステムを利用するユーザーを File Services Manager で管理する場合に，ユーザー情報を登録します。
2	NIS サーバ	ファイルシステムを利用するユーザーを NIS サーバで管理する場合に，ユーザー情報を登録します。
3	ユーザー認証用 LDAP サーバ	ファイルシステムを利用するユーザーをユーザー認証用 LDAP サーバで管理する場合に，ユーザー情報を登録します。
4	KDC サーバ	Kerberos 認証を使用する場合に，ユーザー認証で使用する情報を登録します。 このほか，File Services Manager，NIS サーバまたはユーザー認証用 LDAP サーバのどれかでユーザー情報を管理する必要があります。

注 *

NFS クライアントで管理されているユーザー情報と同じユーザー情報を File Services Manager にも登録してください。

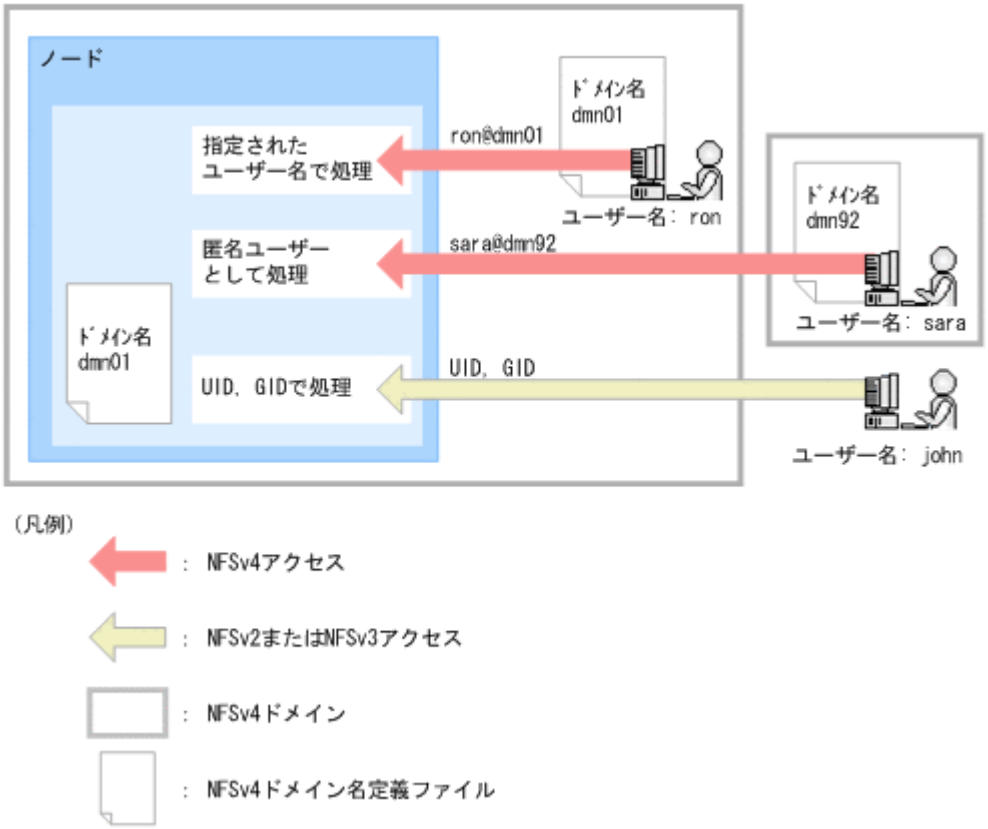
16.2 NFSv4 ドメインを設定しているときのユーザー管理

NFSv4 ドメインを設定すると，NFSv4 プロトコルでアクセスする NFS クライアントをドメイン内のユーザーに限定できます。

NFSv4 ドメイン内のユーザーが NFSv4 プロトコルで HVFP にアクセスする際には，ユーザー名，グループ名を UID，GID に変換する（ID マッピングを行う）ために，ID マッピング用サーバまたは File Services Manager によるユーザー管理が必要になります。

NFSv4 ドメインを設定しているときの NFS 共有へのアクセスを次の図に示します。

図 16-1：NFSv4 ドメインを設定しているときの NFS 共有へのアクセス



NFSv4 ドメインは，HVFP のノードと NFS クライアント，または Virtual Server と NFS クライアントから構成され，ノードまたは Virtual Server ごとに 1 つだけ設定できます。Kerberos 認証を併用して運用する場合には，NFSv4 ドメインと KDC サーバドメインの範囲は同一にする必要があります。

ノードまたは Virtual Server が属する NFSv4 ドメインに NFS クライアントを参加させるには，クライアントマシンの NFSv4 ドメイン名定義ファイルに，NFSv4 ドメイン名を設定する必要があります。

アクセスを要求したユーザーがノードまたは Virtual Server の属する NFSv4 ドメインに参加している NFS クライアントのユーザーかどうかは，ユーザーの識別情報（ユーザー名 @NFSv4 ドメイン名）から判断されます。ほかの NFSv4 ドメインに参加している NFS クライアントのユーザーが NFSv4 プロトコルでアクセスを要求した場合，またはアクセスを要求したユーザーの ID マッピングに失敗した場合は，匿名ユーザーとしてアクセスが許可されます。また，どの NFSv4 ドメインにも参加していない NFS クライアントのユーザーは，UID および GID で処理されます。

NFSv4 ドメインを設定している場合，NFS 共有にアクセスしたユーザーの情報は一時的にキャッシュされます。キャッシュの有効時間は 10 分間です。ユーザー情報の変更によって，実際のユーザー情報と，キャッシュされているユーザー情報に差異が発生していて，かつキャッシュの有効時間内に NFS 共有にアクセスする際には，`nfscacheflush` コマンドを実行する必要があります。

17

NFS クライアントのユーザー認証

この章では，NFS クライアントのユーザー認証の方法および注意事項について説明します。

17.1 ユーザー認証方式

HVFP が提供する NFS サービスでは，次に示す方式のユーザー認証を利用できます。

- UNIX（AUTH_SYS）認証
- Kerberos 認証

システム管理者は，ユーザー認証方式や使用する機能を設定するため，NFS サービスまたは NFS 共有ごとにセキュリティフレーバーを選択します。NFS クライアントは HVFP のファイルシステムをマウントする際に，対象の NFS 共有に設定されているセキュリティフレーバーから，使用するユーザー認証方式を指定します。

17.2 UNIX（AUTH_SYS）認証

UNIX（AUTH_SYS）認証とは，ログイン時にユーザーが指定したユーザー名とパスワードを使用して，NFS クライアント側で実施されるユーザー認証方式です。

UNIX 認証を使用してファイル共有にアクセスするユーザーが所属するグループの数は，16 個以下にしてください。17 個以上のグループに所属している場合，17 番目以降の所属グループに対するアクセス権が無効になります。

17.3 Kerberos 認証

HVFP で利用できる Kerberos 認証の機能を次に示します。これらの機能と UNIX（AUTH_SYS）認証（sys）は，NFS サービスまたは NFS 共有ごとに設定するセキュリティフレーバーとして選択できます。

- krb5
  Kerberos 5 を使用したユーザー認証方式です。
- krb5i
  Kerberos 5 を使用したユーザー認証に加えて，送受信するデータの整合性を検証する機能を利用できます。
- krb5p
  Kerberos 5 を使用したユーザー認証とデータの整合性を検証する機能に加えて，送受信するデータを暗号化する機能を利用できます。

krb5，krb5i，krb5p の順番でセキュリティを高めることができますが，同時にオーバーヘッドも増加します。システム管理者は，HVFP の運用環境を考慮して，使用するセキュリティフレーバーを選択してください。

Kerberos 認証を利用する運用の場合，KDC サーバ，HVFP のノードまたは Virtual Server および NFS クライアントの間で時刻がずれないようにしてください。時刻にずれがあると，NFS クライアントからファイルシステムがマウントできないことや，NFS 共有にアクセスできないことがあります。

Kerberos 認証を使用してファイル共有にアクセスするユーザーが所属するグループの数は，32 個以下にしてください。33 個以上のグループに所属している場合，33 番目以降の所属グループに対して Kerberos 認証できません。

18

共有ディレクトリへの NFS アクセス

この章では，NFS クライアントから共有ディレクトリにアクセスする場合の手順と注意事項について説明します。

18.1 アクセス方法

NFS クライアントから共有ディレクトリにアクセスするためには，ファイルシステムをマウントする必要があります。NFS クライアントからファイルシステムをマウントする方法については，「18.2 ファイルシステムのマウントと見え方」を参照してください。

HVFP のファイルシステムをマウントする際には，ノードまたは Virtual Server の仮想 IP アドレスに対応するホスト名を指定します。

このため，NFS クライアントとノードまたは Virtual Server の両方で，ホスト名の名前解決ができ，かつ名前解決によって得られる仮想 IP アドレスが NFS クライアントとノードまたは Virtual Server とで一致している必要があります。

また，ファイルロックを使用する場合も，仮想 IP アドレスに対応するホスト名を指定してください。ホスト名ではなく仮想 IP アドレスを指定してマウントすると，ファイルロックが正常に動作しないおそれがあります。

18.2 ファイルシステムのマウントと見え方

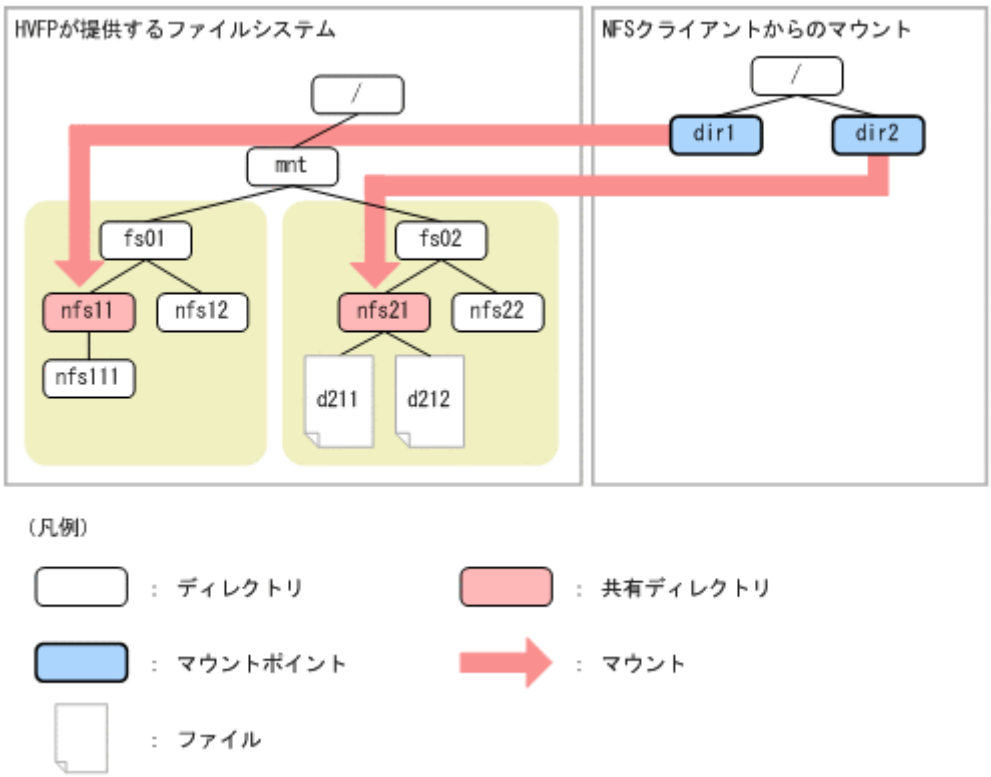
NFS クライアントから共有ディレクトリをマウントすることで，ファイルシステムにアクセスできるようになります。NFSv4 クライアントの場合は，共有ディレクトリのほか，ルートディレクトリをマウントすることもできます。

この節では，共有ディレクトリまたはルートディレクトリをマウントする方法と，NFS クライアントからのファイルシステムの見え方について説明します。

18.2.1 共有ディレクトリをマウントするとき

NFS クライアントから，共有ディレクトリをマウントした場合の例を次の図に示します。

図 18-1：共有ディレクトリのマウント例



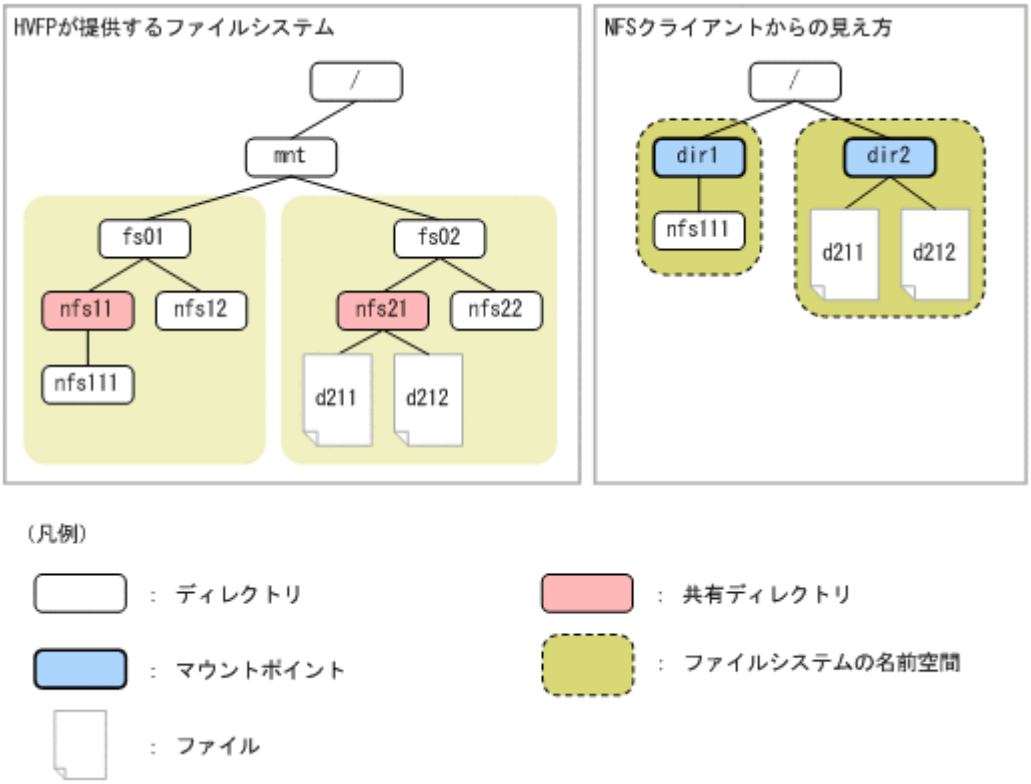
mount コマンドの実行例を次に示します。

```
mount -o vers=3 node01:/mnt/fs01/nfs11 /dir1
mount -o vers=3 node01:/mnt/fs02/nfs21 /dir2
```

NFS クライアントから共有ディレクトリをマウントした場合，各共有ディレクトリ以下のディレクトリやファイルで構成されたディレクトリツリーがファイルシステムの名前空間となります。複数の共有ディレクトリにアクセスする場合は，共有ディレクトリごとにマウントする必要があります。

共有ディレクトリをマウントした場合の NFS クライアントからのファイルシステムの見え方について，次の図に示します。

図 18-2： 共有ディレクトリをマウントした場合のファイルシステムの見え方

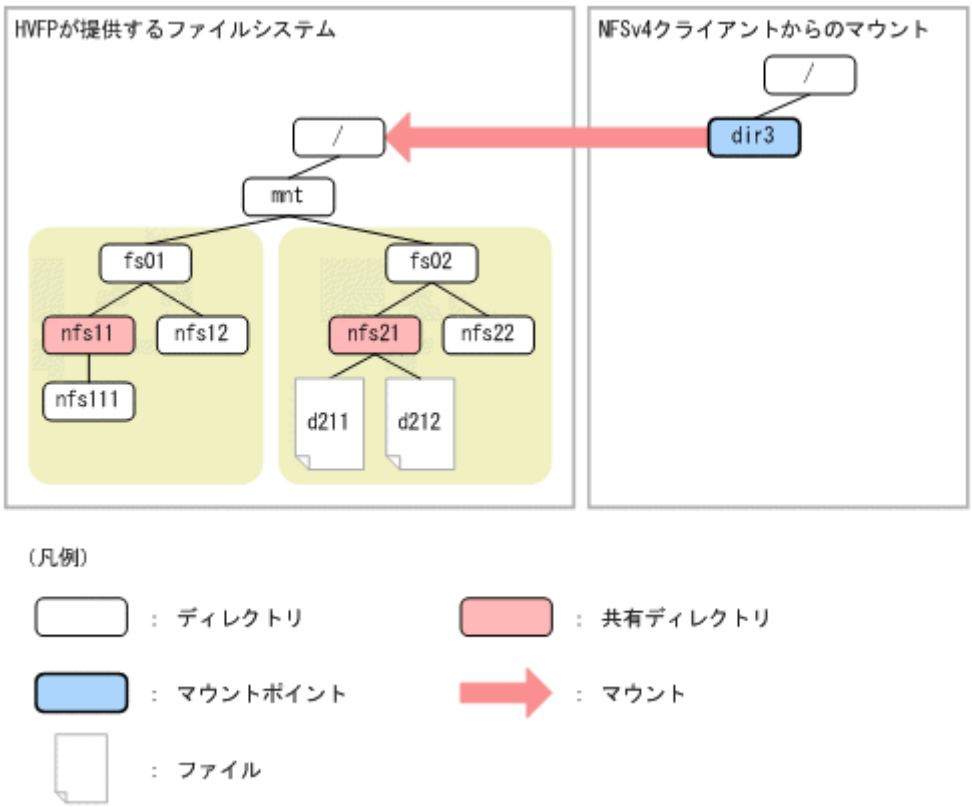


18.2.2 ルートディレクトリをマウントするとき

NFSv4 クライアントからルートディレクトリをマウントすることで，ルートディレクトリ以下のすべての共有ディレクトリをマウントした状態になります。

NFSv4 クライアントからルートディレクトリをマウントした場合の例を次の図に示します。

図 18-3：ルートディレクトリのマウント例



ルートディレクトリを指定した場合の mount コマンドの実行例を次に示します。

```
mount -o vers=4 node01:/ /dir3
```

ファイルシステムのルートディレクトリをマウントすることで，複数の NFS 共有を仮想的に 1 つのファイルシステムとして構成したディレクトリツリーに対して，NFSv4 クライアントからアクセスできるようになります。ルートディレクトリをマウントすれば，同一ディレクトリツリー内のすべての共有ディレクトリにアクセスできるため，共有ディレクトリごとにマウントする必要はありません。

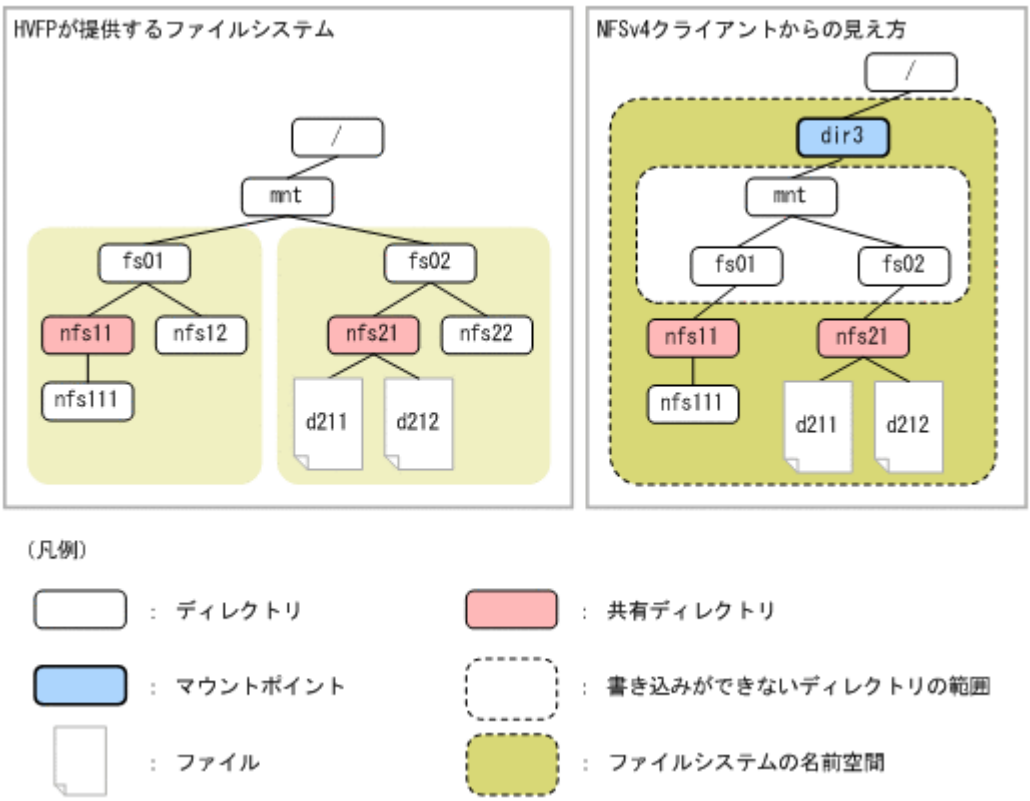
マウントディレクトリと各共有ディレクトリとの間にある直系のディレクトリに対して，NFSv4 クライアントから参照はできますが，書き込みはできません。また，直系のディレクトリ以下のファイルやディレクトリは，NFSv4 クライアントに対して隠蔽された状態となります。

NFS クライアントからルートディレクトリをマウントした場合，マウントディレクトリと各共有ディレクトリとの間にある直系のディレクトリに加えて，すべての共有ディレクトリ以下のディレクトリやファイルで構成されたディレクトリツリーがファイルシステムの名前空間となります。

ただし，Solaris 10 または HP-UX 11i v3 を利用している NFS クライアントから NFSv4 プロトコルを利用してルートディレクトリをマウントした場合，プラットフォームのバージョンによっては，共有ディレクトリ以下のディレクトリやファイルがファイルシステムの名前空間として表示されません。

ルートディレクトリをマウントしたときの NFSv4 クライアントからのファイルシステムの見え方について，次の図に示します。

図 18-4：ルートディレクトリをマウントした場合のファイルシステムの見え方



18.3 NFS クライアントからファイルシステムを利用するときの注意事項

NFS クライアントからファイルシステムを利用するときの注意事項について説明します。なお，HVFP の設定を変更するときの注意事項については，「システム構成ガイド」（IF302）を参照してください。

また，NFS クライアントからスタブファイルにアクセスする場合，処理に時間が掛かることがあります。このため，大量のファイルにアクセスする場合は，このことにも留意してください。スタブファイルについては，「システム構成ガイド」（IF302）を参照してください。

18.3.1 ファイルシステムをマウントするときの注意事項

NFS クライアントからファイルシステムをマウントするときの注意事項を次に示します。

- NFS クライアントから HVFP のファイルシステムをマウントする場合は，hard オプションを指定することを推奨します。soft オプションを指定した場合，NFS クライアントから HVFP にアクセスしているときにフェールオーバーが発生したり，フェールオーバー中に NFS クライアントから HVFP にアクセスしたりすると，NFS クライアントからの要求がエラー（ETIMEDOUT または ECONNRESET）となることがあります。なお，ほとんどの NFS クライアントで，hard オプションがデフォルトになっています。
- HVFP のファイルシステムで 2GB 以上のサイズのファイルを使用する場合は，NFS クライアントのマウントオプションに NFSv3 プロトコルまたは NFSv4 プロトコルのバージョンを明示的に指定してください。NFS クライアントによっては，明示的に指定していないと NFSv2 プロトコルが適用され，HVFP のファイルシステムで 2GB 以上のファイルを使用できないことがあります。

- NFSv4 プロトコルを使用して HVFP のファイルシステムにアクセスする場合は，NFS クライアントのマウントオプションに NFSv4 プロトコルのバージョンを明示的に指定してください。NFS クライアントによっては，明示的に指定していないと NFSv2 または NFSv3 プロトコルが適用されることがあります。
- ファイル操作を中断できない NFS クライアント（Linux ほか）から HVFP のファイルシステムをマウントする場合，`hard` および `intr` オプションを指定する必要があります。これらのオプションを指定しないと，ファイルの操作中に障害が発生したときに操作を中断できないおそれがあります。
- NFS クライアントから HVFP のファイルシステムをマウントする場合は，非 ASCII 文字が含まれるディレクトリを指定しないでください。
- 仮想 IP アドレスを削除または変更する場合は，対象の IP アドレスに対するクライアントからのアクセスを停止してから，NFS クライアントでファイルシステムをアンマウントしておく必要があります。この作業を行わないで仮想 IP アドレスを削除または変更すると，NFS クライアントから HVFP を正常に利用できなくなります。

18.3.2 ファイルロックを利用するときの注意事項

NFS クライアントからファイルロックを利用するときの注意事項を次に示します。

- NFSv2 または NFSv3 プロトコルを使用している場合にファイルロックを使用するときは，仮想 IP アドレスに対するホスト名を，ノードの OS および NFS クライアントの `/etc/hosts` ファイル，NIS サーバまたは DNS サーバに登録して，HVFP と NFS クライアントでの名前解決（正引きおよび逆引き）が同一になるようにしてください。なお，`/etc/hosts` ファイル，NIS サーバまたは DNS サーバの登録情報を追加，削除または変更した場合は，NFS サービスを再起動する必要があります。
- NFS クライアントにて，NFS クライアントの IP アドレスに対するホスト名を名前解決できない場合は，ロックリカバリ処理（フェールオーバー時またはノード再起動時に再度実行されるファイルロック処理）が正しく動作しないおそれがあります。NFS クライアントのホスト名を名前解決する必要があるかどうかをベンダーに確認してください。
- NFSv4 プロトコルを使用している場合にファイルロックを使用するときは，File Services Manager で NFS サービスを設定するときに指定する NFSv4 ドメイン名と，NFS クライアントの NFSv4 ドメイン名が一致している必要があります。
- NFS クライアントが Mac OS X の場合，複数のクライアントから 1 つのファイルをロックしたり，SIGLOST シグナルをサポートしていないクライアントから複数のプロセスで 1 つのファイルをロックしたりしているときに，次に示す処理が HVFP で実行されると，ロック待ちしていたほかのプロセスがロックを取得することがあります。
  - NFS サービス，ノードの OS，または Virtual Server の再起動
  - フェールオーバー
- HVFP では，次のような場合，NFS サービスやノードの OS を再起動したり，Virtual Server を再起動したり，フェールオーバーが発生したりしたときに，ロック待ちしていたほかのプロセスがロックを取得することがあります。
  - 複数のクライアントから 1 つのファイルをロックする
  - SIGLOST シグナルをサポートしていないクライアントから複数のプロセスで 1 つのファイルをロックする
- 次の場合には，NFS クライアントから POSIX ロック（セグメントロック，リージョンロック，またはレコードロック）を利用してレコードロックを取得するときに `ENOLCK` エラーとなることがあります。

- HVFP の NFS 共有にサブツリーチェックをするように設定している場合
- ロック対象のファイルの親ディレクトリから NFS マウントしたディレクトリまでを含むすべてのディレクトリに，HVFP の匿名ユーザーに対する実行権限（x）がない場合

次のどちらかの設定を行うと ENOLCK エラーは発生しません。

- ロック対象ファイルの親ディレクトリから NFS マウントしたディレクトリまでを含むディレクトリのうち，HVFP の匿名ユーザーに対する実行権限（x）がないディレクトリに実行権限（x）を追加してください。
- NFS クライアントで HVFP の NFS 共有ディレクトリをアンマウントし，NFS 共有にサブツリーチェックをしないように設定してください。そのあと，NFS クライアントから HVFP の NFS 共有ディレクトリをマウントしてください。

・ 次の場合には，NFS クライアントからのファイルロック要求に対して EDEADLK エラーが発生しません。NFS クライアントでハングアップしたジョブをキャンセルしてください。

- Solaris 10 または HP-UX 11i v3 を利用している NFS クライアントから NFSv4 プロトコルを利用してファイルロックを要求した際に，デッドロックが発生した場合
- NFS クライアントから NFSv4 プロトコルを利用してロックされているファイルに対して，NFSv2 または NFSv3 プロトコルを利用してファイルロックを要求した際に，デッドロックが発生した場合
- NFS クライアントから NFSv2 または NFSv3 プロトコルを利用してロックされているファイルに対して，NFSv4 プロトコルを利用してファイルロックを要求した際に，デッドロックが発生した場合

・ Linux を利用している NFS クライアントから，TCP プロトコルでマウントしたディレクトリでファイルロックを使用すると，ファイルロックのロック待ちを解除するのに時間が掛かることがあります。
また，Linux を利用している NFS クライアントから，ファイルロックしているプロセスを中断すると，HVFP にロック情報が残り，該当するファイルをロックできなくなることがあります。

・ Linux カーネル 2.4 を利用している NFS クライアントから，HVFP 上のファイルロック待ちのプロセスをキャンセルすると，HVFP にロック情報が残ることがあります。

・ Linux カーネル 2.4.19 以前のカーネルを利用している NFS クライアントでは，ファイルロック待ちのプロセスがロックを確保するまでに 10 秒程度掛かることがあります。

・ NFSv2 または NFSv3 プロトコルを使用している場合，NFS クライアントでネットワークロックマネージャー（nlockmgr）およびネットワークステータスモニター（status）が動作している必要があります。使用する NFS クライアントマシンから次の形式で rpcinfo コマンドを実行して，status と nlockmgr の UDP プロトコルでのサービスが正常に稼働していることを確認します。
rpcinfo -u localhost プログラム名 バージョン
正常に稼働している場合は，「ready and waiting」と出力されます。実行例を次に示します。

```
$ rpcinfo -u localhost nlockmgr 1
program 100021 version 1 ready and waiting
$ rpcinfo -u localhost nlockmgr 3
program 100021 version 3 ready and waiting
$ rpcinfo -u localhost nlockmgr 4
program 100021 version 4 ready and waiting
$ rpcinfo -u localhost status 1
program 100024 version 1 ready and waiting
```

・ Linux カーネル 2.4，2.6.19 ～ 2.6.27 を使用している NFS クライアントから TCP プロトコルでマウントしたディレクトリ上のファイルがファイルロックされている，または，Linux カーネル 2.4.21 より前のカーネルを使用している NFS クライアントから UDP プロトコルでマウントしたディレクトリ上のファイルがファイルロックされていると，次の場合にファイルロックが解除されます。

- フェールオーバーまたはフェールバックが発生したとき
- クラスタを停止してから再起動したとき

ファイルロックが解除されてしまうと，ファイルロック中であったファイルをほかのプロセスがファイルロックできる状態になり，ファイルが破損するおそれがあります。
なお，Linux カーネル 2.6.19 ～ 2.6.27 を使用している NFS クライアントの場合は，NFS クライアントで NFS サービスを起動してから TCP プロトコルでマウントすることで，ファイルロックの解除を防ぐことができます。

- NFS クライアントホストの実装によっては，次のすべての条件に合致すると，書き込み範囲をファイルロックしている場合でも，ファイルのより前方の位置に書き込んだ内容が「0」に置き換わることがあります。この現象は，転送長単位でファイルロックして書き込みを行うことで回避できます。
  - 転送長（マウント時の wsize オプション）より短い長さの書き込みを同一ファイルに対して複数クライアントから同時に実行する。
  - ファイルサイズより後方への書き込みを行い，かつ同一ブロック（転送長を単位として見たブロック）への書き込みを行う。

（例）

NFS クライアントホスト X および NFS クライアントホスト Y から，HVFP のファイルシステムを転送長 32KB でマウントします（mount コマンドのオプションで「wsize=32768」，「rsize=32768」と指定する）。NFS クライアントホスト X のプロセス A が，あるファイルの 0 ～ 1,023 バイト目をファイルロックしてこの範囲に書き込みます。そして，NFS クライアントホスト Y のプロセス B が，同一ファイルの 1,024 ～ 2,047 バイト目をファイルロックしてこの範囲に書き込みます。
このように，プロセス A とプロセス B が同時に動作すると，ファイルのより前方の位置に書き込んだプロセス A の書き込みデータ（0 ～ 1,023 バイトの内容）が「0」に置き換わることがあります。

18.3.3 ファイルシステムを利用するときの注意事項

NFS クライアントからファイルシステムを利用するときの注意事項を次に示します。

- NFS クライアントからシステムコール，ライブラリー関数およびコマンド操作によって HVFP のファイルやディレクトリの作成，更新，削除などを行っているときに HVFP でフェールオーバーが発生した場合，ファイルやディレクトリの作成，更新，削除などは，HVFP 上では正常に完了しても，NFS クライアントではエラーとなることがあります。
- NFS クライアントで TCP プロトコルを使用して HVFP のファイルシステムをマウントし，そのディレクトリ下のサブディレクトリやファイルにアクセスしない状態が続くと，NFS クライアントホストの実装によっては，次のアクセスに 1 ～ 10 秒程度掛かることがあります。また，システムログに ECONNRESET エラーが出力される場合がありますが，NFS サービスを使用してファイルシステムにアクセスするプログラムは正常に動作します。
- NFS クライアントで HVFP にスペシャルファイルを作成する場合，次に示すことに注意してください。
  - HVFP 上のファイルシステムに対してスペシャルファイルを作成する場合，major 番号に指定できる最大値は 4,095，minor 番号に指定できる最大値は 1,048,575 です。
  - NFSv2 プロトコルを使用している場合に，NFS クライアントとして Linux 以外を使用しているときは，NFS クライアントでスペシャルファイルを作成すると，指定した値とは異なる major 番号および minor 番号で作成されることがあります。Linux を使用している場合でも，ディストリビューションによっては同じ現象が発生することがあります。そのため，このような NFS クライアントからは，スペシャルファイルを作成しないでください。

- 64 ビット inode に対応しているファイルシステムでは，NFSv2 プロトコルを使用できません。64 ビット inode に対応するように設定する前に，対象のファイルシステムで NFSv2 プロトコルを使用するクライアントがいないことを確認してください。
- NFS 環境で動作するアプリケーションによっては，64 ビット inode をサポートしていないことがあります。64 ビット inode をサポートしているアプリケーションを使用している場合に限り，64 ビット inode に対応するよう設定してください
- NFS クライアントマシンに HVFP と通信するネットワークインターフェースが複数ある場合は，NFS アクセスが許可されないでエラー（ESTALE エラー）になることがあります。これは，クラスタ管理ソフトウェアなどの利用によって，NFS マウント要求する IP アドレスと NFS アクセスする IP アドレスが異なることがあるためです。
  このような NFS クライアントから HVFP のファイルシステムを利用する場合は，該当する NFS 共有の公開先を次のどれかの方法で指定してください。
  - ワイルドカード（*）を使用する
  - NFS クライアント側で使用するすべてのネットワークインターフェースの IP アドレスを指定する
  - NFS クライアント側で使用するすべてのネットワークインターフェースに対応するホスト名を指定する
  - NFS クライアント側で使用するすべてのネットワークインターフェースの IP アドレスを含む IP ネットワークを指定する
  - NFS クライアント側で使用するすべてのネットワークインターフェースに対応するホスト名を含むネットグループを指定する
  - NFS クライアント側で使用するすべてのネットワークインターフェースに対応するホスト名を含む DNS ドメインを指定する
- ファイルシステムに対して次の処理が実行されている場合に，Solaris を使用している NFS クライアントがそのファイルシステムにアクセスすると，NFS クライアント環境に大量のメッセージが出力されることがあります。
  - ファイルシステムの拡張
  - ファイル共有の拡張
  - 差分格納デバイスの設定，拡張および解除
  - 差分スナップショットの作成および削除
  - 差分スナップショットを使用したオンラインバックアップ
  - horcfreeze コマンドを実行してから horcunfreeze コマンドを実行するまでの間

  NFS クライアントのシステムログファイルのローテーションの設定（ファイル数やファイルサイズなど）には注意してください。
- Solaris 10 を使用しているクライアントからの NFS アクセスがハングアップする場合は，Solaris 10 のドライバーコンフィグレーションパラメーターで SACK 許可オプションを確認してください。SACK 許可オプションを使用できる設定（ndd コマンドの tcp_sack_permitted パラメーターで 1 または 2 を指定）にしていると，NFS アクセスがハングアップすることがあるため，SACK 許可オプションを使用できない設定（tcp_sack_permitted パラメーターで 0 を指定）にしてください。
- HP-UX を利用している NFS クライアントから cp コマンドでファイルをコピーしているときに操作を中断すると，コピー先のファイルの権限が 000 になります。
  また，HP-UX を利用している NFS クライアントからファイルシステムを更新しているときに HVFP でフェールオーバーが発生すると，ファイルシステムを更新していたプロセスがフェールオーバーしたあとでエラー終了することがあります。これらの障害を回避するために，HP 社のホームページで提供されている HP-UX 対策パッチのうち，PHNE_28568（11.11 用）をインストールしてください。なお，これらのパッチについての詳細はベンダーにお問い合わせください。

- NFS クライアントホストに Linux カーネルを使用する場合は，最新パッチを必ず適用してください。最新パッチを適用していないカーネルを使用して NFS アクセスすると，次のような問題が発生することがあります。
  - エラー（エラー番号 528）が発生する
  - ファイルの内容と異なる情報がクライアント側で表示される
  - クライアント側で書き込んだ内容と異なる情報が HVFP のファイルに保存される
- NFS クライアントホストに Linux カーネルを使用する場合，NFS 共有のファイルの読み込み時に EBUSY エラーが発生することがあります。この場合は，アクセスし直してください。
- HP-UX または RPC プログラム番号 100020 を使用しているマシン（rpcinfo -p で「program」に「100020」が表示されるホストマシン）を NFS クライアントとして使用する場合，NFS クライアントでマウントしたディレクトリの下にあるハードリンクファイルの内容を正しく参照できないことがあります。
  NFS 共有を作成するとき，または NFS 共有の情報を編集するときに，次に示すように設定すると，ハードリンクファイルの内容を正しく参照できます。なお，Linux，Solaris を NFS クライアントとして使用する場合，次に示す設定は必要ありません。
  - NFS 共有を作成する場合
    GUI で NFS 共有を作成する場合は，システム管理者が設定を意識する必要はありません。
    コマンドを使用する場合は，nfscreate コマンドの -s オプションに，do_not_perform（デフォルト）を指定してください。
  - NFS 共有の情報を編集する場合
    GUI で NFS 共有を作成した場合は，システム管理者が設定を意識する必要はありません。コマンドを使用した場合は，nfsedit コマンドの -s オプションに，do_not_perform を指定してください。
- NFS クライアントが HVFP のファイルシステムに対してアクセスした際に，「file temporarily unavailable on the server, retrying...」とメッセージが出力された場合は，対象のファイルシステムへのアクセスをシステム管理者が意図的に抑止していることがあります。
- ノードの OS が高負荷状態の場合，NFS クライアントが NFS 共有にアクセスした際，ファイルシステムの使用率が 100% に達する前にデバイス空き領域不足エラー（ENOSPC）になることがあります。
- オープンソースのユーティリティである rsync コマンドのように，更新後の内容を一時ファイルにいったん書き出して，mv コマンドでファイル名をリネームするようなファイル更新処理と，ほかの NFS クライアントからの該当ファイルの読み込み処理が競合することで，読み込み処理が失敗するおそれがあります。
- NFS クライアントから Quota 情報取得コマンドを実行しても，サブツリー Quota の情報を取得できません。サブツリー Quota の情報については，システム管理者に問い合わせてください。
- HVFP のファイルシステムを利用するユーザーの Quota 情報を NFS クライアントから Quota 情報取得コマンドで参照するときに，ブロック使用量や Quota に関する設定値が 1TB を超えていると，オーバーフローして表示されることがあります。
- Advanced ACL タイプのファイルシステムでは，ファイルの最終アクセス日時（atime）および最終編集日時（mtime）を更新する場合に，対象のファイルに対して SYNCHRONIZE 権限が必要です。また，ファイルやディレクトリを移動したり名称を変更したりする（rename）場合にも，対象のファイルやディレクトリ，rename 先の親ディレクトリ，および rename 時に上書きされる既存のファイルやディレクトリに対して SYNCHRONIZE 権限が必要です。NFSv4 プロトコルを使用して Advanced ACL タイプのファイルシステムで ACL を設定する際には，ファイルの最終アクセス日時および最終編集日時を更新したり，ファイル

やディレクトリを移動したり名称を変更したりする必要があるユーザーやグループに対して，SYNCHRONIZE マスクを許可してください。

- NFS クライアントにシステムが使用するファイルまたはディレクトリが表示されることがあります。システムが使用するファイルまたはディレクトリについては，「表 7-4： システムが使用するファイルまたはフォルダに関する注意事項」を参照してください。
- IPv6 接続かつ UDP プロトコルを使用して NFS クライアントから Virtual Server 上のファイルシステムをマウントすると，マウント処理が失敗します。
  NFS クライアントから Virtual Server に接続するときは，IPv4 接続または TCP プロトコルを使用してファイルシステムをマウントしてください。
- MTU に 1,500 を超えた値を設定して運用している場合に，Red Hat Enterprise Linux Server v6.3 以降 （Red Hat Enterprise Linux Server v6.3 以降をベースとした CentOS6.3，Oracle Linux6.4 以降も含む）からの NFS アクセスがハングアップしたときは，RPC 要求の多重度を NFS クライアント側で設定するカーネルコンフィグレーションパラメーター（sunrpc.tcp_slot_table_entries）を確認し，32 に設定してください。32 を超える値が設定されていると，NFS アクセスがハングアップすることがあります。

19

NFS 共有内のファイル・ディレクトリ

この章では，NFS 共有ディレクトリ内に作成するファイル・ディレクトリに関する注意事項について説明します。

19.1 ファイル・ディレクトリ名称

HVFP では，CIFS 共有と併用する際，各国語サポートのため UTF-8 でエンコードしたファイル名やディレクトリ名を使用しています。このため，ファイル名やディレクトリ名の最大長は UTF-8 でエンコードした場合のバイト数で換算する必要があります。

NFS 共有上のファイルやディレクトリの名称の最大長は次の表のようになります。

表 19-1： ファイル名とディレクトリ名の最大長

#	対象	最大長
1	ファイル名	1,023 バイト
2	ディレクトリ名	255 バイト

共有内の .snaps ディレクトリにアクセスして，差分スナップショットを参照する運用では，スナップショット参照時に，スナップショットを示すパス名（27 文字）が付与されるため，クライアントからアクセスできるパス名の最大長が 27 文字短くなります。クライアントからアクセスできるパス名の最大長を超えた名称のファイル・ディレクトリを作成している場合，差分スナップショットに正しくアクセスできなくなります。

19.2 ACL

HVFP で提供する ACL 機能には，POSIX ACL に準拠した ACL を設定できる Classic ACL タイプと，Windows の NTFS ACL に準拠した ACL を設定できる Advanced ACL タイプの 2 種類があります。

Classic ACL タイプと Advanced ACL タイプの差異については，「8.3.1 Classic ACL タイプと Advanced ACL タイプの差異」を参照してください。

HVFP では，ファイルシステム内のファイル共有で，NFS プロトコルだけを使用する場合は Classic ACL タイプ，CIFS プロトコルと NFS プロトコルを併用したり CIFS プロトコルだけを使用したりする場合は Advanced ACL タイプのファイルシステムを構築することを推奨しています。

NFS クライアントのアクセスは，ファイルやディレクトリに設定されたアクセス権や ACL に従って制御されます。

NFSv2 または NFSv3 クライアントから ACL の参照や設定はできません。また，NFSv4 クライアントからは，CIFS クライアントと同様に ACL の参照や設定ができます。

19.3 ファイル属性

RFC3530 で定義されているファイル属性のうち，HVFP で利用できるファイル属性を次の表に示します。

表 19-2： HVFP で利用できる NFSv4 プロトコルのファイル属性

ファイル属性			利用可否
必須属性（mandatory）			○
推奨属性*（recommended）	ACL		○
	作成時間	time_create	○
	DOS ファイル属性	archive，hidden，system	×

ファイル属性	利用可否
名前付き属性（named）	×

（凡例）○：利用できる　×：利用できない

注 *

推奨属性には，そのほかの推奨属性として，次に示す HVFP で利用できる属性と利用できない属性があります。
HVFP で利用できる属性：
cansettime，case_insensitive，case_preserving，chown_restricted，fileid，files_avail，files_free，files_total，fs_location，homogeneous，maxfilesize，maxlink，maxname，maxread，maxwrite，mode，mounted_on_fileid，no_trunc，numlinks，owner，owner_group，rawdev，space_avail，space_free，space_total，space_used，time_access，time_access_set，time_delta，time_metadata，time_modify，time_modify_set
HVFP で利用できない属性：
mimetype，quota_avail_hard，quota_avail_soft，quota_used

19.4 WORM ファイル

ここでは，NFS 共有の WORM ファイルについて説明します。なお，ここに記載したこと以外に，CIFS 共有の場合と共通の特徴があります。共通の特徴については，「8.7 WORM ファイル」を参照してください。

- ファイルを WORM 化するために読み取り専用にするためには，ファイルの所有者（user），所有グループ（group），その他（other）の，すべての書き込み権限（w）を解除します。
- シンボリックリンクファイルを WORM 化しようとした場合，リンク先ファイルが WORM でなければ WORM 化されます。なお，シンボリックリンクファイル自体は WORM 化されません。
- NFSv2 または NFSv3 クライアントは，リテンション期間の最大値として 2038 年以降（正確には 2038 年 1 月 19 日 3 時 14 分 7 秒以降）の日時を指定できません。これは，クライアントの制限によるものです。リテンション期間の最大値が制限されるクライアントの例を次に示します。
  - Linux の 32bit 版カーネルを使ったディストリビューション
  - Solaris（32bit 版）
  - time_t 型が符号付き 32bit 整数（signed long int）で定義されているプラットフォームのクライアント
- NFSv2 または NFSv3 クライアントは，NFS プロトコルの仕様によって，ファイルに対して指定できる atime の時刻は，32 ビットの符号無し整数の範囲になります。このため，リテンション期間として指定できる最大値は，2106 年 2 月 4 日です。これは，クライアントのプラットフォームがファイルの atime として，2038 年以降の日時を指定できる場合でも該当します。
- WORM ファイルの削除は読み取り専用の解除が必要です。
  設定したリテンション期間を過ぎた WORM ファイルは，読み取り専用を解除することで，削除できるようになります。ただし，データの変更はできません。読み取り専用を解除するためには，ファイルの所有者（user），所有グループ（group），その他（other）の，どれか 1 つ

に書き込み権限（w）を設定してください。このとき，読み出し権限（r）および実行権限（x）の設定は変更できません。

20

ファイル共有を利用する時の注意事項

この章では，CIFS，NFS および FTP クライアントで共有しているファイルシステムやファイル共有を利用するときの注意事項について説明します。

20.1 ファイル共有にアクセスするときの注意事項

ファイルまたはディレクトリを CIFS サービスと NFS サービスで共有している環境で，ファイル共有にアクセスするときの注意事項を説明します。

- CIFS サービスで使用するユーザー ID（UID）およびグループ ID（GID）と，NFS サービスで使用するユーザー ID およびグループ ID を一致させる必要があります。
  RID 方式または LDAP 方式（ユーザー ID およびグループ ID の自動割り当て時）のユーザーマッピングを使用する場合，最初に CIFS サービスで使用するユーザー ID およびグループ ID を割り当て，そのユーザー ID およびグループ ID を NFS のクライアントホストでも該当するユーザーに割り当ててください。
  ただし，RID 方式の場合は，割り当てられたグループ ID と同じ ID を NFS クライアントのユーザー ID に割り当てないでください。同様に，割り当てられたユーザー ID と同じ ID をグループ ID に割り当てないでください。該当する ID の CIFS クライアントが，CIFS サービスを利用できなくなるおそれがあります。
  例えば，あるドメインでの ID の範囲を 70000 ～ 100000 とした場合，`Domain Users` のグループ ID は自動的に 70513 に設定されます。このとき，NFS クライアントでユーザー ID を 70513 に割り当てて NFS 共有にアクセスすると，`Domain Users` に所属する CIFS クライアントからアクセスできなくなります。同様に，`Administrator` のユーザー ID は自動的に 70500 に設定されます。このとき，NFS クライアントで，グループ ID を 70500 に割り当てて NFS 共有にアクセスすると，CIFS クライアントから `Administrator` でアクセスできなくなります。この場合は，該当する NFS のユーザーにユーザー ID およびグループ ID を割り当て直したあと，NFS サービスを再起動するほか，キャッシュされているユーザーマッピング情報を CIFS サービス環境から削除する必要があります。
  ユーザーマッピングで割り当てられたユーザー ID およびグループ ID の情報を確認する方法は次のとおりです。
  RID 方式の場合
  `umapidget` コマンドを使用して，RID 方式でマッピングされたユーザーおよびグループの ID または名称を確認できます。
  LDAP 方式（ユーザー ID およびグループ ID の自動割り当て時）の場合
  ［Check for Errors］ダイアログの［List of RAS Information］ページ（［Batch-download］表示）でユーザーマッピング情報としてダウンロードできます。ダウンロードの方法については，「ユーザーズガイド」（IF305）を参照してください。
- CIFS クライアントからは，CIFS 共有内に作成されたシンボリックリンクにアクセスできません。なお，CIFS 共有内のシンボリックリンクは，NFS クライアントなどによって作成されます。
- HVFP の CIFS 共有上で設定されたファイルやディレクトリの権限は，NFS 共有で設定したアクセス権と同じように動作します。
- NFS クライアントおよび CIFS クライアントからの同一ファイルへのアクセスが競合した場合にファイルの更新が反映されないおそれがあるため，読み取り専用のクライアントキャッシュを使用しないよう，CIFS 共有を設定してください。
- NFS サービスを再起動すると，CIFS クライアントからファイルシステムへのアクセスに失敗することがあります。この場合，しばらく待ってから，ファイルシステムにアクセスしてください。
- CIFS クライアントで読み取り専用の権限を設定したファイルを NFS クライアントで使用する場合，NFS クライアントではファイルに設定された読み取り専用の権限は有効になりません。

- ファイル，ディレクトリ名称に非 ASCII 文字を使用するためには，NFS クライアントで使用するファイル，ディレクトリ名称の文字コードを Unicode（UTF-8）に設定する必要があります。
- NFS 共有で使用される文字コードは NFS クライアントの環境に依存するため，EUC や JIS などの文字コードや制御コード (*1) を使用した NFS クライアントが作成したファイルやディレクトリを CIFS 共有側で利用する場合は，ファイル名やディレクトリ名がファイルシステムに保存された名前とは異なる名前で表示されたり，名前が表示されなかったりします。また，CIFS クライアントから当該ファイルにアクセスできなかったり，意図したファイルやディレクトリにアクセスできなかったりする場合があります。そのため，CIFS クライアントと共有する場合は NFS クライアントから作成するファイルやディレクトリの名前は文字コードを UTF-8 にしてください。
  *1 制御コード：0x01 ～ 0x1f,0x22,0x2a,0x2f,0x3a,0x3c,0x3e,0x3f,0x5c,0x7c
  なお，バージョンにおける差異は下記のとおりです。

表 20-1： CIFS クライアントにエクスプローラで表示される名前

UTF-8 以外の文字コード	制御コード	5.7.0-00 より前	5.7.0-00 以降
含まない	含む	別名 *	別名 *
含む	含む	別名 *	別名 *
	含まない	別名 *	なし

* ファイルシステム上の名前とは異なる名前で表示されます。

表 20-2： CIFS クライアントからのファイルオープン / アクセス可否

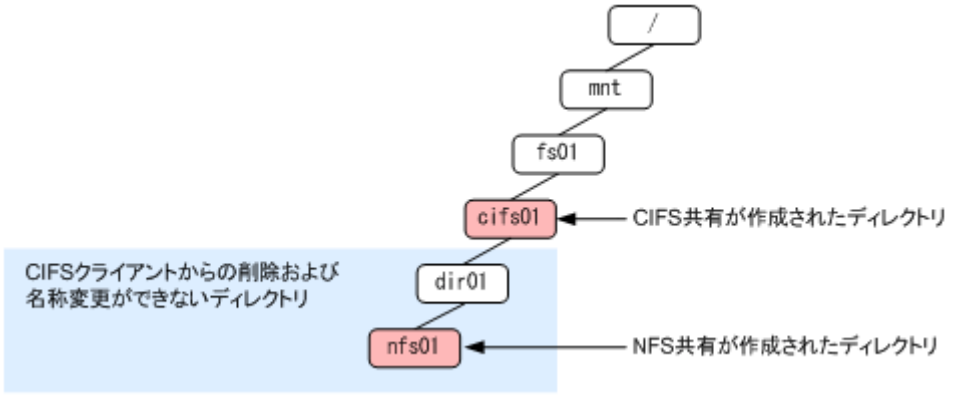
UTF-8 以外の文字コード	制御コード	5.7.0-00 より前	5.7.0-00 以降
含まない	含む	可	可
含む	含む	可	不可
	含まない	可	不可

- CIFS サービスで，ファイル所有者以外でのファイル更新日時の変更を許可すると，そのファイルに書き込み権限のあるすべてのユーザーが CIFS クライアントを経由することでファイル更新日時を変更できます。このファイルの所有者以外のユーザーによるファイル更新日時の変更は，NFS クライアントでは許可されていないため，十分注意してください。
- NFS で作成したファイルを CIFS クライアントから参照する場合 Linux の実行権（--x）は Windows のアーカイブ属性にマッピングされています。そのため，NFS 側でファイルオーナーの実行権限を削除すると Windows 側ではバックアップが完了したと誤認してしまうおそれがあります。
- 大文字と小文字が異なるだけの名称のファイルおよびディレクトリを，NFS クライアントから 1 つのディレクトリに作成しないでください。
  NFS クライアントでは大文字と小文字の違いが区別されますが，CIFS クライアントでは区別されないため，期待したファイルまたはディレクトリに CIFS クライアントからアクセスできないことがあります。

20.2 ディレクトリを操作するときの注意事項

同一のディレクトリツリー内で，NFS 共有の上位のディレクトリに CIFS 共有が作成されている場合，CIFS クライアントからは，NFS 共有と CIFS 共有の間のディレクトリと，NFS 共有が作成されているディレクトリの名称を変更したり，ディレクトリを削除したりできません。このときのディレクトリツリーの例を次の図に示します。

図 20-1： NFS 共有の上位のディレクトリに CIFS 共有が作成されているディレクトリツリーの例



20.3 ファイル共有にアクセスするユーザーの管理方法

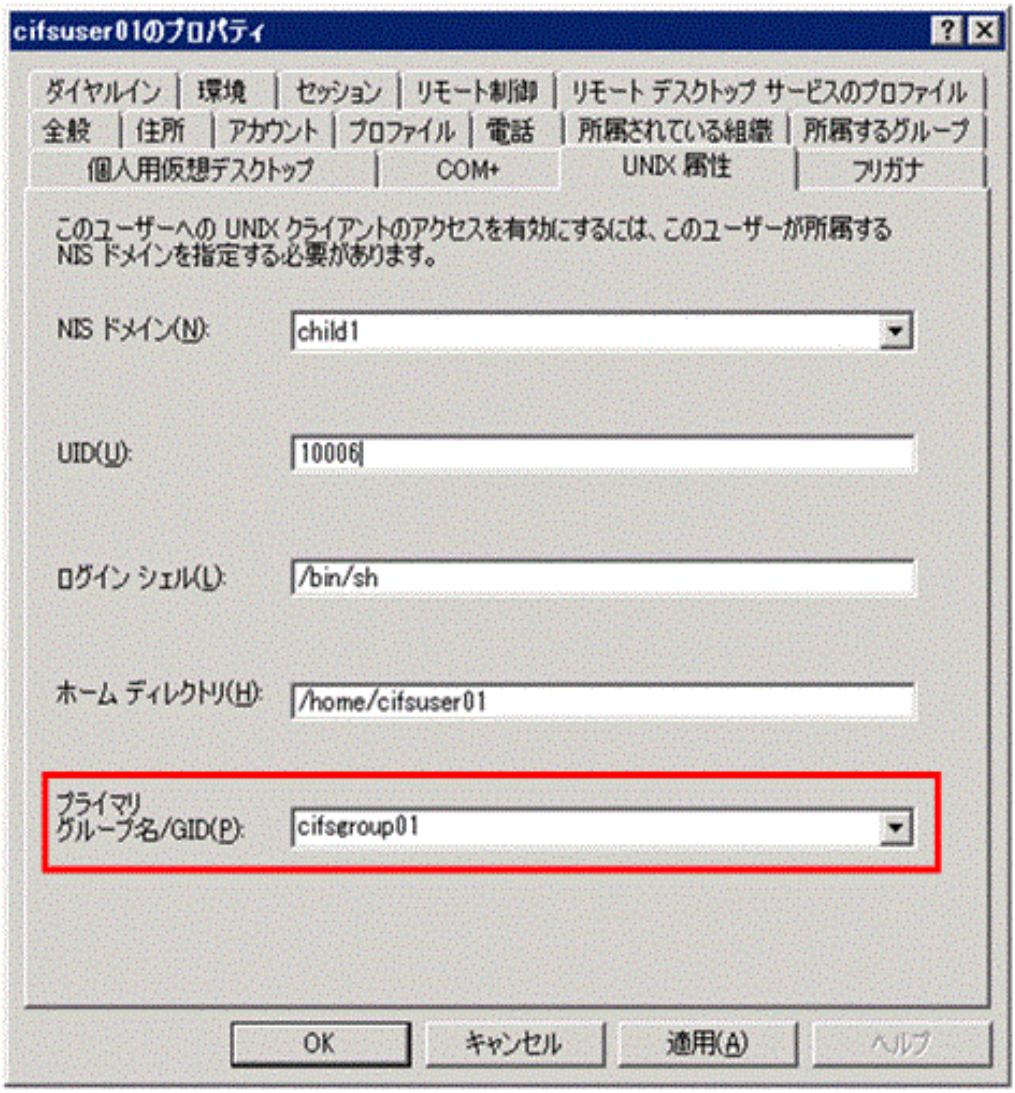
Active Directory スキーマ方式のユーザーマッピングを使用すると，ファイルまたはディレクトリを CIFS サービスと NFS サービスで共有する場合に，各サービスで使用するアカウントを同一ユーザーとして管理できます。

Active Directory スキーマ方式のユーザーマッピングを使用するときの手順を次に示します。

1. CIFS 共有へアクセスするユーザーのユーザー ID とグループ ID をドメインコントローラーに登録します。
   登録手順については，「4.5.1 Active Directory に登録するときの手順」を参照してください。グループ ID として，ユーザーが属するグループではなく，ユーザー自身の gidNumber を使用できます。
2. 管理コンソールから，HVFP が Active Directory ドメインに参加するための設定をします。
   Active Directory ドメインに参加するための手順については，「ユーザーズガイド」（IF305）を参照してください。なお，手順 1 でユーザー自身の gidNumber をグループ ID として登録した場合は，cifsoptset コマンドの use_gidnumber オプションで，ユーザー自身の gidNumber を使用するように CIFS サービスの構成定義を変更する必要があります。

ヒント ユーザー自身の gidNumber は，Active Directory のユーザーのプロパティ画面で［UNIX 属性］タブを表示すると，［プライマリグループ名 /GID］で確認できます。

図 20-2：ユーザーの［プロパティ］画面の［UNIX 属性］タブの表示例



20.4 CIFS，NFS および FTP クライアント間でファイルやディレクトリを共有する場合の注意事項

CIFS，NFS および FTP クライアント間でファイルやディレクトリを共有する場合の注意事項を次に示します。

- NFS および FTP クライアントでは，CIFS クライアントからアクセスできるパス長の上限を超えてファイルやディレクトリを作成できます。CIFS クライアントとファイルやディレクトリを共有するときは，ファイル名，ディレクトリ名，ホスト名または IP アドレス，および共有名を含むパス長が，CIFS クライアントからアクセスできるパス長の上限を超えないようにしてください。ファイルパス名およびディレクトリパス名の最大長については，「8.1.1 サポート文字」を参照してください。
- CIFS クライアントで漢字などのマルチバイト文字を使用して作成したパス長が 256 文字（1024 バイト）を超える場合，NFS クライアントからそのパスを指定してシンボリックファイルを作成すると，NFS クライアントからアクセスできるパス長の上限を超えるため，エラーになります。NFS クライアントとファイルやディレクトリを共有するときは，256 文字（1024 バイト）を超えないパス長になるようにしてください。

A

CIFS サービス利用時のトラブルシュート

CIFS サービスでのエラーなどの詳細情報は，syslog または CIFS ログに出力されます。これらに出力されるメッセージとその対処について説明します。

また，MMC 操作時のエラーと対処について説明します。さらに，CIFS サービスおよびファイル共有の設定についてよくある質問および回答を，FAQ の形式で説明します。

A.1 syslog

ここでは，/var/log/syslog に出力されるメッセージとその対処を次にまとめます。

msg=rc0=[エラーコード](hosts={[外部認証サーバ名称]}[エラー詳細])

外部認証サーバとのアクセスでエラーが発生しました。

対処方法：

外部認証サーバの設定が正しいか，または外部認証サーバが正しく起動されているか確認してください。

[[CHN番号]] error : unable to join. errno:[エラー詳細]

CHA 名称変更後のリソースグループ起動での Active Directory ドメインへの再参加に失敗しました。

対処方法：

Active Directory ドメインのドメインコントローラーとの接続が正しくできるかどうか確認してください。接続を確認後，［CIFS Service Maintenance］ページでドメインに再参加してください。

winbindd environment error. rtn=[エラーコード]

リソースグループ起動に伴う CIFS サービス起動で RID 方式のユーザーマッピング使用時の信頼関係情報取得に失敗しました。

対処方法：

Active Directory ドメインのドメインコントローラーとの接続が正しくできるかどうか確認してください。

Server: [外部認証サーバ名称], [エラー詳細].rtn=[エラーコード]

AD 方式ユーザーマッピング使用時に，外部認証サーバとのスキーマ方式の整合性チェックでエラーが発生しました。

対処方法：

CIFS サービスのユーザーマッピングで使用するネームサービススイッチの設定と，外部認証サーバが使用しているネームサービススイッチが正しいかどうかを確認してください。

cifs.init [CHN 番号]: Warning. Virtual IP address is not defined.

仮想 IP アドレスが設定されていない状態で CIFS サービスが起動（再起動を含む）されました。CIFS サービスは起動されますが，CIFS アクセスはできません。

対処方法：

CIFS アクセスをするには，仮想 IP アドレスを設定してください。

A.2 CIFS ログ

ここでは，CIFS ログ（log.smbd，log.winbindd）に出力されるメッセージとその対処について説明します。

A.2.1 log.smbd

/var/log/cifs/log.smbd に出力されるメッセージとその対処を次にまとめます。

```
Failed to join domain: Invalid configuration ("realm" set to '[指定されたドメイン名]', should be '[ドメインコントローラー側のドメイン名]') and configuration modification was not requested
```

指定されたドメイン名称（DNS 名）が指定されたドメインコントローラー側のドメイン名と一致しません。

対処方法：

ドメイン名称（DNS 名）またはドメインコントローラーを見直し，正しい値を設定して再度実行してください。

```
Connection denied from [クライアントのIPアドレス]
```

クライアントからのコネクションが拒否されました。

対処方法：

次について見直し，必要に応じて設定を変更，または CIFS クライアントからのアクセス状況を調査してください。

- ［Host access restrictions］または［ホスト / ネットワークによるアクセス制限］で該当するクライアントのアクセスが拒否されていないかどうか。
- 接続しているクライアント数が上限値を超えていないかどうか。

```
allowable_number_of_smbd_processes: number of processes ([起動しようとしたプロセス数]) is over allowed limit ([最大プロセス数])
```

接続しているクライアント数が上限を超えました。

対処方法：

CIFS クライアントからのアクセス状況を調査してください。

```
write_socket_data: write failure. Error = Connection reset by peer
write_socket: Error writing {書き込みサイズ} bytes to socket {ディスクリプタ}: ERRNO = Connection reset by peer
Error writing {書き込みサイズ} bytes to client. {戻り値}. (Connection reset by peer)
getpeername failed. Error was Transport endpoint is not connected
```

クライアントからコネクションが切断されました。

対処方法：

タイムアウトなどのためにクライアントからコネクションを切断しました。しばらく経ってから再度 CIFS アクセスしてください。

```
Failed to verify incoming ticket with error
smb2: Failed to verify incoming ticket with error
```

Active Directory ドメインでユーザー認証に失敗しました。

対処方法：

ドメインコントローラー，HVFP のノードまたは Virtual Server および CIFS クライアントの時刻がずれていないかどうかを調査し，時刻がずれている場合は修正してください。また，HVFP のノードまたは Virtual Server をドメインに再参加する前に CIFS アクセスしていないかどうかを調査し，ドメイン再参加前に CIFS アクセスをしている場合は，CIFS クライアントでいったんログオフし，ログインし直してください。

前述に該当しない場合，HVFP のノードまたは Virtual Server をドメインに再参加させてください。

```
Username [ユーザー名] is invalid on this system
smb2: Username [ユーザー名] is invalid on this system
```

ユーザーのアカウントが登録されていません。

対処方法：

次について見直し，必要に応じて設定を変更してください。
ユーザーマッピングを使用しない場合，Active Directory（または CIFS クライアント）に登録されているユーザーアカウントを File Services Manager 上に作成する必要があります。同じユーザーアカウントが，File Services Manager と Active Directory（または CIFS クライアント）の両方に登録されているか確認してください。
ユーザーマッピングを使用していた場合，ユーザー ID，グループ ID の範囲超過，LDAP サーバへのアクセス不正などが考えられます。ユーザーマッピングに関する設定を見直してください。なお，Active Directory スキーマ方式のユーザーマッピングの場合は，Active Directory にユーザー ID やグループ ID が設定されていないことが考えられます。必要なユーザー ID やグループ ID を Active Directory に登録してください。詳細は，「4.5.1 Active Directory に登録するときの手順」を参照してください。

```
create_canon_ace_lists: Some ACEs were skipped. file = [ファイルパス名], SID = [該当ACEのSID]
```

ACL 設定時に，SID から UID，GID への変換に失敗する ACE をスキップして設定しました。

対処方法：

次について見直し，必要に応じて ACL を再設定してください。
ドメインから削除されたアカウントの ACE が ACL に含まれる場合に出力されます。ドメインにアカウントが存在しない場合は，SID を UID，GID に変換できないため，該当の ACE は設定できません。ただし，このメッセージが出力されても，該当の ACE 以外の ACL は設定されます。
ドメインにアカウントが存在する場合でも，このメッセージが出力される場合は，ユーザーマッピング機能が正しく動作していないおそれがあります。log.winbindd のメッセージを確認してください。

```
create_canon_ace_lists: Can't set ACL. All ACEs were skipped. file = [ファイルパス名], SID = [該当ACEのSID]
```

ACL 設定時に，すべてのエントリーについて SID から UID，GID への変換が失敗し，ACL 設定が行えませんでした。

対処方法：

次について見直し，必要に応じて ACL を再設定してください。
ユーザーマッピング機能が正しく動作していないおそれがあります。log.winbindd のメッセージを確認してください。
ACL のすべての ACE が，ドメインから削除されたアカウントである場合にも出力されます。ドメインにアカウントが存在しない SID は UID，GID に変換できないため，該当の ACE は設定できません。

```
ads_secrets_verify_ticket: authentication fails for clock skew too great.
```

ドメインコントローラー，HVFP のノードまたは Virtual Server，および CIFS クライアントの時刻が 5 分以上ずれているため，Kerberos 認証に失敗しました。

対処方法：

ドメインコントローラー，HVFP のノードまたは Virtual Server，および CIFS クライアントの時刻を調査し，ずれを修正してください。

A.2.2 log.winbindd

/var/log/cifs/log.winbindd に出力されるメッセージとその対処を次にまとめます。

idmap_rid_sid_to_id: [ユーザーまたはグループのRID] ([UIDまたはGID]: [ユーザーIDまたはグループID]) too high for mapping of domain: [ドメイン名] ([ドメインでの最小値] -[ドメインでの最大値])

ユーザーマッピング（RID 方式）で割り当てるユーザー ID またはグループ ID が指定されている範囲外です。

対処方法：

該当するドメインのユーザー ID またはグループ ID の範囲を拡張するかもしくは変更してください。

Did not find domain [ドメイン名]

ユーザーマッピングで設定されていないドメインのユーザーでアクセスしています。

対処方法：

該当するドメインのユーザー ID およびグループ ID として使用する範囲を追加してください。

Cannot allocate [UIDまたはGID] above [ユーザーIDまたはグループIDの最大値]!

ユーザーマッピング（自動割り当ての LDAP 方式）で割り当てるユーザー ID またはグループ ID が指定されている範囲外です。

対処方法：

ユーザーマッピングで使用するユーザー ID またはグループ ID の範囲を拡張するかもしくは変更してください。

A [UIDまたはGID] ([UID値またはGID値]) that is out of available range was used (200 - 2147483147). (Name = [SID])

ユーザーマッピング（手動割り当ての LDAP 方式）で LDAP サーバに登録されているユーザー ID またはグループ ID が使用範囲外（200 ～ 2147483147 の範囲外）です。

対処方法：

LDAP サーバに登録されている，そのユーザーまたはグループの UID もしくは GID の値を，200 ～ 2147483147 の範囲内にしてください。

failed to bind to server ldap://[LDAPサーバのIPアドレス]:[LDAPサーバのポート番号] with dn="[LDAPサーバ管理者DN]" Error: [エラー詳細]

ユーザーマッピング（LDAP 方式）で LDAP サーバへのアクセスに失敗しました。

対処方法：

指定した［LDAP server name］または［LDAP server port number］が正しいかどうか，LDAP サーバが正しく稼働しているかどうかを確認してください。

ads_connect for domain [NetBIOS ドメイン名称] failed: [エラー詳細]

Active Directory ドメインのドメインコントローラーへの接続が失敗しました。

対処方法：

指定した［DC server name(s)］が正しいかどうか，ドメインコントローラーが正しく稼働しているかどうかを確認してください。

```
rpc_np_trans_done: return critical error. Error was [エラー詳細]
```

Active Directory ドメインのドメインコントローラーへの接続が切断されました。

対処方法：

指定した［DC server name(s)］，［PDC server name］または［BDC server name］が正しいかどうか，ドメインコントローラーが正しく稼働しているかどうかを確認してください。

```
cli_start_connection: failed to connect to [ドメインコントローラーのコンピュータ名]<20> (0.0.0.0)
```

ドメインコントローラーの名前解決に失敗しました。

対処方法：

HVFP でドメインコントローラーを名前解決できるように，DNS または lmhosts などに登録してください。詳細は，「システム構成ガイド」（IF302）を参照してください。

```
A [UIDまたはGID] ([UID値またはGID値]) that is out of available range was used (200 - 2147483147). (Name = [sAMAccountNameの属性値])
```

AD 方式ユーザーマッピングで外部認証サーバに登録されているユーザー ID またはグループ ID が使用範囲外（200 ～ 2147483147 の範囲外）です。

対処方法：

外部認証サーバに登録されている，そのユーザーまたはグループの UID もしくは GID の値を，200 ～ 2147483147 の範囲内にしてください。

```
Could not get unix ID of SID = [変換するSID], name = [ユーザー名], type = 30000000
```

［ユーザー名］のユーザー ID の取得に失敗しました。

対処方法：

考えられる原因と対処を次に示します。

Name service switch の設定が不一致である。

対処：

［CIFS Service Management］ページ（Setting Type：User mapping）の［Name service switch］で，CIFS サービスの構成定義の設定を見直してください。

ドメインコントローラーに［ユーザー名］のユーザー ID が手動登録されていない。

対処：

ドメインコントローラーに［ユーザー名］のユーザー ID を登録してください。

```
Could not get unix ID of SID = [変換するSID], name = [グループ名], type = 10000000
```

［グループ名］のグループ ID の取得に失敗しました。

対処方法：

考えられる原因と対処を次に示します。

Name service switch の設定が不一致である。

対処：

［CIFS Service Management］ページ（Setting Type：User mapping）の［Name service switch］で，CIFS サービスの構成定義の設定を見直してください。

ドメインコントローラーに［グループ名］のグループ ID が手動登録されていない。

対処：
ドメインコントローラーに［グループ名］のグループ ID を登録してください。

グループ ID としてユーザー自身の gidNumber を使用するように設定されていない。

対処：
cifsoptlist コマンドで，グループ ID としてユーザー自身の gidNumber を使用するように CIFS サービスの構成定義の設定を見直してください。

```
No gidNumber for [変換するSID] !?
```

［変換する SID］の gidNumber の取得に失敗しました。

対処方法：

ドメインコントローラーに登録したユーザーのグループ ID として，ユーザー自身の gidNumber を指定してください。または，cifsoptlist コマンドで，グループ ID としてユーザー自身の gidNumber を使用するように CIFS サービスの構成定義の設定を見直してください。

```
Could not fetch our SID - did we join?
```

Active Directory ドメインへの参加に失敗しています。

対処方法：

［CIFS Service Maintenance］ページの［Rejoin Active Directory Domain］ボタンをクリックして，Active Directory ドメインに再参加してください。

```
add_failed_connection_entry: added domain [ドメイン名] ([IP アドレス]) to failed conn cache
```

HVFP と通信できないドメインコントローラーがドメイン内に存在しているため，CIFS クライアントからの認証処理が遅延しているおそれがあります。

対処方法：

［IP アドレス］に対応するドメインコントローラーが正しく稼働しているか，または HVFP と通信できるかを確認してください。
なお，CIFS クライアント認証時に HVFP からドメインコントローラーへの接続処理によって頻繁にタイムアウトが発生している場合は，対象のドメインコントローラーへの通信を抑止することで CIFS クライアント認証処理の遅延を改善できます。cifsoptset コマンドで，［IP アドレス］に対応するドメインコントローラーへの通信を抑止するように設定してください。

A.3 MMC 操作時のエラーと対処

ここでは，MMC から CIFS 共有の操作をした際に発生するエラーのうち，Windows が表示するエラーメッセージからその原因を判断するのに難しいと思われるものについて，原因の詳細と対策についてまとめます。

なお，エラー画面および操作画面の図は，Windows Server 2012 R2，MMC 3.0 を使用した場合の例です。

A.3.1 共有の追加操作でのエラー

MMC から共有を追加する操作で，共有の作成に失敗した理由が，アクセス拒否の場合についてまとめます。

エラー画面例：

図 A-1： 共有の作成に失敗した際の画面例

原因と対処：

次に挙げる原因が考えられます。各原因の詳細，その際に出力されるメッセージ，対処を示します。

操作権限がない

原因詳細：
MMC から CIFS 共有を操作する権限がありません。
/var/log/syslog に出力されるメッセージ：
特になし
/var/log/cifs/log.smbd に出力されるメッセージ：
特になし
対処：
File Services Manager で登録された CIFS 管理者が操作してください。

不正なファイルシステムを指定した

原因詳細：
共有のパスに，もう一方のノードで作成したファイルシステムを指定しました。
/var/log/syslog に出力されるメッセージ：
`cifs_addshare : Invalid filesystem specified (filesystem=[` 指定したファイルシステム名 `]). Filesystem belongs to CHN[`CHN 番号 `]. Own CHN is CHN[`CHN 番号 `]`
対処：

共有のパスに，操作対象としているノードで作成したファイルシステムを指定してください。

存在しないファイルシステムを指定した

原因詳細：
共有のパスに，存在しないファイルシステムを指定しました。
/var/log/syslog に出力されるメッセージ：
`cifs_addshare : error /enas/bin/cifs_fsname2chnnum(ret=2,fsname=[` 指定したファイルシステム名 `])`
対処：
正しい共有のパスを指定してください。

cifscreate コマンドがエラー終了した

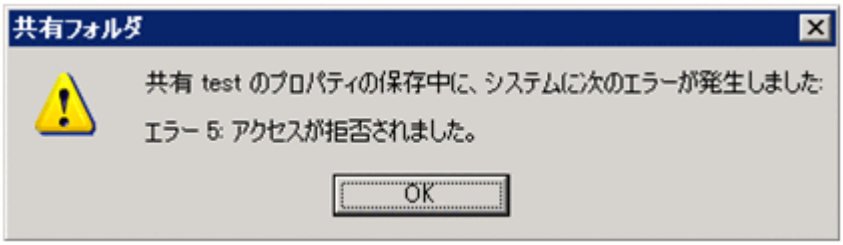
原因詳細：
共有の作成に使用した `cifscreate` コマンドがエラー終了しました。
/var/log/syslog に出力されるメッセージ：
`cifs_addshare : error cifscreate: [`cifscreate コマンドの戻り値 `].`
対処：
`cifscreate` コマンドのエラー要因を取り除いてください。`cifscreate` コマンドのログは，File Services Manager トレースログ（`/enas/log/management.trace`）に出力されます。File Services Manager トレースログを確認してください。

A.3.2 共有のプロパティ変更時のエラー

MMC から共有のプロパティを変更する操作で，共有のプロパティの変更に失敗した理由が，アクセス拒否の場合についてまとめます。

エラー画面例：

図 A-2：共有のプロパティ操作に失敗した際の画面例



原因と対処：

次に挙げる原因が考えられます。各原因の詳細，その際に出力されるメッセージ，対処を示します。

操作権限がない

原因詳細：
MMC から CIFS 共有を操作する権限がありません。
/var/log/syslog に出力されるメッセージ：
特になし
/var/log/cifs/log.smbd に出力されるメッセージ：
特になし
対処：
File Services Manager で登録された CIFS 管理者が操作してください。

cifsedit コマンドがエラー終了した

原因詳細：
共有の編集に使用した cifsedit コマンドがエラー終了しました。
/var/log/syslog に出力されるメッセージ：
cifs_chgshare : error cifsedit: [cifsedit コマンドの戻り値].
対処：
cifsedit コマンドのエラー要因を取り除いてください。cifsedit コマンドのログは，File Services Manager トレースログ（/enas/log/management.trace）に出力されます。File Services Manager トレースログを確認してください。

A.3.3 共有の停止時のエラー

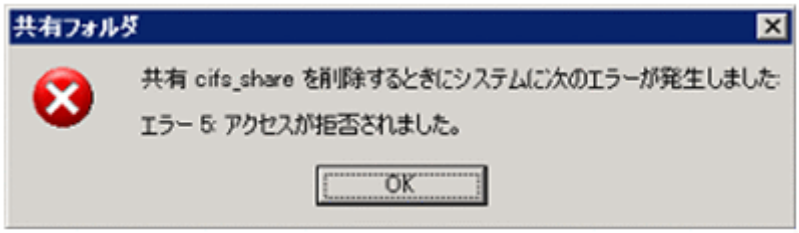
MMC から共有の停止をする（削除する）場合に発生するエラーについて，次にまとめます。

A.3.3.1 アクセス拒否によって共有の停止操作に失敗する

共有の停止に失敗した理由が，アクセス拒否の場合についてまとめます。

エラー画面例：

図 A-3： 共有の停止操作に失敗した際の画面例



原因と対処：

次に挙げる原因が考えられます。各原因の詳細，その際に出力されるメッセージ，対処を示します。

操作権限がない

原因詳細：
MMC から CIFS 共有を操作する権限がありません。
/var/log/syslog に出力されるメッセージ：
特になし
/var/log/cifs/log.smbd に出力されるメッセージ：
特になし
対処：
File Services Manager で登録された CIFS 管理者が操作してください。

cifsdelete コマンドがエラー終了した

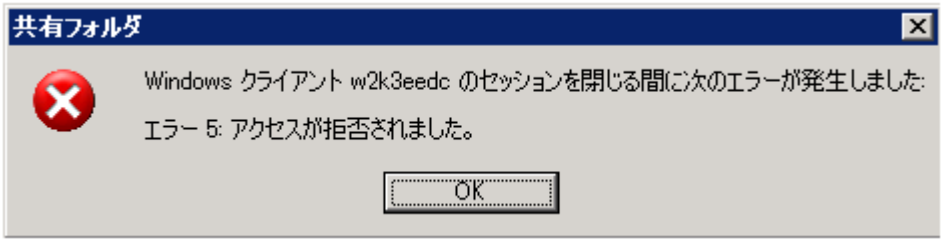
原因詳細：
共有の停止に使用した cifsdelete コマンドがエラー終了しました。
/var/log/syslog に出力されるメッセージ：
cifs_delshare : error cifsdelete: [cifsdelete コマンドの戻り値].
対処：
cifsdelete コマンドのエラー要因を取り除いてください。cifsdelete コマンドのログは，File Services Manager トレースログ（/enas/log/management.trace）に出力されます。File Services Manager トレースログを確認してください。

A.3.3.2 アクセス拒否によってセッションの切断操作に失敗する

セッションの切断に失敗した理由が，アクセス拒否の場合についてまとめます。

エラー画面例：

図 A-4： セッションの切断に失敗した際の画面例



原因と対処：

次に挙げる原因が考えられます。各原因の詳細，その際に出力されるメッセージ，対処を示します。

操作権限がない

原因詳細：
MMC からセッションの切断を操作する権限がありません。
/var/log/syslog に出力されるメッセージ：
特になし
/var/log/cifs/log.smbd に出力されるメッセージ：
特になし
対処：
File Services Manager で登録された CIFS 管理者が操作してください。

操作対象のセッションが存在しない

原因詳細：
切断しようとしたセッションは，存在しません。
/var/log/syslog に出力されるメッセージ：
特になし
/var/log/cifs/log.smbd に出力されるメッセージ：
特になし
対処：
最新の情報を表示し，セッションの状態を確認してください。

A.3.4 開いているファイルを閉じる操作でのエラー

開いているファイルを MMC から閉じる操作をしたときに，失敗した理由がアクセス拒否の場合について示します。

エラー画面例：

図 A-5： ファイルを閉じる操作に失敗した際の画面例

原因と対処：

次に挙げる原因が考えられます。原因の詳細，その際に出力されるメッセージ，対処を示します。

操作権限がない

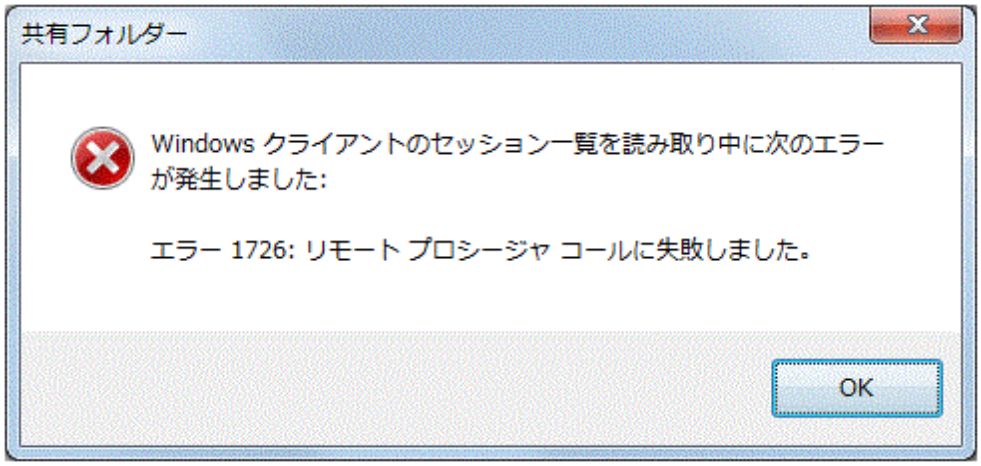
原因詳細：
MMC から開いているファイルを操作する権限がありません。
/var/log/syslog に出力されるメッセージ：
特になし
/var/log/cifs/log.smbd に出力されるメッセージ：
特になし
対処：
File Services Manager で登録された CIFS 管理者が操作してください。

A.3.5 セッションを表示する操作でのエラー

MMC からセッションを表示する操作をしたときに，失敗した理由がリモートプロシージャコール失敗の場合について示します。

エラー画面例：

図 A-6： セッションを表示する操作に失敗した際の画面例



原因と対処：

次に挙げる原因が考えられます。原因の詳細，その際に出力されるメッセージ，対処を示します。

タイムアウトが発生した。

原因詳細：

セッション情報の表示に時間が掛かるため，CIFS クライアントでタイムアウトが発生しました。

/var/log/syslog に出力されるメッセージ：

特になし

/var/log/cifs/log.smbd に出力されるメッセージ：

特になし

対処：

CIFS クライアントがタイムアウトするまでの時間を長くしてください。

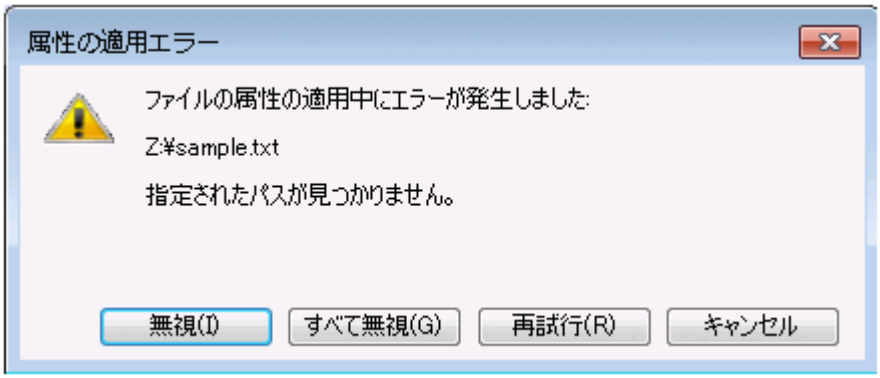
タイムアウトするまでの時間を長くする方法は，Microsoft のサポートに問い合わせてください。

A.4 ファイル操作時のエラーと対処

ここでは，エクスプローラから CIFS 共有の操作をした際に発生するエラーのうち，Windows が表示するエラーメッセージからその原因を判断するのに難しいと思われるものについて，原因の詳細と対策についてまとめます。

エラーメッセージ「指定されたパスが見つかりません。」が表示される場合

図 A-7：エラーメッセージ「指定されたパスが見つかりません。」の表示例



原因と対処：

考えられる原因と対処を次に示します。

クライアントと HVFP の間で通信障害が発生している

対処：

クライアントと HVFP の間の通信状態を確認し，HVFP に再接続したり，クライアントにログオンし直したりして，再度アクセスしてください。

クライアント側でネットワークドライブが切断されている

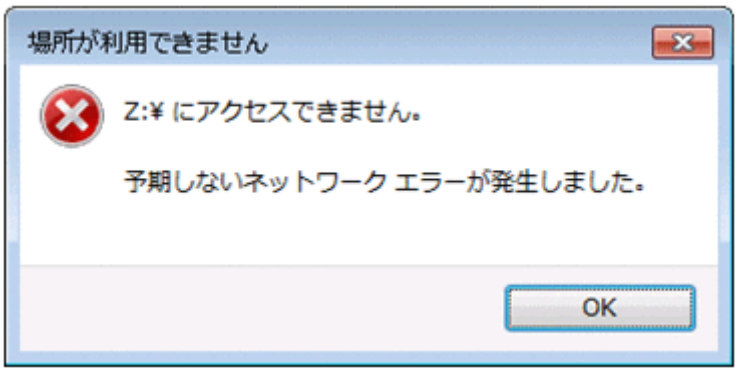
対処：

クライアント側で割り当てたネットワークドライブが切断されていることが考えられます。ネットワークドライブを再度割り当ててください。

エラーメッセージ「予期しないネットワークエラーが発生しました。」が表示される場合

クライアント側で割り当てたネットワークドライブから CIFS サービスにアクセスした際に表示されることがあります。

図 A-8：エラーメッセージ「予期しないネットワークエラーが発生しました。」の表示例



原因と対処：

考えられる原因と対処を次に示します。

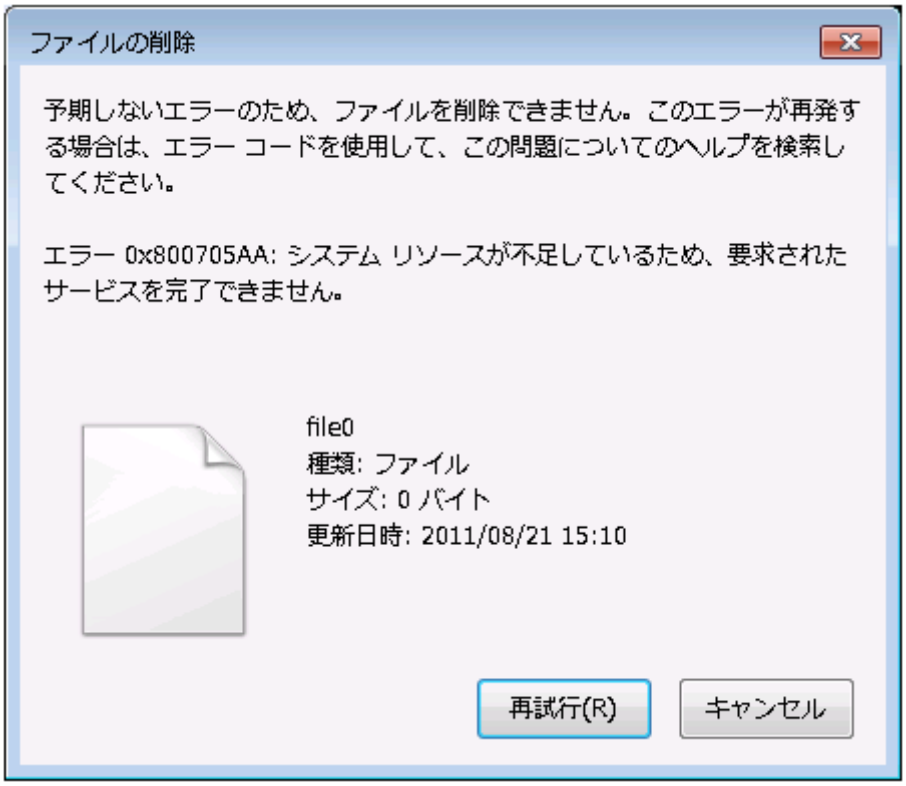
CIFS サービスへのアクセス中に CIFS サービスの再起動，フェールオーバーまたはフェールバックによってセッションが一時的に切断された。

対処：

クライアント側で割り当てたネットワークドライブをいったん切断し，再度割り当ててからアクセスし直してください。

エラーメッセージ「システム リソースが不足しているため，要求されたサービスを完了できません。」が表示される場合

図 A-9：エラーメッセージ「システム リソースが不足しているため，要求されたサービスを完了できません。」の表示例



原因と対処：

考えられる原因と対処を次に示します。

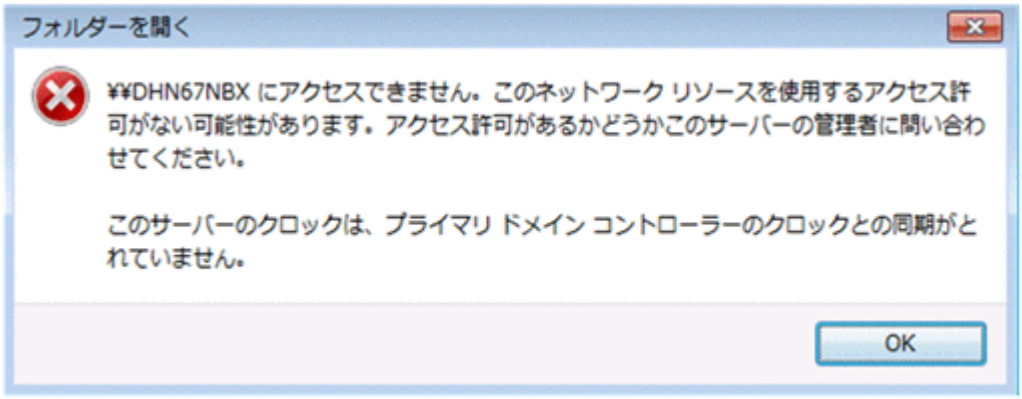
短期間にファイルハンドルの open/close が繰り返された結果，クライアント側でシステムリソース不足が発生した。

対処：

クライアントを再起動するか，しばらく経ってから再試行してください。

エラーメッセージ「このサーバーのクロックは，プライマリ ドメインコントローラーのクロックとの同期がとれていません。」が表示される場合

図 A-10：エラーメッセージ「このサーバーのクロックは，プライマリ ドメインコントローラーのクロックとの同期がとれていません。」の表示例



原因と対処：

考えられる原因と対処を次に示します。

ドメインコントローラー，HVFP のノードまたは Virtual Server，および CIFS クライアントの時刻が同期されていないため，ユーザー認証に失敗した。

対処：

ドメインコントローラー，HVFP のノードまたは Virtual Server，および CIFS クライアントの時刻を同期させてください。また，時刻を同期させたあと，CIFS クライアントはいったんログオフし，ログインし直してください。

SMB2.0 を使用した Windows クライアントから，CIFS 共有のフォルダまたはファイルを正しく参照できない場合

例：

- CIFS 共有にフォルダまたはファイルを作成したあと，クライアントからそのフォルダまたはファイルを参照できない
- CIFS 共有のファイルを削除しようとしても削除できない

原因と対処：

考えられる原因と対処を次に示します。

一時的な障害または Windows に問題が発生している。

対処：

次のどちらかの方法で対処してください。

方法 1

しばらく経ってから再試行してください。

方法 2

SMB2.0 を使用してフォルダまたはファイルを正しく参照できないことを，Microsoft のサポートに問い合わせてください。

CIFS 共有のフォルダまたはファイルにアクセスしたとき，または net view コマンドで共有名を一覧表示したときにエラーメッセージが表示される場合

例：

- net use コマンドで「システム エラー 2148073478 が発生しました。」が表示される。
- dir コマンドを UNC パスに使用した場合に「署名が無効です。」が表示される。
- これらの操作以外で，エラーメッセージ「拡張エラーが発生しました。」が表示される。
- net view コマンドで「システム エラー ネットワークパスが見つかりません。」が表示される。

原因と対処：

考えられる原因と対処を次に示します。

SMB 3.0 を使用しないように設定した HVFP に対して，CIFS クライアントから SMB 3.0 の Secure Negotiate 要求が行われた。

対処：

HVFP の［CIFS Service Management］ページ（Setting Type：Basic）で，CIFS クライアントからのアクセスに対して SMB 3.0 を使用するように設定してください。

ファイル作成時にエラーメッセージ「指定されたサーバーは、要求された操作を実行できません。」が表示される場合

原因と対処：

考えられる原因と対処を次に示します。

- 作成されるファイルのサイズがファイルシステムの空き容量を超える
- 指定されたサイズのファイルを作成すると Quota のブロックの使用量がハードリミットを超える

対処：

ファイルシステムの使用量および Quota のブロック使用量を確認し，ファイルシステムまたはブロックの空き容量を増やしてからファイルを作成するか，別のファイルシステムやフォルダにファイルを作成してください。
なお，cifsoptset コマンドを使用して，作成または上書きするファイルにデータを書き込む前に，ファイルシステムの空き容量があることをチェックするように設定することで，ファイル作成時にエラーメッセージ「ディスクに十分な空き容量がありません。」が表示されるようになる場合があります。

ドメインユーザから CIFS サービスへのアクセスが断続的に不可となり，システムメッセージに KAQG52019-E または KAQG52018-W が出力される場合

原因と対処：

考えられる原因と対処を次に示します。

- HVFP とドメインコントローラー間で時刻が同期されていない。
- HVFP が参照する DNS サーバの SRV レコードに，接続できないドメインコントローラーが存在する。

対処：

HVFP とドメインコントローラー間で時刻同期がされていない場合
　HVFP とドメインコントローラー間の時刻を同期してください。
HVFP とドメインコントローラー間の時刻が同期されている場合

HVFP と通信できないドメインコントローラーが存在しているおそれがあります。
KAQG52019-E または KAQG52018-W で表示されたドメインコントローラーと HVFP が通信できるか確認してください。通信経路の遮断や装置の障害などによって，一時的もしくは恒久的にドメインコントローラーと通信ができなくなっている場合，通信できるように問題を取り除いてください。
ドメインコントローラーと通信できない問題を取り除けない場合は次のどちらかの方法で対処してください。
・通信できないドメインコントローラーの SRV レコードを DNS サーバから削除してください。
・HVFP のルーティング機能を使用して，通信できないドメインコントローラーへのアクセスを拒否し，通信できないドメインコントローラーへ問い合わせをしないようにしてください。HVFP のルーティング機能については，「コマンドリファレンス」または「ユーザーズガイド」を参照ください。

A.5 FAQ

ここでは，CIFS サービスおよびファイル共有の設定についてよくある質問および回答を記載しています。回答で説明している各 GUI 項目の操作方法については，「ユーザーズガイド」（IF305）を参照してください。

A.5.1 CIFS アクセスの性能をチューニングできますか？

デフォルトでは，クローズ要求に同期してディスクドライブに書き込むよう設定されています。書き込むデータの量が多い場合は，一定周期で書き込むように設定することで，性能が向上することがあります。

CIFS クライアントからの書き込み要求に対する動作の設定は，すべてのファイル共有に対するデフォルト設定と，各ファイル共有に対する設定の 2 種類があります。

すべてのファイル共有に対するデフォルト設定を，一定周期で書き込むようにする方法

［CIFS Service Management］ページ（Setting Type：Performance）の［CIFS default setup］で，［Disk synchronization policy］に［Routine disk flush only］を指定します。

各ファイル共有に対する設定を，一定周期で書き込むようにする方法

［共有編集］ダイアログの［アドバンスド］タブの［CIFS］サブタブで，［同期書き込みポリシー］に［定期的なディスクフラッシュだけ］を指定します。なお，［CIFS サービスのデフォルトに従う］を指定するとデフォルト設定に従って書き込むよう設定されます。今後ファイル共有を追加する場合は，［ファイルシステム構築と共有作成］ダイアログまたは［共有追加］ダイアログで同様に指定します。

CIFS クライアントからの書き込み動作の詳細については，「ユーザーズガイド」（IF305）を参照してください。

A.5.2 Windows の administrator のようなアカウントを設定できますか？

［CIFS Service Management］ページ（Setting Type：Administration）の［CIFS service setup］の［CIFS administrator name(s)］で CIFS 管理者として登録したユーザーまたはグループに属するユーザーは，Windows の Administrator と同じように，すべてのファイルやフォルダにアクセスできます。つまり，HVFP 上で root ユーザーとして扱われるので注意してください。なお，「Administrator」または「Administrators」という名称のユーザーまたはグループであっても，

CIFS 管理者として登録されていなければ，ファイルシステムの ACL タイプやユーザー認証方式に関わらず，一般のユーザーまたはグループとして扱われます。

ユーザーマッピングを使用している場合は，次のようにユーザー名またはグループ名にドメイン名を付けて指定します。

＜ドメイン名＞¥＜ユーザー名＞
@＜ドメイン名＞¥＜グループ名＞

A.5.3 「Direct Hosting of SMB」だけを使用して CIFS サービスを運用できますか？

CIFS クライアントからのアクセスを受け付ける方法として，「NetBIOS over TCP/IP」および「Direct Hosting of SMB」の両方からアクセスを受け付けるか，「Direct Hosting of SMB」だけからアクセスを受け付けるかを選択できます。

「Direct Hosting of SMB」だけからアクセスを受け付ける場合は，［CIFS Service Management］ページ（Setting Type：Security）の［CIFS service setup］で，［NetBIOS over TCP/IP］に［Do not use］を指定します。

A.5.4 CIFS クライアントから ACL を設定・参照するためのセキュリティタブを表示できますか？

ファイル共有が存在するファイルシステムが Classic ACL タイプの場合，［共有編集］ダイアログの［アクセス制御］タブの［CIFS］サブタブで，［ACL を有効にする］に［はい］を指定すると，CIFS クライアントから，ファイル共有内のファイルまたはフォルダのプロパティダイアログにセキュリティタブを表示できます。今後ファイル共有を追加する場合は，［ファイルシステム構築と共有作成］ダイアログまたは［共有追加］ダイアログで同様に指定します。

なお，Advanced ACL タイプのファイルシステムの場合は，常にセキュリティタブが表示されます。

A.5.5 ファイルシステムごとにアクセスできるユーザーを制限できますか？

ファイルシステムごとにはできませんが，ファイル共有ごとにアクセスできるユーザーおよびグループを，次のとおり設定することによって制限できます。

- 読み取りおよび書き込みを許可するユーザーおよびグループを指定する
- 読み取りだけを許可するユーザーおよびグループを指定する

ただし，ファイル共有が存在するファイルシステムが読み取り専用でマウントされている場合は，書き込みを許可するユーザーおよびグループを設定しても，書き込みは無効になります。

［共有編集］ダイアログの［アクセス制御］タブの［CIFS］サブタブの［特別に権限設定されたユーザー / グループ］で設定を変更できます。今後ファイル共有を追加する場合は，［ファイルシステム構築と共有作成］ダイアログまたは［共有追加］ダイアログで同様に指定します。

なお，ユーザーマッピングを使用している場合は，コマンドでだけ設定できます。

A.5.6 ファイル共有へのアクセスに時間が掛かることがあります。原因として何が考えられますか？

複数ドメインから HVFP を利用している場合に，ユーザーからのアクセスに時間が掛かるときは，ドメインの信頼関係の構成と，設定されている CIFS サービスの構成定義が一致していないことが

原因として考えられます。ドメインの構成に合わせてCIFSサービスの構成定義を変更してください。CIFSサービスの構成定義の変更については，「ユーザーズガイド」（IF305）を参照してください。

A.5.7 スキャンソフトでオンアクセススキャン機能を有効にしているときに，CIFS共有内のファイルにアクセスすると，「ファイルを開くことができません。」というエラーメッセージが表示されました。

CIFSクライアント側で使用しているスキャンソフトのオンアクセススキャン機能を有効にすると，同時にオープンするファイルが増えるため，上限に達してエラーとなることがあります。オンアクセススキャン機能を無効にすることで，エラーを回避できることがあります。

A.5.8 ファイルまたはフォルダのプロパティ画面のセキュリティタブで，ユーザー名やグループ名ではなくSIDが表示されます。原因として何が考えられますか？

HVFPでは片方向の信頼関係をサポートしていません。片方向の信頼関係ドメインを使用したことが原因として考えられます。このほかに考えられる原因を次に示します。

HVFPのノードまたはVirtual Serverが参加しているドメインから対象のユーザーやグループを削除した。

ユーザーやグループをいったん削除したあとで再登録している場合は，再登録の際に割り当てられたSIDが表示されます。

HVFPのノードまたはVirtual Serverが参加しているドメインと双方向の信頼関係を結んだドメインにアクセスできない。

ドメインが削除または降格されているか，ドメインコントローラーの電源が入っていないおそれがあります。ドメインの状態を確認してください。

ドメインの構成や，登録されているユーザーやグループについては，ドメイン管理者に確認してください。

A.5.9 CIFSクライアントで正しく上書き保存されたMicrosoft Officeファイルが，ほかのCIFSクライアントでは一時ファイル（.tmp）として表示されます。原因として何が考えられますか？

CIFSクライアントで，オフラインファイル機能を使用していることが原因として考えられます。なお，オフラインファイル機能はクライアントサイドキャッシュ（CSC）とも呼ばれます。

ほかのCIFSクライアントからも正しく表示されるようにするためには，ファイルを保存したCIFSクライアントの同期センターで，対象のファイルを同期する必要があります。詳細はMicrosoftのサポートに問い合わせてください。

オフラインファイル機能を使用できないようにすることで再発を防ぐことができます。次のどれかの方法で対処してください。

- CIFS共有内のファイルの更新データをクライアントにキャッシュしないよう，HVFPでCIFS共有の設定を変更します。ただし，CIFS共有内のファイルの更新データをクライアントにキャッシュしないようにすると，CIFSクライアントからのアクセスに時間が掛かるよう

になります。設定を変更する方法については，「ユーザーズガイド」（IF305）を参照してください。

- CIFS 共有内のファイルやプログラムをオフラインのユーザーが利用できないよう，MMC で CIFS 共有の設定を変更します。設定を変更する方法については，「9.5.3 CIFS 共有の情報の変更」を参照してください。
- CIFS クライアントでオフラインファイル機能を無効にします。詳細は Microsoft のサポートに問い合わせてください。

A.5.10 ファイルを作成した直後に対象のファイルが見つからなかったり，ファイルを削除した直後に対象のファイルがみつかったりします。原因として何が考えられますか？

クライアントでファイルやフォルダの情報をキャッシュする SMB2 Client redirector キャッシュの影響が考えられます。SMB2 Client Redirector キャッシュは，クライアントのレジストリによって無効にすることができます。詳細は Microsoft のサポートに問い合わせてください。

B

NFS サービス利用時のトラブルシュート

NFS サービスの利用時に発生するエラーと対処について説明します。

B.1 Kerberos 認証でのエラー

Kerberos 認証が失敗した場合のエラー要因とその対処について説明します。

エラー要因：

ファイルシステムのマウントに失敗したときの Kerberos 認証の失敗結果がキャッシュに保存されていて，かつキャッシュの有効期限内に再びマウント操作を実行した。

対処方法：

`nfscacheflush` コマンドを使用して，キャッシュに保存されている情報を無効にしてください。Kerberos 認証結果のキャッシュの有効期限は，KDC サーバに設定された NFS サービスチケットの有効期限に依存します。通常，チケットの有効期限は 8 ～ 10 時間に設定されています。

エラー要因：

ユーザー情報の変更によって，実際のユーザー情報とキャッシュに保存されているユーザー情報に差異が発生していて，かつキャッシュの有効期限内に NFS 共有にアクセスした。

対処方法：

`nfscacheflush` コマンドを使用して，キャッシュに保存されている情報を無効にしてください。NFS 共有にアクセスしたユーザー情報のキャッシュの有効期限は 10 分間です。

エラー要因：

NFS サービスチケットが送信されていない。

対処方法：

NFS クライアントで `kinit` コマンドを実行して，KDC サーバから NFS サービスチケットの取得ができるかどうか確認してください。

エラー要因：

送信された NFS サービスチケットの有効期限が切れている。

対処方法：

NFS クライアントで `kinit` コマンドを実行して，KDC サーバから再度 NFS サービスチケットを取得してください。

エラー要因：

送信されたユーザー認証チケットの有効期限が切れている。

対処方法：

NFS クライアントで `kinit` コマンドを実行して，KDC サーバから再度ユーザー認証チケットを取得してください。

エラー要因：

NFS クライアントで，gssd デーモンが起動していない。

対処方法：

gssd デーモンを起動してください。起動している場合には，再起動してください。

エラー要因：

NFS クライアントの Kerberos 認証に関する設定が正しくない。

対処方法：

NFS クライアントとして使用している製品のドキュメントを参照してください。

エラー要因：

KDC サーバドメインに参加している各ホスト（KDC サーバ，HVFP のノードまたは Virtual Server，NFS クライアント）の時刻が同期していない。

対処方法：

KDC サーバドメインに参加している各ホストの時刻を同期させてください。ホスト間で時刻が 5 分以上異なると Kerberos 認証ができません。

エラー要因：

KDC サーバ上で，Kerberos チケット処理デーモンが起動していない。

対処方法：

Kerberos チケット処理デーモンを起動してください。起動している場合には，再起動してください。

エラー要因：

DNS サーバに登録してあるホスト名が正しくない。

対処方法：

HVFP のノードまたは Virtual Server のホスト名，KDC サーバのホスト名，各 NFS クライアントのホスト名を確認し，誤りがあれば，DNS サーバに登録してあるホスト名を修正してください。

エラー要因：

KDC サーバの設定が正しくない。

対処方法：

KDC サーバとして使用している製品のドキュメントを参照してください。

エラー要因：

HVFP のノードまたは Virtual Server，KDC サーバ，および NFS クライアントで使用する Kerberos 暗号化タイプが DES-CBC-CRC に統一されていない。

対処方法：

Kerberos 暗号化タイプが DES-CBC-CRC に統一されていない場合には，該当するサービスプリンシパルを設定し直してください。

エラー要因：

NFS サービスの構成定義または NFS 共有の Kerberos 認証に関する設定が正しくない。

対処方法：

NFS サービスおよび NFS 共有の設定を見直し，Kerberos 認証が有効になっていることを確認してください。

エラー要因：

HVFP のノードまたは Virtual Server のキータブファイルの内容が正しくない。

対処方法：

KDC サーバのキータブファイルの内容が，HVFP のノードまたは Virtual Server のキータブファイルへ正しくマージされていることを確認してください。

上記の方法でも対処できないエラーの場合には，次の情報を取得してカスタマーサポートセンターに送付してください。

- 全ログデータ（All log data）
- 次に示す KDC サーバおよび NFS クライアントのファイルまたは情報
  - Kerberos 構成ファイル（krb5.conf）
  - ホスト情報ファイル（hosts）
  - DNS サーバの IP アドレスを設定するファイル（resolv.conf）

- キータブファイル
- システムログ
- 起動プロセス情報

B.2 NFSv4 ドメイン構成でのエラー

NFSv4 ドメイン構成を利用しているときに発生するエラー要因とその対処について説明します。

エラー要因：

NFS クライアントでの NFSv4 ドメイン名の設定が正しくない。

対処方法：

NFS クライアントの NFSv4 ドメイン名定義ファイルで設定してある NFSv4 ドメイン名を，NFS サービスの構成定義で設定してある NFSv4 ドメイン名と一致させてください。

上記の方法でも対処できないエラーの場合には，次の情報を取得してカスタマーサポートセンターに送付してください。

- 全ログデータ（All log data）
- NFS クライアントの NFSv4 ドメイン名定義ファイル

C

Kerberos 認証を利用するときの NFS 環境の構築手順

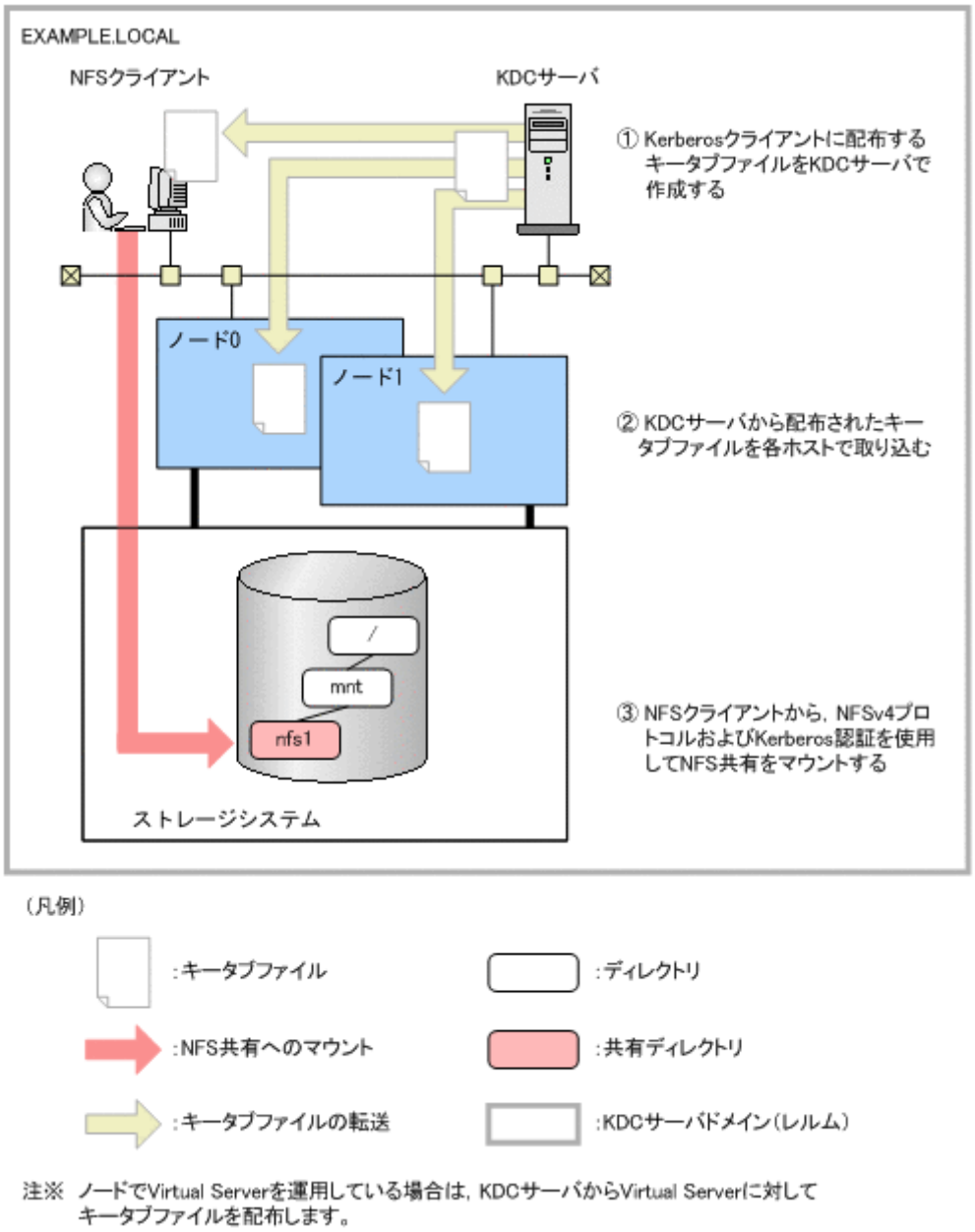
ここでは，Kerberos 認証を利用するときの NFS 環境の構築手順について，実行例を基に説明します。

C.1 構築する NFS 環境の例

概要や前提条件については，「14.3 Kerberos 認証および NFSv4 ドメイン構成を利用するときの NFS 環境の構築」を参照してください。

各手順の実行例は，次の図に示す NFS 環境を構築することを想定しています。

図 C-1： NFS 環境の構築例



また，各ホストに対応するドメイン名やキータブファイルは，次の表のとおり想定しています。

表 C-1： 各ホストに対応するドメイン名やキータブファイル名

#	ホスト	ホスト名（FQDN）	キータブファイル名
1	KDC サーバ	kdc1.example.local	-*1
2	ノード 0	node0.example.local*2	node0.keytab
3	ノード 1	node1.example.local*2	node1.keytab
4	Virtual Server	vserver1.example.local	vserver1.keytab

#	ホスト	ホスト名（FQDN）	キータブファイル名
5	NFS クライアント	cl1.example.local	cl1.keytab

注 *1

Kerberos クライアントの各ホストに配布するキータブファイルを /tmp ディレクトリ内に作成することを想定しています。

注 *2

HVFP の各ノードの仮想 IP アドレスに対応したホスト名です。

C.2 KDC サーバの構築と NFS サービスプリンシパルの追加

KDC サーバの構築手順と NFS サービスプリンシパルの追加手順をプラットフォームごとに説明します。ここで説明する手順は，管理者権限を持つユーザーが KDC サーバ上で実施してください。

C.2.1 KDC サーバを構築する前に

KDC サーバを構築する前に，次のことを確認する必要があります。

- KDC サーバドメインに参加しているすべてのホストの時刻が同期していること
  Kerberos 認証では，各ホストの時刻に 5 分以上の相違があると，エラーが発生するおそれがあります。Kerberos 認証を利用する場合は，NTP サーバを使用することを推奨します。
- KDC サーバドメインに参加しているすべてのホストが，DNS を利用して名前解決できること
  このとき，すべてのホスト名が FQDN で登録されている必要があります。
- HVFP のノード（または Virtual Server），KDC サーバ，および NFS クライアントで使用する Kerberos 暗号化タイプが DES-CBC-CRC であること

C.2.2 Windows Server 2019 の場合

Windows Server 2019 マシンで KDC サーバを構築し，NFS サービスプリンシパルを追加する手順を次に示します。

1. Active Directory ウィザードを使用して，Active Directory を構築します。
2. Windows Server 2019 の場合，DES 暗号化を有効にします。
   Windows Server 2019 は，DES 暗号（DES-CBC-MD5 および DES-CBC-CRC）が既定で両方とも無効になっているため，DES 暗号化を有効にする必要があります。「管理ツール」から「ローカルセキュリティポリシー」を起動し，「セキュリティの設定」－「ローカルポリシー」－「セキュリティオプション」の「ネットワークセキュリティ：Kerberos で許可する暗号化の種類を構成する」をダブルクリックして，「ローカル セキュリティの設定」タブで DES_CBC_CRC をチェックしてください。
3. NFS サービスプリンシパルマッピング用のユーザーアカウントを作成し，Active Directory に追加します。
   Active Directory 管理ツールの［User］-［新規作成］-［ユーザー］を選択し，KDC サーバドメイン内のホストごとに 1 つずつ，ユーザーアカウントを作成します。ここでは，次の条件でユーザーアカウントを作成します。

表 C-2：ユーザーアカウントを作成するホストと対応するユーザーログオン名

#	ホスト	ユーザーログオン名
1	ノード 0	node0
2	ノード 1	node1
3	Virtual Server	vserver1
4	NFS クライアント	cl1

また，作成したユーザーアカウントに対して，DES 暗号を使用できるようにアカウントオプションを設定してください。Windows Server 2019 の場合の設定例を次の図に示します。

図 C-2：アカウントオプションの設定例（Windows Server 2019 の場合）

4. コマンドプロンプトで ktpass コマンドを実行して，キータブファイルを作成します。

```
> ktpass -princ nfs/node0.example.local@EXAMPLE.LOCAL -mapuser node0 -pass
passwd -crypto DES-CBC-CRC -ptype KRB5_NT_PRINCIPAL -out node0.keytab
> ktpass -princ nfs/node1.example.local@EXAMPLE.LOCAL -mapuser node1 -pass
passwd -crypto DES-CBC-CRC -ptype KRB5_NT_PRINCIPAL -out node1.keytab
> ktpass -princ nfs/vserver1.example.local@EXAMPLE.LOCAL -mapuser vserver1 -
pass passwd -crypto DES-CBC-CRC -ptype KRB5_NT_PRINCIPAL -out vserver1.keytab
> ktpass -princ nfs/cl1.example.local@EXAMPLE.LOCAL -mapuser cl1 -pass passwd
-crypto DES-CBC-CRC -ptype KRB5_NT_PRINCIPAL -out cl1.keytab
```

ktpass コマンドの各オプションで指定する情報を次に示します。

-princ

NFS サービスのプリンシパル名（nfs/ ＜ホスト名（FQDN）＞ @ ＜ KDC サーバドメイン名＞）

-mapuser

Active Directory 管理ツールで作成したアカウントユーザーのユーザー名

-pass

Active Directory 管理ツールで作成したアカウントユーザーのパスワード

-crypto

Kerberos 暗号化タイプ（DES-CBC-CRC を指定します）

-ptype

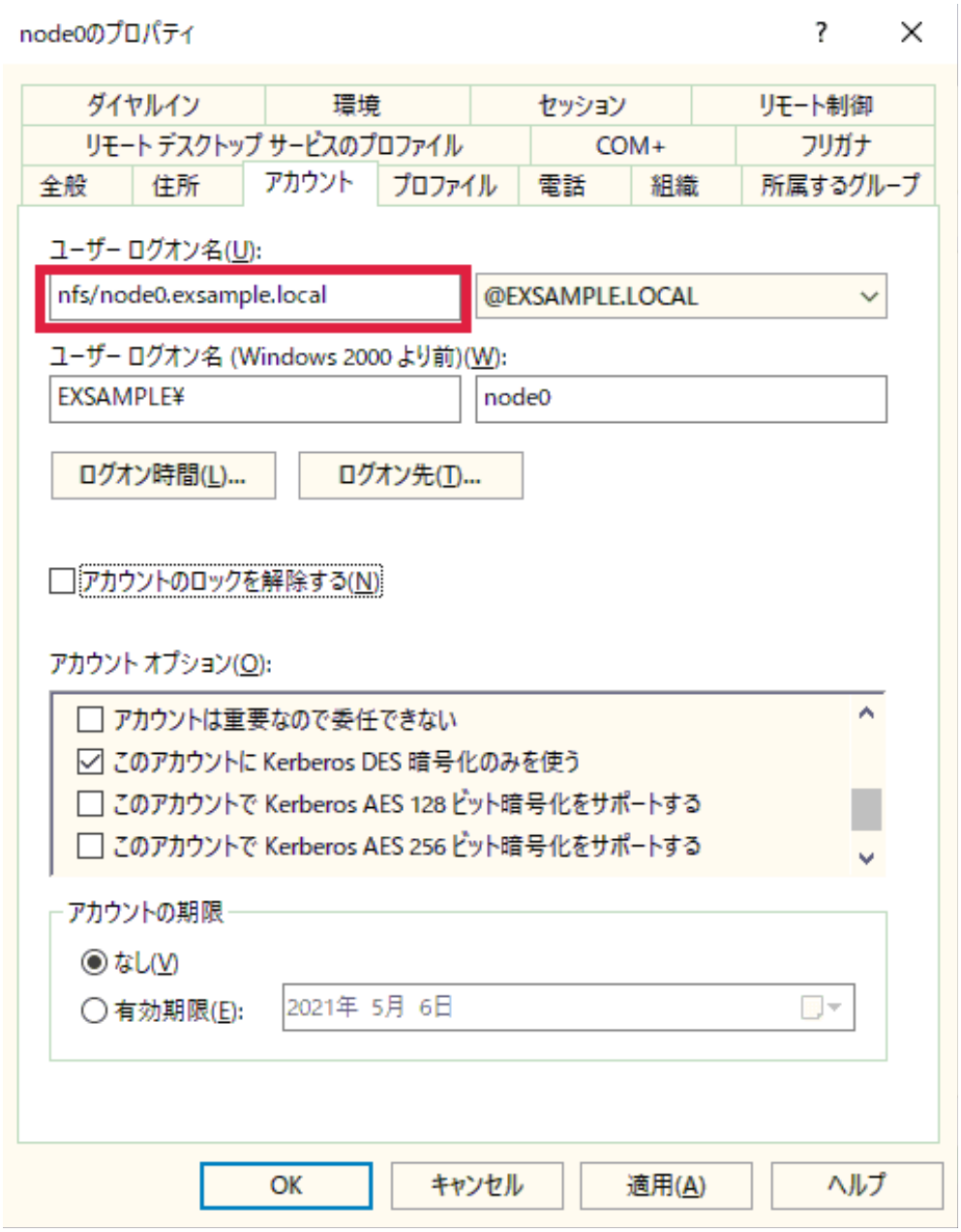
プリンシパルのタイプ

-out

Kerberos クライアントの各ホストに配布するキータブファイル名

ktpass コマンドを実行すると，アカウントユーザーのユーザーログオン名が NFS サービスプリンシパル名にマッピングされます。Windows Server 2019 の場合のマッピング例を次の図に示します。

図 C-3：ktpass コマンド実行後のユーザーログオン名のマッピング例（Windows Server 2019 の場合）



C.2.3 Red Hat Enterprise Linux Advanced Platform v5.2 の場合

ここでは，Red Hat Enterprise Linux Advanced Platform v5.2 の次のバージョンを使用していることを想定しています。

- Linux version 2.6.18-92.el5 (mockbuild@builder16.centos.org) (gcc version 4.1.2 20071124 (Red Hat 4.1.2-42)) #1 SMP Tue Jun 10 18:49:47 EDT 2008
- Red Hat Enterprise Linux Server release 5 (Tikanga)

Red Hat Enterprise Linux Advanced Platform v5.2 マシンで KDC サーバを構築し，NFS サービスプリンシパルを追加する手順を次に示します。

1. krb5-server，krb5-libs および krb5-workstation パッケージがインストールされていることを確認します。

```
# rpm -qa | grep krb
krb5-server-1.5-17
krb5-libs-1.5-17
krb5-workstation-1.5-17
```

2. Kerberos 構成ファイル（krb5.conf）を次のように編集します。

```
# cat /etc/krb5.conf
[logging]
 default = FILE:/var/log/krb5libs.log
 kdc = FILE:/var/log/krb5kdc.log
 admin_server = FILE:/var/log/kadmind.log

[libdefaults]
 default_realm = EXAMPLE.LOCAL
 dns_lookup_realm = false
 dns_lookup_kdc = false
 ticket_lifetime = 24h
 forwardable = yes

[realms]
 EXAMPLE.LOCAL = {
  kdc = kdc1.example.local:88
  admin_server = kdc1.example.local:749
  default_domain = example.local
 }

[domain_realm]
 .example.local = EXAMPLE.LOCAL
 example.local = EXAMPLE.LOCAL

[kdc]
 profile = /var/kerberos/krb5kdc/kdc.conf

[appdefaults]
 pam = {
   debug = false
   ticket_lifetime = 36000
   renew_lifetime = 36000
   forwardable = true
   krb4_convert = false
 }
```

3. kdb5_util ユーティリティを使用して，KDC データベースを作成します。

```
# /usr/kerberos/sbin/kdb5_util -r EXAMPLE.LOCAL create -s
Loading random data
Initializing database '/var/kerberos/krb5kdc/principal' for realm
'EXAMPLE.LOCAL',
master key name 'K/M@EXAMPLE.LOCAL'
You will be prompted for the database Master Password.
It is important that you NOT FORGET this password.
Enter KDC database master key:
Re-enter KDC database master key to verify:
```

4. 管理用アクセス制御リストファイル（kadm5.acl）を次のように編集します。

```
# cat /var/kerberos/krb5kdc/kadm5.acl
*/admin@EXAMPLE.LOCAL      *
```

5. 管理用プリンシパルを作成します。

```
# /usr/kerberos/sbin/kadmin.local -q "addprinc root/admin"
Authenticating as principal root/admin@EXAMPLE.LOCAL with password.
WARNING: no policy specified for root/admin@EXAMPLE.LOCAL; defaulting to no
policy
Enter password for principal "root/admin@EXAMPLE.LOCAL":
Re-enter password for principal "root/admin@EXAMPLE.LOCAL":
Principal "root/admin@EXAMPLE.LOCAL" created.
```

6. Kerberos サーバデーモンを起動します。

```
# /usr/kerberos/sbin/krb524d -m
# /usr/kerberos/sbin/krb5kdc
# /usr/kerberos/sbin/kadmind
```

7. 管理用プリンシパルの初期チケットを取得します。
   初期チケットを取得したあと，正しく取得できたことを確認してください。

```
# kinit root/admin
Password for root/admin@EXAMPLE.LOCAL:
# klist -5
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: root/admin@EXAMPLE.LOCAL

Valid starting     Expires            Service principal
03/26/09 16:08:51  03/27/09 16:08:51  krbtgt/EXAMPLE.LOCAL@EXAMPLE.LOCAL
```

8. kadmin ユーティリティをネットワーク越しに使用するために，KDC サーバのキータブファイル（krb5.keytab）を作成します。

```
# /usr/kerberos/sbin/kadmin.local
Authenticating as principal root/admin@EXAMPLE.LOCAL with password.
kadmin.local:  ktadd -k /etc/krb5.keytab kadmin/admin kadmin/changepw
Entry for principal kadmin/admin with kvno 3, encryption type Triple DES cbc
mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5.keytab.
Entry for principal kadmin/admin with kvno 3, encryption type DES cbc mode with
CRC-32 added to keytab WRFILE:/etc/krb5.keytab.
Entry for principal kadmin/changepw with kvno 3, encryption type Triple DES cbc
mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5.keytab.
Entry for principal kadmin/changepw with kvno 3, encryption type DES cbc mode
with CRC-32 added to keytab WRFILE:/etc/krb5.keytab.
```

9. kadmin ユーティリティを使用して，host プリンシパルを作成します。

```
kadmin.local:  addprinc -randkey host/kdc1.example.local
WARNING: no policy specified for host/kdc1.example.local@EXAMPLE.LOCAL;
defaulting to no policy
Principal "host/kdc1.example.local@EXAMPLE.LOCAL" created.

kadmin.local:  ktadd host/kdc1.example.local
Entry for principal host/kdc1.example.local with kvno 3, encryption type Triple
DES cbc mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5.keytab.
Entry for principal host/kdc1.example.local with kvno 3, encryption type DES
cbc mode with CRC-32 added to keytab WRFILE:/etc/krb5.keytab.

kadmin.local:  listprincs
K/M@EXAMPLE.LOCAL
host/kdc1.example.local@EXAMPLE.LOCAL
kadmin/admin@EXAMPLE.LOCAL
kadmin/changepw@EXAMPLE.LOCAL
kadmin/history@EXAMPLE.LOCAL
kadmin/kdc1@EXAMPLE.LOCAL
krbtgt/EXAMPLE.LOCAL@EXAMPLE.LOCAL
root/admin@EXAMPLE.LOCAL
kadmin.local:
```

10. kadmin ユーティリティを使用して，KDC サーバのキータブファイル（krb5.keytab）に host プリンシパルを追加します。
    host プリンシパルを追加したあと，正しく追加できたことを確認してください。

```
kadmin.local:  addprinc -randkey host/kdc1.example.local
WARNING: no policy specified for host/kdc1.example.local@EXAMPLE.LOCAL;
defaulting to no policy
Principal "host/kdc1.example.local@EXAMPLE.LOCAL" created.

kadmin.local:  ktadd host/kdc1.example.local
Entry for principal host/kdc1.example.local with kvno 3, encryption type Triple
DES cbc mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5.keytab.
Entry for principal host/kdc1.example.local with kvno 3, encryption type DES
cbc mode with CRC-32 added to keytab WRFILE:/etc/krb5.keytab.

kadmin.local:  listprincs
K/M@EXAMPLE.LOCAL
host/kdc1.example.local@EXAMPLE.LOCAL
kadmin/admin@EXAMPLE.LOCAL
kadmin/changepw@EXAMPLE.LOCAL
kadmin/history@EXAMPLE.LOCAL
kadmin/kdc1@EXAMPLE.LOCAL
krbtgt/EXAMPLE.LOCAL@EXAMPLE.LOCAL
root/admin@EXAMPLE.LOCAL
kadmin.local:
```

11.kadmin ユーティリティを使用して，各ホストの NFS サービスプリンシパルを作成し，配布用のキータブファイルに追加します。

```
kadmin.local:  addprinc -randkey nfs/node0.example.local
...
kadmin.local:  ktadd -e des-cbc-crc:normal -k /tmp/node0.keytab  nfs/
node0.example.local
...
kadmin.local:  addprinc -randkey nfs/node1.example.local
...
kadmin.local:  ktadd -e des-cbc-crc:normal -k /tmp/node1.keytab  nfs/
node1.example.local
...
kadmin.local:  addprinc -randkey nfs/vserver1.example.local
...
kadmin.local:  ktadd -e des-cbc-crc:normal -k /tmp/vserver1.keytab  nfs/
vserver1.example.local
...
kadmin.local:  addprinc -randkey nfs/cl1.example.local
...
kadmin.local:  ktadd -e des-cbc-crc:normal -k /tmp/cl1.keytab  nfs/
cl1.example.local
...
kadmin.local:  quit
```

C.2.4 Solaris 10 の場合

ここでは，Solaris 10 の次のバージョンを使用していることを想定しています。

- SunOS 5.10 Generic_137137-09 sun4u sparc SUNW,Sun-Blade-1000
- Solaris 10 10/08 s10s_u6wos_07b SPARC Copyright 2008 Sun Microsystems, Inc. All Rights Reserved.Use is subject to license terms.Assembled 27 October 2008

Solaris 10 マシンで KDC サーバを構築する場合は，事前に，DNS が有効になっていることを確認する必要があります。

Solaris 10 マシンで KDC サーバを構築し，NFS サービスプリンシパルを追加する手順を次に示します。

1. Kerberos 構成ファイル（krb5.conf）を次のように編集します。

```
# cat /etc/krb5/krb5.conf
[logging]
 default = FILE:/var/log/krb5libs.log
 kdc = FILE:/var/log/krb5kdc.log
 admin_server = FILE:/var/log/kadmind.log

[libdefaults]
 default_realm = EXAMPLE.LOCAL
 dns_lookup_realm = false
 dns_lookup_kdc = false
 ticket_lifetime = 24h
 forwardable = yes

[realms]
 EXAMPLE.LOCAL = {
  kdc = kdc1.example.local:88
  admin_server = kdc1.example.local:749
  default_domain = example.local
 }

[domain_realm]
 .example.local = EXAMPLE.LOCAL
 example.local = EXAMPLE.LOCAL

[appdefaults]
 pam = {
   debug = false
   ticket_lifetime = 36000
   renew_lifetime = 36000
   forwardable = true
   krb4_convert = false
 }
```

2. kdb5_util ユーティリティを使用して，KDC データベースを作成します。

```
# /usr/sbin/kdb5_util -r EXAMPLE.LOCAL create -s
...
```

3. 管理用アクセス制御リストファイル（kadm5.acl）を次のように編集します。

```
# cat /etc/krb5/kadm5.acl
#
# Copyright (c) 1998-2000 by Sun Microsystems, Inc.
# All rights reserved.
#
#pragma ident   "@(#)kadm5.acl  1.1     01/03/19 SMI"

*/admin@EXAMPLE.LOCAL *
```

4. 管理用プリンシパルを作成します。

```
# /usr/sbin/kadmin.local
kadmin.local: addprinc root/admin
...
```

5. kadmind サービスのキータブファイル（kadm5.keytab）を作成します。
   キータブファイルを作成したら，kadmin.local コマンドを終了してください。

```
kadmin.local: ktadd -k /etc/krb5/kadm5.keytab kadmin/kdc1.example.local
...
kadmin.local: ktadd -k /etc/krb5/kadm5.keytab changepw/kdc1.example.local
...
kadmin.local: ktadd -k /etc/krb5/kadm5.keytab kadmin/changepw
...
kadmin.local: quit
```

6. Kerberos サーバデーモンを起動します。

```
# svcadm enable -r network/security/krb5kdc
# svcadm enable -r network/security/kadmin
```

   注意：

   DNS が有効になっていない場合は，svcadm コマンドを使用して，Kerberos サーバデーモンを起動できません。

7. 管理用プリンシパルの初期チケットを取得します。
   初期チケットを取得したあと，正しく取得できたことを確認してください。

```
# kinit root/admin
Password for root/admin@EXAMPLE.LOCAL:
# klist -5
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: root/admin@EXAMPLE.LOCAL
```

8. kadmin ユーティリティを使用して，KDC サーバの host プリンシパルを作成します。

```
# /usr/sbin/kadmin -p root/admin
...
kadmin: addprinc -randkey host/kdc1.example.local
...
```

9. kadmin ユーティリティを使用して，kadmind サービスのキータブファイル（kadm5.keytab）に host プリンシパルを追加します。

```
kadmin: ktadd host/kdc1.example.local
...
```

10. kadmin ユーティリティを使用して，各ホストの NFS サービスプリンシパルを作成し，配布用のキータブファイルに追加します。

```
kadmin: addprinc -randkey nfs/node0.example.local
...
kadmin: ktadd -e des-cbc-crc:normal -k /tmp/node0.keytab  nfs/
node0.example.local
...
kadmin: addprinc -randkey nfs/node1.example.local
...
kadmin: ktadd -e des-cbc-crc:normal -k /tmp/node1.keytab  nfs/
node1.example.local
...
kadmin: addprinc -randkey nfs/vserver1.example.local
...
kadmin: ktadd -e des-cbc-crc:normal -k /tmp/vserver1.keytab  nfs/
vserver1.example.local
...
kadmin: addprinc -randkey nfs/cl1.example.local
...
kadmin: ktadd -e des-cbc-crc:normal -k /tmp/cl1.keytab  nfs/cl1.example.local
...
kadmin: quit
```

C.2.5 HP-UX 11i v3 の場合

ここでは，HP-UX 11i v3 の次のバージョンを使用していることを想定しています。

- HP-UX B.11.31 U 9000/800 1801453303 unlimited-user license
- HPUX11i-OE B.11.31 HP-UX Foundation Operating Environment
- HPUX11i-OE.OE B.11.31 HP-UX OE control script product

HP-UX 11i v3 マシンで KDC サーバを構築し，NFS サービスプリンシパルを追加する手順を次に示します。

1. krbsetup コマンドを使用して，Kerberos 設定ファイル（krb5.conf，krb.realms）を作成します。
   krbsetup コマンドでは，対話型処理を行います。

```
# /opt/krb5/sbin/krbsetup

         Kerberos Server Configuration - Main Menu
         ----------------------------------------

         Select one of the following options:


         1) Configure the Server
         2) Start the Kerberos daemons
         3) Stop the Kerberos daemons
         4) Unconfigure the Server
         5) Exit


         6) Help


         Selection: 1
```

   [Enter] キーを押します。

```
         1) Configure the Server with LDAP backend
         2) Configure the Server with C-Tree backend
         0) Return to Previous Menu


         Selection: [0] 2
```

   [Enter] キーを押します。

```
         1) Configure as a Primary Security Server
         2) Configure as a Secondary Security Server


         Selection: 1
```

[Enter] キーを押します。

```
         1) Configure as a Primary Security Server
         2) Configure as a Secondary Security Server


         Selection: 1
```

[Enter] キーを押します。

```
         THIS MACHINE WILL BE CONFIGURED AS A PRIMARY SERVER


         What type of the security mechanism you want to use (DES-MD5/DES-CRC/
DES3)
         If you do not select any security mechanism, the default,
         DES-MD5 will be selected: DES-CRC
         You have selected DES-CRC

         Do you want to stash the principal database key
         on your local disk (y/n)? [y] :y

         Enter the fully qualified name of the Secondary Security Server 1
         press 'q' if you want to skip this and proceed further: q

        Enter the realm name (the allowed chars are "a-z""A-Z""0-9" "." "-" "_"
"*")
         If nothing is typed the default name [ KDC1.EXAMPLE.LOCAL ] will be
         considered: EXAMPLE.LOCAL

         /opt/krb5/krb.conf moved to /opt/krb5/krb.conf.keep

         /opt/krb5/krb.realms moved to /opt/krb5/krb.realms.keep

         /opt/krb5/kpropd.ini moved to /opt/krb5/kpropd.ini.keep

         /etc/krb5.conf moved to /etc/krb5.conf.keep

         Creating krb.conf and krb.realms files
         Copying admin_acl_file and password.policy file onto /opt/krb5 dir

       Do you want to store the log messages in a different directory rather than
         the syslog file (y/n)? [n] : n
         You will be prompted for the database Master Password.
         It is important that you DO NOT FORGET this password.

         Enter Password:
         Re-enter Password:

Kerberos server has been configured successfully.

Kerberos daemons are successfully started
Press Enter to go back to the main menu.
```

[Enter] キーを押します。

```
          Kerberos Server Configuration - Main Menu
          ----------------------------------------

          Select one of the following options:


          1) Configure the Server
          2) Start the Kerberos daemons
          3) Stop the Kerberos daemons
          4) Unconfigure the Server
          5) Exit


          6) Help


          Selection: 5

You have selected 5 Exiting...
```

2. Kerberos 設定ファイル（krb5.conf，krb.realms）の内容を確認します。

```
# cat /opt/krb5/krb.conf
EXAMPLE.LOCAL
EXAMPLE.LOCAL kd1.example.local admin server
# cat /opt/krb5/krb.realms

*.example.local EXAMPLE.LOCAL
```

3. 管理用アクセス制御リストファイル（admin_acl_file）を編集します。
   管理用アクセス制御リストファイルがない場合は，作成してください。

```
# cat /opt/krb5/admin_acl_file
K/M             CI # needed for kadmd on secondaries
*/admin         *  # created by krbsetup can be modified by administrator
```

4. kadminl コマンドを使用して，KDC サーバの host プリンシパルを作成します。

```
# /opt/krb5/admin/kadminl -R "ext host/kd1.example.local"
Connecting as: K/M
Connected to krb5v01 in realm EXAMPLE.LOCAL.
Principal added.
Key extracted.
Disconnected.
```

5. Kerberos デーモン起動ファイル（krbsrv）を次のように編集します。

```
# cat /etc/rc.config.d/krbsrv
KDC=1
ADMD=1
```

6. Kerberos デーモンを起動します。

```
# /sbin/init.d/krbsrv start
Starting Kerberos Server Daemons
/opt/krb5/sbin/kdcd
/opt/krb5/sbin/kadmind
Finished startup.

NOTE : If the machine is a primary server please start the kpropd manually.
For more information on propogation refer 'Installing , Configuring HP's
Kerberos server document'
# /opt/krb5/sbin/kpropd
```

7. kadminl コマンドを使用して，各ホストの NFS サービスプリンシパルを作成し，配布用のキータブファイルに追加します。

```
# /opt/krb5/admin/kadminl
Connecting as: K/M
Connected to krb5v01 in realm EXAMPLE.LOCAL.
Command: ext
Name of Principal (host/kdc1.example.local): nfs/node0.example.local
Service Key Table File Name (/opt/krb5/v5srvtab): /tmp/node0.keytab
Enter policy name (Press enter key to apply default policy) :
Principal added.
Key extracted.

Command: ext
Name of Principal (host/kdc1.example.local): nfs/node1.example.local
Service Key Table File Name (/opt/krb5/v5srvtab): /tmp/node1.keytab
Enter policy name (Press enter key to apply default policy) :
Principal added.
Key extracted.

Command: ext
Name of Principal (host/kdc1.example.local): nfs/vserver1.example.local
Service Key Table File Name (/opt/krb5/v5srvtab): /tmp/vserver1.keytab
Enter policy name (Press enter key to apply default policy) :
Principal added.
Key extracted.

Command: ext
Name of Principal (host/kdc1.example.local): nfs/cl1.example.local
Service Key Table File Name (/opt/krb5/v5srvtab): /tmp/cl1.keytab
Enter policy name (Press enter key to apply default policy) :
Principal added.
Key extracted.

Command: q
Disconnected.
```

C.3 キータブファイルの配布と各ホストでの取り込み

NFS サービスプリンシパルを追加したキータブファイルを，Kerberos クライアントの各ホストに配布し，各ホストで管理しているキータブファイルにマージする手順を説明します。各ホストに配布するキータブファイルの作成については，「C.2 KDC サーバの構築と NFS サービスプリンシパルの追加」を参照してください。

C.3.1 キータブファイルの配布先

ここでは，KDC サーバの構築時に作成したキータブファイルの配布先は，次の表のとおり想定しています。

表 C-3：キータブファイルの配布先

#	キータブファイル名	対象のホスト	配布先
1	node0.keytab	ノード 0	ノード 0：/home/nasroot ノード 1：/home/nasroot*
2	node1.keytab	ノード 1	ノード 0：/home/nasroot* ノード 1：/home/nasroot
3	vserver1.keytab	Virtual Server	Virtual Server：/home/nasroot
4	cl1.keytab	NFS クライアント	NFS クライアント：/tmp

注 *

フェールオーバーしたときにも運用を継続できるよう，クラスタ内のもう片方のノードにもキータブファイルを配布してください。

C.3.2 キータブファイルの配布方法

キータブファイルには，機密情報が含まれています。セキュリティを考慮して，次の方法で各ホストに配布してください。

Windows マシンの場合

安全に複写できるソフトウェアを利用して転送します。

UNIX マシンの場合

scp を利用して転送します。

C.3.3 キータブファイルの取り込み（HVFP のノードの場合）

配布されたキータブファイルを HVFP のノードで取り込む手順を次に示します。

1. nfskeytabadd コマンドを使用して，キータブファイルをマージします。
   ノード 0 とノード 1 の両方でコマンドを実行してください。

```
$ sudo nfskeytabadd -i /home/nasroot/node0.keytab
$ sudo nfskeytabadd -i /home/nasroot/node1.keytab
$ sudo nfskeytablist
slot KVNO Principal
---- ---- ---------------------------------------------------------------------
--
   1    3     nfs/node0.example.local@EXAMPLE.LOCAL
   2    3     nfs/node1.example.local@EXAMPLE.LOCAL
```

C.3.4 キータブファイルの取り込み（Virtual Server の場合）

配布されたキータブファイルを，Virtual Server で取り込む手順を次に示します。

1. nfskeytabadd コマンドを使用して，キータブファイルをマージします。

```
$ sudo nfskeytabadd -i /home/nasroot/vserver1.keytab
$ sudo nfskeytablist
slot KVNO Principal
---- ---- ---------------------------------------------------------------------
--
   1    3     nfs/vserver1.example.local@EXAMPLE.LOCAL
```

C.3.5 キータブファイルの取り込み（NFS クライアントの場合）

ここでは，次のプラットフォームを NFS クライアントで使用していることを想定しています。

表 C-4：NFS クライアントで使用しているプラットフォーム

#	プラットフォーム	バージョン
1	Red Hat Enterprise Linux Advanced Platform v5.6	Linux version 2.6.18-238.el5
		Red Hat Enterprise Linux Server release 5 (Tikanga)
2	Solaris 10	SunOS 5.10 Generic_137137-09 sun4u sparc SUNW,Sun-Blade-1000
		Solaris 10 10/08 s10s_u6wos_07b SPARC Copyright 2008 Sun Microsystems, Inc. All Rights Reserved.Use is subject to license terms.Assembled 27 October 2008
3	HP-UX 11i v3	HP-UX B.11.31 U 9000/800 1801453303 unlimited-user license
		HPUX11i-OE B.11.31 HP-UX Foundation Operating Environment HPUX11i-OE.OE B.11.31 HP-UX OE control script product

配布されたキータブファイルを，NFS クライアントで取り込む手順を次に示します。

1. Kerberos 構成ファイル（krb5.conf）を編集します。
   KDC サーバドメイン名とサーバ名を変更してください。

```
# cat /etc/krb5.conf
[logging]
 default = FILE:/var/log/krb5libs.log
 kdc = FILE:/var/log/krb5kdc.log
 admin_server = FILE:/var/log/kadmind.log

[libdefaults]
 default_realm = EXAMPLE.LOCAL
 dns_lookup_realm = false
 dns_lookup_kdc = false
 ticket_lifetime = 24h
 forwardable = yes

[realms]
 EXAMPLE.LOCAL = {
  kdc = kdc1.example.local:88
  admin_server = kdc1.example.local:749
  default_domain = example.local
 }

[domain_realm]
 .example.local = EXAMPLE.LOCAL
 example.local = EXAMPLE.LOCAL

[kdc]
 profile = /var/kerberos/krb5kdc/kdc.conf

[appdefaults]
 pam = {
   debug = false
   ticket_lifetime = 36000
   renew_lifetime = 36000
   forwardable = true
   krb4_convert = false
 }
```

2. ktutil コマンドを使用して，キータブファイルをマージします。
   対象の NFS クライアントで管理しているキータブファイルを指定してください。ここでは，/etc/krb5.keytab を指定します。

```
# ktutil
ktutil:  rkt /tmp/cl1.keytab
ktutil:  wkt /etc/krb5.keytab
ktutil:  list
slot KVNO Principal
---- ---- ---------------------------------------------------------------------
--
   1    3     nfs/cl1.example.local@EXAMPLE.LOCAL
ktutil:  quit
```

D

Kerberos 認証を利用するときの NFS 共有ディレクトリへのアクセス手順

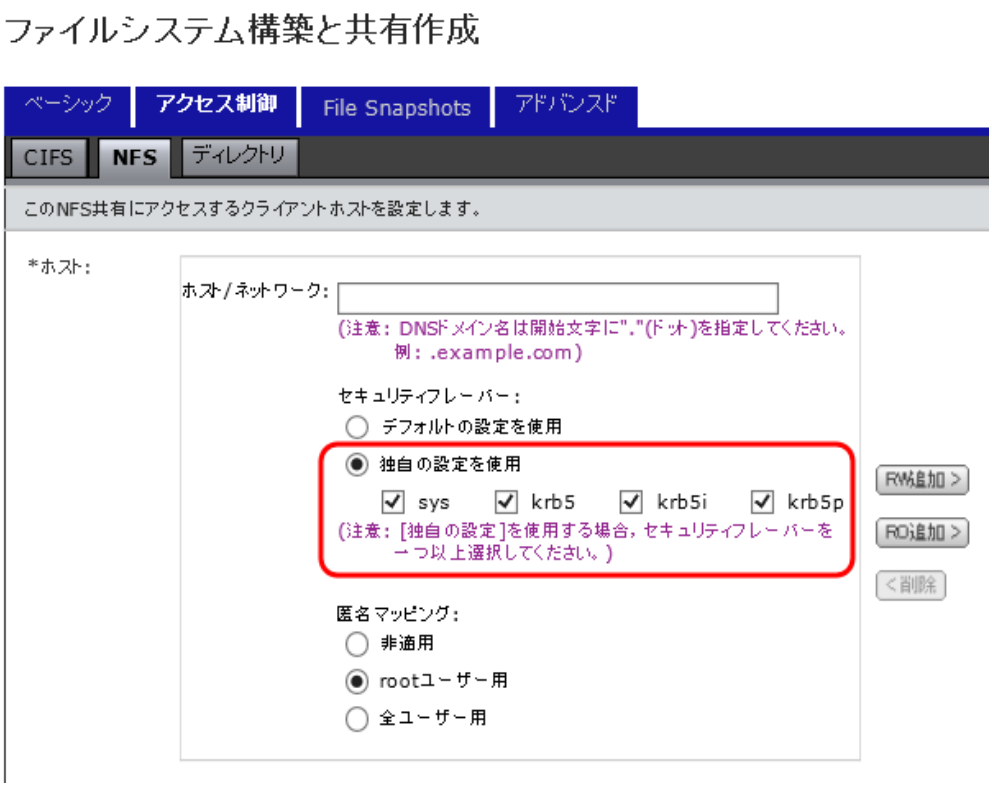
ここでは，Kerberos 認証を利用するときの NFS 共有ディレクトリへのアクセス手順について，実行例を基に説明します。

D.1 File Services Manager でのセキュリティフレーバーの設定

File Services Manager を使用して，NFS 共有を作成するとき，または，NFS サービスの構成定義を変更するときに，Kerberos を利用して認証できるようにセキュリティフレーバーを設定できます。

File Services Manager の GUI を使用して NFS 共有を作成する際のセキュリティフレーバーを指定するときの例を次の図に示します。

図 D-1：セキュリティフレーバーの指定例



NFS 共有の作成時または NFS サービスの構成定義の変更時にセキュリティフレーバーを指定する方法については，「ユーザーズガイド」（IF305）を参照してください。

D.2 NFS クライアントからのマウント

NFS クライアントからは，File Services Manager で設定されているセキュリティフレーバーを指定してマウントします。

Red Hat を使用した NFS クライアントから，各セキュリティフレーバーを指定して，NFSv3 プロトコルで共有ディレクトリ（node0.example.local:/mnt/nfs01）をマウントするときの実行例を次に示します。

- Kerberos 5 を使用する場合

```
# mount -o vers=3,sec=krb5 node0.example.local:/mnt/nfs01 /mnt
# mount
:
node0.example.local:/mnt/nfs01 on /mnt type nfs
(rw,sec=krb5,addr=192.168.0.10)
```

- Kerberos 5（Integrity）を使用する場合

```
# mount -o vers=3,sec=krb5i node0.example.local:/mnt/nfs01 /mnt
# mount
:
node0.example.local:/mnt/nfs01 on /mnt type nfs
(rw,sec=krb5i,addr=192.168.0.10)
```

- Kerberos 5（Privacy）を使用する場合

```
# mount -o vers=3,sec=krb5p node0.example.local:/mnt/nfs01 /mnt
# mount
:
node0.example.local:/mnt/nfs01 on /mnt type nfs
(rw,sec=krb5p,addr=192.168.0.10)
```

- AUTH_SYS を使用する場合

```
# mount -o vers=3,sec=sys node0.example.local:/mnt/nfs01 /mnt
# mount
:
node0.example.local:/mnt/nfs01 on /mnt type nfs (rw,sec=sys,addr=192.168.0.10)
```

D.3 NFS 共有ディレクトリへのアクセス

NFS 共有ディレクトリをマウントしたあと，root ユーザーまたは一般ユーザーの権限でアクセスするためには，KDC サーバドメインに対して，root プリンシパルとユーザープリンシパルをそれぞれ割り当てる必要があります。なお，Windows マシンで KDC サーバを構築している場合，root ユーザーまたは一般ユーザーの権限でアクセスするためには，Active Directory ユーザーとして登録する必要があります。

各ユーザーは，初期チケットを取得すると，NFS 共有ディレクトリにアクセスできるようになります。

通常，チケットの有効期限は 8 ～ 10 時間に設定されています。時間の掛かるバッチ処理などでファイルシステムを利用する場合は，チケットの有効期限を見直して，KDC ポリシーの設定を変更してください。

セカンダリー KDC サーバの追加手順

HVFP では，KDC サーバを 5 台まで追加できます。セカンダリー KDC サーバを追加するときは，プライマリーとセカンダリーの KDC サーバ間で，KDC データベースをレプリケーションする必要があります。

E.1 KDC サーバを追加する手順

Red Hat Enterprise Linux Advanced Platform v5.2 マシンでセカンダリーとして KDC サーバ（kdc2.example.local）を構築し，追加する手順を次に示します。KDC サーバを構築するときの前提条件については，「C.2.1 KDC サーバを構築する前に」を参照してください。

1. krb5-server，krb5-libs および krb5-workstation パッケージがインストールされていることを確認します。

```
# rpm -qa | grep krb
krb5-server-1.5-17
krb5-libs-1.5-17
krb5-workstation-1.5-17
```

2. セカンダリー KDC サーバで kdb5_util ユーティリティを使用して，KDC データベースを作成します。
   プライマリー KDC サーバの KDC データベースと同様に作成してください。

```
# /usr/kerberos/sbin/kdb5_util -r EXAMPLE.LOCAL create -s
Loading random data
Initializing database '/var/kerberos/krb5kdc/principal' for realm
'EXAMPLE.LOCAL',
master key name 'K/M@EXAMPLE.LOCAL'
You will be prompted for the database Master Password.
It is important that you NOT FORGET this password.
Enter KDC database master key:
Re-enter KDC database master key to verify:
```

3. Kerberos 構成ファイル（krb5.conf）を編集します。
   Kerberos 構成ファイルは，プライマリーおよびセカンダリー KDC サーバ間で同じ内容にしてください。

```
# cat /etc/krb5.conf
[logging]
 default = FILE:/var/log/krb5libs.log
 kdc = FILE:/var/log/krb5kdc.log
 admin_server = FILE:/var/log/kadmind.log

[libdefaults]
 default_realm = EXAMPLE.LOCAL
 dns_lookup_realm = false
 dns_lookup_kdc = false
 ticket_lifetime = 24h
 forwardable = yes

[realms]
 EXAMPLE.LOCAL = {
kdc = kdc1.example.local:88
kdc = kdc2.example.local:88
  admin_server = kdc1.example.local:749
  default_domain = example.local
 }

[domain_realm]
 .example.local = EXAMPLE.LOCAL
 example.local = EXAMPLE.LOCAL

[kdc]
 profile = /var/kerberos/krb5kdc/kdc.conf

[appdefaults]
 pam = {
   debug = false
   ticket_lifetime = 36000
   renew_lifetime = 36000
   forwardable = true
   krb4_convert = false
 }
```

4. セカンダリー KDC サーバで kadmin ユーティリティを使用して，host プリンシパルを作成します。

```
# kadmin
Password for root/admin@EXAMPLE.LOCAL:
kadmin:  add_principal -randkey host/kdc2.example.local
WARNING: no policy specified for host/kdc2.example.local@EXAMPLE.LOCAL;
defaulting to no policy
Principal "host/kdc2.example.local@EXAMPLE.LOCAL" created.
```

5. セカンダリー KDC サーバで kadmin ユーティリティを使用して，キータブファイル（krb5.keytab）に host プリンシパルを追加します。
   host プリンシパルを追加したあと，正しく取得できたことを確認してください。

```
kadmin:  ktadd host/kdc2.example.local
Entry for principal host/kdc2.example.local with kvno 3, encryption type Triple
DES cbc mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5.keytab.
Entry for principal host/kdc2.example.local with kvno 3, encryption type DES
cbc mode with CRC-32 added to keytab WRFILE:/etc/krb5.keytab.
```

6. ファイル（kpropd.acl）を作成し，編集します。
   KDC データベースが格納されているディレクトリ（/var/kerberos/krb5kdc）に作成してください。また，作成したファイルに，KDC サーバドメインに参加しているすべてのセカンダリー KDC サーバのホストプリンシパルを追加してください。

```
# cat /var/kerberos/krb5kdc/kpropd.acl
host/kdc1.example.local@EXAMPLE.LOCAL
host/kdc2.example.local@EXAMPLE.LOCAL
```

7. プライマリーおよびセカンダリー KDC サーバで，kpropd デーモンを起動します。

```
# kpropd -S
```

8. プライマリー KDC サーバで，ダンプした KDC データベースのコピーをセカンダリー KDC サーバに転送します。
   cron を使用することで，この操作を定期的に実行できます。

```
# /usr/kerberos/sbin/kdb5_util dump /var/kerberos/krb5kdc/slave_datatrans
# kprop -d -f /var/kerberos/krb5kdc/slave_datatrans kdc2.example.local
3310 bytes sent.
Database propagation to kdc2.example.local: SUCCEEDED
```

9. セカンダリー KDC サーバで，スタッシュファイルを作成します。
   KDC データベースのマスター鍵が保持されます。

```
# /usr/kerberos/sbin/kdb5_util stash
Enter KDC database master key:
```

10. セカンダリー KDC サーバで Kerberos サーバデーモンを起動します。

```
# /usr/kerberos/sbin/krb5kdc
```

WORM 運用のための API

WORM 対応ファイルシステム内のファイルを WORM 化するには，ファイルにリテンション期間（保管期間）を設定して，読み取り専用に設定する必要があります。ファイルのリテンション期間を設定したり，延長したりするには，ユーザーが独自に作成するカスタムアプリケーションを使用します。ここでは，カスタムアプリケーションを作成するための API について説明します。

F.1 CIFS 共有のファイルの WORM 化

CIFS 共有のファイルを WORM 化する場合は，Windows の API を使用します。

F.1.1 WORM 化の手順

ファイルを WORM 化する手順を次にします。

1. 書き込みができるファイルを作成し，データを書き込みます。
2. ファイルにリテンション期間を設定します。
3. ファイルを読み取り専用にします。

F.1.2 WORM 化に必要な API

ファイルを WORM 化するのに必要な Windows の API を次の表に示します。

表 F-1： ファイルの WORM 化に必要な API（CIFS 共有の場合）

関数名	説明	参考資料
SetFileTime	ファイルにリテンション期間を設定します。	https://docs.microsoft.com/en-us/windows/win32/api/fileapi/nf-fileapi-setfiletime
SetFileAttributes	ファイルを読み取り専用にしたり，読み取り専用属性を解除したりします。	https://docs.microsoft.com/ja-jp/windows/win32/api/fileapi/nf-fileapi-setfileattributesa

F.1.2.1 SetFileTime

SetFileTime について説明します。

名称

SetFileTime

書式

```
BOOL SetFileTime(
   HANDLE         hFile,               //ファイルのハンドル
   CONST FILETIME *lpCreationTime,     //設定する作成日時
   CONST FILETIME *lpLastAccessTime,   //設定するアクセス日時
   CONST FILETIME *lpLastWriteTime     //設定する更新日時
);
```

機能説明

指定したファイルのタイムスタンプを更新します。

引数について

lpCreationTime と lpLastWriteTime は WORM 化には必要ないので，NULL（該当するタイムスタンプを更新しないという意味）を指定します。
なお，FILETIME 型はユーザーが直接対話的に扱うのには向いていないため，SYSTEMTIME 型で取得したデータを FILETIME 型に変換するプログラムにすることをお勧めします。FILETIME 型と SYSTEMTIME 型の構造体について，次の表に示します。

表 F-2：FILETIME 型と SYSTEMTIME 型の構造体

構造体名称	メンバー	説明	参考資料
FILETIME	DWORD dwLowDateTime; DWORD dwHighDateTime;	1601 年 1 月 1 日からの 100 ナノ秒間隔の数を表す 64 ビットの値です。SetFileTime の引数としてこの型が必要ですが，ユーザーが直接対話的に扱うのには向いていません。	http://msdn.microsoft.com/ja-jp/library/x3399a54.aspx
SYSTEMTIME	WORD wYear; WORD wMonth; WORD wDay; WORD wDayOfWeek; WORD wHour; WORD wMinute; WORD wSecond; WORD wMilliseconds;	各メンバーを使用して，年，月，日，曜日，時，分，秒およびミリ秒の時刻を表します。	http://msdn.microsoft.com/ja-jp/library/tc6fd5zs.aspx

F.1.2.2 SetFileAttributes

SetFileAttributes について説明します。

名称

SetFileAttributes

書式

```
BOOL SetFileAttributes (
   LPCTSTR   lpFileName,         //ファイル名
   DWORD     dwFileAttributes    //設定する属性
);
```

機能説明

指定したファイルの DOS 属性を設定します。

引数について

ファイルの現在の属性に特定の属性を追加したい場合は，対象ファイルから現在の属性を取得し，取得した属性と追加する属性の値を dwFileAttributes に指定する必要があります。

F.1.3 WORM 化に便利な API

ファイルを WORM 化するプログラムに利用できて便利な Windows の API を幾つか，次の表に示します。

表 F-3：WORM 化に便利な API

関数名	説明	参考資料
SystemTimeToFileTime	SYSTEMTIME 型のデータを SetFileTime が扱う FILETIME 型に変換します。	https://docs.microsoft.com/en-us/windows/win32/api/timezoneapi/nf-timezoneapi-systemtimetofiletime
LocalFileTimeToFileTime	ローカルタイムを協定世界時（UTC）に変換します。	https://docs.microsoft.com/en-us/windows/win32/api/fileapi/nf-fileapi-localfiletimetofiletime

関数名	説明	参考資料
CreateFile	SetFileTime に指定するファイルのハンドルを取得します。	https://docs.microsoft.com/en-us/windows/win32/api/fileapi/nf-fileapi-createfilea
GetFileAttributes	現在のファイル属性を取得します。	https://docs.microsoft.com/en-us/windows/win32/api/fileapi/nf-fileapi-getfileattributesa

F.1.4 サンプルプログラム

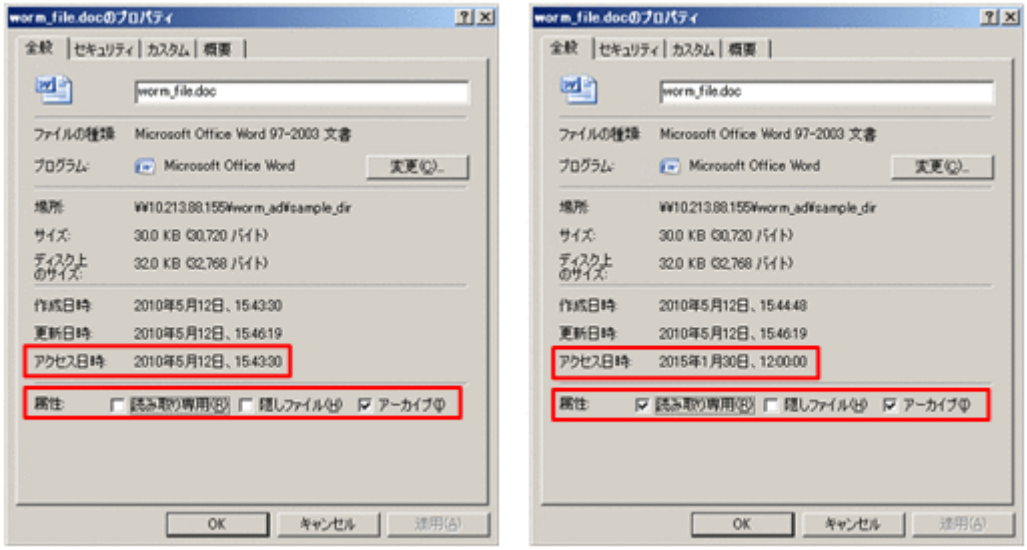
ファイルにリテンション期間を設定し，読み取り専用にする C 言語のプログラムの例を次に示します。

```
#include <windows.h>
#include <stdio.h>
#include <string.h>

void getTimestamp(FILETIME *ftLpTime, char *tcArgtime)
{
        SYSTEMTIME stFileTime;
        FILETIME   ftLocalFileTime;

        /*入力値をSYSTEMTIME型に変換*/
        memset(&stFileTime, 0, sizeof(SYSTEMTIME));
        sscanf(tcArgtime, "%d/%d/%d %d:%d:%d",
                &(stFileTime.wYear), &(stFileTime.wMonth),
                &(stFileTime.wDay), &(stFileTime.wHour),
                &(stFileTime.wMinute), &(stFileTime.wSecond)
        );
        stFileTime.wMilliseconds = 0;

        /*SYSTEMTIME型からFILETIME型に変換*/
        SystemTimeToFileTime(&stFileTime, &ftLocalFileTime);
        /*ローカルタイムを協定世界時(UTC)に変換*/
        LocalFileTimeToFileTime(&ftLocalFileTime, ftLpTime);
}
int main(int argc, char *argv[])
{
        char *filename;
        char *filetime;
        HANDLE h;
        FILETIME ftLastAccessTime;
        DWORD attr;

        /*引数チェック*/
        if (argc != 3) {
                fprintf(stderr, "usage: %s time file ¥n", argv[0]);
                fprintf(stderr, "       ex. time: ¥"2040/12/31 23:59:59¥"¥n");
                return 1;
        }
        filetime = argv[1];
        filename = argv[2];

        /*ファイルのハンドルを取得*/
        h = CreateFile(
                filename, FILE_WRITE_ATTRIBUTES, 0 , NULL ,
                OPEN_EXISTING , FILE_FLAG_BACKUP_SEMANTICS , NULL
        );
        if (h == INVALID_HANDLE_VALUE) {
                fprintf(stderr, "CreateFile error: ");
                return 1;
        }

        /*ファイルにリテンション期間を設定*/
        getTimestamp(&ftLastAccessTime, filetime);
        if (!SetFileTime(h, NULL, &ftLastAccessTime, NULL)) {
                fprintf(stderr, "SetFileTime error: ");
                CloseHandle(h);
                return 1;
        }
        CloseHandle(h);

        /*ファイルに読み取り専用属性を付与*/
        attr = GetFileAttributes(filename);
        attr |= FILE_ATTRIBUTE_READONLY;
        if (!SetFileAttributes(filename, attr)) {
                fprintf(stderr, "SetFileAttributes error: ");
                return 1;
        }

        return 0;
}
```

サンプルプログラムの実行例とサンプルプログラムを実行する前後のファイルのプロパティ表示例を次に示します。この例は，2015 年 1 月 30 日 12 時 00 分 00 秒をファイルのリテンション期間（保存期限）とすることを想定しています。

```
¥¥10.213.88.155¥worm_ad¥sample_dir¥worm.exe "2015/1/30 12:00:00"
¥¥10.213.88.155¥worm_ad¥sample_dir¥worm_file.doc
```

図 F-1： サンプルプログラムを実行する前後のファイルのプロパティ表示例（左：実行前，右：実行後）



F.2 NFS 共有のファイルの WORM 化

NFS 共有のファイルを WORM 化する場合は，システムコールを使用します。

F.2.1 WORM 化の手順

ファイルを WORM 化する手順を次にします。

1. 書き込みができるファイルを作成し，データを書き込みます。
2. ファイルにリテンション期間を設定します。
3. ファイルを読み取り専用にします。

F.2.2 WORM 化に必要な API

ファイルを WORM 化するのに必要な API のシステムコールを次の表に示します。

表 F-4： ファイルの WORM 化に必要な API（NFS 共有の場合）

システムコール	説明
utime() utimes()	ファイルにリテンション期間を設定します。
chmod() fchmod()	ファイルを読み取り専用にしたり，解除したりします。

F.2.2.1 utime()，utimes()

utime()，utimes() について説明します。

名称

utime
utimes

書式

```
#include <sys/types.h>
#include <utime.h>
int utime(const char *filename, const struct utimbuf *times);

#include <sys/time.h>
int utimes(const char *filename, const struct timeval times[2]);
```

機能説明

指定したファイルの最終アクセス時刻（atime）と修正時刻（mtime）を変更します。

引数について

リテンション期間として atime の値を設定し，mtime の値はファイルの現在の設定値を設定してください。なお，atime と mtime を同時に変更した場合は，リテンション期間の変更ではなくファイルの属性変更ということになって，システムコールがエラーとなります。また，WORM ファイルに対して atime の値を変更するシステムコールがある場合，リテンション期間の変更として処理されることがあります。
例として，utimbuf 構造体の設定内容を次に示します。

```
struct utimbuf {
        time_t actime;      //リテンション期間を設定
        time_t modtime;     //ファイルの現在の値を設定
};
```

F.2.2.2 chmod()，fchmod()

chmod()，fchmod() について説明します。

名称

chmod
fchmod

書式

```
#include <sys/stat.h>
int chmod(const char *path, mode_t mode);

int fchmod(int fd, mode_t mode);
```

機能説明

指定したファイルのパーミッションを変更します。

引数について

読み取り専用にする場合は，S_IWUSR（所有者），S_IWGRP（所属グループ）および S_IWOTH（その他ユーザー）の書き込み権限を，すべてオフに設定します。読み取り専用を解除する場合は，S_IWUSR，S_IWGRP および S_IWOTH の書き込み権限のどれかをオンに設定します。読み出し権限および実行権限の設定は変更できません。

F.2.3 サンプルプログラム

ファイルにリテンション期間を設定し，読み取り専用にするプログラムの例を次に示します。

第一引数に対象のファイル，第二引数にリテンション期間を指定してファイルを WORM 化するプログラムの例です。

リテンション期間は現在時刻を基点とした値で指定します。例えば，現在時刻から 300 秒間のリテンション期間を指定する場合，300 を指定します。数字の後に d，m または y を指定することで，リテンション期間を日，月，年で指定できます。なお，プログラムの実行前に NFS クライアントと HVFP のノードまたは Virtual Server の時刻を合わせておく必要があります。

```
#include <stdio.h>
#include <sys/types.h>
#include <utime.h>
#include <sys/stat.h>
#include <unistd.h>
#include <stdlib.h>


typedef enum { false = 0, true = 1 } boolean;

void
usage (char *cmd)
{
        printf ("usage: %s regular-file retention-time¥n", cmd);
        printf ("       retention-time format:¥n");
        printf ("           <numbers>d¥tdays¥n");
        printf ("           <numbers>m¥tmonth¥n");
        printf ("           <numbers>y¥tyear¥n");
        printf ("           <numbers>¥tsecond¥n");
}

time_t
set_worm_file(char *path, time_t retention_time)
{
        struct stat      st;
        struct utimbuf   utim;
        mode_t           new_mod;

        // ファイルの現在のatimeおよびmtimeの値を取得
        if (stat (path, &st) == -1) {
                return 0;
        }

        // リテンション期間を設定（mtimeは変更しない）
        utim.modtime = st.st_mtime;
        utim.actime  = retention_time;

        if (utime (path, &utim) == -1) {
                return 0;
        }

        // ファイルのパーミッションを読み取り専用に変更
        new_mod = (st.st_mode & ~(S_IWUSR | S_IWGRP | S_IWOTH));
        if (chmod (path, new_mod) == -1) {
                return 0;
        }

        if (stat (path, &st) == -1) {
                return 0;
        }

        return st.st_atime;       // success(return current access time).
}
```

```
boolean
is_file (char *path)
{
        struct stat      st;

        if (stat(path, &st) == -1) {
                return false;
        }

        if (S_ISREG(st.st_mode)) {
                return true;
        }

        return false;
}


time_t
convert_time (char *s)
{
        int      value;
        time_t   retval;
        time_t   now_time = time(NULL);

        if (sscanf (s, "%d", &value) == 1) {
                while (*s != '¥0') {
                        if (!isdigit (*s)) {
                                break;
                        }
                        s++;
                }
                switch (*s) {
                case 'd':
                case 'D':
                        printf ("unit is day.(%d)¥n", value);
                        value = (value * 24 * 3600);
                        break;

                case 'm':
                case 'M':
                        printf ("unit is month. (%d)¥n", value);
                        value = (value * 24 * 3600 * 30);
                        break;

                case 'y':
                case 'Y':
                        printf ("unit is year. (%d)¥n", value);
                        value = (value * 24 * 3600 * 30 * 365);
                        break;

                default:
                        printf ("unit is second. (%d)¥n", value);
                        break;
                }
        }

        retval = (time_t)value + now_time;
}


int
main (int ac, char **av)
{
        time_t  result;
        time_t  new_atime;

        if (ac < 3) {
                usage (av[0]);
                exit (0);
        }

        if (!is_file (av[1])) {
                usage (av[0]);
                exit (0);
        }

        // setting time information.
        new_atime = convert_time (av[2]);

        // ファイルをWORM化
        result = set_worm_file (av[1], new_atime);
```

```
        // リテンション期間を表示（表示が0だとWORM化されていない）
        printf ("new access time (%u)¥n", result);

        return 0;
}
```

リテンション期間として 600 秒を設定してファイル file01 を WORM 化するサンプルプログラムの実行例を次に示します。なお，ファイル file01 はサイズが 0 バイトではないと想定しています。

```
$ ./worm file01 600
unit is second. (600)
now time = 1264843082
new access time (1264843682)
```

F.2.4 ファイルアクセス時の WORM 固有のエラーとシステムコール

WORM ファイルにアクセスした場合に，NFS クライアントに返るおそれのある WORM 固有のエラーとクライアントからのシステムコールの関係を次の表に示します。

表 F-5： WORM ファイル関連のシステムコールとアクセス時のエラーとの関係

プロトコルバージョン	プロシジャー／オペレーション	NFS エラー	クライアントからのシステムコール
2	NFSPROC_SETATTR	NFSERR_ACCES NFSERR_IO	chmod，utime システムコール utime システムコールでエラーとなった場合，NFSERR_IO(EIO) を返す。
2	NFSPROC_LOOKUP	NFSERR_ACCES	ファイル参照のシステムコール一般（open システムコールなど）
2	NFSPROC_WRITE	NFSERR_ACCES	write システムコール
2	NFSPROC_CREATE	NFSERR_ACCES	creat システムコール
2	NFSPROC_REMOVE	NFSERR_ROFS	unlink システムコール
2	NFSPROC_RENAME	NFSERR_ACCES NFSERR_IO	rename システムコール ディレクトリの rename は NFSERR_IO を返す。ただし，空のディレクトリの名称変更が許可されている場合は，空のディレクトリの名称を変更できる。
3	NFS3PROC_SETATTR	NFS3ERR_ACCES NFS3ERR_IO	chmod，utime システムコール utime システムコールでエラーとなった場合，NFS3ERR_IO を返す。
3	NFS3PROC_LOOKUP	NFS3ERR_ACCES	ファイル参照システムコール一般（open システムコールなど）
3	NFS3PROC_WRITE	NFS3ERR_ACCES	write システムコール
3	NFS3PROC_CREATE	NFS3ERR_ACCES	creat システムコール
3	NFS3PROC_REMOVE	NFS3ERR_ROFS	unlink システムコール
3	NFS3PROC_RENAME	NFS3ERR_ACCES NFS3ERR_IO	rename システムコール ディレクトリの rename は NFS3ERR_IO を返す。ただし，空のディレクトリの名称変更が許可されている場合は，空のディレクトリの名称を変更できる。
3	NFS3PROC_COMMIT	NFS3ERR_IO	write/close システムコール
4	OP_CLOSE	NFS4ERR_IO	close システムコール
4	OP_COMMIT	NFS4ERR_IO	write/close システムコール
4	OP_CREATE	NFS4ERR_ACCESS	creat システムコール

プロトコルバージョン	プロシジャー/オペレーション	NFS エラー	クライアントからのシステムコール
4	OP_OPEN	NFS4ERR_ACCESS	open システムコール
4	OP_REMOVE	NFS4ERR_ROFS	unlink システムコール
4	OP_RENAME	NFS4ERR_ACCESS NFS4ERR_IO	rename システムコール ディレクトリの rename は NFS4ERR_IO を返す。ただし，空のディレクトリの名称変更が許可されている場合は，空のディレクトリの名称を変更できる。
4	OP_SETATTR	NFS4ERR_ACCESS NFS4ERR_IO	chmod，utime システムコール utime システムコールでエラーとなった場合，NFS4ERR_IO を返す。
4	OP_WRITE	NFS4ERR_ACCESS	write システムコール

なお，クライアントのアプリケーションに返るのは「NFS エラー」列に示した値ですが，アクセスに使用するプロトコルのバージョンによってエラー番号が異なるので，次の表に示すように読み替えてください。

表 F-6：エラー番号の読み替え

エラー番号	読み替え後
NFSERR_ACCES NFS3ERR_ACCES NFS4ERR_ACCES	EACCES
NFSERR_IO NFS3ERR_IO NFS4ERR_IO	EIO
NFSERR_ROFS NFS3ERR_ROFS NFS4ERR_ROFS	EROFS

注　クライアントによっては，ほかのエラー番号が返ることがあります。

G

参考資料

ここでは，参考資料として，関連する Web サイトを示します。

- G.1 Web サイト

G.1 Web サイト

Web サイトの URL を示します。

OpenLDAP

http://www.openldap.org

ADAM

http://technet.microsoft.com/en-us/library/cc736765(WS.10).aspx

略語一覧

ここでは，HVFP のマニュアルで使用している略語を示します。

H.1 HVFP のマニュアルで使用している略語

HVFP のマニュアルでは次に示す略語を使用しています。

ABE	Access Based Enumeration
ACE	access control entry
ACL	access control list
AES	Advanced Encryption Standard
AJP	Apache JServ Protocol
API	application programming interface
ARP	Address Resolution Protocol
ASCII	American Standard Code for Information Interchange
ASN	Abstract Syntax Notation
BDC	Backup Domain Controller
BMC	baseboard management controller
CA	certificate authority
CHA	channel adapter
CHAP	Challenge-Handshake Authentication Protocol
CIFS	Common Internet File System
CIM	Common Information Model
CLI	command line interface
CPU	central processing unit
CSR	certificate signing request
CSV	comma-separated values
CTL	controller
CU	control unit
CV	custom volume
DACL	discretionary access control list
DAR	Direct Access Recovery
DB	database
DBMS	database management system
DC	domain controller
DEP	data execution prevention
DES	Data Encryption Standard
DFS	distributed file system
DIMM	dual in-line memory module
DLL	dynamic-link library
DN	distinguished name
DNS	Domain Name System
DOM	Document Object Model
DOS	Disk Operating System
DRAM	dynamic random access memory
DSA	digital signal algorithm
DTD	Document Type Definition
ECC	error-correcting code
EUC	Extended UNIX Code
FC	Fibre Channel

FC-SP	Fibre Channel - Security Protocol
FIB	forwarding information base
FIFO	First In, First Out
FQDN	fully qualified domain name
FTP	File Transfer Protocol
FV	Fixed Volume
FXP	File Exchange Protocol
GbE	Gigabit Ethernet
GID	group identifier
GMT	Greenwich Mean Time
GPL	GNU General Public License
GUI	graphical user interface
HBA	host bus adapter
H-LUN	host logical unit number
HPFS	High Performance File System
HSSO	HiCommand single sign-on
HTML	HyperText Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
I/O	input/output
ICAP	Internet Content Adaptation Protocol
ICMP	Internet Control Message Protocol
ID	identifier
IP	Internet Protocol
IP-SW	IP switch
JDK	Java Development Kit
JIS	Japanese Industrial Standards
JSP	JavaServer Pages
KDC	Key Distribution Center
LACP	Link Aggregation Control Protocol
LAN	local area network
LBA	logical block addressing
LCD	Local Configuration Datastore
LDAP	Lightweight Directory Access Protocol
LDEV	logical device
LDIF	LDAP Data Interchange Format
LDKC	logical disk controller
LED	light-emitting diode
LF	Line Feed
LTS	long term support
LU	logical unit
LUN	logical unit number
LUSE	logical unit size expansion
LVI	Logical Volume Image
LVM	Logical Volume Manager
MAC	Media Access Control
MD5	Message-Digest algorithm 5

MIB	management information base
MMC	Microsoft Management Console
MP	microprocessor
MSS	maximum segment size
MTU	maximum transmission unit
NAS	Network-Attached Storage
NAT	network address translation
NDMP	Network Data Management Protocol
NetBIOS	Network Basic Input/Output System
NFS	Network File System
NIC	network interface card
NIS	Network Information Service
NTFS	New Technology File System
NTP	Network Time Protocol
OID	object identifier
ORB	object request broker
OS	operating system
PAP	Password Authentication Protocol
PC	personal computer
PCI	Peripheral Component Interconnect
PDC	Primary Domain Controller
PDU	protocol data unit
PID	process identifier
POSIX	Portable Operating System Interface for UNIX
PP	program product
RAID	Redundant Array of Independent Disks
RAM	random access memory
RAS	Reliability Availability Serviceability
RCS	Revision Control System
RD	relational database
RFC	Request for Comments
RID	relative identifier
RPC	remote procedure call
RSA	Rivest, Shamir, and Adleman
SACL	system access control list
SAN	storage area network
SAS	Serial Attached SCSI
SATA	serial ATA
SAX	Simple API for XML
SCSI	Small Computer System Interface
SFTP	SSH File Transfer Protocol
SHA	secure hash algorithm
SID	security identifier
SJIS	Shift JIS
SLPR	Storage Logical Partition
SMB	Server Message Block
SMD5	Salted Message Digest 5

SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
SP	service pack
SSD	solid-state drive
SSH	Secure Shell
SSHA	Salted Secure Hash Algorithm
SSL	Secure Sockets Layer
SSO	single sign-on
SVGA	Super Video Graphics Array
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
TOS	type of service
TTL	time to live
UAC	User Account Control
UDP	User Datagram Protocol
UID	user identifier
UNC	Universal Naming Convention
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UTC	Coordinated Universal Time
UTF	UCS Transformation Format
VDEV	Virtual Device
VLAN	virtual LAN
VLL	Virtual LVI/LUN
WADL	Web Application Description Language
WAN	wide area network
WINS	Windows Internet Name Service
WORM	Write Once, Read Many
WS	workstation
WWN	World Wide Name
WWW	World Wide Web
XDR	External Data Representation
XFS	extended file system
XML	Extensible Markup Language

索引

M

N

O

Q

S

U

W

X

あ

え

か

き

く

さ

り

ろ

iStorage M シリーズ

NAS オプション ソフトウェア

Virtual File Platform

ファイルアクセス（CIFS/NFS）

ユーザーズガイド

ＩＦ ３０６－１１

２０１６年　５月　初　版

２０２２年　５月１１　版

日本電気株式会社

東京都港区芝五丁目７番１号

TEL(03)3454-1111（大代表）