HITACHI
Inspire the Next

# Hitachi Virtual File Platform / Hitachi Data Ingestor

## ファイルアクセス（CIFS/NFS）ユーザーズガイド

## 対象製品

Hitachi Virtual File Platform
4.2.3-03 以降
Hitachi Data Ingestor
4.2.3-03 以降

## 輸出時の注意

本製品を輸出される場合には、外国為替及び外国貿易法の規制並びに米国輸出管理規則など外国の輸出関連法規をご確認の上、必要な手続きをお取りください。
なお、不明な場合は、弊社担当営業にお問い合わせください。

## 商標類

Active Directory は，米国 Microsoft Corporation の，米国およびその他の国における登録商標または商標です。
AIX 5L は，米国およびその他の国における International Business Machines Corporation の商標です。
AIX は，米国およびその他の国における International Business Machines Corporation の商標です。
HP Tru64 UNIX は，Hewlett-Packard Development Company, L.P.の商標です。
HP-UX は，Hewlett-Packard Development Company, L.P.のオペレーティングシステムの名称です。
IRIX は，Silicon Graphics, Inc.の登録商標です。
Itanium は，アメリカ合衆国およびその他の国における Intel Corporation の商標です。
Kerberos は，マサチューセッツ工科大学（MIT : Massachusetts Institute of Technology）で開発されたネットワーク認証のプロトコルの名称です。
Linux は，Linus Torvalds 氏の日本およびその他の国における登録商標または商標です。
Mac OS は，Apple Inc.の商標です。
Macintosh は，米国 Apple Computer, Inc.の商品名称です。
Microsoft Office Word は，米国 Microsoft Corporation の商品名称です。
Microsoft Office および Excel は，米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
Microsoft Office は，米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
Microsoft Word は，米国 Microsoft Corporation の商品名称です。
Microsoft および Excel は，米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
Microsoft および Hyper-V は，米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
Microsoft は，米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
MS-DOS は，米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
NetWare は，米国 Novell, Inc.の登録商標です。
Oracle と Java は，Oracle Corporation 及びその子会社，関連会社の米国 及びその他の国における登録商標です。
This product includes software developed by the Apache Software Foundation (http://www.apache.org/).
This product includes software developed by IAIK of Graz University of Technology.
OS/2 は，米国およびその他の国における International Business Machines Corporation の商標です。
PA-RISC は，Hewlett-Packard Development Company, L.P.の商標です。
POSIX は，the Institute of Electrical and Electronics Engineers, Inc. (IEEE)で制定された標準仕様です。
PowerPoint は，米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
Red Hat は，米国およびその他の国で Red Hat, Inc.の登録商標もしくは商標です。
RSA および BSAFE は，米国 EMC コーポレーションの米国およびその他の国における商標または登録商標です。
SOAP（Simple Object Access Protocol）は，分散ネットワーク環境において XML ベースの情報を交換するための通信プロトコルの名称です。
すべての SPARC 商標は，米国 SPARC International, Inc. のライセンスを受けて使用している同社の米国およびその他の国における商標または登録商標です。SPARC 商標がついた製品は，米国 Sun Microsystems, Inc. が開発したアーキテクチャに基づくものです。
SUSE は日本における Novell, Inc.の商標です。
Turbolinux は，ターボリナックス株式会社の商標または登録商標です。
Ubuntu は，Canonical Ltd.の登録商標です。
UNIX は，The Open Group の米国ならびに他の国における登録商標です。

VMware，VMware vSphere ESX，VMware vSphere ESXi は，米国およびその他の地域における VMware, Inc. の登録商標または商標です。
Windows は，米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
Windows NT は，米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
Windows Server は，米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
Windows Vista は，米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
XFS は，Silicon Graphics, Inc.の商標です。
Hitachi File Services Manager は，米国 EMC コーポレーションの RSA BSAFE(R)ソフトウェアを搭載しています。
This product includes software developed by Ben Laurie for use in the Apache-SSL HTTP server project.
Portions of this software were developed at the National Center for Supercomputing Applications (NCSA) at the University of Illinois at Urbana-Champaign.
This product includes software developed by the University of California, Berkeley and its contributors.
This software contains code derived from the RSA Data Security Inc. MD5 Message-Digest Algorithm, including various modifications by Spyglass Inc., Carnegie Mellon University, and Bell Communications Research, Inc (Bellcore).
Regular expression support is provided by the PCRE library package, which is open source software, written by Philip Hazel, and copyright by the University of Cambridge, England. The original software is available from ftp://ftp.csx.cam.ac.uk/pub/software/programming/pcre/.
This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (http://www.modssl.org/).
This product includes software developed by Daisuke Okajima and Kohsuke Kawaguchi (http://relaxngcc.sf.net/).
This product includes software developed by the Java Apache Project for use in the Apache JServ servlet engine project (http://java.apache.org/).
This product includes software developed by Andy Clark.
その他記載の会社名，製品名は，それぞれの会社の商標もしくは登録商標です。

## 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

2014 年 6 月（第 5 版）K6603835

## 著作権

# 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 Hitachi Virtual File Platform / Hitachi Data Ingestor（HVFP/HDI）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/HDI 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/HDI 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。

・Hitachi File Services Manager

・Configuration Manager

# 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」などの HVFP/HDI 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

Hitachi Content Platform（HCP）と連携している場合は，これらの知識のほかにも，HCP に関する基本的な知識をお持ちであることを前提としています。

# 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/HDI 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/HDI 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/HDI 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/HDI 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/HDI 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/HDI 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/HDI 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/HDI 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 と HDI でマニュアル体系が異なります。使用している製品に対するマニュアル体系を参照してください。

HVFP のマニュアル体系を次に示します。なお，モデルによって，ノードを冗長化するかどうかが異なります。ノードを冗長化する構成をクラスタ構成，冗長化しない構成をシングルノード構成と呼び，運用する構成に応じてお読みいただくマニュアルが異なります。

**表 はじめに -1 HVFP のマニュアル体系**

| マニュアル名 | 内容 |
|---|---|
| Hitachi Virtual File Platform / Hitachi Data Ingestor システム構成ガイド | 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。<br>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。 |
| Hitachi Virtual File Platform セットアップガイド | クラスタ構成の HVFP のセットアップ方法について説明しています。<br>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」をお読みください。 |
| Hitachi Virtual File Platform 仮想サーバ環境セットアップガイド | クラスタ構成の 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。 |
| Hitachi Virtual File Platform ユーザーズガイド | クラスタ構成の 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。 |
| Hitachi Virtual File Platform トラブルシューティングガイド | クラスタ構成の HVFP の障害対策を説明しています。 |
| Hitachi Virtual File Platform シングルノード構成セットアップガイド | シングルノード構成の HVFP のセットアップ方法について説明しています。 |
| Hitachi Virtual File Platform / Hitachi Data Ingestor シングルノード構成ユーザーズガイド | シングルノード構成の 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。 |
| Hitachi Virtual File Platform / Hitachi Data Ingestor シングルノード構成トラブルシューティングガイド | シングルノード構成の HVFP の障害対策を説明しています。 |
| Hitachi Virtual File Platform / Hitachi Data Ingestor コマンドリファレンス | クラスタ構成およびシングルノード構成の 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。 |
| Hitachi Virtual File Platform API リファレンス | クラスタ構成およびシングルノード構成の HVFP の API の使用方法について説明しています。 |
| Hitachi Virtual File Platform / Hitachi Data Ingestor メッセージリファレンス | クラスタ構成およびシングルノード構成の HVFP のメッセージについて説明しています。 |
| Hitachi Virtual File Platform / Hitachi Data Ingestor ファイルアクセス（CIFS/NFS）ユーザーズガイド（このマニュアル） | CIFS または NFS クライアントから，クラスタ構成およびシングルノード構成の 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。 |

HDI のマニュアル体系を次に示します。なお，HDI と HVFP では使用できる機能に相違があります。HVFP と HDI で共有しているマニュアルを参照する前に，「Hitachi Data Ingestor セットアップガイド」で機能の差異を確認してください。

**表 はじめに -2 HDI のマニュアル体系**

| マニュアル名 | 内容 |
|---|---|
| Hitachi Data Ingestor セットアップガイド | HDI を管理するために，最初にお読みいただくマニュアルです。<br>HDI のセットアップ方法について説明しています。 |
| Hitachi Virtual File Platform / Hitachi Data Ingestor システム構成ガイド | HDI 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。 |

| マニュアル名 | 内容 |
|---|---|
| Hitachi Virtual File Platform / Hitachi Data Ingestor シングルノード構成ユーザーズガイド | HDI 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。 |
| Hitachi Virtual File Platform / Hitachi Data Ingestor シングルノード構成トラブルシューティングガイド | HDI の障害対策を説明しています。 |
| Hitachi Virtual File Platform / Hitachi Data Ingestor コマンドリファレンス | HDI で使用できるコマンドの文法について説明しています。 |
| Hitachi Virtual File Platform / Hitachi Data Ingestor メッセージリファレンス | HDI のメッセージについて説明しています。 |
| Hitachi Virtual File Platform / Hitachi Data Ingestor ファイルアクセス（CIFS/NFS）ユーザーズガイド（このマニュアル） | CIFS または NFS クライアントから，HDI 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。 |
| Hitachi Data Ingestor 保守取扱説明書 | 「メッセージリファレンス」や「シングルノード構成トラブルシューティングガイド」などに記載されている，保守員に依頼している作業について，HDI での解決手順を説明しています。 |

# 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) |
| ADAM | Active Directory(R) Application Mode 1.0 |
| File Services Manager | 次の製品を区別する必要がない場合の表記です。<br>・ Configuration Manager<br>・ Hitachi File Services Manager |
| HCP | Hitachi Content Platform |
| HDI | Hitachi Data Ingestor |
| HVFP | Hitachi 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。<br>・ Mac OS(R) X v10.5<br>・ Mac OS(R) X v10.7<br>・ Mac OS(R) X v10.8 |
| 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。<br>・ Solaris 9 オペレーティングシステム SPARC プラットフォーム版<br>・ Solaris 10 オペレーティングシステム SPARC プラットフォーム版 |
| Sun Java System Directory Server | Sun Java(TM) System Directory Server 5.2 |
| VMware ESX | VMware vSphere(R) ESX |
| VMware ESXi | VMware vSphere(R) ESXi(TM) |
| Windows | Microsoft(R) Windows(R) Operating System |
| Windows 2000 Server | 次の製品を区別する必要がない場合の表記です。<br>・ Microsoft(R) Windows(R) 2000 Advanced Server Operating System |

| このマニュアルでの表記 | 製品名称または意味 |
|---|---|
| | ・ Microsoft(R) Windows(R) 2000 Server Operating System |
| Windows 7 | 次の製品を区別する必要がない場合の表記です。<br>・ Microsoft(R) Windows(R) 7 Enterprise x64 Edition<br>・ Microsoft(R) Windows(R) 7 Professional<br>・ Microsoft(R) Windows(R) 7 Professional x64 Edition<br>・ Microsoft(R) Windows(R) 7 Ultimate |
| Windows 8 | 次の製品を区別する必要がない場合の表記です。<br>・ Microsoft(R) Windows(R) 8 32-bit<br>・ Microsoft(R) Windows(R) 8 64-bit<br>・ Microsoft(R) Windows(R) 8 Enterprise 32-bit<br>・ Microsoft(R) Windows(R) 8 Enterprise 64-bit<br>・ Microsoft(R) Windows(R) 8 Pro 32-bit<br>・ Microsoft(R) Windows(R) 8 Pro 64-bit<br>・ Microsoft(R) Windows(R) 8.1 32-bit<br>・ Microsoft(R) Windows(R) 8.1 64-bit<br>・ Microsoft(R) Windows(R) 8.1 Enterprise 32-bit<br>・ Microsoft(R) Windows(R) 8.1 Enterprise 64-bit<br>・ Microsoft(R) Windows(R) 8.1 Pro 32-bit<br>・ Microsoft(R) Windows(R) 8.1 Pro 64-bit |
| Windows NT | Microsoft(R) Windows NT(R) Server Network Operating System |
| Windows Server 2003 | 次の製品を区別する必要がない場合の表記です。<br>・ Microsoft(R) Windows Server(R) 2003, Datacenter Edition for Itanium-based Systems<br>・ Microsoft(R) Windows Server(R) 2003, Datacenter Edition Operating System<br>・ Microsoft(R) Windows Server(R) 2003, Enterprise Edition for Itanium-based Systems<br>・ Microsoft(R) Windows Server(R) 2003, Enterprise Edition Operating System<br>・ Microsoft(R) Windows Server(R) 2003, Enterprise x64 Edition Operating System<br>・ Microsoft(R) Windows Server(R) 2003, Standard Edition Operating System<br>・ Microsoft(R) Windows Server(R) 2003 R2, Enterprise Edition Operating System<br>・ Microsoft(R) Windows Server(R) 2003 R2, Enterprise x64 Edition Operating System<br>・ Microsoft(R) Windows Server(R) 2003 R2, Standard Edition Operating System<br>・ Microsoft(R) Windows Server(R) 2003 R2, Standard x64 Edition Operating System |
| Windows Server 2008 | 次の製品を区別する必要がない場合の表記です。<br>・ Microsoft(R) Windows Server(R) 2008 Enterprise<br>・ Microsoft(R) Windows Server(R) 2008 Enterprise 32-bit<br>・ Microsoft(R) Windows Server(R) 2008 Standard<br>・ Microsoft(R) Windows Server(R) 2008 Standard 32-bit<br>・ Microsoft(R) Windows Server(R) 2008 R2 Enterprise<br>・ Microsoft(R) Windows Server(R) 2008 R2 Standard |
| Windows Server 2012 | 次の製品を区別する必要がない場合の表記です。<br>・ Microsoft(R) Windows Server(R) 2012 Datacenter<br>・ Microsoft(R) Windows Server(R) 2012 Essentials<br>・ Microsoft(R) Windows Server(R) 2012 Foundation<br>・ Microsoft(R) Windows Server(R) 2012 Standard<br>・ Microsoft(R) Windows Server(R) 2012 R2 Datacenter<br>・ Microsoft(R) Windows Server(R) 2012 R2 Essentials<br>・ Microsoft(R) Windows Server(R) 2012 R2 Foundation<br>・ Microsoft(R) Windows Server(R) 2012 R2 Standard |
| Windows Vista | 次の製品を区別する必要がない場合の表記です。<br>・ Microsoft(R) Windows Vista(R) Enterprise |

| このマニュアルでの表記 | 製品名称または意味 |
|---|---|
| | ・ Microsoft(R) Windows Vista(R) Enterprise x64 Edition |
| Windows XP | 次の製品を区別する必要がない場合の表記です。<br>・ Microsoft(R) Windows(R) XP Professional Operating System<br>・ Microsoft(R) Windows(R) XP Professional Operating System x64 Edition |
| Windows XP x64 | Microsoft(R) Windows(R) XP Professional Operating System x64 Edition |

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。

このマニュアルではほかのマニュアルを参照していただきたい場合，以降，「Hitachi Virtual File Platform ユーザーズガイド」と「Hitachi Virtual File Platform / Hitachi Data Ingestor シングルノード構成ユーザーズガイド」を「ユーザーズガイド」と表記し，「Hitachi Virtual File Platform トラブルシューティングガイド」と「Hitachi Virtual File Platform / Hitachi Data Ingestor シングルノード構成トラブルシューティングガイド」を「トラブルシューティングガイド」と表記しています。運用する構成に応じて，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。<br>（例）<br>［ファイルシステム］サブウィンドウ<br>［OK］ボタン<br>［Enter］キー |
| ＜ ＞ | 可変値であることを示します。<br>（例）＜ホスト名＞.＜ポート番号＞<br>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，どれか一つを指定することを示します。<br>（例 1）[A]<br>「何も指定しない」か「A を指定する」ことを示します。<br>（例 2）[B\|C]<br>「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

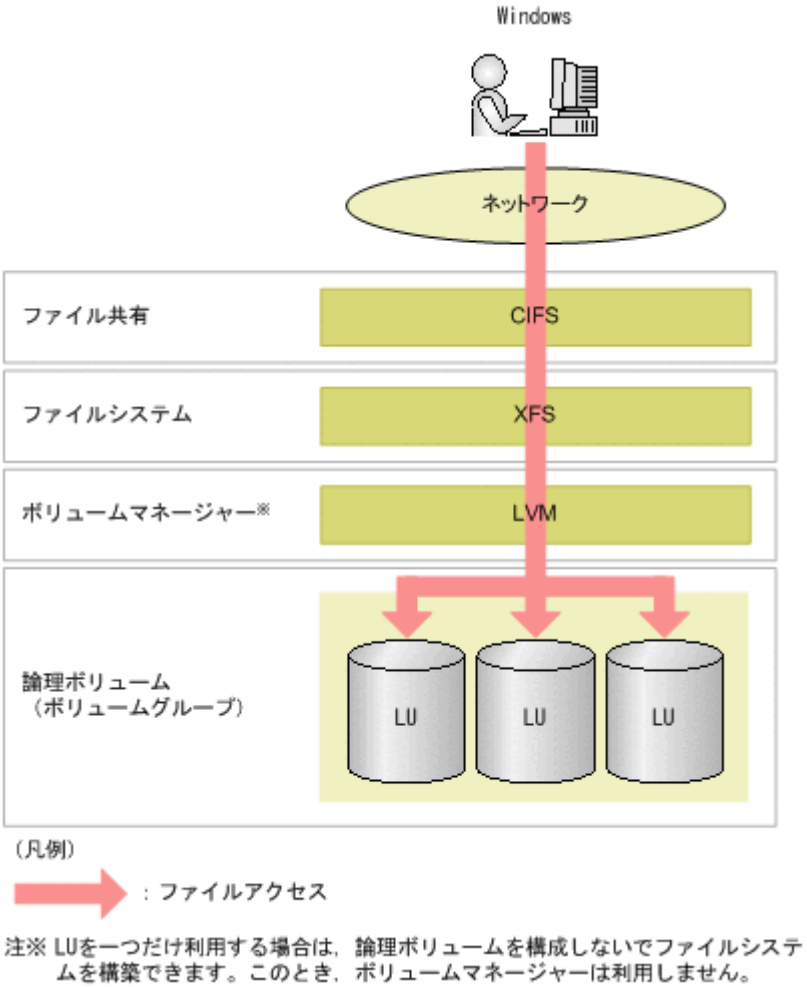
CIFS クライアントは Hitachi Virtual File Platform / Hitachi Data Ingestor（HVFP/HDI）の CIFS サービスを利用してデータにアクセスできます。この章では，CIFS サービス利用の概要について説明します。

# 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**



2

# CIFS サービス利用時のシステムの構成

この章では，HVFP/HDI 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。

## 2.1.1 CIFS クライアント

CIFS クライアントとしてサポートする製品を次に示します。

**表 2-1 CIFS クライアントとしてサポートする製品**

| CIFS クライアントのプラットフォーム | CIFS 接続の可否 | |
|---|---|---|
| | IPv4 接続 | IPv6 接続 |
| Mac OS(R) X v10.5 | ○ | × |
| Mac OS(R) X v10.7 | ○ | ○ |
| Mac OS(R) X v10.8 | ○ | ○ |
| Microsoft(R) Windows(R) 7 Enterprise x64 Edition（SP1） | ○ | ○ |
| Microsoft(R) Windows(R) 7 Professional（SP なし，または SP1） | ○ | ○ |
| Microsoft(R) Windows(R) 7 Professional x64 Edition（SP なし，または SP1） | ○ | ○ |
| Microsoft(R) Windows(R) 7 Ultimate（SP なし，または SP1） | ○ | ○ |
| Microsoft(R) Windows(R) 8 32-bit | ○ | ○ |
| Microsoft(R) Windows(R) 8 64-bit | ○ | ○ |
| Microsoft(R) Windows(R) 8 Enterprise 32-bit | ○ | ○ |
| Microsoft(R) Windows(R) 8 Enterprise 64-bit | ○ | ○ |
| Microsoft(R) Windows(R) 8 Pro 32-bit | ○ | ○ |
| Microsoft(R) Windows(R) 8 Pro 64-bit | ○ | ○ |
| 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 | ○ | ○ |
| Microsoft(R) Windows Server(R) 2003, Datacenter Edition for Itanium-based Systems（SP1） | ○ | × |
| Microsoft(R) Windows Server(R) 2003, Datacenter Edition Operating System（SP1） | ○ | × |
| Microsoft(R) Windows Server(R) 2003, Enterprise Edition for Itanium-based Systems（SP1） | ○ | × |
| Microsoft(R) Windows Server(R) 2003, Enterprise Edition Operating System（SP1） | ○ | × |
| Microsoft(R) Windows Server(R) 2003, Enterprise x64 Edition Operating System | ○ | × |
| Microsoft(R) Windows Server(R) 2003, Standard Edition Operating System（SP1） | ○ | × |
| Microsoft(R) Windows Server(R) 2003 R2, Enterprise Edition Operating System | ○ | × |
| Microsoft(R) Windows Server(R) 2003 R2, Enterprise x64 Edition Operating System | ○ | × |
| Microsoft(R) Windows Server(R) 2003 R2, Standard Edition Operating System（SP2） | ○ | × |

| CIFS クライアントのプラットフォーム | CIFS 接続の可否 | |
|---|---|---|
| | IPv4 接続 | IPv6 接続 |
| Microsoft(R) Windows Server(R) 2003 R2, Standard x64 Edition Operating System（SP2） | ○ | × |
| Microsoft(R) Windows Server(R) 2008 Enterprise（SP なし，または SP2） | ○ | ○ |
| Microsoft(R) Windows Server(R) 2008 Enterprise 32-bit（SP なし，または SP2） | ○ | ○ |
| Microsoft(R) Windows Server(R) 2008 Standard（SP なし，または SP2） | ○ | ○ |
| Microsoft(R) Windows Server(R) 2008 Standard 32-bit（SP なし，または SP2） | ○ | ○ |
| Microsoft(R) Windows Server(R) 2008 R2 Enterprise（SP なし，または SP1） | ○ | ○ |
| Microsoft(R) Windows Server(R) 2008 R2 Standard（SP なし，または SP1） | ○ | ○ |
| 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 | ○ | ○ |
| Microsoft(R) Windows Vista(R) Enterprise（SP1 または SP2） | ○ | ○ |
| Microsoft(R) Windows Vista(R) Enterprise x64 Edition（SP1 または SP2） | ○ | ○ |
| Microsoft(R) Windows(R) XP Professional Operating System (SP2 または SP3) | ○ | × |
| Microsoft(R) Windows(R) XP Professional Operating System x64 Edition（SP2） | ○ | × |

（凡例）○：接続できる　×：接続できない

CIFS クライアントが Windows 7，Windows 8，Windows Server 2008，Windows Server 2012 または Windows Vista の場合, SMB 2.0 を使用して CIFS サービスにアクセスするかどうかを設定できます。

## 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。

**表 2-2 Active Directory ドメインコントローラーとしてサポートする製品**

| Active Directory ドメインコントローラーのプラットフォーム | CIFS 接続の可否 | |
|---|---|---|
| | IPv4 接続 | IPv6 接続 |
| Microsoft(R) Windows Server(R) 2003, Datacenter Edition for Itanium-based Systems（SP1） | ○ | × |
| Microsoft(R) Windows Server(R) 2003, Datacenter Edition Operating System（SP1） | ○ | × |
| Microsoft(R) Windows Server(R) 2003, Enterprise Edition for Itanium-based Systems（SP1） | ○ | × |
| Microsoft(R) Windows Server(R) 2003, Enterprise Edition Operating System（SP1） | ○ | × |
| Microsoft(R) Windows Server(R) 2003, Enterprise x64 Edition Operating System | ○ | × |

| Active Directory ドメインコントローラーのプラットフォーム | CIFS 接続の可否 | |
|---|---|---|
| | IPv4 接続 | IPv6 接続 |
| Microsoft(R) Windows Server(R) 2003, Standard Edition Operating System（SP1） | ○ | × |
| Microsoft(R) Windows Server(R) 2003 R2, Enterprise Edition Operating System | ○ | × |
| Microsoft(R) Windows Server(R) 2003 R2, Enterprise x64 Edition Operating System | ○ | × |
| Microsoft(R) Windows Server(R) 2003 R2, Standard Edition Operating System（SP2） | ○ | × |
| Microsoft(R) Windows Server(R) 2003 R2, Standard x64 Edition Operating System（SP2） | ○ | × |
| Microsoft(R) Windows Server(R) 2008 Enterprise（SP なし，または SP2） | ○ | ○ |
| Microsoft(R) Windows Server(R) 2008 Enterprise 32-bit（SP なし，または SP2） | ○ | ○ |
| Microsoft(R) Windows Server(R) 2008 Standard（SP なし，または SP2） | ○ | ○ |
| Microsoft(R) Windows Server(R) 2008 Standard 32-bit（SP なし，または SP2） | ○ | ○ |
| Microsoft(R) Windows Server(R) 2008 R2 Enterprise（SP なし，または SP1） | ○ | ○ |
| Microsoft(R) Windows Server(R) 2008 R2 Standard（SP なし，または SP1） | ○ | ○ |
| 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 | ○ | ○ |

（凡例）○：接続できる　×：接続できない

Active Directory ドメインコントローラーとして Windows Server 2012 R2 を使用する場合，「SMB 1.0/CIFS ファイル共有のサポート」を無効にしないでください。無効にした場合は，Active Directory ドメインコントローラーとして使用できません。

## 2.2 ネットワークの構成

Hitachi Virtual File Platform / Hitachi Data Ingestor（HVFP/HDI）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/HDI 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 2-3 HVFP/HDI 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/HDI 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/HDI 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
- CIFS クライアントとして，Windows NT を使用する場合

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, 同じ NT ドメイン, 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/HDI 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/HDI 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/HDI 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」を参照してください。

- CIFS クライアントと HVFP/HDI 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/HDI 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/HDI 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/HDI 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/HDI が提供する CIFS サービスがローカルマスタブラウザ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，ローカルマスタブラウザ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ブラウザ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/HDI 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/HDI 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 NT ドメイン構成または Active Directory 構成にしてください。
- HVFP/HDI 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。
  - NT ドメイン構成のとき

    バックアップ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。

    ＜プライマリードメインコントローラーの IP アドレス＞ ＜ドメイン名＞#1B
  - Active Directory ドメイン構成のとき

    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/HDI 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/HDI 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

DNS を利用する場合，認証モードの設定時に指定するドメインコントローラーのサーバ名に対して，DNS で複数の IP アドレスを設定されていて，それにアクセスできない IP アドレスが含まれていると，ドメインコントローラーにアクセスできないおそれがあります。このような場合は，ドメインコントローラーのサーバ名とアクセスできる IP アドレスを，File Services Manager で hosts ファイルに追記してください。

## 2.2.5 DHCP を利用する場合

DHCP を利用する HDI の場合，Windows クライアントで DNS リゾルバキャッシュが有効になっていて名前解決の結果が最新ではなく，CIFS アクセスがエラーになることがあります。この場合は，Windows クライアントで ipconfig /flushdns コマンドを実行して DNS リゾルバキャッシュの内容を破棄し，再度 CIFS アクセスしてください。

3

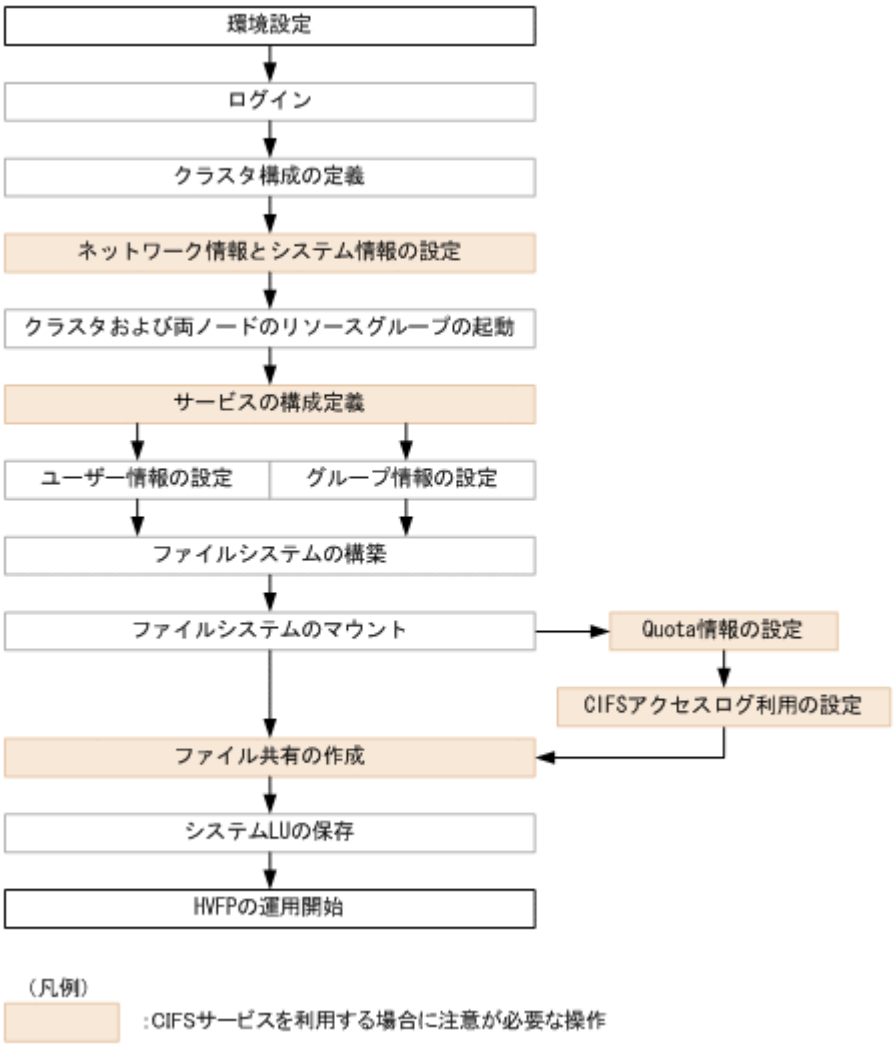
# File Services Manager での CIFS サービスの運用

この章では, HVFP/HDI 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/HDI 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」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/HDI 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」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/HDI 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」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 認証または NT ドメイン認証で，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」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。

### (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」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。<br>IPv4 の場合<br>ネットワークアドレスを指定する場合<br>IP アドレスを指定します<br>（例：「10.203.15.0」）。<br>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<br>＜ネットワークアドレス＞/＜ネットマスク＞<br>（例：「10.203.15.0/255.255.255.0」）<br>IPv6 の場合<br>アドレスプレフィックスを指定する場合<br>IP アドレスを指定します<br>（例：「fe80::223:7dff:0:0」）。<br>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<br>＜アドレスプレフィックス＞/＜プレフィックス長＞<br>（例：「fe80::223:7dff:0:0/64」） |

## (2) 認証モードの設定

CIFS サービスでは 4 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」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。<br>・ 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。<br>・ 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。 |
| 2 | NT server authentication | ［NT Server Authentication］ページで指定する情報について示します。<br>・ 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。<br>・ 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。 |
| 3 | NT domain authentication | ［NT Domain Authentication］ページで指定する情報について示します。<br>・ ［Domain name］には NT ドメイン名を指定します。<br>・ ［Domain administrator 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管理者を指定してください。 |
| 4 | Active Directory authentication | ［Active Directory Authentication］ページで指定する情報について示します。<br>・ ［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。<br>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。<br>・ ［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。<br>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。<br>ここで指定したユーザーは，ノードまたは Virtual Server を，Active Directory ドメインに参加させる際のユーザーアカウントとして使用されます。<br>なお，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，10 台を超えるサーバ（ここでは HVFP/HDI 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 Operator 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 Operator 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。<br>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。<br>◦ 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。<br>◦ 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。<br>・読み取り<br>・DNS ホスト名への検証された書き込み<br>・サービスプリンシパル名への検証された書き込み |

| # | 認証モード | 説明および注意事項 |
|---|---|---|
| | | ・パスワードのリセット<br>・パスワードの変更<br>・アカウントの制限の書き込み<br>・［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。 |

### (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」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。

### (4) SMB 2.0 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/HDI のノードまたは Virtual Server にアクセスします。この SMB プロトコルには，SMB 1.0 と SMB 2.0 があり，HVFP/HDI では CIFS サービスの構成定義で SMB 2.0 を使用するかどうかを選択できます。

ただし，HVFP/HDI では SMB 2.0 の次に示す機能についてはサポートしていません。

- シンボリックリンク
- ファイル属性のキャッシング
- HMAC SHA-256 ハッシュアルゴリズムによるメッセージ署名
- 永続性ファイルハンドル

また，CIFS サービスの構成定義で SMB2.0 を使用するように選択している場合でも，次に示すプラットフォームのクライアントからは SMB 1.0 を使用して CIFS アクセスします。

- Mac OS X
- Windows Server 2003
- Windows XP

なお，CIFS サービスの構成定義で SMB 2.0 を使用するかどうかを変更した場合，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。

## 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」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。

### 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」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。

## 3.5 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。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」，「コマンドリファレンス」を参照してください。なお，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。

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，「8.5 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。

## 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」を参照してください。
- 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/HDI 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 3-4 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<br>• フォルダの作成に成功または失敗したとき<br>• 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<br>• 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<br>• 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<br>• 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<br>• データの読み取りに成功または失敗したとき<br>• 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<br>• フォルダの作成に成功または失敗したとき<br>• 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<br>• 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<br>• 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<br>• 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<br>• 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 3-5 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。 |
| 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。 |
| 判定 | アクセスに成功したかどうかが出力されます。<br>OK<br>アクセスに成功した場合に出力されます。<br>NG<br>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。 |
| 契機 | CIFS アクセスログが採取された契機が出力されます。<br>opendir または closedir<br>フォルダ一覧を表示した場合に出力されます。<br>open または close<br>次のどちらかの場合に出力されます。<br>・データの読み取りを実施した場合<br>・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<br>mkdir<br>フォルダを作成した場合に出力されます。<br>unlink または rmdir<br>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。<br>sys_acl_get_file<br>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。<br>sys_acl_set_file<br>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。<br>chown<br>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。<br>connect または disconnect<br>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。<br>rename<br>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。 |
| 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。<br>O_RDONLY |

| 項目 | 説明 |
|---|---|
| | 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。<br>O_WRONLY<br>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。<br>O_RDWR<br>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。 |
| 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。 |

## 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」および「コマンドリファレンス」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」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/HDI 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/HDI 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 | NT ドメイン | NT ドメイン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。<br>・ 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<br>・ ユーザーマッピングを設定する |
| 5 | 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。<br>・ 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<br>・ 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」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/HDI の CIFS 共有にアクセスする場合，または HVFP/HDI 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/HDI 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/HDI 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/HDI 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。

## (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，「(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/HDI 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ィ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/HDI 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/HDI 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/HDI 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，ウィルスチェックを実施してください。
3. SSH で HVFP/HDI 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/HDI 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。

## (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。

  ¥/[]:|<>+=;,?*"

### (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) 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/HDI 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。

### (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/HDI の CIFS 共有にアクセスしたり，HVFP/HDI 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 ユーザー登録時の注意事項

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 1,023 グループになります。

上記の最大数を超えた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。

# 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/HDI 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/HDI 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/HDI 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/HDI 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，ADAM または Sun Java System Directory Server 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/HDI 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 | ○ |
| ADAM | | ○ |
| Sun Java System Directory Server | | ○ |

（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 ADAM 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，ADAM 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。

ADAM の LDAP サーバでは，検索する最大数（LDAP の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 1,000 エントリーです。
- LDAP サーバ内のユーザーマッピング情報の数が最大数を超えた場合，［Check for Errors］ダイアログの［List of RAS Information］ページ（［Batch-download］表示）でのユーザーマッピング情報のダウンロードに失敗します。そのため，検索結果の最大数が，管理するユーザー数とグループ数の和を超えるよう，`MaxPageSize` の制限を拡張します。

MaxPageSize の制限を拡張する手順を次に示します。なお，［ADAM ADSI 編集］ツールの詳細と，この手順の中で使用する用語については Microsoft 社のドキュメントを参照してください。

1. ［ADAM ADSI 編集］ツールを使用して，構成パーティションに接続します。
2. コンソールツリーを展開して，［CN=Services］，［CN=Windows NT］，［CN=Directory Service］，［CN=Query-Policies］の順にクリックします。
3. 詳細ウィンドウで［CN=Default Query Policy］をダブルクリックし，プロパティ画面で［lDAPAdminLimits］という属性をダブルクリックして，属性値を編集します。
4. ［MaxPageSize=1000］を選択して，［削除］ボタンをクリックします。
5. ［MaxPageSize=＜制限数＞］を入力して，［追加］ボタンをクリックします。

   ＜制限数＞には，File Services Manager でユーザーマッピングの設定を行うときに設定するユーザー ID の範囲とグループ ID の範囲を考慮して，最大ユーザー数と最大グループ数の合計値を設定してください。
6. ［OK］を 2 回クリックし，設定を終了します。

## 4.4.4 Sun Java System Directory Server 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, Sun Java System Directory Server 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。

Sun Java System Directory Server 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 2,000 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, Sun Java System Directory Server を使用して構築した LDAP サーバでの検索結果の最大数を［無制限］に変更する必要があります。

  検索結果の最大数を［無制限］に変更する手順を次に示します。なお，次の手順の中で使用する用語については Sun Java System Directory Server のドキュメントを参照してください。

1. Sun Java System Directory Server を使用して構築した LDAP サーバのコンソールの最上位にある［設定］タブでディレクトリツリーを表示し，［パフォーマンス］を選択します。
2. 右側のパネルで［クライアント制御］タブを選択します。
3. ［LDAP のサイズ制限］と［検索制限］で［無制限］のチェックボックスをチェックします。
4. ［保存］ボタンをクリックします。

   Sun Java System Directory Server の再起動を促すメッセージが表示されます。
5. ［了解］ボタンをクリックします。
6. ［タスク］タブをクリックして，Sun Java System Directory Server の再起動のボタンをクリックします。

   再起動を確認するダイアログが表示されるので，［はい］をクリックします。
7. ［Close］ボタンをクリックして，［Restart Directory Server］のダイアログボックスを閉じます。

## 4.4.5 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。

### (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/HDI 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
```

### (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。

## 4.4.6 ADAM を使用して LDAP サーバを構築するときの設定例

ここでは，ADAM 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。

### (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，ADAM 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/HDI では，LDAP 方式の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.ldf）を提供しています。リモートホストから SCP 機能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.ldf
```

なお，ADAM 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。

```
dn: CN=uidNumber,CN=Schema,CN=Configuration,DC=X
changetype: ntdsSchemaAdd
objectClass: top
objectClass: attributeSchema
cn: uidNumber
attributeID: 1.3.6.1.1.1.1.0
attributeSyntax: 2.5.5.9
isSingleValued: TRUE
showInAdvancedViewOnly: FALSE
adminDisplayName: uidNumber
adminDescription: An integer uniquely identifying a user in an
  administrative domain
oMSyntax: 2
searchFlags: 1
lDAPDisplayName: uidNumber
systemOnly: FALSE
systemFlags: 16

dn: CN=gidNumber,CN=Schema,CN=Configuration,DC=X
changetype: ntdsSchemaAdd
objectClass: top
objectClass: attributeSchema
cn: gidNumber
instanceType: 4
attributeID: 1.3.6.1.1.1.1.1
attributeSyntax: 2.5.5.9
isSingleValued: TRUE
showInAdvancedViewOnly: FALSE
adminDisplayName: gidNumber
adminDescription: An integer uniquely identifying a group in an
  administrative domain
oMSyntax: 2
searchFlags: 1
lDAPDisplayName: gidNumber
systemOnly: FALSE
systemFlags: 16

dn: CN=sambaSID,CN=Schema,CN=Configuration,DC=X
changetype: ntdsSchemaAdd
objectClass: top
objectClass: attributeSchema
cn: sambaSID
instanceType: 4
attributeID: 1.3.6.1.4.1.7165.2.1.20
attributeSyntax: 2.5.5.12
isSingleValued: TRUE
showInAdvancedViewOnly: FALSE
adminDisplayName: sambaSID
adminDescription: Security ID
oMSyntax: 64
searchFlags: 1
lDAPDisplayName: sambaSID
systemOnly: FALSE
systemFlags: 16

dn: CN=sambaUnixIdPool,CN=Schema,CN=Configuration,DC=X
changetype: ntdsSchemaAdd
objectClass: top
objectClass: classSchema
cn: sambaUnixIdPool
instanceType: 4
possSuperiors: container
subClassOf: top
governsID: 1.3.6.1.4.1.7165.1.2.2.7
rDNAttID: cn
showInAdvancedViewOnly: FALSE
adminDisplayName: sambaUnixIdPool
adminDescription: Pool for allocating UNIX uids/gids
objectClassCategory: 3
lDAPDisplayName: sambaUnixIdPool
systemOnly: FALSE
systemPossSuperiors: organizationalUnit
systemPossSuperiors: domainDNS
mustContain: uidNumber
mustContain: gidNumber
```

```
defaultSecurityDescriptor:
 D:(A;;RPWPCRCCDCLCLORCWOWDSDDTSW;;;DA)(A;;RPWPCRCCDCLCLORCWOWDS
 DDTSW;;;SY)(A;;RPLCLORC;;;AU)
systemFlags: 16
defaultHidingValue: FALSE

dn: CN=sambaIdmapEntry,CN=Schema,CN=Configuration,DC=X
changetype: ntdsSchemaAdd
objectClass: top
objectClass: classSchema
cn: sambaIdmapEntry
instanceType: 4
possSuperiors: container
subClassOf: top
governsID: 1.3.6.1.4.1.7165.1.2.2.8
rDNAttID: cn
showInAdvancedViewOnly: FALSE
adminDisplayName: sambaIdmapEntry
adminDescription: Mapping from a SID to an ID
objectClassCategory: 3
lDAPDisplayName: sambaIdmapEntry
systemOnly: FALSE
systemPossSuperiors: organizationalUnit
systemPossSuperiors: domainDNS
mustContain: sambaSID
mayContain: gidNumber
mayContain: uidNumber
defaultSecurityDescriptor:
 D:(A;;RPWPCRCCDCLCLORCWOWDSDDTSW;;;DA)(A;;RPWPCRCCDCLCLORCWOWDS
 DDTSW;;;SY)(A;;RPLCLORC;;;AU)
systemFlags: 16
defaultHidingValue: FALSE

dn: CN=sambaSidEntry,CN=Schema,CN=Configuration,DC=X
changetype: ntdsSchemaAdd
objectClass: top
objectClass: classSchema
cn: sambaSidEntry
instanceType: 4
possSuperiors: container
subClassOf: top
governsID: 1.3.6.1.4.1.7165.1.2.2.9
rDNAttID: sambaSID
showInAdvancedViewOnly: FALSE
adminDisplayName: sambaSidEntry
adminDescription: Structural Class for a SID
objectClassCategory: 1
lDAPDisplayName: sambaSidEntry
systemOnly: FALSE
systemPossSuperiors: organizationalUnit
systemPossSuperiors: domainDNS
mustContain: sambaSID
defaultSecurityDescriptor:
 D:(A;;RPWPCRCCDCLCLORCWOWDSDDTSW;;;DA)(A;;RPWPCRCCDCLCLORCWOWDS
 DDTSW;;;SY)(A;;RPLCLORC;;;AU)
systemFlags: 16
defaultHidingValue: FALSE
```

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，コマンドプロンプトで，次のコマンドを 1 行で入力して実行してください。

```
ldifde -i -f C:¥samba.ldf -s localhost:<port> -j . -k -c
"CN=Schema,CN=Configuration,DC=X" #schemaNamingContext
```

この例では，スキーマファイルが C:¥samba.ldf として保存されます。なお，<port>には ADAM をインストールするときに設定した LDAP ポート番号を指定します。`ldifde` コマンドは ADAM や Active Directory をインストールした場合にシステムに存在するコマンドです。ADAM の `ldifde` コマンドを使用するには，［スタート］－［すべてのプログラム］－［ADAM］－［ADAM ツール コマンド プロンプト］を選択してください。

### (2) index の設定

ADAM 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 を設定してください。

ADAM を使用すると，スキーマを拡張したときに，拡張した属性 `uidNumber`，`gidNumber`，`sambaSID` に index が設定されています。システムの既存の属性である objectClass に index を設定する手順を次に示します。なお，［ADAM ADSI 編集］ツールの詳細と，この手順の中で使用する用語については Microsoft 社のドキュメントを参照してください。

1. ［ADAM ADSI 編集］ツールを使用して，スキーマパーティションに接続します。
2. コンソールツリーを展開して，詳細ウィンドウで［cn=Object-Class］をダブルクリックします。
3. プロパティ画面にある［searchFlags］という属性をダブルクリックして，属性値を編集します。

   設定されている値は「8」になっているので，「9」に変更します。すでにほかの値に変更されている場合，設定されている値によって次のように指定してください。

   - 奇数の場合

     変更しないでそのまま設定します。
   - 偶数の場合

     設定されている値に 1 を足した値を設定します。
4. ［OK］を 2 回クリックして，ダイアログ画面を閉じます。

## 4.4.7 Sun Java System Directory Server を使用して LDAP サーバを構築するときの設定例

ここでは，Sun Java System Directory Server 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。

### (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，Sun Java System Directory Server 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/HDI では，LDAP 方式の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.ldif）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.ldif
```

なお，Sun Java System Directory Server 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。

```
dn: cn=schema
changetype:modify
add: attributeTypes
attributeTypes: ( 1.3.6.1.4.1.7165.2.1.20 NAME 'sambaSID' DESC 'Security ID'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 SINGLE-VALUE X-ORIGIN 'user defined' )
-
add:objectClasses
objectClasses: ( 1.3.6.1.4.1.7165.1.2.2.7 NAME 'sambaUnixIdPool' SUP top
  AUXILIARY MUST ( uidNumber $ gidNumber ) X-ORIGIN 'user defined' )
-
add:objectClasses
objectClasses: ( 1.3.6.1.4.1.7165.1.2.2.8 NAME 'sambaIdmapEntry' SUP top
```

```
  AUXILIARY MUST sambaSID MAY ( uidNumber $ gidNumber ) X-ORIGIN
  'user defined' )
-
add:objectClasses
objectClasses: ( 1.3.6.1.4.1.7165.1.2.2.9 NAME 'sambaSidEntry' SUP top
  STRUCTURAL MUST sambaSID X-ORIGIN 'user defined' )
-
```

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，次のコマンドを実行して，スキーマを拡張します。パスワードを要求されたときには，インストールしたときに cn=Directory Manager に設定されたパスワードを入力してください。

```
#ldapmodify -h <host> -p <port> -D "cn=Directory Manager" -w - -f samba.ldif
```

ldapmodify コマンドは，Sun Java System Directory Server で提供されているコマンドを使用してください（OpenLDAP で提供されている同じコマンドは使用しないでください）。<host>には，Sun Java System Directory Server を使用して構築した LDAP サーバのホスト名を指定します。また，<port>には，Sun Java System Directory Server をインストールするときに設定した LDAP ポート番号を指定します。

### (2) index の設定

Sun Java System Directory Server 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 を設定してください。

Sun Java System Directory Server を使用すると，属性 objectClass に等価インデックスが設定されています。ユーザーマッピングを利用する場合，Sun Java System Directory Server の定義で，uidNumber，gidNumber，sambaSID に等価インデックス（eq）を設定することを推奨します。

uidNumber，gidNumber，sambaSID に等価インデックス（eq）を設定する手順を次に示します。なお，次の手順の中で使用する用語については Sun Java System Directory Server のドキュメントを参照してください。

1. Sun Java System Directory Server を使用して構築した LDAP サーバのコンソールの最上位にある［設定］タブで［データ］ノードを展開し，インデックスを生成するサフィックスを選択します。
2. 右側のパネルで［インデックス］タブを選択します。

   システムインデックスのテーブルは変更できません。
3. ［追加インデックス］テーブルの属性でインデックスを追加します。
4. インデックスが生成されていない属性のインデックスを追加するときは，［属性の追加］ボタンをクリックします。

   ダイアログが表示されるので，インデックスを生成する uidNumber，gidNumber，sambaSID を選択し，［了解］をクリックします。
5. 属性のインデックスを変更するときは，［追加インデックス］テーブルで，その属性で維持するインデックスのタイプのチェックボックスを選択します。

   uidNumber，gidNumber，sambaSID の［等価］インデックスのチェックボックスにチェックが付いていることを確認し，［実在］インデックスのチェックボックスのチェックを外してください。そのほかのチェックボックスにはチェックを付けないでください。
6. ［保存］をクリックして，新しいインデックス設定を保存します。

   新しいインデックスを利用するには，データベースファイルの更新が必要であることを示すダイアログが表示されます。

サフィックスのインデックスの再生成を行うか，サフィックスを再初期化できます。ここでは，まだマッピング情報が登録されてないため，［何もしない］を選択します。

# 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。

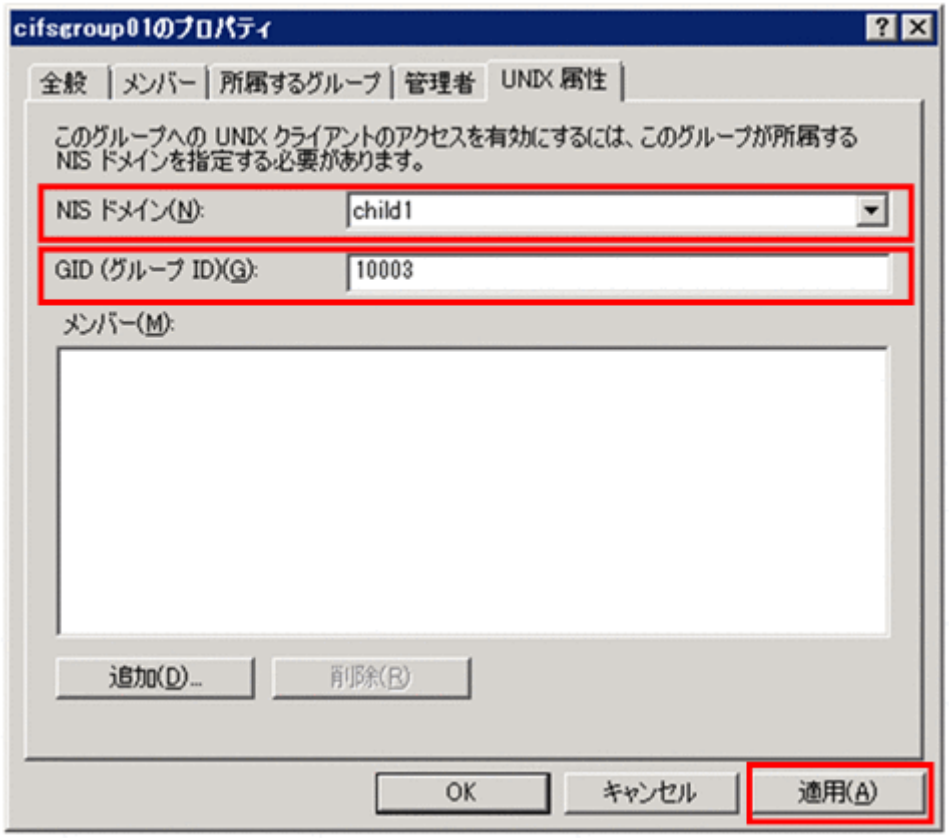
ここでは，その手順について説明します。

### (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




## (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

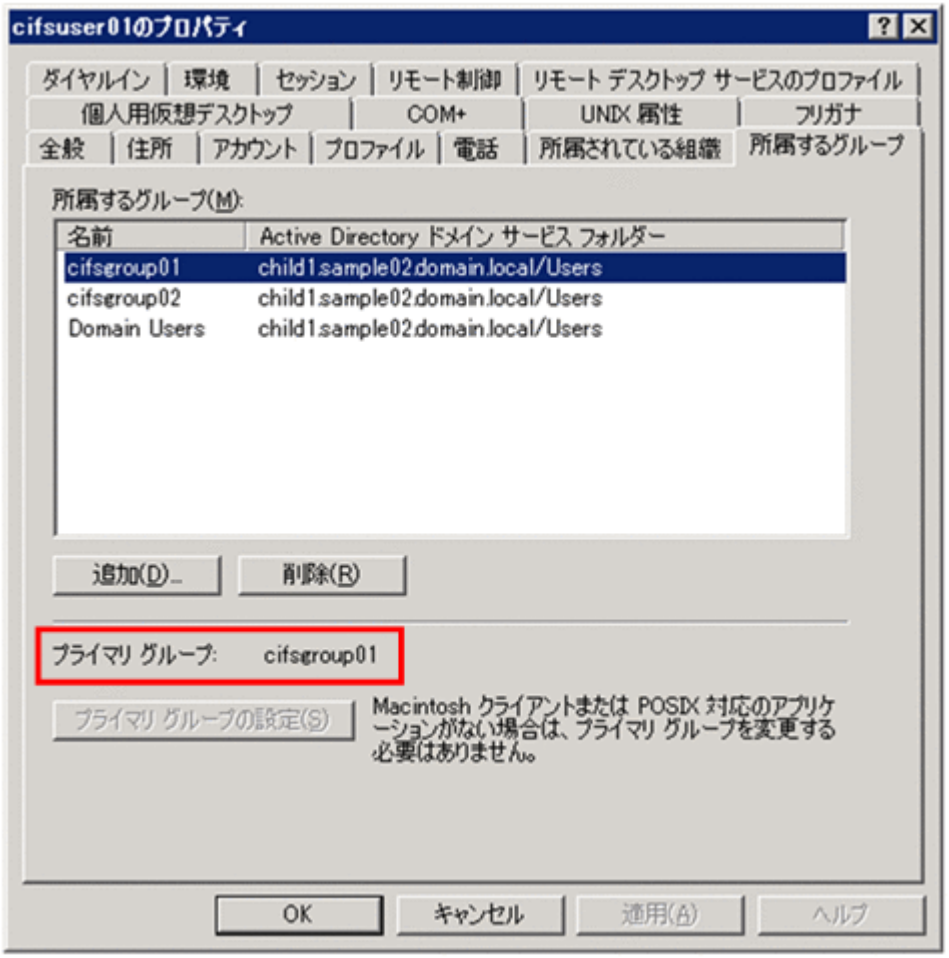
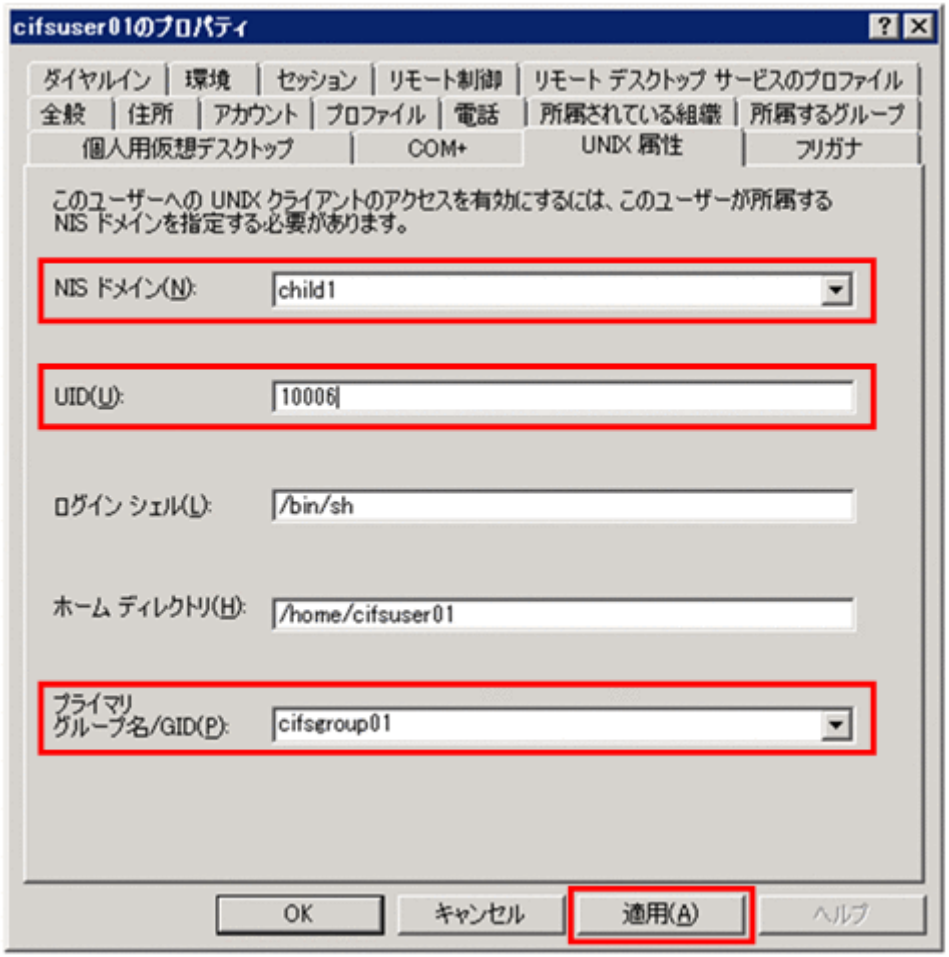


図 4-3 ユーザーの［プロパティ］画面の［UNIX 属性］タブの表示例




## 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。

### (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 または NT ドメイン内のグループの 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 または NT ドメイン内のグループの 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
```

### (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 または NT ドメイン内のユーザーの 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 または NT ドメイン内のユーザーの 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 または NT ドメイン内のユーザーの 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

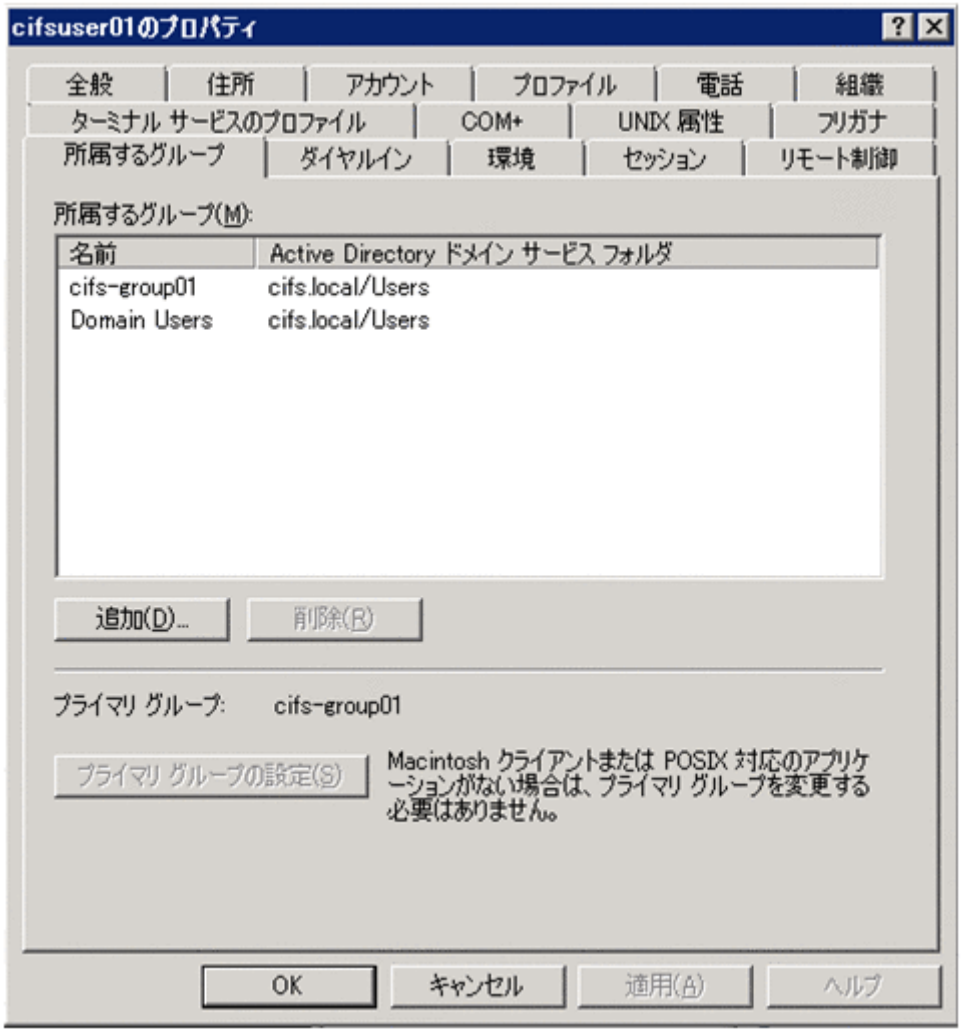
ここでは，ユーザーマッピングの方式が Active Directory スキーマ方式で，かつ［CIFS Service Management］ページ（Setting Type：User mapping）の［User mapping setup］で［Name service switch］に［Using LDAP as a network information service (RFC2307)］を指定してユーザーを管理する場合について補足説明します。

HVFP/HDI 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。

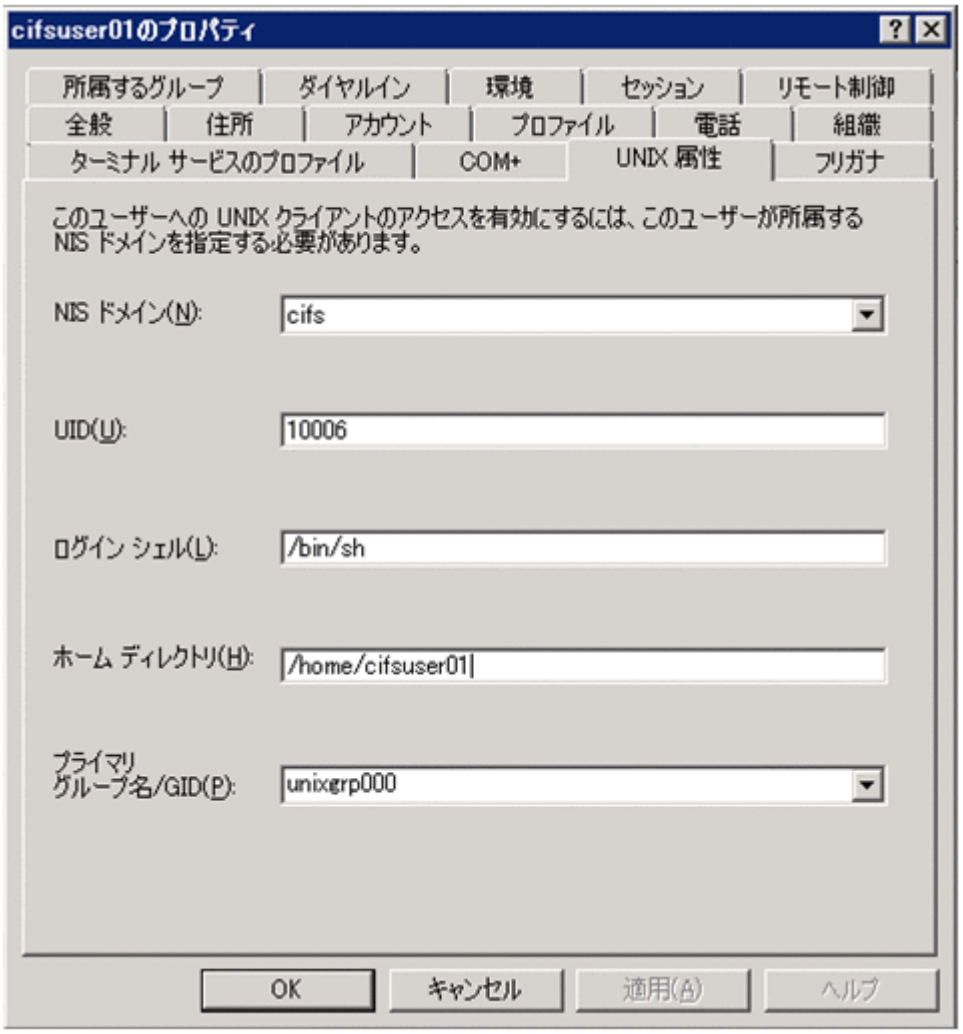
**図 4-4 ［所属するグループ］タブの表示例**




- 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/HDI 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。

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 NT server 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。

CIFS サービスの認証モードが NT Server Authentication のときに，SMB パスワードを管理しているサーバで，匿名のクライアントからの接続を拒否しないように設定してください。匿名のクライアントからの接続が拒否されている場合，CIFS サービスの起動に失敗します。

## 5.3 NT domain 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 NT ドメイン認証をする場合は，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 NT ドメイン認証をする場合は，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。

NT ドメイン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 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に示す内容を確認してください。

NT ドメイン認証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，CIFS サービスを再起動してください。

- 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）

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/HDI 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/HDI 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

# 5.4 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。

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 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）

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/HDI 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/HDI 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/HDI 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/HDI 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

HVFP/HDI 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/HDI 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/HDI 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。

## 5.5 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。 |

| # | 確認項目 | 確認内容 | 対策 |
|---|---|---|---|
| 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」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」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。

ユーザーマッピングで使用する LDAP サーバへの接続が失敗した場合は，接続の失敗を検知してから 5 分間は LDAP サーバへアクセスできません。そのため，CIFS サービスで LDAP サーバへアクセスする必要があるユーザー（新規ドメインユーザー，キャッシュをクリアしたあとのドメインユーザー）は，CIFS サービスにアクセスできなくなります。この場合，LDAP サーバへ接続できなくなる障害を取り除き，5 分後または CIFS サービスを再起動したあとに CIFS サービスへアクセスし

てください。障害を取り除くときにLDAPサーバを再起動する場合，LDAPサーバを再起動したあとにCIFSサービスを再起動してください。

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，5分後またはCIFSサービスを再起動したあとにCIFSサービスへアクセスしてください。

CIFSクライアントから短時間・大量接続をする際，HVFP/HDI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/HDI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/HDI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/HDI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/HDI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/HDI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/HDI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/HDI 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/HDI 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「8.2 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，UID および GID を解決できることが前提です。 |
| | | グループ | 不可 | 可 | － |
| | | 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 | － |
| 3 | ACL の移行 | 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※1※2（POSIX ACL にマッピング） | 可 | － |
| | | SACL（監査 ACL） | 不可※3 | 不可※3 | － |
| 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※3 | 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※3 | 可 | － |
| | | 隠し属性 | 可※3 | 可 | － |

| # | 項目 | | Classic ACL タイプ | Advanced ACL タイプ | 備考 |
|---|---|---|---|---|---|
| | | ディレクトリ属性 | 可 | 可 | ― |
| | | 暗号化属性 | 不可※3 | 不可※3 | 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※3 | 不可※3 | 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 | ― |
| 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※4 | 不可※4 | ― |

（凡例）可：移行できる　不可：移行できない　―：備考なし

注※1

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※2

DACL に HVFP/HDI で認識できないユーザーまたはグループが含まれている場合，その ACE は除外して移行されます。

注※3

HVFP/HDI 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※4

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/HDI 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。 |

| # | コマンド／アプリケーション | 移行に関する留意事項 |
|---|---|---|
| | | HVFP/HDI 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/HDI で認識できるユーザーとは，HVFP/HDI 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/HDI で認識できるユーザー・グループとなり，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/HDI 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/HDI で認識できないユーザー・グループとなります。

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/HDI 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/HDI 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」を参照してください。
- CIFS サービス構成定義の認証方法が NT ドメイン認証または Active Directory 認証以外の場合，もしくは NT ドメイン認証または 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/HDI 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/HDI 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/HDI 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/HDI 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/HDI 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/HDI 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。

## 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/HDI 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/HDI 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/HDI 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」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/HDI 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」を参照してください。

参考

HVFP/HDI 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/HDI 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/HDI 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/HDI 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/HDI 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」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/HDI 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/HDI 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。

- ¥¥<ノード名または 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※

ノード名または Virtual Server 名は，HVFP/HDI 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。

なお，IPv6 接続で CIFS 共有にアクセスする場合，ノード名，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/HDI 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/HDI 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/HDI 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（クラスタ構成の場合）および表 7-3 CIFS クライアントの最大接続数および CIFS 共有数の上限値（シングルノード構成の場合）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/HDI 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/HDI にアクセスしなかった場合，HVFP/HDI 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」を参照してください。

  ユーザーが，HVFP/HDI 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/HDI 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（クラスタ構成の場合）**

| 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） |
|---|---|---|---|---|
| VFP2010 | － | × | 5,000 | 7,500 |
| | | ○ | 2,000 | 256 |
| VFP2100 | － | × | 12,000 | 7,500 |
| | | ○ | 4,800 | 256 |
| VFP2300 | － | × | 12,000 | 7,500 |
| | | ○ | 4,800 | 256 |
| VFP100N | － | × | 5,000 | 7,500 |
| | | ○ | 2,000 | 256 |
| VFP300N | － | × | 12,000 | 7,500 |
| | | ○ | 4,800 | 256 |
| VFP500N | － | × | 24,000 | 7,500 |
| | | ○ | 9,600 | 256 |
| VFP110 | － | × | 6,000 | 7,500 |
| | | ○ | 2,000 | 256 |
| VFP200N | 16GB | × | 6,000 | 7,500 |

| モデル | メモリー量 | 自動<br>リロード | CIFS クライアントの<br>最大接続数<br>（1 クラスタ当たり） | CIFS 共有数の上限<br>（1 クラスタ当たり） |
|---|---|---|---|---|
| | | ○ | 2,000 | 256 |
| | 32GB | × | 12,000 | 7,500 |
| | | ○ | 4,800 | 256 |
| VFP600N | 32GB | × | 24,000 | 7,500 |
| | | ○ | 9,600 | 256 |
| | 64GB | × | 24,000 | 7,500 |
| | | ○ | 9,600 | 256 |
| | 96GB | × | 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

**表 7-3 CIFS クライアントの最大接続数および CIFS 共有数の上限値（シングルノード構成の場合）**

| モデル | 自動<br>リロード | CIFS クライアントの<br>最大接続数<br>（ノード当たり） | CIFS 共有数の上限<br>（ノード当たり） |
|---|---|---|---|
| HDI | × | 30 | 7,500 |
| | ○ | 30 | 256 |
| VFP50 | × | 100 | 7,500 |
| | ○ | 100 | 256 |
| VFP70 | × | 300 | 7,500 |
| | ○ | 300 | 256 |
| VFP80 | × | 300 | 7,500 |
| | ○ | 300 | 256 |
| VFP110 | × | 6,000 | 7,500 |
| | ○ | 2,000 | 256 |
| VFP2010 | × | 5,000 | 7,500 |
| | ○ | 2,000 | 256 |
| VFP200N | × | 6,000 | 7,500 |
| | ○ | 2,000 | 256 |

（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と，クライアントからの書き込み要求およびクローズ要求に同期して書き込む設定をしている CIFS 共有内で，ファイルに先にアクセスした CIFS クライアントに書き込み要求がキャッシュされているときに，ほかの CIFS クライアントから同一のファイルを開こうとすると，書き込みとディスクドライブへのフラッシュが優先して実行されます。そのため，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。

- 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ように設定した場合，複数クライアントから 1 つのファイルに同時にアクセスすると，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アクセス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 共有内に保存してください。なお，読み取り専用のクライアントキャッシュを使用するように設定すると，複数の CIFS クライアントから 1 つのファイルへの読み取りアクセスが競合してもアクセス遅延は発生しません。ただし，書き込みアクセスや排他アクセスの場合は，アクセス遅延が発生するおそれがあります。
- 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/HDI 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 10,000 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。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 7-4 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。 |

| 操作 | 確認事項 |
|---|---|
| | ・［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。<br>・ 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。<br>・ 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。<br>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」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。<br>・［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。<br>・ 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。<br>・ オンラインバックアップが実行中でない。<br>・［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。<br>・ 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」および「コマンドリファレンス」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」を参照してください。
- Hitachi Content Platform（HCP）と連携しているファイルシステムのスタブファイルを CIFS クライアントが削除した場合に，HCP の障害などで HCP 上でのファイルの削除処理が失敗しても，削除できたように CIFS クライアントに表示されることがあります。このため，HCP 連携しているファイルシステムのスタブファイルを削除した場合は，対象ファイルのフォルダを再表示するなどして，削除されているかどうかを確認してください。
- LU 障害の回復に伴ってファイルシステムを再作成する場合は，HCP にマイグレートしていたデータを HVFP/HDI のファイルシステムにリストアできます。HCP にデータをマイグレートしていたファイルシステムをリストアする手順については，「トラブルシューティングガイド」を参照してください。

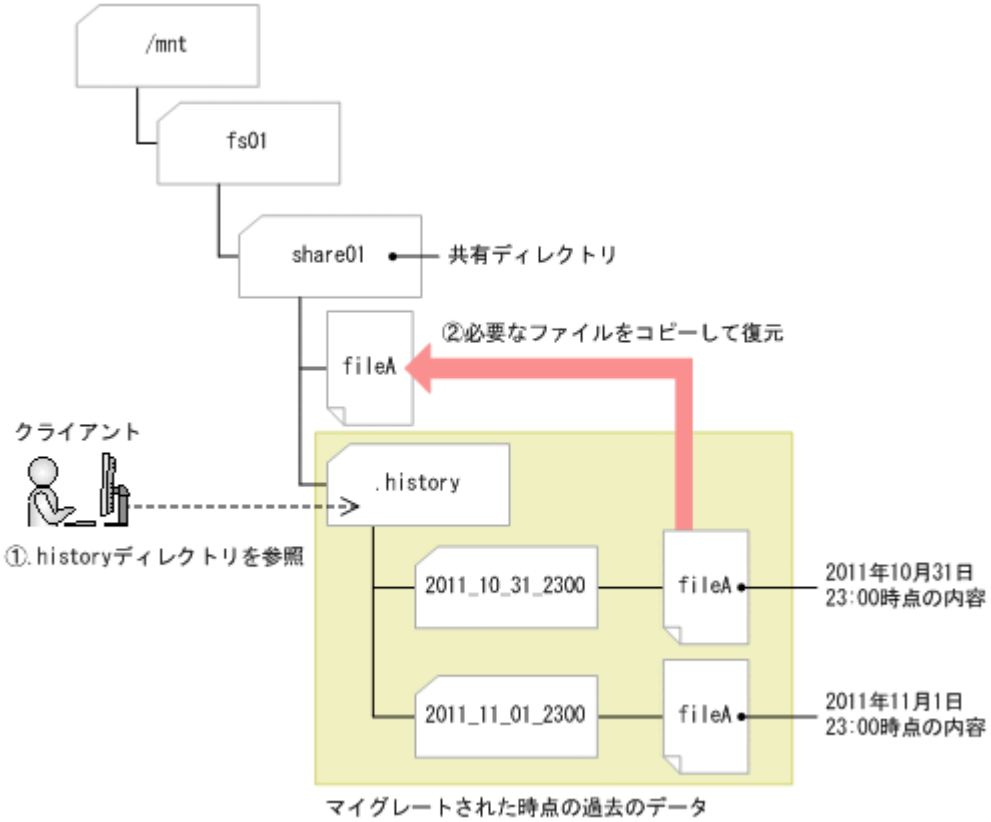
  システム管理者が回復手順を実施したあと，すべてのデータがリストアされるまでに時間が掛かるため，リストアされていないデータにクライアントがアクセスすることがあります。このとき，親ディレクトリに大量のデータが格納されていると，ファイル一覧の表示に時間が掛かるため，CIFS クライアントでタイムアウトが発生し，アクセスに失敗するおそれがあります。CIFS

クライアントでネットワークエラーなどのエラーが表示された場合は，しばらくしてから再度アクセスしてください。

- HCP と連携しているファイルシステムの場合，CIFS クライアントに.arc というフォルダが表示されることがありますが，.arc フォルダはシステムが使用するフォルダなので操作しないでください。
- HCP にマイグレートされたデータは，HCP のバージョン管理（versioning）によって，マイグレーションが実行された日時ごとに世代管理されます。HVFP/HDI では，HCP で世代管理されているデータを使用して，マイグレーションが実行された時点のディレクトリ構成を再現できます。再現されたディレクトリを HVFP/HDI のクライアントに公開することで，クライアントが誤ってファイルを削除してしまった場合でも，ファイル単位でデータを復元できます。

  マイグレーションが実行された時点のディレクトリ構成を再現するように設定すると，ファイルシステムの共有ディレクトリ下に，.history という読み取り専用のディレクトリが作成されます。.history ディレクトリ下には，マイグレーションが実行された日時を示すディレクトリ（過去バージョンディレクトリ）が作成されます。このディレクトリの種別や更新日時などの属性情報は，マイグレーションが実行されたときの共有ディレクトリの情報が復元されています。ディレクトリ内のファイルにクライアントがアクセスすると，HCP からデータがリコールされて，マイグレートされた時点のデータを参照できます。アクセスされたファイルのデータだけがリコールされ，リコールされたデータはファイルがクローズされる際に削除されるため，ファイルシステムの使用量を最小限に抑えられます。

**図 7-1 バージョン管理を利用したファイルの復元**




バージョン管理を利用したファイルの復元を有効にする前に考慮しておくことを次に示します。

- .history ディレクトリに格納するデータの保持期間に，運用に応じた日数を設定してください。

- 対象のファイルシステムに障害が発生してデータをリストアした場合は，.historyディレクトリも復元されます。ただし，保持期間を過ぎたファイルやディレクトリは復元されません。

バージョン管理を利用したファイルの復元を有効にするためには，マイグレーションポリシーを設定したり，ファイルシステムを構築したりするときに，HCPにマイグレートしたファイルの過去バージョンをクライアントに公開するかどうかを設定します。設定方法については，「ユーザーズガイド」または「コマンドリファレンス」を参照してください。

なお，CIFSクライアントが.historyディレクトリを参照するには，共有ディレクトリで，すべてのファイルとフォルダが表示されるよう設定する必要があります。

- 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。
- HCPにマイグレートされたデータをエンドユーザーごとにほかのHVFP/HDIから使用する場合に，通信障害などが原因でHVFP/HDI間でデータが同期されていない状態でホームディレクトリを更新したとき，更新したユーザーのホームディレクトリ下に.conflictディレクトリが作成されて，更新したデータが読み取り専用で格納されることがあります。

  ホームディレクトリローミング対応ファイルシステムのファイルを操作した場合，エンドユーザーはホームディレクトリ下の.conflictディレクトリに必要なファイルが格納されていないか，確認してください。なお，.conflictディレクトリ下のファイルを利用する場合，ホームディレクトリ内の.conflictディレクトリ以外の任意の場所にファイル単位でコピーしてから使用してください。ディレクトリごとコピーすると，アクセス権が意図したとおりに設定されないことがあります。

  エンドユーザーが.conflictディレクトリを参照するには，すべてのファイルとフォルダが表示されるようクライアント側で設定する必要があります。

## 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 でウィ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 でウィ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ィ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ィ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，ウィ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/HDI 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/HDI 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

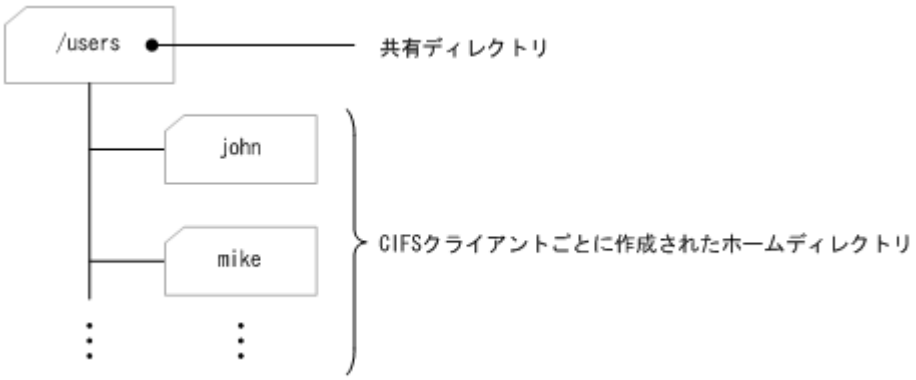
コマンドを利用して複数ユーザーを登録する際に，ホームドライブおよびホームディレクトリのパスを設定できます。コマンドを利用してホームドライブを設定しても，ホームディレクトリは自動的に作成されません。

## 7.4.1 ホームディレクトリの自動作成機能とは

HVFP/HDI 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 7-2 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，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/HDI 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」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/HDI 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/HDI 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］<br>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。<br>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。<br>所有ユーザー：root<br>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］<br>（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。<br>［ユーザー名/グループ名］<br>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。<br>［権限］<br>［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］<br>（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。<br>所有者：RW（読み取りおよび書き込みを許可）<br>グループ：RO（読み取りだけを許可）<br>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/HDI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/HDI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

ファイル名称およびディレクトリ名称の注意事項について説明します。

## 8.1.1 サポート文字

HVFP/HDI 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称・ディレクトリ名称を使用しています。CIFS 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 8-1 パス名とファイル名の最大長**

| 対象 | 名称の最大長 |
|---|---|
| | Windows・HVFP/HDI |
| 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 |

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ります。

## 8.1.2 8.3 形式の MS-DOS ファイル名

HVFP/HDI 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/HDI 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。

## 8.1.3 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。

# 8.2 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/HDI 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/HDI 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，File Services Manager で特定のユーザーまたはグループに対してアクセス権限を与える場合，次のユーザーは指定できません。

- 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

## 8.2.1 Classic ACL タイプと Advanced ACL タイプの差異

HVFP/HDI 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/HDI 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<br>フォルダ：126 | ファイル：700<br>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 |
| 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 |
| 拡張属性 | | 不可 | 不可 |
| ファイル時刻 | 精度 | 秒 | 秒 |

| 大項目 | 小項目※ | Classic ACL タイプ | Advanced ACL タイプ |
|---|---|---|---|
| | 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　ー：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。

## 8.2.2 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/HDI 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 | ○ | ○ | × | × | ○ | ○ | × | × |
| 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

## (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/HDI 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/HDI 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/HDI 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/HDI 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/HDI 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/HDI 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。

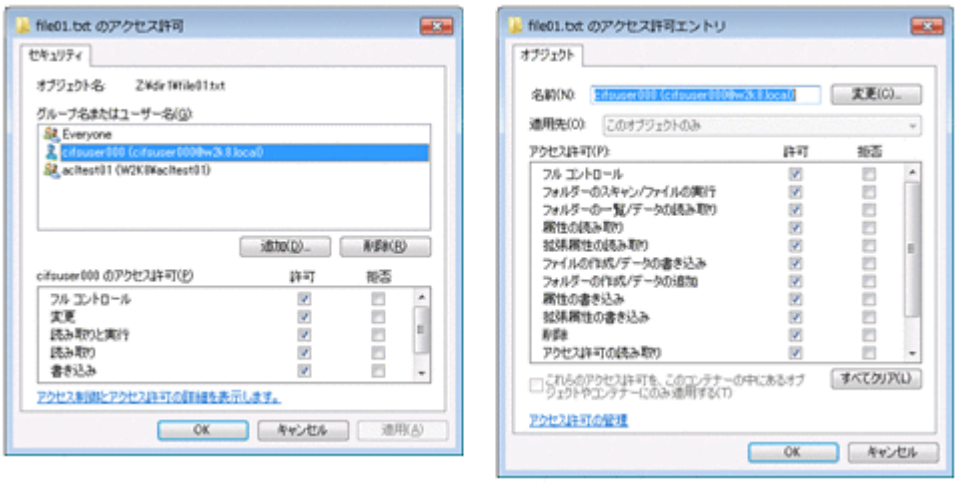
### (2) ファイルの ACL の設定・表示方法

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

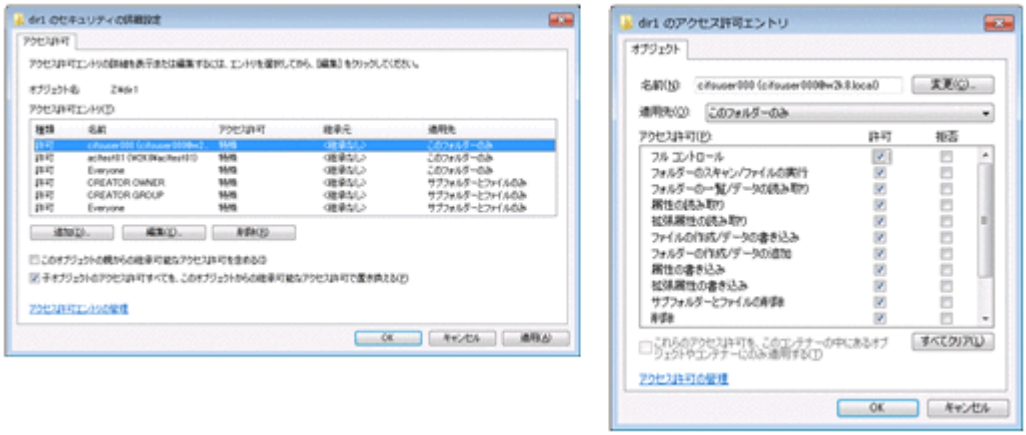
## (3) フォルダの ACL の設定・表示方法

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/HDI 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。

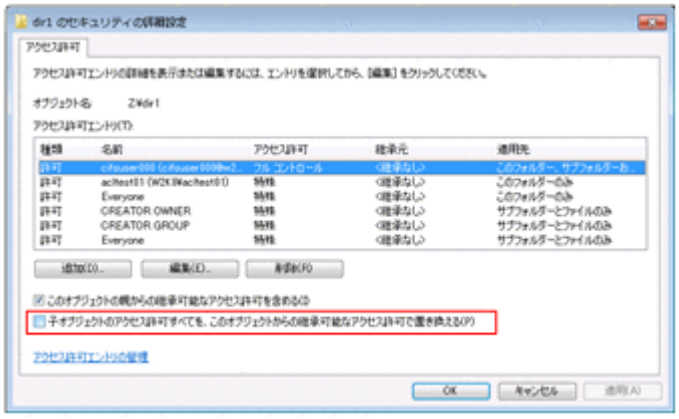
- 上記以外のユーザー，グループの場合

  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，「(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<br>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「(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。

### (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/HDI 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/HDI 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**

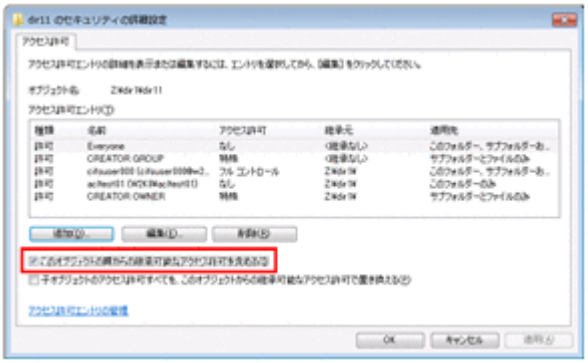
| デフォルト ACL 設定有無 | 権限付与対象エントリー | 設定されるアクセス ACL |
|---|---|---|
| なし | 所有者 | ［新規ファイルのアクセス権限］/［新規ディレクトリのアクセス権限］指定値 |
| | 所有グループ | ［新規ファイルのアクセス権限］/［新規ディレクトリのアクセス権限］指定値 |
| | Everyone | ［新規ファイルのアクセス権限］/［新規ディレクトリのアクセス権限］指定値 |
| | 追加した ACE | 存在しない |
| 所有者<br>所有グループ<br>Everyone | 所有者 | デフォルト ACL と［新規ファイルのア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

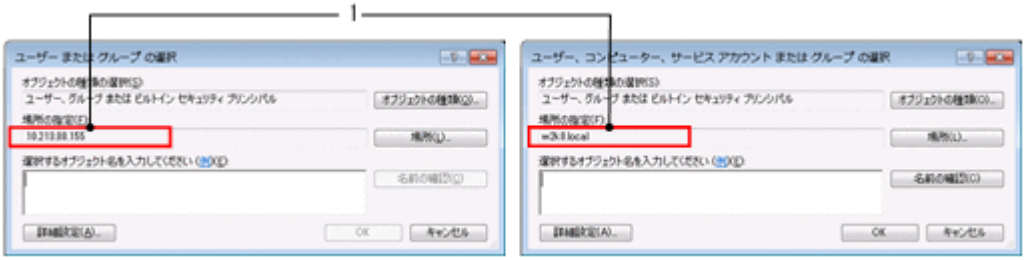
- 親フォルダからの継承を有効にし，フォルダにデフォルト ACL を設定した状態で，ファイル所有者と更新ユーザーがそれぞれ異なる主グループに属している場合，Microsoft Excel／Word／PowerPoint によるファイル更新によって更新前の所有者，所有者の主グループに対する ACL は，それぞれファイル更新後の所有者，所有者の主グループに対する権限へと置き変わる場合があります。これによって，更新前の所有者および所有者の主グループに属するユーザーがアクセス不可となることがあります。

## (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，NT サーバ認証，Active Directory 認証または NT ドメイン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/HDI 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 認証または NT ドメイン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/HDI 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。

Active Directory 認証または NT ドメイン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/HDI 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/HDI 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/HDI 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/HDI のノードまたは Virtual Server のホスト名を表示しても，HVFP/HDI 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。

### (6) ファイル作成時の ACL

HVFP/HDI 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/HDI 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。

### (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/HDI 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) 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）。

### (9) 無効な ACE

ACE の SID が，ビルトイングループやドメイン外アカウントなどの UID 解決できない SID であった場合には，その 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。

### (10) Windows での ACL 設定値の HVFP/HDI のファイルパーミッションへのマッピング

HVFP/HDI 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/HDI 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/HDI 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/HDI 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/HDI 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/HDI 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。

## 8.2.3 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。

### (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

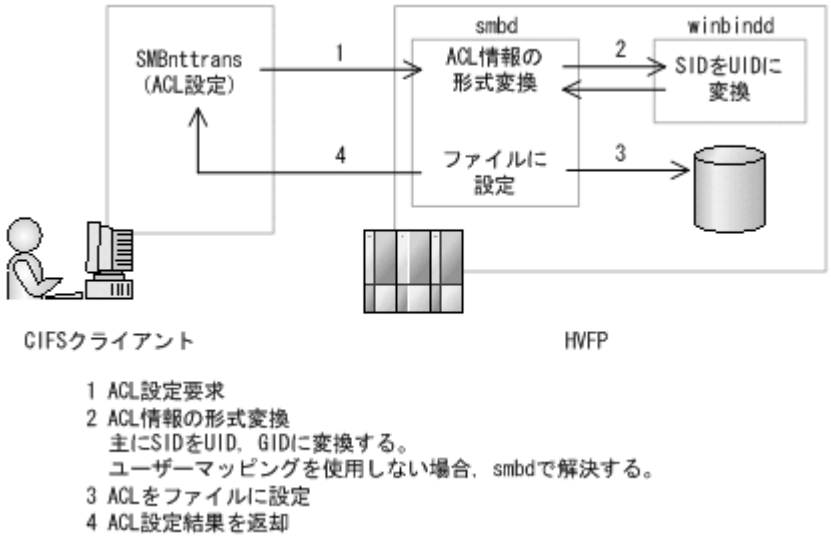
ファイル・ディレクトリへのアクセス権限設定

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/HDI 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**

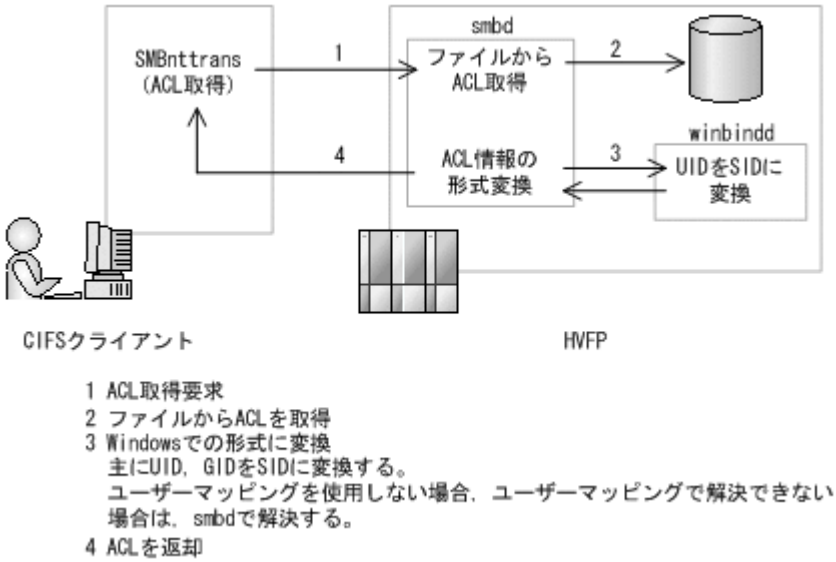



ファイル・ディレクトリのアクセス権限取得

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




## (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 2000 Server | Windows Server 2003, 2008, 2012 | 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。

## (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/HDI 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。 | × |
| 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<br>FILE_READ_ATTRIBUTES<br>FILE_READ_DATA<br>FILE_READ_EA<br>READ_CONTROL<br>SYNCHRONIZE | ○※1 |
| 30 | GENERIC_WRITE | － | 次のフラグの組み合わせ<br>FILE_APPEND_DATA<br>FILE_WRITE_ATTRIBUTES<br>FILE_WRITE_DATA<br>FILE_WRITE_EA<br>READ_CONTROL<br>SYNCHRONIZE | ○※1 |
| 29 | GENERIC_EXECUTE | － | 次のフラグの組み合わせ<br>FILE_READ_ATTRIBUTES<br>READ_CONTROL<br>SYNCHRONIZE<br>FILE_EXECUTE | ○※1 |
| 28 | GENERIC_ALL | － | 次のフラグの組み合わせ<br>DELETE_ACCESS<br>READ_CONTROL_ACCESS<br>WRITE_DAC_ACCESS<br>WRITE_OWNER_ACCESS<br>SYNCHRONIZE_ACCESS<br>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 |

| Bit | アクセス権 | Windows GUI 上の表記 | 説明 | 対応 |
|---|---|---|---|---|
| 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。 | ○ |
| 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/HDI 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/HDI 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/HDI 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 | 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。

## (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/HDI 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。

### (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。

### (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/HDI 側では特にチェックしません。

### (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) 無効な ACE

ACE の SID が，ビルトイングループやドメイン外アカウントなどの UID 解決できない SID であった場合には，その 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。

### (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/HDI 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”<br>（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<br>（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/HDI 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/HDI 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/HDI 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<br>（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。

## (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。

## (11) Advanced ACL タイプファイルシステムへの移行

HVFP/HDI 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/HDI 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。

## (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<br>種類：許可<br>名前：作成ユーザー<br>アクセス許可：フルコントロール<br>適用先：このフォルダのみ<br>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※<br>種類：許可または拒否（指定したモードによる）<br>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<br>アクセス許可：設定されている許可<br>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，「(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 |
| ACE | CIFS 共有内に新規に作成するファイル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<br>種類：許可<br>名前：作成ユーザー |

| 項目 | 内容 |
| --- | --- |
| | アクセス許可：フルコントロール<br>CIFS 共有内に新規に作成するファイルのアクセス権を設定している場合※<br>種類：許可または拒否（指定したモードによる）<br>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<br>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，「(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。

## (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/HDI 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/HDI 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」を参照してください。

## (14) ファイル属性の変更について

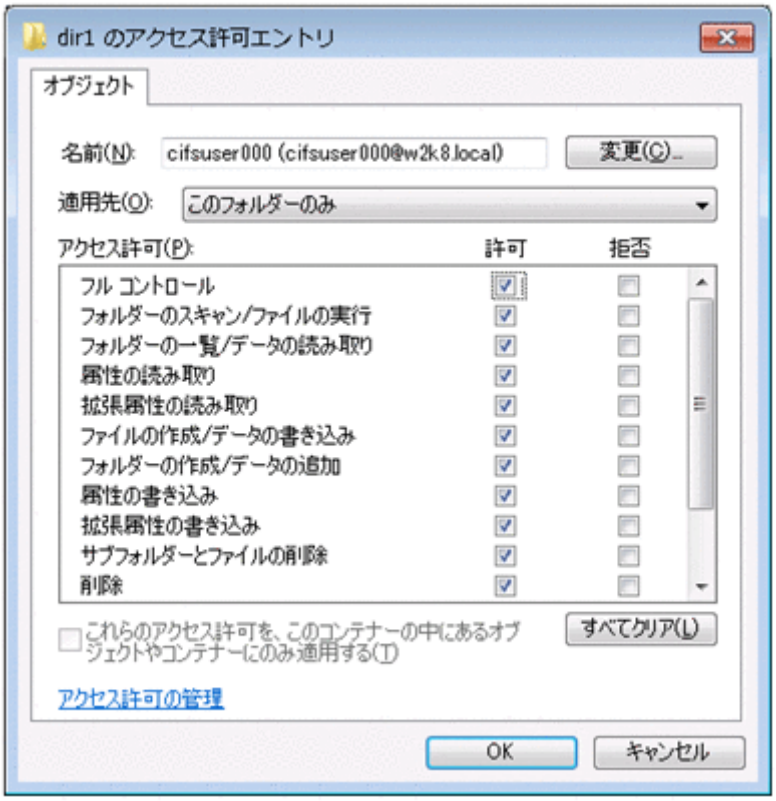
Advanced ACL タイプファイルシステムでファイル属性を変更した場合に，変更結果がエクスプローラの表示に即座に反映されないことがあります。その場合は，エクスプローラの［表示］メニューから［最新の情報に更新］を実行してください。

## (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/HDI 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<br>ro：設定される<br>none：設定されない | rw：設定される<br>ro：設定される<br>none：設定される |
| 削除 | rw：設定される<br>ro：設定されない<br>none：設定されない | rw：設定されない<br>ro：設定されない<br>none：設定されない |
| アクセス許可の変更 | rw：設定される<br>ro：設定されない<br>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<br>rw：設定される<br>ro：設定される<br>none：設定される<br>アクセス権の設定対象がグループまたはその他の場合<br>rw：設定されない<br>ro：設定されない<br>none：設定されない |
| 所有権の取得 | rw：設定される<br>ro：設定されない<br>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<br>rw：設定される<br>ro：設定される<br>none：設定される |

| 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 |
|---|---|---|
| | | アクセス権の設定対象がグループまたはその他の場合<br>rw：設定されない<br>ro：設定されない<br>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<br>ro：設定される<br>none：設定されない | rw：設定される<br>ro：設定される<br>none：設定される |
| アクセス許可の読み取り | rw：設定される<br>ro：設定される<br>none：設定されない | rw：設定される<br>ro：設定される<br>none：設定される |
| アクセス許可の変更 | rw：設定されない<br>ro：設定されない<br>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<br>rw：設定される<br>ro：設定される<br>none：設定される<br>アクセス権の設定対象がグループまたはその他の場合<br>rw：設定されない<br>ro：設定されない<br>none：設定されない |
| 所有権の取得 | rw：設定されない<br>ro：設定されない<br>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<br>rw：設定される<br>ro：設定される<br>none：設定される<br>アクセス権の設定対象がグループまたはその他の場合<br>rw：設定されない<br>ro：設定されない<br>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/HDI 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/HDI 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。

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 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。

## 8.3.1 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/HDI 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。

### (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/HDI 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/HDI 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 | 不可 | 不可 |

| 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 |
|---|---|---|---|
| | 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）。 | | |
| 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※

「(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。

## (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。

## (3) アーカイブ属性に関する注意事項

アーカイブ属性についての注意事項を次に示します。

- 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。

## (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。

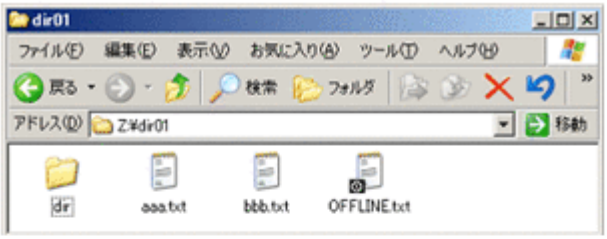
## (5) オフライン属性について

HVFP/HDI は，HCP にマイグレーションされたり，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」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。

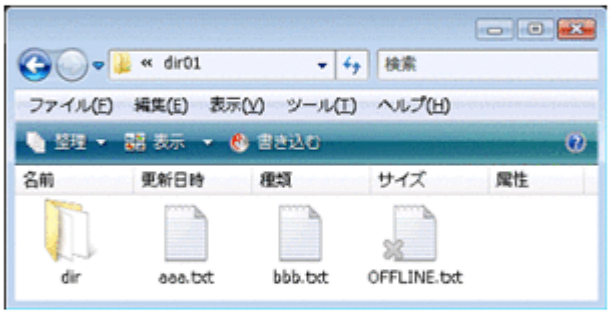
CIFS クライアントがオフライン属性のファイルをエクスプローラで表示した場合，アイコンの左下に，例えば，Windows XP では時計の印，Windows Vista では×印が付きます。エクスプローラの属性列には，オフライン属性を示す文字「O」が表示されます。ただし，オフライン属性のショートカットファイルの場合は，アイコンが表示されなくなることがあります。ショートカットファイルかどうかは，エクスプローラの種類列の表示で判別できます。コマンドプロンプトでファイルの一覧を表示した場合，オフライン属性のファイルはファイルサイズが括弧で囲まれます。

**図 8-9 エクスプローラでのオフライン属性の表示例**

アイコン表示例（Windows XP）

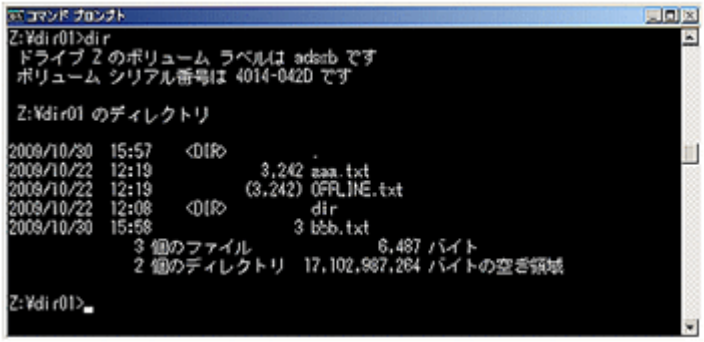



アイコン表示例（Windows Vista）




属性列の表示例（Windows Vista）


**図 8-10 コマンドプロンプトでのオフライン属性の表示例**




## 8.3.2 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/HDI 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/HDI 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/HDI 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 |
| 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」の一つです。

以上のように HVFP/HDI 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。

# 8.4 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。

## 8.4.1 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」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。

## 8.4.2 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。

## 8.4.3 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/HDI 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。

## 8.4.4 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。

### (1) ファイルタイムスタンプの管理方式

HVFP/HDI 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/HDI |
|---|---|---|
| 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。

### (2) ファイルタイムスタンプの更新精度

HVFP/HDI 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/HDI |
|---|---|---|
| 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 |

## 8.4.5 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。

# 8.5 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/HDI 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/HDI 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/HDI 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/HDI 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/HDI 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/HDI | Windows | HVFP/HDI | 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/HDI 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/HDI | Windows | HVFP/HDI | 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/HDI 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。

## 8.5.1 Quota 設定内容の CIFS クライアントでの確認可否

HVFP/HDI 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/HDI 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 |
| 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 設定ではなく，共有ディレクトリで有効な Quota 設定です。そのため，共有ディレクトリ以外のディレクトリに対してドライブ割り当てをした場合，そのディレクトリで有効な Quota の設定値とは異なる値が，ディスク容量に表示される場合があります。また，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，「8.5.2 ディスク使用量に応じたディスク容量表示」および「8.5.3 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。

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 8-11 Quota 設定なしの時のディスク容量表示**

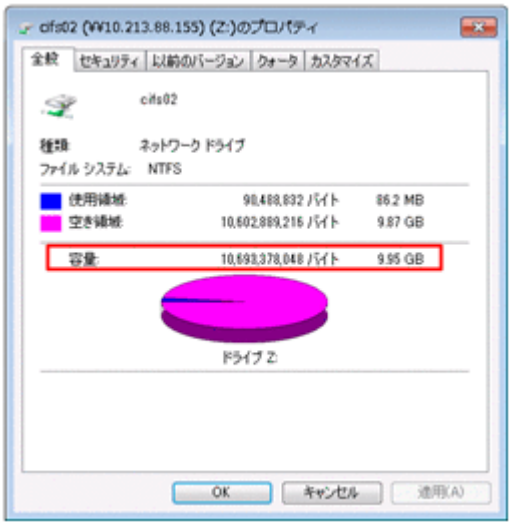
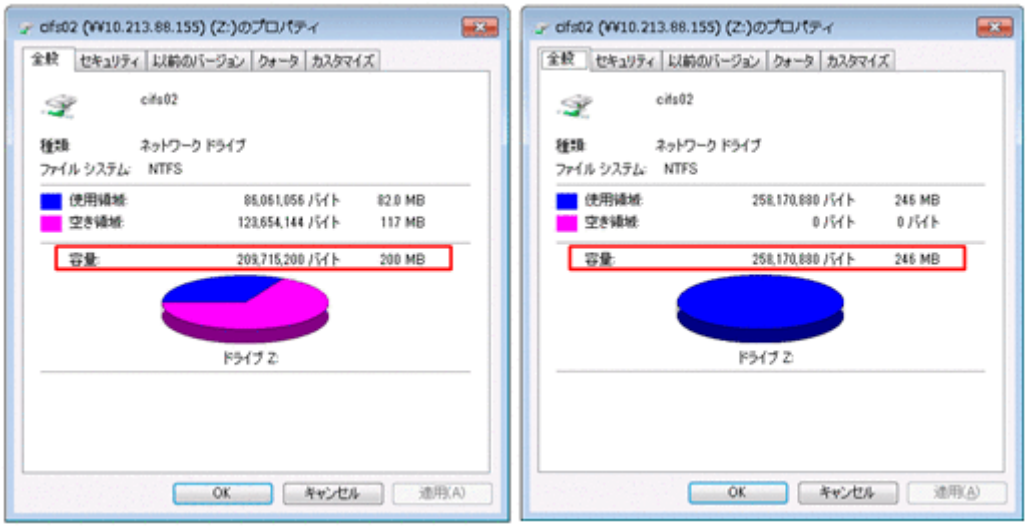



**図 8-12 Quota 設定ありの時のディスク容量表示（左は使用量が Quota 制限内の場合，右は使用量が Quota 制限を超過した場合）**



## 8.5.2 ディスク使用量に応じたディスク容量表示

HVFP/HDI 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/HDI 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/HDI 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<br>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/HDI 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/HDI 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<br>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

## 8.5.3 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。

### (1) HVFP/HDI の場合

HVFP/HDI 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）**

<table>
<tr><th colspan="4">ディレクトリごとの Quota（サブツリー Quota）</th><th colspan="3">ファイルシステムごとの Quota</th><th rowspan="2">ディスク容量</th></tr>
<tr><th>ユーザー</th><th>デフォルト</th><th>グループ</th><th>ディレクトリ</th><th>ユーザー</th><th>デフォルト</th><th>グループ</th></tr>
<tr><td>ブロック容量制限あり</td><td colspan="6">－</td><td>サブツリーユーザー Quota のブロック容量リミット値</td></tr>
<tr><td>Quota の設定なし</td><td>ブロック容量制限あり</td><td colspan="5">－</td><td>サブツリーデフォルト Quota のブロック容量リミット値</td></tr>
<tr><td colspan="2">ブロック容量制限なし</td><td>ブロック容量制限あり</td><td colspan="4">－</td><td>サブツリーグループ Quota のブロック容量リミット値</td></tr>
<tr><td colspan="3">ブロック容量制限なし</td><td>ブロック容量制限あり</td><td colspan="3">－</td><td>サブツリーディレクトリ Quota のブロック容量リミット値</td></tr>
<tr><td colspan="4">ブロック容量制限なし</td><td>ブロック容量制限あり</td><td colspan="2">－</td><td>ユーザー Quota のブロック容量リミット値</td></tr>
<tr><td colspan="4">ブロック容量制限なし</td><td>Quota の設定なし</td><td>ブロック容量制限あり</td><td>－</td><td>デフォルト Quota のブロック容量リミット値</td></tr>
<tr><td colspan="6">ブロック容量制限なし</td><td>ブロック容量制限あり</td><td>グループ Quota のブロック容量リミット値</td></tr>
<tr><td colspan="7">ブロック容量制限なし</td><td>ファイルシステムのサイズ</td></tr>
</table>

（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）**

<table>
<tr><th colspan="4">ディレクトリごとの Quota（サブツリー Quota）</th><th colspan="3">ファイルシステムごとの Quota</th><th rowspan="2">ディスク容量</th></tr>
<tr><th>ユーザー</th><th>デフォルト</th><th>グループ</th><th>ディレクトリ</th><th>ユーザー</th><th>デフォルト</th><th>グループ</th></tr>
<tr><td>使用量が制限を超過</td><td colspan="6">－</td><td>サブツリーユーザー Quota のブロック使用量</td></tr>
<tr><td>使用量は制限内</td><td colspan="6">使用量が，少なくとも 1 つの制限を超過</td><td>サブツリーユーザー Quota のブロック容量リミット値</td></tr>
<tr><td colspan="2">ブロック容量制限なし</td><td>使用量が制限を超過</td><td colspan="4">－</td><td>サブツリーグループ Quota のブロック使用量</td></tr>
<tr><td colspan="2">ブロック容量制限なし</td><td>使用量は制限内</td><td colspan="4">使用量が，少なくとも 1 つの制限を超過</td><td>サブツリーグループ Quota のブロック容量リミット値</td></tr>
<tr><td colspan="3">ブロック容量制限なし</td><td>使用量が制限を超過</td><td colspan="3">－</td><td>サブツリーディレクトリ Quota のブロック使用量</td></tr>
<tr><td colspan="3">ブロック容量制限なし</td><td>使用量は制限内</td><td colspan="3">使用量が，少なくとも 1 つの制限を超過</td><td>サブツリーディレクトリ Quota のブロック容量リミット値</td></tr>
<tr><td colspan="4">ブロック容量制限なし</td><td>使用量が制限を超過</td><td colspan="2">－</td><td>ユーザー Quota のブロック使用量</td></tr>
<tr><td colspan="4">ブロック容量制限なし</td><td>使用量は制限内</td><td colspan="2">使用量が，少なくとも 1 つの制限を超過</td><td>ユーザー Quota のブロック容量リミット値</td></tr>
<tr><td colspan="6">ブロック容量制限なし</td><td>使用量が制限を超過</td><td>グループ Quota のブロック使用量</td></tr>
<tr><td colspan="6">ブロック容量制限なし</td><td>使用量は制限内</td><td>グループ Quota のブロック容量リミット値</td></tr>
</table>

（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。

## (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 |

| 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※ |
| 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※ |

| 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 | | |
| | | | | 「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/HDI 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。

## 8.6 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」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。

# 8.7 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。

## 8.7.1 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」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 8-13 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 8-14 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 8-13 ABE が有効な場合**

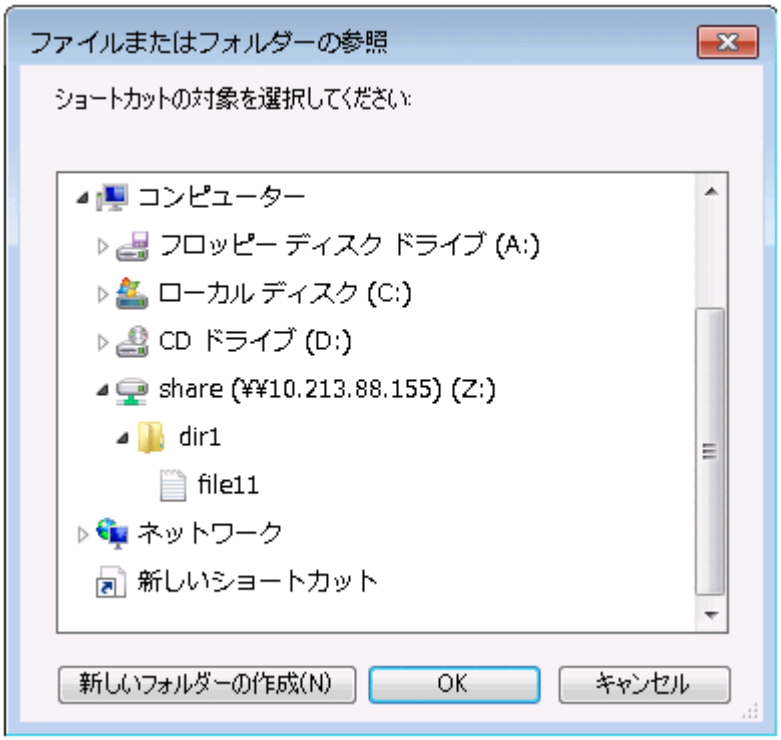
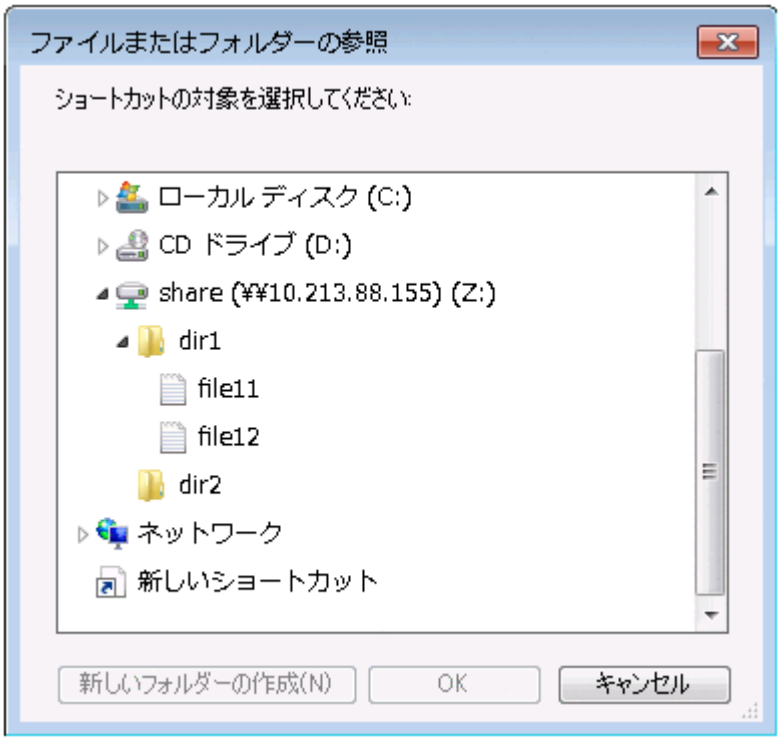



**図 8-14 ABE が無効の場合**

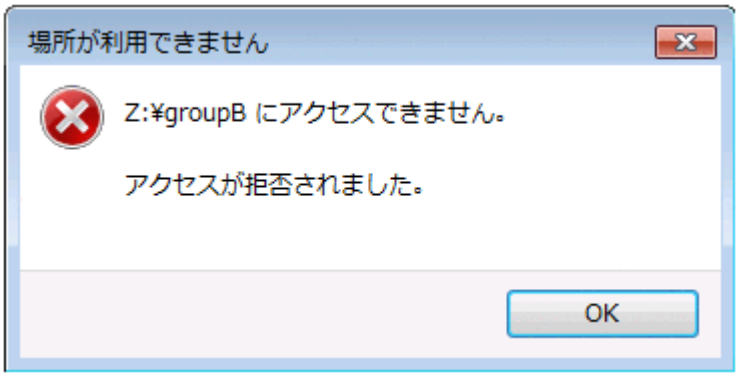



ショートカットファイルも ABE による表示／非表示の対象になります。したがって，ABE を有効にすると，読み取り権限のないショートカットファイルは表示されません。ショートカットファイルの読み取り権限があり，ファイル本体に読み取り権限がない場合，ショートカットファイルは表示されますが，ファイル本体は表示されません。

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 8-15 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**




## 8.7.2 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 4 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

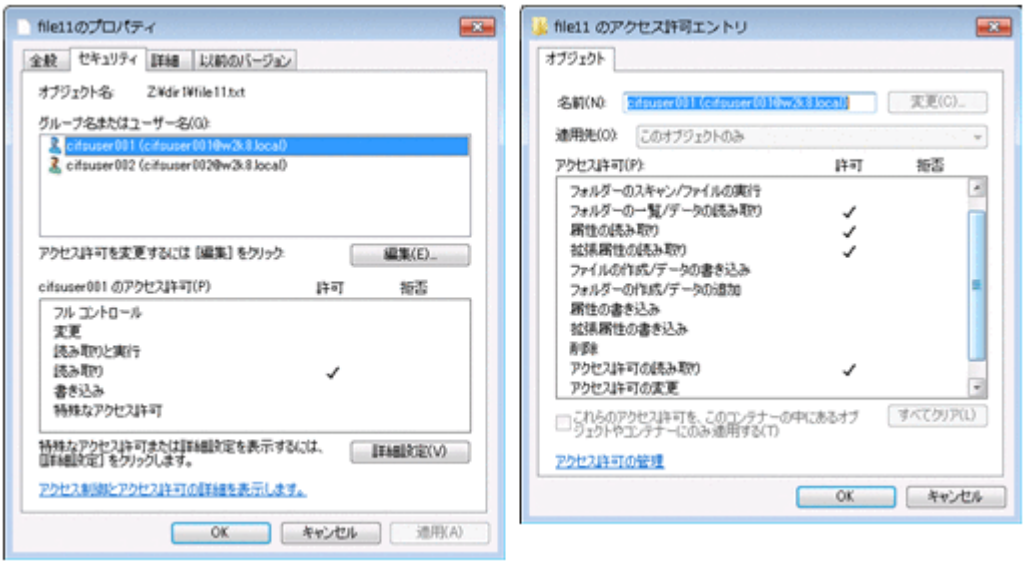
ファイルやフォルダの表示に必要な読み取り権限の有無は，この 4 つの権限の論理和で判定されます。例えば，「フォルダの一覧/データの読み取り」だけを許可されているユーザーが，「属性の読み取り」，「拡張属性の読み取り」および「アクセス許可の読み取り」を許可されているグループに所属して操作した場合，ファイルやフォルダは表示されます。

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」および「拡張属性の読み取り」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/HDI 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 8-16 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）




# 8.8 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/HDI 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 の管理ツールの一つである「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/HDI 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/HDI の MMC 連携

HVFP/HDI 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/HDI 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/HDI 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/HDI 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/HDI 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/HDI 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/HDI 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/HDI 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」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/HDI 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/HDI に接続する必要があります。

ここで説明する Windows の操作説明は，Windows 7 を使用していることを想定して記載しています。

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/HDI 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/HDI 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/HDI 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/HDI 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/HDI 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/HDI 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/HDI 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。<br>例：share1 |
| フォルダー パス | ○ | CIFS 共有のパスが表示されます。<br>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。<br>・ Windows<br>・ Macintosh<br>・ 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。<br>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/HDI 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。<br>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。<br>「`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 |

| 項目名 | 説明 |
|---|---|
| | 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。<br>シンボリックリンクを含むパスは指定できません。また，「.history」および「.snaps」というディレクトリ名は指定できません。加えて，「.arc」，「.lost+found」，「.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。<br>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。<br>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（$）を除いた末尾に指定したりできません。また，末尾に指定したスペースは削除されます。<br>なお，global，homes，printers，admin$，c$，global$，homes$，ipc$および printers$は，CIFS 共有名として指定できません。<br>英大文字と英小文字に関係なく，ノードまたは Virtual Server で一意な名称を指定してください。 |
| 説明 | 作成する CIFS 共有の説明を指定します。<br>256 文字以内で指定してください。<br>指定できる文字は英数字，感嘆符（!），番号記号（#），ドル記号（$），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。<br>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/HDI 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。<br>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。 |

| 項目名 | 説明 |
|---|---|
| | 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。<br>ただし，HVFP/HDI 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。<br>HVFP/HDI の CIFS クライアントの最大接続数については，表 7-2 および表 7-3 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。<br>・ 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<br>・ 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<br>・ 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/HDI 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/HDI 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/HDI 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/HDI 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。<br>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。<br>例：adam |
| 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。<br>・ Windows<br>・ Macintosh<br>・ 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

CIFS 管理者は 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したり，ファイルを閉じたりできます。

CIFS クライアントが開いている HVFP/HDI 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/HDI 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/HDI 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。<br>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。<br>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。<br>・ Windows<br>・ Macintosh<br>・ 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。<br>・ 読み取り<br>・ 書き込み<br>・ 書き込みと読み取り<br>・ 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/HDI 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/HDI 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<br>• 変更<br>• 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 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 9-8 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

注※

HVFP/HDI の CIFS 共有だけで操作できます。

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 9-9 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

# 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 2003，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 9-1 フォルダの参照画面例参照）から選択できます。

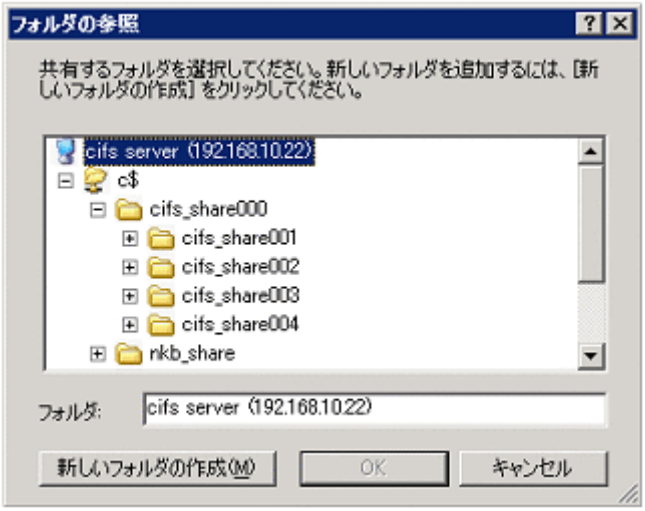
  フォルダの参照画面で，C$フォルダの直下には，ファイルシステムがフォルダとして表示されます。このとき，マウントされているファイルシステムだけが表示されます。

  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）。

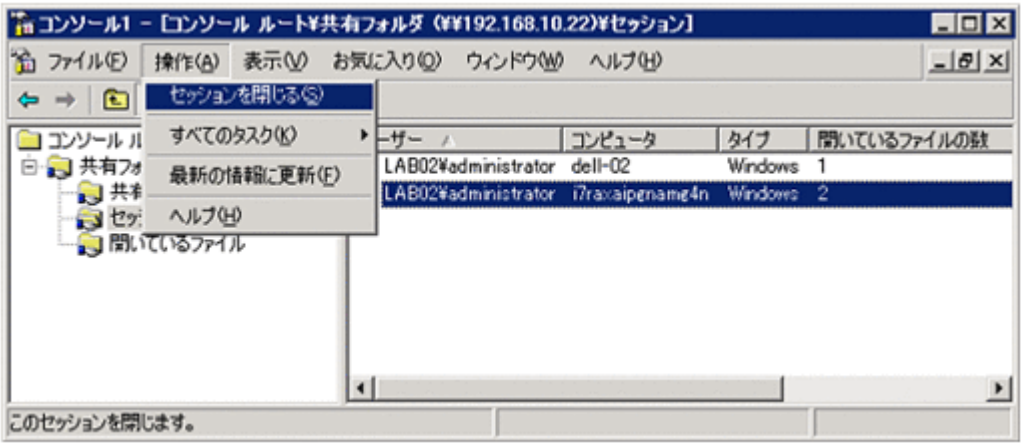
**図 9-1 フォルダの参照画面例**




- 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 9-2 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 9-2 セッションの操作画面例 1**

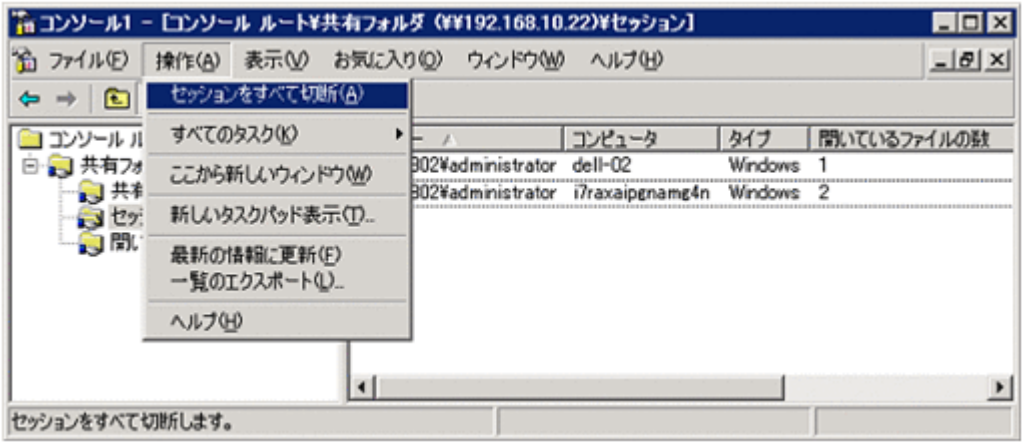



- すべてのセッションを切断する操作について

  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 9-3 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。

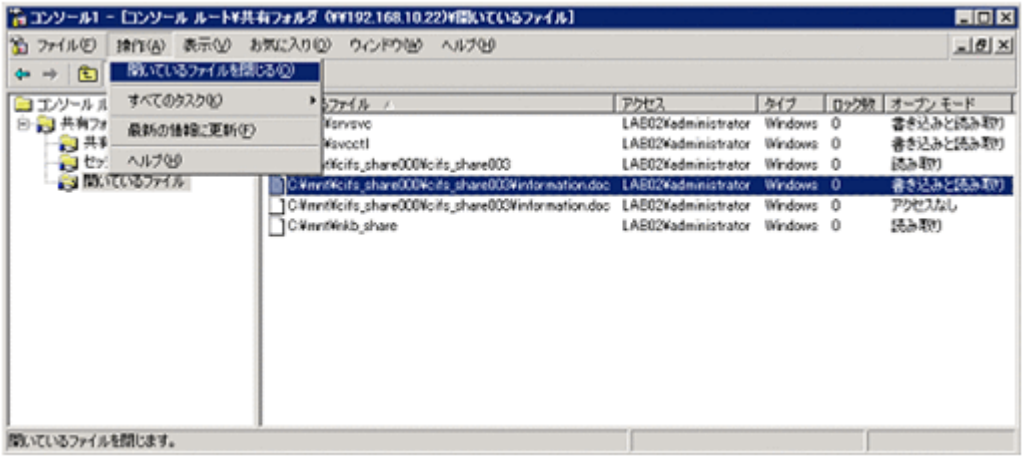
**図 9-3 セッションの操作画面例 2**




- 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 9-4 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。

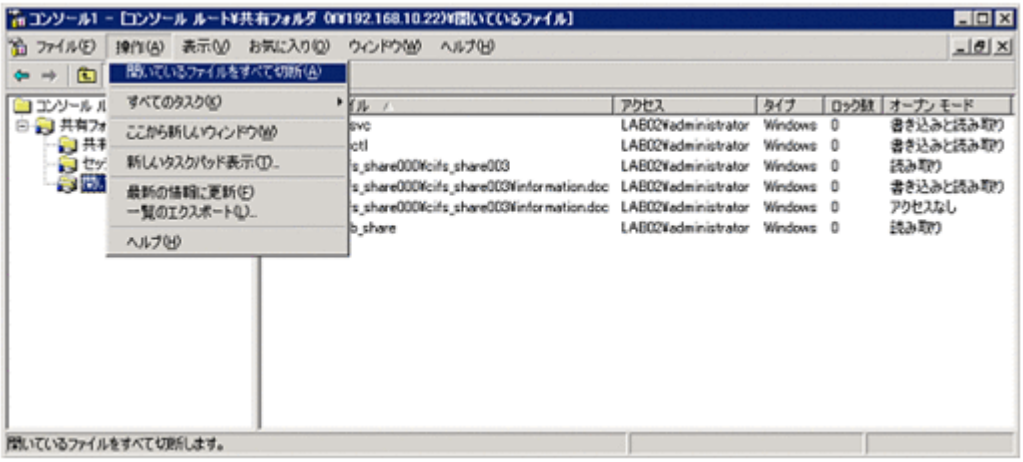
**図 9-4 任意のファイルを閉じる操作の画面例**




- 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 9-5 すべて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，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 9-5 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。

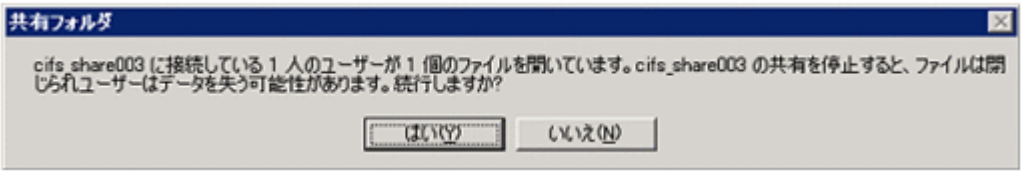
**表 9-10 MMC のバージョンによるアクセス許可のデフォルト値の違い**

| 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 9-6 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」および「ユーザーズガイド」を参照してください。

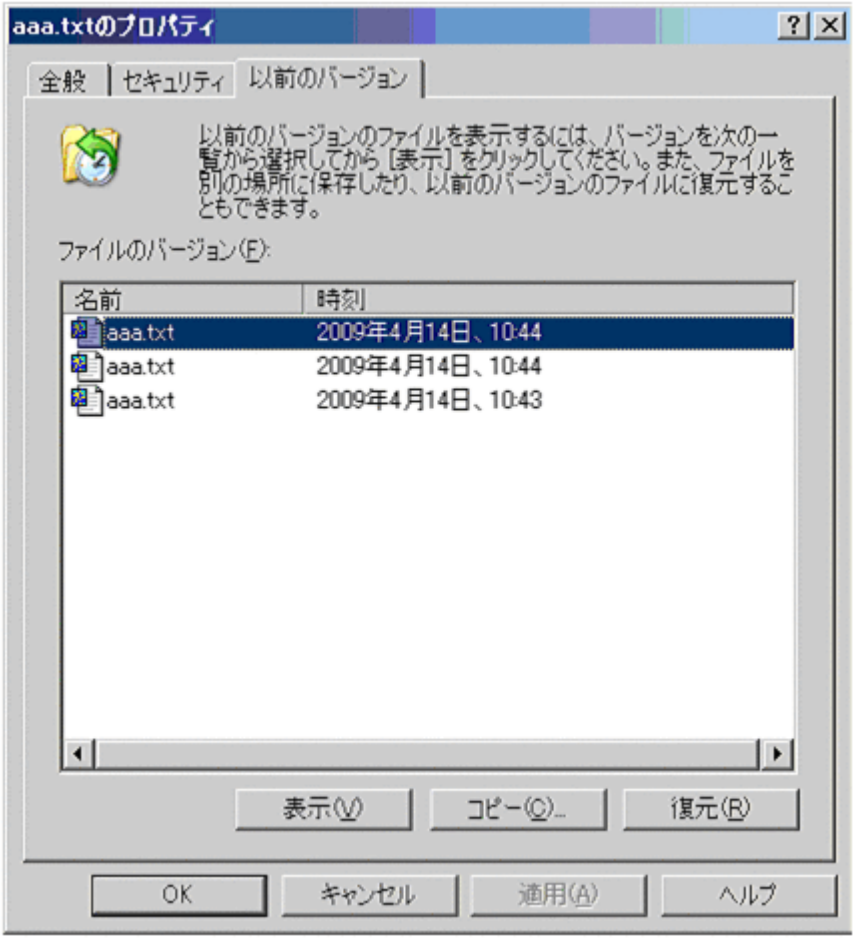
# 10.1 Volume Shadow Copy Service の概要

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。Volume Shadow Copy Service を使用すれば，システム管理者は差分スナップショットをマウントするだけで公開できます。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が 1 つ以上マウントされている場合に，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**




［時刻］には差分スナップショットの作成時刻が表示されます。

# 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/HDI 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 に対応しているプラットフォームは次のとおりです。

- Windows 7
- Windows 8
- Windows Server 2003
- Windows Server 2008
- Windows Server 2012
- Windows Vista
- Windows XP

## 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。

- CIFS クライアントが参照する［以前のバージョン］タブでの差分スナップショットの表示条件は，参照対象がファイルかフォルダかで異なります。ファイルについては，差分スナップショッ

トに対象のファイルが存在する場合に以前のバージョンのファイルとして表示されます。フォルダについては, 差分スナップショットに対象のフォルダが存在しない場合も以前のバージョンのフォルダとして表示されることがありますが，アクセスしようとするとエラーになります。

- ［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
- 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，CIFS クライアントが差分スナップショットを参照できるようになるまで時間が掛かることがあります。
- 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 10-1 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 | ○ | ○ | × |
| ［表示］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。

# 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/HDI 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 NT の場合

CIFS クライアントが Windows NT の場合，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。

## 11.3 Windows Server 2003 の場合

CIFS クライアントが Windows Server 2003 で，CIFS サービスの認証モードが NT Server Authentication の場合，クライアントに次の設定をしてください。

ドメインコントローラー構成以外の場合には「管理ツール」の「ローカル セキュリティ ポリシー」で，ドメインコントローラー構成の場合には「管理ツール」の「ドメイン コントローラ セキュリティ ポリシー」で，「ローカル ポリシー」の「セキュリティオプション」の「ネットワークセキュリティ：LAN Manager 認証レベル」を次のどちらかに設定してください。

- LM と NTLM 応答を送信する
- LM と NTLM を送信する
  ネゴシエーションの場合，NTLMv2 セッションセキュリティを使用します。

## 11.4 Windows XP x64 の場合

CIFS クライアントが Windows XP x64 で，CIFS サービスの認証モードが NT Server Authentication の場合，クライアントに次の設定をしてください。

「管理ツール」の「ローカル セキュリティ ポリシー」で，「ローカル ポリシー」の「セキュリティオプション」の「ネットワークセキュリティ：LAN Manager 認証レベル」を次のどちらかに設定してください。

- LM と NTLM 応答を送信する
- LM と NTLM を送信する
  ネゴシエーションの場合，NTLMv2 セッションセキュリティを使用します。

# 11.5 Windows Vista の場合

CIFS クライアントが Windows Vista の場合の注意事項を次に示します。

## 11.5.1 CIFS サービスの認証モードが NT Server Authentication の場合

クライアントに次の設定をしてください。

「管理ツール」の「ローカル セキュリティ ポリシー」で，「ローカル ポリシー」の「セキュリティ オプション」の「ネットワークセキュリティ：LAN Manager 認証レベル」を次のどちらかに設定してください。

- LM と NTLM 応答を送信する
- LM と NTLM を送信する
  ネゴシエーションの場合，NTLMv2 セッションセキュリティを使用します。

## 11.5.2 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。

### (1) ACL を追加する場合

HVFP/HDI 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
- 認証方式が次のどれかである
  - ローカル認証
  - NT サーバ認証
  - NT ドメイン認証かつ，ユーザーマッピングを使用しない
  - Active Directory 認証かつ，ユーザーマッピングを使用しない

### (2) Quota を使用する場合

エクスプローラを使用してファイルを共有内に移動するまたは貼り付ける際に，ファイル作成後のブロック使用量または inode 数が HVFP/HDI で設定したソフトリミットを超過する状態であると，ハードリミット未超過であっても，ファイル作成に失敗することがあります。なお，COPY コマンドや XCOPY コマンドを使用して，共有にソフトリミットを超えるファイルを作成できます。

### (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 2007 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 Vista で Microsoft 2007 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。

### (4) ネットワークドライブを使用する場合

ネットワークドライブを使用してパス名が最大長に近いファイル・ディレクトリのプロパティを表示した場合，セキュリティタブが表示されなくて，ACL の参照・設定ができません。プロパティのセキュリティタブが表示されない場合には，ファイル・ディレクトリの名前を一時的に短い名前に変更してください。

次のすべての条件が重なった場合に，セキュリティタブが表示されません。

- ネットワークドライブを使用
- ネットワークドライブ上の対象ファイル・ディレクトリのパス名が，UNC 形式のパス名（¥¥サーバ名¥共有名¥・・・）に直したときに 259 文字を超える

## 11.5.3 MMC を使用する場合

Windows Vista 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。

### (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/HDI 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

### (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
- 認証方式が次のどれかである
  - ローカル認証
  - NT サーバ認証
  - NT ドメイン認証かつ，ユーザーマッピングを使用しない
  - Active Directory 認証かつ，ユーザーマッピングを使用しない

# 11.6 Windows Server 2008 の場合

CIFS クライアントが Windows Server 2008 の場合の注意事項を次に示します。

## 11.6.1 CIFS サービスの認証モードが NT Server Authentication の場合

クライアントに次の設定をしてください。

「管理ツール」の「ローカル セキュリティ ポリシー」で，「ローカル ポリシー」の「セキュリティ オプション」の「ネットワークセキュリティ：LAN Manager 認証レベル」を次のどちらかに設定してください。

- LM と NTLM 応答を送信する
- LM と NTLM を送信する
  ネゴシエーションの場合，NTLMv2 セッションセキュリティを使用します。

## 11.6.2 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。

### (1) ACL を追加する場合

HVFP/HDI 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
- 認証方式が次のどれかである
  - ローカル認証
  - NT サーバ認証
  - NT ドメイン認証かつ，ユーザーマッピングを使用しない
  - Active Directory 認証かつ，ユーザーマッピングを使用しない

### (2) Quota を使用する場合

エクスプローラを使用してファイルを共有内に移動するまたは貼り付ける際に，ファイル作成後のブロック使用量または inode 数が HVFP/HDI で設定したソフトリミットを超過する状態であると，ハードリミット未超過であっても，ファイル作成に失敗することがあります。なお，COPY コマンドや XCOPY コマンドを使用して，共有にソフトリミットを超えるファイルを作成できます。

### (3) ネットワークドライブを使用する場合

ネットワークドライブを使用してパス名が最大長に近いファイル・ディレクトリのプロパティを表示した場合，セキュリティタブが表示されなくて，ACL の参照・設定ができません。プロパティのセキュリティタブが表示されない場合には，ファイル・ディレクトリの名前を一時的に短い名前に変更してください。

次のすべての条件が重なった場合に，セキュリティタブが表示されません。

- ネットワークドライブを使用

- ネットワークドライブ上の対象ファイル・ディレクトリのパス名が，UNC 形式のパス名（¥¥サーバ名¥共有名¥・・・）に直したときに 259 文字を超える

### 11.6.3 MMC を使用する場合

Windows Server 2008 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。

#### (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/HDI 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

#### (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
- 認証方式が次のどれかである
  - ローカル認証
  - NT サーバ認証
  - NT ドメイン認証かつ，ユーザーマッピングを使用しない
  - Active Directory 認証かつ，ユーザーマッピングを使用しない

### 11.6.4 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。

## 11.7 Windows 7 の場合

CIFS クライアントが Windows 7 の場合の注意事項を次に示します。

### 11.7.1 CIFS サービスの認証モードが NT Server Authentication の場合

クライアントに次の設定をしてください。

「管理ツール」の「ローカル セキュリティ ポリシー」で，「ローカル ポリシー」の「セキュリティ オプション」の「ネットワークセキュリティ：LAN Manager 認証レベル」を次のどちらかに設定してください。

- LM と NTLM 応答を送信する
- LM と NTLM を送信する
  ネゴシエーションの場合，NTLMv2 セッションセキュリティを使用します。

## 11.7.2 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。

### (1) ACL を追加する場合

HVFP/HDI 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
- 認証方式が次のどれかである
  - ローカル認証
  - NT サーバ認証
  - NT ドメイン認証かつ，ユーザーマッピングを使用しない
  - Active Directory 認証かつ，ユーザーマッピングを使用しない

### (2) Quota を使用する場合

エクスプローラを使用してファイルを共有内に移動するまたは貼り付ける際に，ファイル作成後のブロック使用量または inode 数が HVFP/HDI で設定したソフトリミットを超過する状態であると，ハードリミット未超過であっても，ファイル作成に失敗することがあります。なお，COPY コマンドや XCOPY コマンドを使用して，共有にソフトリミットを超えるファイルを作成できます。

### (3) ネットワークドライブを使用する場合

ネットワークドライブを使用してパス名が最大長に近いファイル・ディレクトリのプロパティを表示した場合，セキュリティタブが表示されなくて，ACL の参照・設定ができません。プロパティのセキュリティタブが表示されない場合には，ファイル・ディレクトリの名前を一時的に短い名前に変更してください。

次のすべての条件が重なった場合に，セキュリティタブが表示されません。

- ネットワークドライブを使用
- ネットワークドライブ上の対象ファイル・ディレクトリのパス名が，UNC 形式のパス名（¥¥サーバ名¥共有名¥・・・）に直したときに 259 文字を超える

### (4) 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 7 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。

## 11.7.3 MMC を使用する場合

Windows 7 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。

### (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/HDI 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

### (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
- 認証方式が次のどれかである
  - ローカル認証
  - NT サーバ認証
  - NT ドメイン認証かつ，ユーザーマッピングを使用しない
  - Active Directory 認証かつ，ユーザーマッピングを使用しない

# 11.8 Windows 8 の場合

CIFS クライアントが Windows 8 の場合の注意事項を次に示します。

## 11.8.1 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。

### (1) ACL を追加する場合

HVFP/HDI 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
- 認証方式が次のどれかである
  - ローカル認証
  - NT サーバ認証
  - NT ドメイン認証かつ，ユーザーマッピングを使用しない
  - Active Directory 認証かつ，ユーザーマッピングを使用しない

### (2) Quota を使用する場合

エクスプローラを使用してファイルを共有内に移動するまたは貼り付ける際に，ファイル作成後のブロック使用量または inode 数が HVFP/HDI で設定したソフトリミットを超過する状態であると，ハードリミット未超過であっても，ファイル作成に失敗することがあります。なお，COPY コマンドや XCOPY コマンドを使用して，共有にソフトリミットを超えるファイルを作成できます。

### (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 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。

## 11.8.2 MMC を使用する場合

Windows 8 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。

### (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/HDI 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

### (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

・ 認証方式が次のどれかである

- ローカル認証
- NT サーバ認証
- NT ドメイン認証かつ，ユーザーマッピングを使用しない
- Active Directory 認証かつ，ユーザーマッピングを使用しない

# 11.9 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。

## 11.9.1 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。

### (1) ACL を追加する場合

HVFP/HDI 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

・ 認証方式が次のどれかである

- ローカル認証
- NT サーバ認証
- NT ドメイン認証かつ，ユーザーマッピングを使用しない
- Active Directory 認証かつ，ユーザーマッピングを使用しない

### (2) Quota を使用する場合

エクスプローラを使用してファイルを共有内に移動するまたは貼り付ける際に，ファイル作成後のブロック使用量または inode 数が HVFP/HDI で設定したソフトリミットを超過する状態であると，ハードリミット未超過であっても，ファイル作成に失敗することがあります。なお，COPY コマンドや XCOPY コマンドを使用して，共有にソフトリミットを超えるファイルを作成できます。

### 11.9.2 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。

#### (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/HDI 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

#### (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
- 認証方式が次のどれかである
  - ローカル認証
  - NT サーバ認証
  - NT ドメイン認証かつ，ユーザーマッピングを使用しない
  - Active Directory 認証かつ，ユーザーマッピングを使用しない

### 11.9.3 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。

## 11.10 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。

### 11.10.1 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

## 11.10.2 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

## 11.10.3 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。

- CIFS 共有にファイルをドロップまたはペーストする場合，データコピー前にブロック使用量または inode 使用量が HVFP/HDI で設定したソフトリミットを超過した状態であると，ハードリミットを超えていなくても，クライアントでの操作が失敗することがあります。
- 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/HDI 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/HDI 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。

- CIFS 共有で複数のユーザーがファイルを操作しているとき，「読み出しと書き込み」権限があるにも関わらず，ファイルの更新に失敗することがあります。

  この場合は，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，操作するユーザーまたはそのユーザー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。

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 |
|---|---|---|---|---|---|
| VFP2010 | 6GB | 2～3 未満 | × | 2,000 | 7,500 |
| | | | ○ | 1,000 | 256 |
| | | 3～4 | × | 285×割り当てたメモリー量※＋1,430 | 7,500 |
| | | | ○ | 71×割り当てたメモリー量※＋858 | 256 |
| VFP2100 | 12GB | 2～3 未満 | × | 2,000 | 7,500 |
| | | | ○ | 1,000 | 256 |
| | | 3～8 | × | 285×割り当てたメモリー量※＋1,430 | 7,500 |
| | | | ○ | 71×割り当てたメモリー量※＋858 | 256 |
| VFP2300 | 12GB | 2～3 未満 | × | 2,000 | 7,500 |
| | | | ○ | 1,000 | 256 |
| | | 3～8 | × | 285×割り当てたメモリー量※＋1,430 | 7,500 |
| | | | ○ | 71×割り当てたメモリー量※＋858 | 256 |
| VFP100N | 6GB | 2～3 未満 | × | 2,000 | 7,500 |
| | | | ○ | 1,000 | 256 |
| | | 3～4 | × | 285×割り当てたメモリー量※＋1,430 | 7,500 |
| | | | ○ | 71×割り当てたメモリー量※＋858 | 256 |
| VFP300N | 12GB | 2～3 未満 | × | 2,000 | 7,500 |
| | | | ○ | 1,000 | 256 |
| | | 3～8 | × | 285×割り当てたメモリー量※＋1,430 | 7,500 |
| | | | ○ | 71×割り当てたメモリー量※＋858 | 256 |
| VFP500N | 24GB | 2～3 未満 | × | 2,000 | 7,500 |
| | | | ○ | 1,000 | 256 |
| | | 3～16 未満 | × | 285×割り当てたメモリー量※＋1,430 | 7,500 |
| | | | ○ | 71×割り当てたメモリー量※＋858 | 256 |
| | | 16～18 | × | 375×割り当てたメモリー量※ | 7,500 |

| 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 |
|---|---|---|---|---|---|
| | | | ○ | 175×割り当てたメモリー量※－800 | 256 |
| VFP110 | 16GB | 2～3未満 | × | 2,000 | 7,500 |
| | | | ○ | 1,000 | 256 |
| | | 3～12 | × | 285×割り当てたメモリー量※＋1,430 | 7,500 |
| | | | ○ | 71×割り当てたメモリー量※＋858 | 256 |
| VFP200N | 16GB | 2～3未満 | × | 2,000 | 7,500 |
| | | | ○ | 1,000 | 256 |
| | | 3～12 | × | 285×割り当てたメモリー量※＋1,430 | 7,500 |
| | | | ○ | 71×割り当てたメモリー量※＋858 | 256 |
| | 32GB | 2～3未満 | × | 2,000 | 7,500 |
| | | | ○ | 1,000 | 256 |
| | | 3～16未満 | × | 285×割り当てたメモリー量※＋1,430 | 7,500 |
| | | | ○ | 71×割り当てたメモリー量※＋858 | 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 |
| VFP600N | 32GB | 2～3未満 | × | 2,000 | 7,500 |
| | | | ○ | 1,000 | 256 |
| | | 3～16未満 | × | 285×割り当てたメモリー量※＋1,430 | 7,500 |
| | | | ○ | 71×割り当てたメモリー量※＋858 | 256 |
| | | 16～26 | × | 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 |
| | 64GB | 2～3未満 | × | 2,000 | 7,500 |
| | | | ○ | 1,000 | 256 |
| | | 3～16未満 | × | 285×割り当てたメモリー量※＋1,430 | 7,500 |
| | | | ○ | 71×割り当てたメモリー量※＋858 | 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 |

| 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 |
|---|---|---|---|---|---|
| | | 33～56 | × | 24,000 | 7,500 |
| | | | ○ | 9,600 | 256 |
| | 96GB | 2～3未満 | × | 2,000 | 7,500 |
| | | | ○ | 1,000 | 256 |
| | | 3～16未満 | × | 285×割り当てたメモリー量※＋1,430 | 7,500 |
| | | | ○ | 71×割り当てたメモリー量※＋858 | 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

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

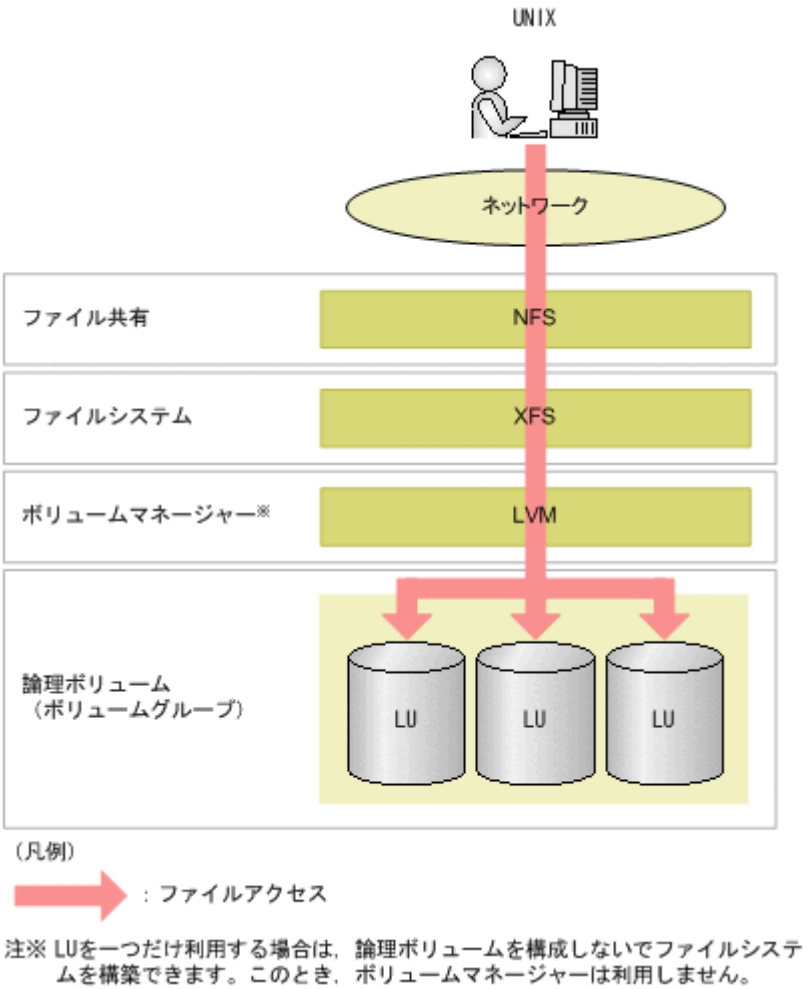
NFS クライアントは HVFP/HDI の NFS サービスを利用してデータにアクセスできます。この章では，NFS サービス利用の概要について説明します。

# 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**




HVFP/HDI 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」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/HDI 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/HDI 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。

## 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。

**表 14-1 NFS クライアントとしてサポートする製品**

| 製品名 | NFSv2，NFSv3 クライアント | NFSv4 クライアント※ | IPv6 接続 |
|---|---|---|---|
| AIX 5L V5.2 | ○ | － | － |
| AIX 5L V5.3（5300-09 以降） | ○ | ○ | － |
| AIX V6.1 | ○ | ○ | ○ |
| AIX V7.1 | ○ | ○ | ○ |
| FreeBSD 5.4 | ○ | － | － |
| FreeBSD 6.1 | ○ | － | － |
| HP-UX 11i | ○ | － | － |
| HP-UX 11i v2（PA-RISC） | ○ | － | － |
| HP-UX 11i v3（HP-UX 11i-OE B.11.31 以降，HP-UX 11i-OE.OE B.11.31 以降） | ○ | ○ | ○ |
| HP Tru64 UNIX 5.1 | ○ | － | － |
| IRIX 6.5 | ○ | － | － |
| Oracle Direct NFS Client（Oracle Database 11g Release 2（11.2.0.3.0）for linux（x86）） | △ | － | － |
| Oracle Direct NFS Client（Oracle Database 11g Release 2（11.2.0.3.0）for Microsoft Windows（x64）） | △ | － | － |
| Red Hat Linux 8.0 | ○ | － | － |
| Red Hat Enterprise Linux AS v3 | ○ | － | － |
| Red Hat Enterprise Linux AS v4（x86） | ○ | － | － |
| Red Hat Enterprise Linux Advanced Platform v5.6（Linux version 2.6.18-238.el5 以降） | ○ | ○ | － |
| Red Hat Enterprise Linux Server v6.1 | ○ | ○ | － |
| Solaris 9 オペレーティングシステム（SunOS 5.9）SPARC プラットフォーム版 | ○ | － | － |
| 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（Solaris 10 10/08 以降） | ○ | ○ | ○ |
| SUSE Linux 8.0 | ○ | － | － |
| SUSE Linux 9.0 | ○ | － | － |
| SUSE Linux 10 SP1 | ○ | － | － |
| Turbolinux 10 Server | ○ | － | － |
| Ubuntu 8.04 LTS | ○ | ○ | － |
| Ubuntu 10.04 LTS | ○ | ○ | － |
| VMware ESX 4.0 | △ | － | － |
| VMware ESX 4.1 | △ | － | － |
| VMware ESXi 5.0 | △ | － | － |

（凡例）○：サポートしている　－：サポートしていない　△：NFSv3 プロトコルだけをサポートする

注※

NFSv4 プロトコルを使用する場合，NFS クライアントとして使用する製品によっては，HVFP/HDI が提供する機能の一部を利用できない場合があります。使用する製品のドキュメントを参照して，それぞれの機能が利用できるかどうかを確認してください。

これらの製品は，VMware ESX 3 以降で動作するときにもサポート対象となります。

## 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。

- AIX 5L V5.3
- 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) 2003, Datacenter Edition for Itanium-based Systems（SP1，SP2）
- Microsoft(R) Windows Server(R) 2003, Datacenter Edition Operating System（SP1，SP2）
- Microsoft(R) Windows Server(R) 2003, Enterprise Edition for Itanium-based Systems（SP1，SP2）
- Microsoft(R) Windows Server(R) 2003, Enterprise Edition Operating System（SP1，SP2）
- Microsoft(R) Windows Server(R) 2003, Enterprise x64 Edition Operating System
- Microsoft(R) Windows Server(R) 2003, Standard Edition Operating System（SP1，SP2）
- Microsoft(R) Windows Server(R) 2008 Enterprise
- Microsoft(R) Windows Server(R) 2008 Enterprise 32-bit
- Microsoft(R) Windows Server(R) 2008 Standard
- Microsoft(R) Windows Server(R) 2008 Standard 32-bit
- Microsoft(R) Windows Server(R) 2008 R2 Enterprise
- Microsoft(R) Windows Server(R) 2008 R2 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
- Sun Java(TM) System Directory Server 5.2

NIS サーバ

HVFP/HDI では，UNIX マシンのほか，Active Directory ドメインコントローラーを 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。

ID マッピング用サーバとして 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) 2003, Datacenter Edition for Itanium-based Systems（SP1，SP2）
- Microsoft(R) Windows Server(R) 2003, Datacenter Edition Operating System（SP1，SP2）
- Microsoft(R) Windows Server(R) 2003, Enterprise Edition for Itanium-based Systems（SP1，SP2）
- Microsoft(R) Windows Server(R) 2003, Enterprise Edition Operating System（SP1，SP2）
- Microsoft(R) Windows Server(R) 2003, Enterprise x64 Edition Operating System
- Microsoft(R) Windows Server(R) 2003, Standard Edition Operating System（SP1，SP2）
- Microsoft(R) Windows Server(R) 2003 R2, Enterprise Edition Operating System
- Microsoft(R) Windows Server(R) 2003 R2, Enterprise x64 Edition Operating System
- Microsoft(R) Windows Server(R) 2008 Enterprise
- Microsoft(R) Windows Server(R) 2008 Enterprise 32-bit

Windows Server 2003（SP1，SP2）のとき

Active Directory を構築したあと，Windows Services for UNIX Version 3.5（SFU）をインストールします。

Windows Server 2003 R2 または Windows Server 2008 のとき

Active Directory を構築します。また，GUI を使用するときは，UNIX 用 ID 管理ツールをインストールします。

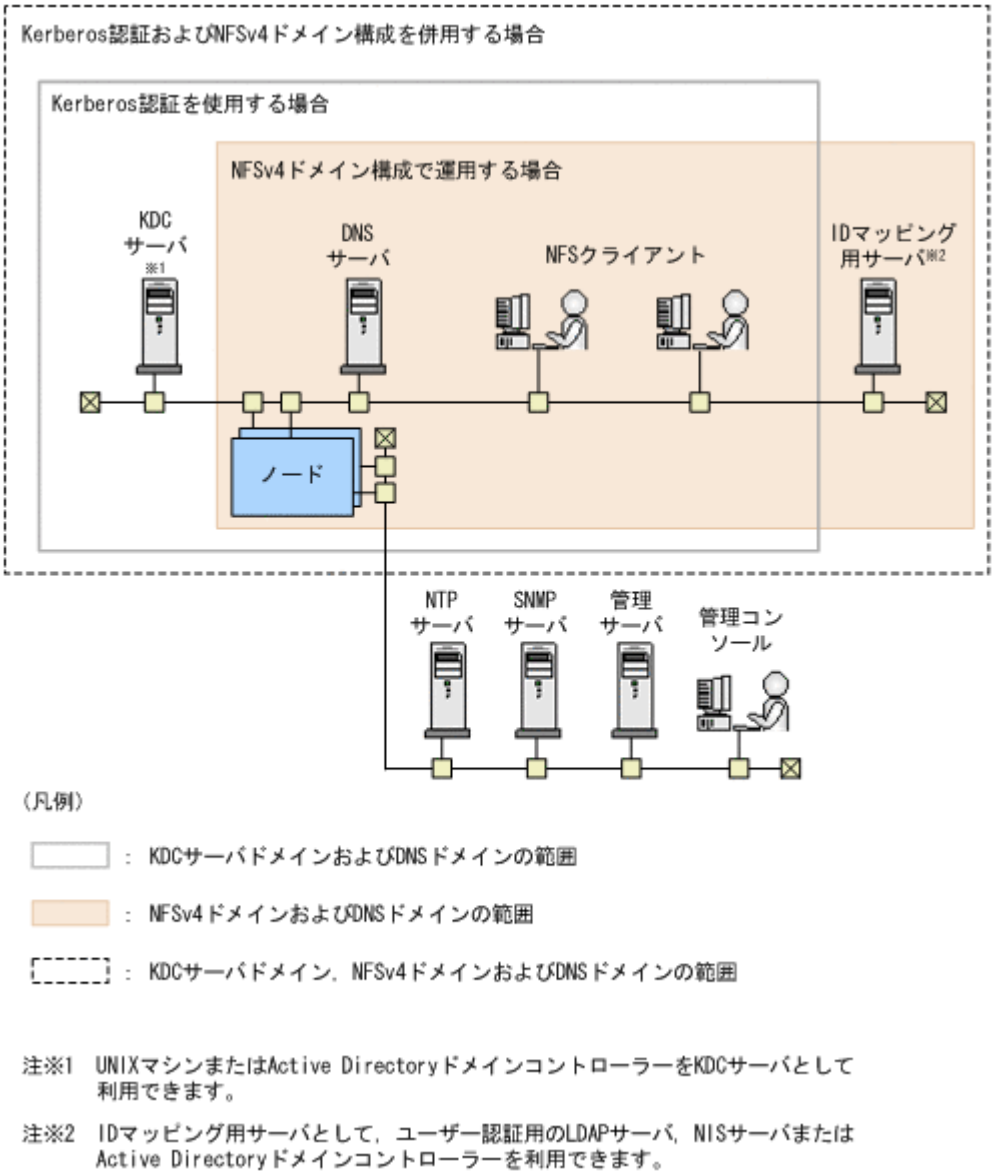
# 14.2 ネットワークの構成

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。

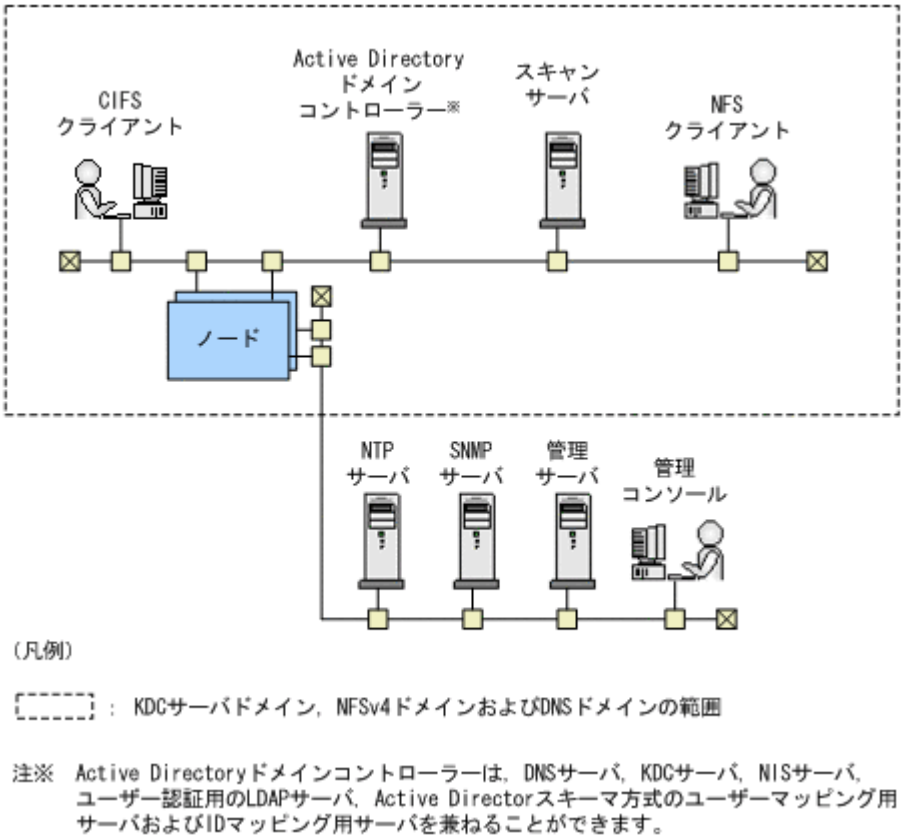
注※2　IDマッピング用サーバとして，ユーザー認証用のLDAPサーバ，NISサーバまたはActive Directoryドメインコントローラーを利用できます。

KDC サーバドメインや NFSv4 ドメインは，HVFP/HDI 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/HDI 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/HDI 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/HDI 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/HDI 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/HDI 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/HDI 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/HDI 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。

### (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。

### (2) キータブファイルの転送と組み込み

HVFP/HDI 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/HDI 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/HDI 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/HDI 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。

### (3) HVFP/HDI 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/HDI 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 サーバ名は，IP アドレスまたはホスト名で指定します。ドット（.）付きのホスト名でも指定できます。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。

### (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/HDI 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/HDI 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/HDI 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。

### (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。

### (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/HDI 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/HDI 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/HDI 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/HDI 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。

### (3) HVFP/HDI 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/HDI 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。

### (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

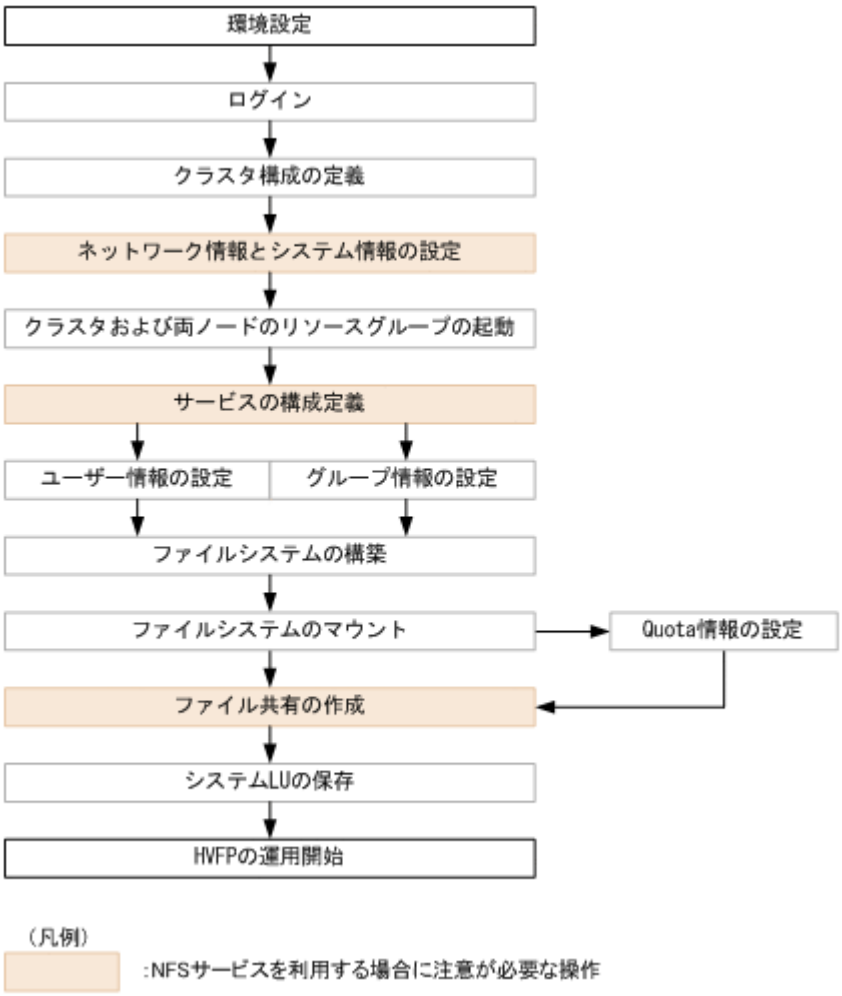
# File Services Manager での NFS サービスの運用

この章では，HVFP/HDI 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/HDI 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」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/HDI 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/HDI 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」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/HDI 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」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」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/HDI 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」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。<br>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。<br>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。<br>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」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」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/HDI 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。<br>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。

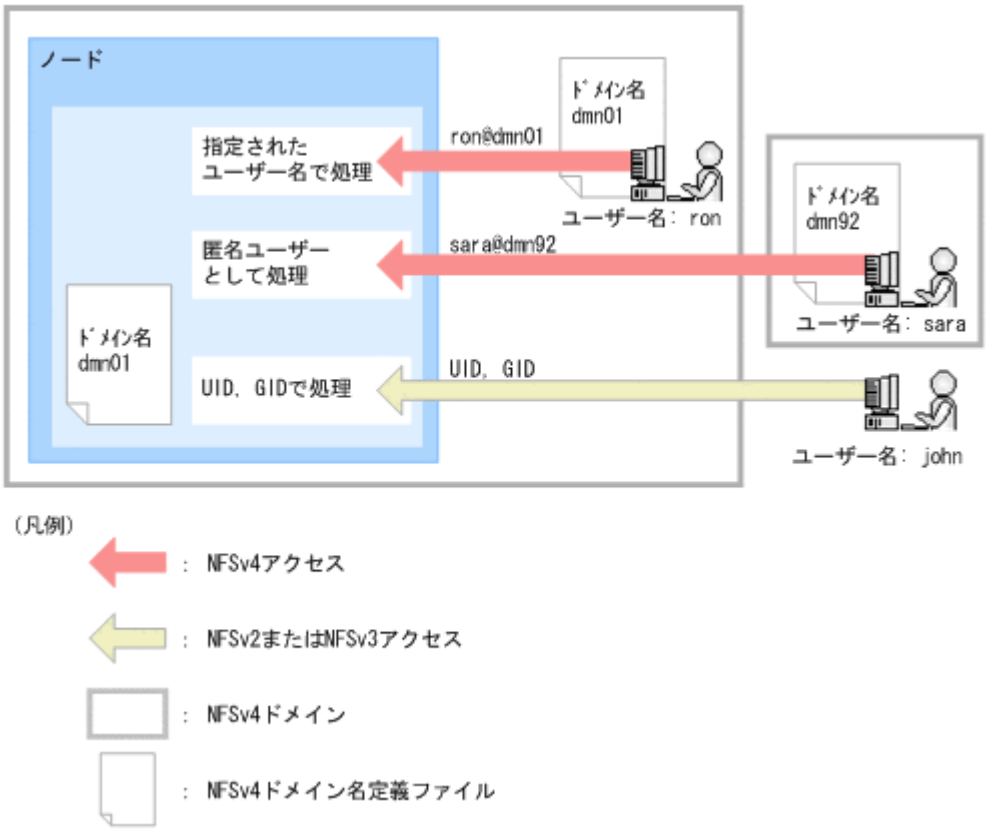
# 16.2 NFSv4 ドメインを設定しているときのユーザー管理

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/HDI 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/HDI 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/HDI 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/HDI 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/HDI 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/HDI 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/HDI 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/HDI 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

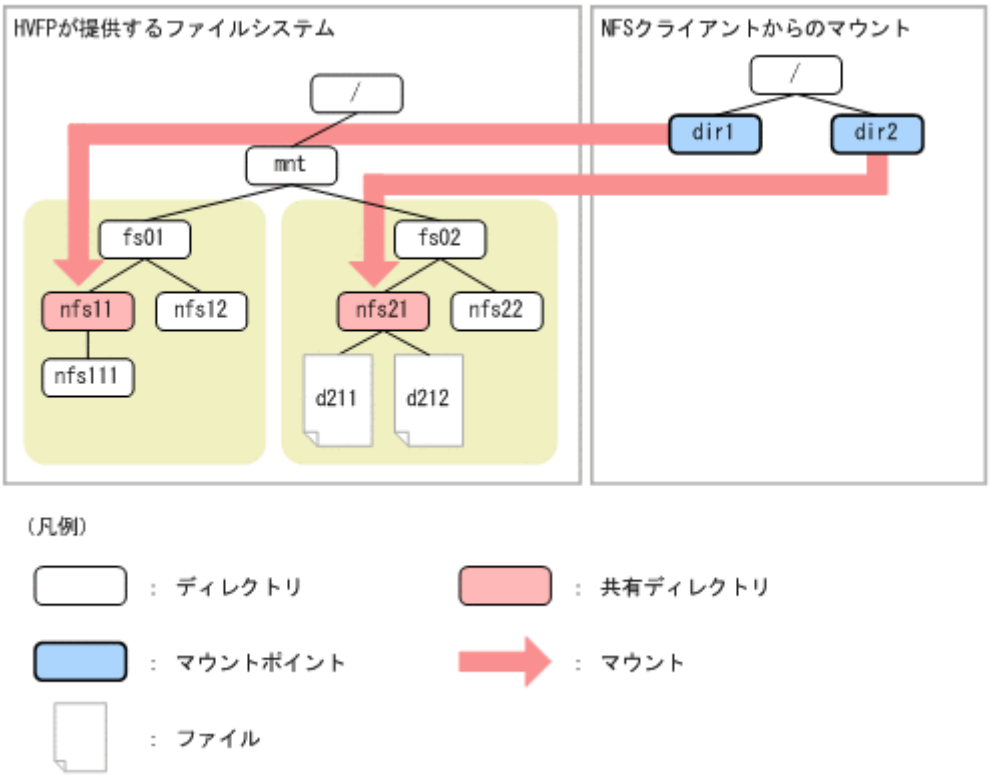
NFS クライアントから共有ディレクトリをマウントすることで，ファイルシステムにアクセスできるようになります。NFSv4 クライアントの場合は，共有ディレクトリのほか，ルートディレクトリをマウントすることもできます。

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**



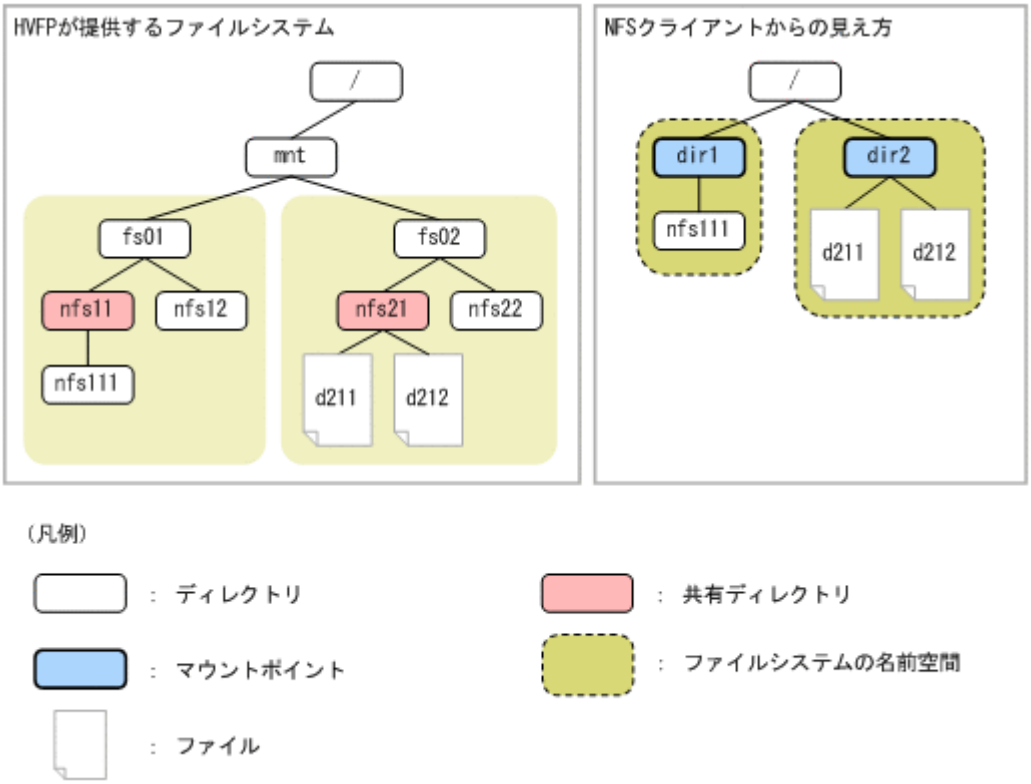
mount コマンドの実行例を次に示します。

```
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**

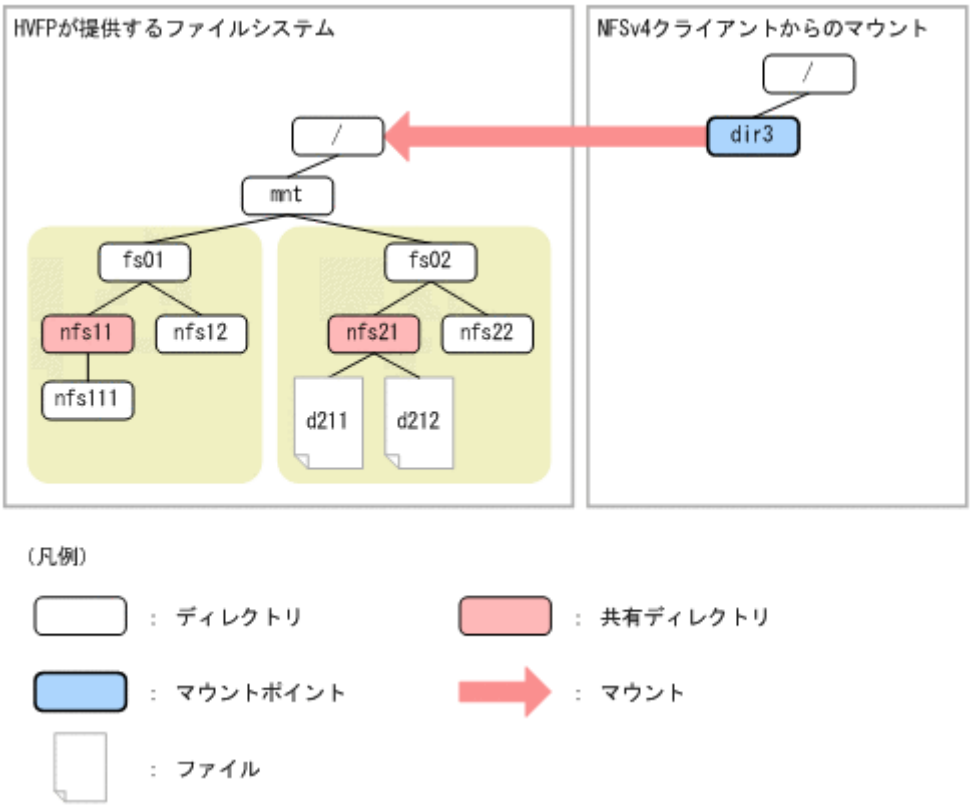



## 18.2.2 ルートディレクトリをマウントするとき

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。

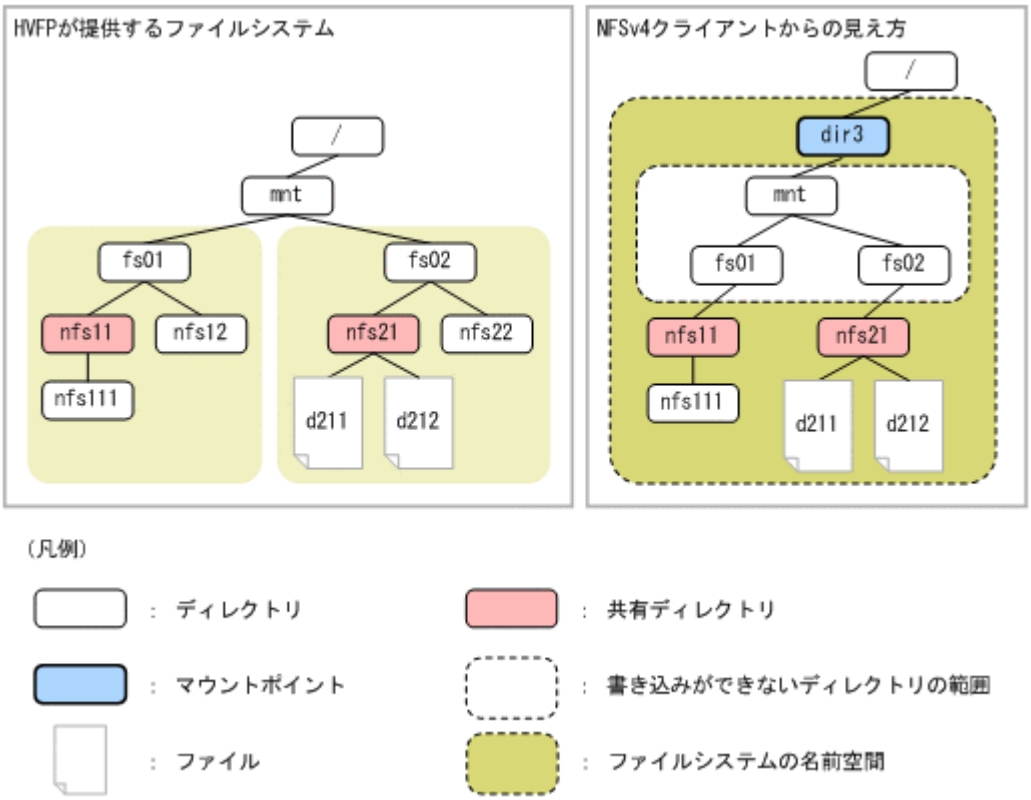
マウントディレクトリと各共有ディレクトリとの間にある直系のディレクトリに対して，NFSv4 クライアントから参照はできますが，書き込みはできません。また，直系のディレクトリ以下のファイルやディレクトリは，NFSv4 クライアントに対して隠蔽された状態となります。

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/HDI 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」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」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/HDI 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/HDI 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/HDI 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/HDI 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/HDI 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/HDI 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/HDI 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/HDI 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/HDI 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 アドレスと，NFS クライアントのホスト名（HVFP/HDI との通信に用いる IP アドレスのホスト名や正式ホスト名）に対する名前解決（IP アドレスからホスト名への変換）ができる必要があります。また，これらの名前解決の結果が，HVFP/HDI 側と NFS クライアント側とで一致している必要があります。

  ノードの OS のシステムファイルで IP アドレスやホスト名を管理する場合は，`/etc/hosts` ファイルに追記してください。なお，`/etc/hosts` ファイルの情報を追加，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。
- 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。
- HVFP/HDI 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/HDI 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/HDI 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/HDI 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/HDI 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/HDI 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/HDI 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/HDI 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/HDI 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/HDI 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/HDI 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/HDI 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/HDI 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/HDI 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/HDI 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/HDI 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。
- NFS クライアントマシンに HVFP/HDI 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/HDI 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。

・ IRIX を利用している NFS クライアントからマウントしたディレクトリで，新しく作成されたディレクトリ内にファイルを作成する操作を階層ごとに繰り返す処理を行った場合，階層が深くなると処理が停止するおそれがあります。

・ 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/HDI 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/HDI 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。
- AIX を NFS クライアントとして使用する場合，HVFP/HDI との NFS 通信では非特権ポート（1024 番以上のインターネットポート）がデフォルトとして使用されます。セキュリティを向上させるためには，スーパーユーザーだけが作成できる特権ポート（1024 番より小さなインターネットポート）を使用することを推奨します。特権ポートを使用すると，一般ユーザーは，HVFP/HDI にアクセスするときに，AIX の NFS クライアントシステムを使用する必要があり，NFS サービスを使用する際のセキュリティが向上します。特権ポートを使用するための設定については，ベンダーへお問い合わせください。

  特権ポートを使用する場合は，NFS 共有を作成または属性を変更する際に，発信ポートが制限されないよう設定してください。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。発信ポートが制限されないよう自動的に設定されます。コマンドを使用する場合は，nfscreate コマンドまたは nfsedit コマンドを実行する際に，-t オプションに do_not_perform（デフォルト）を指定してください。
- 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，AIX，IRIX，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/HDI 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と，読み込み処理が失敗することがあります。
- 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/HDI 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。
- Solaris または HP-UX を使用している NFSv4 クライアントが，バージョン管理を利用したファイルの復元を有効にしたファイルシステム内のサブディレクトリをマウントした場合，クライアントは.history ディレクトリ内のデータを参照できません。マイグレートされた時点の過去のデータを参照する場合は，サブディレクトリ下の.history ディレクトリにある，マイグレーションが実行された日時を示すディレクトリをマウントするよう，クライアントに依頼してください。

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/HDI 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 | 255 バイト |
| 2 | ディレクトリ名 | 255 バイト |

なお，HCP と連携しているファイルシステムの NFS 共有では，ファイル名，ディレクトリ名の文字コードが Unicode（UTF-8）になるようにしてください。

# 19.2 ACL

HVFP/HDI 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，「8.2.1 Classic ACL タイプと Advanced ACL タイプの差異」を参照してください。

HVFP/HDI 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/HDI 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/HDI 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 | × |
| 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/HDI で利用できる属性と利用できない属性があります。

HVFP/HDI 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/HDI 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，「8.6 WORM ファイル」を参照してください。

- ファイルの WORM 化は ACL ではなく，ファイル属性の「読み取り専用」の設定を契機としています。ACL ですべての書き込み権限を無効にしても，ファイルは WORM 化されません。
- 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）
  - AIX（32bit 版および AIX 5L 以前のバージョン）
  - 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。

20

# ファイル共有を利用するときの注意事項

この章では，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」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/HDI 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。
- 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設定にしてください。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する設定は，CIFS サービスで管理されているため，データの不整合が発生するおそれがあります。
- 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。

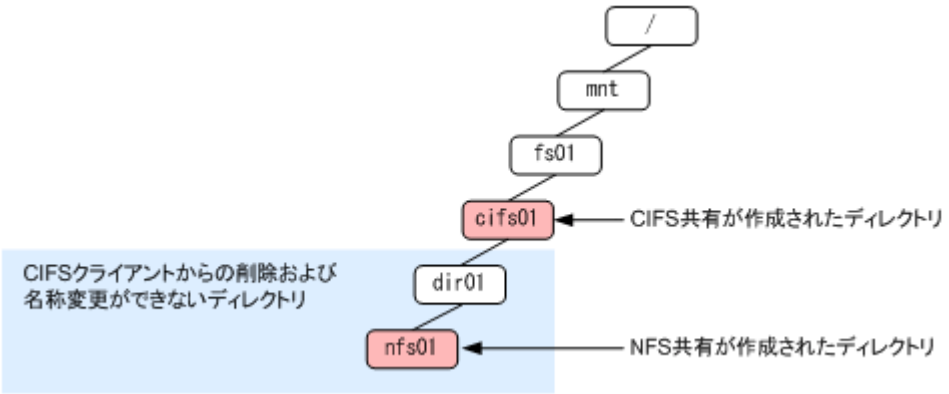
- NFS 共有で使用される文字コードは NFS クライアントの環境に依存するため，EUC や JIS などの文字コードを使用した NFS クライアントが作成したファイルやディレクトリを CIFS 共有側で利用する場合は，ファイル名やディレクトリ名が正しく表示されません。
- CIFS サービスで，ファイル所有者以外でのファイル更新日時の変更を許可すると，そのファイルに書き込み権限のあるすべてのユーザーが CIFS クライアントを経由することでファイル更新日時を変更できます。このファイルの所有者以外のユーザーによるファイル更新日時の変更は，NFS クライアントでは許可されていないため，十分注意してください。
- 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。詳細は「8.2.3 Advanced ACL タイプ」の(12)を参照してください。
- 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。ドメインコントローラーとして Windows Server 2003 R2 以降を使用している場合は，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/HDI が Active Directory ドメインに参加するための設定をします。

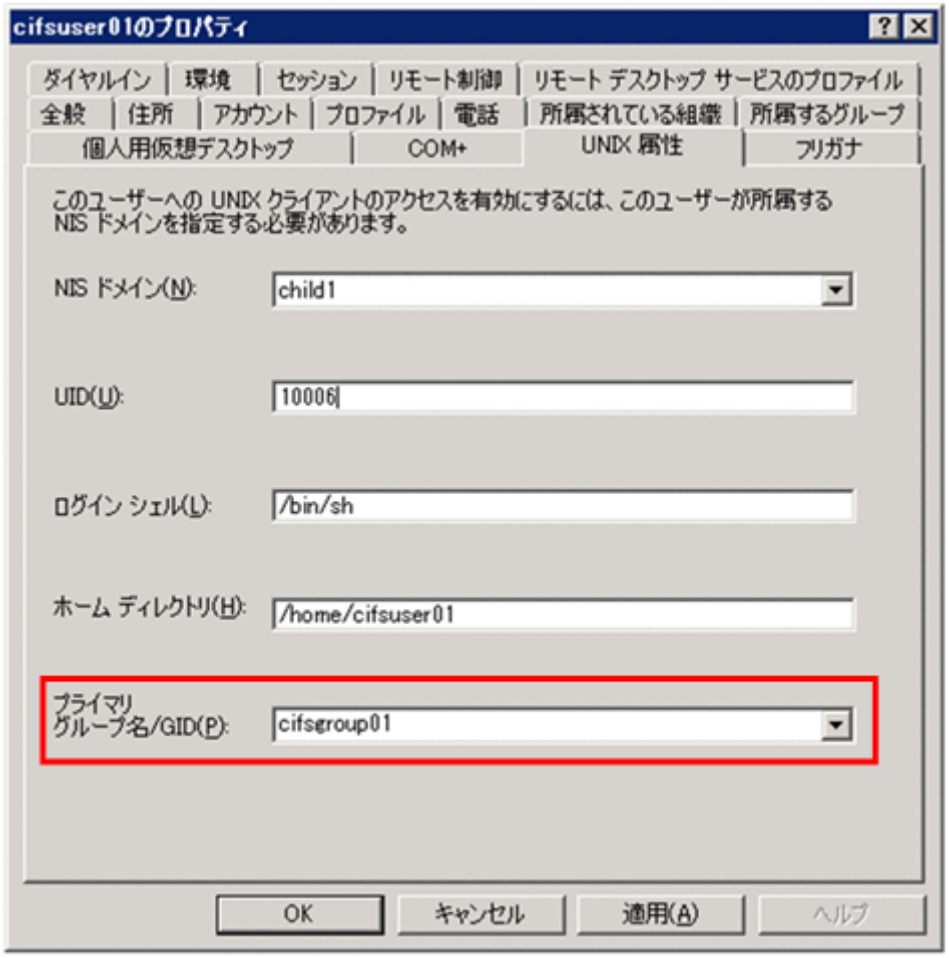
   Active Directory ドメインに参加するための手順については，「ユーザーズガイド」を参照してください。なお，手順 1 でユーザー自身の gidNumber をグループ ID として登録した場合は，cifsoptset コマンドの use_gidnumber オプションで，ユーザー自身の gidNumber を使用するように CIFS サービスの構成定義を変更する必要があります。

---

**参考** 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**



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 NT ドメインまたは Active Directory ドメインへの再参加に失敗しました。

対処方法：

NT ドメインまたは 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，NT ドメイン認証の場合は CIFS サービスを再起動，Active Directory 認証の場合は［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：

NT ドメインまたは 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/HDI 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/HDI 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/HDI 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/HDI 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/HDI 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 ドメインまたは NT 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/HDI 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」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。

# 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。

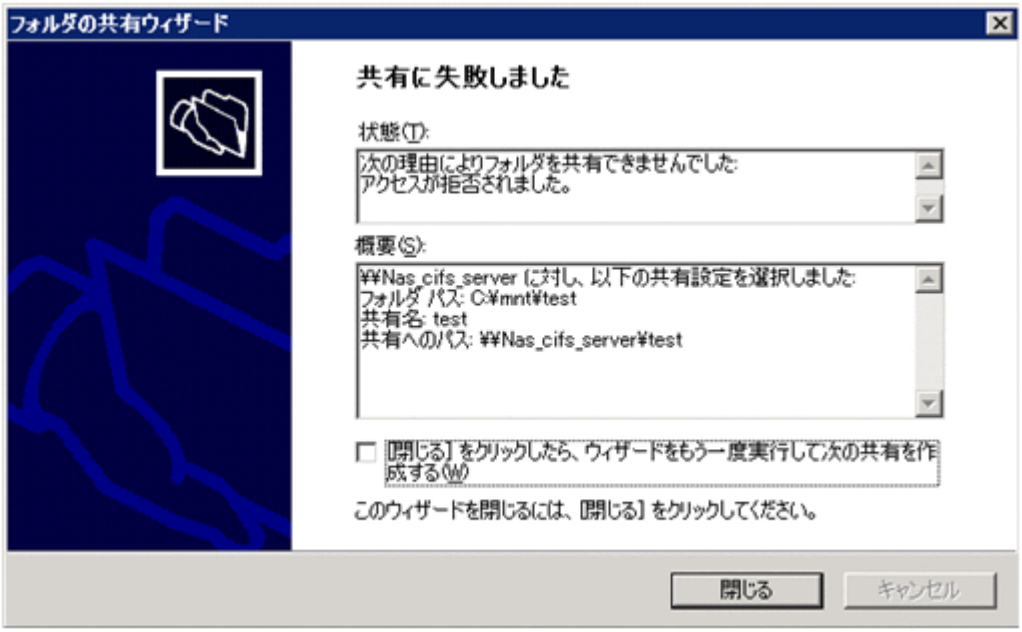
なお，エラー画面および操作画面の図は，Windows Server 2003，MMC 3.0 を使用した場合の例です。

## 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：

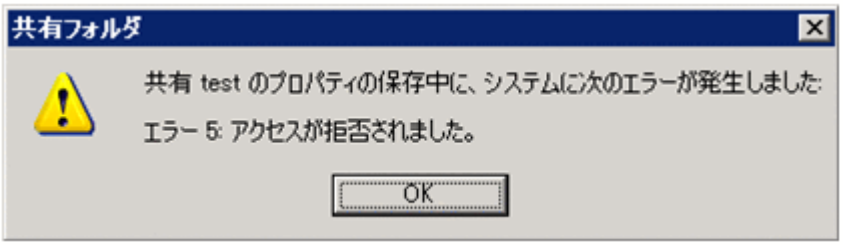
cifscreate コマンドのエラー要因を取り除いてください。cifscreate コマンドのログは，File Services Manager トレースログ（/enas/log/management.trace）に出力されます。File Services Manager トレースログを確認してください。

## 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

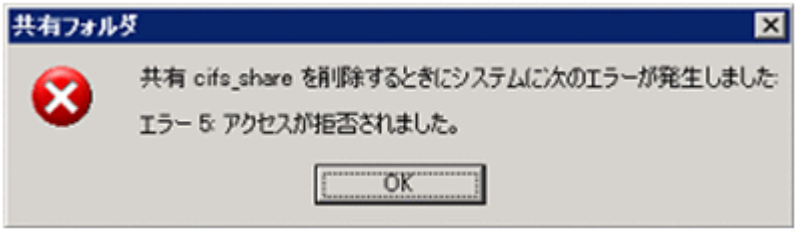
MMC から共有の停止をする（削除する）場合に発生するエラーについて，次にまとめます。

### (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：

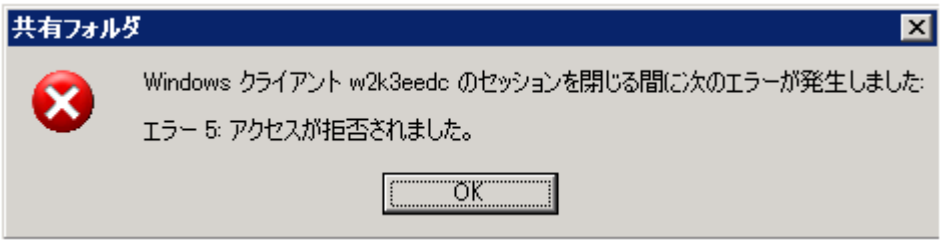
cifsdelete コマンドのエラー要因を取り除いてください。cifsdelete コマンドのログは，File Services Manager トレースログ（/enas/log/management.trace）に出力されます。File Services Manager トレースログを確認してください。

### (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：

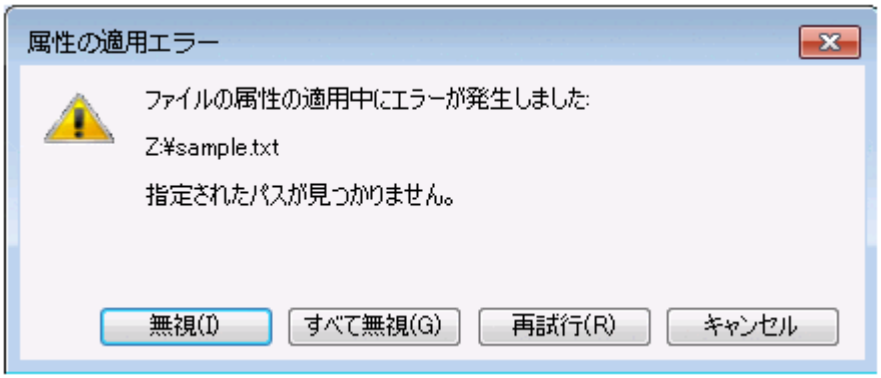
File Services Manager で登録された CIFS 管理者が操作してください。

## A.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-6 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/HDI の間で通信障害が発生している

対処：

クライアントと HVFP/HDI の間の通信状態を確認し，HVFP/HDI 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

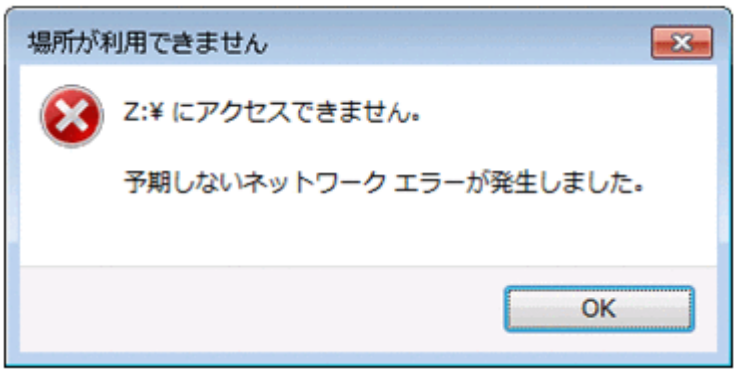
対処：

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-7 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。

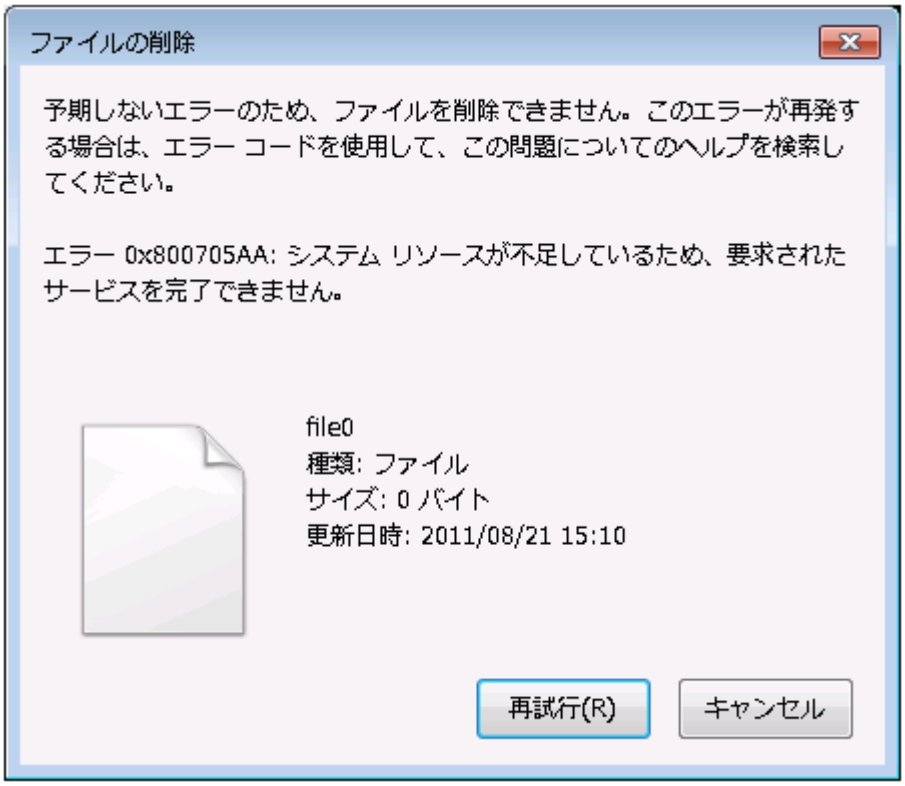
CIFS サービスへのアクセス中に CIFS サービスの再起動，フェールオーバーまたはフェールバックによってセッションが一時的に切断された。

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-8 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。

### 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。

# 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」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」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/HDI 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。

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/HDI 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/HDI 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/HDI 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/HDI 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/HDI 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保守員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保守員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

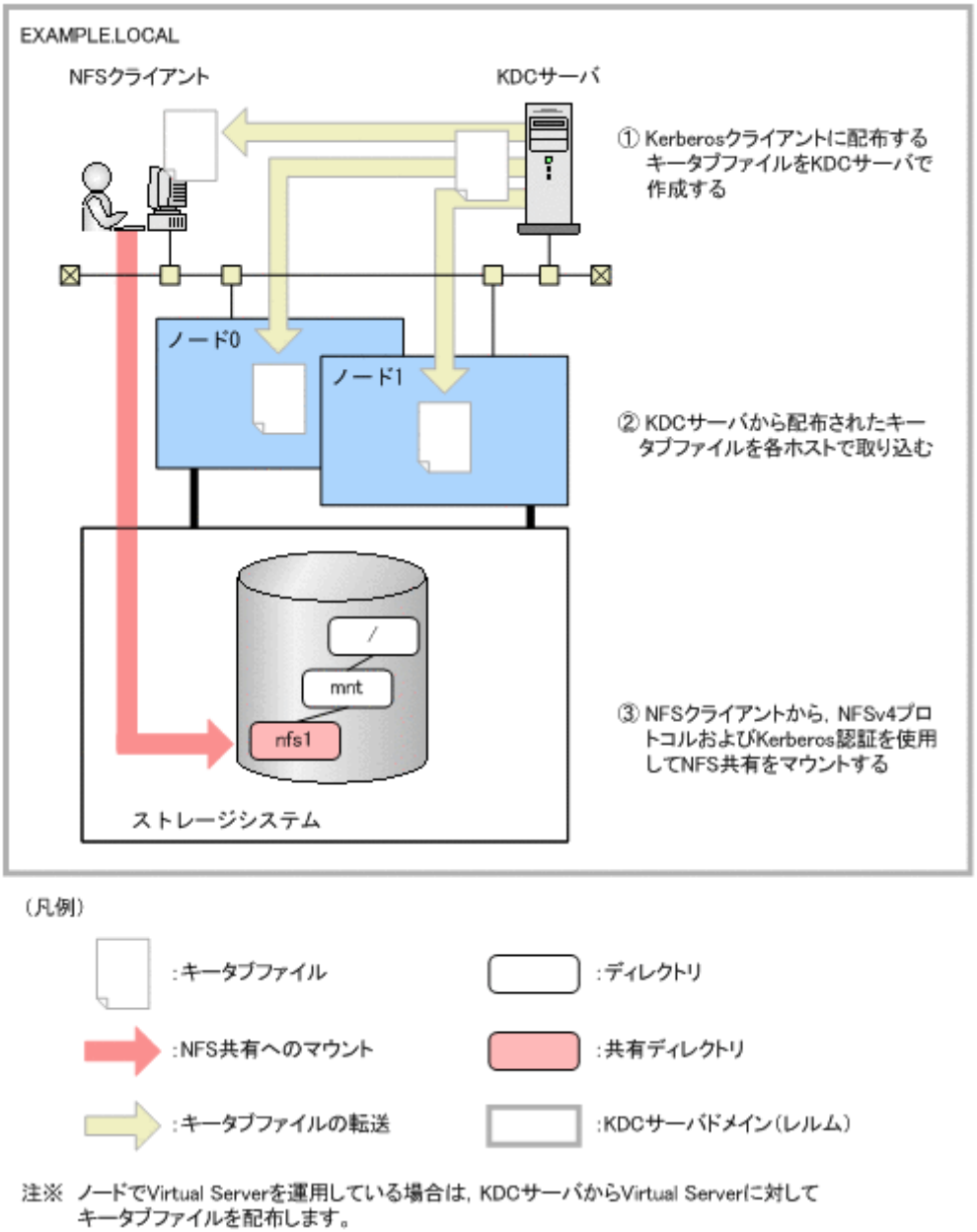
ここでは，Kerberos 認証を利用するときの NFS 環境の構築手順について，実行例を基に説明します。

# 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 |

| # | ホスト | ホスト名（FQDN） | キータブファイル名 |
|---|---|---|---|
| 4 | Virtual Server | vserver1.example.local | vserver1.keytab |
| 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/HDI 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/HDI 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 2003 または Windows Server 2008 の場合

Windows Server 2003 または Windows Server 2008 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 2003 の場合，サポートツールをインストールします。

   デフォルトでインストールされていないサポートツールが必要となります。インストールメディアに格納されている次のプログラムを実行してください。

   `support¥tools¥suptools.msi`

   また，インストールが完了したあと，次のプログラムが正しくインストールされていることを確認してください。

   - `Program Files¥Support Tools¥ksetup.exe`
   - `Program Files¥Support Tools¥ktpass.exe`
3. Windows Server 2008 R2 の場合，DES 暗号化を有効にします。

   Windows Server 2008 R2 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。

4. 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。

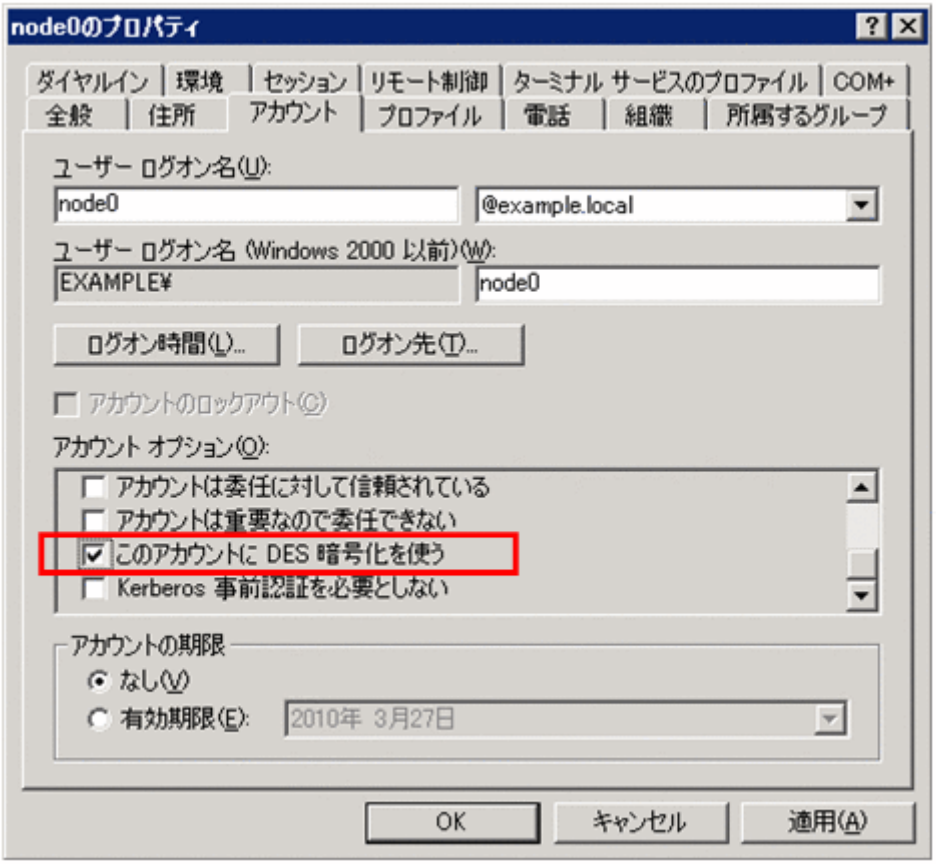
   Active Directory 管理ツールの［User］-［新規作成］-［ユーザー］を選択し，KDC サーバドメイン内のホストごとに 1 つずつ，ユーザーアカウントを作成します。ここでは，次の条件でユーザーアカウントを作成します。

**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 2003 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 2003 の場合）**




5. 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`

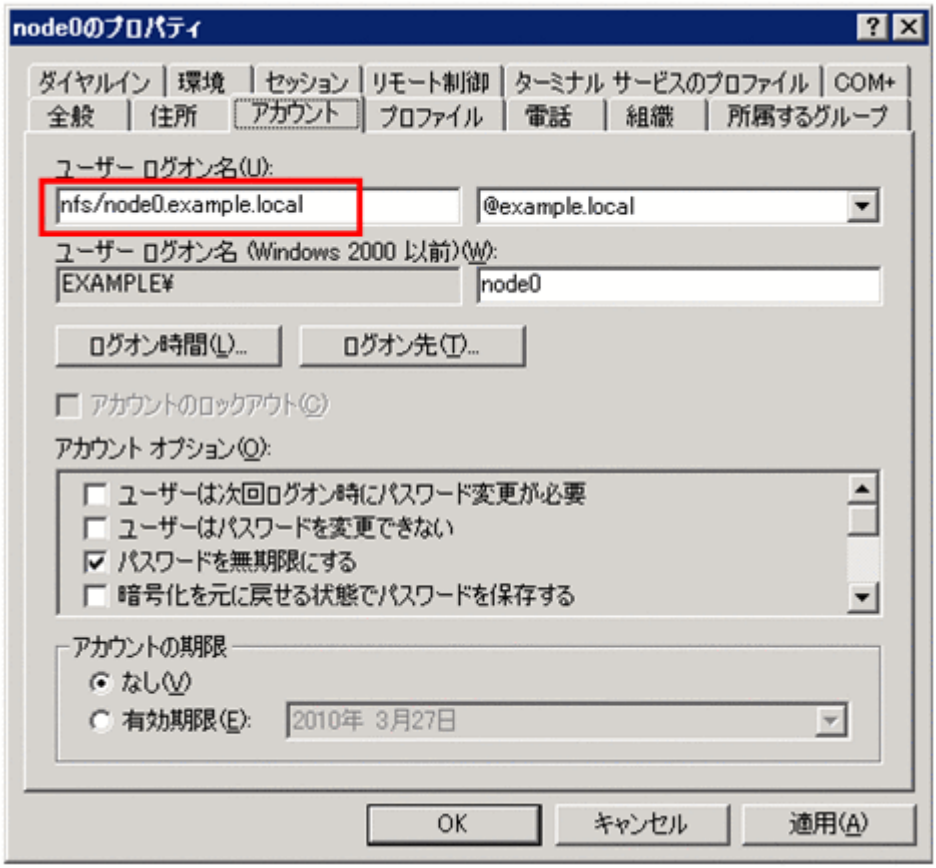
プリンシパルのタイプ

`-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 2003 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 2003 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.2.6 AIX 5L V5.3 の場合

ここでは，AIX 5L V5.3 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。

- AIX 3 5 000B9B6F4C00
- 5300-09

なお，AIX 5L V5.3 マシンで Kerberos 認証を使用するためには，次のファイルセットをインストールする必要があります。

- krb5.client.rte
- modcrypt.base
- clic.rte

AIX 5L V5.3 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. mkkrb5srv コマンドを使用して，KDC データベースを作成します。

```
# mkkrb5srv -r EXAMPLE.LOCAL -d example.local -s kdc1.example.local
...
```

2. 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
[libdefaults]
```

```
        default_realm = EXAMPLE.LOCAL
        default_keytab_name = FILE:/etc/krb5/krb5.keytab
        default_tkt_enctypes = des3-cbc-sha1 arcfour-hmac aes256-cts des-cbc-
md5 des-cbc-crc
        default_tgs_enctypes = des3-cbc-sha1 arcfour-hmac aes256-cts des-cbc-
md5 des-cbc-crc

[realms]
        EXAMPLE.LOCAL = {
                kdc = kdc1.example.local:88
                admin_server = kdc1.example.local:749
                default_domain = example.local
        }

[domain_realm]
        .example.local = EXAMPLE.LOCAL
        kdc1.example.local = EXAMPLE.LOCAL

[logging]
        kdc = FILE:/var/krb5/log/krb5kdc.log
        admin_server = FILE:/var/krb5/log/kadmin.log
        default = FILE:/var/krb5/log/krb5lib.log
```

3. KDC タイプを確認します。

```
# cat /etc/krb5/krb5_cfg_type
master
```

4. 管理用プリンシパルの初期チケットを取得します。

```
# kinit admin/admin@EXAMPLE.LOCAL
```

5. kadmin.local コマンドを使用して，root ユーザーのプリンシパルを作成します。

```
# /usr/krb5/sbin/kadmin.local
kadmin.local:  addprinc -e des-cbc-crc:normal root
...
```

6. kadmin.local 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，その host プリンシパルを KDC サーバのキータブファイル（krb5.keytab）に追加します。

   host プリンシパルを追加したら，kadmin.local コマンドを終了してください。

```
kadmin.local:  addprinc -randkey host/kdc1.example.local
...
kadmin.local:  ktadd host/kdc1.example.local
...
kadmin.local:  q
```

7. 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追加し，配布用のキータブファイルを作成します。

   キータブファイルを作成したら，kadmin ユーティリティを終了してください。

```
# /usr/krb5/sbin/kadmin
...
kadmin:  add_principal -e des-cbc-crc:normal -randkey nfs/node0.example.local
...
kadmin:  ktadd -e des-cbc-crc:normal -k /tmp/node0.keytab nfs/
node0.example.local
...
kadmin:  add_principal -e des-cbc-crc:normal -randkey nfs/node1.example.local
...
kadmin:  ktadd -e des-cbc-crc:normal -k /tmp/node1.keytab nfs/
node1.example.local
...
kadmin:  add_principal -e des-cbc-crc:normal -randkey nfs/
vserver1.example.local
...
kadmin:  ktadd -e des-cbc-crc:normal -k /tmp/vserver1.keytab nfs/
vserver1.example.local
...
```

```
kadmin:  add_principal -e des-cbc-crc:normal -randkey nfs/cl1.example.local
...
kadmin:  ktadd -e des-cbc-crc:normal -k /tmp/cl1.keytab nfs/cl1.example.local
...
kadmin:  q
```

8. KDC サーバを再起動します。

```
# /usr/krb5/sbin/stop.krb5
...
# /usr/krb5/sbin/start.krb5
...
```

# 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<br>ノード 1 : /home/nasroot※ |
| 2 | node1.keytab | ノード 1 | ノード 0 : /home/nasroot※<br>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/HDI のノードの場合）

配布されたキータブファイルを HVFP/HDI 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<br>HPUX11i-OE.OE B.11.31 HP-UX OE control script product |
| 4 | AIX 5L V5.3 | AIX 3 5 000B9B6F4C00 |
| | | 5300-09 |

NFS クライアントでキータブファイルを取り込む手順は，使用しているプラットフォームが AIX かどうかで異なります。

配布されたキータブファイルを，AIX 以外の 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
```

また，配布されたキータブファイルを，AIX 5L V5.3 の NFS クライアントで取り込む手順を次に示します。

1. krb5.client.rte，modcrypt.base および clic.rte ファイルセットがインストールされていることを確認します。

```
# lslpp -l krb5.client.rte
  Fileset                      Level  State      Description

----------------------------------------------------------------------------
Path: /usr/lib/objrepos
  krb5.client.rte            1.4.0.8  COMMITTED  Network Authentication
Service Client

Path: /etc/objrepos
krb5.client.rte            1.4.0.8  COMMITTED  Network Authentication
Service Client
# lslpp -l | grep modcrypt.base
  modcrypt.base.includes     5.3.7.1  COMMITTED  Cryptographic Library
Include
modcrypt.base.lib          5.3.7.1  COMMITTED  Cryptographic Library
# lslpp -l | grep clic.rte
  clic.rte.includes         3.24.0.1  COMMITTED  CryptoLite for C Library
  clic.rte.kernext          3.24.0.1  COMMITTED  CryptoLite for C Kernel
```

```
  clic.rte.lib              3.24.0.1  COMMITTED  CryptoLite for C Library
clic.rte.kernext          3.24.0.1  COMMITTED  CryptoLite for C Kernel
```

2. Kerberos クライアントとしてセットアップを実施します。

```
# config.krb5 -C -d example.local -r EXAMPLE.LOCAL -c kdc1.example.local -s
kdc1.example.local
```

3. 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 KDC サーバ名を変更してください。

```
# cat /etc/krb5/krb5.conf
[libdefaults]
        default_realm = EXAMPLE.LOCAL
        default_keytab_name = FILE:/etc/krb5/krb5.keytab
        default_tkt_enctypes = des3-cbc-sha1 arcfour-hmac aes256-cts des-cbc-
md5 des-cbc-crc
        default_tgs_enctypes = des3-cbc-sha1 arcfour-hmac aes256-cts des-cbc-
md5 des-cbc-crc

[realms]
        EXAMPLE.LOCAL = {
                kdc = kdc1.example.local:88
                admin_server = kdc1.example.local:749
                default_domain = example.local
        }

[domain_realm]
        .example.local = EXAMPLE.LOCAL
        kdc1.example.local = EXAMPLE.LOCAL

[logging]
        kdc = FILE:/var/krb5/log/krb5kdc.log
        admin_server = FILE:/var/krb5/log/kadmin.log
        default = FILE:/var/krb5/log/krb5lib.log
```

4. 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。

```
# /usr/krb5/sbin/ktutil
ktutil:  rkt /tmp/cl1.keytab
ktutil:  wkt /etc/krb5/krb5.keytab
ktutil:  list
slot KVNO Principal
---- ----
---------------------------------------------------------------------
1    3     nfs/cl1.example.local@EXAMPLE.LOCAL
ktutil:  quit
```

5. マージされたキータブファイルを使用するために，gssd デーモンをセットアップします。

```
# nfshostkey -p nfs/aix.example.local -f /etc/krb5/krb5.conf
```

6. gssd デーモンを開始します。

```
# chnfs -S -B
```

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

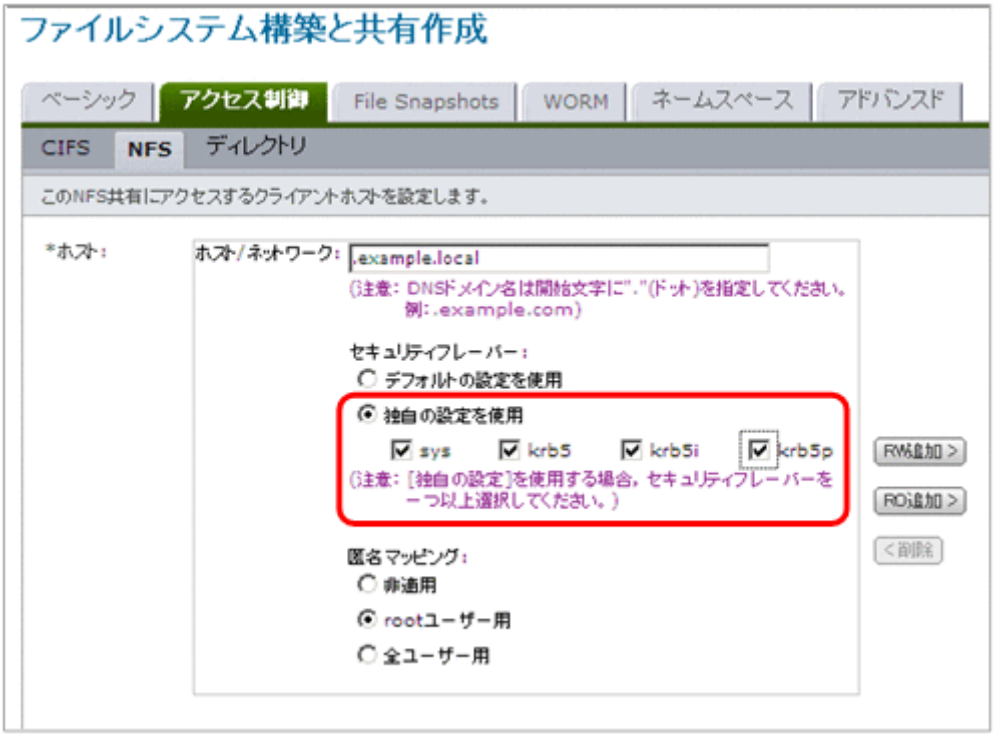
ここでは，Kerberos 認証を利用するときの NFS 共有ディレクトリへのアクセス手順について，実行例を基に説明します。

# 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」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。

E

# セカンダリー KDC サーバの追加手順

HVFP/HDI 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
```

F

# 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。 | http://msdn.microsoft.com/ja-jp/library/cc429940.aspx |
| 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。 | http://msdn.microsoft.com/ja-jp/library/cc429784.aspx |

### (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;<br>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 | http://msdn.microsoft.com/ja-jp/library/x3399a54.aspx |

| 構造体名称 | メンバー | 説明 | 参考資料 |
|---|---|---|---|
| | | ザーが直接対話的に扱うのには向いていません。 | |
| SYSTEMTIME | WORD wYear;<br>WORD wMonth;<br>WORD wDay;<br>WORD wDayOfWeek;<br>WORD wHour;<br>WORD wMinute;<br>WORD wSecond;<br>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 |

### (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。 | http://msdn.microsoft.com/ja-jp/library/cc429961.aspx |
| LocalFileTimeToFileTime | ローカルタイムを協定世界時（UTC）に変換します。 | http://msdn.microsoft.com/ja-jp/library/cc429894.aspx |
| CreateFile | SetFileTime に指定するファイルのハンドルを取得します。 | http://msdn.microsoft.com/ja-jp/library/cc429198.aspx |
| GetFileAttributes | 現在のファイル属性を取得します。 | http://msdn.microsoft.com/ja-jp/library/cc429313.aspx |

## F.1.4 サンプルプログラム

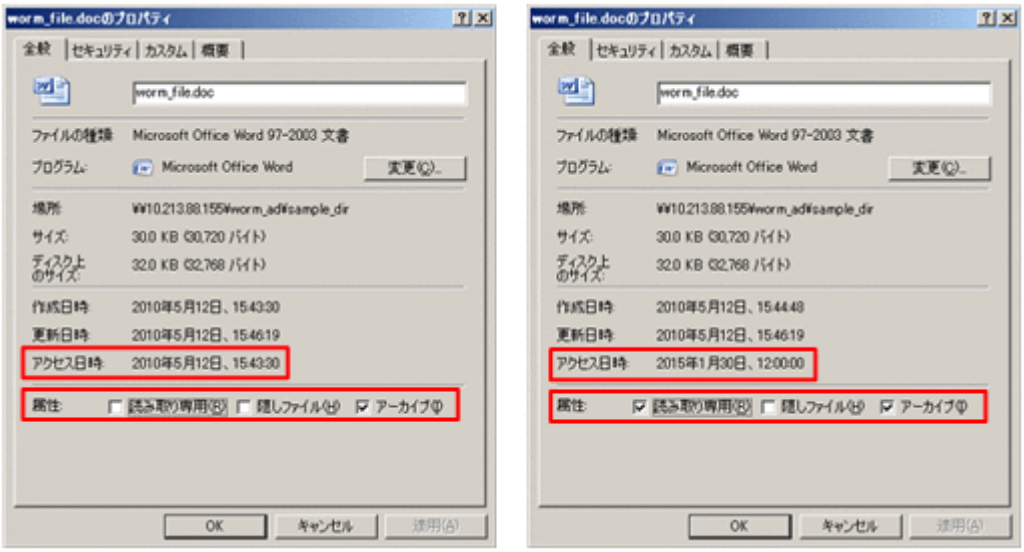
ファイルにリテンション期間を設定し，読み取り専用にする C 言語のプログラムの例を次に示します。

```
#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()<br>utimes() | ファイルにリテンション期間を設定します。 |
| chmod()<br>fchmod() | 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。 |

### (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
};
```

### (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。読み取り専用属性を解除する場合は，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。

## 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/HDI 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<br>NFSERR_IO | chmod，utime システムコール<br>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<br>NFSERR_IO | rename システムコール<br>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<br>NFS3ERR_IO | chmod，utime システムコール<br>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<br>NFS3ERR_IO | rename システムコール<br>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 |
| 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<br>NFS4ERR_IO | rename システムコール<br>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 |

| 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 |
|---|---|---|---|
| | | | 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<br>NFS4ERR_IO | chmod，utime システムコール<br>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<br>NFS3ERR_ACCES<br>NFS4ERR_ACCES | EACCES |
| NFSERR_IO<br>NFS3ERR_IO<br>NFS4ERR_IO | EIO |
| NFSERR_ROFS<br>NFS3ERR_ROFS<br>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

Web サイトの URL を示します。

OpenLDAP

http://www.openldap.org

ADAM

- 英語

  http://technet.microsoft.com/en-us/library/cc736765(WS.10).aspx

- 日本語

  http://technet.microsoft.com/ja-jp/library/cc779554(WS.10).aspx

# H

# 略語一覧

ここでは，HVFP/HDI のマニュアルで使用している略語を示します。

# H.1 HVFP/HDI のマニュアルで使用している略語

HVFP/HDI 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 |
| DDNS | Dynamic Domain Name System |
| DEP | data execution prevention |
| DES | Data Encryption Standard |
| DFS | distributed file system |
| DIMM | dual in-line memory module |
| DHCP | Dynamic Host Configuration Protocol |
| 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 |
| RADIUS | Remote Authentication Dial In User Service |
| 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 |
| UPnP | Universal Plug and Play |
| 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

## し



## す



## せ



## て



## と



## な



## に



## ふ



## ほ



## め



## ゆ

## り



## ろ