

Hitachi Virtual File Platform / Hitachi Data Ingestor

システム構成ガイド（イントラ掲載用）

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。

ActiveX 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。

ALog ConVerter は、株式会社網屋の登録商標です。

Ethernet は、富士ゼロックス株式会社の登録商標です。

Firefox は Mozilla Foundation の登録商標です。

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。

Internet Explorer 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。

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。

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。

Microsoft .NET は、お客様、情報、システムおよびデバイスを繋ぐソフトウェアです。

Mozilla は、Mozilla Foundation の、米国およびその他の国における商標です。

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.

POSIX は、the Institute of Electrical and Electronics Engineers, Inc. (IEEE)で制定された標準仕様です。

RC4 は、EMC 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。

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。

Symantec は、Symantec Corporation 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。

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 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。

インテル, Intel, および Intel Core 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。

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7版）K6603834

著作権

All Rights Reserved. Copyright (C) 2013, 2014, Hitachi, Ltd.

目次

はじめに.....	23
対象読者.....	24
マニュアルの構成.....	24
マニュアル体系.....	25
関連マニュアル.....	26
このマニュアルでの表記.....	27
このマニュアルで使用する記号.....	29
このマニュアルで使用する構文要素.....	30
コマンドの書式で使用する記号.....	30
KB（キロバイト）などの単位表記について.....	30
1. Hitachi Virtual File Platform / Hitachi Data Ingestor の概要.....	31
1.1 Hitachi Virtual File Platform / Hitachi Data Ingestor とは.....	32
1.2 Hitachi Content Platform との連携.....	35
2. システム構成.....	39
2.1 ハードウェア構成.....	40
2.1.1 ストレージシステムとノードの構成.....	40
2.1.2 HVFP/HDI で必要な外部サーバや外部装置.....	40
2.1.3 NDMP 機能を使用する場合に HVFP/HDI で必要な外部サーバや外部装置.....	43
2.2 ネットワーク構成.....	44
2.2.1 CIFS 共有を利用する場合のネットワーク構成.....	48
(1) CIFS クライアントとノードが同じサブネットに接続されている場合.....	49
(2) CIFS クライアントがノードと異なるサブネットに接続されている場合.....	50
(3) 複数のポートで CIFS サービスを利用する場合.....	52
2.2.2 リンク結合を使用するとき.....	53
(1) 特長.....	54
(2) リンク結合を使用する前に.....	54
(3) 推奨するリンク結合の構成.....	54
(4) 構成例.....	55
2.2.3 VLAN を使用するとき.....	58
(1) 特長.....	58
(2) VLAN を使用する前に.....	58
(3) VLAN インターフェースの設定.....	59
(4) 構成例.....	59
2.2.4 VLAN とリンク結合を併用するとき.....	60
2.3 ライセンス.....	60
2.4 HCP 連携時のシステム構成.....	62

2.4.1 ストレージシステムを共有して連携する場合	62
2.4.2 ネットワークを介して連携する場合	64
3. 外部サーバの環境設定	65
3.1 HVFP/HDI で必要な外部サーバ	66
3.2 管理サーバの環境設定	67
3.2.1 管理サーバのマシン要件	67
3.2.2 管理サーバのクラスタ構成	70
3.2.3 コマンドプロンプトからの管理者権限でのコマンド実行	71
3.3 管理コンソールの環境設定	72
3.3.1 管理コンソールのマシン要件	72
3.3.2 管理コンソールで Internet Explorer を使用する場合の設定	74
(1) Internet Explorer を使用する場合の注意事項	74
(2) Internet Explorer の設定	74
3.3.3 管理コンソールで Firefox を使用する場合の設定	76
3.4 NIS サーバの環境設定	78
3.5 LDAP サーバの環境設定	78
3.5.1 LDAP サーバを利用する際の注意事項	79
3.5.2 OpenLDAP を使用する場合の注意事項	79
3.5.3 Sun Java System Directory Server を使用する場合の注意事項	80
3.5.4 ADAM を使用する場合の注意事項	80
3.5.5 OpenLDAP を使用する場合の設定例	81
(1) スキーマファイルの作成	81
(2) index ディレクティブの設定	82
3.5.6 Sun Java System Directory Server を使用する場合の設定例	82
(1) スキーマファイルの作成	82
(2) index の設定	83
3.5.7 ADAM を使用する場合の設定例	84
(1) スキーマファイルの作成	84
(2) index の設定	86
3.6 ドメインコントローラーの環境設定	87
3.7 KDC サーバの環境設定	88
3.8 RADIUS サーバの環境設定	89
3.9 SNMP マネージャーの環境設定	89
3.9.1 SNMP マネージャーとして使用するマシンの設定	89
3.9.2 specific-trap の設定	89
3.9.3 日立固有 MIB オブジェクトの定義ファイルの取得方法	90
3.9.4 SNMP エージェントのバージョン	91
3.9.5 SNMP エージェントの起動時および停止時のトラップ通知	91
3.10 NTP サーバの環境設定	91
3.11 スキャンサーバの環境設定	92
3.12 ノードに SAN で接続されたテープ装置の環境設定	95
3.12.1 テープドライブの情報の登録	95
3.12.2 テープドライブの登録情報の有効化	95
3.12.3 テープドライブの登録情報の解除	96
3.12.4 ノードに SAN で接続されたテープ装置を設定する上での注意事項	96
3.12.5 テープ装置の交換	96
3.12.6 テープ装置の取り外し	97
3.13 SMTP サーバの環境設定	97
3.14 ALog マネージャーサーバの環境設定	97
3.15 DHCP サーバの環境設定	97
3.16 DNS サーバの環境設定	98

4. 運用を開始する前に.....	99
4.1 運用上の注意事項（必ずお読みください）.....	100
4.2 クラスタ構成を管理する前に.....	102
4.3 クライアントのユーザー情報を管理する前に.....	104
4.4 ユーザーマッピングでの運用を開始する前に.....	104
4.4.1 HVFP/HDI を利用できるドメインの範囲.....	104
4.4.2 ユーザーマッピングの方式.....	107
(1) RID 方式.....	107
(2) LDAP 方式.....	107
(3) Active Directory スキーマ方式.....	108
4.4.3 ユーザーマッピングの方式の変更.....	108
4.4.4 ユーザー ID とグループ ID の範囲の検討例（RID 方式の場合）.....	110
4.5 ファイルシステムの運用を開始する前に.....	113
4.5.1 LU（デバイスファイル）やボリュームグループの作成方法.....	114
4.5.2 LU を割り当てるときの注意事項.....	115
4.5.3 Virtual Server で利用する LU.....	116
4.5.4 ローカルデータの暗号化機能を使用するときの注意事項.....	116
4.5.5 ファイルシステム使用量に関する警告の通知.....	117
4.5.6 ストライピング機能を使用するとき.....	120
(1) ストライピング機能とは.....	120
(2) ストライピング機能を使用するときの注意事項.....	122
4.5.7 ファイルシステムで利用する ACL タイプの選択.....	122
4.5.8 Advanced ACL タイプのファイルシステムへの移行.....	125
(1) ファイルシステム移行時の注意事項.....	126
(2) 移行後のファイルシステム容量の見積もり.....	128
(3) ファイルシステムの移行手順.....	128
4.5.9 WORM 対応ファイルシステムの運用.....	130
(1) 自動コミットを使用して WORM 化する.....	131
(2) クライアントから手動で WORM 化する.....	131
(3) WORM 対応ファイルシステムを運用するときの注意事項.....	132
4.5.10 階層ファイルシステムの運用.....	132
(1) 階層ファイルシステムで使用する LU.....	133
(2) 階層ファイルシステムを運用するときの注意事項.....	134
4.5.11 複数ファイルのデータ集約による容量節約.....	134
4.5.12 CIFS 走査チェックのバイパス機能.....	135
4.6 Quota の運用を開始する前に.....	136
4.6.1 Quota 管理で設定できる情報.....	137
(1) ユーザー、グループまたはディレクトリに対する Quota の設定.....	138
(2) デフォルト Quota の設定.....	139
(3) 猶予期間の設定.....	139
(4) Quota 監視方法の設定.....	139
(5) Quota を設定するときの注意事項.....	141
4.6.2 ファイルシステムごとに Quota を管理する場合.....	142
4.6.3 サブツリー Quota を管理する場合.....	143
4.6.4 Quota を管理する場合の注意事項.....	144
4.6.5 Quota 管理の運用例.....	145
4.7 ファイル共有の運用を開始する前に.....	147
4.7.1 NFS 共有を運用する前に確認しておくこと.....	147
4.7.2 CIFS 共有を運用する前に確認しておくこと.....	147
4.7.3 CIFS 共有を作成する前に確認しておくこと.....	148
4.7.4 ホームドライブを設定するとき.....	148
4.7.5 MMC と連携するとき.....	149
4.7.6 CIFS アクセスログを利用するとき.....	149
4.7.7 Classic ACL タイプのファイルシステムで ACL を設定するとき.....	149
4.7.8 ALog ConVerter と連携するとき.....	149

(1) ALog ConVerter との連携を開始する手順 (クラスタ構成の場合)	150
(2) ALog ConVerter との連携を開始する手順 (シングルノード構成の場合)	151
4.7.9 TFTP サービスを使用するとき	151
4.8 リアルタイムスキャン機能の運用を開始する前に	152
4.8.1 リアルタイムスキャン機能を運用する場合の注意事項	153
(1) リアルタイムスキャンの動作	153
(2) リアルタイムスキャンでエラーが発生した場合	153
(3) 一時ファイル	154
(4) WORM ファイル	155
(5) スタブファイル	155
(6) Anti-Virus Enabler ライブラリトレースログファイル (antiviruslib.trace) の管理	155
(7) ログイン中の CIFS クライアント数の表示	156
4.8.2 スキャンサーバを登録する際の注意事項	156
4.8.3 リアルタイムスキャン機能の運用設計	156
(1) リアルタイムスキャンの性能低下によって発生する問題点	156
(2) スキャン条件やログファイルの確認	157
(3) レポート情報ファイル (antivirus_report.csv) の確認	158
(4) ユーザー統計情報ファイル (antivirus_stat.csv) の確認	160
(5) 性能低下の改善方法の検討	161
4.8.4 リアルタイムスキャン機能のスキャン条件の見直し	164
(1) キャッシュのサイズを増やす	164
(2) スキャンタイムアウト時間を増やす	164
(3) ウイルススキャンの実行回数を減らす	164
(4) 一時ファイルの作成を抑止する	165
(5) スキャン対象を選定する	165
4.9 システム設定情報の管理を開始する前に	166
4.10 障害情報の管理を開始する前に	167
4.10.1 管理サーバの障害情報	167
4.10.2 ノードや Virtual Server の障害情報	167
4.10.3 SNMP による障害通知の利用方法	167
4.10.4 E-mail による障害通知の利用方法	168
4.11 SNMP によるシステム監視を開始する前に	168
4.12 ほかのファイルサーバからデータをインポートする前に	168
4.12.1 ほかのファイルサーバからデータをインポートするときのシステム構成	169
4.12.2 ほかのファイルサーバからデータをインポートするときの注意事項	171
4.13 クライアントがファイルシステムの利用を開始する前に	173
4.13.1 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	173
4.13.2 CIFS 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	174
4.13.3 FTP 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	174
5. HVFP/HDI のバックアップ運用	177
5.1 バックアップ運用の概要	178
5.2 NDMP 機能の運用について	178
5.2.1 NDMP 機能の概要	179
5.2.2 バックアップメディアの容量の見積もり	180
5.2.3 オンラインバックアップに使用する差分格納デバイスの設定	181
5.2.4 バックアップおよびリストア対象のデータについて	182
5.2.5 バックアップおよびリストアの実施時間について	182
5.2.6 インクリメンタルバックアップの運用について	182
5.2.7 NDMP サーバへのアクセス制限について	184
5.2.8 バックアップまたはリストア時の通信経路について	185
5.2.9 バックアップまたはリストア中に実行できない操作	185
5.2.10 File Services Manager から操作する場合の注意事項	185
5.2.11 ノード上の OS を起動する場合の注意事項	186

5.2.12	バックアップ管理ソフトウェアの機能制限	186
5.2.13	WORM 対応ファイルシステムのバックアップおよびリストアに関する注意事項	187
	(1) バックアップを実行する場合	187
	(2) リストアを実行する場合	187
5.2.14	データ集約されているファイルシステムのバックアップ、リストアについて	188
5.3	ファイルスナップショット機能の運用について	188
5.3.1	ファイルスナップショット機能の概要	189
5.3.2	ファイルスナップショット機能を運用するための前提条件	189
5.3.3	ファイルシステムと差分格納デバイスの管理	189
	(1) ファイルシステムおよび差分格納デバイス容量の拡張について	190
	(2) 差分格納デバイスに使用するデバイスファイルについて	191
	(3) 差分格納デバイスの容量の見積もりについて	191
	(4) 差分格納デバイスの使用量に関する設定について	192
	(5) ファイルシステムへのデータ書き込みについて	192
	(6) CIFS サービスの構成定義について	192
	(7) 仮想 LU の未使用領域の解放について	192
5.3.4	差分スナップショットの管理	192
	(1) 差分スナップショットの予約世代数について	193
	(2) 確保できる差分スナップショットの数について	193
	(3) 差分スナップショットの作成・削除に掛かる時間について	197
	(4) 差分スナップショットの更新時刻・参照時刻について	198
5.3.5	同時に実行できない操作	198
5.3.6	ファイルスナップショット機能の注意事項	198
	(1) Backup Restore のボリュームレプリケーション連携機能を運用する場合の注意事項	198
	(2) Hitachi File Remote Replicator を運用する場合の注意事項	199
	(3) HCP と連携する場合の注意事項	199
	(4) シングルノード構成で運用する場合の注意事項	199
5.4	差分スナップショットの運用例	199
5.4.1	差分スナップショットの運用方法の検討と設定（クラスタ構成の場合）	199
	(1) 想定するシステム構成	199
	(2) HOME ファイルシステムでの差分スナップショットの運用	200
	(3) DOCUMENT ファイルシステムでの差分スナップショットの運用	202
5.4.2	差分スナップショットの運用方法の検討と設定（シングルノード構成の場合）	203
	(1) 想定するシステム構成	203
	(2) HOME ファイルシステムでの差分スナップショットの運用と設定	203
5.4.3	運用テストの実施	204
	(1) HOME ファイルシステムの運用テスト	204
	(2) DOCUMENT ファイルシステムの運用テスト	204
5.4.4	差分スナップショットの運用開始	205
	(1) HOME ファイルシステムでの作業	205
	(2) DOCUMENT ファイルシステムでの作業	206
5.4.5	クライアント側での操作	206
	(1) HOME ファイルシステムの差分スナップショットの操作	206
	(2) DOCUMENT ファイルシステムの差分スナップショットの操作	208
5.4.6	運用状況の監視	208
5.4.7	運用完了後の作業	209
5.5	差分格納デバイスの容量の設計	210
5.5.1	HCP にデータがマイグレートされないファイルシステムの場合の見積もり式	211
5.5.2	HCP にデータがマイグレートされるファイルシステムの場合の見積もり式	212
5.5.3	階層ファイルシステムの場合の見積もり式	213
	(1) Tier 1 の場合の見積もり式	213
	(2) Tier 2 の場合の見積もり式	214
5.5.4	差分格納デバイスを構成するデバイスファイルの前提条件	215
5.5.5	HCP にデータがマイグレートされないファイルシステムの場合の見積もり例	216
5.5.6	HCP にデータがマイグレートされるファイルシステムの場合の見積もり例	217
5.6	差分格納デバイスの使用量に関する設定	218

5.6.1	警告閾値の設定	219
5.6.2	あふれ防止動作および動作閾値の設定	219
5.6.3	あふれ時の動作の設定	220
5.7	ファイルスナップショット機能で運用しているファイルシステムの拡張	220
5.8	差分スナップショットの自動作成の運用	221
5.8.1	自動作成スケジュールの動作	222
	(1) 差分スナップショットの自動作成の動作	222
	(2) 差分スナップショットの自動マウント・公開の動作	222
	(3) 予約世代数または自動作成の上限数に達した場合のシステムの動作	224
	(4) 自動マウントの上限数に達した場合のシステムの動作	225
5.8.2	自動作成スケジュールを運用する際の注意事項	226
	(1) スケジュールの設定に関する注意事項	226
	(2) 差分スナップショットを自動マウントする場合の注意事項	227
	(3) 差分スナップショットをファイルシステムの共有内に自動公開する場合の注意事項	227
	(4) 差分スナップショットにファイル共有を自動作成する場合の注意事項	229
	(5) Volume Shadow Copy Service を使用して差分スナップショットを公開する場合の注意事項	229
	(6) スケジュール設定後の注意事項	230
5.8.3	HFRR コピー用差分スナップショットの自動作成	230
	(1) HFRR コピー用差分スナップショット自動作成の動作	230
	(2) HFRR コピー用差分スナップショットのマウント・公開の動作	231
	(3) HFRR コピー用差分スナップショットを自動作成する場合の注意事項	231
5.9	Hitachi File Remote Replicator について	232
5.9.1	Hitachi File Remote Replicator とは	232
5.9.2	Hitachi File Remote Replicator でできること	233
	(1) データ保全性の強化	233
	(2) サイトの切り替え	233
	(3) ストレージ資源の有効利用	234
5.9.3	ボリューム構成	234
5.9.4	セカンダリーサイトの最新差分スナップショット公開	236
5.9.5	サイト間でのデータコピーの仕組み	237
	(1) 全コピーの処理の概略	238
	(2) 差分コピーの処理の概略	238
5.9.6	使用上の注意事項	239
5.10	Hitachi File Remote Replicator を使用する場合の運用設計	239
5.10.1	ファイルシステムの運用設計	239
5.10.2	差分格納デバイスの運用設計	239
	(1) セカンダリーファイルシステムの差分格納デバイスの設計	239
	(2) プライマリーファイルシステムの差分格納デバイスの設計	240
5.10.3	Hitachi File Remote Replicator の運用設計	241
	(1) HFRR ベア名の検討	242
	(2) コピー対象の差分スナップショットとコピー時間帯の検討	242
	(3) セカンダリーサイトでのファイル共有作成のための検討	242
5.10.4	運用上の注意事項	243
	(1) ファイルシステムの違いに関係なく考慮すること	243
	(2) WORM 対応ファイルシステムの場合に考慮すること	244
6.	HCP と連携して運用を開始する前に	247
6.1	マイグレーションを管理するための機能	248
6.1.1	ファイルシステムとネームスペースの対応	248
6.1.2	ファイルのスタブ化	248
6.1.3	データ転送前後の内部処理	249
6.1.4	HVFP/HDI へのリコール	250
6.1.5	バージョン管理を利用したファイルの復元	251
6.2	HCP と連携する前に確認すること	252
6.2.1	HVFP/HDI から HCP へアクセスするためのアカウント	256

(1) HCP のバージョンが 5.0 以降の場合.....	256
(2) HCP のバージョンが 04-10 以前の場合.....	256
6.2.2 マイグレート先のネームスペース.....	257
6.2.3 ほかの HVFP/HDI からマイグレートされた HCP のデータを読み取り専用で公開するために.....	257
6.2.4 マイグレートされた HCP のデータをほかの HVFP/HDI からエンドユーザーごとに使用できるようにするために.....	258
(1) マイグレートされた HCP のデータをほかの HVFP/HDI からエンドユーザーごとに使用できるようにする場合の注意事項.....	259
(2) マイグレートされた HCP のデータをほかの HVFP/HDI からエンドユーザーごとに使用できるようにするために必要な作業.....	262
6.2.5 HCP にマイグレートしたデータを使用して HVFP/HDI を回復するために.....	263
7. Hitachi File Services Manager のインストールと環境設定.....	265
7.1 Hitachi File Services Manager をインストール・アンインストールする.....	266
7.1.1 Hitachi File Services Manager を新規インストールする.....	266
7.1.2 Hitachi File Services Manager をアップグレード・上書きインストールする.....	269
7.1.3 Hitachi NAS Manager から Hitachi File Services Manager にアップグレードインストールする.....	272
7.1.4 Hitachi File Services Manager をアンインストールする.....	275
(1) アンインストールする前に.....	275
(2) アンインストールの実行.....	276
7.1.5 Hitachi File Services Manager をインストールするときの前提条件.....	277
7.2 Hitachi File Services Manager をインストール・アンインストールする（管理サーバをクラスタ構成で運用する場合）.....	279
7.2.1 Hitachi File Services Manager を新規インストールする（管理サーバをクラスタ構成で運用する場合）.....	280
(1) 管理サーバをクラスタ構成にする.....	280
(2) 新規インストールする前に.....	280
(3) 管理サーバの実行系ノードでの新規インストール.....	280
(4) 管理サーバの待機系ノードでの新規インストール.....	284
7.2.2 Hitachi File Services Manager をアップグレード・上書きインストールする（管理サーバをクラスタ構成で運用する場合）.....	286
(1) 管理サーバの実行系ノードでのアップグレード・上書きインストール.....	286
(2) 管理サーバの待機系ノードでのアップグレード・上書きインストール.....	287
7.2.3 Hitachi File Services Manager を新規・アップグレード・上書きインストールする（Hitachi Command Suite 製品をクラスタ構成で運用している場合）.....	288
7.2.4 Hitachi File Services Manager をアンインストールする（管理サーバをクラスタ構成で運用する場合）.....	291
7.3 Hitachi File Services Manager を起動・停止する.....	292
7.3.1 常駐プロセス一覧.....	293
7.3.2 Hitachi File Services Manager を起動する.....	293
(1) Windows のメニューから実行する場合.....	293
(2) コマンドを使用する場合.....	293
7.3.3 Hitachi File Services Manager を停止する.....	293
(1) Windows のメニューから実行する場合.....	294
(2) コマンドを使用する場合.....	294
7.3.4 Hitachi File Services Manager の稼働状態を確認する.....	294
(1) Windows のメニューから実行する場合.....	294
(2) コマンドを使用する場合.....	295
7.4 システム管理者のアカウントを管理する.....	295
7.4.1 システム管理者のアカウントに関するセキュリティを設定する.....	296
(1) パスワードの条件を設定する.....	297
(2) アカウントの自動ロックに関して設定する.....	298
7.4.2 System アカウントのロックに関して設定する.....	298
7.4.3 システム管理者のアカウントのロックを解除する.....	299
7.4.4 LDAP サーバで外部認証する.....	300

(1) データ構造と認証方法の確認.....	301
(2) exauth.properties ファイルの設定（認証方式が LDAP の場合）.....	303
(3) 情報検索用のユーザーアカウントの登録（認証方式が LDAP の場合）.....	308
(4) 外部認証サーバおよび外部認可サーバとの接続確認（認証方式が LDAP の場合）.....	310
7.4.5 RADIUS サーバで外部認証する.....	311
(1) exauth.properties ファイルの設定（認証方式が RADIUS の場合）.....	312
(2) 情報検索用のユーザーアカウントの登録（認証方式が RADIUS の場合）.....	318
(3) 共有秘密鍵の設定.....	319
(4) 外部認証サーバおよび外部認可サーバとの接続確認（認証方式が RADIUS の場合）.....	320
7.4.6 KDC サーバで外部認証する.....	321
(1) exauth.properties ファイルの設定（認証方式が Kerberos の場合）.....	322
(2) 情報検索用のユーザーアカウントの登録（認証方式が Kerberos の場合）.....	326
(3) 外部認証サーバおよび外部認可サーバとの接続確認（認証方式が Kerberos の場合）.....	328
(4) Kerberos 認証に使用できる暗号タイプ.....	329
7.4.7 Device Manager に接続してユーザーアカウントを管理する.....	330
(1) バージョン 8.0 以降の Device Manager がインストールされている管理サーバにインストールしたとき.....	330
(2) Device Manager とは別のマシンにインストールしたとき.....	330
7.4.8 Hitachi Command Suite 共通コンポーネントのセキュリティを設定する（LDAP サーバとの通信）.....	331
(1) LDAP サーバの証明書の入手.....	331
(2) トラストストアファイルへの証明書のインポート.....	332
7.5 Hitachi File Services Manager の環境を設定する.....	333
7.5.1 ログファイルの設定を変更する.....	333
7.5.2 Hitachi File Services Manager の GUI で Virtual Server を削除する際の動作モードを設定する.....	335
7.5.3 ファイルスナップショット機能の情報更新の設定を変更する.....	335
7.5.4 ライセンスの情報更新の設定を変更する.....	336
7.5.5 Hitachi Command Suite 共通コンポーネントのポート番号を変更する.....	337
7.5.6 SSL を設定する.....	339
7.5.7 管理サーバとノードの通信に必要な SSL の証明書をインポートする.....	339
7.5.8 警告バナーの設定.....	339
(1) メッセージファイルの作成.....	340
(2) メッセージの登録.....	340
(3) メッセージの削除.....	341
7.5.9 Hitachi File Services Manager の監査ログの採取と確認.....	341
(1) Hitachi File Services Manager の監査ログの採取を設定する.....	342
(2) Hitachi File Services Manager の監査ログを確認する.....	343
7.6 管理サーバのメンテナンス.....	345
7.6.1 管理サーバのデータベースをバックアップ・リストアする.....	345
(1) データベースをバックアップする.....	345
(2) データベースをリストアする.....	347
7.6.2 管理サーバを非クラスタ構成からクラスタ構成に移行する.....	349
(1) クラスタ構成に移行する前に.....	349
(2) 管理サーバの実行系ノードでの設定.....	349
(3) 管理サーバの待機系ノードでの設定.....	353
7.6.3 管理サーバのデータベースを移行する.....	355
(1) データベースを移行する前に.....	355
(2) 移行元サーバでのデータベースのエクスポート.....	356
(3) 移行先サーバでのデータベースのインポート.....	357
7.6.4 管理サーバのホスト名または IP アドレスを変更する.....	359
7.6.5 管理サーバの時刻を調整する.....	362
7.6.6 管理サーバのネットワークを切断する.....	362
7.6.7 JDK を変更する.....	363
付録 A Advanced ACL タイプのファイルシステムへの移行後に作成される ACL.....	365
A.1 Advanced ACL タイプのファイルシステムへの移行後に作成される ACL.....	366

付録 B ノードの Power ランプスイッチの操作方法.....	369
B.1 OS の起動.....	370
B.2 OS の強制停止.....	370
付録 C ノード上のポートの配置.....	371
C.1 ポートの配置.....	372
付録 D 外部サーバやサービスの IPv6 の対応状況.....	375
D.1 IPv6 で利用できる外部サーバやサービスの一覧.....	376
付録 E バックアップおよびリストア対象となるディレクトリやファイルの属性情報.....	377
E.1 バックアップされる属性情報.....	378
E.2 リストアされる属性情報.....	379
付録 F NFS クライアントから共有内の差分スナップショットのデータをディレクトリ単位でコピーする 方法.....	381
F.1 操作例 1 (find コマンドおよび cpio コマンドを使用した例)	382
F.2 操作例 2 (tar コマンドを使用した例)	382
付録 G 障害に備えて予備のシングルノード構成の HVFP を使用したシステムを構築する方法.....	383
G.1 事前の準備と注意事項.....	384
G.2 予備のシングルノード構成の HVFP を使用したシステムを構築する.....	385
G.3 障害が発生したときに予備の HVFP で運用を再開する.....	387
付録 H 略語一覧.....	389
H.1 HVFP/HDI のマニュアルで使用している略語.....	390
用語解説.....	395
索引.....	401

目次

図 1-1 HVFP のシステムの概要.....	32
図 1-2 複数のファイルサーバの運用の集約.....	35
図 1-3 ストレージシステムを共有した HVFP と HCP の連携.....	36
図 1-4 ネットワークを介した HVFP/HDI と HCP の連携.....	37
図 2-1 クラスタ構成で NDMP 機能を使用する場合のハードウェア構成例.....	44
図 2-2 HVFP/HDI のネットワーク構成例（Virtual Server を使用していない場合）.....	45
図 2-3 BMC ポートの接続構成.....	46
図 2-4 単一のワークグループに属しているネットワークの例.....	49
図 2-5 複数のワークグループに属しているネットワークの例.....	49
図 2-6 単一の NT ドメインに属しているネットワークの例.....	50
図 2-7 ノードとプライマリドメインコントローラーが同じサブネットにあるネットワークの例（NT ドメイン構成）.....	51
図 2-8 ノードとプライマリドメインコントローラーが別のサブネットにあるネットワークの例（NT ドメイン構成）.....	51
図 2-9 ノードとドメインコントローラーが同じサブネットにあるネットワークの例（Active Directory ドメイン構成）.....	52
図 2-10 複数のポートで CIFS サービスを利用するネットワークの例.....	53
図 2-11 HVFP/HDI で推奨する二段階リンク結合の構成例.....	55
図 2-12 二段階リンク結合を利用した場合のネットワークの構成例（正常運用時）.....	56
図 2-13 二段階リンク結合を利用した場合のネットワークの構成例（リンク障害発生時）.....	57
図 2-14 二段階リンク結合を利用した場合のネットワークの構成例（ハードウェア障害発生時）.....	58
図 2-15 VLAN を使用した場合のネットワークの構成例.....	60
図 2-16 ストレージシステムを共有して HVFP と HCP を連携するときのシステム構成例.....	63
図 2-17 ネットワークを介して HVFP と HCP を連携するときのシステム構成例.....	64
図 4-1 HVFP/HDI のクラスタ構成.....	102
図 4-2 クライアントが利用するサービスの流れの例（フェールオーバー時）.....	103
図 4-3 ルートドメインに参加している場合.....	105
図 4-4 子のドメインに参加し、フォレスト間に信頼関係がある場合.....	106
図 4-5 子のドメインに参加し、フォレスト間に信頼関係がない場合.....	106
図 4-6 フォレスト間の信頼関係が片方向の場合.....	107
図 4-7 RID 方式によるユーザー ID やグループ ID の割り当て例.....	111
図 4-8 ユーザー ID およびグループ ID の見積もり例.....	112
図 4-9 ユーザー ID およびグループ ID の設定例.....	113
図 4-10 HVFP/HDI の暗号化機能の対象.....	116
図 4-11 ファイルシステム使用量に関する警告が通知される契機（ブロック使用量を監視する場合）.....	118
図 4-12 ファイルシステム使用量に関する警告が通知される契機（inode 使用量を監視する場合）.....	119
図 4-13 ストライピング機能の運用例.....	121

図 4-14 ストライピング機能の運用例（ファイルシステム拡張時）	122
図 4-15 移行後にユーザーのアクセス権の権限が小さくなる場合の例（その 1）	127
図 4-16 移行後にユーザーのアクセス権の権限が小さくなる場合の例（その 2）	128
図 4-17 WORM ファイルの動作	131
図 4-18 階層ファイルシステムの構造と動作	133
図 4-19 サブツリー Quota の管理	137
図 4-20 ファイルシステムごとの Quota の設定例	143
図 4-21 マウントポイント直下のディレクトリへのサブツリー Quota の設定例	144
図 4-22 Quota 管理の運用例	146
図 4-23 リアルタイムスキャンの性能改善フローチャート（スキャンタイムアウトが頻発している場合）	162
図 4-24 リアルタイムスキャンの性能改善フローチャート（スキャンサーバとの接続エラーが頻発している場合）	163
図 4-25 リアルタイムスキャンの性能改善フローチャート（ファイルの操作に時間が掛かる場合）	163
図 4-26 ほかのファイルサーバからのインポートの概要	169
図 4-27 ほかのファイルサーバからデータをインポートするときのシステム構成例	170
図 5-1 NDMP 機能の概要	179
図 5-2 バックアップの履歴情報	183
図 5-3 1つの NDMP ポリシーで運用した場合の増分バックアップ	184
図 5-4 シングルノード構成の場合の差分格納デバイス	190
図 5-5 自動作成の上限数まで作成・確保できる場合の予約世代数の内訳	194
図 5-6 自動作成の上限数まで作成・確保できない場合の予約世代数の内訳	194
図 5-7 自動作成された差分スナップショットが削除される条件（上限数をファイルシステム全体で管理する場合）	195
図 5-8 自動作成された差分スナップショットが削除される条件（上限数を作成間隔ごとに管理する場合）	196
図 5-9 想定するシステム構成	200
図 5-10 差分スナップショットの運用例（HOME ファイルシステム）	201
図 5-11 差分スナップショットの運用例（DOCUMENT ファイルシステム）	202
図 5-12 スケジュールの設定内容	204
図 5-13 運用開始後のシステム管理者の作業	205
図 5-14 クライアントから差分スナップショットへのアクセス（HOME ファイルシステム）	207
図 5-15 障害の検知方法の例	209
図 5-16 差分格納デバイスの使用量とシステムの動作の関係	219
図 5-17 差分スナップショットが公開されている共有内のディレクトリ構造	223
図 5-18 Hitachi File Remote Replicator の概要	232
図 5-19 データ安全性の強化	233
図 5-20 サイトの切り替え	234
図 5-21 ボリューム構成	235
図 5-22 HFRR ペアの構成	236
図 5-23 セカンダリーサイトの最新差分スナップショット公開の概略	237
図 5-24 全コピーの処理の概略	238
図 5-25 差分コピーの処理の概略	238
図 6-1 ファイルシステムとテナントおよびネームスペースの対応	248
図 6-2 ファイルのスタブ化	249
図 6-3 HCP のレプリカのシステムによるリコール処理の継続	251
図 6-4 バージョン管理を利用したファイルの復元	252
図 6-5 マイグレートされた HCP のデータをほかの HVFP/HDI からエンドユーザーごとに使用する場合のデータの 流れ	259
図 7-1 [Hitachi File Services Manager のインストールへようこそ（新規）] ダイアログ	266
図 7-2 [インストールフォルダの設定] ダイアログ	267
図 7-3 [Hitachi File Services Manager のデータベースファイル格納先の設定] ダイアログ	268
図 7-4 [Hitachi File Services Manager のインストールへようこそ（上書き）] ダイアログ	270
図 7-5 [Hitachi File Services Manager のデータベースファイル格納先の設定] ダイアログ（新規インストール以外の 場合）	271

図 7-6 [Hitachi File Services Manager のインストールへようこそ (アップグレード)] ダイアログ	273
図 7-7 [Hitachi File Services Manager のデータベースファイル格納先の設定] ダイアログ (新規インストール以外の 場合)	274
図 7-8 [Hitachi File Services Manager のアンインストール] ダイアログ	276
図 7-9 階層構造モデルの例	302
図 7-10 フラットモデルの例	302
図 C-1 ポートの配置の例 (VFP110 または VFP200N の拡張スロット 1 に GbE カードを搭載しているとき)	372
図 C-2 ポートの配置の例 (VFP110 または VFP200N の拡張スロット 1 に 10GbE カードを搭載しているとき)	372
図 C-3 ポートの配置の例 (VFP600N の拡張スロット 1 と 2 に GbE カードを搭載しているとき)	372
図 C-4 ポートの配置の例 (VFP600N の拡張スロット 1 と 2 に 10GbE カードを搭載しているとき)	373
図 G-1 予備のシングルノード構成の HVFP を使用したシステムの構成	385

表目次

表 はじめに -1 HVFP のマニュアル体系.....	25
表 はじめに -2 HDI のマニュアル体系.....	26
表 2-1 HVFP のライセンス（クラスタ構成の場合）.....	60
表 2-2 HVFP のライセンス（シングルノード構成でストレージシステムを使用しない場合）.....	61
表 2-3 HVFP のライセンス（シングルノード構成でストレージシステムを使用する場合）.....	61
表 2-4 HDI のライセンス.....	62
表 3-1 HVFP/HDI で必要な外部サーバ.....	66
表 3-2 管理サーバのマシン要件.....	68
表 3-3 Hitachi File Services Manager に必要な仮想メモリー容量.....	69
表 3-4 Hitachi Command Suite 製品の仮想メモリーの推奨値.....	70
表 3-5 クラスタ構成で管理サーバを運用する場合の適用 OS とクラスタソフトウェア.....	71
表 3-6 Windows のスタートメニュー（Windows 8 または Windows Server 2012 の場合はスタート画面のアプリ一覧）からの操作とメニュー項目.....	71
表 3-7 管理コンソールのマシン要件.....	72
表 3-8 Internet Explorer の設定.....	75
表 3-9 Firefox の設定.....	76
表 3-10 HVFP/HDI の specific-trap.....	90
表 3-11 リアルタイムスキャンの性能改善に関する設定項目（Symantec 社のスキャンソフトを使用する場合）.....	93
表 3-12 Hitachi Server Protect Agent のセットアップに必要な情報.....	93
表 3-13 リアルタイムスキャンの性能改善に関する設定項目（マカフィー社のスキャンソフトを使用する場合）.....	95
表 4-1 ファイルシステム使用量に関する警告が通知される契機.....	119
表 4-2 Advanced ACL タイプと Classic ACL タイプのファイルシステムの相違.....	124
表 4-3 表示されるアクセス権の詳細.....	125
表 4-4 階層ファイルシステムでの LU と階層の関係.....	133
表 4-5 Quota 管理で設定する情報.....	138
表 4-6 ソフトリミットや猶予期間の超過を検知した場合に通知される情報.....	139
表 4-7 Quota を設定したユーザーの例.....	141
表 4-8 リアルタイムスキャンの性能低下時に確認する必要がある情報.....	157
表 4-9 レポート情報ファイル（antivirus_report.csv）に出力される内容.....	158
表 4-10 エラーが発生した場合にレポート情報ファイルの付加情報（ErrorInfo）に出力される内容.....	159
表 4-11 ウイルス感染ファイルを検出した場合にレポート情報ファイルの付加情報（Action）に出力される内容.....	159
表 4-12 ユーザー統計情報ファイル（antivirus_stat.csv）に出力される内容.....	160
表 4-13 CPU に関する MIB オブジェクト.....	168
表 4-14 メモリーに関する MIB オブジェクト.....	168
表 4-15 ネットワークに関する MIB オブジェクト.....	168
表 5-1 バックアップ管理ソフトウェアで提供されている機能と NDMP 機能での利用可否.....	186
表 5-2 同じパス名のファイルが存在する場合のリストアの可否.....	187

表 5-3 データ集約されたファイルシステムをバックアップ、リストアする場合の注意事項.....	188
表 5-4 チャンクサイズによるファイルシステムおよび差分格納デバイス容量の拡張上限.....	190
表 5-5 バックグラウンド処理に掛かる時間の目安（システム負荷が低く、I/O 競合がない状態の場合）.....	197
表 5-6 差分格納デバイスの設定内容（クラスタ構成時の HOME ファイルシステム）.....	201
表 5-7 自動作成スケジュールの設定内容（クラスタ構成時の HOME ファイルシステム）.....	202
表 5-8 差分格納デバイスの設定内容（DOCUMENT ファイルシステム）.....	203
表 5-9 差分スナップショットの設定内容（シングルノード構成時の HOME ファイルシステム）.....	204
表 5-10 デフォルトのチャンクサイズ.....	211
表 5-11 自動作成された差分スナップショットのマウントおよびファイル共有の設定例.....	223
表 5-12 自動作成処理が開始された時点で削除対象になる差分スナップショットの例（上限数をファイルシステム全体で管理する場合）.....	225
表 5-13 自動作成処理が開始された時点で削除対象になる差分スナップショットの例（上限数を作成間隔ごとに管理する場合）.....	225
表 5-14 自動マウント処理が開始された時点でアンマウント対象になる差分スナップショットの例（上限数をファイルシステム全体で管理する場合）.....	226
表 5-15 自動マウント処理が開始された時点でアンマウント対象になる差分スナップショットの例（上限数を作成間隔ごとに管理する場合）.....	226
表 5-16 HFRR ペア数の上限（クラスタ構成の場合）.....	241
表 5-17 HFRR ペア数の上限（シングルノード構成の場合）.....	241
表 5-18 HFRR ペア数の上限（Virtual Server の場合）.....	241
表 5-19 セカンダリーサイトでのファイル共有作成のための検討項目と条件.....	242
表 6-1 タスクの処理状況と、GUI に表示されるステータスや処理時間の影響因子との対応.....	250
表 7-1 インストールするコンポーネントと必要な空き容量.....	277
表 7-2 HBase Storage Mgmt Common Service をリソースとして登録するための設定.....	283
表 7-3 HBase Storage Mgmt Web Service をリソースとして登録するための設定.....	283
表 7-4 HiRDB をリソースとして登録するための設定.....	283
表 7-5 Hitachi File Services Manager および Hitachi Command Suite 共通コンポーネントの常駐プロセス.....	293
表 7-6 security.conf ファイルで指定するパスワードの条件.....	297
表 7-7 security.conf ファイルで指定するアカウントの自動ロックに関する設定.....	298
表 7-8 user.conf ファイルのプロパティ（System アカウントのロックに関する設定の変更）.....	299
表 7-9 LDAP サーバで認証する場合の exauth.properties ファイルの設定項目（共通項目）.....	303
表 7-10 LDAP サーバで認証する場合の exauth.properties ファイルの設定項目（外部認証サーバの情報を直接指定するとき）.....	304
表 7-11 LDAP サーバで認証する場合の exauth.properties ファイルの設定項目（外部認証サーバと StartTLS で通信するとき）.....	306
表 7-12 LDAP サーバで認証する場合の exauth.properties ファイルの設定項目（外部認証サーバの情報を DNS サーバに照会するとき）.....	306
表 7-13 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目（共通項目）.....	313
表 7-14 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目（外部認証サーバの設定）.....	313
表 7-15 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目（外部認可サーバの共通設定）.....	314
表 7-16 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目（外部認可サーバの情報を直接指定するとき）.....	315
表 7-17 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目（外部認可サーバと StartTLS で通信するとき）.....	316
表 7-18 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目（外部認可サーバの情報を DNS サーバに照会するとき）.....	316
表 7-19 KDC サーバで認証する場合の exauth.properties ファイルの設定項目（共通項目）.....	322
表 7-20 KDC サーバで認証する場合の exauth.properties ファイルの設定項目（外部認証サーバの情報を直接指定するとき）.....	323
表 7-21 KDC サーバで認証する場合の exauth.properties ファイルの設定項目（外部認証サーバの情報を DNS サーバに照会するとき）.....	324

表 7-22 KDC サーバで認証する場合の exauth.properties ファイルの設定項目（外部認可サーバの設定）	324
表 7-23 KDC サーバで認証する場合の exauth.properties ファイルの設定項目（外部認可サーバと StartTLS で通信するとき）	325
表 7-24 user.properties ファイルのプロパティ（ログファイルの設定）	334
表 7-25 user.properties ファイルのプロパティ（動作モードの設定）	335
表 7-26 user.properties ファイルのプロパティ（ファイルスナップショット機能の情報更新の設定変更）	336
表 7-27 user.properties ファイルのプロパティ（ライセンスの情報更新の設定変更）	337
表 7-28 Hitachi Command Suite 共通コンポーネントの変更できるポート番号	337
表 7-29 Hitachi Command Suite 共通コンポーネントのポート番号設定ファイル	338
表 7-30 Hitachi File Services Manager で出力できる監査ログの種類	341
表 7-31 Hitachi File Services Manager の監査ログとして出力される監査事象	342
表 7-32 auditlog.conf ファイルに設定する項目	342
表 7-33 監査事象の重要度（Severity）とイベントログの種類	343
表 7-34 メッセージ部に出力される情報	344
表 7-35 HBase Storage Mgmt Common Service をリソースとして登録するための設定	352
表 7-36 HBase Storage Mgmt Web Service をリソースとして登録するための設定	352
表 7-37 HiRDB をリソースとして登録するための設定	352
表 7-38 ホスト名を変更するための項目（SSL を設定していない場合）	360
表 7-39 ホスト名を変更するための項目（SSL を設定している場合）	360
表 7-40 ホスト名を変更するための項目（pdsys ファイルおよび def_pdsys ファイル）	360
表 7-41 ホスト名を変更するための項目（pdutysys ファイルおよび def_pdutysys ファイル）	361
表 7-42 ホスト名を変更するための項目（HiRDB.ini ファイル）	361
表 7-43 ホスト名を変更するための項目（cluster.conf ファイル）	361
表 7-44 ホスト名を変更するための項目（pdsys ファイルおよび def_pdsys ファイル）	363
表 7-45 ホスト名を変更するための項目（pdutysys ファイルおよび def_pdutysys ファイル）	363
表 7-46 ホスト名を変更するための項目（HiRDB.ini ファイル）	363
表 A-1 ファイルシステム移行前後のアクセス権の対応	366
表 A-2 移行前のアクセス権の差分と移行後のアクセス権の対応	367
表 C-1 ポートの配置	373
表 D-1 外部サーバの IPv6 対応状況	376
表 D-2 HVFP/HDI が提供するサービスや機能の IPv6 対応状況	376
表 E-1 メディアにバックアップされる Quota 情報	378
表 E-2 メディアにバックアップされるディレクトリおよびファイルの属性	378
表 E-3 ACL タイプが異なる場合のリストア結果（WORM 機能を使用していないファイルシステムのバックアップデータ）	379
表 E-4 ACL タイプが異なる場合のリストア結果（WORM 対応ファイルシステムのバックアップデータ）	379



はじめに

このマニュアルは、Hitachi Virtual File Platform / Hitachi Data Ingestor (HVFP/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、システムのセットアップ方法などについて説明したものです。

- 対象読者
- マニュアルの構成
- マニュアル体系
- 関連マニュアル
- このマニュアルでの表記
- このマニュアルで使用する記号
- このマニュアルで使用する構文要素
- コマンドの書式で使用する記号
- KB (キロバイト) などの単位表記について

対象読者

このマニュアルは、HVFP/HDI を運用・管理する方（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、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. Hitachi Virtual File Platform / Hitachi Data Ingestor の概要	HVFP/HDI の特長や機能概要について説明しています。
2. システム構成	HVFP/HDI のハードウェア、ネットワークおよびプログラムの構成について説明しています。
3. 外部サーバの環境設定	HVFP/HDI を運用・管理するために必要な外部サーバの環境設定について説明しています。
4. 運用を開始する前に	HVFP/HDI の運用を開始するに当たり、システム管理者が理解または考慮する必要があることについて説明しています。
5. HVFP/HDI のバックアップ運用	HVFP/HDI のバックアップ運用に関して、システム管理者が理解または考慮する必要があることについて説明しています。
6. HCP と連携して運用を開始する前に	HCP と連携して HVFP/HDI の運用を開始するに当たり、システム管理者が理解または考慮する必要があることについて説明しています。
7. Hitachi File Services Manager のインストールと環境設定	管理サーバに Hitachi File Services Manager をインストールしたり、環境設定を実施したりするときの操作手順について説明しています。
A. Advanced ACL タイプのファイルシステムへの移行後に作成される ACL	Classic ACL タイプのファイルシステムから Advanced ACL タイプのファイルシステムに移行する際に作成される ACL について説明しています。
B. ノードの Power ランプスイッチの操作方法	保守作業時に HVFP/HDI のノードの Power ランプスイッチを操作して、OS を起動または停止する方法について説明しています。
C. ノード上のポートの配置	クラスタ構成のノード上のポートの配置について説明しています。
D. 外部サーバやサービスの IPv6 の対応状況	HVFP/HDI で使用する外部サーバや、HVFP/HDI が提供するサービスなどの IPv6 の対応状況について説明しています。

章	内容
E. バックアップおよびリストア対象となるディレクトリやファイルの属性情報	メディアにバックアップされる、または、メディアからリストアされるディレクトリやファイルの属性情報について説明しています。
F. NFS クライアントから共有内の差分スナップショットのデータをディレクトリ単位でコピーする方法	NFS クライアントから、共有内の差分スナップショットのデータをディレクトリ単位でコピーする方法について説明しています。
G. 障害に備えて予備のシングルノード構成の HVFP を使用したシステムを構築する方法	予備のシングルノード構成の HVFP を用意し、障害が発生したときに予備の HVFP でファイルシステムの運用を再開できるようにシステムを構築するための方法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。
用語解説	HVFP/HDI のマニュアルで使用している用語の意味を説明しています。

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 (このマニュアル)	HVFP を運用するために、最初にお読みいただくマニュアルです。 HVFP の運用を開始する前に理解または検討しておいていただきたいことや、外部サーバの環境設定などについて説明しています。
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。 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。

マニュアル名	内容
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	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、事前を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。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 (このマニュアル)	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。
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	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、事前を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。

関連マニュアル

このマニュアルの関連マニュアルを次に示します。必要に応じてお読みください。

Hitachi Command Suite 製品のマニュアル

- Hitachi Command Suite Software ユーザーズガイド
- Hitachi Command Suite Software CLI リファレンスガイド
- Hitachi Command Suite Software メッセージガイド
- Hitachi Command Suite Software インストールガイド
- Hitachi Command Suite Software システム構成ガイド

- Hitachi Command Suite Replication Manager Software システム構成ガイド
- Hitachi Command Suite Tuning Manager - Agent for RAID
- Hitachi Command Suite Tuning Manager - Storage Mapping Agent
- Hitachi Command Suite Tuning Manager - Agent for SAN Switch
- Hitachi Command Suite Tuning Manager - Agent for Network Attached Storage

Virtual Storage Platform 関連のマニュアル

- Hitachi Virtual File Platform エンタープライズアレイ機能連携ユーザーズガイド

Universal Storage Platform V/VM 関連のマニュアル

- Hitachi Virtual File Platform エンタープライズアレイ機能連携ユーザーズガイド

HUS VM 関連のマニュアル

- Hitachi Virtual File Platform エンタープライズアレイ機能連携ユーザーズガイド

HUS100 シリーズ関連のマニュアル

- Hitachi Virtual File Platform ミッドレンジアレイ機能連携ユーザーズガイド
- Hitachi Storage Navigator Modular 2 (for GUI) ユーザーズガイド

Hitachi AMS2000 シリーズ関連のマニュアル

- Hitachi Virtual File Platform ミッドレンジアレイ機能連携ユーザーズガイド
- Hitachi Storage Navigator Modular 2 (for GUI) ユーザーズガイド

HCP のマニュアル

- Hitachi Content Platform HVFP/HDI 連携セットアップガイド
- Hitachi Content Platform 運用ガイド

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
ALog ConVerter	ALog ConVerter(R)
Compute Systems Manager	Hitachi Compute Systems Manager
Device Manager	Hitachi Device Manager Software
Dynamic Provisioning	Hitachi Dynamic Provisioning
Dynamic Tiering	Hitachi Dynamic Tiering
File Services Manager	次の製品を区別する必要がない場合の表記です。 <ul style="list-style-type: none"> • Configuration Manager • Hitachi File Services Manager
Firefox	Mozilla Firefox(R)

このマニュアルでの表記	製品名称または意味
Global Link Manager	Hitachi Global Link Manager Software
HCP	Hitachi Content Platform
HDI	Hitachi Data Ingestor
Hitachi AMS2000 シリーズ	Hitachi Adaptable Modular Storage 2000 シリーズ
HUS100 シリーズ	次の製品を区別する必要がない場合の表記です。 <ul style="list-style-type: none"> • Hitachi Unified Storage 150 • Hitachi Unified Storage 130 • Hitachi Unified Storage 110
HUS VM	Hitachi Unified Storage VM
HVFP	Hitachi Virtual File Platform
Internet Explorer	Windows(R) Internet Explorer(R)
OpenLDAP	OpenLDAP 2.x
Replication Manager	Hitachi Replication Manager Software
ShadowImage	次の製品を区別する必要がない場合の表記です。 <ul style="list-style-type: none"> • ShadowImage • ShadowImage in-system replication
Solaris 10	Solaris 10 オペレーティングシステム SPARC プラットフォーム版
Sun Java System Directory Server	Sun Java(TM) System Directory Server 5.2
Tiered Storage Manager	Hitachi Tiered Storage Manager Software
TrueCopy	次の製品を区別する必要がない場合の表記です。 <ul style="list-style-type: none"> • TrueCopy • TrueCopy Asynchronous • TrueCopy Extended Distance • TrueCopy remote replication
Tuning Manager	Hitachi Tuning Manager Software
Universal Storage Platform V/VM	次の製品を区別する必要がない場合の表記です。 <ul style="list-style-type: none"> • Hitachi Universal Storage Platform V • Hitachi Universal Storage Platform VM • Hitachi Universal Storage Platform H20000 • Hitachi Universal Storage Platform H24000
Virtual Storage Platform	次の製品を区別する必要がない場合の表記です。 <ul style="list-style-type: none"> • Hitachi Virtual Storage Platform • Hitachi Virtual Storage Platform VP9500
Windows	Microsoft(R) Windows(R) 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。 <ul style="list-style-type: none"> • Microsoft(R) Windows(R) 7 Enterprise x64 Edition • Microsoft(R) Windows(R) 7 Professional • Microsoft(R) Windows(R) 7 Professional x64 Edition • 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。 <ul style="list-style-type: none"> • 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
Windows Server 2003	次の製品を区別する必要がない場合の表記です。 <ul style="list-style-type: none"> • Microsoft(R) Windows Server(R) 2003, Datacenter Edition Operating System

このマニュアルでの表記	製品名称または意味
	<ul style="list-style-type: none"> Microsoft(R) Windows Server(R) 2003, Enterprise Edition Operating System Microsoft(R) Windows Server(R) 2003, Standard Edition Operating System Microsoft(R) Windows Server(R) 2003, Web Edition Operating System
Windows Server 2003 R2	次の製品を区別する必要がない場合の表記です。 <ul style="list-style-type: none"> Microsoft(R) Windows Server(R) 2003 R2, Datacenter Edition Microsoft(R) Windows Server(R) 2003 R2, Enterprise Edition Microsoft(R) Windows Server(R) 2003 R2, Standard Edition
Windows Server 2008	次の製品を区別する必要がない場合の表記です。 <ul style="list-style-type: none"> Microsoft(R) Windows Server(R) 2008 Datacenter Microsoft(R) Windows Server(R) 2008 Enterprise Microsoft(R) Windows Server(R) 2008 Standard
Windows Server 2008 R2	次の製品を区別する必要がない場合の表記です。 <ul style="list-style-type: none"> Microsoft(R) Windows Server(R) 2008 R2 Datacenter Microsoft(R) Windows Server(R) 2008 R2 Enterprise 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。 <ul style="list-style-type: none"> Microsoft(R) Windows Server(R) 2012 Datacenter Microsoft(R) Windows Server(R) 2012 Standard
Windows Vista	次の製品を区別する必要がない場合の表記です。 <ul style="list-style-type: none"> Microsoft(R) Windows Vista(R) Business Microsoft(R) Windows Vista(R) Enterprise Microsoft(R) Windows Vista(R) Ultimate
Windows XP	Microsoft(R) Windows(R) XP Professional Edition

なお、このマニュアルでは Hitachi File Remote Replicator 固有の処理に関することを指す場合、Hitachi File Remote Replicator を略して HFRR と表記することがあります。

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 または Windows Server 2008 までの Windows 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。 (例) [ファイルシステム] サブウィンドウ [OK] ボタン

記号	意味
	[Enter] キー
< >	可変値であることを示します。 (例) <ホスト名>.<ポート番号> 実際のホスト名が「host0」、ポート番号が「1024」の場合、「host0.1024」と指定することを示します。
[]・[]	「-」の前に示したメニューから、「-」の後ろのメニュー項目を選択することを表します。

このマニュアルで使用する構文要素

このマニュアルで使用する構文要素（設定値やファイル名などに指定できる値）の種類を、次のように定義します。

種類	定義
英大文字	A~Z
英小文字	a~z
英字	A~Z a~z
数字	0~9
英数字	A~Z a~z 0~9

注 すべて半角で指定してください。

コマンドの書式で使用する記号

このマニュアルでは、次に示す記号を使用してコマンドを説明しています。

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

KB（キロバイト）などの単位表記について

1KB（キロバイト）、1MB（メガバイト）、1GB（ギガバイト）、1TB（テラバイト）、1PB（ペタバイト）はそれぞれ1,024バイト、1,024²バイト、1,024³バイト、1,024⁴バイト、1,024⁵バイトです。

Hitachi Virtual File Platform / Hitachi Data Ingestor の概要

この章では、Hitachi Virtual File Platform / Hitachi Data Ingestor (HVFP/HDI) の特長や機能概要について説明します。

- [1.1 Hitachi Virtual File Platform / Hitachi Data Ingestor とは](#)
- [1.2 Hitachi Content Platform との連携](#)

1.1 Hitachi Virtual File Platform / Hitachi Data Ingestor とは

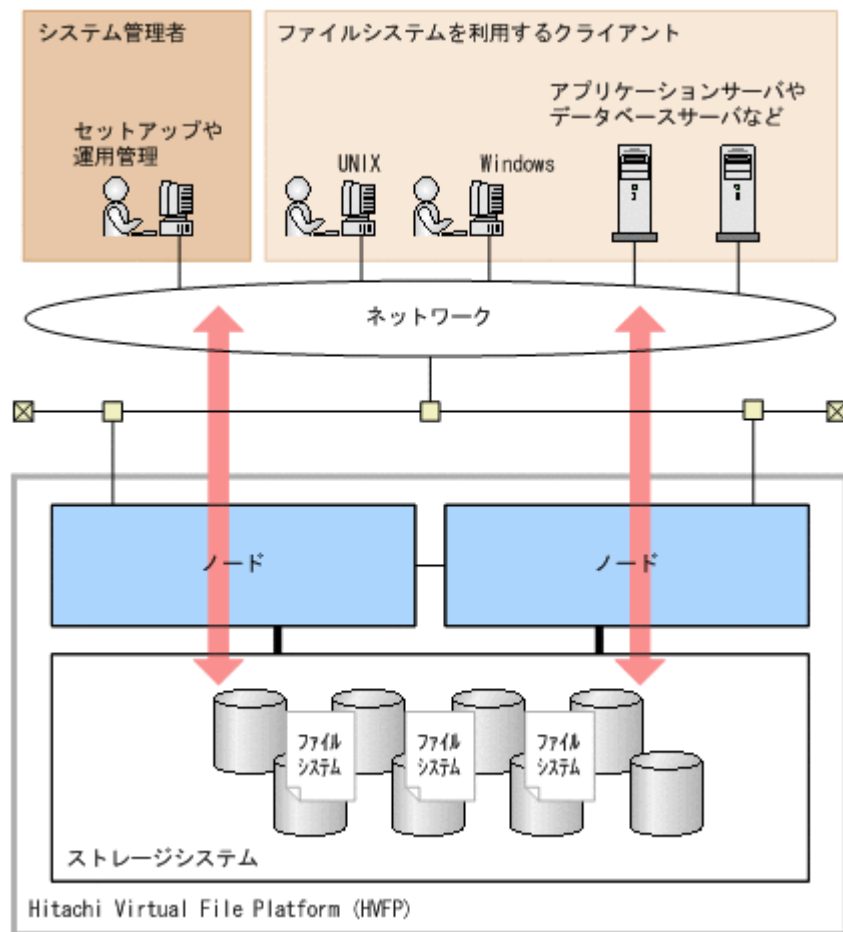
Hitachi Virtual File Platform / Hitachi Data Ingestor (HVFP/HDI) とは、プラットフォームの異なるクライアントがデータを共有するためのサービスを提供するシステムです。ノードと呼ばれるファイルサーバ部分と、データを集約して格納するためのストレージ部分で構成され、ノード上のネットワークポートを介してクライアントにファイルシステムサービスを提供します。

HVFP/HDI のモデルによって、ノードを冗長化するかどうか異なります。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ます。

HVFP/HDI のシステム管理者は、管理コンソールから、システムのセットアップ、運用状況の監視、設定変更、障害監視、データのバックアップやリストアなどを行います。

HVFP の場合のシステムの概要を次の図に示します。

図 1-1 HVFP のシステムの概要



HVFP/HDI の主な特長は次のとおりです。

既存のシステムを生かしたオープンなデータ共有環境の実現

構築済みの LAN 環境を生かして、ストレージシステムでのデータの統合管理を実現できます。また、異種プラットフォーム間でストレージシステム内のデータ共有を実現できます。

効率的で柔軟な容量管理

ストレージシステムの容量仮想化機能を実現する Dynamic Provisioning と連携すると、ストレージシステム上の物理的なボリュームよりも大きな容量を、仮想的なボリュームとしてファ

イルシステムに割り当てることができます。容量が不足する前にシステムを停止することなくディスクを追加できるため、ストレージシステムの使用効率の向上や導入コストの削減を実現できます。また、共有ディレクトリごとに使用できる容量を運用に応じて見直すことで、ファイルシステムに割り当てられたボリュームの空き容量を効率的に利用することもできます。

高可用性の確保（クラスタ構成の場合）

HVFP/HDI では、NFS サービスや CIFS サービスなどを安定して供給するために、2 台のノードでクラスタを構成します。ノードに障害が発生した場合でも、クラスタ内の別のノードにサービスが引き継がれ、サービスの安定供給を実現できます。また、フェールオーバー機能と連携して、ハードウェア、ソフトウェアまたは HVFP/HDI が提供しているサービスのオンラインメンテナンスも実現できます。

安全性の確保

Anti-Virus Enabler を利用してリアルタイムスキャンを実施することで、ファイルシステム内のデータ資産をウイルスから守ります。

コンプライアンスに対応したデータ保管

WORM (Write Once, Read Many) に対応したファイルシステム内のファイルを WORM 化することでデータの改ざんや削除を防ぎ、コンプライアンスに対応した長期間のデータ保管を実現します。

暗号技術を使用したセキュアなデータ保存（シングルノード構成の場合）

シングルノード構成で内蔵ハードディスクからユーザー LU を作成している場合、ファイルシステムで使用するユーザー LU を暗号化することで、情報漏洩のリスクを低減できます（ローカルデータの暗号化）。HVFP/HDI では共通鍵暗号方式 (XTS-AES 暗号、鍵長 256 ビット) を使用します。暗号化には対応するライセンスが必要です。

最適なディスクドライブへのファイル移動（クラスタ構成の場合）

ファイルシステムを階層構成で運用することで、ファイルの種類や利用頻度に応じた最適なディスクドライブにファイルシステム内のファイルを自動で移動できます。

多様なバックアップ運用

データを複製することで、ファイルシステム上で共有している重要なデータ資産を守り、障害に備えることができます。

運用方法は、バックアップデータの取得方法やデータの保管先に合わせて選択できます。

HVFP/HDI で利用できるバックアップ運用には、NDMP 機能、ボリュームレプリケーション連携機能、ファイルスナップショット機能などがあります。

Hitachi Command Suite 製品との連携（クラスタ構成の場合）

Hitachi Command Suite 製品のうち、次の製品と連携できます。

- Device Manager

Device Manager と連携することで、ストレージシステムのボリュームとファイルシステムの対応を一元管理できます。また、Hitachi Command Suite 製品のシングルサインオン機能も利用できます。

- Tuning Manager

ファイルシステムの使用状況や、ノードの OS の性能情報などを参照できます。

ほかのファイルサーバからのインポート

HVFP/HDI 以外のファイルサーバで使用しているファイル共有のデータを HVFP/HDI にインポートできます。複数のファイルサーバのデータを同時にインポートできます。これによって、ファイルサーバの運用を HVFP/HDI に集約できます。

HVFP/HDI では、インポート先のファイルシステムを運用しながら、データをインポートできます。すべてのファイルやディレクトリのインポートが完了していない状態でもクライアントからのアクセスを再開でき、ファイルシステムの運用を停止する時間を短縮できます。

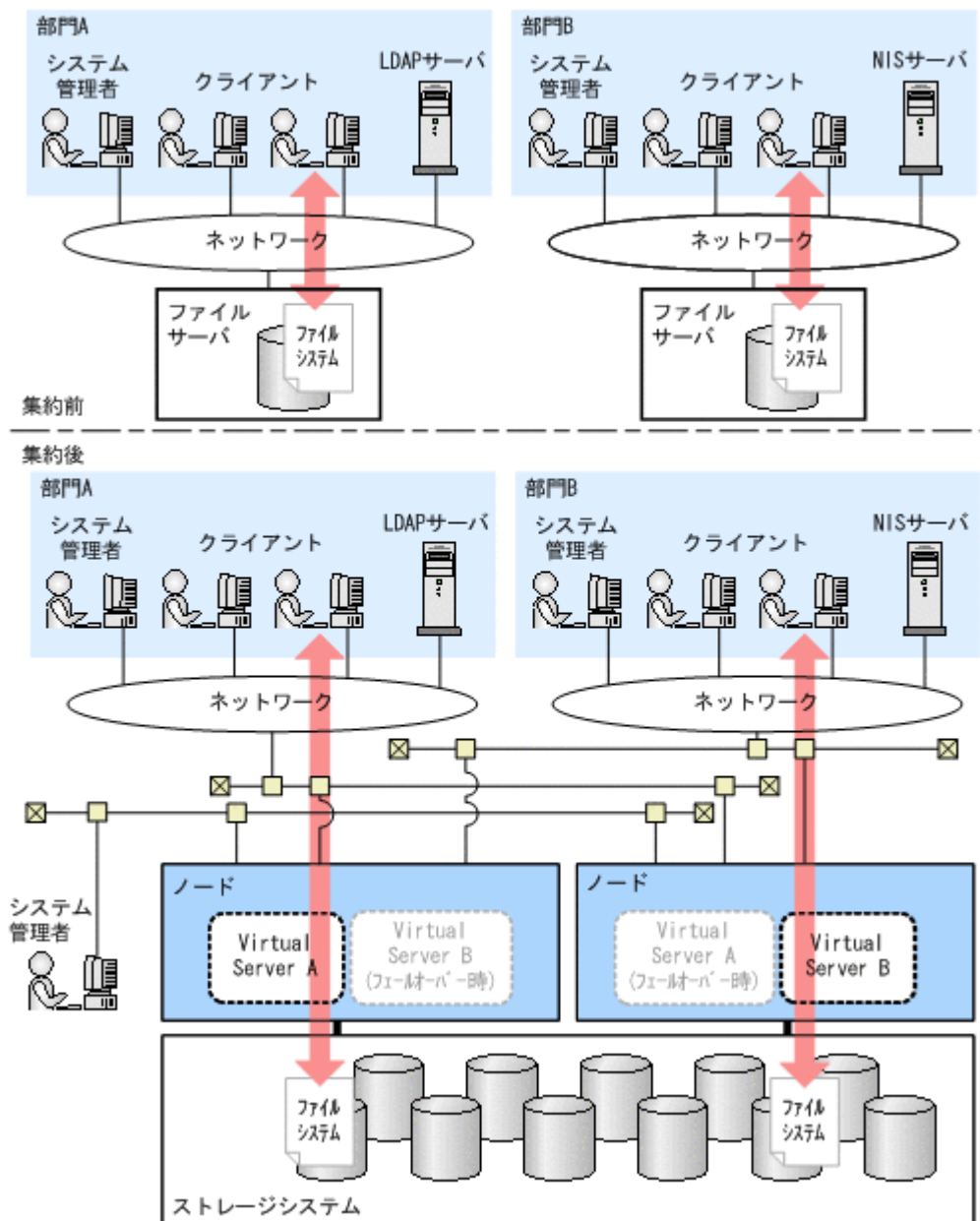
複数のファイルサーバの集約（クラスタ構成の場合）

Virtual Server と呼ばれる複数の仮想サーバを構築することで、異なるファイルサーバで運用されていた複数のシステムを集約して管理できます。HVFP/HDI で Virtual Server を運用するときの特長を次に示します。

- 別々のファイルサーバで運用していたシステムをドメインを分離した状態で集約できるため、ユーザーの認証方式を見直す必要がありません。LDAP サーバや NIS サーバなどの認証サーバは集約したあとも引き続き使用できます。
- システムを集約することで、ネットワークやハードウェアなどの共通の設定を集中管理できます。
- ネットワークやハードウェアに障害が発生すると、障害が発生した Virtual Server はもう一方のノードへ自動的にフェールオーバーするため、サービスを継続しながら障害回復やリプレースなどの保守作業ができます。Virtual Server ごとにフェールオーバーおよびフェールバックができます。

複数のファイルサーバの運用を HVFP/HDI に集約するときの例を次に示します。

図 1-2 複数のファイルサーバの運用の集約



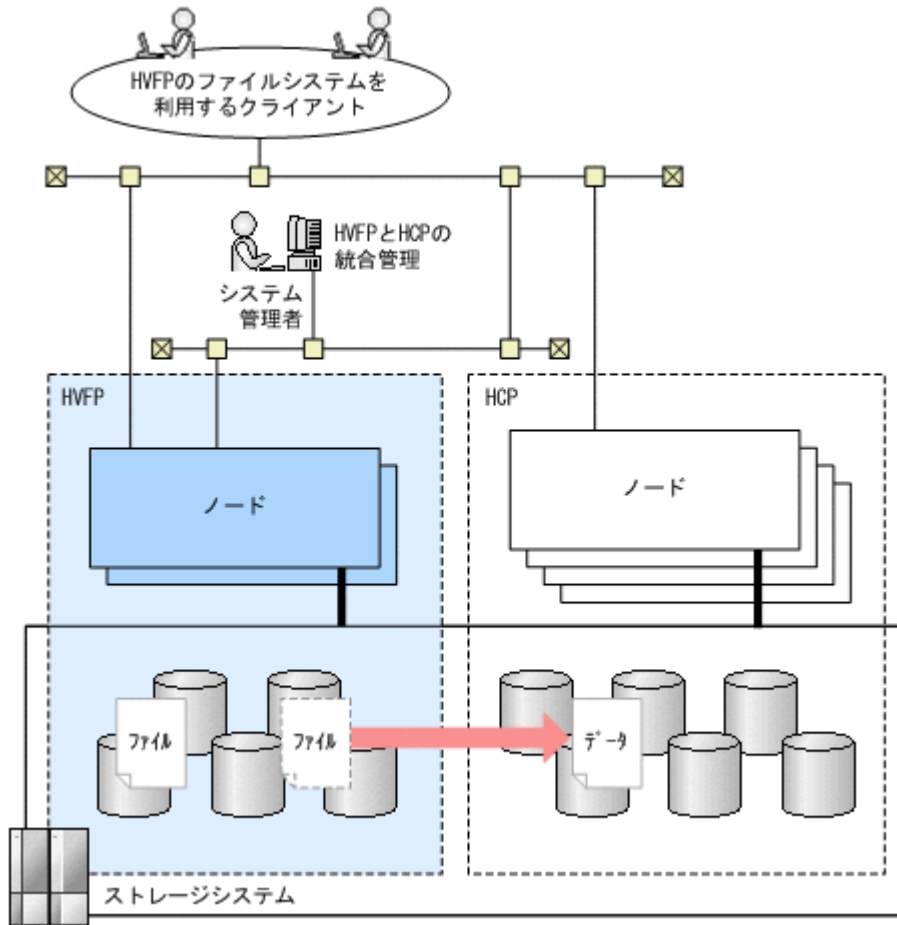
1.2 Hitachi Content Platform との連携

Hitachi Content Platform (HCP) とは、さまざまなシステムで生成された大量のコンテンツをアーカイブして長期的に保管するためのシステムです。容量の拡張性に優れているほか、アーカイブしたデータへの迅速なアクセスを実現します。

HVFP/HDI と HCP が連携することで、高性能なファイルシステムサービスを提供しながら、日々蓄積される大量のデータを効率的に管理できます。

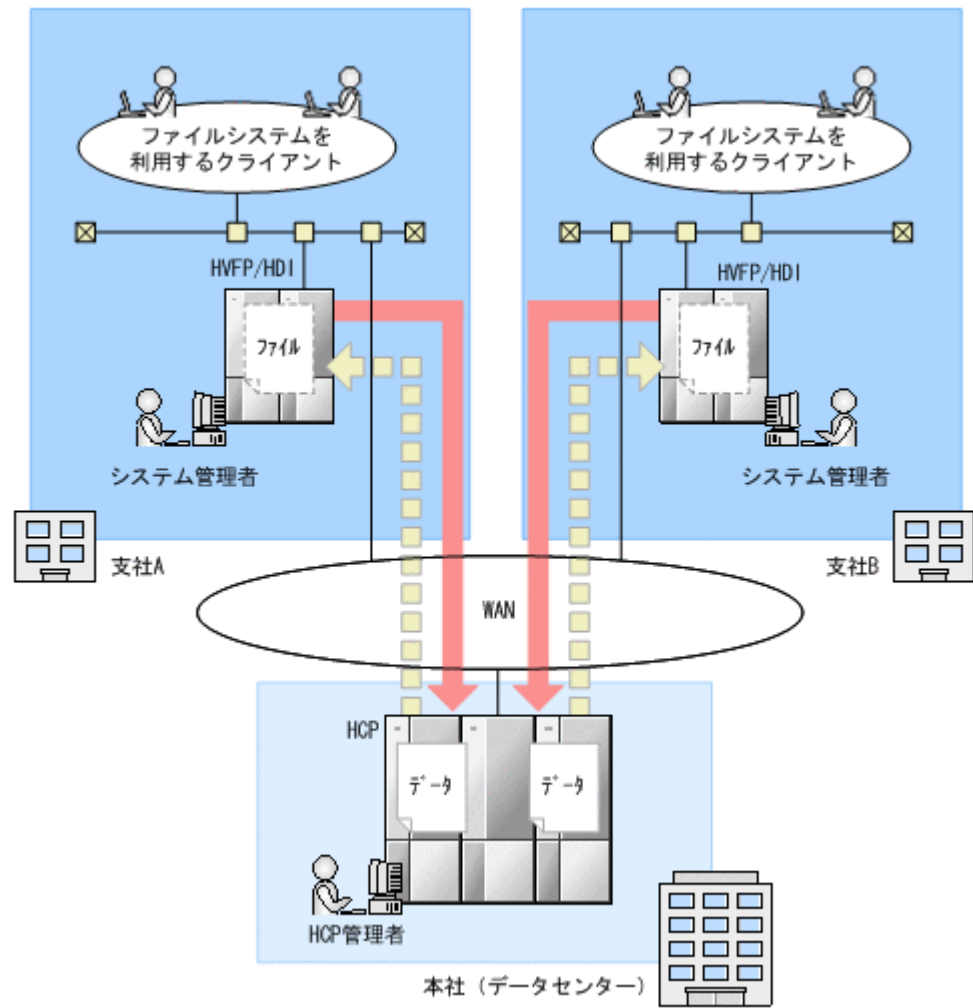
例えば、データの改ざんや削除を防止するためにファイルを WORM 化し、アクセス頻度の低いファイルから HCP に定期的にマイグレートすることで、アーカイブされたデータを効率的に管理しながら、コンプライアンスに対応したファイルシステムを運用できます。HCP にアーカイブされた過去のバージョンのデータを HVFP/HDI のクライアントに公開すれば、クライアントが必要なときにデータをリストアできます。

図 1-3 ストレージシステムを共有した HVFP と HCP の連携



また、分散した拠点で運用されている HVFP/HDI のファイルシステムのデータを、ネットワークを介して HCP にマイグレートすることで、大規模システムでのデータの集中管理を実現できます。各拠点のファイルシステムは HVFP/HDI のシステム管理者によって運用管理され、各拠点から送られてくるデータは HCP 管理者によって集中管理されます。HCP で集中管理されたデータは、各拠点の HVFP/HDI 間で共有することもできます。

図 1-4 ネットワークを介した HVFP/HDI と HCP の連携



システム構成

この章では、HVFP/HDI のシステム構成について説明します。また、HVFP/HDI が HCP と連携するときのシステム構成についても説明します。

- 2.1 ハードウェア構成
- 2.2 ネットワーク構成
- 2.3 ライセンス
- 2.4 HCP 連携時のシステム構成

2.1 ハードウェア構成

HVFP/HDI のファイルシステムサービスを運用するためには、ストレージシステムやノードのほか、ネットワーク上に外部サーバや外部装置が必要です。ここでは、HVFP/HDI のハードウェア構成について説明します。

2.1.1 ストレージシステムとノードの構成

クラスタ構成およびシングルノード構成でストレージシステムを使用する HVFP/HDI のノードはファイバーチャネルでストレージシステムに接続され、データポート、管理ポートおよび BMC ポートなどの各種ポート、DVD ドライブおよび内蔵ハードディスクなどが搭載されています。ノードのハードウェア情報については、HVFP/HDI に添付されているマニュアルを参照してください。また、各種ポートの配置や名称については、「付録 C. ノード上のポートの配置」を参照してください。

2.1.2 HVFP/HDI で必要な外部サーバや外部装置

ストレージシステムとノードのほかに、HVFP/HDI のシステムで必要となる外部サーバや外部装置について説明します。

管理コンソール

GUI またはコマンドを使用する際に必要なマシンです。また、次のプログラムも使用できます。

Storage Navigator

クラスタ構成の HVFP/HDI で、ストレージシステムに Virtual Storage Platform, Universal Storage Platform V/VM または HUS VM を使用している場合に、Universal Volume Manager などを操作するために必要なプログラムです。デバイスファイルがどのディスクドライブに実在するのかを調べる際に使用できます。

管理コンソールの環境設定については、「3.3 管理コンソールの環境設定」を参照してください。

管理サーバ (クラスタ構成の場合)

クラスタ構成の HVFP/HDI を運用・管理する際に必要なマシンです。Hitachi File Services Manager をインストールします。1 台の管理サーバで最大 16 クラスタを管理できます。

管理サーバは管理コンソールとしても使用できます。

管理サーバで必要となるプログラムについて説明します。

Hitachi File Services Manager

GUI を利用して HVFP/HDI を運用または管理するプログラムです。ノード上の Configuration Manager と連携して、HVFP/HDI のセットアップや運用を管理するための GUI の機能を提供します。Configuration Manager との総称を File Services Manager と呼びます。

1 台の管理サーバから複数のクラスタを管理すると、管理サーバとノードにインストールされているプログラムのバージョンが異なることがあります。管理サーバにインストールされている Hitachi File Services Manager より古い製品のプログラムがノードにインストールされている場合は、GUI に表示されない情報があったり、GUI の項目が非活性になったりします。このようなときは、ノード上にインストールされているプログラムのバージョンに対応したマニュアルを参照してください。

複数の管理サーバから同一クラスタを管理すると、管理サーバ間の情報に不整合が発生し、対象のクラスタに対して予期しない設定が行われるおそれがあります。このため、複数の管理サーバで同一クラスタを管理しないでください。

Device Manager

ストレージシステムのディスクリソースやハードウェア構成を統合管理するプログラムです。Device Manager と連携することで、ストレージシステムのボリュームとファイルシステムの対応を一元管理できます。

Hitachi File Services Manager とは異なるマシンにインストールして運用することもできます。Hitachi File Services Manager とは異なるマシンにインストールした Device Manager の GUI から Hitachi File Services Manager を使用する場合は、「[7.4.7 Device Manager に接続してユーザーアカウントを管理する](#)」に従って、Hitachi File Services Manager の設定を変更してください。

Hitachi Command Suite 共通コンポーネント

Hitachi File Services Manager と Hitachi Command Suite 製品に共通する機能を提供するコンポーネントです。Hitachi File Services Manager または Hitachi Command Suite 製品の一部としてインストールされます。GUI へのログイン、管理サーバの統合ログ出力、Web サービスなどの機能を提供します。

Hitachi Storage Navigator Modular 2

ストレージシステムに Hitachi AMS2000 シリーズまたは HUS100 シリーズを使用している場合に、ディスクドライブの配置やパリティグループを考慮して LU を作成または削除するために必要なプログラムです。

Hitachi File Services Manager から管理サーバにインストールされた Hitachi Storage Navigator Modular 2 の GUI を表示できます。Hitachi File Services Manager から Hitachi Storage Navigator Modular 2 の GUI を表示する場合に、ストレージシステムで Password Protection 機能または Account Authentication 機能を有効にしているときは、ストレージシステムに「nasmgr」というアカウントを作成しておく必要があります。また、nasmgr アカウントのパスワードには、ノードに設定されている管理サーバの認証パスワードを設定してください（Password Protection 機能では、認証パスワードの先頭から 12 文字目までを設定します）。

管理サーバの環境設定については、「[3.2 管理サーバの環境設定](#)」を参照してください。

NTP サーバ

各ノードに正しい時刻を反映させるサーバです。Virtual Server を作成している場合、クラスター内の Virtual Server 間で共有するため、Physical Node 上で登録してください。NTP サーバでの障害に備えて、2 台の NTP サーバを使用することを推奨します。NTP サーバの環境設定については「[3.10 NTP サーバの環境設定](#)」を参照してください。

SNMP マネージャー

SNMP を利用して、システム情報を参照したり、障害通知を受けたりする場合に必要なマネージャーです。Virtual Server を作成している場合は、Physical Node および Virtual Server 上でそれぞれ登録できます。SNMP マネージャーの環境設定については「[3.9 SNMP マネージャーの環境設定](#)」を参照してください。

DNS サーバ

DNS を利用してホスト名を検索する場合に必要なサーバです。

NIS サーバ

NIS を利用してユーザーおよびホストの情報を検索する場合に必要なサーバです。NIS サーバの環境設定については、「[3.4 NIS サーバの環境設定](#)」を参照してください。

WINS サーバ

HVFP/HDI を利用する CIFS クライアントが、WINS を利用して名前解決する場合に必要なサーバです。

KDC サーバ

次の目的で使用する場合に必要なサーバです。

- ユーザー認証用
NFS サービスで Kerberos 認証を利用してユーザーを認証する場合に必要です。
- システム管理者のアカウント認証用
Kerberos 認証を利用してシステム管理者のアカウントを認証する場合に必要です。
KDC サーバの環境設定については、「[3.7 KDC サーバの環境設定](#)」を参照してください。

RADIUS サーバ

RADIUS 認証を利用してシステム管理者のアカウントを認証する場合に必要なサーバです。
RADIUS サーバの環境設定については「[3.8 RADIUS サーバの環境設定](#)」を参照してください。

ドメインコントローラー

HVFP/HDI で Active Directory 認証または NT ドメイン認証を利用してユーザーを認証する場合に必要なサーバです。Active Directory ドメインコントローラーを使用している場合は、NFS サービスで Kerberos 認証を利用してユーザーを認証する際に、KDC サーバとしても利用できます。

LDAP サーバ

次の目的で使用する場合に必要なサーバです。

- ユーザー認証用
LDAP サーバでユーザー情報を管理する場合に必要です。
- ユーザーマッピング用
CIFS クライアントに対して自動的に割り当てられた、または LDAP 管理者によって手動で割り当てられたユーザー ID やグループ ID の情報を、LDAP サーバのデータベースに格納する場合に必要です。
使用する LDAP サーバを切り替えるときは、File Services Manager で設定を変更する必要があります。
- システム管理者のアカウント認証用
LDAP サーバでシステム管理者のアカウントを認証する場合に必要です。
LDAP サーバの環境設定については、「[3.5 LDAP サーバの環境設定](#)」を参照してください。

スキャンサーバ

リアルタイムスキャン機能を利用する場合に必要なサーバです。スキャンサーバの環境設定については、「[3.11 スキャンサーバの環境設定](#)」を参照してください。

FTP サーバ

ダンプファイルを一括ダウンロードする場合に必要なサーバです。シングルノード構成および Virtual Server OS LU 上のシステム設定情報を定時保存する場合の転送先にも指定できます。

プロキシサーバ

HVFP/HDI と HCP 間の http または https 通信を中継する場合に必要なサーバです。

SMTP サーバ

E-mail を利用して、障害通知を受ける場合に必要なサーバです。Virtual Server を作成している場合は、Physical Node および Virtual Server 上でそれぞれ登録できます。SMTP サーバの環境設定については「[3.13 SMTP サーバの環境設定](#)」を参照してください。

ALog マネージャーサーバ (ALog ConVerter のマネージャーサーバ)

ALog ConVerter を使用して、NFS 共有以外へのユーザーアクセスを記録した監査ログを管理する場合に必要なサーバです。ALog マネージャーサーバの環境設定については、ALog ConVerter のドキュメントを参照してください。

DHCP サーバ

HDI を運用・管理する際に、DHCP を利用してノードのネットワーク情報を設定するときに必要なサーバです。DHCP サーバの環境設定については「[3.15 DHCP サーバの環境設定](#)」を参照してください。

このほか、エンドユーザーが HVFP/HDI の GUI を使用する場合は、管理コンソールの要件に従ったマシンが必要です。管理コンソールのマシン要件については、「[3.3 管理コンソールの環境設定](#)」を参照してください。

また、Hitachi File Remote Replicator を使用する場合は、プライマリーサイトとセカンダリーサイトの両方が、HVFP/HDI として運用するためのハードウェアの前提条件を満たすように、環境を構築する必要があります。両サイトはソフトウェア構成も一致させる必要があるため、システム管理者は、インストールされているソフトウェアの構成とバージョンがサイト間で同じになるよう管理してください。

2.1.3 NDMP 機能を使用する場合に HVFP/HDI で必要な外部サーバや外部装置

NDMP 機能を使用する場合に必要な外部サーバや装置について説明します。

Backup Restore でサポートしているバックアップ管理ソフトウェアおよび各ソフトウェアを使用する上での注意事項については、HVFP/HDI に添付されている Backup Restore の補足資料を参照してください。

バックアップサーバ

バックアップサーバは、バックアップ管理ソフトウェアがインストールされているサーバです。バックアップサーバは、メディアサーバを兼ねることができます。バックアップサーバには、バックアップ管理ソフトウェアが必要です。

メディアサーバ

メディアサーバは、テープ装置を管理するサーバです。メディアサーバには、バックアップ管理ソフトウェアが必要です。

テープ装置

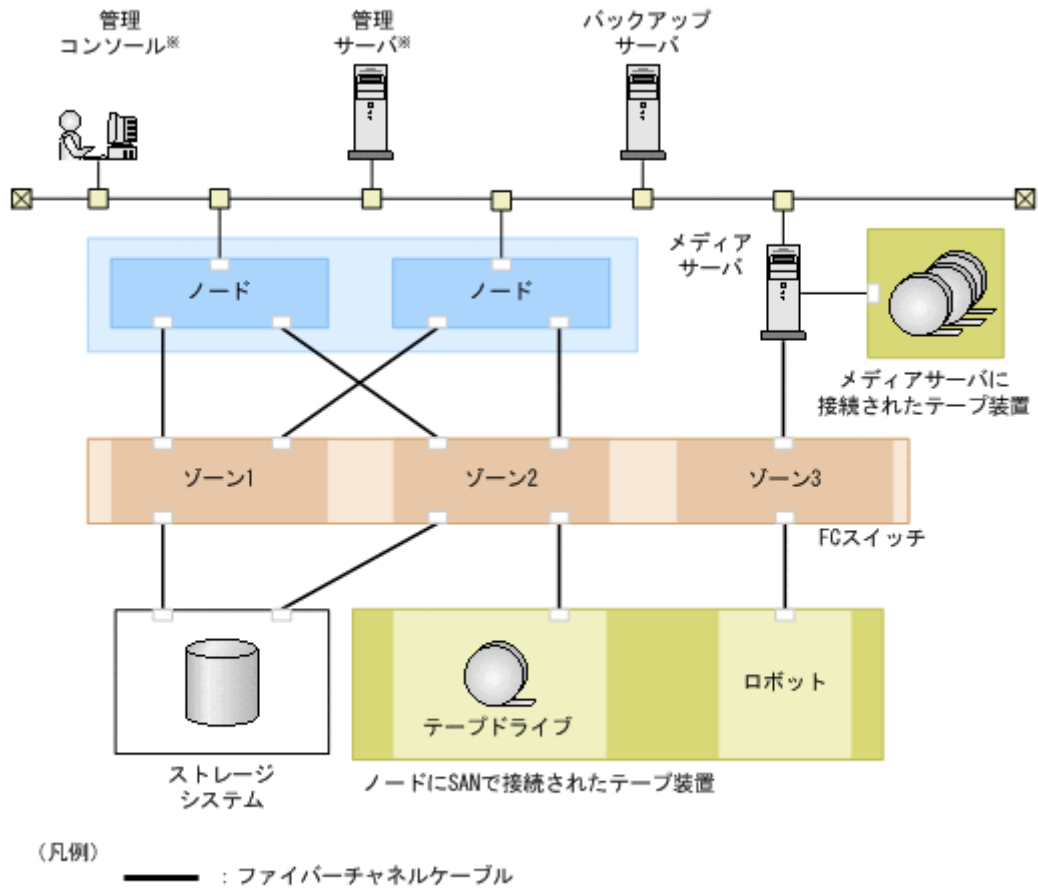
ファイルシステムのデータをバックアップしたり、テープ装置からデータをリストアしたりできます。

メディアサーバに接続して使用できるテープ装置については、バックアップ管理ソフトウェアのドキュメントを参照してください。

ノードに SAN で接続して使用できるテープドライブの規格、テープ装置のベンダー名や機種名などの詳細については、弊社担当営業にお問い合わせください。

クラスタ構成の場合に、Backup Restore を使用して NDMP 機能を使用するときのハードウェア構成の例を次に示します。

図 2-1 クラスタ構成で NDMP 機能を使用する場合のハードウェア構成例



注※ 管理コンソールと管理サーバは、同一マシンで運用することもできます。

ノードに SAN で接続されたテープ装置を使用する場合は、メディアサーバがロボットを管理し、NDMP サーバがテープドライブを管理する構成にします。

Virtual Server を使用して HVFP/HDI を運用する場合、ノードに SAN で接続するテープ装置については、すべての Virtual Server でバックアップサーバ、メディアサーバおよびテープ装置を共有する構成を推奨します。

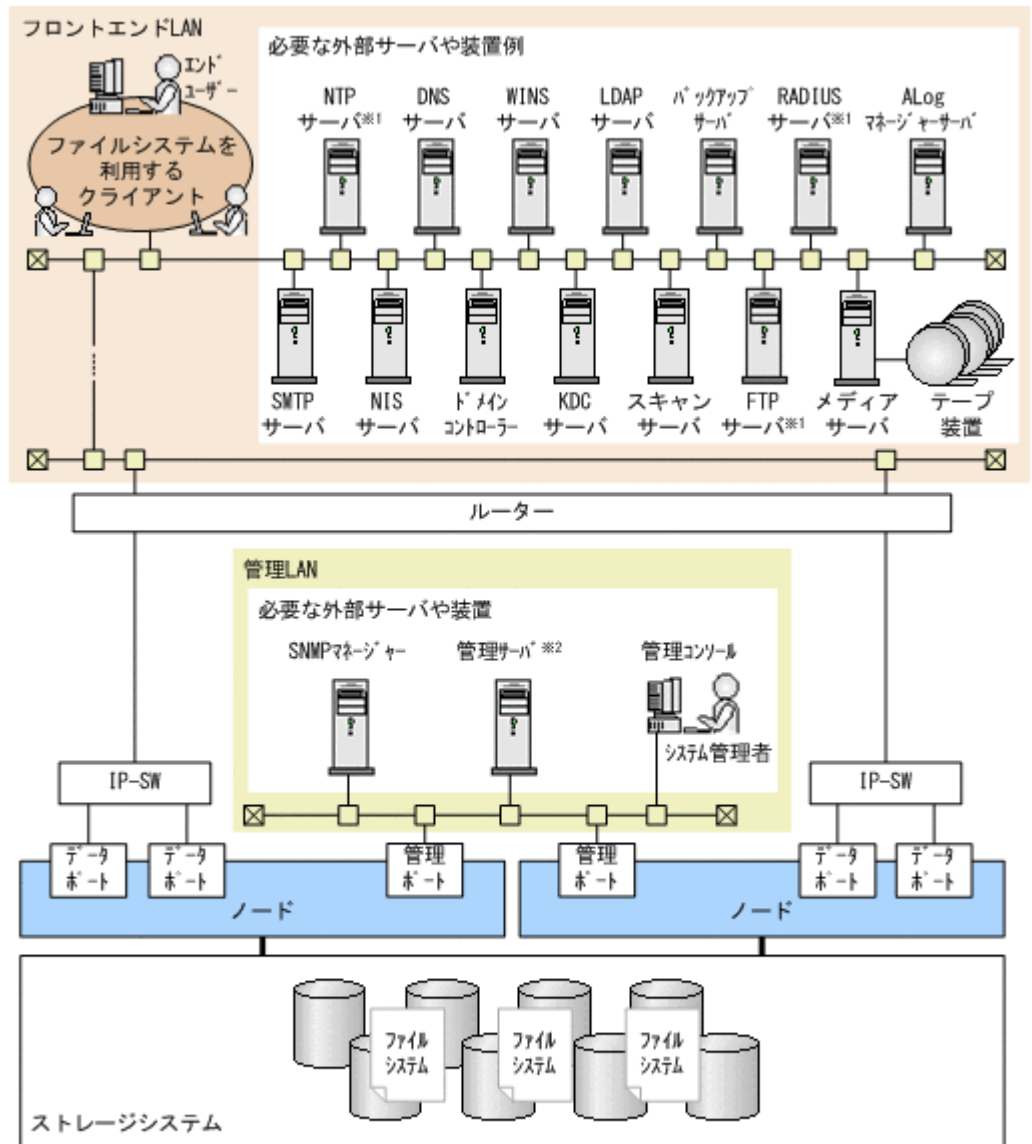
2.2 ネットワーク構成

HVFP/HDI のネットワークは、システム管理者が HVFP/HDI を運用および管理するために使用する管理 LAN と、クライアントがストレージシステムや内蔵ハードディスク内に格納されたりソースにアクセスするために使用するフロントエンド LAN で構成されます。

クラスタ構成の HVFP/HDI で、Virtual Server を使用していない場合のネットワーク構成例を次の図に示します。Virtual Server を使用する場合のネットワーク構成については、「仮想サーバ環境セットアップガイド」を参照してください。シングルノード構成の場合のネットワーク構成については、「シングルノード構成セットアップガイド」を参照してください。

なお、保守員が保守作業や障害対策を行う場合は、保守 LAN を使用します。

図 2-2 HVFP/HDI のネットワーク構成例（Virtual Server を使用していない場合）



注※1 必要に応じて管理サーバと通信できるように設定してください。

注※2 管理コンソールの前提ソフトウェアを管理サーバにインストールして、1台のマシンで運用することもできます。

ノードの管理ポートおよびデータポートはそれぞれ、管理 LAN とフロントエンド LAN に接続します。使用できるデータポートの種別や名称は、ノードの拡張スロットに搭載したオプションカードの構成によって異なります。オプションカードの構成と使用できるデータポートの関係については、「付録 C. ノード上のポートの配置」を参照してください。

クライアントは、データポートに設定された仮想 IP アドレスを使用してファイルシステムにアクセスします。障害によってフェールオーバーが発生してクラスタ内の別のノードでサービスが提供される場合でも、同じ名称のインターフェースに仮想 IP アドレスが引き継がれるため、クライアントは継続してアクセスできます。

管理ポートに対して仮想 IP アドレスを設定して、管理 LAN に設置した管理コンソールからもファイルシステムにアクセスできます。また、管理ポートをデータポートとして使用することもできます。

システム管理者は、ネットワーク構成、ファイルシステムのマウント、または Virtual Server が稼働するノードなどを計画的に設計することで、ファイルへのアクセスを両ノードに分散し、1つのノードに掛かる負荷を軽減できます。

HVFP/HDI は IPv4 および IPv6 をサポートしています。IPv4 と IPv6 のネットワークが共存する環境でも利用できます。

このほか、HCP と連携する場合のシステムの構成や必要な条件については、「[2.4 HCP 連携時のシステム構成](#)」を参照してください。

ネットワークを構成する前に

- SNMP マネージャー、管理コンソールおよび管理サーバは、管理 LAN に接続してください。
- File Services Manager の GUI を利用するエンドユーザーが使用するマシンは、フロントエンド LAN 上に配置してください。
- ノード内のデータポート、リンク結合の仮想ポート、または VLAN の仮想的なインターフェースに割り当てる固有 IP アドレスおよび仮想 IP アドレスはすべて異なるネットワークセグメントにする必要があります。
- 同一クラスタ内のノード間で対応しているポート（同一名称のポート）にそれぞれ割り当てる固有 IP アドレスおよび仮想 IP アドレスは、同じネットワークセグメントにする必要があります。
- ノードと、外部サーバまたはクライアントマシンとの間で通信できるように、File Services Manager でルーティング情報を設定する必要があります。
- ノード、外部サーバおよびクライアントのマシンの時刻は合わせておく必要があります。
- クラスタ構成の場合、ノードの BMC ポートの接続構成には、次の構成があります。

- 管理ポートが接続されている IP スイッチに BMC ポートを接続する構成

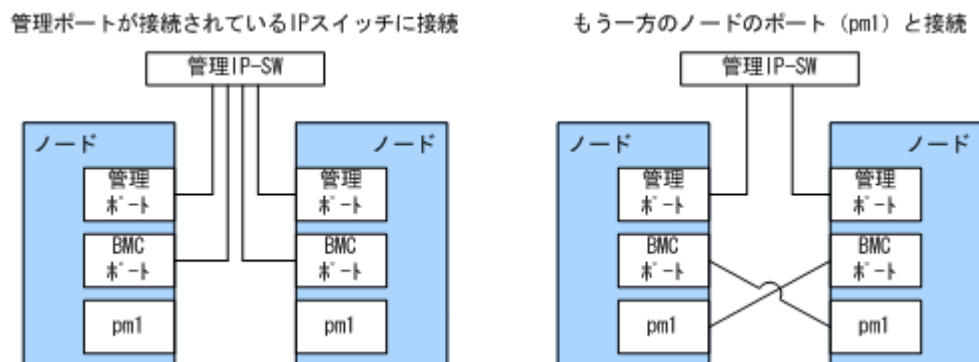
BMC ポートのネットワークアドレスは、mng0 のネットワークアドレスと同じにする必要があります。

- もう一方のノードのポート (pm1) と BMC ポートを接続する構成

BMC ポートのネットワークアドレスは、mng0 のネットワークアドレスと別にする必要があります。

接続構成を変更するときは、必ず `bmcctl` コマンドを使用して BMC ポートの設定を変更してください。

図 2-3 BMC ポートの接続構成



管理ポートが接続されている IP スイッチに BMC ポートを接続する場合は、Hitachi File Services Manager からノードの OS を起動できます。

フロントエンド LAN に設置した管理コンソールからシステムを管理する前に

フロントエンド LAN に設置した管理コンソールからもシステムを管理できます。フロントエンド LAN に設置した管理コンソールからシステムを管理するときの注意事項を次に示します。

- 管理サーバとノードの接続には固有 IP アドレスを使用します。管理用として使用するデータポートには固有 IP アドレスを必ず設定してください。
- フロントエンド LAN に設置した管理コンソールからシステムを管理する運用であっても、HVFP/HDI でクラスタを構築する場合や、ネットワーク障害を回復する場合など、管理 LAN に設置した管理コンソールから操作が必要となることがあります。管理サーバおよび管理コンソールは、適切なネットワーク上にマシンを移動するか、管理 LAN とフロントエンド LAN のどちらにもマシンを用意してください。なお、接続するネットワークを変更する際には、管理サーバおよび管理コンソールに設定されている IP アドレスを修正する必要があります。
- ファイルシステムのアクセス状況によっては、File Services Manager の GUI の処理に時間が掛かることがあります。
- Hitachi Storage Navigator Modular 2 で LU を作成する際には、管理用として使用するフロントエンド LAN に、ストレージシステムのコントローラ (CTL) の管理ポートを接続してください。
- 管理用として使用するデータポートと、管理コンソールまたは管理サーバとの間で通信する際に、ネットワークアドレス変換機能 (NAT) は利用できません。
- 管理用として使用するデータポートの設定を変更するときは、管理 LAN に設置した管理コンソールから変更してください。フロントエンド LAN に設置した管理コンソールから設定を変更すると、File Services Manager の GUI が応答しなくなるおそれがあります。その場合は、タイトルバーの [X] ボタンをクリックして画面を閉じてください。
- 管理用として使用するデータポートをリンク結合する際に設定を誤ると、フロントエンド LAN に設置した管理コンソールから File Services Manager の GUI を利用できなくなります。システム管理者は、管理 LAN に設置した管理コンソールからネットワークを設定し直してください。
- 使用しているストレージシステムが Hitachi AMS2000 シリーズまたは HUS100 シリーズの場合、管理用として使用するデータポートに対して、VLAN インターフェースは作成できません。
- ソフトウェアの更新は、管理 LAN に設置した管理コンソールから実施してください。

なお、システム導入時に次の設定が完了していない場合、管理 LAN に設置した管理コンソールから設定する必要があります。

- HVFP/HDI でのクラスタ構成の定義
- データポートの設定

管理サーバおよび管理コンソールを管理 LAN から利用できるようにネットワークを構築してください。必要な設定が完了したあと、管理サーバおよび管理コンソールをフロントエンド LAN から利用できるようにネットワーク構成を変更して、運用を開始してください。

また、障害発生時に次の作業を行う場合、管理 LAN に設置した管理コンソールから操作する必要があります。

- フロントエンド LAN のネットワーク障害の回復
- データポートのリンク障害の回復
- 保存していたシステム LU 情報の回復

このほか、障害を回復するために、保守員から指示を受けてクラスタを操作するときにも、管理 LAN に設置した管理コンソールから操作する必要があります。フロントエンド LAN から利用していた管理サーバおよび管理コンソールを管理 LAN から利用できるようにネットワーク構成を変更してください。必要な作業が完了したあと、管理サーバおよび管理コンソールをフロントエンド LAN から再度利用できるようにネットワーク構成を変更して、運用を再開してください。

Backup Restore のボリュームレプリケーション連携機能で使用するネットワークを構成する前に Backup Restore のボリュームレプリケーション連携機能の運用を目的としたポートに仮想 IP アドレスを指定しないでインターフェースを作成すると、このインターフェースでリンク障害が発生しても、フェールオーバーや障害通知が発生しません。このため、Backup Restore のボリュームレプリケーション連携機能の運用で使用しているネットワークで発生した障害が HVFP/HDI の運用に影響を与えることを防ぎます。

Hitachi File Remote Replicator で使用するネットワークを構成する前に

- サイト間で転送されるデータは暗号化されていないため、VPN (Virtual Private Network) 技術などを使用してセキュアな LAN 環境を構築することをお勧めします。
- サイト間で転送されるデータの量やコピーを実行する時間帯を考慮して、Hitachi File Remote Replicator で使用するネットワークに十分な回線速度を確保してください。
- 両サイトでは、時刻を正しく設定しておくことをお勧めします。HFRR ペアを構成するファイルシステムが WORM 対応ファイルシステムの場合、両サイトの時刻が同期しているとコピーできます。
- Hitachi File Remote Replicator は IPv4 と IPv6 のどちらでもサイト間の通信ができますが、両サイトの IP のバージョンが異なっていると、サイト間通信を実現するために IPv4/IPv6 トランスレータの設置や IPv4 と IPv6 間の通信を考慮した情報の設定が必要です。このため、両サイトの IP のバージョンは一致させて運用することをお勧めします。

2.2.1 CIFS 共有を利用する場合のネットワーク構成

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

CIFS クライアントは、ノードの仮想 IP アドレスを指定するか、名前解決サービスを利用して、CIFS 共有にアクセスできます。

CIFS クライアントは CIFS 共有にアクセスする際に、ブラウジング機能を利用することもできます。ブラウジング機能を利用する場合の注意事項を次に示します。

- DNS, WINS, 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、ネットワークを構成してください。
- NetBIOS over TCP/IP プロトコルを使用した CIFS クライアントのアクセスを受け付けるように [CIFS Service Management] ページ (Setting Type : Security) で設定してください。設定していない場合は、次の不具合が生じます。
 - 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しません。
 - CIFS クライアント側で表示されるコンピューター一覧に、HVFP/HDI が提供する CIFS サービスが表示されません。
 - 同じサブネットの CIFS クライアントからブロードキャストを使用して名前解決できません。
- 同じサブネット上に設置されたドメインコントローラーを起動または停止するたびにローカルマスタブラウザの選定 (12 分程度) が発生します。また、同じサブネット上にドメインコントローラーがない場合、ローカルマスタブラウザが再起動されるとローカルマスタブラウザの選定や各マシンの情報の取得に時間が掛かります。ローカルマスタブラウザが動作するまで、CIFS クライアントは CIFS 共有にアクセスできません。
- CIFS クライアント側で表示されるコンピューター一覧は、ローカルマスタブラウザから提供された情報に基づいており、各コンピュータの稼働状況に対応していません。このため、コンピューター

ター一覧に表示されていても、停止しているコンピュータに対して CIFS クライアントはアクセスできません。

以降では、ブラウジング機能を利用する場合のネットワーク構成について説明します。

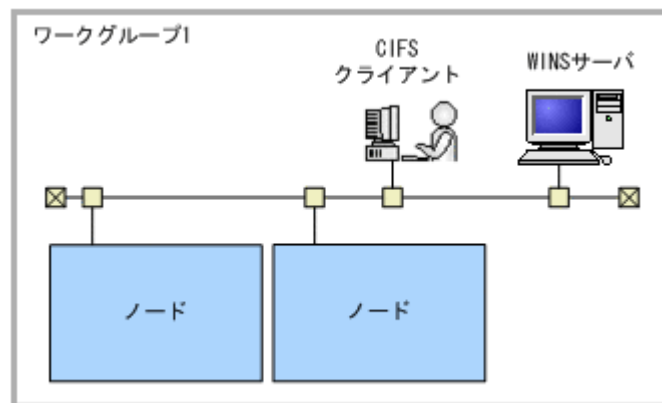
(1) CIFS クライアントとノードが同じサブネットに接続されている場合

CIFS クライアントとノード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。

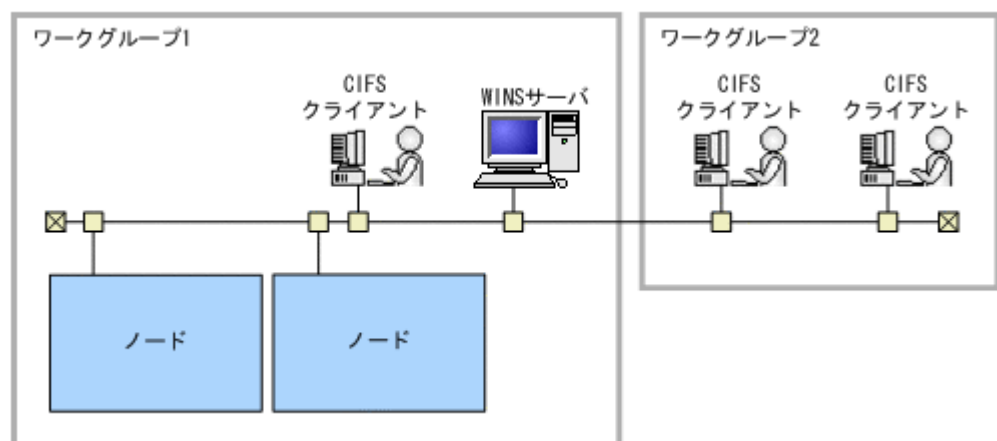
CIFS クライアントとノードが単一のワークグループに属しているネットワークの例を次の図に示します。

図 2-4 単一のワークグループに属しているネットワークの例



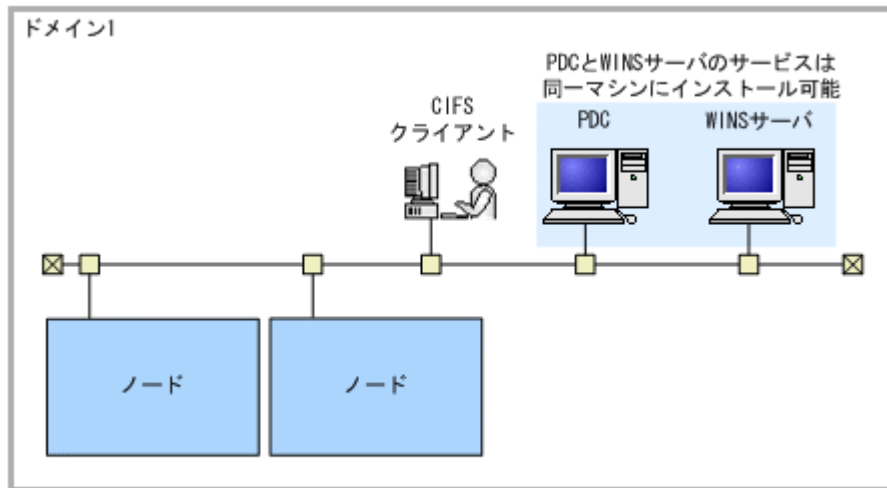
CIFS クライアントとノードが複数のワークグループに属しているネットワークの例を次の図に示します。

図 2-5 複数のワークグループに属しているネットワークの例



CIFS クライアントとノードが単一の NT ドメインに属しているネットワークの例を次の図に示します。

図 2-6 単一の NT ドメインに属しているネットワークの例



(凡例)

PDC: プライマリドメインコントローラー

(2) CIFS クライアントがノードと異なるサブネットに接続されている場合

CIFS クライアントがノードと異なるサブネットに接続されている場合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 ドメイン構成にしてください。
- ノード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
```

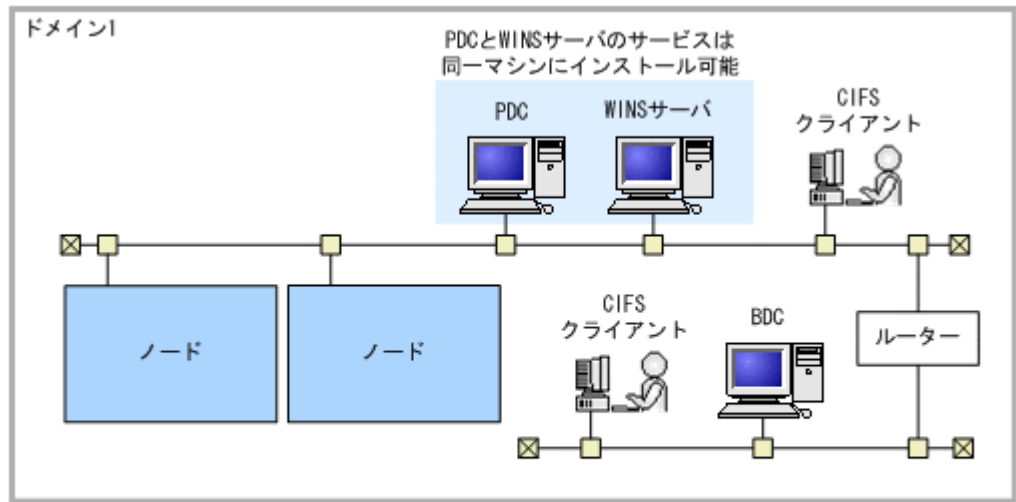
Active Directory ドメイン構成のとき

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。

```
<ノード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
```

NT ドメイン構成のときに、ノードとプライマリドメインコントローラーが同じサブネットにあるネットワークの例を次の図に示します。

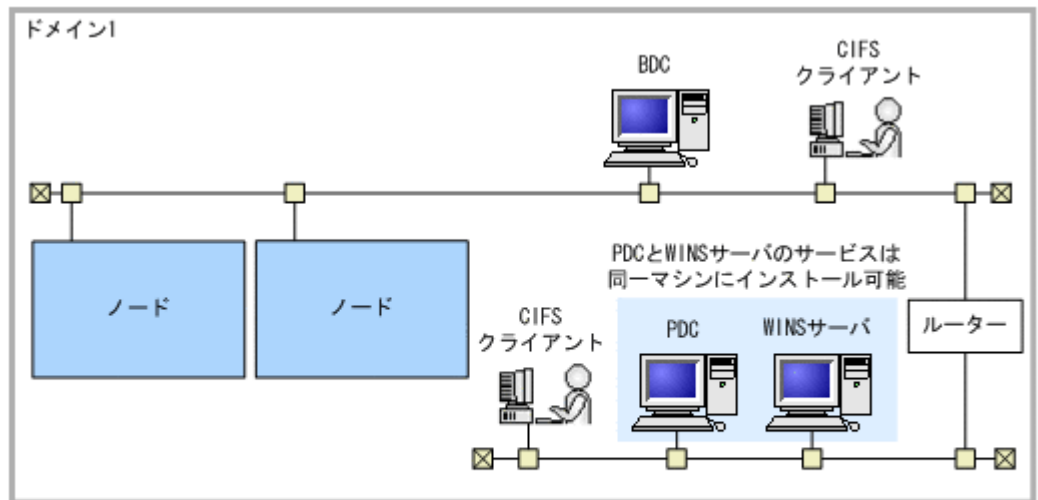
図 2-7 ノードとプライマリドメインコントローラーが同じサブネットにあるネットワークの例 (NT ドメイン構成)



(凡例)
 PDC: プライマリドメインコントローラー
 BDC: バックアップドメインコントローラー

NT ドメイン構成のときに、ノードとプライマリドメインコントローラーが別のサブネットにあるネットワークの例を次の図に示します。

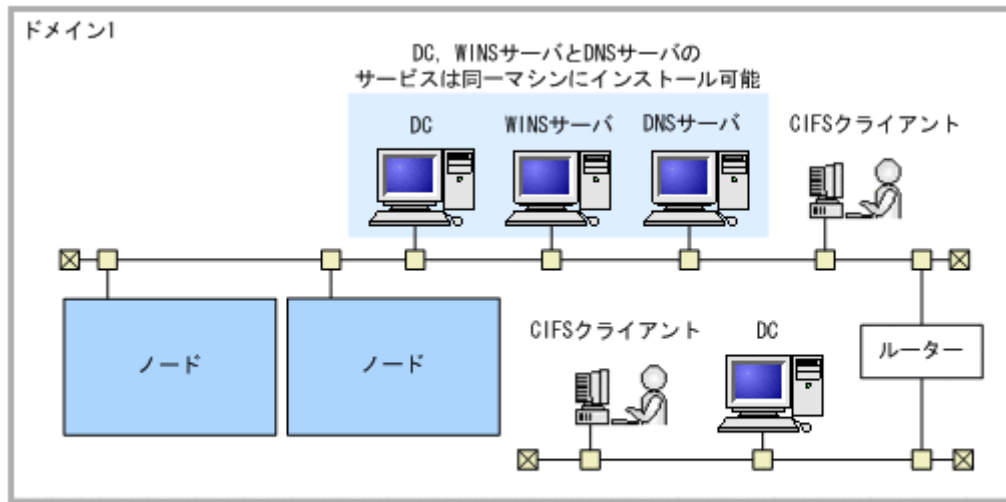
図 2-8 ノードとプライマリドメインコントローラーが別のサブネットにあるネットワークの例 (NT ドメイン構成)



(凡例)
 PDC: プライマリドメインコントローラー
 BDC: バックアップドメインコントローラー

Active Directory ドメイン構成で、ノードとプライマリドメインコントローラーが同じサブネットにあるネットワークの例を次の図に示します。

図 2-9 ノードとドメインコントローラーが同じサブネットにあるネットワークの例（Active Directory ドメイン構成）



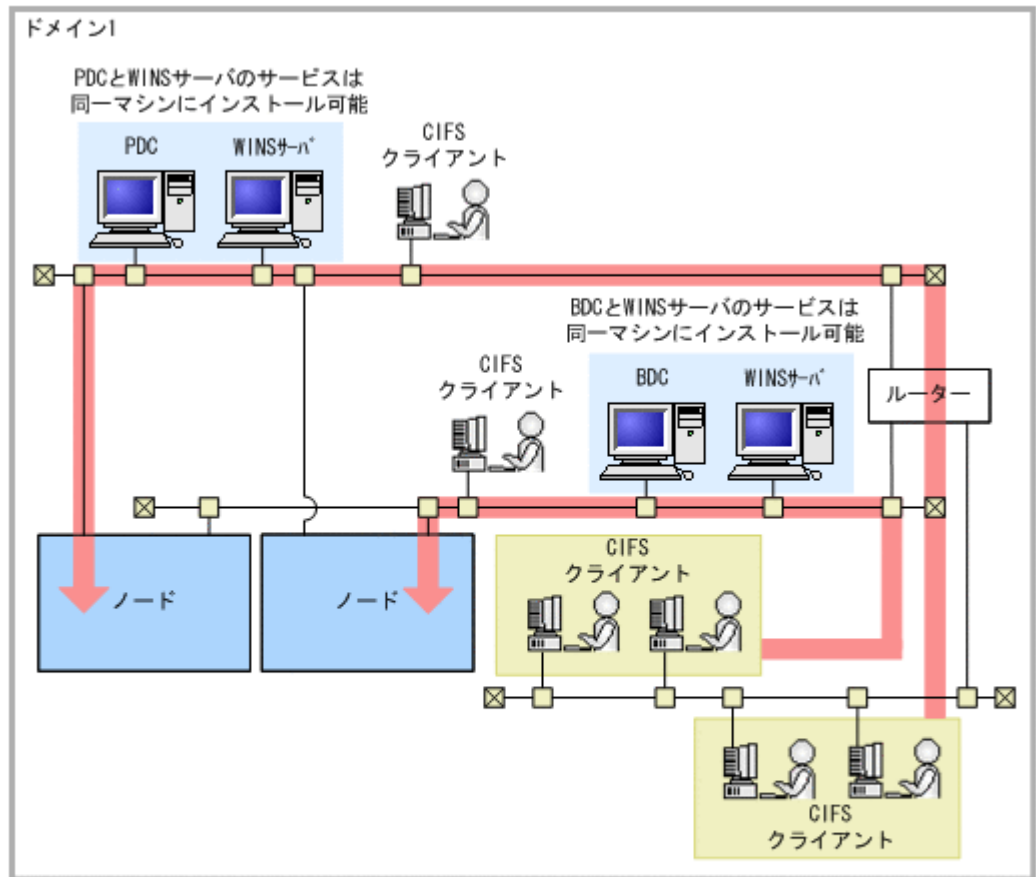
(凡例)

DC：ドメインコントローラー

(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、各ポートが接続するサブネットごとに別々の WINS サーバが必要です。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。

図 2-10 複数のポートで CIFS サービスを利用するネットワークの例



(凡例)

PDC: プライマリドメインコントローラー

BDC: バックアップドメインコントローラー

➡ : アクセスの流れ

2.2.2 リンク結合を使用するとき

HVFP/HDI では、リンク結合機能として、リンク集約、リンク交代、およびこれらを併用する二段階リンク結合を利用できます。

リンク集約

リンク集約とは、集約する複数のポートを同じスイッチに接続し、各ポートを同時に利用する機能です。リンク集約を構成することで、通信に使用できる帯域を増やせます。また、一部のポートにリンク障害が発生しても、同じスイッチに接続したほかのポートで処理を継続できます。

リンク交代

リンク交代とは、2つのポートをグループ化し、障害に備えて片方のポートを待機させる機能です。ハードウェア障害（スイッチまたはNICの障害）が発生すると、自動的にポートが切り替わり、待機していたポートで処理を継続できます。

二段階リンク結合

リンク集約を使用して構成した仮想ポートを含む2つのポートに対してリンク交代を設定する機能です。リンク集約とリンク交代を併用することで、通信に使用できる帯域を増やししながら、リンク障害およびハードウェア障害のどちらにも対応できるため、HVFP/HDIでは、二段階リンク結合を利用してネットワークを構築することを推奨します。二段階リンク結合を使

用する場合は、クライアントと HVFP/HDI との通信を安定させるために、必ずタグ付き VLAN を併用してください。

ここでは、HVFP/HDI のリンク結合機能で推奨するネットワーク構成について説明します。

(1) 特長

HVFP/HDI でリンク結合を使用する場合の特長を次に示します。

- ネットワークに接続しているすべての物理ポートをリンク結合している場合は、一部のポートでリンク障害が発生しても、フェールオーバーを回避できます (すべてのポートでリンク障害が発生した場合はフェールオーバーが発生します)。
- リンク集約によってグループ化した複数の物理ポートを同時に使用することで、1つのインターフェースとしての通信速度を向上できます。
- リンク結合した仮想ポートに IP アドレスを設定するため、すべての物理ポートに設定する場合と比べて、管理する IP アドレスの数が少なくなります。
- HVFP/HDI では、リンク結合と VLAN を併用できます。なお、二段階リンク結合を使用する場合は、必ず VLAN を併用してください。VLAN とリンク結合を併用する前に、「[2.2.4 VLAN とリンク結合を併用するとき](#)」を参照してください。

(2) リンク結合を使用する前に

リンク結合を使用する前に次のことを確認してください。

- メディアタイプが異なるポート同士はリンク結合できません。すべて同じメディアタイプのポートでリンク結合を構成してください。
- Ethernet 規格が異なるポート同士はリンク結合できません。GbE のポート同士または 10GbE のポート同士でリンク結合を構成してください。
- リンク結合を使用する前に、ノードを接続するネットワーク環境の構築 (スイッチの設定など) が必要です。
- リンク集約を使用する場合、IEEE802.3ad (Dynamic LACP) をサポートしたスイッチが必要です。LACP モードは、「Active」に設定してください。
- ノードと接続するスイッチの種類によっては、リンク集約するポート数に制限が生じることがあります。集約できるポート数の上限については、使用しているスイッチのドキュメントを参照してください。
- ノードと接続するスイッチには、STP (Spanning Tree Protocol) の拡張機能として Port Fast/Uplink fast (または Fast Forwarding) 機能を持つスイッチがあります。HVFP/HDI を継続して運用するために、フロントエンド LAN と直接接続するノードのポートの Port Fast/Uplink fast 機能を有効にすることを推奨します。
- ノード内にリンク結合されていないポートがある場合、リンク結合されていないポートで障害が発生するとフェールオーバーが発生するため、すべてのポートでリンク結合することを推奨します。
- HVFP/HDI では、3つ以上のポートにリンク交代を設定した構成はサポートしていません。

(3) 推奨するリンク結合の構成

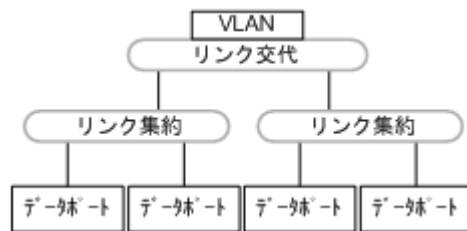
リンク集約を使用すると、一部のポートにリンク障害が発生しても、同じスイッチに接続したほかのポートで処理を継続できます。また、リンク交代を使用すると、スイッチまたは NIC のハードウェア障害が発生しても、自動的にポートが切り替わり、待機していたポートで処理を継続できます。

HVFP/HDI では、リンク障害またはハードウェア障害のどちらが発生しても運用を継続できるよう、二段階リンク結合を構成することを推奨します。また、ノード内にリンク結合されていないポートがある場合、リンク結合されていないポートで障害が発生するとフェールオーバーが発生するため、すべてのポートでリンク結合することを推奨します。

HVFP/HDI では、二段階リンク結合を構成する場合、実行系を待機系以上の性能にして構成することを推奨します。ただし、実行系と待機系の性能の差が大きい場合、待機しているポートに切り替わったときにシステム性能が大幅に低下することで、運用に支障が出るおそれがあります。待機系でも最低限の運用が継続できる性能を確保して、ネットワークを構成してください。

HVFP/HDI で推奨する二段階リンク結合の構成例を次の図に示します。

図 2-11 HVFP/HDI で推奨する二段階リンク結合の構成例



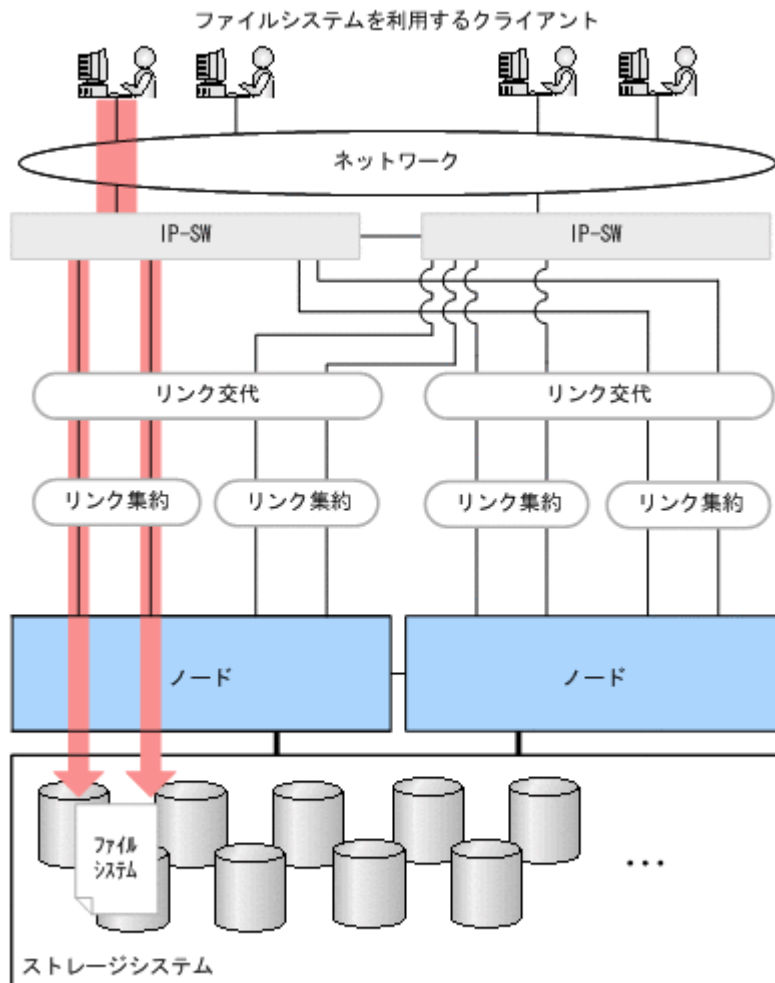
なお、次に示すリンク結合の構成はサポートしていません。

- ・ 3つ以上のポートにリンク交代を設定した構成
- ・ リンク交代ポートにリンク結合を設定する構成
- ・ リンク集約ポートにリンク集約を設定する構成

(4) 構成例

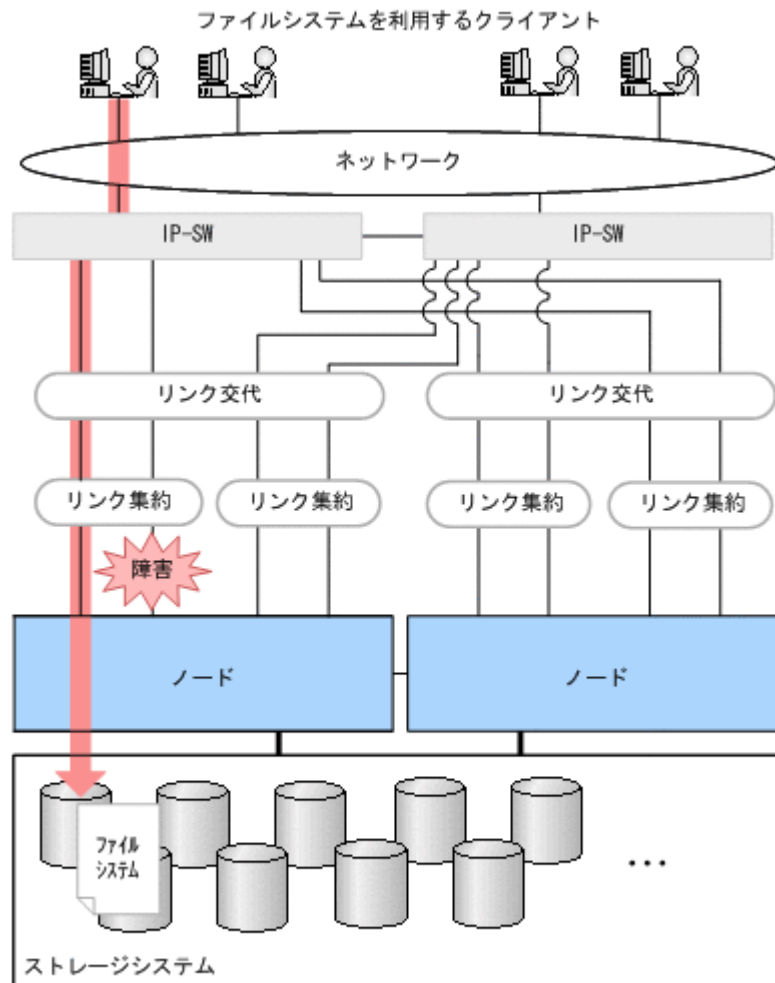
二段階リンク結合を使用した場合のネットワークの構成例を次に示します。

図 2-12 二段階リンク結合を利用した場合のネットワークの構成例（正常運用時）



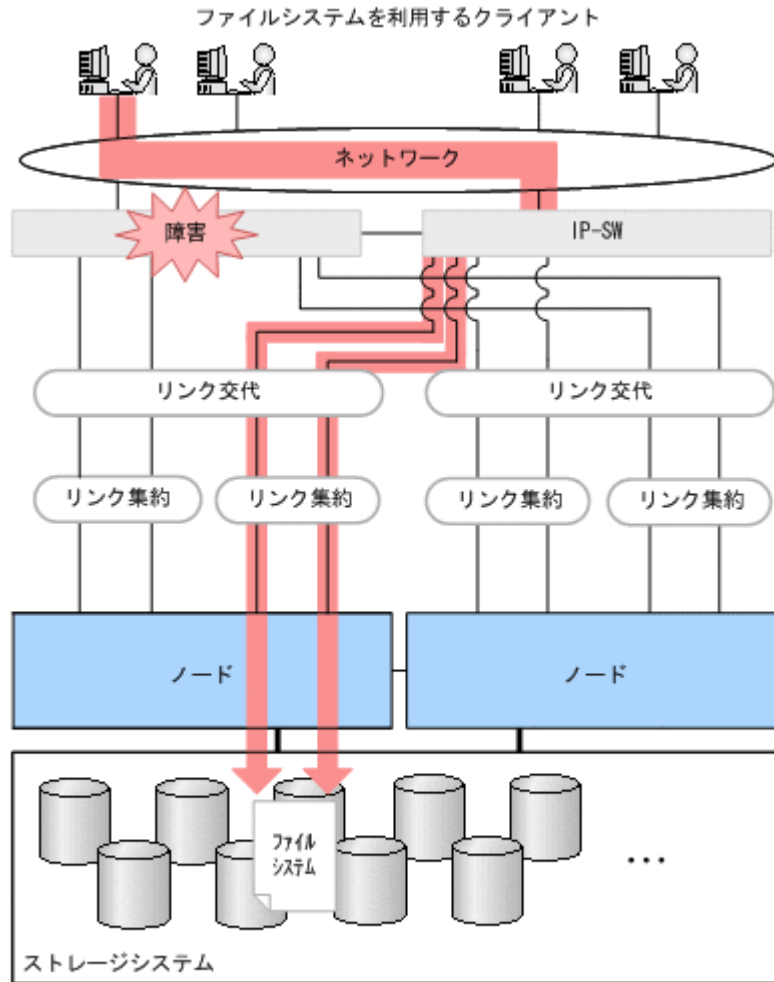
注 リンク集約を接続するスイッチには、IEEE802.3ad (Dynamic LACP) に対応しているスイッチを設置する必要があります。

図 2-13 二段階リンク結合を利用した場合のネットワークの構成例（リンク障害発生時）



注 リンク集約を接続するスイッチには、IEEE802.3ad (Dynamic LACP) に対応しているスイッチを設置する必要があります。

図 2-14 二段階リンク結合を利用した場合のネットワークの構成例（ハードウェア障害発生時）



注 リンク集約を接続するスイッチには、IEEE802.3ad (Dynamic LACP) に対応しているスイッチを設置する必要があります。

2.2.3 VLAN を使用するとき

HVFP/HDI では、VLAN を使用してネットワークを構成できます。ここでは、HVFP/HDI で使用できる VLAN の概要について説明します。

(1) 特長

HVFP/HDI で VLAN を使用する場合の特長を次に示します。

- IEEE802.1Q で規定されているタグ付き VLAN を使用できます。
- VLAN を使用したネットワーク構成でも、ノードに障害が発生した場合にフェールオーバーすることで、サービスを継続して提供しながら障害回復やリプレースなどの保守作業ができます。
- VLAN ごとに MTU 値（通信ネットワークで、転送 1 回につき送信できるデータの最大値）を設定できます。

(2) VLAN を使用する前に

HVFP/HDI で VLAN を使用するには、IEEE802.1Q で規定されているタグ付き VLAN に対応したスイッチが必要です。

(3) VLAN インターフェースの設定

VLAN を使用するとき、データポートに仮想的なインターフェース (VLAN インターフェース) が作成されます。VLAN インターフェースには、VLAN ID という識別子を与える必要があります。

また、フェールオーバーが発生した場合に、同じ IP アドレスでリソースグループに接続できるようにするために、VLAN インターフェースには、仮想 IP アドレスを設定できます。両方のノードでリンクダウンなどの障害を検知するために、仮想 IP アドレスは両方のノードに設定することを推奨します。仮想 IP アドレスを設定しない場合は、障害が発生していないか、[Check for Errors] ダイアログの [List of RAS Information] ページ ([List of Messages] 表示) でシステムメッセージを確認する必要があります。

1 クラスタあたりに設定できる VLAN ID の数と範囲、および仮想 IP アドレスの数を次に示します。

VLAN ID の数

VLAN ID は、1 クラスタあたり 256 個まで設定できます。ただし、仮想 IP アドレスの数が最大 (1 クラスタあたり 256 個) に達すると、それ以上 VLAN ID を設定できません。

VLAN ID の範囲

VLAN ID は、1~4094 の範囲で設定できます。クラスタ内で重複する VLAN ID は設定できません。

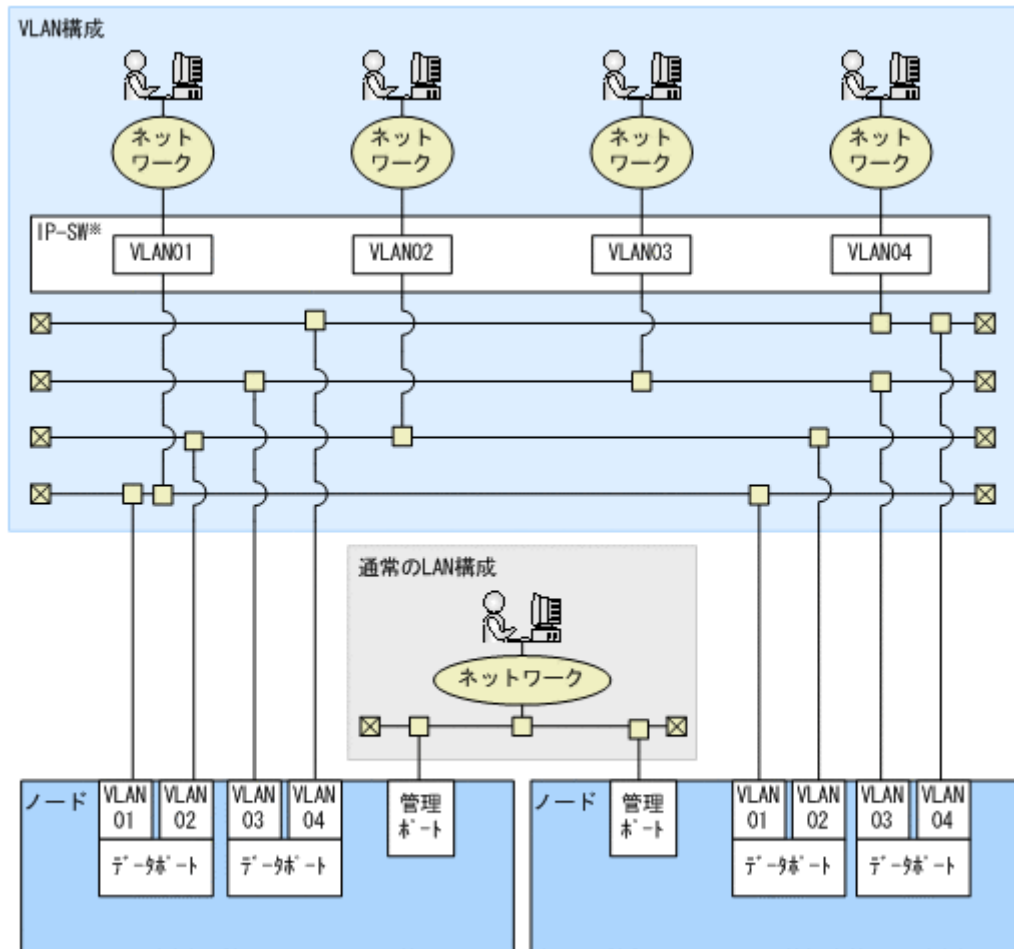
仮想 IP アドレスの数

仮想 IP アドレスは、1 クラスタあたり 256 個まで設定できます。

(4) 構成例

VLAN を使用した場合のネットワークの構成例を次に示します。

図 2-15 VLAN を使用した場合のネットワークの構成例



注※ IEEE802.1Qに対応しているスイッチを設置する必要があります。

2.2.4 VLAN とリンク結合を併用するとき

HVFP/HDI では、VLAN とリンク結合を併用してネットワークを構築できます。VLAN とリンク結合を併用してネットワークを構築すると、VLAN の特長とリンク結合の特長を併せ持ったネットワークを構築できます。VLAN の特長であるセキュリティの向上、容易で自由度の高いネットワーク設計に加えて、リンク結合の特長である帯域幅の拡大と可用性の向上も実現できます。

VLAN とリンク結合を併用したネットワークを構築するには、リンク結合を設定して複数のポートを 1 つの論理的なポートに結合し、さらにこの論理的なポートに VLAN インターフェースを設定します。

2.3 ライセンス

HVFP/HDI のライセンス体系を次の表に示します。

表 2-1 HVFP のライセンス (クラスタ構成の場合)

ライセンス名	説明
Hitachi Basic Operating System File Extension	HVFP のシステムの基本的な機能を利用するためのライセンスです。

ライセンス名	説明
Hitachi File Remote Replicator	Hitachi File Remote Replicator を使用するためのライセンス (オプション) です。 Hitachi File Remote Replicator を使用して差分スナップショットを別のサイトに遠隔バックアップするときに必要です。
Hitachi File Retention Utility	WORM 対応ファイルシステムを作成するためのライセンス (オプション) です。 WORM に対応したファイルシステムを運用するときに必要です。
Hitachi File Migrator	HVFP のファイルシステムのデータを HCP にマイグレートするためのライセンス (オプション) です。 HCP と連携して運用するときに必要です。
Hitachi File System Importer	ほかのファイルサーバのデータを HVFP にインポートするためのライセンス (オプション) です。 ほかのファイルサーバからデータをインポートするときに必要です。
Hitachi Dynamic Tiering for File	ファイルシステムを階層構成で運用するためのライセンス (オプション) です。 ファイルの種類や利用頻度に応じた最適なディスクドライブにファイルを移動させるときに必要です。
Enterprise Storage Connection	ストレージシステムに Virtual Storage Platform または Universal Storage Platform V/VM を使用するときに必要なライセンス (オプション) です。

表 2-2 HVFP のライセンス (シングルノード構成でストレージシステムを使用しない場合)

ライセンス名	説明
Hitachi Basic Operating System File Extension for Entry	HVFP のシステムの基本的な機能を利用するためのライセンスです。 このライセンスで、WORM に対応したファイルシステムを運用したり、HCP と連携して運用したりすることもできます。
Hitachi Basic Operating System File Extension for Entry with Data Encryption Feature	HVFP のシステムの基本的な機能およびユーザー LU の暗号化機能を利用するためのライセンスです。 このライセンスで、WORM に対応したファイルシステムを運用したり、HCP と連携して運用したりすることもできます。
Hitachi File Remote Replicator	Hitachi File Remote Replicator を使用するためのライセンス (オプション) です。 Hitachi File Remote Replicator を使用して差分スナップショットを別のサイトに遠隔バックアップするときに必要です。
Hitachi File System Importer	ほかのファイルサーバのデータを HVFP に移行するためのライセンス (オプション) です。 ほかのファイルサーバからデータを移行するときに必要です。

表 2-3 HVFP のライセンス (シングルノード構成でストレージシステムを使用する場合)

ライセンス名	説明
Hitachi Basic Operating System File Extension	HVFP のシステムの基本的な機能を利用するためのライセンスです。
Hitachi File Remote Replicator	Hitachi File Remote Replicator を使用するためのライセンス (オプション) です。 Hitachi File Remote Replicator を使用して差分スナップショットを別のサイトに遠隔バックアップするときに必要です。
Hitachi File Retention Utility	WORM 対応ファイルシステムを作成するためのライセンス (オプション) です。 WORM に対応したファイルシステムを運用するときに必要です。

ライセンス名	説明
Hitachi File Migrator	HVFP のファイルシステムのデータを HCP にマイグレートするためのライセンス（オプション）です。 HCP と連携して運用するときが必要です。
Hitachi File System Importer	ほかのファイルサーバのデータを HVFP に移行するためのライセンス（オプション）です。 ほかのファイルサーバからデータを移行するときが必要です。

表 2-4 HDI のライセンス

ライセンス名	説明
Hitachi Basic Operating System File Extension for Entry	HDI のシステムの基本的な機能を利用するためのライセンスです。 このライセンスで、WORM に対応したファイルシステムを運用したり、 HCP と連携して運用したりすることもできます。
Hitachi Basic Operating System File Extension for Entry with Data Encryption Feature	HDI のシステムの基本的な機能およびユーザー LU の暗号化機能を利用するためのライセンスです。 このライセンスで、WORM に対応したファイルシステムを運用したり、 HCP と連携して運用したりすることもできます。
Hitachi File System Importer	ほかのファイルサーバのデータを HDI に移行するためのライセンス（オプション）です。 ほかのファイルサーバからデータを移行するときが必要です。

2.4 HCP 連携時のシステム構成

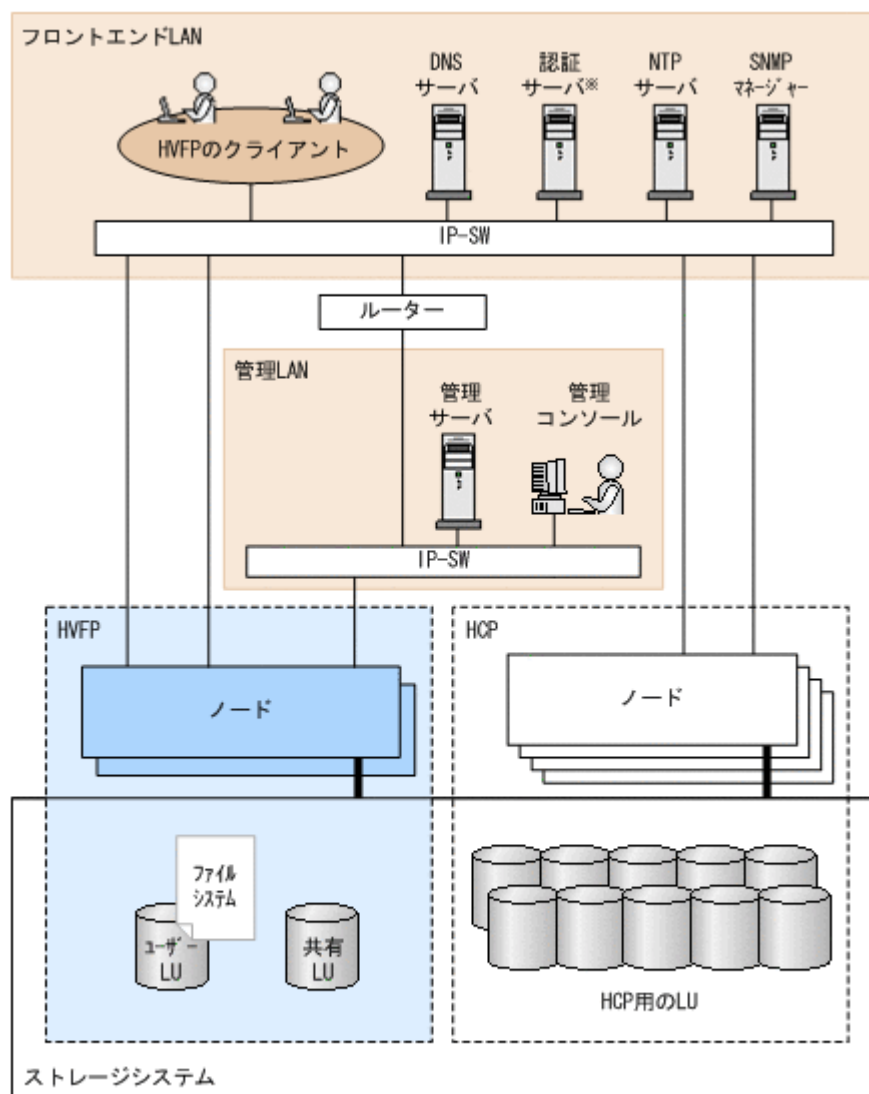
HVFP/HDI と HCP を連携するときのシステム構成について説明します。

なお、HCP や HVFP/HDI の各機器の時刻を同期させるため、NTP サーバを使用することを推奨します。

2.4.1 ストレージシステムを共有して連携する場合

ストレージシステムを共有して、HVFP/HDI と HCP を連携するときのシステム構成の例を次の図に示します。

図 2-16 ストレージシステムを共有して HVFP と HCP を連携するときのシステム構成例



注※ HVFPでは認証サーバとして、KDCサーバ、ドメインコントローラーやLDAPサーバなどを使用できます。

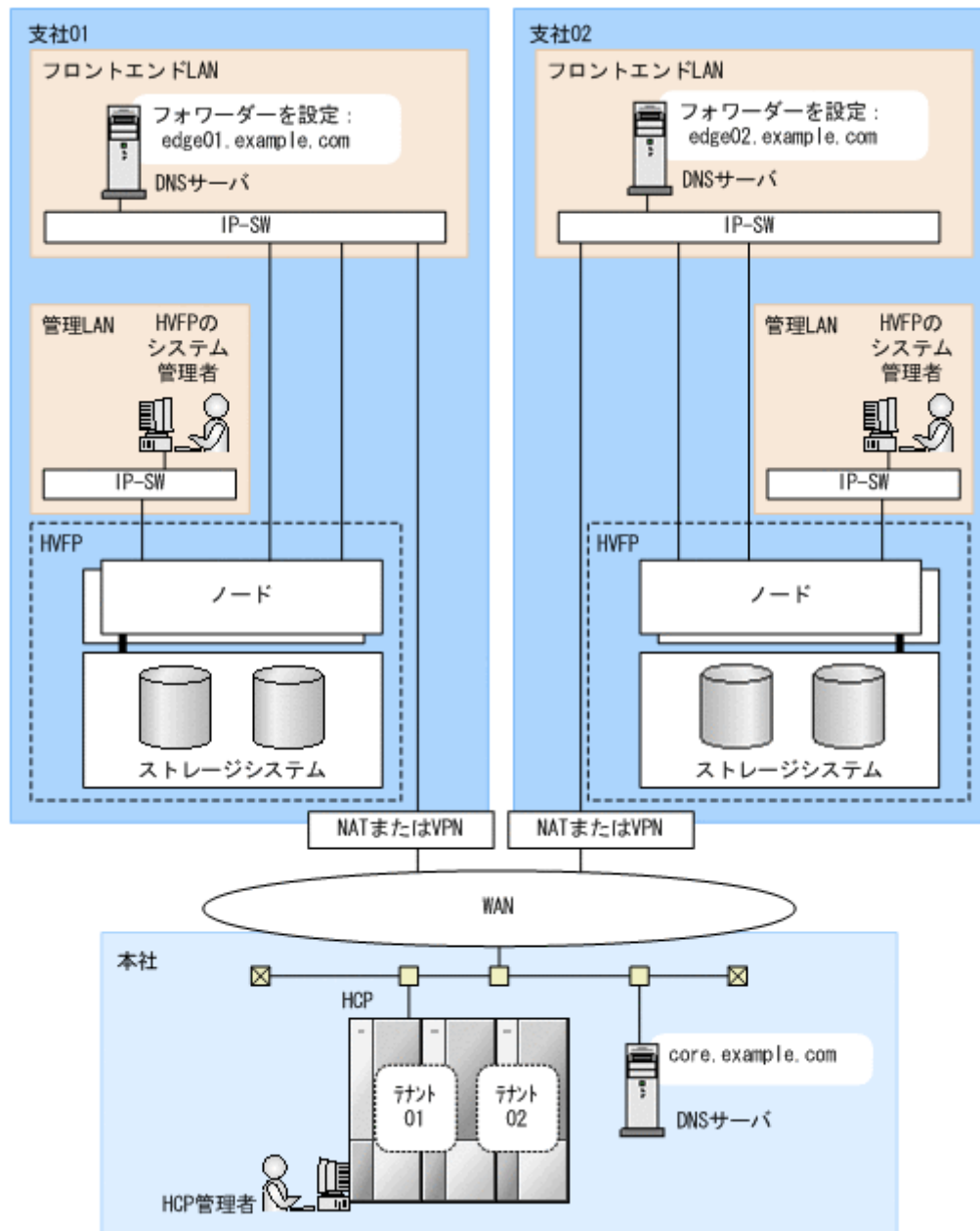
ストレージシステムを共有してHVFP/HDIとHCPを連携するときに必要な条件を次に示します。

- クライアントからのデータアクセスに使用されるポートは、HVFP/HDIおよびHCPともにフロントエンドLANに接続してください。
- 管理LANとフロントエンドLANの間にルーターを設置し、管理LAN上の管理コンソールからフロントエンドLAN上のHCPにhttpまたはhttpsで通信できるように設定してください。管理LANとフロントエンドLANの間に設置するルーターの設定については、HCPのマニュアルを参照してください。また、外部サーバをフロントエンドLANに設置する場合は、必要に応じて、外部サーバと管理サーバが通信できるように設定してください。
- DNSサーバはフロントエンドLANに設置してください。
- HVFP/HDIの管理コンソールでHCPのGUIを使用する場合、HCPを名前解決できるDNSサーバを管理コンソールに登録しておく必要があります。

2.4.2 ネットワークを介して連携する場合

ネットワークアドレス変換機能（NAT）や仮想プライベートネットワーク機能（VPN）を使用して、ネットワーク（WAN）経由で HVFP/HDI と HCP を連携するときのシステム構成の例を次の図に示します。

図 2-17 ネットワークを介して HVFP と HCP を連携するときのシステム構成例



ネットワークを介して HVFP/HDI と HCP を連携するとき、各拠点の HVFP/HDI で必要となる条件を次に示します。

- HVFP/HDI で利用している DNS サーバに対して、HCP のノードを名前解決できるようにフォワーダーを設定してください。
- HVFP/HDI で使用するテナントの作成を HCP 管理者に依頼してください。

外部サーバの環境設定

HVFP/HDI のシステムを運用・管理するためには、ネットワーク上に幾つかの外部サーバを設置する必要があります。

この章では、外部サーバの環境設定について説明します。

- 3.1 HVFP/HDI で必要な外部サーバ
- 3.2 管理サーバの環境設定
- 3.3 管理コンソールの環境設定
- 3.4 NIS サーバの環境設定
- 3.5 LDAP サーバの環境設定
- 3.6 ドメインコントローラーの環境設定
- 3.7 KDC サーバの環境設定
- 3.8 RADIUS サーバの環境設定
- 3.9 SNMP マネージャーの環境設定
- 3.10 NTP サーバの環境設定
- 3.11 スキャンサーバの環境設定
- 3.12 ノードに SAN で接続されたテープ装置の環境設定
- 3.13 SMTP サーバの環境設定
- 3.14 ALog マネージャーサーバの環境設定
- 3.15 DHCP サーバの環境設定
- 3.16 DNS サーバの環境設定

3.1 HVFP/HDI で必要な外部サーバ

HVFP/HDI で必要な外部サーバを次の表にまとめます。

表 3-1 HVFP/HDI で必要な外部サーバ

外部サーバ	説明	HVFP/HDI と連携するために必要な設定情報
ALog マネージャサーバ	ALog ConVerter を使用して、NFS 共有以外へのユーザーアクセスを記録した監査ログを管理する場合に必要です。	<ul style="list-style-type: none"> IP アドレスまたはホスト名 FTP ユーザー名およびパスワード
DHCP サーバ	HDI の場合に、DHCP を利用して、ノードの IP アドレスやデフォルトゲートウェイなどのネットワーク情報を設定するときに必要です。	なし
DNS サーバ	DNS を利用してホスト名を検索する場合に必要です。Virtual Server を運用する場合は、Physical Node および Virtual Server でそれぞれ登録してください。	IP アドレス
FTP サーバ	ダンプファイル、Virtual Server の設定情報、および Physical Node と Virtual Server の全ログファイルをダウンロードする場合に必要です。転送先のディレクトリを作成してください。	<ul style="list-style-type: none"> IP アドレスまたはホスト名 ユーザー名およびパスワード 転送先のディレクトリ
KDC サーバ	NFS サービスで Kerberos 認証を利用してユーザーを認証する場合に必要なサーバです。Virtual Server を運用する場合は、Virtual Server ごとに登録してください。	<ul style="list-style-type: none"> サーバ名 ドメイン名
LDAP サーバ	LDAP サーバでユーザー情報を管理する場合に必要です。Virtual Server を運用する場合は、Virtual Server ごとに登録してください。ユーザー認証用の LDAP サーバは、NFSv4 ドメインでの ID マッピング用のサーバとしても利用できます。	<ul style="list-style-type: none"> IP アドレスまたはホスト名 ポート番号 ルート識別名 (DN 形式) 管理者名 (DN 形式) およびパスワード
	自動的に割り当てられたユーザー ID やグループ ID の情報を LDAP サーバのデータベースに格納する場合に必要です。Virtual Server を運用する場合は、Virtual Server ごとに登録してください。	<ul style="list-style-type: none"> IP アドレスまたはホスト名 ポート番号 ルート識別名 (DN 形式) ユーザーマッピングアカウントを追加する識別名 (DN 形式) 管理者名 (DN 形式) およびパスワード
NIS サーバ	NIS を利用してユーザーおよびホストの情報を検索する場合に必要です。Virtual Server を運用する場合は、Physical Node および Virtual Server でそれぞれ登録してください。	<ul style="list-style-type: none"> ドメイン名 IP アドレスまたはホスト名 (特定のサーバを使用する場合)
NTP サーバ	NTP サーバを利用して正しい時刻を Physical Node に反映させる場合に必要です。	IP アドレスまたはホスト名
SNMP マネージャ	SNMP を利用してシステム情報を参照したり、障害通知を受けたりする場合に必要です。Virtual Server を運用する場合は、Virtual Server ごとに登録してください。なお、SNMP マネージャは、管理 LAN に接続してください。	SNMPv2 を使用する場合 <ul style="list-style-type: none"> コミュニティ名 IP アドレスまたはサーバ名 SNMPv3 を使用する場合 <ul style="list-style-type: none"> ユーザー名 セキュリティレベル 認証種別および認証パスワード 暗号化種別および暗号用パスワード

外部サーバ	説明	HVFP/HDI と連携するために必要な設定情報
SMTP サーバ	E-mail を利用して障害通知を受ける場合に必要です。Virtual Server を運用する場合は、Virtual Server ごとに登録してください。なお、SMTP サーバは、フロントエンド LAN に接続してください。	<ul style="list-style-type: none"> SMTP サーバの IP アドレスまたはホスト名 (FQDN) ポート番号 E-mail の送信先アドレス E-mail の送信元アドレス E-mail の返信先アドレス 通知する障害のメッセージレベル
WINS サーバ	CIFS クライアントが WINS を利用して名前解決する場合に必要です。Virtual Server を運用する場合は、Virtual Server ごとに登録してください。なお、HVFP/HDI では WINS クライアント機能をサポートしていないため、Physical Node または Virtual Server の仮想 IP アドレスと NetBIOS 名は、WINS サーバに手動で登録してください。	なし
スキャンサーバ	リアルタイムスキャン機能を利用する場合に必要です。Virtual Server を運用する場合は、Virtual Server ごとに最大 32 台登録できます。	<ul style="list-style-type: none"> IP アドレスまたはホスト名 ポート番号
ドメインコントローラー	HVFP/HDI が、Active Directory 認証または NT ドメイン認証を利用してユーザーを認証する場合に必要です。Virtual Server を運用する場合は、Virtual Server ごとに登録してください。	<ul style="list-style-type: none"> サーバ名 管理者名およびパスワード
	Active Directory スキーマ方式のユーザーマッピングを使用する場合に必要です。Virtual Server を運用する場合は、Virtual Server ごとに登録してください。	ネームサービススイッチ (SFU または RFC2307 スキーマ)
	NFSv4 ドメインで ID マッピングする場合に必要です。Virtual Server を運用する場合は、Virtual Server ごとに登録してください。	<ul style="list-style-type: none"> サーバ名 管理者名およびパスワード ネームサービススイッチ (SFU または RFC2307 スキーマ)
プロキシサーバ	HVFP/HDI と HCP 間の http または https 通信を中継する場合に必要です。Virtual Server を運用する場合は、Virtual Server ごとに登録してください。	<ul style="list-style-type: none"> IP アドレスまたはホスト名 ポート番号 ユーザー名およびパスワード (ユーザー認証する場合)
管理コンソール	HVFP/HDI の GUI またはコマンドを使用する際に必要なマシンです。	なし
管理サーバ	Hitachi File Services Manager がインストールされたマシンです。管理サーバは管理コンソールとしても使用できます。	なし

3.2 管理サーバの環境設定

ここでは、管理サーバの環境設定について説明します。

3.2.1 管理サーバのマシン要件

管理サーバのマシン要件を次に示します。

表 3-2 管理サーバのマシン要件

項目	要件
適用 OS	<ul style="list-style-type: none"> • Microsoft(R) Windows(R) 7 Enterprise (SP なし, または SP1) • Microsoft(R) Windows(R) 7 Enterprise x64 Edition (SP なし, または 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) 7 Ultimate x64 Edition (SP なし, または SP1) • Microsoft(R) Windows(R) 8 32-bit^{※1} • Microsoft(R) Windows(R) 8 64-bit^{※1} • Microsoft(R) Windows(R) 8 Enterprise 32-bit^{※1} • Microsoft(R) Windows(R) 8 Enterprise 64-bit^{※1} • Microsoft(R) Windows(R) 8 Pro 32-bit^{※1} • Microsoft(R) Windows(R) 8 Pro 64-bit^{※1} • Microsoft(R) Windows(R) XP Professional Edition (SP3) • Microsoft(R) Windows(R) Vista Business 32-bit (SP1 または SP2) • Microsoft(R) Windows(R) Vista Business 64-bit (SP1 または SP2) • Microsoft(R) Windows(R) Vista Enterprise 32-bit (SP1 または SP2) • Microsoft(R) Windows(R) Vista Enterprise 64-bit (SP1 または SP2) • Microsoft(R) Windows(R) Vista Ultimate 32-bit (SP1 または SP2) • Microsoft(R) Windows(R) Vista Ultimate 64-bit (SP1 または SP2) • Microsoft(R) Windows Server(R) 2003, Datacenter Edition (SP1 または SP2) • Microsoft(R) Windows Server(R) 2003, Datacenter x64 Edition (SP1 または SP2) • Microsoft(R) Windows Server(R) 2003, Enterprise Edition (SP1 または SP2) • Microsoft(R) Windows Server(R) 2003, Enterprise x64 Edition (SP1 または SP2) • Microsoft(R) Windows Server(R) 2003, Standard Edition (SP1 または SP2) • Microsoft(R) Windows Server(R) 2003, Standard x64 Edition (SP1 または SP2) • Microsoft(R) Windows Server(R) 2003 R2, Datacenter Edition (SP なし, または SP2) • Microsoft(R) Windows Server(R) 2003 R2, Datacenter x64 Edition (SP なし, または SP2) • Microsoft(R) Windows Server(R) 2003 R2, Enterprise Edition (SP なし, または SP2) • Microsoft(R) Windows Server(R) 2003 R2, Enterprise x64 Edition (SP なし, または SP2) • Microsoft(R) Windows Server(R) 2003 R2, Standard Edition (SP なし, または SP2) • Microsoft(R) Windows Server(R) 2003 R2, Standard x64 Edition (SP なし, または SP2) • Microsoft(R) Windows Server(R) 2008 Datacenter 32-bit (SP1 または SP2) • Microsoft(R) Windows Server(R) 2008 Datacenter 64-bit (SP1 または SP2) • Microsoft(R) Windows Server(R) 2008 Enterprise 32-bit (SP1 または SP2) • Microsoft(R) Windows Server(R) 2008 Enterprise 64-bit (SP1 または SP2) • Microsoft(R) Windows Server(R) 2008 Standard 32-bit (SP1 または SP2) • Microsoft(R) Windows Server(R) 2008 Standard 64-bit (SP1 または SP2)

項目	要件
	<ul style="list-style-type: none"> Microsoft(R) Windows Server(R) 2008 R2 Datacenter (SPなし, または SP1) 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^{※1} Microsoft(R) Windows Server(R) 2012 Standard^{※1}
CPU	最小構成 Dual-Core プロセッサ 推奨構成 Quad-Core 以上のプロセッサ
メモリー容量	最小値 2GB 推奨値 4GB 以上 ^{※2}
空きディスク容量	最小値 4GB 推奨値 5GB 以上
LAN カード	10/100Ethernet LAN カード マシン本体や LAN ケーブルがギガビット対応の場合, ギガビットクラスの LAN カードも使用できます。
DVD-ROM ドライブ	必須

注※1

ユーザーインターフェースとして「モダン UI」と「デスクトップ」が用意されていますが、「デスクトップ」を使用してください。

注※2

ほかのソフトウェア製品と同時に使用する場合, 各ソフトウェア製品の値を合計したメモリー容量が必要です。

なお, 管理サーバに十分な仮想メモリーが確保されていないと, プログラムの動作が不安定になったり, 起動しなくなったりすることがあります。Hitachi File Services Manager を安定して動作させるには, OS やほかのプログラムで使用する仮想メモリーに加えて, 次に示す仮想メモリーが必要です。

表 3-3 Hitachi File Services Manager に必要な仮想メモリー容量

プログラム	仮想メモリー容量(MB)	
Hitachi File Services Manager		1,024
Hitachi Command Suite 共通コンポーネント	Hitachi Command Suite 共通コンポーネントのメモリーヒープサイズが Small の場合	1,524
	Hitachi Command Suite 共通コンポーネントのメモリーヒープサイズが Medium の場合	1,780
	Hitachi Command Suite 共通コンポーネントのメモリーヒープサイズが Large の場合	2,292

また、管理サーバに Hitachi Command Suite 製品をインストールした場合は、その分の仮想メモリーも必要です。Hitachi Command Suite 製品のバージョン 7.6.0 時点での、各製品の仮想メモリーの推奨値を次に示します。これらを合計した値より大きい容量の仮想メモリーを確保してください。

表 3-4 Hitachi Command Suite 製品の仮想メモリーの推奨値

製品名	仮想メモリー容量(MB)	
Hitachi Command Suite ^{※1} <ul style="list-style-type: none"> • Device Manager • Tiered Storage Manager • Replication Manager • Host Data Collector 	Device Manager のメモリーヒープサイズが Small の場合	3,300
	Device Manager のメモリーヒープサイズが Medium の場合	3,500
	Device Manager のメモリーヒープサイズが Large の場合	3,900
Tuning Manager		1,500
Global Link Manager		300
Compute Systems Manager		2,500
Hitachi Storage Navigator Modular 2 ^{※2}		200

注※1

Device Manager, Tiered Storage Manager, Replication Manager および Host Data Collector は常に一緒にインストールされます。

注※2

Hitachi Storage Navigator Modular 2 はバージョン 23.50 時点での仮想メモリー容量です。最新の仮想メモリー容量については、Hitachi Storage Navigator Modular 2 のマニュアルを参照してください。



参考

- 管理サーバに、Device Manager エージェントをインストールしている場合には、Device Manager エージェントに必要な仮想メモリーを確保する必要があります。Device Manager エージェントの仮想メモリーの値は `server.agent.maxMemorySize` プロパティで設定してください。`server.agent.maxMemorySize` プロパティについては、「Hitachi Command Suite Software システム構成ガイド」を参照してください。
- 管理サーバに、Replication Manager Application エージェントをインストールしている場合には、Replication Manager Application エージェントに必要な仮想メモリーを確保する必要があります。仮想メモリーの値については、「Hitachi Command Suite Replication Manager Software システム構成ガイド」を参照してください。
- 管理サーバに、Tuning Manager シリーズのエージェントをインストールしている場合には、各エージェントに必要な仮想メモリーを確保する必要があります。仮想メモリーの値については、各エージェントのマニュアルに記載されているメモリー所要量の説明を参照してください。

3.2.2 管理サーバのクラスタ構成

管理サーバは、Active-Standby 型のクラスタリングに対応しています。クラスタを構成するそれぞれのサーバのうち、業務を実行しているサーバを実行系ノード、実行系ノードの障害時に業務を引き継げるよう待機しているサーバを待機系ノードと呼びます。

実行系ノードで障害が発生した場合、クラスタソフトウェアが異常を検知して、待機系ノードを実行系に切り替えます。これによって、業務を中断することなく管理サーバを運用できます。

クラスタ構成で管理サーバを運用する場合の適用 OS と、必要なクラスタソフトウェアを次に示します。

表 3-5 クラスタ構成で管理サーバを運用する場合の適用 OS とクラスタソフトウェア

適用 OS	クラスタソフトウェア
Microsoft(R) Windows Server(R) 2003, Enterprise Edition Operating System [※]	Microsoft Cluster Service
Microsoft(R) Windows Server(R) 2003 R2, Enterprise Edition [※]	Microsoft Cluster Service
Microsoft(R) Windows Server(R) 2008 Enterprise Edition Operating System	Microsoft Failover Cluster
Microsoft(R) Windows Server(R) 2012 Datacenter Microsoft(R) Windows Server(R) 2012 Standard	Microsoft Failover Cluster

注※

使用できるアーキテクチャーは、x86 だけです。

3.2.3 コマンドプロンプトからの管理者権限でのコマンド実行

Windows Vista をはじめ、UAC 機能を持つ Windows OS で UAC が有効になっている場合、コマンドプロンプトからコマンドを実行するときに、管理者権限に昇格して実行しなければならないコマンドがあります。管理サーバのコマンドプロンプトからマニュアルに記載されているコマンドを実行する場合は、特別な注意書きがないかぎり、管理者権限に昇格して実行してください。

管理者権限に昇格してコマンドを実行するには、次に示す 2 つの方法があります。コマンドプロンプトの出力結果が確実に参照できるように、1 の方法でコマンドを実行することを推奨します。

1. 管理者権限に昇格済みのコマンドプロンプトでコマンドを実行する（推奨）。

Windows 7 までの Windows の場合、スタートメニューからコマンドプロンプトのアイコンを選択し、右クリックメニューから [管理者として実行] を選択すると、管理者権限に昇格済みのコマンドプロンプトが開かれます。

Windows 8 または Windows Server 2012 の場合、「デスクトップ」画面左下の角にマウスカーソルを移動して小さな「スタート」画面を右クリックし、「管理メニュー」から「コマンドプロンプト（管理者）」を選択すると、管理者権限に昇格済みのコマンドプロンプトが開かれます。

2. 通常のコマンドプロンプトからコマンドを実行し、管理者への昇格要求メッセージを承認する。管理者権限に昇格して実行していない通常のコマンドプロンプトからコマンドを実行すると、管理者権限への昇格要求メッセージが表示されます。昇格要求を承認してください。

ただし、この方法の場合、コマンドプロンプトに出力されるコマンドの実行結果が、コマンドを実行したコマンドプロンプトとは別のコマンドプロンプトに表示されます。また、その実行結果が表示されたコマンドプロンプトは自動的に閉じられます。

管理者への昇格要求メッセージを承認しなかった場合、コマンドは実行されませんが、リターンコードが 0（正常終了）でコマンドの実行を終了します。

参考：

Windows のスタートメニュー（Windows 8 または Windows Server 2012 の場合はスタート画面のアプリ一覧）から次の表に示す操作をする場合も、メニュー項目のアイコンを選択し、右クリックメニューから [管理者として実行] を選択してください。

表 3-6 Windows のスタートメニュー（Windows 8 または Windows Server 2012 の場合はスタート画面のアプリ一覧）からの操作とメニュー項目

操作	メニュー項目
Hitachi File Services Manager の起動	[Start - HFSM]
Hitachi File Services Manager の停止	[Stop - HFSM]

操作	メニュー項目
Hitachi File Services Manager の稼働状態の確認	[Status - HFSM]
Hitachi File Services Manager のログ取得	[Get Logs - HFSM]
Hitachi File Services Manager のアンインストール	[Uninstall - HFSM]

3.3 管理コンソールの環境設定

ここでは、管理コンソールの環境設定について説明します。

3.3.1 管理コンソールのマシン要件

管理コンソールに使用するマシンの要件を次に示します。なお、HVFP/HDI の管理コンソールで HCP の GUI を使用する場合、管理コンソールは HCP のコンソールとしてのマシン要件も満たしている必要があります。HCP のコンソールとしてのマシン要件については、HCP のドキュメントを参照してください。

表 3-7 管理コンソールのマシン要件

項目	要件
OS	<ul style="list-style-type: none"> • Microsoft(R) Windows(R) 7 Enterprise (SP なし, または SP1) • Microsoft(R) Windows(R) 7 Enterprise x64 Edition (SP なし, または 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) 7 Ultimate x64 Edition (SP なし, または SP1) • Microsoft(R) Windows(R) 8 32-bit^{※1} • Microsoft(R) Windows(R) 8 64-bit^{※1} • Microsoft(R) Windows(R) 8 Enterprise 32-bit^{※1} • Microsoft(R) Windows(R) 8 Enterprise 64-bit^{※1} • Microsoft(R) Windows(R) 8 Pro 32-bit^{※1} • Microsoft(R) Windows(R) 8 Pro 64-bit^{※1} • Microsoft(R) Windows(R) 8.1 32-bit^{※1} • Microsoft(R) Windows(R) 8.1 64-bit^{※1} • Microsoft(R) Windows(R) 8.1 Enterprise 32-bit^{※1} • Microsoft(R) Windows(R) 8.1 Enterprise 64-bit^{※1} • Microsoft(R) Windows(R) 8.1 Pro 32-bit^{※1} • Microsoft(R) Windows(R) 8.1 Pro 64-bit^{※1} • Microsoft(R) Windows(R) XP Professional Edition (SP3) • Microsoft(R) Windows(R) Vista Business 32-bit (SP1 または SP2) • Microsoft(R) Windows(R) Vista Business 64-bit (SP1 または SP2) • Microsoft(R) Windows(R) Vista Enterprise 32-bit (SP1 または SP2) • Microsoft(R) Windows(R) Vista Enterprise 64-bit (SP1 または SP2) • Microsoft(R) Windows(R) Vista Ultimate 32-bit (SP1 または SP2) • Microsoft(R) Windows(R) Vista Ultimate 64-bit (SP1 または SP2) • Microsoft(R) Windows Server(R) 2003, Datacenter Edition (SP1 または SP2) • Microsoft(R) Windows Server(R) 2003, Datacenter x64 Edition (SP1 または SP2) • Microsoft(R) Windows Server(R) 2003, Enterprise Edition (SP1 または SP2)

項目	要件
	<ul style="list-style-type: none"> • Microsoft(R) Windows Server(R) 2003, Enterprise x64 Edition (SP1 または SP2) • Microsoft(R) Windows Server(R) 2003, Standard Edition (SP1 または SP2) • Microsoft(R) Windows Server(R) 2003, Standard x64 Edition (SP1 または SP2) • Microsoft(R) Windows Server(R) 2003 R2, Datacenter Edition (SP なし, または SP2) • Microsoft(R) Windows Server(R) 2003 R2, Datacenter x64 Edition (SP なし, または SP2) • Microsoft(R) Windows Server(R) 2003 R2, Enterprise Edition (SP なし, または SP2) • Microsoft(R) Windows Server(R) 2003 R2, Enterprise x64 Edition (SP なし, または SP2) • Microsoft(R) Windows Server(R) 2003 R2, Standard Edition (SP なし, または SP2) • Microsoft(R) Windows Server(R) 2003 R2, Standard x64 Edition (SP なし, または SP2) • Microsoft(R) Windows Server(R) 2008 Datacenter 32-bit (SP1 または SP2) • Microsoft(R) Windows Server(R) 2008 Datacenter 64-bit (SP1 または SP2) • Microsoft(R) Windows Server(R) 2008 Enterprise 32-bit (SP1 または SP2) • Microsoft(R) Windows Server(R) 2008 Enterprise 64-bit (SP1 または SP2) • Microsoft(R) Windows Server(R) 2008 Standard 32-bit (SP1 または SP2) • Microsoft(R) Windows Server(R) 2008 Standard 64-bit (SP1 または SP2) • Microsoft(R) Windows Server(R) 2008 R2 Datacenter (SP なし, または SP1) • 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^{※1} • Microsoft(R) Windows Server(R) 2012 Standard^{※1} • Microsoft(R) Windows Server(R) 2012 R2 Datacenter^{※1} • Microsoft(R) Windows Server(R) 2012 R2 Standard^{※1} • Red Hat Enterprise Linux(R) 5.6^{※2} • Red Hat Enterprise Linux(R) 5.6 Advanced Platform^{※2} • Red Hat Enterprise Linux(R) 6.4^{※2}
メモリー	512MB 以上
CPU	管理コンソールにインストールする OS の推奨 CPU
モニターの解像度	1,024×768 ピクセル以上
モニターの表示色	16,777,216 色 (True color, 32 ビット) 以上
WWW ブラウザー ^{※3}	<p>次の WWW ブラウザーを使用できます。</p> <ul style="list-style-type: none"> • Internet Explorer 7.0 (SP なし, 32 ビット版) • Internet Explorer 8.0 (SP なし, 32 ビット版) • Internet Explorer 9.0 (SP なし, 32 ビット版) • Internet Explorer 10.0 (SP なし, 32 ビット, デスクトップ版) • Internet Explorer 11.0^{※4} (SP なし, 32 ビット, デスクトップ版) • Firefox 3.6.x^{※5} (x86 版, OS が Red Hat Enterprise Linux(R)の場合) • Firefox ESR 10.0.x^{※5} (x86 版, OS が Red Hat Enterprise Linux(R)の場合)

項目	要件
	<ul style="list-style-type: none"> Firefox ESR 17.0.x^{※5} (x86 版, OS が Red Hat Enterprise Linux(R)の場合) Firefox ESR 24.1.x^{※5} (x86 版, OS が Red Hat Enterprise Linux(R)の場合)

注※1

ユーザーインターフェースとして「モダン UI」と「デスクトップ」が用意されていますが、「デスクトップ」を使用してください。

注※2

UPnP (Universal Plug and Play) を使用した HDI へのログインはできません。

注※3

Hitachi File Services Manager から Hitachi Storage Navigator Modular 2 の GUI を表示する場合は、Hitachi Storage Navigator Modular 2 の WWW ブラウザーの要件も満たしている必要があります。Hitachi Storage Navigator Modular 2 のドキュメントで、対応する WWW ブラウザーを確認してください。

注※4

Internet Explorer 11.0 を使用する場合、画面上のアンカーまたはボタンのクリックによって、別のウィンドウまたはタブを開く操作をすると、不要なウィンドウ（空白や遷移途中のウィンドウ）が同時に表示されることがあります。この場合、不要なウィンドウを閉じてください。この問題が繰り返し発生する場合は、新しい Windows のユーザーアカウントを作成し、新しいユーザーでブラウザを操作してください。

注※5

x は末尾のバージョン番号に依存しないことを示します。

3.3.2 管理コンソールで Internet Explorer を使用する場合の設定

ここでは、WWW ブラウザーに Internet Explorer を使用する場合の設定について説明します。WWW ブラウザーの設定を変更する場合は、すべてのブラウザを閉じてから実施してください。なお、ここでは Internet Explorer 7.0 の設定を例に説明します。使用している Internet Explorer のバージョンが異なっている場合の設定は、Internet Explorer のヘルプを参照してください。

(1) Internet Explorer を使用する場合の注意事項

Internet Explorer を使用する場合の注意事項を次に示します。

- タブブラウジング機能は使用できません。
- 一部のダイアログで証明書エラーやセキュリティの警告が表示されることがあります。
HVFP/HDI では、ノードと管理コンソールの間で https 通信を行うため、証明書エラーやセキュリティの警告が表示されても問題ありません。
- メニューバーの表示有無の設定を変更すると、正しく動作しないことがあります。
- フォントサイズを拡大または縮小すると、GUI 表示が乱れたり、スクロールバーが表示されなくなったりすることがあります。

(2) Internet Explorer の設定

Internet Explorer を使用する場合に設定する項目を次の表に示します。表に示したもの以外については、Internet Explorer のデフォルト設定をそのまま使用してください。

表 3-8 Internet Explorer の設定

種別	設定内容
文字サイズの設定	「中」に設定する
キャッシュの設定※1	[Web サイトを表示するたびに確認する] ラジオボタンを選択する
信頼済みサイトゾーンへの URL の設定※2	<ul style="list-style-type: none"> ・ [このゾーンの世界にはすべてサーバの確認 (https:) を必要とする] チェックボックスのチェックを外す ・ [この Web サイトをゾーンに追加する] テキストボックスに、管理サーバと管理対象の全ノードや全 Virtual Server の URL, about:internet を追加する※3
ポップアップブロックの設定※4	[許可する Web サイトのアドレス] テキストボックスに、管理サーバと管理対象の全ノードや全 Virtual Server の URL を追加する※3
ダウンロード防止機能の設定※5	<ul style="list-style-type: none"> ・ [ファイルのダウンロード] を有効にする ・ [ファイルのダウンロード時に自動的にダイアログを表示] を有効にする (Internet Explorer 7.0 または Internet Explorer 8.0 を使用する場合) ・ [暗号化されたページをディスクに保存しない] チェックボックスのチェックを外す
セキュリティの設定	<ul style="list-style-type: none"> ・ [ActiveX コントロールとプラグインの実行] を有効にする ・ [スクリプトを実行しても安全だとマークされている ActiveX コントロールのスクリプト実行] を有効にする ・ [アクティブスクリプト] を有効にする ・ [IFRAME のプログラムとファイルの起動] を有効にするか、または [ダイアログを表示する] を指定する ・ [暗号化されていないフォームデータの送信] を有効にするか、または [ダイアログを表示する] を指定する
アニメーションの再生の設定	[Web ページのアニメーションを再生する] チェックボックスをチェックする
プロキシの設定※6	プロキシサーバを使用している場合、[プロキシの設定] ダイアログの [例外] テキストボックスに、管理サーバと管理対象の全ノードや全 Virtual Server のアドレスを追加する
タブブラウザの設定	[常に新しいタブでポップアップを開く] 以外のラジオボタンを選択する
拡張保護モードの設定	[拡張保護モードを有効にする] チェックボックスのチェックを外す (Internet Explorer 10.0 以降を使用する場合)

注※1

キャッシュの設定が異なると、File Services Manager や、ノード上で動作するプログラムをバージョンアップした場合に、古いバージョンの GUI が表示されたり、GUI がフリーズしたりするおそれがあります。

注※2

Internet Explorer セキュリティ強化の構成機能が有効になっていると、GUI 操作が制限されることがあります。

この場合は、管理サーバと管理対象の全ノードや全 Virtual Server の URL、および about:internet を、Internet Explorer でセキュリティゾーンの信頼済みサイトゾーンに登録してください。

注※3

URL の指定形式を次に示します。

- 管理サーバの場合

http://<管理サーバの IP アドレスまたはホスト名>

- ノードの場合
クラスタ構成の場合：
https://< Physical Node の管理ポートの固有 IP アドレス>
https://< Physical Node の管理ポートの仮想 IP アドレス>
シングルノードの場合：
https://<管理ポートの IP アドレス>
- Virtual Server の場合
https://< Virtual Server の管理 IP アドレス>
- about:internet

注※4

WWW ブラウザーのポップアップブロックが有効になっていると、ログイン画面が表示されなかったり、操作がエラーになったりすることがあります。このため、ポップアップがブロックされないようあらかじめ設定してください。

注※5

ダウンロード防止機能が有効になっていると、GUI を使用して障害情報や設定情報ファイルなどをダウンロードできません。

また、ダウンロード元となるノードおよび Virtual Server を信頼済みサイトとして登録しておく必要があります。

注※6

プロキシサーバを使用している場合、管理サーバと管理対象の全ノードや全 Virtual Server を例外として設定しておかないと、正しい GUI が表示されません。

3.3.3 管理コンソールで Firefox を使用する場合の設定

ここでは、WWW ブラウザーに Firefox を使用する場合の設定について説明します。WWW ブラウザーの設定を変更する場合は、すべてのブラウザを閉じてから実施してください。

Firefox を使用する場合に設定する項目を次の表に示します。表に示したもの以外については、Firefox のデフォルト設定をそのまま使用してください。

表 3-9 Firefox の設定

種別	設定内容
キャッシュの設定※1	次に示す手順で設定します。 1. アドレスバーに about:config を入力して、設定項目の一覧を表示します。 2. 表示された設定項目の一覧から、 [browser.cache.check_doc_frequency] を選択して、ダブルクリックします。 3. 表示されたダイアログに 1 (意味はページを表示するごとにページの更新を確認する) を入力して、[OK] ボタンをクリックします。
ポップアップブロックの設定※2	[Firefox の設定] ダイアログの [コンテンツ] タブで、[ポップアップウィンドウをブロックする] の [許可サイト] ボタンをクリックし、[サイトのアドレス] テキストボックスに次の IP アドレスを指定します。 <ul style="list-style-type: none"> • 管理サーバの IP アドレス • 管理対象の全ノードの固有 IP アドレス • 管理対象の全 Virtual Server の管理 IP アドレス
アドオンの設定※3	[Firefox の設定] ダイアログの [セキュリティ] タブで、[アドオンのインストールを求められたときに警告する] の [許可サイト] ボタン

種別	設定内容
	<p>をクリックし、[サイトのアドレス] テキストボックスに次の IP アドレスを指定します。</p> <ul style="list-style-type: none"> 管理サーバの IP アドレス 管理対象の全ノードの固有 IP アドレス 管理対象の全 Virtual Server の管理 IP アドレス
JavaScript の設定※3	<p>[Firefox の設定] ダイアログの [コンテンツ] タブで次のように設定します。</p> <p>JavaScript を有効にする チェックボックスをチェックします。</p>
セキュリティ例外の承認	<p>管理サーバ、管理対象のノードおよび Virtual Server にアクセスした際やこれらからファイルをダウンロードしようとした際などに「接続の安全性を確認できません」が表示されたら、次に示す手順でセキュリティ例外として承認してください。</p> <ol style="list-style-type: none"> [危険性を理解した上で接続するには] をクリックします。 [例外を追加] ボタンをクリックします。 [URL] に表示される管理サーバ、管理対象のノードおよび Virtual Server のサイトが間違いではないことを確認し、[セキュリティ例外を承認] ボタンをクリックします。
操作画面を適切に閉じる設定※4	<p>次に示す手順で設定します。</p> <ol style="list-style-type: none"> アドレスバーに about:config を入力して、設定項目の一覧を表示します。 表示された設定項目の一覧から、[dom.allow_scripts_to_close_windows] を選択して、ダブルクリックします。 設定が初期値の false から true に切り替わるのを確認して、[OK] ボタンをクリックします。
プロキシの設定※5	<p>プロキシサーバを使用している場合、[Firefox の設定] ダイアログ [詳細] パネルの [ネットワーク] タブで [接続] の [接続設定] ボタンをクリックし、[プロキシなしで接続] テキストボックスに次のアドレスを指定します。</p> <ul style="list-style-type: none"> 管理サーバの IP アドレス 管理対象の全ノードの固有 IP アドレス 管理対象の全 Virtual Server の管理 IP アドレス

注※1

キャッシュの設定が異なると、File Services Manager や、ノード上で動作するプログラムをバージョンアップした場合に、古いバージョンの GUI が表示されたり、GUI がフリーズしたりするおそれがあります。

注※2

WWW ブラウザーのポップアップブロックが有効になっていると、ログイン画面が表示されなかったり、操作がエラーになったりすることがあります。このため、ポップアップがブロックされないようにあらかじめ設定してください。

注※3

設定していないと、HVFP/HDI の GUI が正しく動作しないことがあります。

注※4

設定していないと、操作時に開いた画面が閉じないことがあります。

注※5

プロキシサーバを使用している場合、管理サーバと管理対象の全ノードや全 Virtual Server を例外として設定しておかないと、正しい GUI が表示されません。

3.4 NIS サーバの環境設定

HVFP/HDI では、UNIX マシンのほか、ドメインコントローラーを NIS サーバとして利用できません。

NIS サーバで HVFP/HDI のユーザー情報を管理する際の注意事項を次に示します。

- ユーザー名およびグループ名に使用できる文字は、1 文字目には英数字、2 文字目以降は英数字、ハイフン (-) およびアンダーライン (_) です。
- File Services Manager およびユーザー認証用の LDAP サーバで登録されたユーザー名、グループ名、ユーザー ID およびグループ ID と重複しないようにしてください。File Services Manager で登録されたユーザー名、グループ名、ユーザー ID およびグループ ID と重複していると、そのユーザーおよびグループには Quota を設定できません。
- CIFS クライアントに対してユーザーマッピングを使用する場合は、ユーザーマッピングで設定した範囲内のユーザー ID およびグループ ID は使用できません。
- File Services Manager のエンドユーザーサービス機能を利用する場合は、DES または MD5 アルゴリズムでパスワードが暗号化されている必要があります。

NFSv4 ドメインを利用して HVFP/HDI を運用している場合は、HVFP/HDI で使用する NIS サーバを ID マッピング用のサーバとして利用できます。

3.5 LDAP サーバの環境設定

HVFP/HDI で LDAP サーバを利用する場合、サーバを構築するための要件は次のとおりです。

ユーザー認証用の LDAP サーバを構築する場合

サーバを構築するために必要な製品は次のとおりです。どれか 1 つを使用して LDAP サーバを構築してください。

- OpenLDAP
- Sun Java System Directory Server

ユーザー認証用として構築された LDAP サーバは、NFSv4 ドメインでの ID マッピング用のサーバとしても利用できます。

ユーザーマッピング用の LDAP サーバを構築する場合

サーバを構築するために必要な製品は次のとおりです。どれか 1 つを使用して LDAP サーバを構築してください。

- OpenLDAP
- Sun Java System Directory Server
- ADAM

システム管理者のアカウント認証用の LDAP サーバを構築する場合（外部認証サーバとだけ連携するとき）

LDAP v3 に準拠しているソフトウェアを使用する必要があります。

システム管理者のアカウント認証用の LDAP サーバを構築する場合（外部認可サーバとも連携するとき）

次の要件を満たした外部認証サーバと外部認可サーバが同一マシンで稼働している必要があります。

前提 OS

- Windows Server 2003

- Windows Server 2003 R2
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012

ソフトウェア

Active Directory

プロトコル

LDAP v3

3.5.1 LDAP サーバを利用する際の注意事項

LDAP サーバを利用する際の注意事項は次のとおりです。

ユーザー認証用の LDAP サーバを利用する場合

- ユーザー名およびグループ名に使用できる文字は、1文字目には英数字、2文字目以降は英数字、ハイフン (-) およびアンダーライン (_) です。
- File Services Manager および NIS サーバで登録されたユーザー名、グループ名、ユーザー ID およびグループ ID と重複しないようにしてください。File Services Manager で登録されたユーザー名、グループ名、ユーザー ID およびグループ ID と重複していると、そのユーザーおよびグループには Quota を設定できません。
- CIFS クライアントに対してユーザーマッピングを使用する場合は、ユーザーマッピングで設定した範囲内のユーザー ID およびグループ ID は使用できません。
- File Services Manager のエンドユーザーサービス機能を利用する場合は、DES、MD5、SMD5、SHA または SSHA のどれかのアルゴリズムでパスワードが暗号化されている必要があります。

ユーザーマッピング用の LDAP サーバを利用する場合

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です。CIFS 共有にアクセスしているユーザーがないことを確認してから、[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てください。

再起動後に、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。

3.5.2 OpenLDAP を使用する場合の注意事項

OpenLDAP を使用して LDAP サーバを構築するときは、sizelimit ディレクティブの設定が必要です。

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、クラスタ構成の HVFP/HDI で [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、クラスタ構成の HVFP/HDI の [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
```

なお、ユーザー認証用の LDAP サーバを利用する場合、スキーマファイルを作成する必要はありません。

3.5.3 Sun Java System Directory Server を使用する場合の注意事項

Sun Java System Directory Server を使用して LDAP サーバを構築するときは、クライアント制限の設定が必要です。

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) ページ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、クラスタ構成の HVFP/HDI で [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、クラスタ構成の HVFP/HDI の [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 Microsystems 社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 を再起動するため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。

なお、ユーザー認証用の LDAP サーバを利用する場合、スキーマファイルを作成する必要はありません。

3.5.4 ADAM を使用する場合の注意事項

ADAM を使用してユーザーマッピング用の LDAP サーバを構築するときは、検索制限数の設定が必要です。

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。

なお、サポート対象外のため、ユーザー認証用の LDAP サーバを構築する際に ADAM は使用できません。

3.5.5 OpenLDAP を使用する場合の設定例

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説明します。

(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、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.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 の数が増えると、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。index ディレクティブは、LDAP サーバの定義で、次のとおり設定することを推奨します。

ユーザー認証用の LDAP サーバの場合

```
index uidNumber,gidNumber,objectClass,uid,cn,memberUid eq
```

ユーザーマッピング用の LDAP サーバの場合

```
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。なお、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。

3.5.6 Sun Java System Directory Server を使用する場合の設定例

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説明します。

(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 <ホスト名> -p <ポート番号> -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)。ホスト名には、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、ポート番号には、Sun Java System Directory Server をインストールするときに設定した LDAP サーバの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 の定義で、次のとおり等価インデックスを設定することを推奨します。

ユーザー認証用の LDAP サーバの場合

uidNumber, gidNumber, memberUid, uid[※], cn[※]に等価インデックス (eq) を設定
注[※] デフォルトで、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用の LDAP サーバの場合

uidNumber, gidNumber, sambaSID に等価インデックス (eq) を設定

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 Microsystems 社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属性を選択し、[了解] をクリックします。

ユーザー認証用の LDAP サーバの場合

uidNumber, gidNumber, memberUid, uid[※], cn[※]を選択します。
注[※] デフォルトで、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用の LDAP サーバの場合

uidNumber, gidNumber, sambaSID を選択します。

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。

ユーザー認証用の LDAP サーバの場合

uidNumber, gidNumber, memberUid, uid 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不要とします。また, cn の [等価], [実在], [部分文字列] 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不要とします。

ユーザーマッピング用の LDAP サーバの場合

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不要とします。

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いないため, [何もしない] を選択します。

3.5.7 ADAM を使用する場合の設定例

ここでは, ADAM を使用してユーザーマッピング用の LDAP サーバを構築するときの設定例を説明します。

(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
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;;RPWPCRCDDCLCLORCWOWDSDDTSW;;;DA)(A;;RPWPCRCDDCLCLORCWOWDS
  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;;RPWPCRCDCCLCLORCWOWDSDDTSW;;;DA) (A;;RPWPCRCDCCLCLORCWOWDS
  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;;RPWPCRCDCCLCLORCWOWDSDDTSW;;;DA) (A;;RPWPCRCDCCLCLORCWOWDS
  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:<ポート番号> -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、<ポート番号>は ADAM をインストールするときに設定した LDAP ポート番号です。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 の数が増えると、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。

すでに別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。

3.6 ドメインコントローラーの環境設定

Active Directory スキーマ方式のユーザーマッピング用または NFSv4 ドメインでの ID マッピング用として利用する場合、ドメインコントローラーは次の条件を満たす必要があります。

Windows Server 2003 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, Windows Server 2008 または Windows Server 2012 のとき

Active Directory を構築します。なお、Windows Server 2003 R2, Windows Server 2008 で 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。

なお、この条件でバックアップドメインコントローラーを運用するときは、プライマリドメインコントローラーと同じネームサービススイッチ (SFU または RFC2307 スキーマ) を使用してください。

このほか、Active Directory スキーマ方式の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のポリシーで [ドメインコントローラー: LDAP サーバー署名必須] が [署名を必要とする] になっていないことを確認してください。

ドメインコントローラーのポリシーの確認方法は、認証サーバの OS によって異なります。

Windows Server 2003 の場合

[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、[セキュリティの設定] の [ローカル ポリシー] の [セキュリティオプション] の [ドメインコントローラ: LDAP サーバー署名必須] を確認します。

Windows Server 2008 または Windows Server 2012 の場合

[管理ツール] の [グループポリシー管理エディター] によって、[コンピュータの構成] の [ポリシー] の [Windows の設定] の「セキュリティの設定」で、[ローカル ポリシー] の [セキュリティオプション] の [ドメインコントローラ: LDAP サーバー署名必須] を確認します。

CIFS クライアントを認証するドメインコントローラーは、15 バイト以下のコンピュータ名を使用することを推奨します。15 バイトを超えるコンピュータ名を使用する場合は、15 バイトの名称でも HVFP/HDI で名前解決できるよう、コンピュータ名の 15 バイトを超える文字列を削除した名称を DNS または lmhosts などに登録してください。登録されていないと、CIFS サービスの起動やユーザー認証が正常に実施されません。各ドメインコントローラーに対するすべての名称は、システム内で一意にしてください。

また、CIFS サービスの認証に使用するドメインコントローラーで NTLMv2 認証を使用する場合には、ネットワークセキュリティの設定値が [NTLMv2 応答のみ送信 (LM と NTLM を拒否する)] になっていると、CIFS サービスの起動に失敗します。このため、別の値を設定してください。

ドメインコントローラーのネットワークセキュリティの設定方法は、認証サーバの OS によって異なります。

Windows Server 2003 の場合

[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, [セキュリティの設定] の [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] に設定します。

Windows Server 2008 または Windows Server 2012 の場合

[管理ツール] の [グループポリシー管理エディタ] によって, [コンピュータの構成] の [ポリシー] の [Windows の設定] の 「セキュリティの設定」 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] に設定します。

このほか, NFS サービスで Kerberos 認証を利用してユーザーを認証する場合は, Active Directory ドメインコントローラーを KDC サーバとして使用できます。KDC サーバの環境設定については, 「[3.7 KDC サーバの環境設定](#)」を参照してください。

3.7 KDC サーバの環境設定

KDC サーバを利用する場合, サーバを構築するための要件は次のとおりです。

ユーザー認証用の KDC サーバを構築する場合

UNIX マシンまたは Active Directory ドメインコントローラーを KDC サーバとして使用できます。

ただし, CIFS サービスの Active Directory 認証と NFS サービスの Kerberos 認証を同時に運用する場合は, Active Directory ドメインコントローラーを共有する必要があります。将来的に CIFS サービスでの Active Directory 認証を運用する予定がある場合は, 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ことを推奨します。

なお, UNIX マシンを KDC サーバとして使用している場合に, CIFS サービスの Active Directory 認証の運用を新たに開始するときは, KDC サーバの定義をいったん削除してください。そのあと, Active Directory 認証で使用する Active Directory ドメインコントローラーを KDC サーバとして再度定義してから, NFS サービスを再起動してください。

システム管理者のアカウント認証用の KDC サーバを構築する場合

KDC サーバとして使用するマシンは, 次の要件を満たす必要があります。なお, 外部認証サーバと外部認可サーバを併用するときは, 外部認証サーバと外部認可サーバを同一マシンで稼働させてください。

前提 OS

- Windows Server 2003
- Windows Server 2003 R2
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012

ソフトウェア

Active Directory

プロトコル

- 外部認証サーバ: Kerberos v5
- 外部認可サーバ: LDAP v3

3.8 RADIUS サーバの環境設定

RADIUS 認証方式でシステム管理者のユーザーアカウントを認証する場合、RADIUS サーバとして使用するマシンは、次の要件を満たす必要があります。

外部認証サーバとだけ連携するとき

PPP の認証プロトコルとして、RFC2865 に準拠した PAP または CHAP に対応している必要があります。

外部認可サーバとも連携するとき

次の要件を満たした外部認証サーバと外部認可サーバが必要です。なお、外部認証サーバと外部認可サーバは、同一マシンでも、別マシンでもかまいません。

外部認証サーバ

PPP の認証プロトコルとして、RFC2865 に準拠した PAP または CHAP に対応している必要があります。

外部認可サーバ

次の要件を満たす必要があります。

前提 OS :

- Windows Server 2003
- Windows Server 2003 R2
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012

ソフトウェア : Active Directory

プロトコル : LDAP v3

3.9 SNMP マネージャーの環境設定

ここでは、SNMP マネージャーの環境設定について説明します。

3.9.1 SNMP マネージャーとして使用するマシンの設定

SNMP マネージャーとして使用するマシンでは、文字コードを Unicode (UTF-8) に設定してください。なお、SNMP マネージャーで受信する Trap メッセージに非 ASCII 文字が含まれている場合は、メッセージが正しく表示されません。

3.9.2 specific-trap の設定

SNMP マネージャーで HVFP/HDI の specific-trap を設定すると、HVFP/HDI から発行された SNMP トラップを SNMP マネージャーで受信するかどうかを指定できます。運用方法に合わせて、必要な分だけ specific-trap を設定すれば、HVFP/HDI から発行された特定のトラップだけを SNMP マネージャーで受信することもできます。

HVFP/HDI の specific-trap の enterprise-OID は次のとおりです。

.1.3.6.1.4.1.116.3.11.5

HVFP/HDI の specific-trap を次の表に示します。

表 3-10 HVFP/HDI の specific-trap

ID	specific-trap	内容
0	stdTrapNotice	このトラップは無効です。
1	stdEventTrapFatalError	Fatal Error レベルのメッセージを受信しました。
2	stdEventTrapError	Error レベルのメッセージを受信しました。
3	stdEventTrapWarning	Warning レベルのメッセージを受信しました。
4	stdEventTrapInformation	Information レベルのメッセージを受信しました。
5	stdQuotaTrapFSSoftLimit	HVFP/HDI に設定された Quota のソフトリミットを超過したユーザーまたはグループが検出されました。
6	stdQuotaTrapFSLimitExceeded	HVFP/HDI に設定された Quota の猶予期間を超過したユーザーまたはグループが検出されました。
7	stdCoreTrap	core ファイルが検出されました。
8	stdQuotaTrapFSSummary	次のユーザーまたはグループが検出されました。 <ul style="list-style-type: none"> • HVFP/HDI に設定された Quota のソフトリミットを超過した • HVFP/HDI に設定された Quota の猶予期間を超過した
9	stdQuotaTrapFSDetailSuppress	HVFP/HDI に設定された、ファイルシステムごとの Quota の個別通知が抑止されました。
10	stdQuotaTrapFSSubtreeSoftLimit	HVFP/HDI に設定されたサブツリー Quota のソフトリミットの超過が検出されました。
11	stdQuotaTrapFSSubtreeLimitExceeded	HVFP/HDI に設定されたサブツリー Quota の猶予期間の超過が検出されました。
12	stdQuotaTrapFSSubtreeSummary	次のユーザー、グループまたはディレクトリが検出されました。 <ul style="list-style-type: none"> • HVFP/HDI に設定されたサブツリー Quota のソフトリミットを超過した • HVFP/HDI に設定されたサブツリー Quota の猶予期間を超過した
13	stdQuotaTrapFSSubtreeDetailSuppress	HVFP/HDI に設定された、ディレクトリごとのサブツリー Quota の個別通知が抑止されました。

3.9.3 日立固有 MIB オブジェクトの定義ファイルの取得方法

SNMP マネージャーに日立固有 MIB オブジェクトの MIB 定義ファイルを取り込む場合、HVFP/HDI とともに提供されるメディアからロードしてください。

注意：

SNMP マネージャーには、最新の MIB 定義ファイルをロードしてください。

古い MIB 定義ファイルがロードされていると、MIB オブジェクトの取得が SNMP マネージャーで正しく認識されないおそれがあります。

日立固有 MIB オブジェクトの MIB 定義ファイルのパスを次に示します。

```
¥etc¥snmp¥STD-EX-MIB.txt
```

MIB 定義ファイルをロードする手順については、利用している SNMP プログラムのドキュメントを参照してください。

なお、1 台の SNMP マネージャーで HVFP/HDI と Hitachi Essential NAS Platform を管理する場合に、Hitachi Essential NAS Platform の MIB グループ名およびオブジェクト名を使用して運用したいときは、Hitachi Essential NAS Platform のメディアに格納されている次の MIB 定義ファイルを使用してください。

```
¥etc¥snmp¥E-NAS-EX-MIB.txt
```

3.9.4 SNMP エージェントのバージョン

HVFP/HDI では、ノード上の SNMP エージェントとして net-snmp 5.4.1 を使用しています。利用している SNMP プログラムによっては、net-snmp の Web サイトから MIB 定義ファイルをダウンロードして、SNMP マネージャーにロードする必要があります。SNMP プログラムのバージョンを確認したり、MIB 定義ファイルをロードしたりする手順については、利用している SNMP プログラムのドキュメントを参照してください。

3.9.5 SNMP エージェントの起動時および停止時のトラップ通知

HVFP/HDI のノード上の SNMP エージェントは、SNMP エージェントが起動または停止した際に次のテキストを SNMP マネージャーにトラップで通知します。

起動時のトラップテキスト

```
オブジェクト名 : coldStart
OID : .1.3.6.1.6.3.1.1.5.1
```

停止時のトラップテキスト

```
オブジェクト名 : nsNotifyShutdown
OID : .1.3.6.1.4.1.8072.4.0.2
```

このメッセージは、通常、OS が起動または停止した際に SNMP エージェントの起動または停止とともに通知されますが、次のタイミングで SNMP エージェントが再起動された際にも通知されません。

- File Services Manager で/etc/snmp/snmpd.conf ファイルを更新したとき
- 毎日 00:00 (SNMP エージェントが自動的に再起動されたとき)

SNMP エージェントが起動または停止した際に通知されるトラップは、SNMP マネージャー側の設定で抑止できます。

3.10 NTP サーバの環境設定

Windows Server (Windows Server 2003 や Windows Server 2008, Windows Server 2012 など) を NTP サーバとして使用する場合は、ネットワーク上のほかの NTP サーバと時刻を同期できるように設定する必要があります。[ローカルグループポリシーエディター] (gpedit.msc) の [コンピューターの構成] - [管理用テンプレート] - [システム] - [Windows タイムサービス] で次のとおり設定してから、Windows タイムサービスを再起動してください。

[タイムプロバイダ]

```
[Windows NTP クライアントを構成する] : 有効にする
[Windows NTP クライアントを有効にする] : 有効にする
[Windows NTP サーバを有効にする] : 有効にする
```

[Windows NTP クライアントを構成するのプロパティ]

```
[NtpServer] : 同期先の NTP サーバの IP アドレスを指定する
[種類] : 「NTP」を指定する
```

[SpecialPollInterval] : 3,600 以下の値を指定する

なお、ほかの NTP サーバと時刻を同期できない環境で Windows Server を NTP サーバとして運用しなければならない場合は、次のとおり設定してから Windows タイムサービスを再起動してください。

[タイムプロバイダ]

[Windows NTP クライアントを構成する] : 有効にする

[Windows NTP クライアントを有効にする] : 無効にする

[Windows NTP サーバを有効にする] : 有効にする

[グローバル構成設定のプロパティ]

[LocalClockDispersion] : 「0」を指定する

3.11 スキャンサーバの環境設定

ここでは、スキャンサーバの環境設定について説明します。

まず、ネットワーク上に設置したスキャンサーバに、スキャンソフトをインストールします。1つのクラスタまたは Virtual Server 内で利用できるスキャンソフトは、同一製品の同一バージョンだけです。複数のスキャンサーバを利用する場合は注意してください。

スキャンサーバは、クラスタまたは Virtual Server 内ですべて同じ設定にしてください。また、スキャンサーバのウイルス定義ファイルは、新ウイルスに対応するため、すべて同じ時期に最新のファイルに更新してください。

スキャンソフトをインストールしたスキャンサーバで、HVFP/HDI と連携するために必要となる設定は次のとおりです。スキャンソフトの設定手順や注意事項については、利用するスキャンソフトのドキュメントを参照してください。

Symantec 社のスキャンソフトを使用する場合

- 接続プロトコルの設定
HVFP/HDI との接続プロトコルとして、ICAP インターフェースを利用できるように設定します。
- バインドアドレス (bind address) の設定
接続するクライアントを制限する場合、ノードがスキャンサーバのクライアントとしてアクセスできるようにバインドアドレスを設定します。
- ポート番号の設定
HVFP/HDI で指定したスキャンサーバのポート番号と同じ値を設定します。HVFP/HDI 側とスキャンサーバ側で入力したポート番号が異なる場合、HVFP/HDI はスキャンサーバに接続できません。
- 感染ファイルの修復方法の設定
感染ファイルを検出したときのスキャンサーバの対応について設定します。
- データの細流化の設定
データの細流化を無効にします。細流化を有効にすると、データにウイルスが入っているおそれがあるのでご注意ください。

また、次の表に示す項目の設定を変更することで、リアルタイムスキャンの性能を改善できることがあります。スキャンサーバの性能を考慮した上で、必要に応じて、設定を変更してください。

表 3-11 リアルタイムスキャンの性能改善に関する設定項目（Symantec 社のスキャンソフトを使用する場合）

項目	内容	効果
Number of available threads for scanning	スキャン処理に使用するスレッド数を指定します。	同時にスキャンできるファイル数が増えることがあります。
Threshold number of queued requests	スキャン要求の待ち受けキューサイズを指定します。	
Maximum RAM used for in-memory file system	スキャン処理に使用するメモリーサイズの上限值を指定します。	スキャン時間が短くなることがあります。
Maximum file size stored within the in-memory file system	メモリー上でスキャンを実行するときにスキャン対象とするファイルサイズの上限值を指定します。	

各項目の詳細や推奨される値については、利用するスキャンソフトのドキュメントを参照してください。

トレンドマイクロ社のスキャンソフトを使用する場合

- スキャンサーバの環境設定

スキャンサーバの OS に Windows Server 2008 R2 を使用している場合、スキャンサーバ上でメモリリークが発生することがあります。Microsoft のページから修正プログラム (KB2647452) を入手して、適用してください。Microsoft の次のページを参考にしてください。

<http://support.microsoft.com/kb/2647452>
- スキャンソフトの設定

スキャンソフトで、ウイルスのリアルタイム検索の設定を変更したり、スキャン対象外のファイルを指定したりします。

リアルタイム検索に次のとおり設定してください。

 - [リアルタイム検索を有効にする] チェックボックスがチェックされている
 - [入力/出力] ラジオボタンが選択されている
 - [マップされたネットワークドライブの検索] チェックボックスがチェックされている

スキャンするファイルを制限する場合は、スキャン対象から除外するファイルを指定してください。
- Hitachi Server Protect Agent のインストールと設定

Hitachi Server Protect Agent は、HVFP/HDI とスキャンソフトを連携させてリアルタイムスキャンを実施するために必要です。スキャンサーバにインストールメディアをセットし、HSPA フォルダに格納されている HspaInstaller.msi を実行することで、Hitachi Server Protect Agent のインストールが開始されます。インストールが完了したあと、Hitachi Server Protect Agent Manager を起動して、次の情報を設定する必要があります。情報を指定したあとに必ず [OK] ボタンをクリックして、設定を完了させてください。

表 3-12 Hitachi Server Protect Agent のセットアップに必要な情報

情報種別	項目
スキャンサーバと接続するノードの情報 ([ベーシック] タブで設定) ※1 (最大 32 ノード)	ホスト名※2 :
	IP アドレス※3 :
	CIFS 管理者のユーザー名※4※5 :
	CIFS 管理者のパスワード :

情報種別	項目
Anti-Virus Enabler との連携に使用する設定 ([アドバンスド] タブで設定) (任意)	ポート番号 :
	タイムアウト時間 (0~900 秒) :
	キューサイズ (1~ 500) :
	キュー数 (1~4) :
	ログファイルサイズ (1~10MB) :
	ログファイル数 (1~10) :
	トレースログサイズ (1~10MB) :
	トレースログ数 (1~10) :

注※1

ノードの情報が変更された場合は、Hitachi Server Protect Agent Manager の設定内容も変更してください。

注※2

ホスト名に含まれる英字の大文字と小文字は区別されるため、登録するノードのホスト名と、大文字と小文字が一致するようにしてください。

注※3

指定した IP アドレスを使用して HVFP/HDI にアクセスします。スキャンサーバにネットワークインターフェースが複数ある場合は、リアルタイムスキャンの要求を受け付けるネットワークインターフェースと、HVFP/HDI にアクセスするネットワークインターフェースが同じになるようにしてください。

注※4

CIFS ユーザーの認証方式に Active Directory 認証を使用している場合は、ユーザー名に Active Directory ドメインの NetBIOS 名を付けて、次のように指定してください。

< Active Directory ドメインの NetBIOS 名 > ¥ < ユーザー名 >

なお、スキャンサーバを Active Directory ドメインに参加させる必要はありません。

注※5

指定された CIFS 管理者のユーザー情報を使用して CIFS 共有にアクセスし、リアルタイムスキャンを実施します。

○ DHCP を使用する場合 (HDI の場合)

ノードの IP アドレスが DHCP によって変更される場合、Hitachi Server Protect Agent ではスキャンサーバとの接続に使用するノードの IP アドレスとして FQDN を指定する必要があります。このとき、リアルタイムスキャンを実施するたびに HDI のノードが名前解決されるため、レスポンス性能が低下します。また、ノードの IP アドレスが DHCP によって変更された場合、変更前の情報がスキャンサーバ上にキャッシュされているため、変更後の情報が反映されるまでに時間が掛かることがあります。このため、DHCP サーバの設定でノードおよびスキャンサーバのポートに固定の IP アドレスを割り当てるようにし、Hitachi Server Protect Agent では IP アドレスを指定することを推奨します。

マカフィー社のスキャンソフトを使用する場合

ストレージ連携のためのアドオンをインストールしてください。また、次のとおり設定を変更してください。

○ バインドアドレスの設定

HVFP/HDI と接続するために、HVFP/HDI で指定したスキャンサーバの IP アドレスを指定します。

○ ポート番号の設定

HVFP/HDI で指定したスキャンサーバのポート番号と同じ値を設定します。

- スキャンアイテムのオプション
圧縮ファイル内部のスキャンの実行を有効にします。
- 脅威が検出された場合のアクション
最初に実行するアクションとして「駆除」を設定します。
- 不審なプログラムの検出時のアクション
最初に実行するアクションとして「駆除」を設定します。

また、次の表に示す項目の設定を変更することで、リアルタイムスキャンの性能を改善できることがあります。スキャンサーバの性能を考慮した上で、必要に応じて、設定を変更してください。

表 3-13 リアルタイムスキャンの性能改善に関する設定項目（マカフィー社のスキャンソフトを使用する場合）

項目	内容	効果
最大スキャンタイム（秒）	スキャン処理のタイムアウト時間を指定します。	スキャンタイムアウトするファイルが減ることがあります。
スキャンスレッド数	スキャン処理に使用するスレッド数の最大値を指定します。	同時にスキャンできるファイル数が増えることがあります。

各項目の詳細や推奨される値については、利用するスキャンソフトのドキュメントを参照してください。

3.12 ノードに SAN で接続されたテープ装置の環境設定

ここでは、ノードに SAN で接続されたテープ装置の設定について説明します。ノードに SAN で接続されたテープ装置は、クラスタ構成で運用している場合に使用できます。

3.12.1 テープドライブの情報の登録

ノードに SAN で接続するテープ装置は、物理的に接続しただけでは使用できません。テープ装置を新規に導入した際には、保守員および SAN 管理者によるテープ装置の設置（テープ装置の接続や FC スイッチのゾーニングの設定など）が完了したあと、システム管理者がテープドライブの情報を NDMP サーバに登録する必要があります。

複数のノードまたは Virtual Server でテープドライブを共有する場合は、共有するテープドライブの情報を各 NDMP サーバに登録します。ノードまたは Virtual Server ごとに異なるテープドライブを使用する場合は、それぞれのノードで使用するテープドライブの情報だけを NDMP サーバに登録してください。

テープドライブの情報を NDMP サーバに登録する手順については、「コマンドリファレンス」を参照してください。

また、テープドライブの情報がすでに登録されているかどうかを確認するには、オプションを指定しないで `tapelist` コマンドを実行します。

3.12.2 テープドライブの登録情報の有効化

テープドライブを登録したあとでテープドライブの登録情報が無効になった場合は、登録情報を有効にするまで、そのテープドライブを使用したバックアップおよびリストアを実行できません。

テープドライブの登録情報は、次の場合に無効になります。

- Virtual Server を再起動した場合

- Virtual Server のフェールオーバーが発生した場合
- システム管理者が手動で登録情報を無効にした場合 (-i オプションを指定して `tapedel` コマンドを実行した場合)
- リソースグループでの運用から Virtual Server での運用に移行した場合

テープドライブの登録情報が無効になった場合は、そのテープドライブを使用したバックアップやリストアを開始する前に、登録情報を有効にしてください。

3.12.3 テープドライブの登録情報の解除

ノードに SAN で接続されたテープ装置が不要になった場合、システム管理者は、バックアップ管理ソフトウェアでテープドライブの登録情報を削除したあとに、NDMP サーバに登録されているテープドライブの登録情報を解除します。テープドライブの登録情報を解除する手順については、「コマンドリファレンス」を参照してください。

3.12.4 ノードに SAN で接続されたテープ装置を設定する上での注意事項

ノードに SAN で接続されたテープ装置を設定する上での注意事項を次に示します。

- バックアップ管理ソフトウェアでブロック長を変更できるテープ装置を使用する場合、バックアップ後にブロック長を変更すると、そのテープ装置にバックアップしたデータをリストアに使用できなくなるおそれがあります。
- テープドライブは、バックアップやリストアを実行するノードまたは Virtual Server に登録されたものを使用してください。異なるノードまたは Virtual Server に登録されたテープドライブを使用すると、バックアップまたはリストアするデータが LAN 上に流れるおそれがあります。
- 縮退運用時は、バックアップまたはリストアの際にエラーが発生することがあるほか、バックアップまたはリストアを実行するためには設定変更が必要になることがあります。縮退運用時の注意事項については、「トラブルシューティングガイド」を参照してください。

3.12.5 テープ装置の交換

テープ装置を交換する場合、システム管理者は、保守員や SAN 管理者と連携して、次の流れで作業を実施します。手順の中で使用しているコマンドの詳細については「コマンドリファレンス」を参照してください。

1. バックアップ管理ソフトウェアで、交換するテープ装置の登録を解除します。
2. `tapedel` コマンドを実行して、すべてのノードおよび Virtual Server で、NDMP サーバに登録されたテープドライブの情報を解除します。
3. SAN 管理者と連携して、使用を取りやめるテープ装置に接続されている FC ケーブルを外します。
4. 保守員または SAN 管理者と連携して、テープ装置を交換します。
5. SAN 管理者と連携して、交換したテープ装置に FC ケーブルを接続します。
6. `tapeadd` コマンドを実行して、テープドライブを NDMP サーバに登録します。
7. バックアップ管理ソフトウェアで、交換したテープ装置の情報を登録します。

3.12.6 テープ装置の取り外し

テープ装置の使用を取りやめる場合、システム管理者は、保守員や SAN 管理者と連携して、次の流れで作業を実施します。手順の中で使用しているコマンドの詳細については「コマンドリファレンス」を参照してください。

1. バックアップ管理ソフトウェアで、使用を取りやめるテープ装置の登録を解除します。
2. `tapedel` コマンドを実行して、すべてのノードおよび Virtual Server で、NDMP サーバに登録されたテープドライブの情報を解除します。
3. SAN 管理者と連携して、使用を取りやめるテープ装置に接続されている FC ケーブルを外します。
4. テープ装置を取り外します。

3.13 SMTP サーバの環境設定

HVFP/HDI で障害が発生したりユーザーが操作ミスしたりした場合に E-mail によって障害通知として受け取るには、HVFP/HDI からの E-mail をあらかじめ設定した送信先に配信できる SMTP サーバが必要です。ここでは、SMTP サーバの環境設定について説明します。

HVFP/HDI のノードや Virtual Server が接続されている LAN に SMTP サーバがすでにある場合はそれを利用できます。HVFP/HDI のノードや Virtual Server が接続されている LAN に SMTP サーバがない場合は、その LAN 上に新たに SMTP サーバを設置するか、SMTP サーバがある既存のネットワークとルーティングをする必要があります。

なお、E-mail を受信するクライアントは、Unicode (UTF-8) をサポートしている必要があります。

3.14 ALog マネージャーサーバの環境設定

HVFP/HDI と ALog ConVerter との連携を開始する前に、ALog マネージャーサーバの設定を変更する必要があります。ALog マネージャーサーバの設定については、ALog ConVerter のドキュメントを参照してください。

3.15 DHCP サーバの環境設定

HDI の場合、DHCP を利用してノードのインターフェースを設定するときは、DHCP サーバが必要です。ここでは、DHCP サーバの環境設定について説明します。

ノードのホスト名を DNS サーバに自動的に登録するために、DHCP サーバと DNS サーバで DDNS 機能を有効にしてください。DNS サーバの環境設定については、「3.16 DNS サーバの環境設定」を参照してください。

HDI で使用する次の設定情報を DHCP サーバで管理できます。

- インターフェースの IP アドレスおよびサブネットマスク
- デフォルトゲートウェイ
- MTU 値 (1,500 に設定してください。)
- DNS サーバ (設定する DNS サーバは 2 台以内にしてください。)
- ノードが所属するドメインおよび名前解決の検索対象にしたいドメイン
- ルーティング情報 (スタティックルート)

ルーティング情報は HDI で設定せず、DHCP サーバで管理することをお勧めします。

DHCP サーバで DNS サーバの情報を管理する場合、HDI で DNS サーバを設定しても、ノードの OS を再起動すると、DHCP サーバでの設定が使用されるようになります。

3.16 DNS サーバの環境設定

HDI で DHCP を利用する場合、ノードのホスト名を DNS サーバに自動的に登録するために、DNS サーバの環境設定が必要です。次のとおり設定してください。

- DDNS 機能を有効にしてください。また、DHCP サーバからの DNS レコードの動的更新を許可するように、セキュリティの設定を変更してください。
- 使用されていないリソースレコードを削除できるよう、古いリソースレコードの清掃を有効にしてください。

運用を開始する前に

この章では、HVFP/HDI の運用を開始するに当たり、システム管理者が理解または考慮する必要があることについて説明します。

なお、HVFP/HDI のバックアップ運用については、「[5. HVFP/HDI のバックアップ運用](#)」を参照してください。

HCP と連携して HVFP/HDI の運用を開始する場合は、先に「[6. HCP と連携して運用を開始する前に](#)」を参照してください。

注意：

「[4.1 運用上の注意事項（必ずお読みください）](#)」を必ず参照してください。

- [4.1 運用上の注意事項（必ずお読みください）](#)
- [4.2 クラスタ構成を管理する前に](#)
- [4.3 クライアントのユーザー情報を管理する前に](#)
- [4.4 ユーザーマッピングでの運用を開始する前に](#)
- [4.5 ファイルシステムの運用を開始する前に](#)
- [4.6 Quota の運用を開始する前に](#)
- [4.7 ファイル共有の運用を開始する前に](#)
- [4.8 リアルタイムスキャン機能の運用を開始する前に](#)
- [4.9 システム設定情報の管理を開始する前に](#)
- [4.10 障害情報の管理を開始する前に](#)
- [4.11 SNMP によるシステム監視を開始する前に](#)
- [4.12 ほかのファイルサーバからデータをインポートする前に](#)
- [4.13 クライアントがファイルシステムの利用を開始する前に](#)

4.1 運用上の注意事項（必ずお読みください）

システム管理者が HVFP/HDI の運用を管理するときの注意事項を次に示します。

- HVFP/HDI のシステムの構成を変更した場合は、システム LU の設定情報ファイルをダウンロードし、システム外の記録媒体に保管する必要があります。
- GUI を利用して HVFP/HDI を運用しているときには、コマンドでの操作を実行しないでください。
- 同一クラスタ内または同一 Virtual Server 内では、システムの構成に関する情報の設定・更新を同時に実行できません。このため、複数のシステム管理者が登録されている場合、情報を設定・変更できるシステム管理者を 1 人だけとする運用にしてください。
- ノードの管理 IP アドレス、またはストレージシステムのコントローラーの管理ポートの IP アドレスにホスト名を指定する場合は、管理サーバに対して、名前解決ができるよう事前に設定する必要があります。
- HVFP/HDI の運用開始後に DNS サーバの設定情報を変更する場合は、変更後にクラスタ内の両ノードの OS を再起動する必要があります。
- NFS 共有を利用する場合には、HVFP/HDI の運用を開始したあとに、名前解決が行える環境 (NFS クライアントマシンの IP アドレスとホスト名を、ノードの OS の /etc/hosts ファイル、NIS サーバまたは DNS サーバに登録し、ホスト名から IP アドレスへの変換が行える環境) を変更しないでください。NFS 共有を作成したあとに名前解決の環境が変更されると、ファイルシステムに対する NFS クライアントからのアクセスがエラーになることがあります。
- NFS サービスを停止する場合は、NFS サービスを起動するまで NFS 共有にアクセスしないよう、NFS クライアントホストの管理者に連絡してください。
- [Network & System Configuration] ダイアログの [DNS, NIS, LDAP Setup] ページに情報を設定した DNS サーバに、クライアントホストのホスト名を登録して運用する場合は、NFS クライアントホストの名前解決 (正引き参照および逆引き参照) が短時間で正常応答することを事前に確認してください。DNS による名前解決に問題がないか確認する方法については、「トラブルシューティングガイド」を参照してください。DNS サーバが短時間で正常応答しない場合は、DNS サーバの設定を見直してください。

また、[Network & System Configuration] ダイアログの [DNS, NIS, LDAP Setup] ページに情報を設定した DNS サーバに、NFS クライアントホストを登録しない運用にする場合は、NFS クライアントホストの名前解決 (正引き参照および逆引き参照) が短時間でエラー応答することを事前に確認してください。DNS サーバが短時間でエラー応答しない場合は、逆引きゾーンを DNS サーバに定義するなど、[DNS, NIS, LDAP Setup] ページで設定した DNS サーバが別の DNS サーバに名前解決のための問い合わせしないよう設定して、DNS サーバへの問い合わせ処理に時間が掛からないようにしてください。

DNS サーバへの問い合わせ処理に時間が掛かる状態で HVFP/HDI を運用した場合、NFS 共有の作成、NFS 共有の削除、NFS 共有の属性変更、フェールオーバーおよびフェールバックに失敗することがあります。

- CIFS サービスでドメインコントローラーまたはユーザーマッピング用の LDAP サーバを指定していて、DNS によってそれらの名前解決を行う場合は、次のことを確認してください。
 - ドメインコントローラーおよび LDAP サーバが DNS サーバによって名前解決 (正引き) できること。
 - ドメインコントローラーおよび LDAP サーバの名前解決 (正引きおよび逆引き) の際に、DNS サーバが短時間で応答すること。

DNS による名前解決に問題がないか確認する方法については、「トラブルシューティングガイド」を参照してください。DNS サーバが正常に応答しない場合は、DNS サーバのレコード、ゾーンまたは再帰の設定などを見直してください。

- 名前解決が行える環境で運用する場合、次のことに注意してホスト名を登録・削除してください。
 - 特定のホストに対する NFS 共有を作成する場合は、NFS 共有を作成する前にホスト名を登録しておいてください。
 - ネットグループを指定して NFS 共有を作成する場合は、該当するファイルシステムをマウントする NFS クライアントのホスト名の名前解決 (IP アドレスからホスト名、ホスト名から IP アドレスへの変換) が、常に一定である必要があります。
 - 特定のホストに対する NFS 共有で使用されているホスト名を削除する場合は、該当する NFS 共有を削除してからホスト名を削除してください。
 - NFS 共有でファイルロックを行う場合、ファイルロックを保持している NFS クライアントが異常終了して再起動できないときにはファイルロック情報を削除する必要があります。ファイルロック情報を削除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。
- ユーザー情報を登録するときにシステム管理者が設定するパスワードは、一時的な運用としてください。システム管理者は、[Local Users] ダイアログの [Add User] ページや [Batch Operation] ページなどで追加した各ユーザーに対して、各自でパスワードを変更するよう連絡する必要があります。
- Active Directory を使用する場合、Active Directory 認証されたユーザーが CIFS 共有にアクセスできます。HVFP/HDI でローカルに認証されたユーザーは CIFS 共有にアクセスできません。
- システムダウン障害などクラスタ内の両ノードの OS が停止する障害が発生し、片方のノードだけを起動して運用を再開した場合は、[Check for Errors] ダイアログの [List of RAS Information] ページ ([List of messages] 表示) で、KAQG72011-E メッセージが出力されていないかを確認してください。事前に設定している場合は SNMP トラップまたは E-mail でも通知されます。KAQG72011-E メッセージが出力されたノードの OS を停止するまでは、もう一方のノードの OS を起動しないでください。
- フェールオーバーが発生した場合、フェールオーバーしたリソースグループに関連するサービスの起動、停止および再起動は実行できません。
- [Cluster Management] ダイアログの [Browse Cluster Status] ページ ([Resource group status] 表示) にある [Resource group status] に「Online / No error」と表示されると、File Services Manager からファイルシステム、NFS サービス、CIFS サービスまたは仮想 IP アドレスを管理できるようになります。クラスタが正常に稼働してからリソースグループが起動されるため、[Browse Cluster Status] ページ ([Cluster / Node status] 表示) の [Cluster status] でクラスタの状態が「ACTIVE」と表示された直後では、起動処理中のリソースグループが「Online Pending」と表示され、ファイルシステム、NFS サービス、CIFS サービスまたは仮想 IP アドレスは利用できません。利用する前にリソースグループの状態を参照し、「Online / No error」と表示されていることを確認してください。
- HVFP/HDI では、リソースグループを起動する場合、障害を検出したリソースを閉塞し、そのほかの正常なリソースでリソースグループを構成します。リソースグループが部分的に閉塞すると、ノード上のサービスが一部停止した状態で、残りのサービスが提供されます。このとき、[Cluster Management] ダイアログの [Browse Cluster Status] ページ ([Resource group status] 表示) では「Online / No error」が表示され、リソースグループのエラー情報を確認できません。
リソースグループの部分閉塞が発生するおそれのある契機を次に示します。
 - HVFP/HDI の運用開始時
 - フェールオーバー・フェールバックの発生時
 - リソースグループの再起動時

これらの操作を行った場合、また、ユーザーがファイルシステムにアクセスできないのに [Browse Cluster Status] ページ ([Resource group status] 表示) で「Online / No error」と表示されている場合は、リソースグループの部分閉塞が発生していないか、[Check for Errors] ダイアログの [List of RAS Information] ページ ([List of messages] 表示) でシステムメッセージを確認する必要があります。

システム管理者は、システムメッセージのうち、KAQG72006-E メッセージが出力されていないか確認してください。

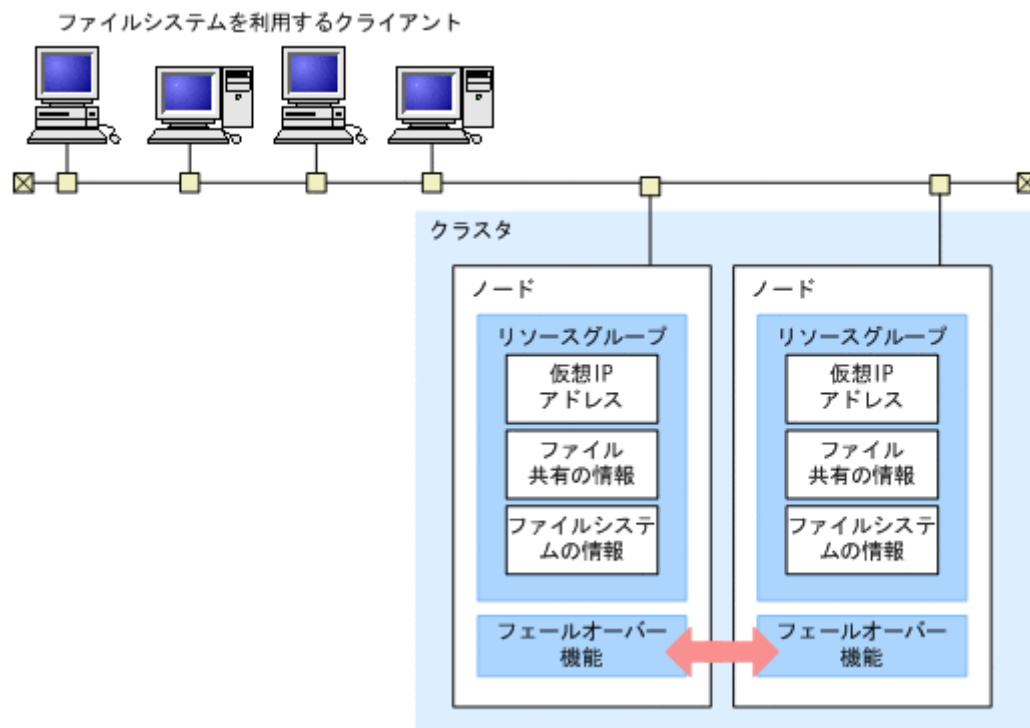
なお、リソースのタイプによっては、閉塞したリソースを使用していた、ほかのリソースも閉塞することがあります。例えば、論理ボリュームが閉塞すると、閉塞した論理ボリューム上に作成したファイルシステムも閉塞します。この場合、閉塞したリソースごとに KAQG72006-E メッセージが出力されます。

- OS 停止などの理由でファイルシステムを管理するための処理が中断すると、同じ操作を再度実行できないことがあります。この場合は、メッセージに従って対処する前に、Processing Node のリフレッシュ処理を実行するか、fslist コマンドでファイルシステムの状態を確認してから、操作を実行してください。

4.2 クラスタ構成を管理する前に

クラスタを構成するノード上には、NFS 共有設定および CIFS 共有設定の情報、仮想 IP アドレスの情報、およびノードにマウントされているファイルシステムの情報などを 1 つのグループとして管理するリソースグループが稼働しています。通常運用時には、1 つのノードに 1 つのリソースグループが稼働しています。HVFP/HDI のクラスタ構成を次の図に示します。

図 4-1 HVFP/HDI のクラスタ構成

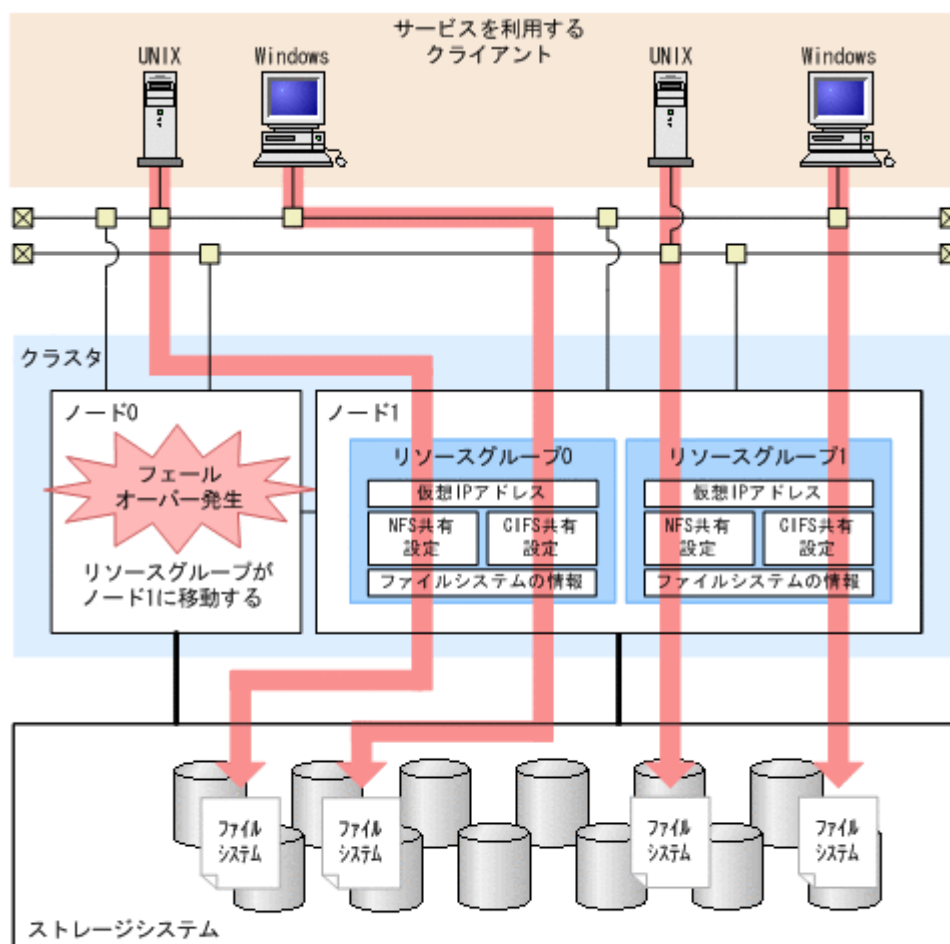


フェールオーバーが必要な障害が発生した場合、障害情報がフェールオーバー機能に通知され、自動的にフェールオーバーが発生します。システム管理者は、File Services Manager を使用して、フェールオーバーが発生したことを確認できます。

HVFP/HDI では、フェールオーバーすることで、サービスを継続して提供しながら障害回復やリブレースなどの保守作業ができます。

フェールオーバーしたときにクライアントが利用するサービスの流れを次の図に示します。

図 4-2 クライアントが利用するサービスの流れの例（フェールオーバー時）



(凡例)

➡ : ファイルアクセス

リソースグループや Virtual Server 上のサービスに接続するときクライアントが利用する IP アドレスを仮想 IP アドレスといいます。仮想 IP アドレスは、リソースグループや Virtual Server が稼働するノードが変更しても、移動先のノードに引き継がれます。クライアントは仮想 IP アドレスでサービスに接続しているため、フェールオーバー時にもファイルにアクセスできます。仮想 IP アドレスは、ノード内の各インターフェースに対応づけられています。リソースグループや Virtual Server がクラスタ内の別のノードに移動した場合は、移動先でも同じインターフェースに対応づけられます。例えば、eth1 に対応づけられていた仮想 IP アドレスは、移動先の eth1 に対応づけられます。

HVFP/HDI では、リソースグループや Virtual Server ごとに別のファイルシステムをマウントして、サービスを提供します。システム管理者は、ネットワーク構成、ファイルシステムのマウント、または Virtual Server が稼働するノードなどを計画的に設計することで、ファイルへのアクセスを両ノードに分散し、1つのノードに掛かる負荷を軽減できます。

障害が回復してから、フェールオーバーしたリソースグループや Virtual Server を元のノードにフェールバックすることで、通常運用を再開します。システム管理者は、リソースグループや

Virtual Server が稼働しているノードを変更することで、フェールバックできます。フェールバックは、保守員の指示に従って操作してください。

4.3 クライアントのユーザー情報を管理する前に

HVFP/HDI ではクライアントをユーザー ID やグループ ID で識別します。クライアントのユーザー情報は、次の方法で管理できます。各方法で管理できるユーザー情報の上限値は、クラスタ（シングルノードの場合はノード）または Virtual Server 当たりの数です。

HVFP/HDI で管理する

HVFP/HDI に登録されたユーザー情報を 2,000 件まで管理できます。

NIS サーバまたは LDAP サーバで管理する

HVFP/HDI, NIS サーバおよび LDAP サーバに登録されたユーザー情報を合わせて 50,000 件まで管理できます。事前に NIS サーバまたは LDAP サーバの情報を HVFP/HDI 登録しておく必要があります。なお、NIS サーバでの管理は IPv4 を使用する場合に利用できます。

Active Directory または NT ドメインで管理する

ユーザー認証に使用するユーザー情報に対してユーザー ID やグループ ID を割り当てるために、ユーザーマッピングを使用するか、HVFP/HDI, 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 ID やグループ ID のユーザー情報を管理する必要があります。

各ドメインで管理できるユーザー情報の上限値は、使用するドメインコントローラーの OS に依存します。また、利用する全ドメイン（信頼関係先を含む）で、ユーザーマッピングを使用できるユーザー数の上限は次のとおりです。

AD スキーマ方式を使用している場合

2,147,482,948（全ドメインのユーザー ID 数の合計）

RID 方式を使用している場合

2,147,412,648（全ドメインのユーザー ID 数とグループ ID 数の合計）

なお、NT ドメインでの管理は IPv4 を使用する場合に利用できます。

4.4 ユーザーマッピングでの運用を開始する前に

HVFP/HDI と Windows では、ユーザーを識別する ID の種別が異なります。HVFP/HDI ではユーザー ID やグループ ID を利用し、Windows では SID（セキュリティ識別子）と呼ばれる一意の ID を利用します。

HVFP/HDI では、Active Directory 認証または NT ドメイン認証で CIFS クライアントを認証する場合、ユーザーマッピングを使用することで、ファイルシステムにアクセスした CIFS クライアントに対して、ユーザー ID やグループ ID が割り当てられます。

このほか、ユーザーマッピングを使用すると、32 グループ以上のグループに所属するユーザーも管理できます。

ここでは、HVFP/HDI で提供しているユーザーマッピングの方式や事前に検討が必要な設定情報について説明します。

4.4.1 HVFP/HDI を利用できるドメインの範囲

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。

HVFP/HDI を利用するユーザーは、ノードまたは Virtual Server が参加しているドメインと、双方向の信頼関係を結んだドメインに所属している必要があります。

フォレスト間で信頼関係を結ぶ場合は、ルートドメイン同士が双方向の信頼関係を結んでいる必要があります。

フォレスト間で片方向の信頼関係を結んだドメインに所属しているユーザーは CIFS 共有にアクセスできません。

HVFP/HDI の CIFS 共有を利用できるドメインの範囲を次の図に示します。

図 4-3 ルートドメインに参加している場合

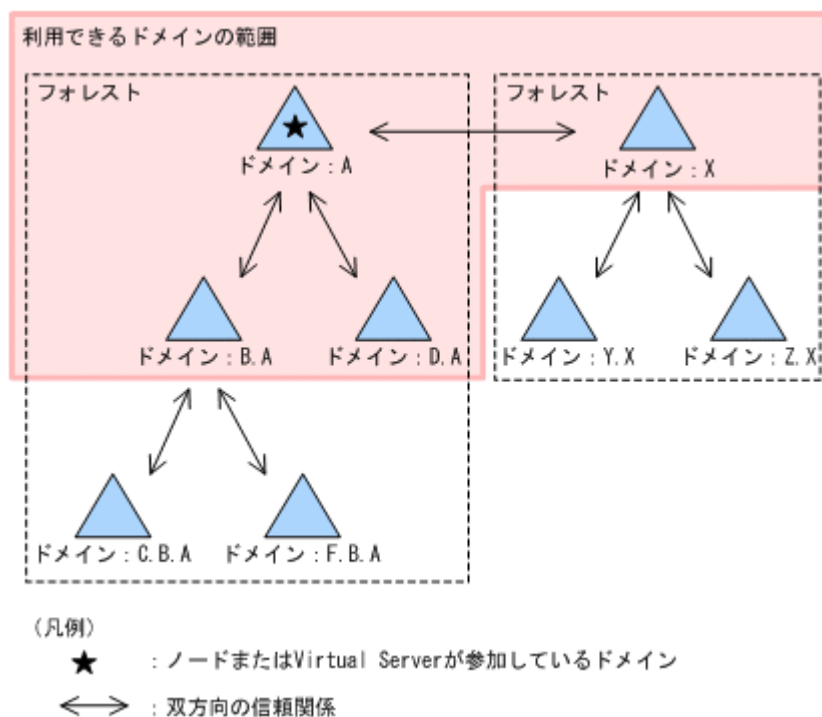
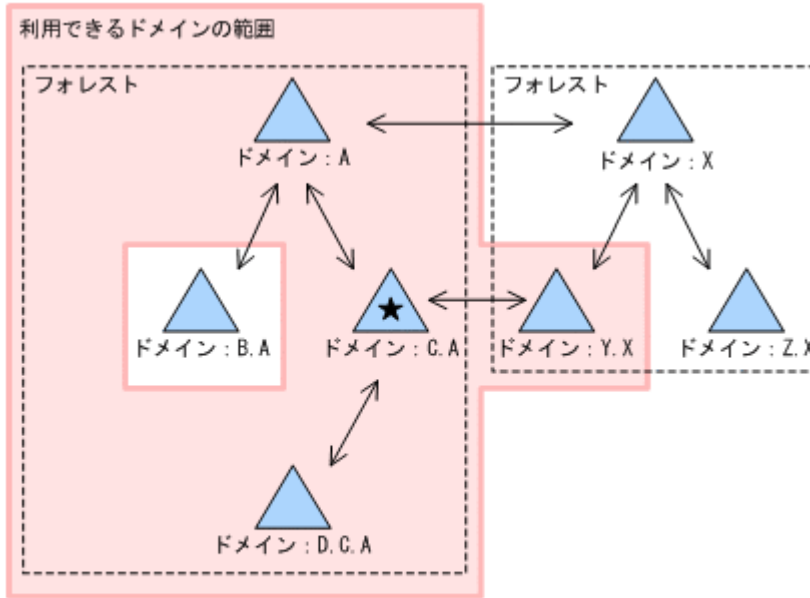


図 4-4 子のドメインに参加し、フォレスト間に信頼関係がある場合

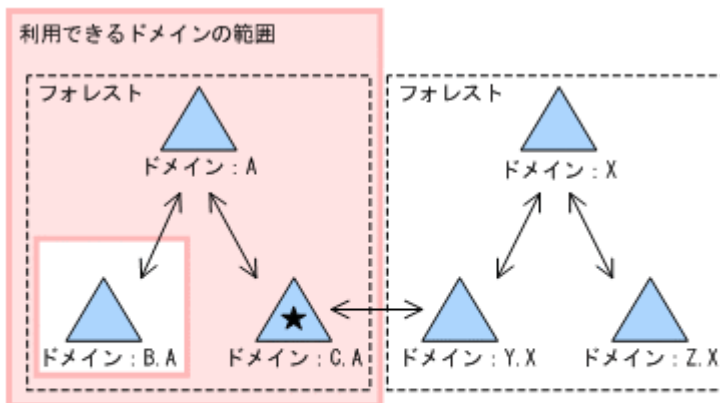


(凡例)

★ : ノードまたはVirtual Serverが参加しているドメイン

↔ : 双方向の信頼関係

図 4-5 子のドメインに参加し、フォレスト間に信頼関係がない場合

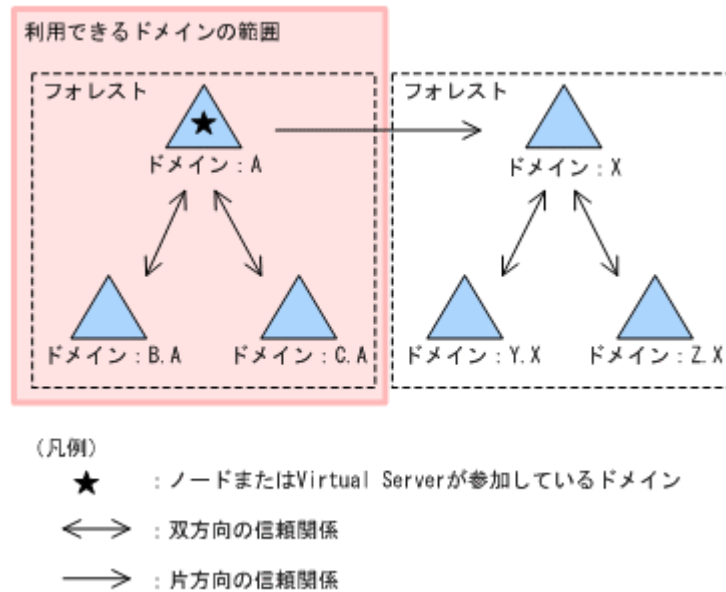


(凡例)

★ : ノードまたはVirtual Serverが参加しているドメイン

↔ : 双方向の信頼関係

図 4-6 フォレスト間の信頼関係が片方向の場合



ノードまたは Virtual Server が Active Directory ドメインに参加している場合に、ノードまたは Virtual Server が参加したドメインと親子関係にないドメインに所属しているユーザーが HVFP/HDI を利用するためには、明示的に信頼関係を結ぶよう設定する必要があります。

4.4.2 ユーザーマッピングの方式

HVFP/HDI で提供しているユーザーマッピングの方式は次のとおりです。

- RID 方式（自動割り当て）
- LDAP 方式（自動割り当てまたは手動割り当て）
- Active Directory スキーマ方式（手動割り当て）

HVFP/HDI では、障害の影響を受けにくい RID 方式を利用することを推奨しています。

(1) RID 方式

RID 方式は、Active Directory 認証または NT ドメイン認証で CIFS クライアントを認証する場合に利用できます。

RID 方式のユーザーマッピングを使用すると、CIFS クライアントが HVFP/HDI のファイルシステムにアクセスする際、SID を構成する RID（相対識別子）が変換され、ユーザー ID やグループ ID が自動的に割り当てられます。

RID 方式では、File Services Manager でドメインごとにユーザー ID やグループ ID の範囲を設定します。このため、システム管理者は、ドメイン単位でユーザーやグループを管理できます。また、RID 方式のユーザーマッピングを使用すると、マッピング情報をデータベース化したり、外部サーバで管理したりしないため、ユーザー ID やグループ ID を割り当てるまでに掛かる時間が短く、ネットワークや外部サーバで発生する障害の影響を受けにくくなります。

なお、RID 方式で管理できるドメインは 256 個までです。ドメインが 257 個以上の場合にユーザーマッピングを使用するには、LDAP 方式または Active Directory スキーマ方式を選択してください。

(2) LDAP 方式

LDAP 方式は、Active Directory 認証または NT ドメイン認証で CIFS クライアントを認証する場合に利用できます。

LDAP 方式のユーザーマッピングを使用すると、ユーザー ID およびグループ ID を自動的に割り当てるか、手動で割り当てるかを選択できます。

自動割り当てを選択した場合、CIFS クライアントが HVFP/HDI のファイルシステムにアクセスしたときに、File Services Manager で指定した範囲内でユーザー ID やグループ ID が自動的に割り当てられます。割り当てられたユーザー ID やグループ ID の情報は、外部サーバとして用意された LDAP サーバのデータベースに登録され、CIFS クライアントが再度アクセスしたときに、すでに割り当てられたユーザー ID やグループ ID が使用されます。

手動割り当てを選択した場合、事前に LDAP サーバのデータベースに登録されたユーザー情報に従って、ユーザー ID およびグループ ID が割り当てられます。

(3) Active Directory スキーマ方式

Active Directory スキーマ方式は、Active Directory 認証で CIFS クライアントを認証する場合に利用できます。

Active Directory スキーマ方式のユーザーマッピングを使用すると、NFS クライアントと CIFS クライアントで異なる識別 ID の対応を、Active Directory のユーザー属性の一つとして管理できます。また、ユーザーマッピングのために外部サーバを用意する必要はなく、事前にドメインコントローラーに登録されたユーザー情報に従って、ユーザー ID およびグループ ID が割り当てられます。

4.4.3 ユーザーマッピングの方式の変更

ユーザーマッピングの方式の違いによって、ユーザー ID やグループ ID の割り当て方が異なるため、同一の CIFS クライアントに対して、それぞれ異なる ID が割り当てられます。

HVFP/HDI の運用を開始してからユーザーマッピングの方式を変更すると、CIFS クライアントに割り当てるユーザー ID やグループ ID が変わることによって、アクセス権のなかったユーザーが、変更前に作成したファイルやフォルダにアクセスできるようになるおそれがあります。CIFS 管理者は、ファイルやフォルダのユーザー ID やグループ ID を、変更後の方式で管理するユーザー ID やグループ ID に置換するために、Windows のバックアップ機能を利用してファイルシステムを移行する必要があります。

ここでは、ユーザーマッピングの方式を LDAP 方式（自動割り当て）から RID 方式に変更するときに、ファイルシステムを移行するための手順を次に示します。

1. エンドユーザーに連絡します。
作業中、CIFS 共有にアクセスしないよう、エンドユーザーに連絡してください。
2. CIFS クライアントホストのアクセスを制限します。
[Access Protocol Configuration] ダイアログの [CIFS Service Management] ページ (Setting Type : Security) にある [Host access restrictions] で、ファイルシステムの移行を実施する CIFS クライアントホストだけがアクセスできるように制限してください。
3. CIFS 管理者を設定します。
ファイルシステムの移行を実施する CIFS 管理者を [Access Protocol Configuration] ダイアログの [CIFS Service Management] ページ (Setting Type : Administration) にある [CIFS administrator name(s)] で設定してください。
4. 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てください。
5. 移行元 CIFS 共有上にあるデータをバックアップするよう、CIFS 管理者に依頼します。

バックアップするときは、Windows 付属のバックアップ機能を利用することを推奨します。そのほかの方法でバックアップした場合、リストア時に ACL やファイル属性を正しく復元できないことがあります。なお、NFS クライアントで作成したデータは、Windows 付属のバックアップ機能では移行できません。

6. ユーザーマッピングの方式を変更します。
[Access Protocol Configuration] ダイアログの [CIFS Service Management] ページ (Setting Type : User mapping) にある [User mapping setup] に必要な情報を指定してください。
7. 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てください。
8. 移行先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。移行先ファイルシステムを構築する際、ファイルシステムの容量は、移行元ファイルシステムの容量と等しいか、それよりも大きくなるよう設定してください。そのほかの項目については、移行元ファイルシステムと同等になるよう設定してください。
9. 移行先ファイルシステムに Quota を設定します。
移行元ファイルシステムで、デフォルト Quota またはユーザーやグループに対する Quota を設定していた場合は、移行先ファイルシステムに同等の値を設定してください。
デフォルト Quota およびユーザーやグループに対する Quota の設定には、quotaset コマンドを使用してください。使用できるブロック容量と inode 数を制限しないユーザーやグループに対しては、それぞれのソフトリミットおよびハードリミットに「0」を指定してください。
10. 移行先 CIFS 共有を作成します。
[共有追加] ダイアログで、移行先とする CIFS 共有を作成してください。このとき、移行先 CIFS 共有の名前は移行元 CIFS 共有と異なる名前を設定してください。移行先 CIFS 共有は、移行元 CIFS 共有と同等の設定にしてください。
11. サブツリー Quota を設定します。
移行元 CIFS 共有の共有ディレクトリでサブツリー Quota を設定していた場合は、移行先 CIFS 共有の共有ディレクトリに同等の値を設定してください。
サブツリー Quota の設定には、stquotaset コマンドを使用してください。使用できるブロック容量と inode 数を制限しないユーザーやグループに対しては、それぞれのソフトリミットおよびハードリミットに「0」を指定してください。
12. 移行先 CIFS 共有上にデータをリストアするよう、CIFS 管理者に依頼します。
手順 10 で作成した移行先 CIFS 共有上に、手順 5 でバックアップしたデータをリストアするよう CIFS 管理者に依頼します。
13. データを正しく移行できていることを確認します。
移行元のデータと移行先のデータを比較し、正しく移行できていることを確認してください。少なくとも、次の点について確認することを推奨します。
 - フォルダの構造が一致している
 - ファイルの内容が一致している
 - オーナー、ACL、ファイル属性が一致している
14. 必要に応じて、移行元 CIFS 共有を解除します。
移行先 CIFS 共有の名前を移行元 CIFS 共有の名前に変更する場合は、次のウィンドウまたはタブで [共有解除] ボタンをクリックして、移行元の CIFS 共有を解除してください。
クラスタ構成の場合：
 - [共有] サブウィンドウ

- [< Physical Node >] または [< Virtual Server >] サブウィンドウの [共有] タブ
 - [< ファイルシステム >] サブウィンドウの [共有] タブ
- シングルノード構成の場合 :
- [共有] ウィンドウ
 - < ファイルシステム名 > ウィンドウの [共有] タブ
15. 必要に応じて、移行元ファイルシステムを削除します。
- 移行元ファイルシステムが不要な場合は削除できます。移行元ファイルシステムは、次のウィンドウまたはタブで [ファイルシステム削除] ボタンをクリックして削除してください。
- クラスタ構成の場合 :
- [ファイルシステム] サブウィンドウ
 - [< Physical Node >] または [< Virtual Server >] サブウィンドウの [ファイルシステム] タブ
- シングルノード構成の場合 : [ファイルシステム] ウィンドウの [ファイルシステム] タブ
16. 必要に応じて、移行先 CIFS 共有の名前を変更します。
- 手順 14 で移行元 CIFS 共有を解除した場合、移行先 CIFS 共有の名前を移行元 CIFS 共有の名前に変更できます。移行先 CIFS 共有の名前は、[共有編集] ダイアログで変更してください。
17. 必要に応じて、設定した CIFS 管理者を削除します。
- 手順 3 で設定した CIFS 管理者が不要な場合は、[Access Protocol Configuration] ダイアログの [CIFS Service Management] ページ (Setting Type : Administration) にある [CIFS administrator name(s)] で CIFS 管理者を削除してください。
18. CIFS クライアントホストのアクセス制限を解除します。
- 手順 2 で設定した CIFS クライアントホストのアクセス制限を [Access Protocol Configuration] ダイアログの [CIFS Service Management] ページ (Setting Type : Security) にある [Host access restrictions] で解除してください。
19. 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てください。

注意 :

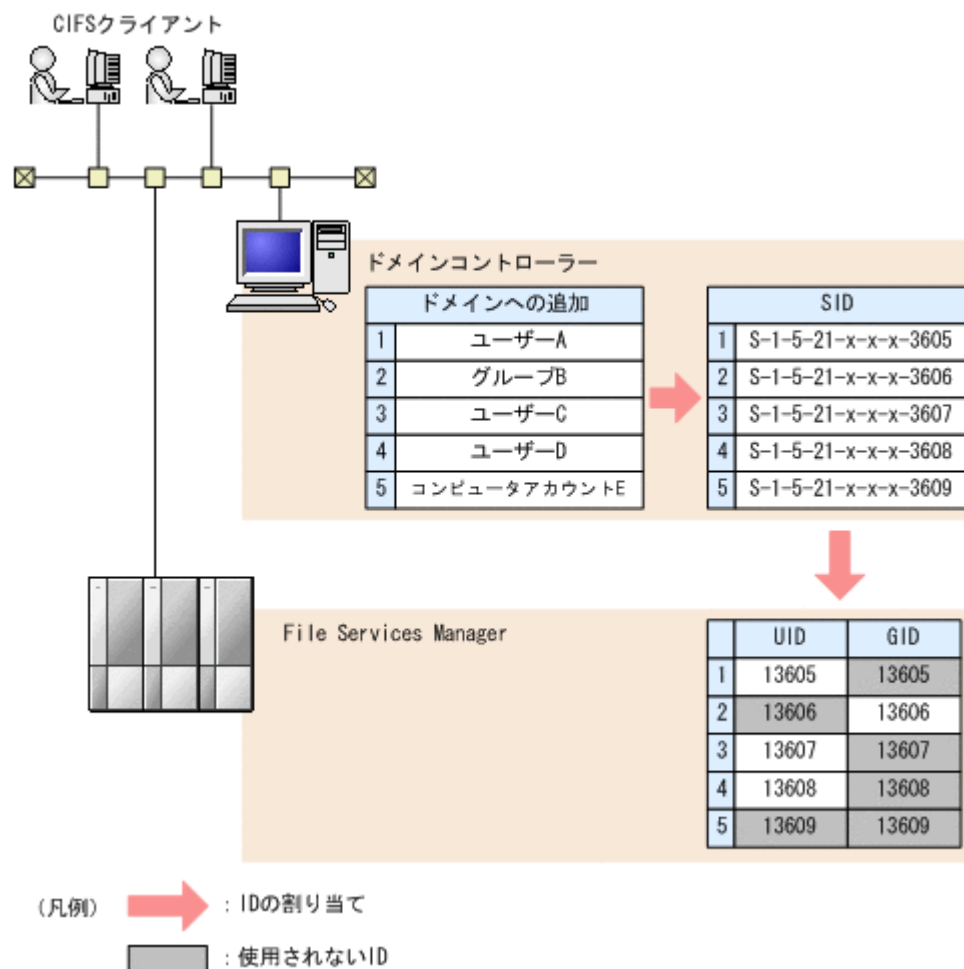
ユーザーマッピングの方式を変更したあとは、移行元の CIFS 共有を削除してください。移行元のファイルやフォルダのプロパティ画面を参照すると、不正なキャッシュが残るため、CIFS アクセスエラーとなることがあります。なお、CIFS サービス環境にキャッシュされているユーザーマッピング情報は [Access Protocol Configuration] ダイアログの [CIFS Service Maintenance] ページで削除してください。

4.4.4 ユーザー ID とグループ ID の範囲の検討例 (RID 方式の場合)

RID は、ユーザー、グループまたはコンピュータアカウントなどの種別に関係なく、オブジェクトごとに 1 つずつ与えられます。このため、RID 方式でユーザー ID やグループ ID を割り当てるとき、使用されない ID が発生します。ユーザー ID やグループ ID の範囲を検討するときには、使用されない ID があることを考慮してください。

RID 方式のユーザーマッピングを使用した場合に、ユーザー ID やグループ ID がどのように割り当てられるのか、次の図に示します。

図 4-7 RID 方式によるユーザー ID やグループ ID の割り当て例



ユーザーマッピングを使用するときに設定するユーザー ID やグループ ID の範囲の最小値は、運用開始後に変更できません。将来的な運用計画、別のドメインや外部サーバで使用するユーザー ID やグループ ID の範囲なども考慮し、余裕を持って、ユーザーマッピングを使用するときに設定する ID の範囲を検討してください。ユーザー ID やグループ ID の範囲を変更するときに、追加したい ID の領域を確保できない場合、ファイルシステムを再構築する必要があります。

なお、ユーザーマッピングを使用するときに設定する ID の範囲は、将来的に増加する SID の数を考慮するほか、少なくとも、検討時に使用されている RID の範囲が含まれている必要があります。検討時に使用されている RID の最大値から、使用されている RID の範囲を特定し、ユーザーマッピングを使用するときに設定する ID の範囲に問題がないことを確認してください。

システム管理者は、Microsoft 社から提供されているアプリケーションなどを使用して、ドメインコントローラーに最後に追加されたオブジェクトの SID を取得し、現在使用されている RID の最大値を確認できます。また、同一ドメイン内に複数のドメインコントローラーがある場合は、各ドメインコントローラーに最後に追加されたオブジェクトの SID を取得し、最大の RID を確認します。SID の取得手順については、利用するアプリケーションのドキュメントを参照してください。

例えば、次の条件で RID 方式のユーザーマッピングを使用すると仮定します。

- ・ 設定するドメインは 2 個 (Domain1 および Domain2)
- ・ 設定するドメインは互いに直接信頼関係を結んでいる
- ・ 検討時に使用されている RID の最大値は 8000
- ・ 各ドメインで毎年追加されるユーザーは 1,000 ユーザー (ただし、2 年目からは毎年 1,000 ユーザーを削除する)

- 各ドメインで毎年追加されるコンピュータアカウントは 1,000 件（ただし、2 年目からは毎年コンピュータアカウント 1,000 件を削除する）
- グループやほかのオブジェクトは追加・削除されない
- 設定するドメインの運用開始時から 100 年間運用する
- 検討時には予測できないオブジェクトの増加に対応するため、設定する ID の範囲に 50% の余裕値を加える

検討時に各ドメインで利用する SID の数

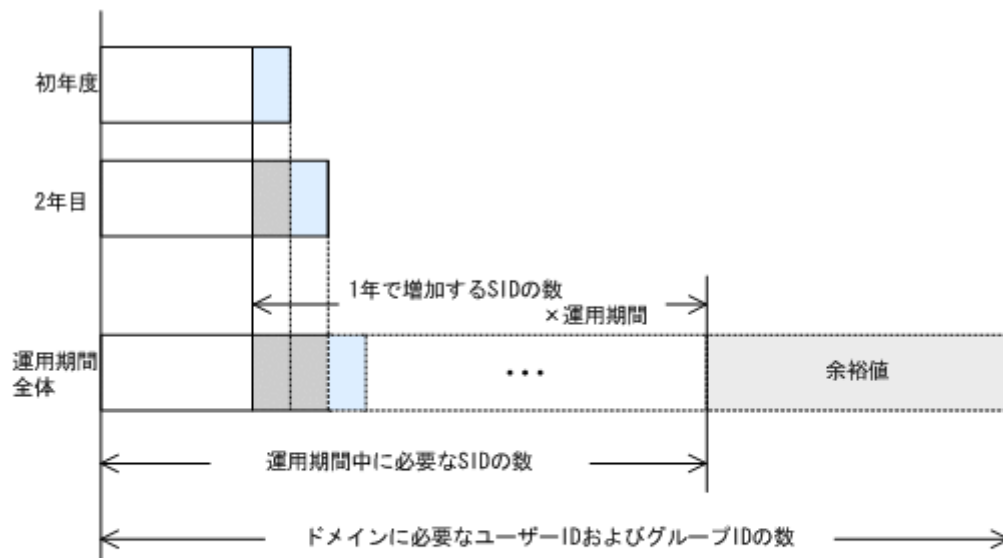
$$\begin{aligned} \text{SID の数} &= (\text{検討時に使用されている RID の最大値}) \\ &= 8,000 \end{aligned}$$

初年度以降に各ドメインで毎年増加する SID の数

$$\begin{aligned} \text{SID の数} &= (\text{追加されるユーザー}) + (\text{追加されるコンピュータアカウント}) \\ &= 1,000 + 1,000 = 2,000 \end{aligned}$$

この条件で必要とされるユーザー ID およびグループ ID の見積もり例を次の図に示します。

図 4-8 ユーザー ID およびグループ ID の見積もり例



(凡例)

- : 検討時に使用されているSIDの数
- : 1年で増加するSIDの数
- : 1年で削除されるSIDの数

計 2,000 件のオブジェクトが毎年追加されるため、SID は毎年 2,000 ずつ増加します。なお、初年度以降、計 2,000 件のオブジェクトが毎年削除されますが、削除されたオブジェクトが利用していた ID は再利用できません。

各ドメイン (Domain1 および Domain2) で必要な ID の数

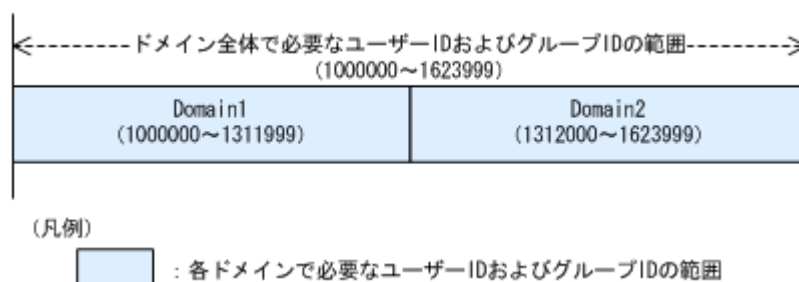
$$\begin{aligned} \text{1 ドメインに必要な ID の数} &= (\text{検討時の SID の数} + \\ &\quad (\text{1 年で増加する SID の数} \times \text{運用予定年数})) \times \\ &\quad (100 (\%) + \text{余裕値} (\%)) \\ &= (8,000 + (2,000 \times 100)) \times 1.5 = 312,000 \end{aligned}$$

ドメイン全体に必要な ID の数 (各ドメインに必要な ID の数の合計)

ドメイン全体に必要な ID の数=1 個目のドメインに必要な ID の数+
2 個目のドメインに必要な ID の数+...
312,000+312,000=624,000

ユーザー ID およびグループ ID は、70000~2147483147 の範囲で指定します。この見積もり例で、ユーザー ID およびグループ ID の最小値を 1000000 とした場合に設定する範囲の例を次に示します。

図 4-9 ユーザー ID およびグループ ID の設定例



ドメイン全体に必要なユーザー ID およびグループ ID の範囲

1000000~1623999

Domain1 で必要なユーザー ID およびグループ ID の範囲

1000000~1311999

Domain2 で必要なユーザー ID およびグループ ID の範囲

1312000~1623999

4.5 ファイルシステムの運用を開始する前に

HVFP/HDI では、最大で 1PB のファイルシステムを構築できます。また、ボリュームマネージャー機能 (LVM) を利用して、1 つまたは複数の LU からファイルシステムを構築できます。LU とは「logical unit」の略で、論理的に分割されたディスク領域のことです。Dynamic Provisioning と連携している場合は、仮想 LU を割り当てることもできます。ノードに複数のストレージシステムを接続して運用している場合、同一のストレージシステム内の LU からファイルシステムを構築する必要があります。

クラスタ構成の場合、LU をユーザー LU (デバイスファイル) として割り当て、ファイルシステムに使用します。

シングルノード構成の場合、ファイルシステムにはボリュームグループを使用します。ボリュームグループは、内蔵ハードディスクまたはストレージシステム内の LU を管理する単位です。1 つのボリュームグループに 1 つまたは複数の LU を割り当てます。1 つのボリュームグループを複数のファイルシステムで使用できます。

ファイルシステムを構築するときの注意事項を次に示します。

- ファイルシステムの使用率が 100%に近い状態で運用を継続すると、次のような問題が発生するおそれがあります。ファイルシステムの使用率が 95%を超えないように運用することを推奨します。
 - ファイルシステムへのアクセス性能が低下したり、ファイルの作成に失敗したりする。

- HCP からのデータをリコールしたり、ほかのファイルサーバからデータをインポートしたりするときエラーが発生する。
- ファイル移動タスク、容量削減タスクおよびマイグレーションタスクが正しく実行されない。

fsfullmsg コマンドで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できます。

- ファイルシステム内に作成できるファイル数の目安は次のとおりです。
 - Advanced ACL タイプのファイルシステム：約 2 億 4,000 万個
 - HCP にデータをマイグレートするファイルシステム：約 2 億 4,000 万個
 - そのほかのファイルシステム：約 40 億個

上限を超えるファイルを作成する場合は、別のファイルシステムを使用してください。ファイル数が上限を超えることを防ぐため、fsfullmsg コマンドで inode の使用数を監視して、警告閾値を超えたときに通知される SNMP トラップ (KAQG90003-W) を SNMP マネージャーで受信するよう設定できます。また、fslist コマンドで、inode の使用数 (I-node used) や残数 (I-node free) を定期的に確認することもできます。

- HVFP/HDI のファイルシステムでは、ファイルごとに 1 ブロック (4KB) が割り当てられます。
- HVFP/HDI で構築したファイルシステムは、CIFS クライアント環境との互換性を高めるために、ファイルの最終アクセス日時 (atime)、最終更新日時 (ctime) および最終編集日時 (mtime) のほか、ファイルの作成日時も記録できます。ただし、NFS クライアントからは作成日時を参照できません。

このほか、ファイルシステムを管理するに当たって知っておく必要があることを、以降で説明します。

4.5.1 LU (デバイスファイル) やボリュームグループの作成方法

HVFP/HDI で運用する LU には、ファイルシステムに使用するユーザー LU と、クラスタ構成やファイルシステムなどに関する設定情報を格納する共有 LU があります。

ストレージシステムにファイルシステムを構築する場合、システム管理者は、Device Manager または Hitachi Storage Navigator Modular 2 で LU を作成します。Device Manager または Hitachi Storage Navigator Modular 2 を使用すると、ディスクドライブの配置やパリティグループ、I/O 性能などを考慮して LU を作成できます。LU を作成する手順は、Device Manager または Hitachi Storage Navigator Modular 2 のマニュアルを参照してください。ストレージシステムの管理者が異なるときは、ストレージシステムの管理者に LU の作成を依頼してください。クラスタ構成の場合は、共有 LU として使用する LU もストレージシステムに作成してください。共有 LU には 70GB の容量が必要です。

ファイルシステムを構築または拡張するときに自動作成される LU を含めて、クラスタ構成の場合は最大 511 個かつ LUN が 16 進数で 0000~01FF の範囲で、シングルノード構成の場合は最大 256 個かつ LUN が 16 進数で 00~FF の範囲で作成できます。

なお、ノードの内蔵ハードディスクをファイルシステムで使用するシングルノード構成の場合は、ノードの OS を起動した際に、内蔵ハードディスクから LU が自動的に割り当てられます。このため、システム管理者が LU を作成する必要はありません。

LU を作成したあと、運用に合わせて次の作業を実施してください。

クラスタ構成の場合

初期導入時は、ノードへの FC パスが設定された LU は、ユーザー LU (デバイスファイル) として自動的に割り当てられます。メンテナンス時など、ユーザー LU に自動的に割り当てら

れないように設定を変更した場合は、システム管理者が手動で割り当ててください。ノードへの FC パスが設定された LU をユーザー LU として手動で割り当てる方法については、「コマンドリファレンス」を参照してください。

シングルノード構成の場合

初期導入時は、内蔵ハードディスクやノードへの FC パスが設定されたストレージシステムの LU は、新規に作成されたボリュームグループに自動的に割り当てられます。LU をボリュームグループに自動的に割り当てる場合、同じドライブ種別（仮想 LU の場合は同じプール）で、同じ筐体内（内蔵ハードディスクまたは同じストレージシステム）にある LU ごとにボリュームグループが作成・管理されます。

内蔵ハードディスクやストレージシステムを増設し、新規に LU を作成する場合は、WWW ブラウザーを使用して HVFP/HDI のシステムにログインすることで、自動的に LU をボリュームグループに割り当てることができます。ディスクを増設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。

4.5.2 LU を割り当てるときの注意事項

クラスタ構成の場合はファイルシステムに、シングルノード構成の場合はボリュームグループに LU を割り当てるときの注意事項を次に示します。

- LU のドライブ種別によって、I/O 性能や処理速度が異なります。システム管理者は、ファイルシステムの用途やドライブの特性などを十分に考慮して、使用する LU を決定してください。
- 冗長構成が異なる LU を混在して使用しないでください。ファイルシステムやボリュームグループを構成する LU の冗長構成が異なる場合、最も冗長度が少ない LU の耐障害性に依存します。Hitachi AMS2000 シリーズまたは HUS100 シリーズを使用している場合は、ファイルシステムやボリュームグループを作成する前に、Hitachi Storage Navigator Modular 2 を使用して LU を確認してください。Virtual Storage Platform、Universal Storage Platform V/VM または HUS VM を使用している場合やストレージシステムの管理者が異なる場合は、ストレージシステムの管理者に問い合わせてください。
- ストレージシステムに作成した LU の容量を変更した場合、クラスタ構成では Processing Node のリフレッシュ処理を実行してください。シングルノード構成では fpstatus コマンドを実行してください。
- Dynamic Provisioning と連携して仮想 LU をファイルシステムやボリュームグループに割り当てる場合は、仮想 LU が属するプールの容量が不足しないように運用する必要があります。プールの容量が不足すると、ファイルシステムを利用するクライアントでアプリケーションが異常終了したり、HVFP/HDI で障害が発生したりするおそれがあります。なお、複数のプールから作成された仮想 LU を使用しているファイルシステムでは、どれか 1 つでもプールの容量が不足すると、ファイルシステムの使用量が上限に達していなくても、障害が発生するおそれがあります。
- ファイルシステム内のファイルを大量に削除した場合には、dpreclaim コマンドを実行して、ファイルシステムで使用している仮想 LU の未使用領域を解放できます。1GB 以上のデータを削除したときや差分スナップショットを削除したときなどにコマンドを実行することで、仮想 LU が属するプールの容量不足を防ぎます。
dpreclaim コマンドを実行する前に次のことを確認してください。
 - Hitachi AMS2000 シリーズまたは HUS100 シリーズを使用している場合、dpreclaim コマンドを実行しても仮想 LU の未使用領域を解放できないことがあります。コマンドを実行したあと、Hitachi Storage Navigator Modular 2 を使用して DP プールを最適化してください。
 - ファイルスナップショット機能を運用している場合、ユーザーデータが格納されなくなった領域も差分スナップショットの管理のために使用されます。このため、dpreclaim コマン

ドを実行しても十分な効果を期待できません。自動作成される差分スナップショットの上限を引き下げたときなど、差分格納デバイスの使用量が大幅に減少した際に dpreclaim コマンドを実行してください。

- DP プール内のページ単位で未使用領域が解放されるため、ページ全体が未使用領域になるまでは解放できません。このため、dpreclaim コマンドを実行しても、削除したファイル分の容量を解放できないことがあります。
- 削除したファイルシステムやボリュームグループに割り当てていた仮想 LU の容量を解放するためには、仮想 LU を削除する必要があります。

4.5.3 Virtual Server で利用する LU

Virtual Server を使用する場合、システム管理者は、作成された LU のうち、容量が 50GB 程度の LU を Virtual Server OS LU として Virtual Server に割り当てます。また、Virtual Server 上で構築・運用するファイルシステムに使用するための LU を割り当てます。ファイルシステムの容量だけでなく、Virtual Server OS LU に使用する容量を考慮して Virtual Server に LU を割り当ててください。指定できるユーザー LU 数の上限値については、「仮想サーバ環境セットアップガイド」を参照してください。

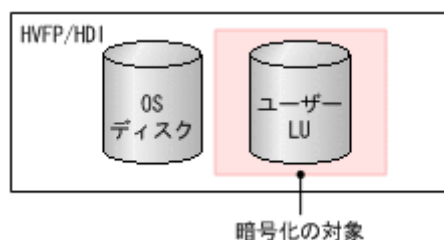
Virtual Server に割り当てたユーザー LU の容量を変更する場合は、LU の割り当てをいったん解除してから、容量を変更してください。LU の容量を変更したあと、Processing Node のリフレッシュ処理を実行してから、再度 Virtual Server で利用するユーザー LU として割り当ててください。

4.5.4 ローカルデータの暗号化機能を使用するときの注意事項

ユーザー LU を暗号化する機能（ローカルデータの暗号化機能）を使用する前に、次のことを確認してください。

- ローカルデータの暗号化機能で暗号化の対象となるのはユーザー LU だけです。また、ファイルやディレクトリなどのユーザーデータはファイルシステムにアクセスするときに復号されます。

図 4-10 HVFP/HDI の暗号化機能の対象



- システムを構築するときに暗号化機能を設定すると、運用開始後に切り替えることはできません。暗号化機能の設定を変更する場合は、システムを構築し直す必要があります。
- 暗号化に使用する共通鍵は、HVFP/HDI のシステム LU または HCP のどちらかに保存されます。システム設定情報を HCP に定時保存する場合は、HCP に鍵が保存されます。そのため、システム設定情報を HCP に定時保存する場合は、ノードの OS を起動する前に、HCP が正常に稼働していること、および HVFP/HDI と HCP が正常に通信できる状態であることを確認してください。
- システム設定情報を HCP に定時保存しない場合、システム LU に保存されている鍵が破損すると、ユーザーデータを使用できなくなります。鍵を復旧するためには、システム設定情報を回復する必要があります。そのため、システムの設定やファイルシステムの構築など、HVFP/HDI の運用を開始するために必要な情報の設定が完了したあと、[Backup Configuration] ダイアログでシステム設定情報ファイルをダウンロードし、必ずシステム外の記録媒体に保管してください。

い。運用開始後も、システムの設定を変更したときには必ず手動でシステム設定情報を保存して、システム設定情報ファイルをシステム外の記録媒体に保管してください。

- システム設定情報を HCP に定時保存する場合、HCP に保存されている鍵を取得できなくなると、ユーザーデータを使用できなくなります。障害発生に備えて、暗号化機能を有効にしたら、`encdisplaykey` コマンドでシステム外の記録媒体に保存するための鍵を表示し、保存しておくことをお勧めします。システム外の記録媒体に鍵を保存したら、HCP に保存されている鍵とシステム外の記録媒体に保存した鍵を `encverifykey` コマンドで照合してください。

4.5.5 ファイルシステム使用量に関する警告の通知

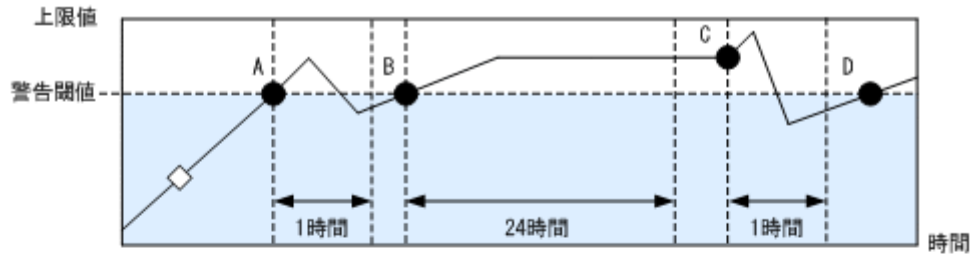
障害情報の SNMP 通知または E-mail 通知を設定している場合、ファイルシステムの使用量が上限に達したり、設定された値（警告閾値）を超えたりした際に、ファイルシステムの使用状況に関する警告が通知されます。

初期導入時は、使用量が警告閾値を超えると、ファイルシステムの使用量に関する警告が通知されるように設定されています。システム管理者は、ファイルシステムの使用量に関して警告が通知されるよう設定したり、設定を解除したりできます。また、設定した情報を参照したり、警告閾値を変更したりできます。

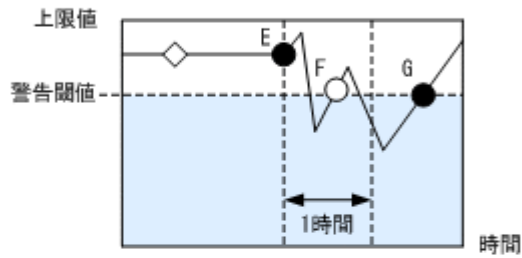
警告が通知されるよう設定した場合、ファイルシステムの使用量が上限に達したり、警告閾値を超えたりしたときには、メッセージ（KAQG90002-W から KAQG90005-W）が通知されます。一度警告が通知されたあとは、ファイルシステムの使用状況に応じて、以降に警告が通知される契機が変わります。警告が通知される契機を次の図に示します。

図 4-11 ファイルシステム使用量に関する警告が通知される契機（ブロック使用量を監視する場合）

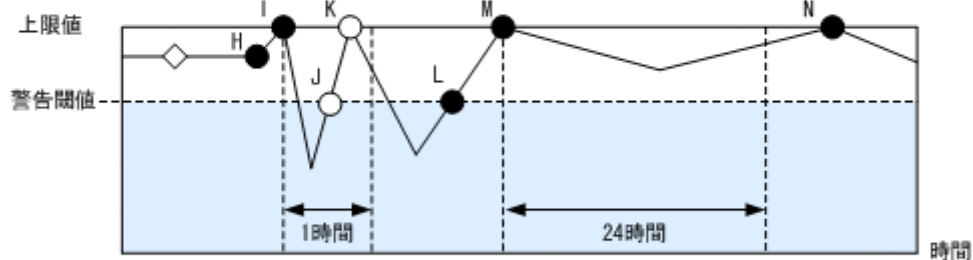
例 (1)



例 (2)



例 (3)



例 (4)

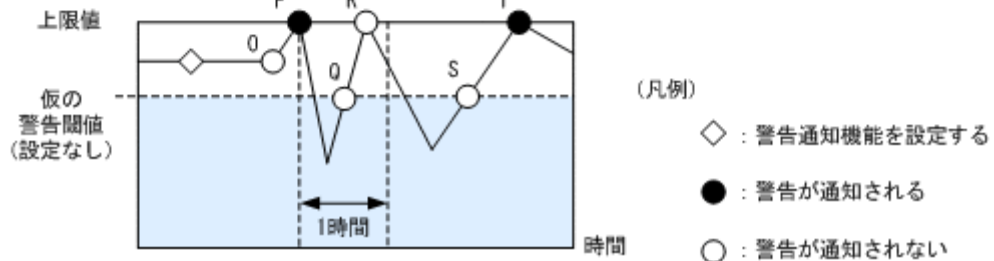
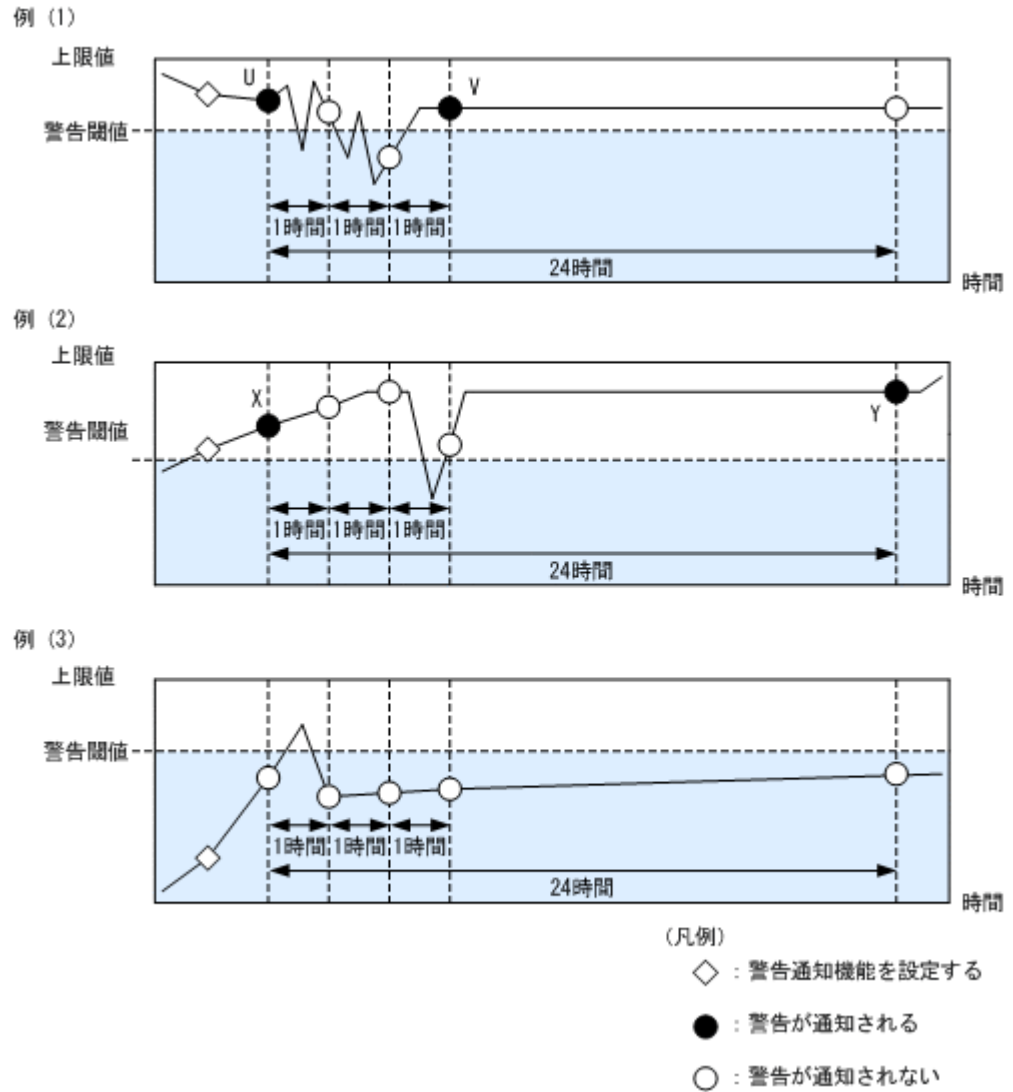


図 4-12 ファイルシステム使用量に関する警告が通知される契機 (inode 使用量を監視する場合)



inode 使用量は 1 時間間隔で監視され、その際に警告も通知されます。

ファイルシステム使用量に関する警告が通知される契機を次の表に示します。

表 4-1 ファイルシステム使用量に関する警告が通知される契機

状態	警告が通知される契機	図中の記号
ブロック使用量が警告閾値を超過	警告が通知されるよう設定したあと、ブロック使用量が警告閾値を初めて超えたとき	A
	警告が通知されるよう設定した時点でブロック使用量が警告閾値を超えていて、そのあとでファイルシステムを使用したとき	E, H
	次の 2 つの条件を満たすとき	B, D, G, L
	<ul style="list-style-type: none"> ・ 以前にブロック使用量が警告閾値を超えたときの警告から 1 時間が経過※1 ・ ブロック使用量が警告閾値を超過 	
ブロック使用量が上限に到達	次の 2 つの条件を満たすとき	C
	<ul style="list-style-type: none"> ・ 以前にブロック使用量が警告閾値を超えたときの警告から、警告閾値を超えたままの状態 で 24 時間が経過 ・ ファイルシステムを使用した 	
ブロック使用量が上限に到達	警告が通知されるよう設定したあと、ブロック使用量が初めて上限に到達したとき	I, P

状態	警告が通知される契機	図中の記号
	次の 2 つの条件を満たすとき <ul style="list-style-type: none"> • 以前にブロック使用量が上限に到達したときの警告から 1 時間が経過※1 • ブロック使用量が警告閾値を下回ってから再度上限に到達※2 	M, T
	次の 2 つの条件を満たすとき <ul style="list-style-type: none"> • 以前にブロック使用量が上限に到達したときの警告から、警告閾値を超えたままの状態が 24 時間以上経過 • ブロック使用量が再度上限に到達 	N
inode 使用量が警告閾値を超過	警告が通知されるよう設定してから初めて inode 使用量を監視した際に、警告閾値を超えていたとき	U, X
	以前に inode 使用量を監視した時点では警告閾値を超えていなかったが、その 1 時間後に inode 使用量を監視した際に警告閾値を超えていたとき	V
	次の 2 つの条件を満たすとき <ul style="list-style-type: none"> • 以前に inode 使用量が警告閾値を超えたときの警告から、監視した時点での inode 使用量が警告閾値を超えたままの状態が 24 時間が経過 • inode 使用量を監視した際に警告閾値を超過 	Y

注 次の操作を実行すると、それまでの状態に関わらず、警告が通知されるよう最初に設定した時点の状態に戻ります。

- 設定を解除し、再度設定したとき
- 警告閾値を変更したとき
- ファイルシステムをアンマウントしたあと、再度マウントしたとき
- 警告閾値を百分率 (%) で指定したあと、ファイルシステムを拡張したとき (警告閾値が再計算される時)

注※1

一度警告が通知されてから 1 時間が経過するまでの間、同じ警告が再度通知されることはありません (図中の記号 F, J, K, R の場合)。

注※2

警告閾値が「0」の場合、ブロック使用量が上限に達してから再度上限に到達するまでの間に、警告閾値を下回ったかどうかを判断するため、仮の警告閾値が設定されます。ただし、ブロック使用量が仮の警告閾値を超過しても警告は通知されません (図中の記号 O, Q, S の場合)。

4.5.6 ストライピング機能を使用するとき

HVFP/HDI では、ボリュームマネージャーのストライピング機能を使用したファイルシステムを構築できます。

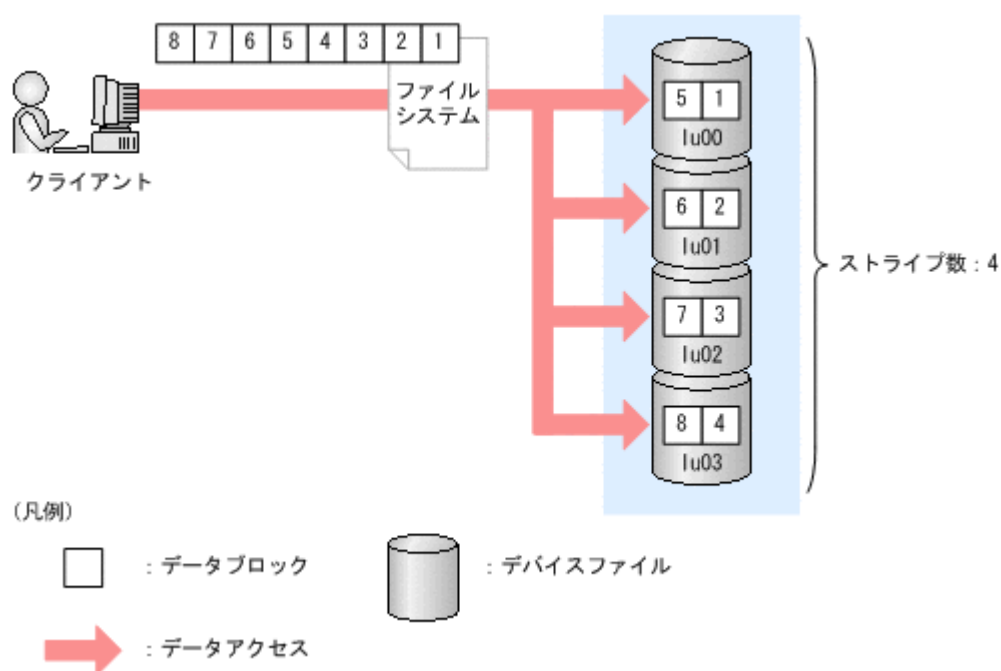
(1) ストライピング機能とは

ストライピング機能は、ボリュームマネージャー (LVM) が提供する機能の一つです。ストライピング機能を使用することで、ファイルシステムの連続したデータブロックが任意のサイズに分割され、複数のデバイスファイルに均等に割り当てられます。分割されたデータブロックに対して並列に I/O 処理が行われるため、ファイルシステムへのアクセス速度の向上が期待できます。

ストライピング機能を使用したときのデータブロックの割り当てについて次の図に示します。ファイルシステムを構築するときに指定したデバイスファイルの数がストライプ数になります。また、

指定したデバイスファイルの順にデータブロックが割り当てられます。図の例では lu00, lu01, lu02, lu03 の順に指定しています。

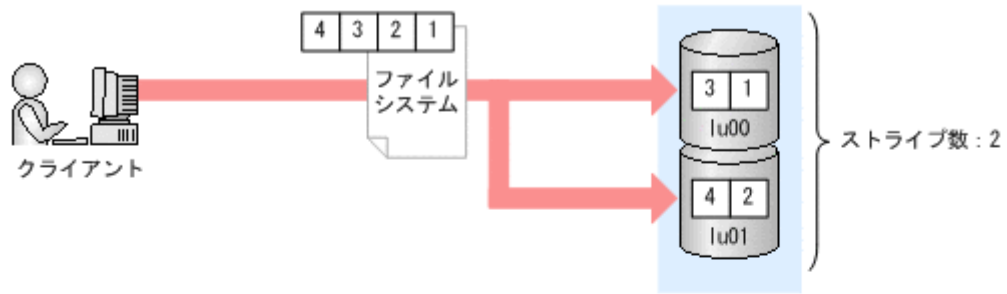
図 4-13 ストライピング機能の運用例



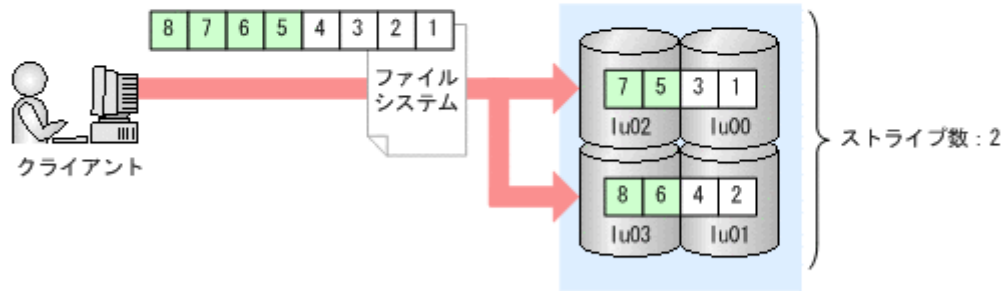
また、ストライピング機能を使用しているファイルシステムの容量を拡張したときのデータブロックの割り当てについて次の図に示します。ファイルシステム容量を拡張しても、拡張前と同じストライプ数が適用されます。

図 4-14 ストライピング機能の運用例（ファイルシステム拡張時）

■ファイルシステム容量の拡張前



■ファイルシステム容量の拡張後（lu02およびlu03を追加）



(凡例)



ファイルシステムの構築時に lu00, lu01 の順序で指定し、拡張時に lu02, lu03 の順序で指定した場合、lu00 と lu02, lu01 と lu03 がそれぞれ 1 本のストライプとして設定されます。

(2) ストライピング機能を使用するときの注意事項

ボリュームマネージャーのストライピング機能を使用するときの注意事項を次に示します。

- ファイルシステムを構築したり拡張したりする際にすべて同じ容量のデバイスファイルを指定してください。
- ファイルシステムを拡張するときは、ストライプ数と同じ数のデバイスファイルを指定してください。
- パリティグループがすべて異なるデバイスファイルを指定してファイルシステムを構築してください。同じパリティグループのデバイスファイルを指定してファイルシステムを構築すると、ストライピング機能を使用したときにアクセス性能を改善できないことがあります。
- ファイルスナップショット機能を使用する場合は、作成元のファイルシステムと差分格納デバイスでそれぞれ別々にストライピング機能を使用できます。

4.5.7 ファイルシステムで利用する ACL タイプの選択

HVFP/HDI では、ファイルやディレクトリに対してアクセス制御リスト（ACL）を設定できます。HVFP/HDI が提供するファイルシステムには、NTFS ACL に準拠した ACL を設定できる Advanced ACL タイプと、POSIX ACL に準拠した ACL を設定できる Classic ACL タイプの 2 つがあります。

システム管理者は、ファイルシステムを構築する際に、ファイルシステムで使用する ACL タイプを選択します。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ます。

NFS クライアントから、各 ACL タイプのファイルシステムを利用する場合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たクライアントから、Advanced ACL タイプまたは Classic ACL タイプのファイルシステムでファイルをコピーしても、元のファイルの ACL はコピーされません。なお、NFSv4 プロトコルを使用したクライアントの場合は、クライアントの環境によって、ACL をコピーできるかどうか異なります。
- NFSv2 プロトコルを使用したクライアントから Advanced ACL タイプのファイルシステムにアクセスできません。
- NFS クライアントから `chgrp` コマンドを実行する場合、ファイルシステムで使用している ACL タイプによって、コマンドを実行できるユーザーが異なります。

Advanced ACL タイプ

root ユーザーのほか、「所有権の取得」のアクセス権限があるユーザーもコマンドを実行できます。

Classic ACL タイプ

root ユーザーだけがコマンドを実行できます。

- NFS クライアントから `ln` コマンドを実行してシンボリックリンクを作成する場合、ファイルシステムで使用している ACL タイプによって、リンクファイルのパーミッションモードが異なります。

Advanced ACL タイプ

親ディレクトリのアクセス制御エントリ（ACE）に依存してパーミッションモードが設定されます。

Classic ACL タイプ

固定値（777）が設定されます。

なお、リンクファイルのアクセス権限は、リンクファイルのパーミッションモードではなく、シンボリックリンク先のファイルのパーミッションモードに従います。

- 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、HVFP/HDI で管理されていないユーザーまたはグループが Advanced ACL に設定されているファイルに対して、Advanced ACL を参照するコマンドを実行するとエラーになることがあります。例えば、Advanced ACL タイプのファイルシステムで、オプションなしの `ls` コマンドを実行すると結果が正常に表示されますが、`-l` オプションを指定した `ls` コマンドを実行するとエラーになります。
- NFSv4 プロトコルを利用すると、NFS クライアントから ACL を参照または設定できます。ただし、Linux を利用している NFS クライアントからは、HVFP/HDI で設定できる ACE の上限が規定の値を下回ることがあるため、ACE を設定できなくなることがあります。ACE の上限については、表 4-2 Advanced ACL タイプと Classic ACL タイプのファイルシステムの相違を参照してください。

Advanced ACL タイプと Classic ACL タイプのファイルシステムの相違について、次の表に示します。

表 4-2 Advanced ACL タイプと Classic ACL タイプのファイルシステムの相違

項目	Advanced ACL タイプ	Classic ACL タイプ
準拠する仕様	NTFS ACL※1	POSIX ACL
ファイルまたはディレクトリの所有者	ユーザーまたはグループ	ユーザー
ACE の上限※2	700 個	128 個（アクセス ACL およびデフォルト ACL の上限はそれぞれ 64 個）
ACE の種別	許可または拒否	許可
設定するアクセス権※3	<ul style="list-style-type: none"> フルコントロール 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 	<ul style="list-style-type: none"> 読み取り 書き込み 実行
ファイルまたはディレクトリの新規作成時に設定される ACL	親ディレクトリから継承した ACL ただし、親ディレクトリから継承した ACL が設定されていない場合は、CIFS 共有を作成するときに設定した初期パーミッション	CIFS 共有を作成するときに設定した初期パーミッション
利用できるファイル属性（DOS 属性）	<ul style="list-style-type: none"> 読み取り専用属性 アーカイブ属性 ディレクトリ属性 隠しファイル属性 システムファイル属性 	<ul style="list-style-type: none"> 読み取り専用属性 ディレクトリ属性

注※1

HVFP/HDI では、随意アクセス制御リスト（DACL）だけをサポートします。Windows 標準の監査機能は利用できません。HVFP/HDI が提供する CIFS アクセスログを利用してください。

注※2

Windows の NTFS ACL では 700 個を超える ACE を設定できますが、HVFP/HDI が提供するファイルシステムで設定できる ACE の上限値は 700 個または 128 個（アクセス ACL およびデフォルト ACL の上限はそれぞれ 64 個）です。

注※3

NFS クライアントから NFSv4 ACL を設定すると、対象のファイルシステムで使用している ACL タイプに応じてアクセス権がマッピングされます。

4.5.8 Advanced ACL タイプのファイルシステムへの移行

HVFP/HDI では、運用中の Classic ACL タイプのファイルシステムを Advanced ACL タイプのファイルシステムに移行できます。

Classic ACL タイプのファイルシステムと Advanced ACL タイプのファイルシステムでは、アクセス許可の権限に対する評価方法に次のような相違があります。

Advanced ACL タイプのファイルシステム

ユーザーのアクセス権とは、ユーザーに権限が与えられていない場合でも、所属グループやその他 (Everyone) に与えられた権限で評価されます。例えば、ユーザーに対して書き込み権限が与えられていなくても、所属グループやその他 (Everyone) に書き込み権限が設定されていれば、ユーザーはファイルを更新できます。

Classic ACL タイプのファイルシステム

ユーザーのアクセス権とは、ユーザーに与えられた権限だけで評価されます。例えば、ユーザーに対して読み取りだけを許可する権限が設定されている場合、所属グループやその他 (Everyone) に書き込み権限が与えられていても、ユーザーはファイルを更新できません。

これらの評価方法の相違から、Windows のプロパティ画面で表示される「アクセス許可」でチェックされた権限が、その他 (Everyone) よりも少ない所属グループやユーザー、または、所属グループよりも少ないユーザーに対して、移行前のアクセス権の権限を超えないようにするために、移行後のファイルシステムでは拒否の ACE が追加されます。

また、ファイルシステムの移行前後で、Windows のプロパティ画面の「アクセス許可」に表示されている内容が変わることがあります。例えば、移行前には「フルコントロール」が表示されていても、移行後には「特殊」が表示されることがあります。

Classic ACL タイプのファイルシステムで設定された ACL の継承関係やアクセス権を引き継いで ACL が変換されるため、移行前後で ACL が異なることがあります。ファイルやディレクトリを利用する CIFS クライアントが意図しない ACL に変換された場合、移行後のファイルシステムで ACL を再設定する必要があります。システム管理者は、ファイルシステム移行時の注意事項を十分に確認した上で、移行するかどうかを決定してください。

移行後のファイルシステムでは、クライアントから確認できるアクセス権の見え方よりも、ファイルやディレクトリへのアクセス可否が変わらないことを優先して ACL が作成されます。クライアントの ACL の運用によっては、移行前後でアクセス権の見え方が異なることで、ファイルシステムを運用しにくくなる場合があります。

Classic ACL タイプのファイルシステムを Advanced ACL タイプのファイルシステムに移行するときの注意事項については、「[\(1\) ファイルシステム移行時の注意事項](#)」を参照してください。

参考：

以降でアクセス権を説明するときは、次の形式で表示します。
「< 8 進数で表したアクセス権 > (< 略称で表したアクセス権 >)」
表示されるアクセス権の詳細について次の表に示します。

表 4-3 表示されるアクセス権の詳細

8 進数で表したアクセス権	略称で表したアクセス権	説明
7	rwx	読み取り、書き込みおよび実行のアクセス権を表します。
6	rw-	読み取りおよび書き込みのアクセス権を表します。
5	r-x	読み取りおよび実行のアクセス権を表します。
4	r--	読み取りのアクセス権を表します。
3	-wx	書き込みおよび実行のアクセス権を表します。

8進数で表したアクセス権	略称で表したアクセス権	説明
2	-w-	書き込みのアクセス権を表します。
1	--x	実行のアクセス権を表します。
0	---	アクセス権がないことを表します。

(1) ファイルシステム移行時の注意事項

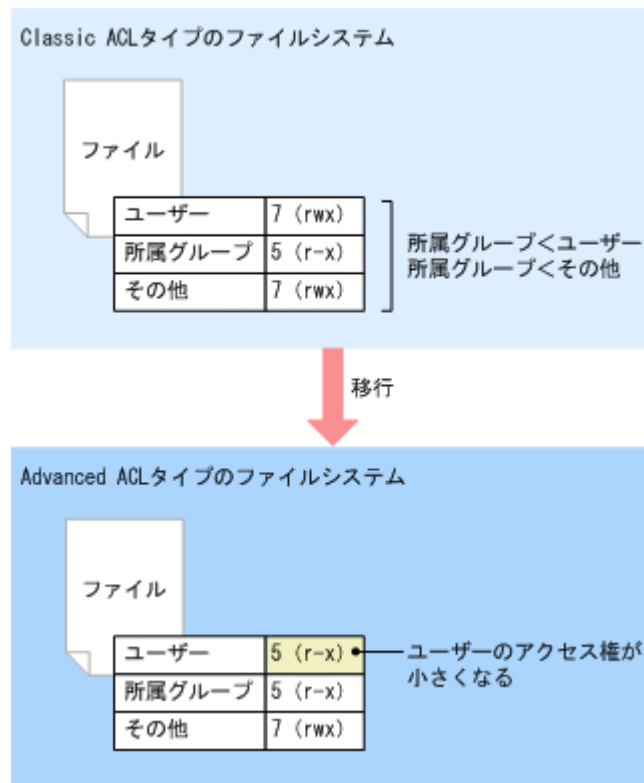
HVFP/HDI では、Classic ACL タイプから Advanced ACL タイプのファイルシステムに移行しても、継承関係やアクセス権を継続できるように ACL を作成します。

Classic ACL タイプのファイルシステムで設定されるアクセス権は許可だけですが、継承関係やアクセス権を継続するために、移行後に作成される ACL には拒否の ACE が追加されることもあります。移行前に Classic ACL タイプのファイルシステムで設定したアクセス権と、移行後に作成されるアクセス権との対応については、「付録 A. Advanced ACL タイプのファイルシステムへの移行後に作成される ACL」を参照してください。

このほか、Classic ACL タイプから Advanced ACL タイプのファイルシステムに移行するときの注意事項を次に示します。

- CIFS クライアントの「ファイルの実行」のアクセス権は、Classic ACL タイプのファイルシステムでは「4 (r--)」に対応しますが、Advanced ACL タイプのファイルシステムでは「1 (--x)」に対応します。移行するファイルシステムにアクセス権が「4 (r--)」の実行形式のファイルがある場合は、アクセス権に「1 (--x)」を追加しないと、移行後にファイルを実行できなくなります。移行前にアクセス権を変更するか、移行時に `fsctl` コマンドで「1 (--x)」を追加してください。なお、親ディレクトリのアクセス権に「1 (--x)」がない場合に、`fsctl` コマンドでファイルのアクセス権に「1 (--x)」を追加すると、継承関係にあった親ディレクトリと配下のファイルのアクセス権に相違が発生し、継承関係がなくなります。
- アクセス可否は変わりませんが、クライアントから確認できるアクセス権の見え方が移行前後で異なることがあります。移行後にユーザーのアクセス権の権限が小さくなる場合の例（その 1）を次の図に示します。

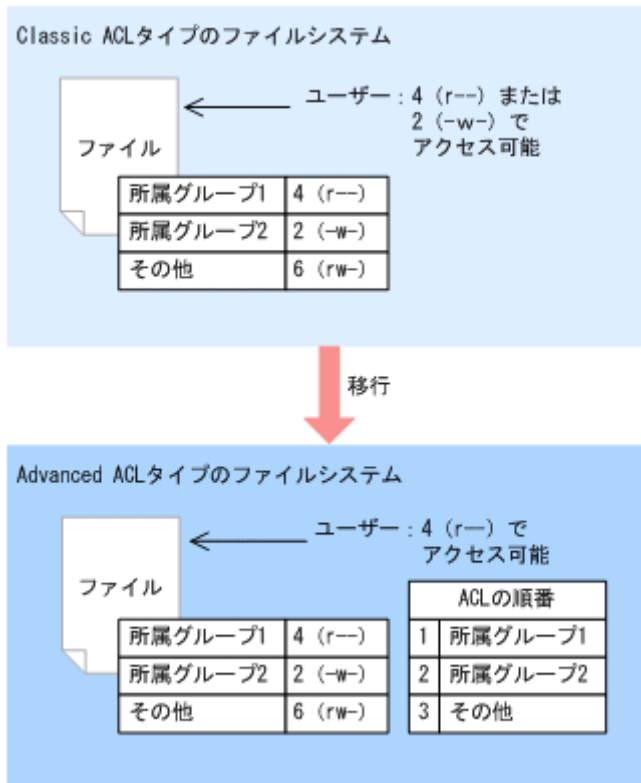
図 4-15 移行後にユーザーのアクセス権の権限が小さくなる場合の例（その 1）



あるユーザーが、その他 (Everyone) よりもアクセス権の権限が小さいグループに所属し、ユーザーのアクセス権の権限がグループより大きい場合、ファイルシステムを移行するとグループに対して拒否の ACE が追加されます。Advanced ACL タイプのファイルシステムでは拒否の ACE が許可の ACE より先に評価されるため、移行後にユーザーのアクセス権の権限が小さくなります。

- 移行後のファイルシステムでアクセス可否に影響がある場合は、アクセス権の権限が小さくなるように ACL が作成されます。移行後にユーザーのアクセス権の権限が小さくなる場合の例（その 2）を次の図に示します。

図 4-16 移行後にユーザーのアクセス権の権限が小さくなる場合の例（その2）



あるユーザーが、その他（Everyone）よりもアクセス権の権限が小さい2つ以上のグループに所属し、自分が所有者でないファイルに対してグループごとに異なる権限が与えられている場合は、移行後にユーザーのアクセス権の権限が小さくなります。

- ファイルシステムを移行すると、Windowsのプロパティ画面で表示される [アクセス許可] の情報が移行前後で異なることがあります。例えば、設定されたアクセス権が「7 (rwx)」の場合、Classic ACLタイプのファイルシステムでは、「フルコントロール」の権限が与えられているように表示されますが、移行後には「削除」だけが許可されていないよう表示されます。
- Advanced ACLタイプのファイルシステムでは、NFSv2プロトコルを利用できません。移行後のファイルシステムでNFSv2プロトコルを利用するクライアントがないことを確認してください。
- HVFP/HDIでは、Classic ACLタイプからAdvanced ACLタイプのファイルシステムに移行してもQuota情報が引き継がれます。

(2) 移行後のファイルシステム容量の見積もり

Advanced ACLタイプのファイルシステムに移行することで、各ACEの情報が増えるため、ファイルシステム容量が増加します。通常の場合、Advanced ACLタイプのファイルシステムでは、1ファイルまたは1ディレクトリ当たり4KBの領域をACEの格納領域として使用します。システム管理者は、十分な空き領域を確保してからファイルシステムを移行してください。

なお、1ファイルまたは1ディレクトリに対してACEが使用する領域は最大64KBです。Classic ACLタイプのファイルシステムで設定したACEの数が多い場合は、ファイルシステム容量を見積もる際に考慮してください。

(3) ファイルシステムの移行手順

移行するファイルシステムに、アクセス権が「4 (r--)」の実行形式のファイル（CIFSクライアントから実行できるファイル）がある場合、移行後にファイルを実行できなくなります。システム管

理者は、移行前にアクセス権を変更するようファイル所有者に依頼するか、`fsctl` コマンドでファイルのアクセス権を変更する必要があります。

`fsctl` コマンドを実行すると、指定した拡張子のファイルのアクセス権が自動的に変更されます。システム管理者がファイルの拡張子を特定できなかったり、ファイル所有者以外にファイルのアクセス権を変更できない運用だったりする場合は、ファイル所有者にアクセス権の変更を依頼してください。

Classic ACL タイプのファイルシステムを Advanced ACL タイプのファイルシステムに移行する手順を次に示します。

1. エンドユーザーに連絡します。

作業中、移行するファイルシステムにアクセスしないようエンドユーザーに連絡してください。また、アクセス権が「4 (r--)」の実行形式のファイルに対して、ファイル所有者がアクセス権を変更する場合は、事前に対応を依頼してください。

2. 移行するファイルシステムのバックアップを取得します。

3. 実行形式のファイルのアクセス権に「1 (-x)」を追加します。

移行後もファイルを実行できるよう、`fsctl` コマンドで「4 (r--)」の実行形式のファイルのアクセス権に「1 (-x)」を追加してください。

```
$ sudo fsctl -c -x -o add_exeauth filesystem03/unit15
filesystem03/unit15: Wait ..... Success
```

4. すべてのファイル共有の設定情報を記録します。

`cifslist` コマンドまたは `nfslist` コマンドで、移行するファイルシステム内のすべてのファイル共有の設定情報を確認し、記録してください。

```
$ sudo cifslist -v -O all
List of File Shares:
The number of CIFS share(1)
Name of file share           : unit15
Shared directory             : /mnt/filesystem03/unit15
Use ACL                       : use
Server specification         : --
Comment for file share       :
Permission mode              : rw
Browse permission            : permit
File access permissions      : rw,rw,rw
Directory access permissions : rw,rw,rw
Write disallowed users       : sys04
Write disallowed groups      : --
Write allowed users          : --
Write allowed groups         : --
Guest account access         : default
Disk synchronization policy  : default
CIFS client cache            : default
File timestamp changeable    : default
Home directory               : do_not_use
CIFS access log (success)    : none
CIFS access log (failure)    : none
ACL type                      : Classic ACL
Client access policy         : parallel
Volume Shadow Copy Service   : default
Read-only cache for conflicts : default
Access Based Enumeration     : default

$ sudo nfslist -O all
List of File Shares:
The number of NFS share(1)
Shared directory             : /mnt/filesystem03/unit14
Public destination host/network : host01
Permission mode / Synchronous writing : rw_sync
Anonymous mapping           : root_only
Anonymous UID                : 65534
Anonymous GID                : 65534
Transmission port restriction : do_not_perform
Subtree check                 : do_not_perform
Access check with lock request : do not perform
```

```
Maximum rsize (KB)           : --
Host/network name resolution : OK
Security flavor              : sys,krb5i
```

5. すべてのファイル共有を解除します。

cifsdelete コマンドまたは nfsdelete コマンドで、ファイルシステム内のすべてのファイル共有を解除してください。

```
$ sudo cifsdelete -x unit15
$ sudo nfsdelete -d /mnt/filesystem03/unit14 -a
```

6. ファイルシステムをアンマウントします。

fsumount コマンドでファイルシステムをアンマウントしてください。

```
$ sudo fsumount filesystem03
```

7. ファイルシステムの ACL タイプを Advanced ACL タイプに変更してマウントします。

fsmount コマンドで、ファイルシステムの ACL タイプを Classic ACL タイプから Advanced ACL タイプに変更し、マウントしてください。

```
$ sudo fsmount -w -c filesystem03
```

8. ファイルの ACL タイプを Advanced ACL タイプに変換します。

fsctl コマンドでディレクトリやファイルの ACL タイプを Classic ACL タイプから Advanced ACL タイプに変換してください。

```
$ sudo fsctl -c -x -o advanced_acl filesystem03
filesystem03: Wait ..... Success
```

注意：

手順 7 でファイルシステムの ACL タイプを変更すると、ファイルシステム内のファイルやディレクトリに対してアクセスがあった際に、自動的にファイルやディレクトリの ACL タイプが変更されます。しかし、移行後のファイルシステムで空き容量が不足していると、ファイルやディレクトリの ACL タイプが変更されないことがあります。システム管理者は、ファイルシステムの十分な空き容量を確認し、fsctl コマンドを使用して、能動的にファイルやディレクトリの ACL タイプを変更してください。

9. ファイル共有を再度作成します。

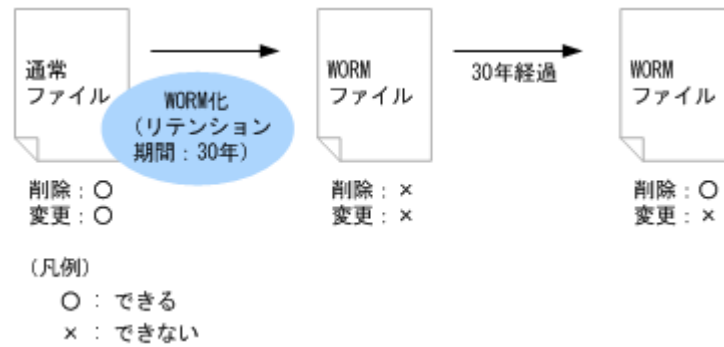
cifscreate コマンドまたは nfscreate コマンドでファイル共有を再度作成してください。

```
$ sudo cifscreate -x unit15 -d /mnt/filesystem03/unit15 -D add:sys04
$ sudo nfscreate -d /mnt/filesystem03/unit14 -H host01
```

4.5.9 WORM 対応ファイルシステムの運用

WORM 機能を有効にしたファイルシステム (WORM 対応ファイルシステム) では、ファイルを一定期間削除または変更できない状態にして保管できます。削除または変更できない状態のファイルを WORM ファイルと呼びます。また、ファイルを削除または変更できない期間をリテンション期間 (保管期間) と呼び、WORM ファイルごとに設定できます。リテンション期間が過ぎたファイルは削除できますが、変更できません。

図 4-17 WORM ファイルの動作



ファイルを WORM 化する方法を次に示します。

- 自動コミットを使用して WORM 化する
- クライアントから手動で WORM 化する

(1) 自動コミットを使用して WORM 化する

WORM 対応ファイルシステムを構築する際に、自動コミットを使用するかどうか設定できます。自動コミットを使用すると、読み取り専用にしたファイルに対して変更がない状態で一定期間（自動コミット期間）が経過したあと、初めてそのファイルにアクセスがあった契機で WORM 化されます。

自動コミットで WORM 化されたファイルは、デフォルトリテンション期間として指定した値がリテンション期間として設定されます。なお、自動コミット期間を過ぎていないファイルをクライアントから手動で WORM 化するときには、クライアントで指定した値がリテンション期間として設定されます。

(2) クライアントから手動で WORM 化する

ファイルの最終アクセス日時 (atime) をリテンション終了日時に変更してから、そのファイルを読み取り専用を設定すると WORM 化されます。

ファイルを読み取り専用にする日時からリテンション終了日時までの期間が、WORM 対応ファイルシステムを構築する際に指定した最小または最大リテンション期間の範囲内になるように atime を変更してください。

クライアントから atime を変更するためには、ユーザーが独自にカスタムアプリケーションを作成する必要があります。WORM 運用のカスタムアプリケーションを作成するための API については、「ファイルアクセス (CIFS/NFS) ユーザーズガイド」を参照してください。

ファイルを WORM 化したあとも atime を変更すれば、リテンション期間を延長できます。一度リテンション期間を過ぎたファイルは、読み取り専用を解除し、atime をリテンション終了日時に変更してから読み取り専用にすることで、リテンション期間を再設定できます。なお、リテンション期間が過ぎたファイルは削除できますが、変更できません。

Linux を使用している NFSv4 クライアントからファイルを WORM 化したり、リテンション期間を変更したりする場合は、Linux カーネル 2.6.35 以降を使用するか、次の修正パッチを適用してください。

パッチ名

```
NFSv4: Fix an embarrassing typo in encode_attr()
```

コミット ID

```
d3f6baaa34c54040b3ef30950e59b54ac0624b21
```

なお、ファイルを読み取り専用にした日時からリテンション終了日時までの期間が、最小または最大リテンション期間の範囲外の場合は、次のとおり設定されます。

- 読み取り専用にした日時から指定したリテンション終了日時までの期間が最大リテンション期間より大きい場合は、最大リテンション期間がリテンション期間として設定されます。
- 読み取り専用にした日時から指定したリテンション終了日時までの期間が最小リテンション期間より小さい場合は、最小リテンション期間がリテンション期間として設定されます。
- 指定したリテンション終了日時が読み取り専用にした日時から 24 時間を超えた過去の場合は、次のとおり最大リテンション期間が無期限かどうかで動作が異なります。
 - 最大リテンション期間が無期限のときはリテンション期間が無期限になります。
 - 最大リテンション期間が無期限でないときは WORM 化されません。
- 指定したリテンション終了日時が読み取り専用にした日時から 24 時間以内の過去の場合は、WORM 化されません。

(3) WORM 対応ファイルシステムを運用するときの注意事項

WORM 対応ファイルシステムを運用するときの注意事項は次のとおりです。

- WORM 機能の有効・無効の設定はファイルシステムの構築後に変更できません。
- WORM 対応ファイルシステム内のディレクトリの名称を変更する場合は、ファイルシステムの WORM の設定で、空ディレクトリの名称変更を許可してください。なお、バージョン 4.0.0-00 以降に構築した WORM 対応ファイルシステムのデフォルトの設定では、ディレクトリの名称を変更できません。
- WORM 対応ファイルシステムは構築したあとに ACL タイプを変更できません。
- リテンション期間を過ぎていない WORM ファイルにアクセスしても atime は更新されません。
- WORM 対応ファイルシステムにファイルの作成日時が記録されるように設定しても、WORM ファイルの作成日時は記録されません。
- リテンション期間を過ぎていない WORM ファイルを含むファイルシステムは削除できません。
- サイズが 0 バイトの空ファイルは WORM 化されません。
- HCP にマイグレートしたデータを HVFP/HDI にリストアして WORM 対応ファイルシステムを回復した場合、リテンション期間を過ぎていないファイルは、削除または変更のためのアクセスを受けるまで WORM 化されません。

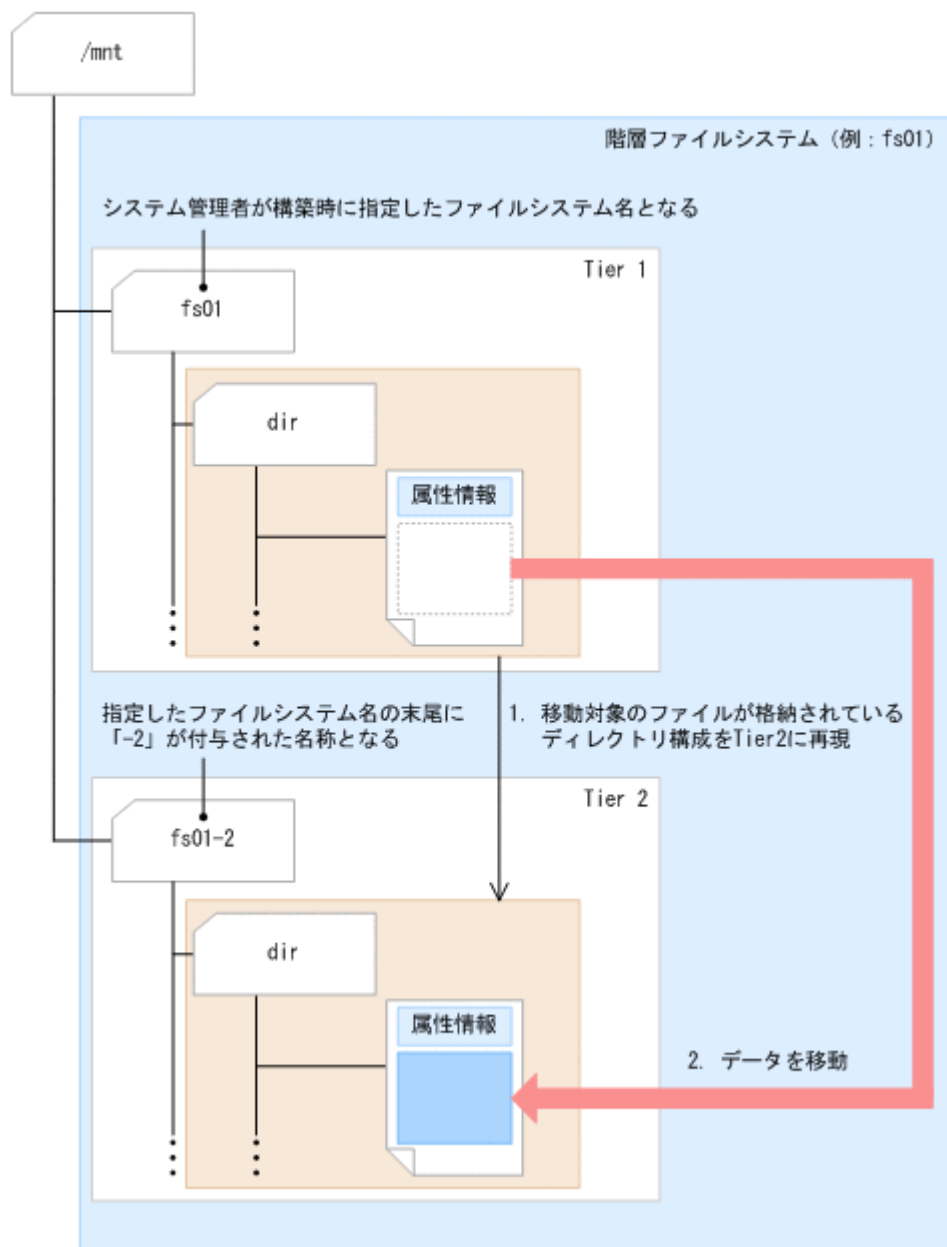
4.5.10 階層ファイルシステムの運用

HVFP/HDI のファイルシステムでは、異なるドライブ種別の LU を階層として分類できます。階層構成のファイルシステム（階層ファイルシステム）では、ファイルの種類や利用頻度に適した性能のディスクドライブで構成された階層に、データを移動させることができます。

ファイルシステムを階層構成で構築すると、ファイルシステムに使用する LU のドライブ種別を基に、第 1 階層のファイルシステム（Tier 1）と第 2 階層のファイルシステム（Tier 2）が作成されます。第 1 階層には、比較的高性能なディスクドライブ（SAS ドライブ）を使用します。ユーザーデータはまず第 1 階層に格納されます。そのあと、システム管理者が指定したポリシーに従って、ファイルシステム内の対象ファイルのデータが第 1 階層から第 2 階層へ自動で移動されます。

階層ファイルシステムでは、これらの階層のファイルシステムをまとめて 1 つのファイルシステムとして使用します。クライアントがファイルシステムにアクセスする際に、階層を意識する必要はありません。ファイルのデータが第 1 階層から第 2 階層へ移動されても、システム管理者やクライアントが設定を変更することなく、対象ファイルを参照または編集できます。

図 4-18 階層ファイルシステムの構造と動作



階層ファイルシステム内の各階層に配置されたファイルへのアクセス性能は、各階層で使用する LU と同じドライブ種別の LU を使用する通常のファイルシステムの場合とほぼ同じです。

(1) 階層ファイルシステムで使用する LU

階層ファイルシステムでは、ドライブ種別が異なる 2 個以上の LU を使用します。

GUI で新規にファイルシステムを構築する場合、階層ファイルシステムで使用する全 LU を選択すれば、ドライブ種別に応じて、各階層に LU が自動的に割り当てられます。階層ファイルシステムで使用する LU と割り当てられる階層の関係を次の表に示します。

表 4-4 階層ファイルシステムでの LU と階層の関係

LU	割り当てられる階層
SAS ドライブで構成されている LU 異なる種別のドライブで構成されている仮想 LU	第 1 階層 (Tier 1)
SAS 7.2K ドライブで構成されている LU	第 2 階層 (Tier 2)

LU	割り当てられる階層
SATA ドライブで構成されている LU 外部ストレージシステムの LU	

CLI でファイルシステムを構築する場合は、表 4-4 階層ファイルシステムでの LU と階層の関係を参考にして、使用する LU を指定してください。

また、既存のファイルシステムを拡張時に階層ファイルシステムに変更する場合、すでに使用されている LU は第 1 階層の LU として使用されます。表 4-4 階層ファイルシステムでの LU と階層の関係を参考にして、第 2 階層で使用する LU を指定してください。

(2) 階層ファイルシステムを運用するときの注意事項

階層ファイルシステムを運用するときの注意事項は次のとおりです。

- 階層ファイルシステムに対して、次の機能は使用できません。
 - ストライピング機能
 - HCP へのデータのマイグレーション
 - ほかのファイルサーバからのインポート
 - Hitachi File Remote Replicator
- ファイル共有、CIFS アクセスログ、および Quota の管理は、第 1 階層のファイルシステム (Tier 1) だけを対象とします。
- 複数ファイルのデータを集約するよう設定する場合は、第 2 階層のファイルシステム (Tier 2) だけがデータ集約の対象になります。
- 階層ファイルシステムを作成する際には、先頭 14 文字が一意になるようにファイルシステム名を指定してください。
- 第 2 階層のファイルシステム (Tier 2) には、ファイルシステム名として指定した名称の先頭 14 文字に「-2」を与えた名称が自動的に割り当てられます。例えば、ファイルシステム名として「filesystem12345」を指定すると、第 2 階層のファイルシステム名は「filesystem1234-2」となります。
- ファイル移動のタスクを実行中にファイルが更新されると、そのファイルは移動されません。次にタスクが実行されるときに移動されます。
- パスに改行コードが含まれているファイルのデータは第 2 階層のファイルシステム (Tier 2) へ移動されません。
- 1 つのファイルに対して、マイグレーション、ファイル移動、容量削減のタスクのうち、2 つ以上の異なるタスクが同時に実行されないようにしてください。なお、同時に実行された場合はエラーが表示されますが、次のタスク実行時に正常に処理されます。

4.5.11 複数ファイルのデータ集約による容量節約

HVFP/HDI では、内容が重複している複数のファイルのデータを集約することで、ディスクの使用量を節約できます (重複排除機能)。動画や画像を含むプレゼンテーション資料など、サイズの大きなファイルを複数のクライアントがコピーして使用している場合、効果的に使用量を節約できます。

複数のファイルのデータを集約するときは、次のことに注意してください。

- 複数ファイルのデータを集約するようファイルシステムに設定すると、設定を解除することはできません。
- 複数ファイルのデータを集約するよう設定したファイルシステムでは、1 ファイルごとに最大 10KB の管理領域が必要です。ファイルシステムの容量を検討する際に考慮してください。

- 更新頻度の低いファイルがデータ集約の対象となるようポリシー（容量削減ポリシー）を設定してください。更新頻度の高いファイルがデータ集約されると、ディスク使用量を節約できないことがあります。容量削減ポリシーは、[タスク管理] ダイアログまたは容量削減ウィザードで設定できます。
- 次に示す条件に1つでも該当するファイルは、データ集約の対象になりません。
 - サイズが 16KB 以下である
 - パスに改行コードが含まれている
- サイズが 16KB 以下のファイルや、[タスク管理] ダイアログで設定した容量削減ポリシーによってデータ集約の対象から除外するファイルの数が多い場合は、容量削減タスクの実行に時間が掛かることがあります。その場合は、`arcfilterpolicyset` コマンドを使用して、データ集約の対象から除外するファイルの条件（フィルタリングポリシー）を追加で設定してください。フィルタリングポリシーを設定すると、タスク管理情報から最終編集日時（mtime）が古いファイルが削除され、タスクの実行時間が改善することがあります。
- 階層ファイルシステムの場合は、第 2 階層のファイルシステム（Tier 2）だけがデータ集約の対象になります。
- 3.2.0-00 より前のバージョンの HVFP/HDI で作成されたファイルシステムには、複数ファイルのデータを集約するよう設定できません。
- 1つのファイルに対して、マイグレーション、ファイル移動、容量削減のタスクのうち、2つ以上の異なるタスクが同時に実行されないようにしてください。なお、同時に実行された場合はエラーが表示されますが、次のタスク実行時に正常に処理されます。

4.5.12 CIFS 走査チェックのバイパス機能

CIFS 走査チェックのバイパス機能とは、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（ディレクトリ、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 CIFS アクセスできるようにする機能です。

オブジェクトの例を次に示します。

```
/mnt/fs01/dir1/dir12/access.txt
```

この場合、`dir1` ディレクトリ、`dir12` ディレクトリにアクセス権限がなくても、`access.txt` ファイルにアクセス権限があれば、`access.txt` ファイルの絶対パスを指定することでアクセスできます。

CIFS 走査チェックのバイパス機能はファイルシステム単位で有効化したり、無効化したりできます。

CIFS 走査チェックのバイパス機能を無効にすると、HVFP/HDI では、オブジェクトにアクセスするには、そこに至るすべての上位ディレクトリに「フォルダのスキャン/ファイルの実行」権限（ファイルパーミッションでは、Advanced ACL タイプの場合は「1 (-x)」、Classic ACL タイプの場合は「4 (r--)」）が必要です。また、ディレクトリの階層で管理者を分けて運用している場合は、各階層の管理者に ACL の設定変更を依頼する必要があります。

このほかに、次に示す注意事項があります。

- バージョン 4.2.0-00 以降、ファイルシステムの作成時には、CIFS 走査チェックのバイパス機能がデフォルトで有効に設定されます。ただし、ホームディレクトリローミング対応ファイルシステムでは CIFS 走査チェックのバイパス機能は無効です。
- 差分スナップショットは、それを作成したファイルシステムで CIFS 走査チェックのバイパス機能が有効かどうかによって依存します。作成した差分スナップショット単位で CIFS 走査チェックのバイパス機能を有効化したり、無効化したりすることはできません。

- バージョン 4.2.0-00 より前の HVFP/HDI から更新インストールを実施すると、各ファイルシステムの CIFS 走査チェックのバイパス機能は無効に設定されます。
- バージョン 4.2.0-00 より前のシステム LU または Virtual Server OS LU に格納されていたシステム設定情報の保存データでシステムを回復した場合、CIFS 走査チェックのバイパス機能は無効となります。
- バージョン 4.2.0-00 より前のシステムで HCP にマイグレートされていたデータを、`arcrestore` コマンドを使用して CIFS 走査チェックのバイパス機能が有効なファイルシステムにリストアした場合は、CIFS 走査チェックのバイパス機能は有効となります。

必要に応じてファイルシステムの設定を変更してください。

4.6 Quota の運用を開始する前に

HVFP/HDI では、ファイルシステムごと、またはディレクトリごとに Quota を管理できます。HVFP/HDI では、ディレクトリごとに設定する Quota をサブツリー Quota と呼びます。

ファイルシステムごとの Quota の管理

ファイルシステムごとに Quota を管理すると、ユーザーやグループに対してファイルシステムごとの Quota を設定したり、ファイルシステムに対してデフォルト Quota を設定したりできます。

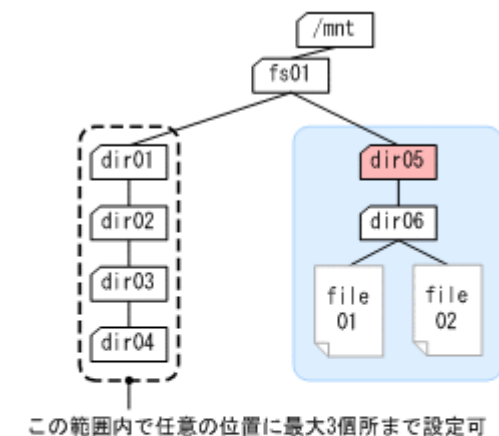
サブツリー Quota の管理

サブツリー Quota は、ファイルシステムのディレクトリごとに管理できます。サブツリー Quota を管理すると、ユーザーやグループに対してディレクトリごとの Quota を設定したり、ディレクトリに対して Quota やデフォルト Quota を設定したりできます。

ファイルシステムのどのディレクトリに対してもサブツリー Quota を設定できます。サブツリー Quota は、ディレクトリツリーの最上位から最下位まで親子関係でつながっている範囲内で、任意の位置に最大 3 個所まで設定できます。なお、GUI を使用する場合は、ファイル共有の容量を管理することで、マウントポイント直下のディレクトリに対して Quota を設定できます。

1 つのファイルシステムに複数のファイル共有を作成して運用する場合、マウントポイント直下に作成した共有ディレクトリにサブツリー Quota を設定することで、それぞれのファイル共有の容量を柔軟に管理できます。1 つのファイルシステムで Quota を設定できるディレクトリ数は最大 1,023 個です。なお、Quota を設定できるユーザーやグループ数に上限はありません。

図 4-19 サブツリー Quota の管理



(凡例)

- : ディレクトリ
- : サブツリーQuotaを設定したディレクトリ
- : サブツリーQuotaの監視対象範囲

ファイルシステムごとに設定した Quota とサブツリー Quota を併用すると、ユーザーがファイルやディレクトリを作成・更新できなくなったとき、それぞれの Quota 情報を確認して要因を特定する必要があります。このため、HVFP/HDI では、どちらか一方だけを設定して Quota を管理することを推奨します。システム管理者は、効率的に Quota を管理できるよう、ファイルシステムの運用に応じて設定してください。

ユーザーのブロック使用量には、ファイルが実際に占有している容量が加算されます。HCP と連携したマイグレーションを運用している場合はリコールによって、内容が重複している複数のファイルのデータを集約する運用をしている場合はファイルの更新によって、ユーザーのブロック使用量が予期せず上限に達するおそれがあります。このため、HCP にデータをマイグレートしているファイルシステムや、重複ファイルの容量削減を有効にしたファイルシステムを運用する場合は、Quota を設定しないでください。

Quota を設定しない場合は、障害情報の SNMP 通知または E-mail 通知を使用してファイルシステムの使用量を監視することを推奨します。また、fsfullmsg コマンドで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することもできます。

SNMP トラップ通知に使用する MIB オブジェクトについては、「ユーザーズガイド」を参照してください。

ディレクトリツリーの最上位から最下位まで親子関係でつながっている範囲内では、サブツリー Quota を設定したディレクトリの上位のディレクトリ名を変更すると、Quota 情報を正しく管理できなくなります。このため、サブツリー Quota を設定したディレクトリの上位のディレクトリ名を変更する場合は、いったんサブツリー Quota の設定を解除し、ディレクトリの名称を変更してからサブツリー Quota を設定し直してください。なお、この手順に従わないで、ディレクトリ名を変更して Quota 情報を正しく管理できなくなった場合は、変更前のディレクトリ名に戻すことで正しく管理できるようになります。

4.6.1 Quota 管理で設定できる情報

HVFP/HDI の Quota 管理で設定できる情報を次に示します。

- ユーザー、グループまたはディレクトリに対する Quota の設定

- デフォルト Quota の設定
- 猶予期間の設定
- Quota 監視方法の設定

ファイルシステムごとに設定した Quota とサブツリー Quota のそれぞれの管理方法で設定できる情報を次の表に示します。

表 4-5 Quota 管理で設定する情報

設定情報	ファイルシステムごとの Quota の管理		サブツリー Quota の管理	
	GUI	コマンド	GUI	コマンド
ユーザーに対する Quota	○	○	×	○
グループに対する Quota	○	○	×	○
ディレクトリに対する Quota	×	×	○※	○
デフォルト Quota	○	○	×	○
猶予期間	○	○	×	○
Quota 監視方法	○	○	×	○
ディレクトリに設定された Quota の解除	×	×	×	○

(凡例) ○：設定できる ×：設定できない

注※

マウントポイント直下のファイル共有の容量として管理します。

ここでは、Quota の各設定および Quota を設定するときの注意事項について説明します。

(1) ユーザー、グループまたはディレクトリに対する Quota の設定

ユーザーまたはグループに対して Quota を設定できます。また、サブツリー Quota を管理している場合は、ディレクトリに対しても Quota を設定できます。ユーザー、グループまたはディレクトリに対する Quota として、次の項目を設定します。

ハードリミット設定

ユーザー、グループまたはディレクトリごとに、使用するブロック容量と inode 数の上限値（ハードリミット）を設定できます。ハードリミットで設定した値を超えて、新たにブロックを割り当てたり、ファイルやディレクトリを作成したりできません。

ソフトリミット設定

ユーザー、グループまたはディレクトリごとに、使用するブロック容量と inode 数の警告値（ソフトリミット）を設定できます。ソフトリミットで設定した値を超えた状態で、一定の期間（猶予期間）を経過すると、新たにブロックを割り当てたり、ファイルやディレクトリを作成したりできません。

ファイルを作成・更新できない場合、ソフトリミットを下回るまでファイルを削除すると、新しくファイルを作成・更新できます。

なお、ソフトリミットにはハードリミット以下の値を設定してください。

GUI でファイル共有の容量を指定する場合は、ディレクトリに対してハードリミット（使用するブロック容量の上限）だけが設定されます。

(2) デフォルト Quota の設定

デフォルト Quota を設定しておく、Quota が設定されていないユーザーに対しても、ブロック容量と inode 数の使用量を制限できます。ユーザー、グループまたはディレクトリに対して設定した Quota と同様にハードリミットおよびソフトリミットを設定できます。

デフォルト Quota として設定した値は、Quota が設定されていないユーザーが、デフォルト Quota が設定されているファイルシステムやディレクトリを初めて使用したとき（ファイルを作成したとき）に適用されます。

デフォルト Quota は、ユーザーマッピングで登録されたユーザーを含むすべてのユーザーに対して適用されます。

(3) 猶予期間の設定

ユーザーまたはグループがソフトリミットで設定した値を超えた状態で、ファイルの作成またはブロックの割り当てができる一定の期間（猶予期間）を設定できます。

(4) Quota 監視方法の設定

設定された時刻に Quota 情報を監視します。ソフトリミットや猶予期間を超過したユーザーまたはグループの情報は、SNMP トラップ、E-mail 通知、または management.log ファイルで確認できます。

Quota 情報を監視する時刻（Quota 監視時刻）と、ソフトリミットおよび猶予期間を超過したユーザー・グループを検知した場合の SNMP トラップの通知方法をファイルシステムごとに設定できます。なお、Quota を設定していれば、Quota 監視時刻とは関係なく、設定したハードリミットや猶予期間に達した時点でディスクの使用量が制限されます。

SNMP トラップでの通知方法には次の 2 種類があります。

サマリー通知モード（推奨）

ソフトリミットや猶予期間を超過したユーザー、グループまたはディレクトリを検知した場合に、超過したユーザー、グループまたはディレクトリの数を通知します。management.log ファイルおよび E-mail 通知には、サマリー通知と同じ情報が出力されます。

個別通知モード

ソフトリミットや猶予期間を超過したユーザー、グループまたはディレクトリを検知した場合に、ユーザー、グループまたはディレクトリごとに Quota 情報を通知します。ソフトリミットや猶予期間を超過したユーザー、グループまたはディレクトリの数が、それぞれ 100 を超えている場合は、個別通知が抑止され、超過しているユーザー、グループまたはディレクトリの数だけが SNMP マネージャーに通知されます。なお、サブツリー Quota を管理する場合は、ユーザーおよびグループに対して設定された Quota に対して個別通知モードを利用できません。

ソフトリミットや猶予期間の超過を検知した場合に通知される情報を次の表に示します。

表 4-6 ソフトリミットや猶予期間の超過を検知した場合に通知される情報

項目	サマリー通知	個別通知		
		ソフトリミットを超過した場合	猶予期間を超過した場合	個別通知が抑止された場合
通知日時	○	○	○	○
ホスト名※1	○	○	○	○
ノード番号※2	○	○	○	○
装置識別番号	○	○	○	○
ファイルシステム名	○※3	○※4	○※4	○

項目	サマリー通知	個別通知		
		ソフトリミットを超過した場合	猶予期間を超過した場合	個別通知が抑止された場合
管理種別※5	×	○	○	○
ユーザー名またはグループ名	×	○	○	×
ユーザー ID またはグループ ID	×	○	○	×
超過種別 (block/inode)	×	○	○	×
現在の使用量 (ブロック使用量の単位: KB)	×	○	○	×
ソフトリミット (ブロック使用量の単位: KB)	×	○	○	×
ハードリミット (ブロック使用量の単位: KB)	×	○	○	×
残りの猶予期間 (単位: 秒)	×	○	×	×
猶予期間の設定値 (単位: 日)	×	×	○	×
ブロック使用量のソフトリミットを超過しているユーザー、グループまたはディレクトリの数	○	×	×	○
ブロック使用量の猶予期間を超過しているユーザー、グループまたはディレクトリの数	○	×	×	○
inode 使用量のソフトリミットを超過しているユーザー、グループまたはディレクトリの数	○	×	×	○
inode 使用量の猶予期間を超過しているユーザー、グループまたはディレクトリの数	○	×	×	○

(凡例) ○: 通知される ×: 通知されない

注※1

Virtual Server でファイルシステムを運用している場合は、Virtual Server 名が通知されます。

注※2

Virtual Server でファイルシステムを運用している場合は、「-」となります。

注※3

ユーザーまたはグループに対してサブツリー Quota を設定している場合は、次の形式で表示されます。

<ファイルシステム名>/<ディレクトリ名>

注※4

ユーザー、グループまたはディレクトリに対してサブツリー Quota を設定している場合は、次の形式で表示されます。

<ファイルシステム名>/<ディレクトリ名>

注※5

ファイルシステムごとに Quota を管理している場合は、user または group が通知されます。サブツリー Quota を管理している場合は、subtree, subtree_user または subtree_group が通知されます。

(5) Quota を設定するときの注意事項

Quota を設定するときの注意事項を次に示します。

- ブロック使用量は、ファイルシステムによって 4KB 単位で管理されています。また、割り当てるブロックは、データの書き込みだけでなく、システム管理のためにも使用されます。このため、ファイルサイズの合計がブロック使用量のリミット以下でも、ブロック使用量がリミットを超える場合があります。1MB 以上の余裕を持って、リミットの値を設定してください。
- 匿名マッピングされていない root ユーザー（NFS クライアント）および CIFS 管理者には、ユーザー、グループまたはディレクトリに対する Quota やデフォルト Quota による制限はありません。また、匿名マッピングされていない root グループに属するユーザー（NFS クライアント）は、グループに対する Quota による制限はありません。このほか、次の操作についても、ユーザー、グループまたはディレクトリに対する Quota やデフォルト Quota による制限はありません。
 - CIFS アクセスログの退避（設定したログ採取契機に従って自動的に採取される場合も含む）
 - システム管理者としての GUI およびコマンド操作
 - NDMP 機能を使用したリストア
- 特定のユーザーと、そのユーザーの属するグループの両方に Quota を設定した場合は、より設定値の小さい Quota が有効になります。Quota を設定したユーザーの例を次の表に示します。

表 4-7 Quota を設定したユーザーの例

ユーザー名	ユーザーに設定された Quota	プライマリーグループ	所属グループ
ユーザー A	20GB	グループ 1	グループ 1
ユーザー B	20GB	グループ 1	グループ 1
ユーザー C	20GB	グループ 1	グループ 1
ユーザー D	30GB	グループ 2	グループ 1, グループ 2

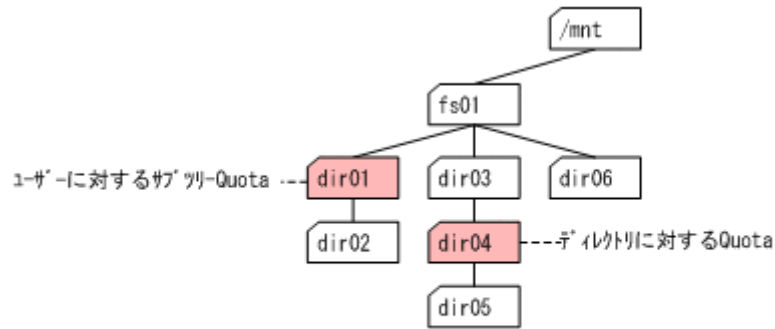
この例を使用してグループ 1 に設定された Quota が 25GB とした場合に、各ユーザーが使用できるブロック容量について説明します。

ユーザー A, B, C には 20GB の Quota が設定されているため、ユーザー A, B, C が使用できるブロック容量は 20GB です。ユーザー A がブロック容量を 20GB 使用しているとき、ユーザー B, C の使用できるブロック容量はあわせて 5GB となります。

ユーザー D のプライマリーグループ（グループ 2）に Quota が設定されていない場合、ユーザー D は 30GB までブロック容量を使用できます。ただし、グループ 1 のファイルをグループの実行権限で更新する場合は、使用できるブロック容量は 25GB に制限されます。

- 次の文字が含まれるディレクトリにはサブツリー Quota を設定できません。
" * : < > ? ¥ |
- ディレクトリツリーの最上位から最下位まで親子関係でつながっている範囲内では、ユーザーまたはグループに対するサブツリー Quota、もしくはデフォルト Quota を設定したディレクトリの下位のディレクトリにはサブツリー Quota を設定できません。

例えば、次のように、dir01にユーザーに対するサブツリー Quota を設定していると、dir02にはサブツリー Quota を設定できません。dir04にディレクトリに対する Quota を設定していると、dir03にはディレクトリに対する Quota を設定できますが、ユーザーまたはグループに対するサブツリー Quota、もしくはデフォルト Quota は設定できません。



ディレクトリ名	サブツリー-Quotaの設定可否
dir02	×
dir03	△
dir05	○
dir06	○

(凡例)

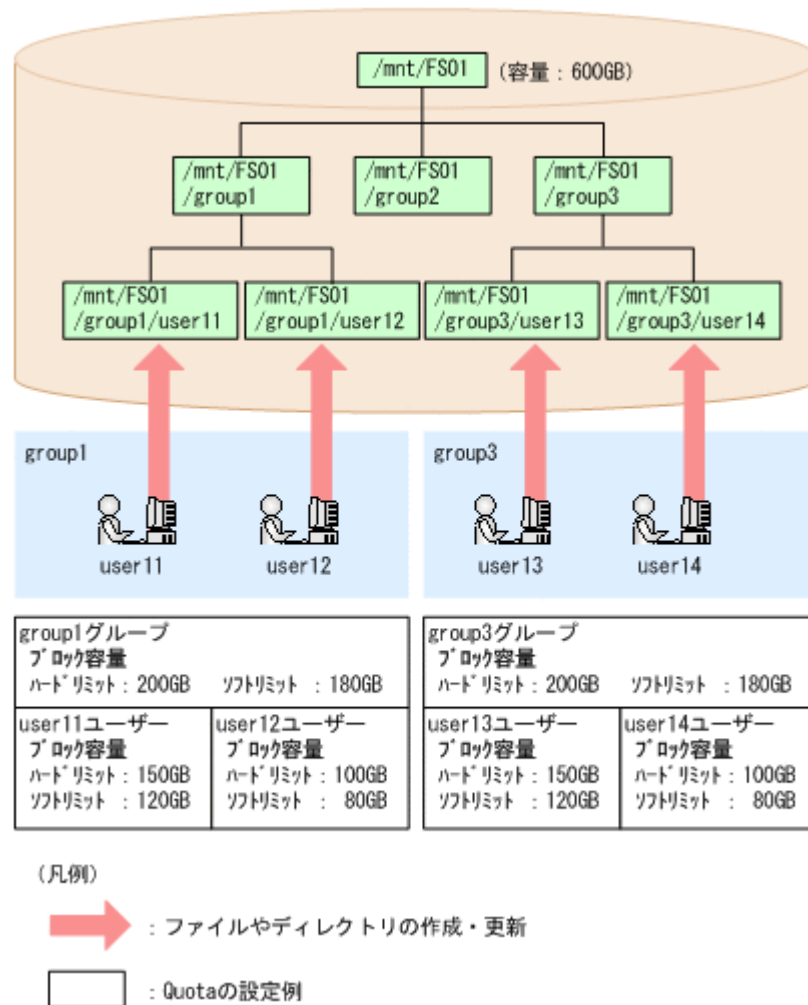
- : ディレクトリ
- : サブツリー-Quotaを設定したディレクトリ
- : 設定可
- △ : 一部設定可 (ディレクトリに対するQuotaだけ)
- × : 設定不可

4.6.2 ファイルシステムごとに Quota を管理する場合

多数のユーザーが1つのファイルシステムを共有する場合は、ユーザーやグループに対して Quota を設定すると、ファイルシステムを利用する特定のユーザーやグループが容量を占有しないように制限できます。

このような運用で設定する Quota の例を次に示します。

図 4-20 ファイルシステムごとの Quota の設定例



例えば、FS01 ファイルシステムを使用している user11 ユーザーや group1 グループに対してユーザーやグループの Quota を設定することで、user11 ユーザーや group1 グループが FS01 ファイルシステムで使用できるブロック容量を制限できます。

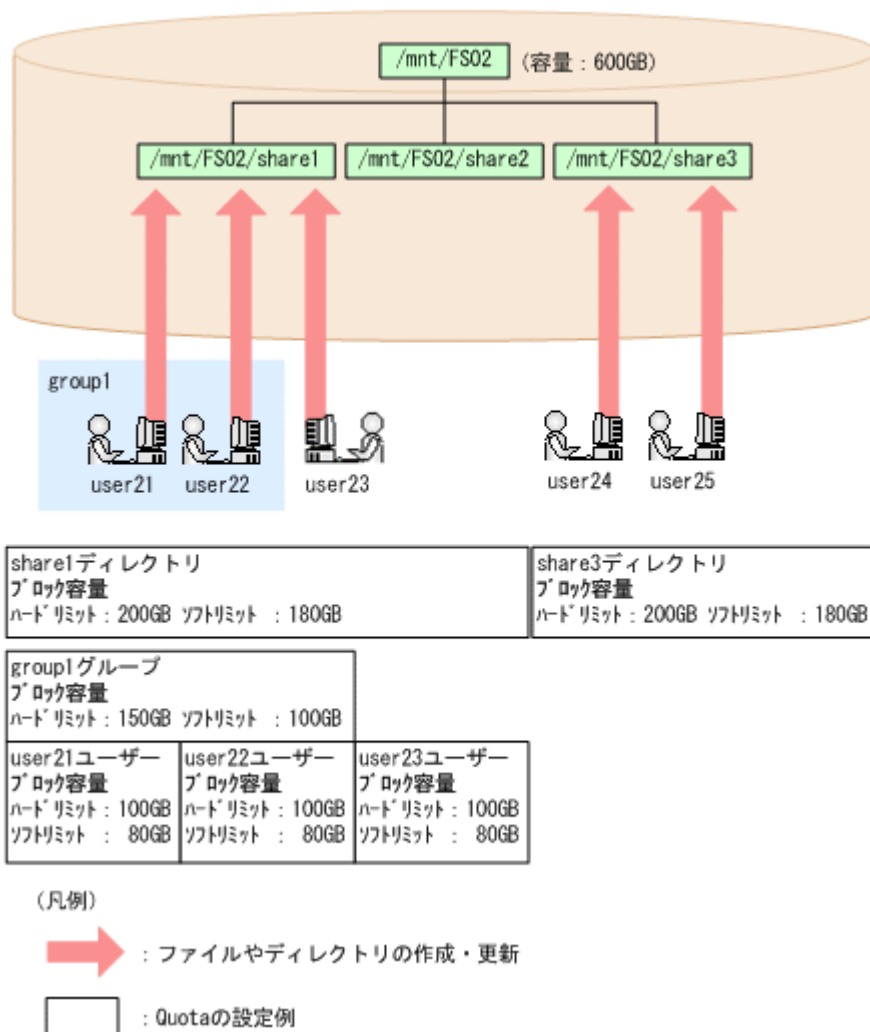
4.6.3 サブツリー Quota を管理する場合

1つのファイルシステムをマウントポイント直下のディレクトリ単位に分けて、ユーザーやグループに公開する場合、公開する共有ディレクトリにサブツリー Quota を設定すると、特定の共有ディレクトリによってファイルシステム全体の容量を圧迫することのないように制限できます。

サブツリー Quota を設定する場合、ディレクトリ内で使用できる容量に上限を設けられるため、ディレクトリをファイルシステムのように運用できます。サブツリー Quota では、ディレクトリ内で使用できる容量を任意の数値で設定できるため、容量を柔軟に拡張したり縮小したりできます。

このような運用で設定するサブツリー Quota の例を次に示します。

図 4-21 マウントポイント直下のディレクトリへのサブツリー Quota の設定例



例えば、FS02 ファイルシステムの share1 ディレクトリに対して Quota を設定することで、share1 ディレクトリ内で使用できるブロック容量を制限できます。また、share1 ディレクトリを使用している user21 ユーザーや group1 グループに対して Quota を設定することで、user21 ユーザーや group1 グループが share1 ディレクトリで使用できるブロック容量を制限できます。

このほか、FS02 ファイルシステムの share3 ディレクトリに対して、使用できるブロック容量の上限を 200GB に設定していますが、ファイルシステムの運用に応じて拡張することもできます。

4.6.4 Quota を管理する場合の注意事項

ここでは、Quota を管理する場合の注意事項について説明します。

- Quota を管理するには、対象のファイルシステムをマウントするときに、Quota 機能を有効にしておく必要があります。
- マウント中のファイルシステムの Quota 管理を開始する場合は、ファイルシステムを一度アンマウントし、Quota 機能を有効にして再度マウントしてください。このとき、ファイルシステムの容量が不足していると、マウントしても Quota 管理機能を利用できません。システム管理者は、ファイルシステムを拡張するか、不要なファイルを削除して空き容量を確保してから、再度マウントする必要があります。

また、再度マウントしたときにシステム内部でチェックが行われるため、ファイルシステムの使用量が多いほど、マウント処理が完了するまでに時間が掛かります。

- Quota 情報は、SNMP トラップでも確認できます。なお、ファイルシステムに登録されたユーザーやグループの数が多くなると、SNMP マネージャーから Quota 情報を参照する際に時間が掛かるため、`/etc/snmp/snmpd.conf` ファイルを直接編集することで、ファイルシステムに登録されているユーザーやグループの数に応じて SNMP マネージャーからの参照を抑止するよう設定できます。

また、ファイルシステムごとに Quota を管理する場合の注意事項について説明します。

- GUI 操作モードで運用している場合、次のどちらかの環境では [Edit Quota] ダイアログの [List of Quota Information] ページに遷移できません。コマンド操作モードに切り替えるか、コマンドを使用して Quota を管理してください。
 - File Services Manager, NIS サーバおよびユーザー認証用の LDAP で登録されたユーザーの総数が 10,000 を超えている環境
 - File Services Manager, NIS サーバおよびユーザー認証用の LDAP で登録されたグループの総数が 10,000 を超えている環境
- コマンド操作モードで運用している場合は、GUI からは次の操作を実行できません。
 - ユーザーまたはグループの Quota 情報の参照
 - ユーザーまたはグループごとの Quota の設定
- ユーザーマッピングで登録されたユーザーやグループの Quota 管理には、コマンドを使用します。
- ユーザーマッピングで登録されたユーザーに Quota を設定する運用の場合は、Quota を監視する時刻を設定することを推奨します。

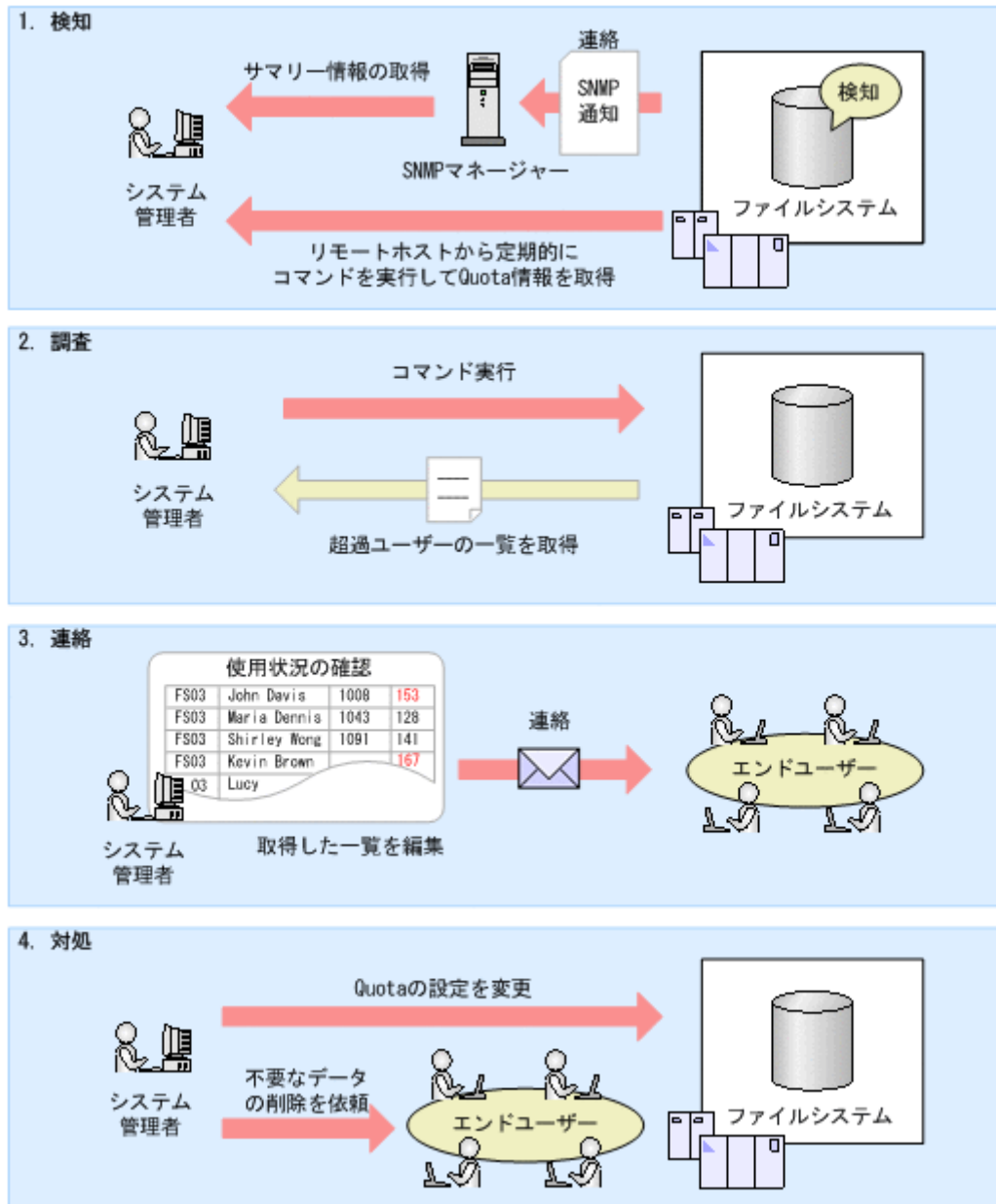
このほか、サブツリー Quota を管理する場合の注意事項について説明します。

- 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、各クライアントからシステム管理者に問い合わせる運用にする必要があります。

4.6.5 Quota 管理の運用例

Quota 管理の代表的な運用例を次の図に示します。

図 4-22 Quota 管理の運用例



1. 検知

システム管理者は、SNMPトラップまたはE-mail通知や、リモートホストから定期的にコマンドを実行して取得したQuota情報を契機に、ファイルシステムを利用しているユーザーがQuotaを超過していることを検知します。
2. 調査

Quota超過を検知した場合、ファイルシステムの使用状況を確認するため、Quotaを超過したユーザーのQuota情報をコマンドで取得します。
3. 連絡

取得したQuota情報を確認し、Quotaを超過しているユーザーに連絡します。
4. 対処

エンドユーザーのファイルシステムの利用状況に応じて、次のように対処できます。

 - Quotaの設定を変更する
 - エンドユーザーに不要なデータを削除させる

SNMP トラップのサマリー通知または E-mail 通知と、コマンドを使用した Quota 管理を併用して運用することで、ファイルシステムを使用するユーザーおよびグループの数が多い環境でも、システム管理者は比較的容易に個々の使用量を管理できます。

4.7 ファイル共有の運用を開始する前に

UNIX や Windows などのプラットフォームの異なるユーザーが、NFS や CIFS のサービスを利用して、ストレージシステムに格納されているファイルシステムやディレクトリにアクセスするためには、システム管理者がファイル共有を作成しておく必要があります。

ここでは、システム管理者がファイル共有を管理するに当たり、知っておく必要があることについて説明します。

4.7.1 NFS 共有を運用する前に確認しておくこと

NFS クライアントからファイルシステムをマウントしたあと、root ユーザーの権限でファイルを書き込むためには、次の設定を見直す必要があります。

匿名マッピングされるユーザー

GUI でファイルシステムを構築するとき、デフォルトでは [匿名マッピング] に [root ユーザー用] が指定されています。

なお、NFS 共有作成時のデフォルトのアクセス権は次のとおりです。

- Classic ACL タイプのファイルシステム : 755
- Advanced ACL タイプのファイルシステム : Everyone full control

このほか、Kerberos 認証を利用する際に、ファイルシステムに対して NFS クライアントから時間の掛かるバッチ処理などを実施する場合、または Linux を利用している NFS クライアントからファイルシステムにアクセスする場合は、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。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。

4.7.2 CIFS 共有を運用する前に確認しておくこと

HVFP/HDI では、クラスタ構成の場合は 1 クラスタ当たり、シングルノード構成の場合は 1 ノード当たりの CIFS クライアントの最大接続数が設定されています。この値は、CIFS サービスの構成定義で、CIFS 共有の設定を自動的にリロードして CIFS クライアント環境に反映させるように設定しているかどうかで異なります。また、最大接続数は、製品モデルやノードのメモリーサイズによっても異なります。CIFS クライアントの最大接続数および CIFS 共有数については、「ファイルアクセス (CIFS/NFS) ユーザーズガイド」を参照してください。

なお、CIFS クライアントの最大接続数は、論理的に接続できる数の最大値です。個々の CIFS クライアントからの問い合わせの流量によっては CPU 利用率が高くなって、最大接続数に達していても、CIFS クライアントへの CIFS サービスからの応答性が低下することがあります。具体的には、複数のクライアントから次に示す操作をした場合です。

- 大容量ファイルの読み取りや書き込みをした場合。
 - 多数のファイルの読み取りや書き込みをした場合。
 - 頻繁なフォルダの一覧表示やファイル、フォルダの属性取得・変更をした場合。
 - エクスプローラなどを利用して複数クライアントから同一フォルダの変更を監視した場合。
- この場合、クライアントからのフォルダ内容監視リクエストに対し応答を返さないように `cifsoptset` コマンドで設定することで、CIFS サービスからの応答性が低下するのを抑えられます。

cifsoptset コマンドで change_notify が no となるように CIFS サービスの構成定義を変更すると、CIFS クライアントで表示されるフォルダやファイルの情報は手動で更新する必要があります。なお、手動で更新しても最新の情報が表示されない場合は、しばらくしてから再度更新してください。

デフォルトでは、自動リロードするように設定されています。自動リロードしないように設定されていると、CIFS 共有の設定を変更した際に CIFS クライアント環境に設定内容を反映するため、CIFS サービスの再起動または CIFS クライアントマシンへの再ログインなどの操作を実行する必要があります。CIFS サービスを再起動する際には、次のことに注意してください。

- Virtual Server を使用していない場合、縮退運用中に CIFS 共有の設定を変更するときは、フェールバックしたあと、CIFS サービスを再起動する必要があります。
- コマンドを使用して CIFS 共有の設定を変更した場合は、CIFS サービスを再起動する必要があります。

このほか、自動リロードしないように設定されているときには、次のことを考慮する必要があります。

- 差分スナップショットにファイル共有を自動作成する機能を使用できません。差分スナップショットをファイルシステムの共有内に自動公開する機能または Volume Shadow Copy Service の使用を検討してください。
- シェルスクリプトを使用したボリュームレプリケーション連携機能の自動運用はできません。スクリプトで作成した CIFS 共有にクライアントからアクセスするためには、CIFS サービスの再起動または CIFS クライアントマシンへの再ログイン操作が必要です。

4.7.3 CIFS 共有を作成する前に確認しておくこと

CIFS 共有を作成する前に次のことを確認してください。

- HVFP/HDI が提供する CIFS 共有では、ファイル名やディレクトリ名の文字コードとして Unicode (UTF-8) が使用されます。
- ユーザーマッピングで登録されたユーザーおよびグループに対して、CIFS 共有へのアクセス権を個別に設定する場合にはコマンドを使用してください。GUI からは、ユーザー・グループごとに CIFS 共有に対するアクセス権を設定することはできません。
- CIFS 共有を作成する前に、ファイルの作成日時が記録されるようにファイルシステムに設定しておくことをお勧めします。システム管理者がファイルシステム内にファイルの作成日時が記録されるよう設定することで、CIFS クライアントはファイルの作成日時を確認できます。

GUI を使用してファイルシステムを構築する場合には、作成日時が記録されるように自動的に設定されます。コマンドを使用してファイルシステムを構築する場合は、作成日時が記録されるようにオプションを指定します。また、既存のファイルシステムの場合は、コマンドで設定を変更できます。

4.7.4 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。

詳細については、「ファイルアクセス (CIFS/NFS) ユーザーズガイド」を参照してください。

4.7.5 MMC と連携するとき

HVFP/HDI では、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」機能を MMC (Microsoft Management Console) から利用して、CIFS 共有を管理できます。詳細については、「ファイルアクセス (CIFS/NFS) ユーザーズガイド」を参照してください。

4.7.6 CIFS アクセスログを利用するとき

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。詳細については、「ファイルアクセス (CIFS/NFS) ユーザーズガイド」を参照してください。

4.7.7 Classic ACL タイプのファイルシステムで ACL を設定するとき

HVFP/HDI では、コマンドを利用して ACL を設定することで、オーナー、所有グループおよびその他に対してだけでなく、特定のユーザーまたはグループに対しても、ディレクトリやファイルへのアクセス権を設定できます。File Services Manager で ACL を設定すると、ディレクトリのモードよりも詳細にアクセスを制御できます。

Classic ACL タイプのファイルシステムで利用できる ACL には、次の 3 種類があります。

- アクセス ACL
指定したディレクトリに設定される ACE です。
- デフォルト ACL
指定したディレクトリの下に作成されたディレクトリおよびファイルに設定される ACE です。
- マスク
所有グループ、特定のユーザーおよび特定のグループに対して、有効なアクセス権を制限する ACE です。通常、マスクを設定する必要はありません。

なお、CIFS クライアントから ACL を操作する場合は、「ファイルアクセス (CIFS/NFS) ユーザーズガイド」を参照してください。

4.7.8 ALog ConVerter と連携するとき

ALog ConVerter と連携すると、NFS 共有以外へのユーザーアクセスを記録した監査ログを ALog ConVerter で管理できます。ストレージシステム上のファイルシステムまたは OS ディスクに出力された監査ログは、FTP 経由で ALog マネージャーサーバに転送されます。

事前に、ALog マネージャーサーバで HVFP/HDI との連携に必要な設定を完了してください。ALog マネージャーサーバの設定については、ALog ConVerter のドキュメントを参照してください。

監査ログは、ALog ConVerter と連携しているときに記録されます。監査ログの内容は、ALog ConVerter の機能を使用して確認できます。

なお、監査ログは、HVFP/HDI の CIFS アクセスログとは異なります。監査ログについては、ALog ConVerter のドキュメントを参照してください。CIFS アクセスログについては、「ファイルアクセス (CIFS/NFS) ユーザーズガイド」を参照してください。

監査ログの出力処理は、HVFP/HDI の性能に影響します。クラスタ構成およびストレージシステムを接続しているシングルノード構成の場合は、ストレージシステム上に作成したファイルシステムに監査ログを出力することを推奨します。ただし、Virtual Server の場合は、出力先をファイルシステムにするかどうかで性能に差異はないため、ファイルシステムに監査ログを出力する必要はありません。

ファイルシステムに監査ログを出力するときの注意事項を次に示します。

- 監査ログの出力先として、容量が 20GB 以上のファイルシステムをストレージシステム上に作成してください。ノードごとに作成する必要があります。
- 作成したファイルシステムは、監査ログの出力以外の用途で使用しないでください。また、ファイル共有を作成しないでください。
- 監査ログの出力先のファイルシステムはアンマウントしないでください。アンマウントすると、監査ログを出力できなくなります。
- ALog ConVerter との連携を無効にした場合は、監査ログを出力していたファイルシステムを必要に応じて削除してください。
- 監査ログの出力先を変更する場合は、ALog ConVerter との連携を無効にしたあと、再設定する必要があります。

(1) ALog ConVerter との連携を開始する手順（クラスタ構成の場合）

クラスタ構成の HVFP/HDI で、ALog ConVerter との連携を開始する手順を次に示します。なお、Virtual Server を運用している場合は、Virtual Server ごとに設定する必要があります。

1. ALog マネージャーサーバを名前解決する場合は、IP アドレスとホスト名を、DNS サーバ、または、Physical Node 上もしくは Virtual Server 上の /etc/hosts ファイルに登録します。
/etc/hosts ファイルは [Network & System Configuration] ダイアログの [Edit System File] ページで編集してください。
2. 監査ログをファイルシステムに出力する場合は、ファイルシステムを作成します。
監査ログを出力するファイルシステムの設定には条件があります。次のとおりコマンドを実行してください。
`sudo fscreate <ファイルシステム名> <20GB 以上のデバイスファイル名>`
3. 手順 2 でファイルシステムを作成した場合は、ファイルシステムをマウントします。
次のとおりコマンドを実行してください。
`sudo fsmount -w <ファイルシステム名>`
4. CIFS, FTP, SFTP および TFTP サービスを停止します。
次のとおりサービスごとにコマンドを実行してください。
`sudo svctl -s <対象のサービス (cifs, ftp, sftp または tftp)> --stop`
5. ALog ConVerter との連携を有効にします。
次のとおりコマンドを実行してください。なお、--interval オプションの指定は任意です。

ストレージシステム上のファイルシステムに監査ログを出力する場合

```
sudo alogctl --on --server <ALog マネージャーサーバ名>  
-u <ユーザー名> -p <パスワード> --interval <監査ログの転送間隔>  
--file-system <ファイルシステム名>
```

OS ディスクに監査ログを出力する場合

```
sudo alogctl --on --server <ALog マネージャーサーバ名>  
-u <ユーザー名> -p <パスワード> --interval <監査ログの転送間隔>
```

6. 手順 4 で CIFS, FTP, SFTP および TFTP サービスを停止した場合は起動します。
次のとおりサービスごとにコマンドを実行してください。
`sudo svctl -s <対象のサービス (cifs, ftp, sftp または tftp)> --start`
7. Physical Node 上でコマンドを実行した場合は、クラスタ内のもう一方のノードで、手順 2~6 を実行してください。

(2) ALog ConVerter との連携を開始する手順 (シングルノード構成の場合)

シングルノード構成の HVFP/HDI で、ALog ConVerter との連携を開始する手順を次に示します。

1. ALog マネージャーサーバを名前解決する場合は、IP アドレスとホスト名を、DNS サーバまたはノード上の `/etc/hosts` ファイルに登録します。

`/etc/hosts` ファイルは [Network & System Configuration] ダイアログの [Edit System File] ページで編集してください。

2. 監査ログをファイルシステムに出力する場合は、ファイルシステムを作成します。
監査ログを出力するファイルシステムの設定には条件があります。次のとおりコマンドを実行してください。

```
sudo fscreate --vgr <ボリュームグループ名※> -s 20 <ファイルシステム名>
```

注※ 内蔵ハードディスクではなく、ストレージシステム上のボリュームグループを指定してください。

3. 手順 2 でファイルシステムを作成した場合は、ファイルシステムをマウントします。
次のとおりコマンドを実行してください。

```
sudo fsmount -w <ファイルシステム名>
```

4. CIFS, FTP, SFTP および TFTP サービスを停止します。

次のとおりサービスごとにコマンドを実行してください。

```
sudo svctl -s <対象のサービス (cifs, ftp, sftp または tftp)> --stop
```

5. ALog ConVerter との連携を有効にします。

次のとおりコマンドを実行してください。なお、`--interval` オプションの指定は任意です。

ストレージシステム上のファイルシステムに監査ログを出力する場合

```
sudo alogctl --on --server <ALog マネージャーサーバ名>  
-u <ユーザー名> -p <パスワード> --interval <監査ログの転送間隔>  
--file-system <ファイルシステム名>
```

OS ディスクに監査ログを出力する場合

```
sudo alogctl --on --server <ALog マネージャーサーバ名>  
-u <ユーザー名> -p <パスワード> --interval <監査ログの転送間隔>
```

6. 手順 4 で CIFS, FTP, SFTP および TFTP サービスを停止した場合は起動します。

次のとおりサービスごとにコマンドを実行してください。

```
sudo svctl -s <対象のサービス (cifs, ftp, sftp または tftp)> --start
```

4.7.9 TFTP サービスを使用するとき

TFTP サービスを使用すると、ネットワークブートするためのブートイメージファイルを共有内に格納して、クライアントマシンから使用できます。ここでは、TFTP サービスを使用するときに必要な設定や注意事項について説明します。

TFTP サービスの構成定義

- TFTP サービスを起動する前に、`tftpset` コマンドで TFTP クライアントに公開するディレクトリを設定してください。クラスタ構成の場合、両ノードで同じ設定にする必要があります。
- TFTP サービスを起動している間、公開ディレクトリの削除や、公開ディレクトリがあるファイルシステムのアンマウントを実施しないでください。
- TFTP サービスを起動したら、ノードの OS または Virtual Server が起動または再起動する際に TFTP サービスが自動的に起動するよう、`svstartupset` コマンドで設定しておくことを推奨します。

セキュリティに関する設定

- TFTP クライアントに公開するファイルに対して、その他 (Everyone) に読み取りまたは書き込みを許可してください。
- その他 (Everyone) に書き込み権限が設定されていれば、TFTP クライアントは公開ディレクトリ内のファイルを更新できます。ただし、ファイルおよびディレクトリの新規作成はできません。
- TFTP クライアントに公開しないファイルは、公開ディレクトリ内に格納しないでください。TFTP クライアントに公開しないファイルが公開ディレクトリ内にある場合は、その他 (Everyone) が読み取りおよび書き込みできないよう、ファイルに対してアクセス権を設定する必要があります。
- PXE ブートに使用するファイルに対して、その他 (Everyone) への実行権限を設定してください。
- 不特定多数のクライアントから公開ディレクトリにアクセスされるリスクを低減するため、TFTP クライアントとノードは LAN で接続することを推奨します。WAN での接続は避けてください。

TFTP クライアントおよび外部サーバに関する設定

- ネットワークブートする場合、DHCP サーバなどの外部サーバを使用して、HVFP/HDI の IP アドレスやブートイメージファイルのパスなどの情報をクライアントマシンに取得させる必要があります。クラスタ構成の場合は、ノードまたは Virtual Server の仮想 IP アドレスを使用してクライアントマシンから HVFP/HDI にアクセスするように設定してください。

外部サーバやネットワークブートに使用するソフトウェアなどの環境設定については、それぞれのサーバやソフトウェアのドキュメントを参照してください。

- TFTP クライアントからファイルまたはディレクトリを操作する場合は、公開ディレクトリ以降のパスを指定してください。

例えば、次のように、公開ディレクトリが「/mnt/filesystem01/tftp」で、公開ディレクトリ直下にある「boot」ディレクトリ内のファイル「pxelinux.0」を操作する場合は、「/boot/pxelinux.0」と指定してください。

TFTP クライアントからファイルを操作するときの指定例：

- 公開ディレクトリ：/mnt/filesystem01/tftp
- 操作するファイル：/mnt/filesystem01/tftp/boot/pxelinux.0
- TFTP クライアントの指定：/boot/pxelinux.0

- 名称に円記号 (¥) または非 ASCII 文字が含まれているファイルおよびディレクトリは操作できません。
- シングルノード構成の場合、ノードの起動処理中から TFTP アクセスを繰り返すと、起動処理が完了したあとも TFTP アクセスに失敗することがあります。ノードを再起動するときは、ノードの起動処理が完了するまで TFTP アクセスを停止するよう、クライアントに依頼してください。

4.8 リアルタイムスキャン機能の運用を開始する前に

File Services Manager はネットワーク上に設置したスキャンサーバと連携して、リアルタイムスキャンを実施したり、スキャン結果を通知したりできます。

リアルタイムスキャン機能を利用すると、CIFS クライアントがストレージシステム内のファイルにアクセスしたり、ストレージシステムにファイルを格納したりするときに、該当するファイルのスキャンがスキャンサーバで実施されます。

ウイルス感染ファイルを検出すると、ウイルス情報や感染ファイルを操作していたクライアント情報が、システムログ (syslog) に出力されます。事前に設定している場合は SNMP トラップまたは E-mail でも通知されます。

4.8.1 リアルタイムスキャン機能を運用する場合の注意事項

ここでは、リアルタイムスキャン機能を運用する場合の注意事項を説明します。

(1) リアルタイムスキャンの動作

リアルタイムスキャンの動作を次に示します。

- リアルタイムスキャンは、CIFS クライアントがファイルの一部を参照または更新した場合でもファイル全体をスキャンするため、データベースなどファイルの一部を参照または更新する環境には適していません。
- CIFS クライアント側の Windows エクスプローラでファイルをクリックしたり、右クリックしたりしたときにも、リアルタイムスキャンが実施されます。
- リアルタイムスキャンは、通常のファイル (stat()によって通常のファイルと判断されたファイル) に対して実行されます。キャラクターデバイスファイルや FIFO ファイルなど、通常のファイルでないファイルの場合、スキャンは実行されず、常にアクセスが許可されます。
- 同一の CIFS クライアントから多重にファイルアクセスを行う場合、各ファイルに対してリアルタイムスキャンが実施されます。このため、すべての CIFS アクセス要求が受け付けられるまでに時間が掛かり、CIFS クライアント側でスキャン中のタイムアウトが発生し、エラー終了することがあります。シーケンシャルにアクセスするなど、CIFS クライアント側で多重アクセスを抑える運用を行ってください。なお、HVFP/HDI では、CIFS クライアント側でタイムアウトが発生すると、スキャン処理中のファイルの処理が終了するまでスキャンを続行します。
- リアルタイムスキャンは、Windows の移動ユーザープロファイル機能を使用している環境には適していません。移動ユーザープロファイル機能を使用していると、CIFS クライアントのログオンおよびログオフの処理に続けて、CIFS 共有内の大量のファイルを参照または更新する処理が実行されるため、各ファイルに対してリアルタイムスキャンが実施されます。1KB のファイルのスキャン処理に掛かる時間は数十ミリ秒ですが、スキャン対象のファイル数が数百個以上になると、処理に掛かる時間は合計で数十秒以上になります。このため、スキャン処理に時間が掛かって、クライアントが体感するログオンおよびログオフの処理時間が長くなる場合があります。

(2) リアルタイムスキャンでエラーが発生した場合

リアルタイムスキャンでエラーが発生した場合の注意事項を次に示します。

- リアルタイムスキャン中にエラーが発生した場合、設定によっては、スキャンが完了していないファイルが CIFS 共有内に保存されるおそれがあります。リアルタイムスキャン中にエラーが発生した場合は、SNMP トラップまたは E-mail でも通知されます。システム管理者は障害情報を確認し、リアルタイムスキャンの設定やスキャンサーバの設定に要因があった場合は設定内容を見直してください。
- リアルタイムスキャンでエラーが発生した場合でも、CIFS クライアントが使用していたアプリケーションによっては、クライアントにエラーが通知されないことがあります。CIFS クライアントから、ファイルがコピーされていない、データが更新されていないなどの問い合わせがあった場合、システム管理者は障害情報を確認して、ウイルス感染またはスキャンエラーが発生していないか確認してください。

- [Virus Scan Server Configuration] ダイアログの [Scan Conditions] ページの [Procedure if scanning fails] で [Deny access] を選択した場合、CIFS クライアントがファイルをコピーしたあとでスキャンに失敗すると、コピーしたファイルはストレージシステム内から削除されます。
また、CIFS クライアントがファイルを更新したあとでスキャンに失敗すると、更新内容が取り消され、ファイルは更新前の状態に戻ります。
- [Virus Scan Server Configuration] ダイアログの [Scan Conditions] ページの [Maximum size for scanning] で [Permit access to files that have exceeded the maximum size] チェックボックスをチェックしていない場合に、CIFS クライアントが [Maximum file size] で指定した上限値を超えるファイルをコピーすると、コピーが完了したあとで、コピーされたファイルは削除されます。
また、CIFS クライアントがファイルを更新した際のファイルサイズが、システム管理者が [Maximum file size] に指定した上限値を超えていた場合には、更新内容が取り消され、ファイルは更新前の状態に戻ります。
- [Virus Scan Server Configuration] ダイアログの [Scan Conditions] ページの [Method of dealing with infected file] で [Deny access] を選択した場合、CIFS クライアントがコピーしたファイルがウイルスに感染しているときには、コピーしたファイルがストレージシステムから削除されます。
また、CIFS クライアント更新したファイルがウイルスに感染している場合、更新内容が取り消され、ファイルは更新前の状態に戻ります。
- スキャンサーバへの接続処理でタイムアウトまたはエラーが発生すると、[Virus Scan Server Configuration] ダイアログの [Scan Conditions] ページで設定した値に応じてスキャンサーバが切り替えられ、継続してリアルタイムスキャンを利用できます。ただし、スキャン処理中にスキャンサーバで障害が発生した場合は、別のスキャンサーバに切り替えられずに、リアルタイムスキャンが終了します。スキャンに失敗したファイルにアクセスしていた CIFS クライアントの操作結果は、[Virus Scan Server Configuration] ダイアログの [Scan Conditions] ページで設定した、スキャンに失敗した場合の対処方法に応じて決定されます。

(3) 一時ファイル

Symantec 社またはマカフィー社のスキャンソフトを使用する場合、スキャン条件によっては、一時ファイルが作成されます。一時ファイルが作成される運用の場合の注意事項を次に示します。

- [Virus Scan Server Configuration] ダイアログの [Scan Conditions] ページで、[Scan timing] に [Read and write] または [Write only] が設定されていて、かつ次のどれかの設定が行われている場合は、スキャン対象ファイルを更新した際のウイルス感染またはウイルススキャンエラーに備えて、スキャン対象のファイルと同じフォルダに一時ファイルが作成されます。
 - [Method of dealing with infected file] で [Deny access] が設定されているとき
 - [Maximum size for scanning] で [Specify] を設定し、かつ [Permit access to files that have exceeded the maximum size] が設定されていないとき
 - [Procedure if scanning fails] で [Deny access] が設定されているとき

一時ファイルは次の形式で作成されます。

.ava <プロセス ID><ユニークな文字列>_<スキャン対象のファイル名>_bak

可変値である<プロセス ID>は 5 文字、<ユニークな文字列>は 6 文字です。

このため、CIFS クライアントがファイルを更新する際にリアルタイムスキャンを実施する場合には、スキャンするファイルのサイズ以上の空き容量がファイルシステム内に必要です。十分な空き容量がないと、ファイルの更新に失敗します。

- ・ システム障害が発生すると、一時ファイルが残る場合があります。一時ファイルが残ったままの状態になると、ディスク容量を圧迫することがあります。スキャン対象のファイルにウイルスの感染やデータの破損がないかどうかを確認し、削除または修復してください。
- ・ 作成される一時ファイルは、スキャン対象のファイルの名称より 20 文字長くなります。そのため、ファイルパスが Windows の制限値である 255 文字よりも長くなり、一時ファイルにアクセスできなくなるおそれがあります。一時ファイルにアクセスできない場合、親フォルダの名称を変更してファイルパスを一時的に 255 文字以下にしたあとに一時ファイルを削除または修復してください。
- ・ CIFS クライアントでエクスプローラの詳細ウィンドウが有効な場合、詳細ウィンドウに表示される情報を取得するためにファイルのオープン処理が実行され、オープン処理を契機としてリアルタイムスキャンが実施されます。一時ファイルを作成する設定にしていると、一時ファイルが作成または削除されるたびに、エクスプローラの詳細ウィンドウに表示されているファイル（エクスプローラ上で選択しているファイル）の情報を再取得するためのオープン処理が実行され、対象のファイルに対するスキャンが繰り返されます。
一時ファイルを作成する設定にする場合は、詳細ウィンドウを無効にするか、詳細ウィンドウに表示されるファイルに対する内部的なオープン処理を抑止するため、`cifsoptset` コマンドで `change_notify` が `no` となるように CIFS サービスの構成定義を変更することを推奨します。

(4) WORM ファイル

WORM ファイルをスキャンする場合の注意事項を次に示します。

- ・ WORM ファイルはデータが更新されないため、デフォルトでスキャン対象から除外されています。スキャンサーバを交換した場合やウイルス定義ファイルを更新した場合などに、すべてのファイルをスキャンしたいときは、WORM ファイルをスキャンするよう設定できます。WORM ファイルをスキャンするよう設定する方法については、「コマンドリファレンス」を参照してください。
- ・ WORM ファイルでウイルス感染が検知されても、リテンション期間の範囲内であるファイルは削除できません。
- ・ スキャン実施時に検出されたウイルスがスキャンサーバで修復できるウイルスであっても、WORM ファイルは修復できません。このとき、スキャン条件で設定した内容に関わらず、ウイルスに感染した WORM ファイルへのクライアントからのアクセスを拒否します。感染ファイルの内容が必要な場合は、スキャンを実施するタイミングに [Write only] を設定して、該当するファイルをコピーしてください。コピーしたファイルは修復され、クライアントから内容を参照できます。

(5) スタブファイル

スタブファイルをスキャンすると、HCP から HVFP/HDI ヘデータがリコールされるため、スキャン処理に時間が掛かることがあります。デフォルトでスキャン対象となっています。スタブファイルをスキャン対象から除外するよう設定できます。スタブファイルをスキャン対象から除外するよう設定する方法については、「コマンドリファレンス」を参照してください。

(6) Anti-Virus Enabler ライブラリトレースログファイル (antiviruslib.trace) の管理

Anti-Virus Enabler ライブラリトレースログファイル (antiviruslib.trace) には、スキャン対象のファイルのパスが含まれます。ファイルのパスは CIFS クライアントのユーザー情報であるため、Anti-Virus Enabler ライブラリトレースログファイルの管理には十分注意してください。

Anti-Virus Enabler ライブラリトレースログファイルは、[Check for Errors] ダイアログの [List of RAS Information] ページ ([Batch-download] 表示) からダウンロードできます。

(7) ログイン中の CIFS クライアント数の表示

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] ページにある [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。

4.8.2 スキャンサーバを登録する際の注意事項

ウイルススキャン要求が 1 台のスキャンサーバに集中した場合、スキャンサーバでのウイルススキャン処理が失敗するおそれがあります。リアルタイムスキャンの性能が低下した場合は、HVFP/HDI の利用環境で必要十分な台数となるように調整してください。リアルタイムスキャン機能の運用設計については、「4.8.3 リアルタイムスキャン機能の運用設計」を参照してください。

また、利用環境に関わらず、スキャンサーバでの障害発生に備えて 2 台以上のスキャンサーバを登録することを推奨します。

参考：

次に示すマシン要件のスキャンサーバ 1 台に対して、100KB のプレーンテキストのウイルススキャン要求が同時に 2,000 プロセス以上発生した場合や、15MB の圧縮ファイル（解凍後は 30MB）のウイルススキャン要求が同時に 60 プロセス以上発生した場合は、スキャンサーバでのウイルススキャン処理に失敗するおそれがあります。

CPU：インテル(R) Core(TM)2 Duo 2.4GHz

メモリー：2GB

スキャンサーバ設定：デフォルト値

4.8.3 リアルタイムスキャン機能の運用設計

リアルタイムスキャンを有効にすると、CIFS 共有のファイルを操作するたびに、一時ファイルの作成やスキャンサーバへのファイル転送などの処理が発生します。このため、リアルタイムスキャンを無効にして CIFS サービスを運用する場合に比べ、HVFP/HDI 全体のアクセス性能が低下します。

また、HVFP/HDI の運用中、ファイルシステムの使用状況やネットワーク環境の変化によって、リアルタイムスキャンの性能が低下することがあります。リアルタイムスキャンの性能は、スキャンの実行回数、スキャン対象のファイルの種類や大きさ、HVFP/HDI 全体の負荷、ネットワークの状態、スキャンサーバの性能、スキャンサーバの台数などの影響を受けます。

リアルタイムスキャンの性能が低下すると、スキャンサーバとの接続エラーやスキャンタイムアウトが頻発します。また、運用を開始した直後と比べて、CIFS 共有のファイルの操作に時間が掛かることもあります。

システム管理者は、ログファイルなどの情報を確認し、リアルタイムスキャン機能を使用した HVFP/HDI を効果的に運用できるよう、ハードウェア構成を見直したり、スキャン条件の設定を調整したりする必要があります。

(1) リアルタイムスキャンの性能低下によって発生する問題点

リアルタイムスキャンの性能が低下すると、HVFP/HDI では次のような問題が発生します。

- スキャンタイムアウトが頻発する
- スキャンサーバとの接続エラーが頻発する
- ファイルの操作に時間が掛かる

システム管理者は、SNMP トラップ、E-mail 通知、または CIFS クライアントからのシステム性能低下の連絡によって、リアルタイムスキャンの性能低下を検知できます。

(2) スキャン条件やログファイルの確認

リアルタイムスキャンの性能低下の要因を特定するためには、スキャン条件の設定を確認したり、ログファイルを採取したりする必要があります。

スキャンタイムアウト時間やスキャン対象のファイルの種類など、スキャン条件で設定した内容は、[Virus Scan Server Configuration] ダイアログの [Scan Conditions] ページで確認してください。また、性能低下の要因を特定するために必要なログファイルは、[Check for Errors] ダイアログの [List of RAS Information] ページ ([Batch-download] 表示) でダウンロードしてください。

リアルタイムスキャンの性能が低下したときに、採取したログファイルで確認する情報を、発生した問題点ごとに次の表に示します。

表 4-8 リアルタイムスキャンの性能低下時に確認する必要がある情報

発生した問題点	ログファイル	確認する情報
スキャンタイムアウトが頻発する	レポート情報ファイル (/enas/log/antivirus_report.csv) ※1	<ul style="list-style-type: none"> スキャンタイムアウトしたファイルのサイズ 利用していたスキャンサーバ名
	ユーザー統計情報ファイル (/enas/log/antivirus_stat.csv) ※1	<ul style="list-style-type: none"> コネクションが確立できなかった回数 スキャンタイムアウトが発生した回数 スキャン処理のスループット
	システム動作情報※2	ネットワーク利用率
スキャンサーバとの接続エラーが頻発する	レポート情報ファイル (/enas/log/antivirus_report.csv) ※1	<ul style="list-style-type: none"> スキャンタイムアウトしたファイルのサイズ 利用していたスキャンサーバ名
	ユーザー統計情報ファイル (/enas/log/antivirus_stat.csv) ※1	<ul style="list-style-type: none"> コネクションを確立できなかった回数 スキャンタイムアウトが発生した回数
	システム動作情報※2	ネットワーク利用率
ファイルの操作に時間が掛かる	レポート情報ファイル (/enas/log/antivirus_report.csv) ※1	<ul style="list-style-type: none"> スキャンタイムアウトしたファイルのサイズ 利用していたスキャンサーバ名
	ユーザー統計情報ファイル (/enas/log/antivirus_stat.csv) ※1	<ul style="list-style-type: none"> コネクションが確立できなかった回数 一時ファイル作成時間 作成された一時ファイルのサイズ スキャンタイムアウトが発生した回数
	システム動作情報※2	<ul style="list-style-type: none"> ネットワーク利用率 ディスクドライブへの I/O 量

※1

Anti-Virus Enabler ロググループに含まれます。

※2

システム動作情報ロググループに含まれます。内容を確認するためには、sar のログファイルを解析できる環境が必要です。

レポート情報ファイルに出力される情報の詳細については、「(3) レポート情報ファイル (antivirus_report.csv) の確認」を参照してください。ユーザー統計情報ファイルに出力される情報の詳細については、「(4) ユーザー統計情報ファイル (antivirus_stat.csv) の確認」を参照してください。

(3) レポート情報ファイル (antivirus_report.csv) の確認

レポート情報ファイル (antivirus_report.csv) には、スキャンサーバの設定によってスキャンが完了しなかったファイルおよびウイルスに感染しているファイルなど、リアルタイムスキャンでエラーが発生したファイルの情報が出力されます。レポート情報ファイルを確認することで、ウイルスに感染するおそれのあるファイルの情報や、リアルタイムスキャンでエラーが発生する要因とその傾向を把握できます。

システム管理者はレポート情報ファイルを確認し、リアルタイムスキャンでエラーが発生したファイルを特定して、必要な対処を実施してください。そのあと、エラーが発生したファイルに対して再度スキャンを実施してください。

SNMP トラップまたは E-mail 通知を使用して、レポート情報ファイルが更新されたことを通知できます。レポート情報ファイルが出力されるごとに通知するか、1日1回設定した時刻に通知するかのどちらかを設定できます。デフォルトでは、更新情報を通知しないよう設定されています。SNMP トラップの通知方法を変更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。

レポート情報ファイルの出力例を次に示します。

```
Date,Factor,FilePath,PID,AdditionalInfo
Tue Jun 22 15:01:03 2010,container violation,"/mnt/test/long.zip",
27372,"ViolationInfo = Container extract time violation - scan incomplete.,
ScanServer = 10.213.89.12"
Tue Jun 22 15:14:29 2010,container violation,"/mnt/test/level5.zip",
32386,"ViolationInfo = Container depth violation - scan incomplete., ScanServer
= 10.213.89.12"
Thu Aug 5 08:48:08 2010,container violation,"/mnt/test/sample.doc",
4900,"ViolationInfo = Container size violation - scan incomplete., ScanServer =
192.168.10.60"
Wed Jul 28 06:14:30 2010,virus found,"/mnt/test/eicar.txt",6142,"Action = The
infected file has been deleted."
Wed Jul 28 07:59:21 2010,virus found,"/mnt/test/hydra.com",30971,"Action = The
infected file has been repaired."
Wed Jul 28 02:19:30 2010,server connect error,"/mnt/test/1M.txt",24483,""
```

レポート情報ファイルに出力される情報を次に示します。

表 4-9 レポート情報ファイル (antivirus_report.csv) に出力される内容

項目	内容
Date	ファイルの情報を取得した日時が「MM DD hh:mm:ss」の形式で出力されます。
Factor	リアルタイムスキャンがエラーとなった要因が出力されます。 scan size exceeded スキャン対象とするファイルサイズの上限値を超えていた場合に出力されます。 scan timeout スキャンタイムアウトした場合に出力されます。 Internal error 内部処理でエラーが発生した場合に出力されます。 server connect error スキャンサーバとの接続に失敗した場合に出力されます。 container violation スキャンサーバの設定によって、コンテナファイルをスキャンできなかった場合に出力されます。 server too busy

項目	内容
	<p>スキャン要求が多いため、スキャンサーバが処理できなかった場合に出力されます。</p> <p>Scan server error スキャンサーバでエラーが発生した場合に出力されます。</p> <p>virus found ウイルス感染ファイルを検出した場合に出力されます。</p> <p>Suspected virus ウイルス感染ファイルを検出したか、またはスキャン処理がエラー終了した場合に出力されます。</p>
FilePath	リアルタイムスキャンでエラーが発生したファイルのパスが出力されます。
PID	ファイルにアクセスした CIFS クライアントのプロセス ID が出力されます。
AdditionalInfo	<p>付加情報が出力されます。</p> <p>FileSize スキャンタイムアウトした場合、スキャンタイムアウトしたファイルのサイズが出力されます。</p> <p>ScanServer スキャンタイムアウトした場合、コンテナファイルをスキャンできなかった場合、スキャンサーバが処理できなかった場合、またはスキャンサーバでエラーが発生した場合、スキャンサーバの IP アドレスまたはホスト名が出力されます。</p> <p>ViolationInfo コンテナファイルをスキャンできなかった場合に、その要因が出力されます。コンテナファイルをスキャンできない要因は、スキャンソフトで設定されているスキャンポリシーに依存します。</p> <p>ErrorInfo スキャンサーバでエラーが発生した場合、エラー内容が出力されます。出力内容の詳細は、表 4-10 を参照してください。</p> <p>Action ウイルス感染ファイルを検出した場合に、実施した対処の内容が出力されます。出力内容の詳細は、表 4-11 を参照してください。</p>

表 4-10 エラーが発生した場合にレポート情報ファイルの付加情報 (ErrorInfo) に出力される内容

項目	内容
No scanning software is installed.	スキャンソフトがスキャンサーバにインストールされていない場合に出力されます。
The scanning software service has stopped.	スキャンソフトのサービスが停止している場合に出力されます。
No information about the CIFS share access user is registered.	スキャンサーバに CIFS 共有アクセス用ユーザーの情報が登録されていない場合に出力されます。
The information about the CIFS share access user is incorrect.	スキャンサーバに登録されている CIFS 共有アクセス用ユーザーの情報が不正な場合に出力されます。
An internal processing error occurred on the scan server.	スキャンサーバで内部処理エラーが発生した場合に出力されます。

表 4-11 ウイルス感染ファイルを検出した場合にレポート情報ファイルの付加情報 (Action) に出力される内容

項目	内容
The infected file has been repaired.	感染ファイルを修復した場合に出力されます。

項目	内容
The infected file has been rolled back.	一時ファイルを使用して、感染ファイルを感染前のファイルに置換した場合に出力されます。
The infected file has been deleted.	感染ファイルを削除した場合に出力されます。
A setting allowed access to the file.	修復できない感染ファイルであったため、スキャン条件の設定に従って、クライアントから感染ファイルへのアクセスを許可した場合に出力されます。
A setting denied access to the file.	修復できない感染ファイルであったため、スキャン条件の設定に従って、クライアントから感染ファイルへのアクセスを拒否した場合に出力されます。
The file is a protected file and cannot be repaired.	感染ファイルが WORM ファイル、または WORM ファイル以外の更新、削除ができないファイルであったため、修復できなかった場合に出力されます。
The file is a protected file and cannot be rolled back.	感染ファイルが WORM ファイルであったため、一時ファイルを使用して、感染ファイルを感染前のファイルに置換できなかった場合に出力されます。
The file is a protected file and cannot be deleted.	感染ファイルがリテンション期間内の WORM ファイル、または WORM ファイル以外の更新、削除ができないファイルであったため、削除できなかった場合に出力されます。
No action taken.	修復できない感染ファイルに対してスキャン条件の設定に従った対処ができなかったため、感染ファイルがそのままになっている場合に出力されます。

(4) ユーザー統計情報ファイル (antivirus_stat.csv) の確認

ユーザー統計情報ファイル (antivirus_stat.csv) には、リアルタイムスキャンの実行回数やスキャン処理のスループットなどの情報が出力されます。ユーザー統計情報ファイルを確認することで、リアルタイムスキャンの利用状況を把握したり、リアルタイムスキャンの性能を改善する際に必要となる情報を取得したりできます。

ユーザー統計情報ファイルは定期的に出力されるため、リアルタイムスキャンの性能が低下することがあります。デフォルトでは、ユーザー統計情報ファイルを出力しないよう設定されています。ユーザー統計情報ファイルを出力するよう設定する方法については、「コマンドリファレンス」を参照してください。

ユーザー統計情報ファイルの出力例を次に示します。

```
StartTime,EndTime,PID,IPAddress,ScanCount,AvoidScanCount,CacheHit,Throughput,CreateBackupTime,CreateBackupSize,ConnectRetry,ScanTimeout,RequestOpen,RequestClose
Thu Aug 19 09:21:17 2010,Thu Aug 19 09:25:20
2010,16776,10.213.77.238,0,16,0,0,0.000,0,0,0,16,0
Thu Aug 19 09:26:15 2010,Thu Aug 19 10:23:04
2010,20868,10.213.77.238,0,35,0,0,0.000,0,0,0,32,3
```

ユーザー統計情報ファイルに出力される情報を次に示します。

表 4-12 ユーザー統計情報ファイル (antivirus_stat.csv) に出力される内容

項目	内容
StartTime	情報の収集を開始した日時が「MM DD hh:mm:ss」の形式で出力されます。
EndTime	情報の収集を終了し、ユーザー統計情報ファイルに情報を出力した日時が「MM DD hh:mm:ss」の形式で出力されます。
PID	情報を出力したプロセスのプロセス ID が出力されます。
IPAddress	CIFS クライアントの IP アドレスが出力されます。

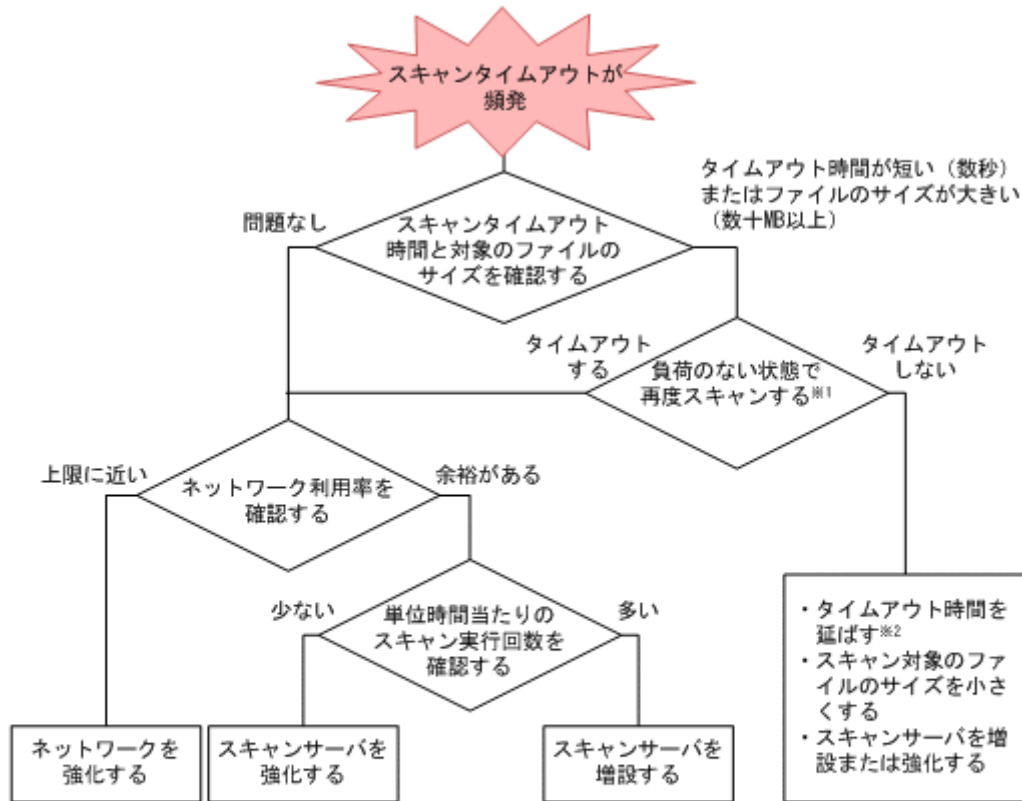
項目	内容
ScanCount	リアルタイムスキヤンの実行回数が出力されます。
AvoidScanCount	スキヤン条件によって、リアルタイムスキヤンが回避された回数が出力されます。
CacheHit	キャッシュヒット率が出力されます（単位は％）。
Throughput	リアルスキヤン処理のスループットが出力されます（単位はKB/秒）。
CreateBackupTime	一時ファイルの作成に掛かった時間の合計が出力されます（単位は秒）。
CreateBackupSize	作成された一時ファイルのサイズの合計が出力されます（単位はMB）。
ConnectRetry	スキヤンサーバに接続する際のリトライ回数が出力されます。
ScanTimeout	スキヤンタイムアウトした回数が出力されます。
RequestOpen	ファイル参照時に要求されたリアルタイムスキヤンの回数が出力されます。
RequestClose	ファイル更新時に要求されたリアルタイムスキヤンの回数が出力されます。

(5) 性能低下の改善方法の検討

システム管理者は必要な情報を採取したら、リアルタイムスキヤンの性能低下の要因に応じた改善方法を検討する必要があります。

発生した問題点ごとにリアルタイムスキヤンの性能を改善する方法を検討するためのフローチャートを図 4-23 リアルタイムスキヤンの性能改善フローチャート（スキヤンタイムアウトが頻発している場合）～図 4-25 リアルタイムスキヤンの性能改善フローチャート（ファイルの操作に時間が掛かる場合）に示します。

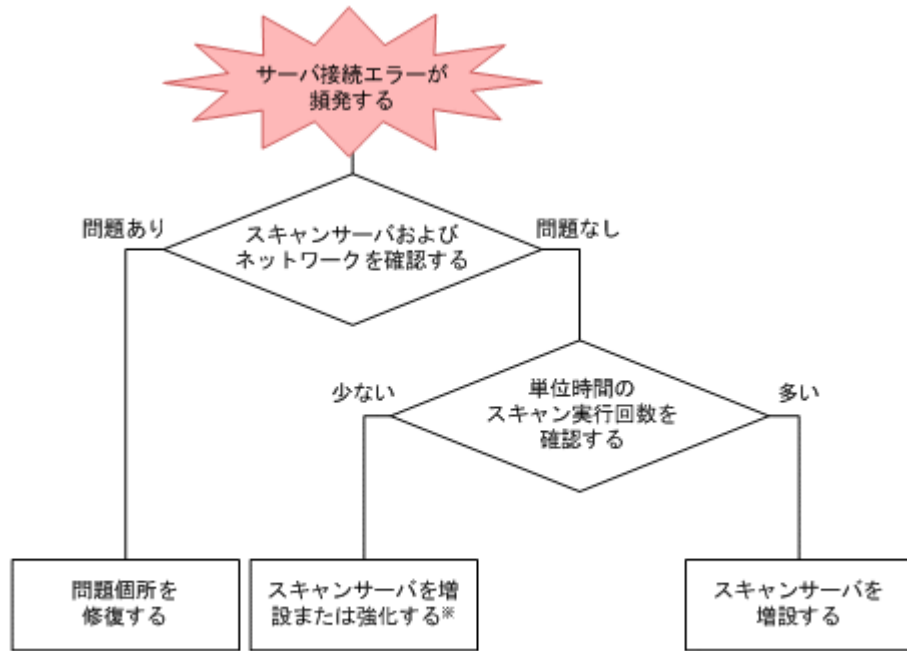
図 4-23 リアルタイムスキャンの性能改善フローチャート(スキャンタイムアウトが頻発している場合)



注※1 ネットワークやスキャンサーバの処理時間の指標があれば、再度スキャンをしなくても、ファイルサイズに対してタイムアウト時間が十分に確保できているかどうか確認できます。

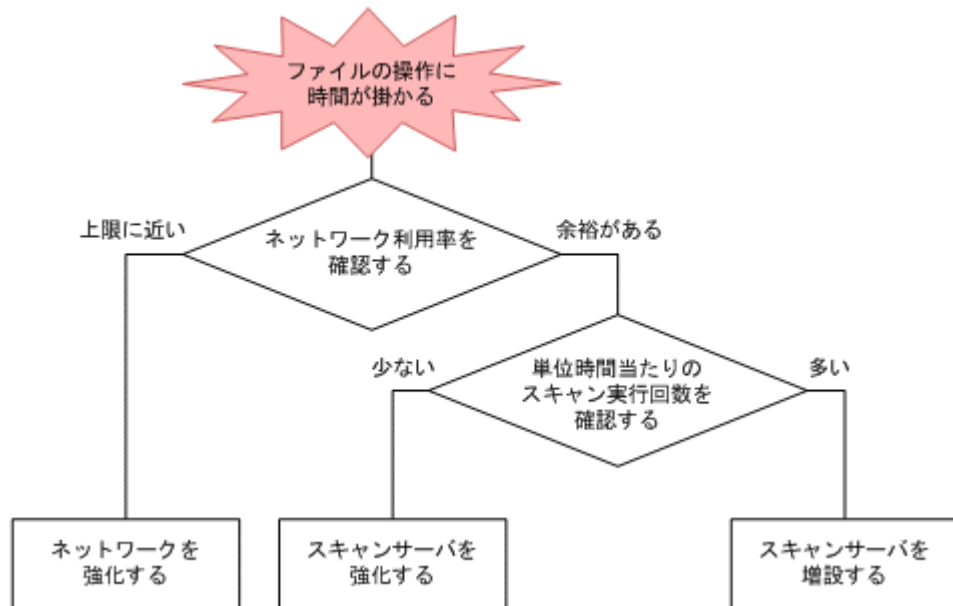
注※2 タイムアウト時間を延ばしても、CIFSクライアント側でタイムアウトすることがあります。その場合は、スキャン対象のファイルサイズの上限を、スキャンタイムアウトしたファイルより小さいサイズに変更するか、スキャンサーバを強化する必要があります。

図 4-24 リアルタイムスキャンの性能改善フローチャート（スキャンサーバとの接続エラーが頻発している場合）



注※ スキャン実行回数が少ない理由として、スキャンサーバの性能が低いために待ち行列が長くなっていることも想定されるため、スキャンサーバの強化が必要なこともあります。

図 4-25 リアルタイムスキャンの性能改善フローチャート（ファイルの操作に時間が掛かる場合）



リアルタイムスキャンの性能を改善する際は、次のことを考慮してください。

スキャンサーバを増設する場合

スキャンサーバとのコネクションを確立できずにエラーが頻発している場合は、スキャンサーバの台数が不足しているおそれがあります。スキャンするファイルの種類やサイズ、同時にアクセスするクライアント数、スキャンサーバのマシン要件などを考慮してスキャンサーバを増設してください。

スキャンサーバを強化する場合

スキャンサーバとのコネクションの確立に問題がなく、ネットワーク利用率も上限に近い状態でない場合は、スキャンサーバの処理性能が不足しているおそれがあります。HVFP/HDI の運用に応じてスキャンサーバを強化してください。なお、サーバの処理性能とスキャン時間の関係については、スキャンソフトのベンダーに確認してください。

ネットワークを強化する場合

ネットワーク利用率が上限に達していて、スキャン処理のスループットも低下している場合、ネットワークの性能によってリアルタイムスキャンの性能が低下しています。HVFP/HDI の運用に応じた転送量を確保できるよう、ネットワークを強化してください。

なお、スキャンサーバの増設や強化、ネットワークの強化など、ハードウェア環境への対策が実現できない場合は、スキャン条件を見直すことで HVFP/HDI への負荷が軽減され、リアルタイムスキャンの性能を改善できます。スキャン条件を見直す方法については「4.8.4 リアルタイムスキャン機能のスキャン条件の見直し」を参照してください。

4.8.4 リアルタイムスキャン機能のスキャン条件の見直し

システム管理者は、[Virus Scan Server Configuration] ダイアログの [Scan Conditions] ページでスキャン条件を見直すことで、リアルタイムスキャンの性能を改善できます。[Check for Errors] ダイアログの [List of RAS Information] ページ ([Batch-download] 表示) でログファイルをダウンロードし、リアルタイムスキャン機能の運用状況に応じて適切な値を設定してください。

(1) キャッシュのサイズを増やす

Symantec 社またはマカフィー社のスキャンソフトを使用する場合、ウイルスに感染していないと判定されたファイルの情報を格納するキャッシュが有効に使用されることで、HVFP/HDI への I/O 負荷を軽減できます。

システム管理者は、ユーザー統計情報ファイルでキャッシュヒット率を確認し、キャッシュヒット率が低い場合は [Cache size of scanning result] に設定されているキャッシュのサイズを増やしてください。なお、HVFP/HDI では、1MB で約 430 ファイル分の情報をキャッシュできます。

(2) スキャンタイムアウト時間を増やす

ネットワーク利用率が低い状態でスキャンタイムアウトが頻発する場合、タイムアウトするまでの時間を増やすことで、スキャンタイムアウトの発生を抑止できます。システム管理者は、システム動作情報のログファイルを確認し、ネットワーク利用率が低い場合は [Connection time-out period] や [Scanning time-out period] に設定されているスキャンタイムアウト時間を増やしてください。

(3) ウイルススキャンの実行回数を減らす

スキャン条件の初期設定では、スキャンを実行するタイミングとして、[Read and Write] が設定されています。[Read only] または [Write only] を設定することで、ウイルススキャンの回数を減らせます。

[Read only] を設定した場合

ファイルへのアクセス時にウイルススキャンが実行されるため、CIFS クライアントへの伝染を抑止できます。

ただし、ウイルス感染しているファイルがストレージシステムに格納されるおそれがあります。

[Write only] を設定した場合

ファイル更新時にウイルススキャンが実行されるため、ウイルスに感染しているファイルがストレージシステムに格納されることを抑止できます。

ただし、ウイルス定義ファイルを最新のものにアップデートしても、スキャン実施時に検出できなかったウイルスが、CIFS クライアントに伝染するおそれがあります。

(4) 一時ファイルの作成を抑止する

Symantec 社またはマカフィー社のスキャンソフトを使用する場合、スキャン対象ファイルを更新した際のウイルス感染またはスキャンエラーに備えて、スキャン対象のファイルと同じフォルダに一時ファイルが作成されます。

システム管理者は、ユーザー統計情報ファイルで一時ファイルの作成時間や作成した一時ファイルのサイズ、システム動作情報のログファイルでディスクドライブへの I/O 量を確認してください。一時ファイルの作成によってディスクドライブへの I/O 負荷が増大している場合は、一時ファイルの作成を抑止することで I/O 負荷を軽減できます。

一時ファイルの作成を抑止する場合には、スキャン条件を次のとおり設定してください。

[Scan timing] で [Read only] を設定している場合

そのほかの設定に関係なく、一時ファイルは作成されません。

[Scan timing] で [Read only] 以外を設定している場合

次のとおり設定すると、一時ファイルは作成されません。

- [Method of dealing with infected file] で [Delete the file] または [Allow access] を設定する※
- [Maximum size for scanning] で [Specify] を選択している場合は、[Permit access to files that have exceeded the maximum size] を設定する
- [Procedure if scanning fails] で [Allow access] を設定する

注※

[Delete the file] を設定した場合、修復できないウイルスを検出すると、ファイルは削除されます。バックアップデータや差分スナップショットを使用してファイルを修復してください。

なお、これらの設定を適用した場合は、一時ファイルによる修復が実施されなくなります。

(5) スキャン対象を選定する

CIFS 共有内に数 100MB を超えるファイルが多数ある場合や、数 GB のファイルがある場合には、ディスクドライブへの I/O 負荷が増加し、HVFP/HDI 全体のレスポンス性能が低下することがあります。また、ファイルの種類によっては、ウイルススキャンの効果を得られないこともあります。

このような場合は、スキャン対象を選定するとディスクドライブへの I/O 負荷を軽減できます。

特定の拡張子のファイルをスキャン対象から除外する

ウイルススキャンの効果を得られるファイルの種類はスキャンソフトのベンダーに確認してください。スキャン対象から除外する拡張子は、[Virus Scan Server Configuration] ダイアログの [Scan Conditions] ページで設定します。

CIFS 共有内の特定のファイルやパスをスキャン対象から除外する

スキャンタイムアウトが発生するような大きなサイズのファイルをレポート情報ファイルから特定できる場合は、該当するファイルやパスをスキャン対象から除外できます。特定のファイルやパスをスキャン対象から除外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。

スキャン対象のファイルのサイズを小さくする

Symantec 社またはマカフィー社のスキャンソフトを使用する場合、レポート情報ファイルでタイムアウトしたファイルのサイズを確認し、スキャン対象ファイルのサイズを見直すことで、該当するファイルをスキャン対象から除外できます。[Maximum size for scanning] の [Maximum file size] でスキャン対象のファイルのサイズを見直してください。

なお、リアルタイムスキャンの対象から除外したファイルに対しては、スキャンソフトをインストールしたマシンを別途用意し、定期的にウイルススキャンを実施するなどの対応を検討してください。

4.9 システム設定情報の管理を開始する前に

HVFP/HDI では、障害が発生した際にも、システム LU および Virtual Server OS LU に格納されているシステム設定情報を回復する機能を提供します。システム LU とは、クラスタの共有 LU および両ノードの OS ディスクの総称です。

OS ディスク

ノード上の OS および OS 上で動作するプログラムが格納される、論理的なディスク領域です。ノードごとに 1 つ割り当てられています。

共有 LU

クラスタ構成やファイルシステムなどに関する設定情報が格納される、ストレージシステムの LU です。クラスタごとに 1 つ割り当てられています。

Virtual Server OS LU

Virtual Server OS LU は、Virtual Server が稼働するために必要な OS やプログラム、設定情報が格納される LU です。Virtual Server ごとに 1 つ割り当てられています。

HVFP/HDI では、システム LU や Virtual Server OS LU を一括して保存するほか、保存したシステム LU または Virtual Server OS LU から情報を抽出したシステム設定情報ファイルをユーザー LU に保存することもできます。

システム LU、Virtual Server OS LU およびシステム設定情報ファイルは、システム管理者が手動で保存したり、設定したスケジュールに従って自動的に保存したりできます。障害が発生した際には、保守員の指示に従い、保存したシステム設定情報ファイルをノードにアップロードしてシステム LU または Virtual Server OS LU を回復できます。

注意：

- システム管理者は、クラスタ構成の定義やファイルシステムの構築など、HVFP/HDI の運用を開始するために必要な情報の設定が完了したあと、ノードの設定情報ファイルをダウンロードし、システム外の記録媒体に保管する必要があります。
- 運用中は、HVFP/HDI のシステムの構成を変更するたびに、手動でノードや Virtual Server の設定情報ファイルを必ずダウンロードしてください。
- 設定情報ファイルをダウンロードしていないと、ストレージシステムやシステム LU、Virtual Server OS LU に障害が発生した場合に回復できなくなるおそれがあります。
- 常にノードや Virtual Server の設定情報ファイルの最新のデータを保管しておかないと、障害が発生した場合にシステム LU や Virtual Server OS LU を正しく回復できないおそれがあります。

システム LU および Virtual Server OS LU は、クラスタごとに 1 世代を保存できます。

システム設定情報ファイルの保存先はシステム管理者が任意に設定できます。また、指定した周期で、自動的にシステム設定情報を保存（定時保存）することもできます。

デフォルトでは、システム設定情報を毎日 00:07（Virtual Server の場合は毎日 03:47、HDI の場合は 12:07）に定時保存する設定となっていますが、定時保存する時刻は、NDMP 機能、ボリュームレプリケーション連携機能、ファイルスナップショット機能および Hitachi File Remote

Replicator のジョブが動作しない時刻に設定してください。また、定時保存する時刻にコマンドの実行や GUI 操作をしないでください。

4.10 障害情報の管理を開始する前に

システム管理者は、HVFP/HDI で障害が発生した場合、障害の発生元や要因を特定するために、管理サーバとノードの障害情報を採取・調査する必要があります。

SNMP 障害通知を利用すれば、事前に設定した SNMP マネージャーに発行されたトラップで、障害の発生元や要因を特定できます。

E-mail による障害通知を利用すれば、事前に設定したシステム管理者などの E-mail アドレスに対して、障害発生時の警告メールを配信できます。

障害要因を特定できない場合には、採取したログファイルを保守員に送付して、障害要因の解析を依頼します。

4.10.1 管理サーバの障害情報

Hitachi Command Suite 共通コンポーネントおよび Hitachi File Services Manager のログファイルは管理サーバ上に出力されます。

Hitachi Command Suite 共通コンポーネントのログファイル

- 統合トレースログファイル
- イベントログ

Hitachi File Services Manager のログファイル

- メッセージログ

システム管理者は、Hitachi File Services Manager のトレースログの最大容量や出力レベルなどの設定を変更できます。

4.10.2 ノードや Virtual Server の障害情報

HVFP/HDI で障害が発生したりユーザーが操作ミスしたりすると、システムメッセージやシステムログなどのログファイルや、core ファイルが障害情報として出力されます。

ノードや Virtual Server の障害情報は、File Services Manager の GUI から、参照、ダウンロードまたは削除ができます。

システム管理者は、ログファイルの保存ファイル数およびファイルの容量を設定したり、core ファイルの保存期間を設定したりできます。

4.10.3 SNMP による障害通知の利用方法

発生した障害によっては、事前に設定した SNMP マネージャーにトラップが発行され、障害情報が通知されます。

SNMP 障害通知を利用する場合は、SNMP マネージャーから定期的に両ノードの MIB 情報を取得し、ノードと通信できることを確認してください。

トラップで通知される障害情報のデータ形式、およびシステムメッセージの確認方法については、「ユーザーズガイド」を参照してください。

4.10.4 E-mail による障害通知の利用方法

発生した障害によっては、E-mail アラート設定ファイル/enas/conf/email_alert.conf に事前に設定したシステム管理者などの E-mail アドレスに対して、障害発生の警告メールが送信されます。

E-mail を使用してシステムを監視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。

4.11 SNMP によるシステム監視を開始する前に

SNMP を使用することで、障害情報をトラップ通知するほかに、MIB オブジェクトの情報を取得してシステムを監視することもできます。CPU、メモリーおよびネットワークを監視するために HVFP/HDI で提供している MIB オブジェクトを次に示します。このほかの MIB オブジェクトについては、「ユーザーズガイド」を参照してください。

表 4-13 CPU に関する MIB オブジェクト

OID	オブジェクト名	説明
.1.3.6.1.4.1.2021.10.1.3	laLoad	システムの負荷状況
.1.3.6.1.4.1.2021.11.9	ssCpuUser	ユーザーが CPU を使っている割合
.1.3.6.1.4.1.2021.11.10	ssCpuSystem	システムが CPU を使っている割合
.1.3.6.1.4.1.2021.11.11	ssCpuIdle	CPU がアイドルである割合
.1.3.6.1.4.1.2021.11.50	ssCpuRawUser	ユーザーが CPU を使っている時間
.1.3.6.1.4.1.2021.11.52	ssCpuRawSystem	システムが CPU を使っている時間
.1.3.6.1.4.1.2021.11.53	ssCpuRawIdle	CPU がアイドルである時間
.1.3.6.1.4.1.2021.11.54	ssCpuRawWait	I/O 待ち CPU 時間

表 4-14 メモリーに関する MIB オブジェクト

OID	オブジェクト名	説明
.1.3.6.1.4.1.2021.4.6	memAvailReal	未使用の物理メモリー量
.1.3.6.1.4.1.2021.4.14	memBuffer	バッファークャッシュ (デバイス I/O 用) の使用量
.1.3.6.1.4.1.2021.4.15	memCached	Page キャッシュ (ファイル I/O 用) の使用量

表 4-15 ネットワークに関する MIB オブジェクト

OID	オブジェクト名	説明
.1.3.6.1.2.1.31.1.1.1.6	ifHCInOctets	ネットワークインターフェース単位の受信バイト数
.1.3.6.1.2.1.31.1.1.1.10	ifHCOctets	ネットワークインターフェース単位の送信バイト数

4.12 ほかのファイルサーバからデータをインポートする前に

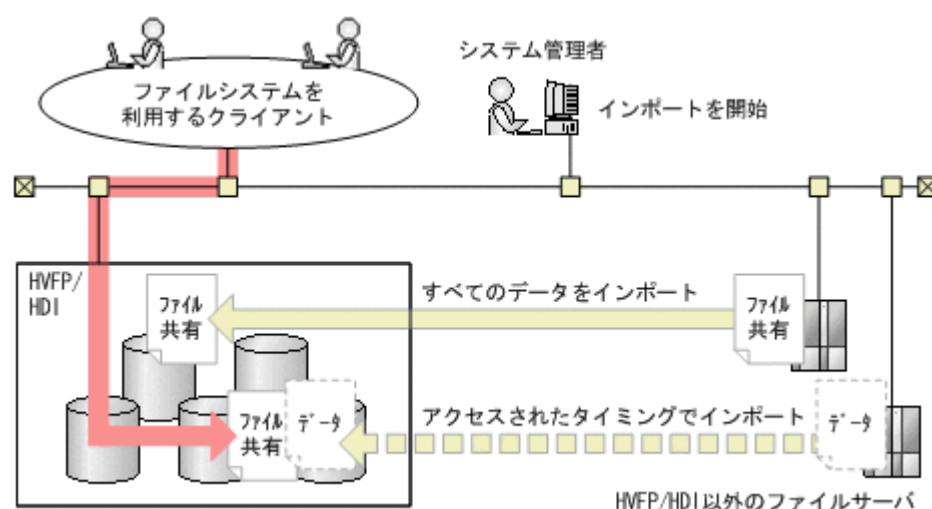
HVFP/HDI では、サービス停止を短時間に抑えて、ほかのファイルサーバからファイルやディレクトリをインポートできます。

ファイルやディレクトリをインポートする方法には、ほかのファイルサーバから共有内のすべてのファイルやディレクトリをインポートする方法と、クライアントがアクセスしたファイルやディレクトリだけをオンデマンドでインポートする方法があります。

オンデマンドでのインポートは、クライアントがインポート対象のファイルやディレクトリにアクセスするタイミングで、アクセス要求のあったファイルやディレクトリだけを HVFP/HDI にインポートします。HVFP/HDI とインポート元のファイルサーバを併用して、HVFP/HDI のファイルシステムの容量を最小限に抑えられます。

すべてのファイルやディレクトリをインポートするよう設定した場合は、オンデマンドでのインポートと並行して、クライアントからのアクセスに関わらず、すべてのファイルやディレクトリを HVFP/HDI にインポートします。HVFP/HDI とインポート元のファイルサーバを併用する期間内に、共有内のすべてのファイルやディレクトリをインポートできます。ほかのファイルサーバを撤去するときは、すべてのファイルやディレクトリをインポートしてください。

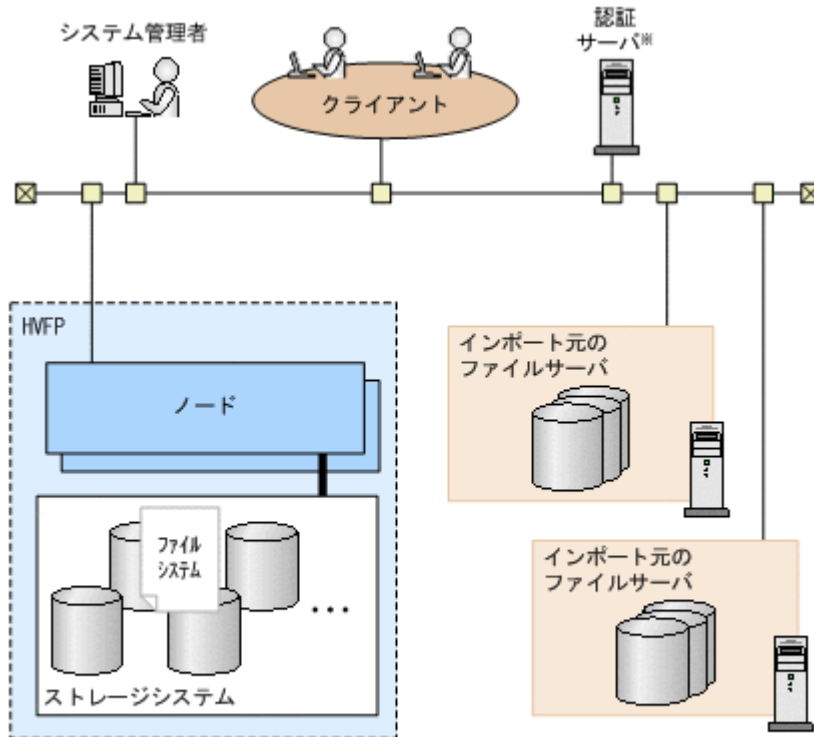
図 4-26 ほかのファイルサーバからのインポートの概要



4.12.1 ほかのファイルサーバからデータをインポートするときのシステム構成

ほかのファイルサーバからファイルやディレクトリをインポートするときのシステム構成の例を次の図に示します。

図 4-27 ほかのファイルサーバからデータをインポートするときのシステム構成例



注※ CIFSクライアントの認証にドメイン認証を使用する場合に必要です。

CIFS クライアントの認証には、ローカル認証およびドメイン認証を使用できます。外部認証サーバには、ドメインコントローラーおよび LDAP サーバを使用できます。

また、システムを構成する際には、次のことに注意してください。

- ・ インポート元のファイルサーバにアクセスできるネットワークに HVFP/HDI を接続します。HVFP/HDI のノードに対して、インポート元のファイルサーバを複数接続できます。
- ・ LDAP サーバでユーザー認証する場合は、インポートするデータに関連するアカウントをユーザー認証用の LDAP に事前に登録してください。
- ・ LDAP 方式のユーザーマッピングを利用する場合は、インポート元のユーザーマッピング用の LDAP の情報と同じ内容を HVFP/HDI に設定してください。
- ・ NFS プロトコルを使用してデータをインポートするときは NFSv2 または NFSv3 プロトコルを使用します。

さらに、次の条件を満たす HVFP/HDI のファイルシステムをインポート先として指定してください。

- ・ 読み取りおよび書き込みを許可してマウントされている
- ・ WORM 機能を使用していない
- ・ 複数ファイルのデータ集約を有効にしていない
- ・ 階層ファイルシステムでない
- ・ ほかの HVFP/HDI からマイグレートされた HCP のデータを共有していない
- ・ Advanced ACL タイプのファイルシステムである (CIFS プロトコルを使用してデータをインポートする場合)
- ・ 共有レベルのセキュリティを使用していない

4.12.2 ほかのファイルサーバからデータをインポートするときの注意事項

ほかのファイルサーバからファイルやディレクトリをインポートするときは、次のことに注意してください。

- インポートを開始する前に、インポート元のファイルサーバへのクライアントからのアクセスを停止し、インポート元のファイル共有を読み取り専用を設定してください。書き込みを許可したままインポートを開始すると、データが破損するおそれがあります。
- インポート先のファイルシステムでは、1 ファイルごとに最大 10KB の管理領域が必要です。ファイルシステムの容量を検討する際に考慮してください。
- インポート先のディレクトリにサブツリー **Quota** を設定する場合は、最上位の共有に対して、クライアントがアクセスしたファイルやディレクトリだけをオンデマンドでインポートするように設定して、インポートを開始してください。そのあと、サブツリー **Quota** を設定してください。**Quota** 設定後、すべてのファイルやディレクトリをインポートするようにインポート方法を変更してください。
- インポート先のファイルシステムに対して **Backup Restore** の機能を使用している場合は、**Backup Restore** の機能で作成したバックアップデータのうち、バックアップ時にインポートが完了していなかったファイルにはアクセスできません。また、インポート先のファイルシステムの差分スナップショット取得時にインポートが完了していなかったファイルにもアクセスできません。
- インポート中でも、インポート先のファイルシステムでファイルスナップショット機能を使用できます。ただし、次の操作はインポートが完了してから実行してください。インポートが完了する前に次の操作を実行すると、インポートされたデータが差分データとして差分格納デバイスに退避され、差分格納デバイスの使用量が上限値に達するおそれがあります。
 - ファイルシステムの拡張
 - ファイルシステムのアンマウント
 - ファイルシステムの設定の変更
 - **HFRR** ペアの定義
- ほかのファイルサーバから **HVFP/HDI** にデータをインポートする際に、**HVFP/HDI** から **HCP** にデータをマイグレートできます。

インポート処理中にマイグレーションを実行したり、インポート先のファイルシステムの残容量が `datamigratelimitset` コマンドで指定した閾値（初期設定は 10%）以下になったりすると、すべてのデータをインポートする処理が一時的に停止して、**HVFP/HDI** でクライアントからアクセスされたデータだけをインポートする処理が実行されます。**HCP** へのマイグレーションが完了すると、インポート先のファイルシステムの残容量が、すべてのデータをインポートする処理が中断したあとで再開する閾値（初期設定は 20%）以上になるまで、ファイルがスタブ化されます。このとき、`arcimplimitset` コマンドで設定したスタブ化の閾値に関わらず、`datamigratelimitset` コマンドの設定に従ってスタブ化されます。インポート先のファイルシステムには、インポート元と比べて十分に大きい容量を割り当ててください。

- インポート先のファイルシステムのデータを **HCP** にマイグレートする場合、マイグレーションの処理時間に影響があるため、すべてのファイルやディレクトリのインポートが完了してからマイグレーションポリシーを設定するか、インポート中も定期的にマイグレーションが実行される運用にしてください。なお、インポート中にマイグレーションが実行されるとすべてのファイルやディレクトリをインポートする処理が一時的に停止し、**HVFP/HDI** でクライアントからアクセスされたファイルやディレクトリだけをインポートする処理が実行されます。マイグレーションが完了したあとにすべてのファイルやディレクトリをインポートする処理が再開します。
- インポート先のファイルシステムのデータを **HCP** にマイグレートする場合、インポート中にマイグレーションが実行されると、`.history` ディレクトリ内にはインポート元サーバを参照するファイルが作成されます。これらのファイルは、ほかのファイルサーバからデータをインポー

トする際の定義情報（インポート定義情報）を削除すると参照できなくなります。この場合、HCP へのマイグレーションが完了したあと、.history ディレクトリ内に作成されたファイルを参照してください。

- すべてのファイルやディレクトリのインポートが完了したら、インポート定義情報を速やかに削除してください。インポート定義情報が残っていると、HCP からのリストアや.history ディレクトリの参照の際に HCP との通信回数が増えるため時間が掛かります。
- クライアントがアクセスしたファイルやディレクトリだけをオンデマンドでインポートする設定の場合、一部のデータが HVFP/HDI にインポートされないことがあります。インポート元のファイルサーバを撤去するときは、撤去する前に、クラスタ構成の場合は datamigratestart コマンドで、シングルノード構成の場合は GUI または datamigratestart コマンドで、すべてのファイルやディレクトリをインポートするよう設定を変更してください。
- ディレクトリの直下にインポートしたファイルまたはディレクトリを削除したり、名称を変更したりした場合、すべてのファイルやディレクトリのインポートを再実行すると、削除や名称変更したファイルまたはディレクトリが再度 HVFP/HDI にインポートされます。
- まだインポートされていないディレクトリへの初回アクセスを契機として、オンデマンドでインポート元サーバからデータがインポートされます。ディレクトリ下のファイルやディレクトリの数が多いとデータのインポートに時間が掛かるため、クライアント側で使用しているエクスプローラなどがタイムアウトすることがあります。インポートの処理は継続しているため、処理が完了するまでしばらく待ってから、対象のディレクトリに再度アクセスしてください。
- インポート中のファイルシステムに対して、全ファイルを対象にした検索のほか、エクスプローラのプロパティ表示、または「フォルダーとデスクトップの説明をポップアップ表示する」機能によるポップアップ表示など、ディレクトリ下を再帰的に走査する処理を実行すると、多数のディレクトリに対してオンデマンドでデータがインポートされるため、時間が掛かります。ディレクトリ下を再帰的に走査する処理は実行しないようにしてください。なお、「フォルダーとデスクトップの説明をポップアップ表示する」機能は、エクスプローラの [フォルダーオプション] で無効にできます。
- ファイルやディレクトリの名称の先頭文字がピリオド (.) の場合、インポート先では隠しファイル属性が付与されます。
- クライアントがアクセスしたファイルやディレクトリだけをオンデマンドでインポートする設定の場合、インポート先のファイルシステムでは、すべての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。オフライン属性については、「ファイルアクセス (CIFS/NFS) ユーザーズガイド」を参照してください。
- インポート先のファイルシステムのデータを、インポート中に HCP にマイグレートする場合、HCP へのマイグレーションが完了していないファイルにはオフライン属性が設定されています。オフライン属性については、「ファイルアクセス (CIFS/NFS) ユーザーズガイド」を参照してください。

また、インポートに使用するプロトコルによって、次のことにも注意してください。

CIFS プロトコルを使用してデータをインポートする場合

- インポート元のファイルサーバが Windows 環境の場合、HVFP/HDI との ACL の仕様差異が原因で、インポートが完了したファイルにアクセスできないことがあります。Windows 環境からユーザー資源を移行したときの仕様差異については、「ファイルアクセス (CIFS/NFS) ユーザーズガイド」を参照してください。
- インポート元の CIFS 共有には、共有の最上位のディレクトリを指定してください。インポート元に指定した CIFS 共有の配下に属する別の CIFS 共有も同時にインポートされます。

- インポート元の CIFS 共有では、アクセスベースの列挙 (Access Based Enumeration) を無効にしてください。インポート元の CIFS 共有でアクセスベースの列挙を有効にしていると、アクセス権がないファイルを検出できません。
- インポート元の共有内のディレクトリをクライアントのネットワークドライブに割り当てている場合は、クライアントからのアクセスを停止するときに、ネットワークドライブの割り当てを解除するよう、クライアントに依頼してください。クライアントからのアクセスを開始するときには、インポート先の共有内のディレクトリをネットワークドライブに割り当てるよう依頼してください。
- ショートカットをインポートした場合、必要に応じて、ショートカットのリンク先を変更する必要があります。クライアントがインポート元のファイルサーバのホスト名や IP アドレスをリンク先に指定しているときは、インポート先のノードのホスト名や IP アドレスに変更するよう、クライアントに依頼してください。
- CIFS クライアントがファイルを更新した際にリアルタイムスキャンを実施するよう設定している場合でも、すべてのファイルやディレクトリのインポートを開始する前に、インポート対象のファイルのウイルススキャンを実施することを推奨します。すべてのファイルやディレクトリをインポートするとき、インポート中のファイルに対してリアルタイムスキャンは実施されません。
また、インポートが完了する前のファイルに CIFS クライアントがアクセスするとき、ファイルのスキャン処理に時間が掛かることがあります。スキャンタイムアウトが発生するような大きなサイズのファイルにクライアントがアクセスするときは、スキャンするファイルのサイズの上限値を小さくしたり、スキャンに失敗したファイルへのアクセスを許可したりすることを検討してください。なお、スキャンタイムアウトが発生してもインポートの処理には影響ありません。
- ドメイン認証を使用してインポートする場合、CIFS サービスが稼働している必要があります。インポート処理中に CIFS サービスが停止すると、インポート処理がエラーになるおそれがあります。その場合は、CIFS サービスを起動後、インポートを再実行してください。

NFS プロトコルを使用してデータをインポートする場合

- ハードリンクの情報もインポートされます。ただし、インポートされたハードリンクが HCP にマイグレートされる際には、1つのファイルとしてマイグレートされます。
- インポート元の共有ディレクトリ以下にハードリンクがある場合、インポート先の共有ディレクトリ以下にサブツリー Quota を設定するときは、同じサブツリー Quota のディレクトリ以下にすべてのハードリンクがインポートされるように、サブツリー Quota を設定してください。サブツリー Quota の範囲が異なるハードリンクはインポートされません。

4.13 クライアントがファイルシステムの利用を開始する前に

この節では、HVFP/HDI のクライアントがファイルシステムの利用を開始する前に、システム管理者が知っておく必要があることを説明します。

4.13.1 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場合で、HVFP/HDI の設定を変更するときの注意事項を次に示します。

- NFS クライアントからマウントしている HVFP/HDI のファイルシステムを再作成する場合は、再作成する前に NFS クライアントでアンマウントし、再作成したあとにマウントしてください。
- NFS クライアントからファイルシステムをマウントした状態で HVFP/HDI の NFS 共有を削除すると、NFS クライアントの実装によっては、NFS クライアントからファイルシステムをアンマウントできないことがあります。この場合、NFS クライアントホストを再起動すると、マウント状態を解除できます。
- NFS クライアントからマウントしているファイルシステムの NFS マウントポイントの属性を変更しても、変更結果を NFS クライアント側で確認できないことがあります。この場合は、NFS クライアントからファイルシステムをマウントし直してください。
- NFS クライアントホストの管理者は、システム管理者が NFS 共有に対する最大転送長を変更する前に、NFS クライアントでファイルシステムをアンマウントする必要があります。システム管理者の依頼を受けてから NFS クライアントでアンマウントし、変更が完了したことを確認してから NFS クライアントで再度マウントしてください。

なお、NFS クライアントからファイルシステムを利用する場合、次に示す場面でもそれぞれ幾つかの注意事項があります。詳細は、「ファイルアクセス (CIFS/NFS) ユーザーズガイド」を参照してください。

- 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
- NFS クライアントからファイルロックを利用するとき
- NFS クライアントからファイルシステムを利用するとき

4.13.2 CIFS 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

CIFS 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は、「ファイルアクセス (CIFS/NFS) ユーザーズガイド」を参照してください。

なお、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。

4.13.3 FTP 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

FTP 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。

- 名称に非 ASCII 文字が含まれているファイルやディレクトリを FTP クライアントから操作する場合は、正しく表示できるようにクライアント側で操作環境の文字コードを設定する必要があります。
- フェールオーバー時やフェールバック時に、FTP クライアントが対象のリソースグループに属するファイルシステムにアクセスしていると、強制的に接続が切断されるか応答待ちになります。ファイルシステムへのアクセスを再開する場合は、再接続してください。
- FTP サービスを使用する場合、anonymous ユーザーは、ファイル名に非 ASCII 文字が含まれているファイルをアップロードできません。
- ftp コマンド指定する HVFP/HDI 上のファイル名またはディレクトリ名が「~< FTP ユーザー名 >」の場合、FTP クライアントからコマンドを実行するときには、絶対パスで指定するか、または上位の階層からの相対パスを付けて指定してください。
絶対パスまたは上位の階層からの相対パスを付けずに、ファイル名またはディレクトリ名に「~<文字列>」だけを指定して ftp コマンドを実行した場合は、次のとおり動作します。
 - <文字列>が HVFP/HDI に登録されているユーザー名の場合：

指定されたユーザーのホームディレクトリが **FTP** ログインディレクトリ下にあるときは、指定されたユーザーのホームディレクトリまたはホームディレクトリと同名のファイルを処理対象とします。

指定されたユーザーのホームディレクトリが **FTP** ログインディレクトリ下にはないときは、エラーとなります。

- <文字列>が **HVFP/HDI** に登録されているユーザー名でない場合：
「~<文字列>」を処理対象とします。
- **FTP** クライアントからファイル名またはディレクトリ名に「~」だけを指定して `ftp` コマンドを実行した場合は、**FTP** ログインディレクトリを処理対象とします。
- **SFTP** サービスは、**SSH2** だけをサポートしています。
- **SFTP** サービスでは、同時にログインするクライアントの数が **500** を超えないようにしてください。 **500** を超えるクライアントが同時にログインすると、システムの動作が不安定になります。

HVFP/HDI のバックアップ運用

この章では、HVFP/HDI のバックアップ運用について、システム管理者が理解または考慮する必要があることについて説明します。

- 5.1 バックアップ運用の概要
- 5.2 NDMP 機能の運用について
- 5.3 ファイルスナップショット機能の運用について
- 5.4 差分スナップショットの運用例
- 5.5 差分格納デバイスの容量の設計
- 5.6 差分格納デバイスの使用量に関する設定
- 5.7 ファイルスナップショット機能で運用しているファイルシステムの拡張
- 5.8 差分スナップショットの自動作成の運用
- 5.9 Hitachi File Remote Replicator について
- 5.10 Hitachi File Remote Replicator を使用する場合の運用設計

5.1 バックアップ運用の概要

HVFP/HDI で利用できるバックアップ運用は次のとおりです。

- NDMP (Network Data Management Protocol) 機能 (Backup Restore)

NDMP をサポートしたバックアップ管理ソフトウェアと連携することで、ファイルシステムのデータをネットワーク上のテープ装置に退避できます。

ファイルスナップショット機能と連携して、ファイルシステムのサービスを継続した状態で、ファイルシステムのバックアップを取得することもできます。

NDMP 機能の運用については「[5.2 NDMP 機能の運用について](#)」を参照してください。

- ボリュームレプリケーション連携機能 (Backup Restore)

RAID Manager と、ストレージシステムの ShadowImage, TrueCopy または Universal Replicator と連携することで、ファイルシステムのデータを任意のノード、Virtual Server またはストレージシステムに複製できます。

ファイルスナップショット機能を使用している場合、ファイルシステムとペアになっている差分格納デバイスも複製します。

ボリュームレプリケーション連携機能のコマンドの文法については「コマンドリファレンス」を参照してください。また、運用方法については「エンタープライズアレイ機能連携ユーザーズガイド」または「ミッドレンジアレイ機能連携ユーザーズガイド」を参照してください。

- ファイルスナップショット機能

ファイルシステムの更新時に差分データをストレージシステム内に蓄積し、そのデータとファイルシステムのデータを使用して、仮想的にスナップショットを作成できます。少量の更新が多く、小規模な回復が必要な環境に有効です。ファイルシステムや差分スナップショットの運用方法によっては、差分データの退避先のディスク容量を抑えることができます。

NDMP 機能と連携すると、差分スナップショットのデータをバックアップできます。ボリュームレプリケーション連携機能を使用すると、ファイルシステムと差分格納デバイスのデータを、任意のノード、クラスタまたはストレージシステムにコピーできます。

ファイルスナップショット機能の運用については「[5.3 ファイルスナップショット機能の運用について](#)」を参照してください。

また、Hitachi File Remote Replicator と連携すると、あるサイトの差分スナップショットを別のサイトに遠隔バックアップし、複製できます。

Hitachi File Remote Replicator については「[5.9 Hitachi File Remote Replicator について](#)」を参照してください。また、Hitachi File Remote Replicator を使用する場合の運用設計については「[5.10 Hitachi File Remote Replicator を使用する場合の運用設計](#)」を参照してください。

これらのバックアップ機能は、ほかの HVFP/HDI からマイグレートされた HCP のデータを共有していないファイルシステムに対して使用できます。また、ボリュームレプリケーション連携機能は、HCP にデータをマイグレートしていないファイルシステムに対して使用できます。

アプリケーションでデータを使用している状態で Backup Restore の機能を利用する場合は、使用中のデータと、バックアップまたはリストアされるデータとの整合性を考慮してください。

5.2 NDMP 機能の運用について

ここでは、NDMP 機能を運用するに当たって、システム管理者が知っておいた方がよいことについて説明します。

5.2.1 NDMP 機能の概要

NDMP 機能は、バックアップ管理ソフトウェアと連携して、ファイルシステムのデータをバックアップメディアにコピーしたり、バックアップメディアのデータをファイルシステムに復元したりします。

ストレージシステム以外のバックアップメディアにデータをコピーするため、ストレージシステムのハードウェアに障害が発生した場合でも、コピーしておいたデータを基にファイルシステムのデータを復旧できます。

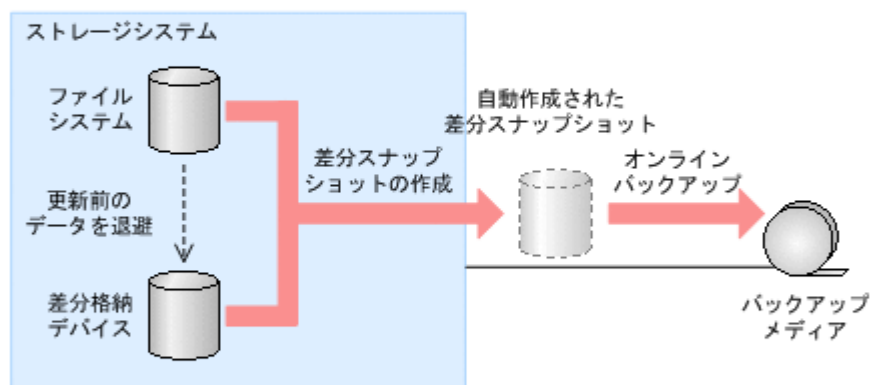
NDMP 機能の概要を次の図に示します。

図 5-1 NDMP 機能の概要

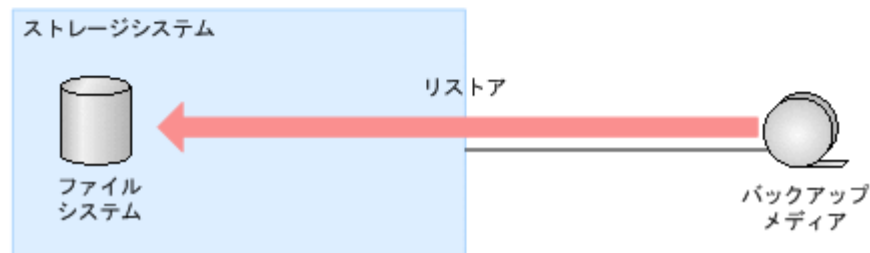
オフラインバックアップでデータをメディアにバックアップする



オンラインバックアップでデータをメディアにバックアップする



データをリストアしてファイルシステムを復元する



NDMP 機能では、次のテープ装置を使用できます。

- ・ メディアサーバに接続されたテープ装置
- ・ ノードに SAN で接続されたテープ装置※

注※

クラスタ構成で運用している場合に使用できます。

バックアップの方法には、オフラインバックアップとオンラインバックアップの 2 種類があります。

オフラインバックアップ

ファイルシステム、またはユーザーが作成した差分スナップショットのデータをメディアにバックアップする方法です。

ファイルシステムの運用を止めてからオフラインバックアップを実行することを推奨しますが、運用中のファイルシステムに対してもオフラインバックアップを実行できます。

ファイルシステムの運用を止めないでオフラインバックアップを実行した場合、デフォルトではオフラインバックアップの正確性チェックが強化されていないため、オフラインバックアップ中にファイルが変更または削除されてもオフラインバックアップ処理が継続されます。

`ndmpfsconfig` コマンドを使用してオフラインバックアップの中断条件を変更すれば、オフラインバックアップの正確性チェックを強化できます。オフラインバックアップの正確性チェックを強化した場合と強化していない場合のオフラインバックアップ処理の動作の違いを次に示します。

- オフラインバックアップの正確性チェックを強化していない場合（デフォルト）
オフラインバックアップ中にファイルが変更または削除されてもオフラインバックアップ処理は成功しますが、バックアップされたファイルの整合性は保証されません。
夜間に行っていたオフラインバックアップが業務開始時間までに終了しなくても、オフラインバックアップ処理を中断したくない場合などに使用できます。
- オフラインバックアップの正確性チェックを強化している場合
オフラインバックアップ中にファイルが変更または削除されたとき、オフラインバックアップ処理はエラー終了します。

オンラインバックアップ

ファイルスナップショット機能と連携してバックアップ用に自動作成した差分スナップショットのデータをメディアにバックアップする方法です。

ファイルシステムの運用を止めなくても、整合性が保証されたバックアップを取得できます。

5.2.2 バックアップメディアの容量の見積もり

バックアップメディアには、バックアップ対象のディレクトリおよびファイルの容量以外に、Quota 情報や inode 情報、ACL 情報などをバックアップするための容量が必要です。メディアの容量が不足した場合は、バックアップがエラー終了します。次の見積もり式で算出される値を目安にして、容量に余裕を持ってバックアップメディアを準備してください。

なお、HCP と連携したマイグレーションを運用している場合、メディアにバックアップされるのはマイグレーション対象外のファイルと、マイグレーション後に更新が発生したファイルだけです。そのため、見積もり式で見積もった容量から、メディアにバックアップされないファイル（マイグレーション後に更新が発生していないファイル）の容量を差し引いて検討してください。例えば、バックアップされないファイルの比率が全体の 60%ある場合、計算式で見積もった値の 40%の容量を目安にしてバックアップメディアを準備します。

データ集約による容量節約が有効なファイルシステムをバックアップした場合、容量が削減された状態でバックアップメディアにデータが格納されます。この場合、バックアップメディアは、バックアップ対象のボリュームのディスク使用量を目安にして準備します。ただし、バックアップ方法によってはデータ集約が解除された状態のデータが格納されます。どのような場合にデータ集約が解除された状態のデータが格納されるかについては、「[5.2.14 データ集約されているファイルシステムのバックアップ、リストアについて](#)」を参照してください。

バックアップメディアの容量の見積もり式 (Advanced ACL タイプの場合)

バックアップメディアの容量 (単位: バイト)

$$= \left\lceil \frac{252(A+B) + 456}{512} \right\rceil \times 512 + \left(\left\lceil \frac{260(G+H) + 586}{512} \right\rceil \times 512 \right) \times I \\ + \left\lceil \frac{2048 + J \times 88}{512} \right\rceil \times 512 \times C + D$$

(凡例)

- ↑ ↑: 小数点以下を切り上げる
- A: ファイルシステムQuotaが設定されているユーザー数
- B: ファイルシステムQuotaが設定されているグループ数
- C: バックアップ対象のディレクトリとファイルの合計数
- D: バックアップ対象のボリュームのディスク使用量 (単位: バイト)
- G: ファイルシステム直下の各ディレクトリでサブツリーQuotaが設定されている平均のユーザー数
- H: ファイルシステム直下の各ディレクトリでサブツリーQuotaが設定されている平均のグループ数
- I: サブツリーQuotaが設定されているディレクトリ数
- J: ディレクトリまたはファイル当たりの運用上の平均ACE設定数

バックアップメディアの容量の見積もり式 (Classic ACL タイプの場合)

バックアップメディアの容量 (単位: バイト)

$$= \left\lceil \frac{252(A+B) + 456}{512} \right\rceil \times 512 + \left(\left\lceil \frac{260(G+H) + 586}{512} \right\rceil \times 512 \right) \times I \\ + \left\lceil \frac{2048 + F(E+5)}{512} \right\rceil \times 512 \times C + D$$

(凡例)

- ↑ ↑: 小数点以下を切り上げる
- A: ファイルシステムQuotaが設定されているユーザー数
- B: ファイルシステムQuotaが設定されているグループ数
- C: バックアップ対象のディレクトリとファイルの合計数
- D: バックアップ対象のボリュームのディスク使用量 (単位: バイト)
- E: ACLを設定しているユーザーまたはグループ名の運用上の平均けた数長
- F: ディレクトリまたはファイル当たりの運用上の平均ACL設定数
- G: ファイルシステム直下の各ディレクトリでサブツリーQuotaが設定されている平均のユーザー数
- H: ファイルシステム直下の各ディレクトリでサブツリーQuotaが設定されている平均のグループ数
- I: サブツリーQuotaが設定されているディレクトリ数

なお、バックアップ対象のボリュームのディスク使用量およびディレクトリとファイルの合計数は、File Services Manager の GUI に表示されるファイルシステムの使用量および inode の使用量または fslist コマンドで表示される Block used (GB) および I-node used で確認してください。データ集約によって容量節約されたファイルシステムの場合、削減後の容量が表示されます。

5.2.3 オンラインバックアップに使用する差分格納デバイスの設定

オンラインバックアップを行う運用の場合は、ファイルシステムのバックアップを取得する前に、差分格納デバイスを設定する必要があります。

オンラインバックアップの場合、テープ装置へのオンラインバックアップは差分スナップショットのデータを基に実行されます (オンラインバックアップ用の差分スナップショットは自動的に作成されます)。差分格納デバイスは、1つのファイルシステムに対して1つだけ設定できます。オンラインバックアップを実行した際に、差分格納デバイスの容量が不足していた場合、および差分スナップショットが予約世代数に達していた場合は、オンラインバックアップがエラー終了します。

差分格納デバイスの容量については「5.5 差分格納デバイスの容量の設計」を、差分スナップショットの予約世代数については、「5.3.4 差分スナップショットの管理」を参照してください。

5.2.4 バックアップおよびリストア対象のデータについて

NDMP 機能では、次のデータがメディアにバックアップされます。

- ファイルシステムの情報 (Quota 情報, WORM 機能に関する設定)
- ディレクトリおよびファイルの情報 (inode, ACL 情報, ファイル属性)
- ディレクトリおよびファイル

参考:

バックアップ対象となるディレクトリおよびファイルの属性情報については、「E.1 バックアップされる属性情報」を参照してください。

NDMP 機能では、メディアにバックアップしたデータは、バックアップ対象と同じクラスタ内のノードまたは Virtual Server にリストアできます。バックアップ対象のノードまたは Virtual Server とは別のクラスタへのリストアは、サポートしていません。

5.2.5 バックアップおよびリストアの実施時間について

サービスの停止やレスポンスの低下など、ユーザーの業務への影響を少なくするために、バックアップおよびリストアは、システム全体の負荷が低い時間帯に実行することを推奨します。

次の操作をした場合、処理が完了するまでに時間が掛かることがありますので、ご注意ください。

- ストレージシステム内のボリューム (ファイルシステムや差分スナップショットなど) に対してクライアントが頻繁にアクセスしている状況で、バックアップまたはリストアを実行する
- ファイルスナップショット機能の操作とバックアップまたはリストアの操作を同時に実行する

5.2.6 インクリメンタルバックアップの運用について

インクリメンタルバックアップとは、前回のバックアップ以降に内容が変更されたデータを対象とするバックアップ方法です。

インクリメンタルバックアップには、次の 2 種類があります。

差分バックアップ

前回の正常なフルバックアップのあとで変更されたデータをすべてバックアップする方法です。

増分バックアップ

前回の正常なフルバックアップ、差分バックアップまたは増分バックアップのあとで変更されたデータをバックアップする方法です。

インクリメンタルバックアップを行う運用の場合は、次のことに注意してください。

- 前回のバックアップ以降に内容を変更していないディレクトリおよびファイルに対して次の操作が実行されていても、インクリメンタルバックアップの対象にはなりません。
 - パスの変更 (移動)
 - 名称の変更
 - 削除

ディレクトリおよびファイルを変更しないでファイルシステムの構成を変更した場合は、フルバックアップを取得することを推奨します。構成を変更した場合にフルバックアップを取得しておかないと、障害発生直前の状態に回復できないことがありますので、注意してください。

- ボリュームレプリケーション連携機能で作成したコピー先ファイルシステムをバックアップ元に指定して、インクリメンタルバックアップを運用することはできません。
- Quota 情報が設定されたファイルシステムやディレクトリをバックアップ元に指定した場合、インクリメンタルバックアップを実行したときにも、Quota 情報はすべてバックアップされます。
- Backup Restore では、インクリメンタルバックアップの履歴情報をファイルシステムごとに管理します。

差分スナップショットをバックアップ元に指定した場合は、差分スナップショットを取得した時刻にバックアップを実行したものとして、履歴情報が記録されます。

例えば、次の2つのファイルシステムに対して、6:00 にオフラインバックアップを実行したと仮定します。

filesystem01

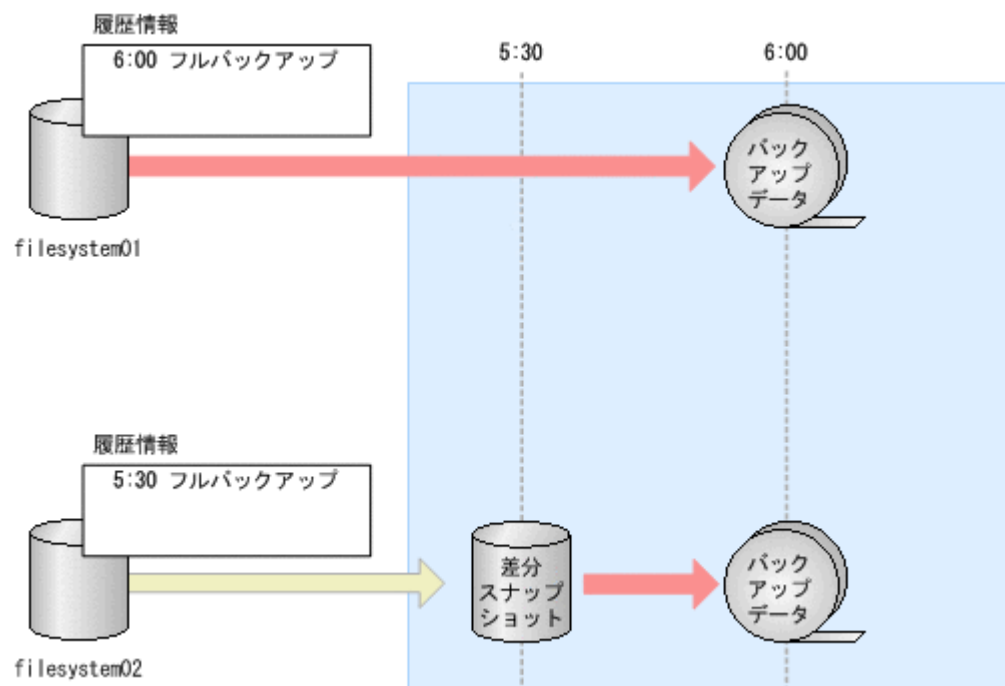
バックアップ元に、ファイルシステムを指定しています。

filesystem02

バックアップ元に、5:30 にあらかじめ取得しておいた差分スナップショットを指定しています。

この場合、履歴情報は次の図のとおり記録されます。

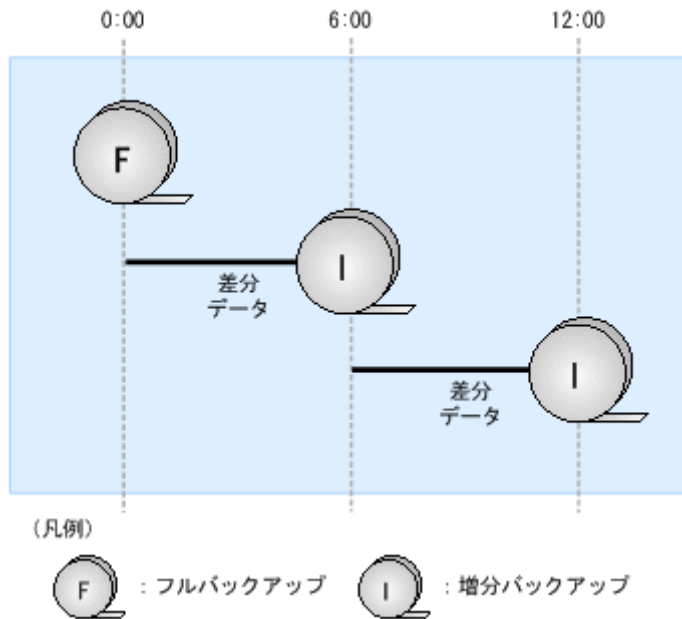
図 5-2 バックアップの履歴情報



filesystem01 の履歴情報は、6:00 にオフラインバックアップを実行したものとして記録されます。一方、filesystem02 の履歴情報は、バックアップ元の差分スナップショットが取得された時刻 (5:30) にオフラインバックアップを実行したものとして記録されます。

- 1つのファイルシステムでは、1つの NDMP ポリシーでインクリメンタルバックアップを運用することを推奨します。1つの NDMP ポリシーで運用した場合に取得される増分バックアップの例を次に示します。

図 5-3 1つの NDMP ポリシーで運用した場合の増分バックアップ



増分バックアップを1つの NDMP ポリシーの下で運用した場合は、同じポリシーで直前に取得されたフルバックアップまたは増分バックアップからの差分データがバックアップされます。6:00 に実行される増分バックアップでは、0:00 以降の差分データがバックアップされます。同様に、12:00 に実行される増分バックアップでは、6:00 以降の差分データがバックアップされます。

5.2.7 NDMP サーバへのアクセス制限について

/etc/hosts ファイルにバックアップサーバの IP アドレスやホスト名などを登録しておく、NDMP サーバにアクセスできるクライアントを/etc/hosts ファイルに登録したバックアップサーバだけに限定できます (/etc/hosts ファイルにバックアップサーバの情報を登録しない場合は、どのクライアントからも NDMP サーバにアクセスできる状態になります)。また、/etc/hosts ファイルに登録されたバックアップサーバ以外のクライアントからアクセスがあった場合には、KAQB14211-W メッセージおよび KAQB14213-W メッセージが NDMP サーバログ (/enas/log/ndmpserver.log) に出力されます。

システム管理者は、HVFP/HDI の運用形態を考慮して、不正なアクセスを防止する場合は、バックアップサーバの情報を次の形式で/etc/hosts ファイルに登録してください。

<IP アドレス> <ホスト名> <バックアップサーバ名> [<ホスト名のエイリアス> ...]

バックアップサーバ名は、必ず「BackupServer」で始まる名称にしてください。また、バックアップサーバ名には、英数字またはアンダーライン (_) を使用してください。/etc/hosts ファイルには、バックアップサーバの情報を最大で 256 個登録できます。257 個以上登録した場合、257 番目以降の情報は無効になります。

/etc/hosts ファイルへの追記例を次に示します。

```
#
# BACKUP SERVER ADDRESS
#
10.208.151.19 back-1 BackupServer01
10.208.151.197 back-2 BackupServer02
```

ノード上の/etc/hosts ファイルに登録した情報は、クラスタ内の両方のノードに反映されます。Virtual Server 上の/etc/hosts ファイルに登録した情報は、情報を登録した Virtual Server だけに反映されます。

また、ノード上で/etc/hosts ファイルを編集したあとには、クラスタ内の両方のノードで NDMP サーバを再起動する必要があります。Virtual Server 上で編集したあとには、/etc/hosts ファイルを編集した Virtual Server 上で NDMP サーバを再起動する必要があります。NDMP サーバを再起動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。

5.2.8 バックアップまたはリストア時の通信経路について

NDMP サーバとメディアサーバ間、NDMP サーバとバックアップサーバ間の通信経路は、File Services Manager で設定したルーティング情報に従います。このため、File Services Manager の設定によっては、バックアップまたはリストア時に NDMP サーバとメディアサーバ間で行われる通信と、NDMP サーバとバックアップサーバ間で行われる通信で、使用されるポートやルーティングが異なることがあります。

5.2.9 バックアップまたはリストア中に実行できない操作

ndmpcontrol コマンドを実行したり、ndmpconfig コマンド、tapeadd コマンドまたは tapedel コマンドを実行して NDMP サーバが自動的に再起動されたりすると、コマンドを実行したノードまたは Virtual Server で処理中のバックアップまたはリストアがエラー終了するおそれがあります。

また、ノードに SAN で接続されたテープ装置を使用したバックアップまたはリストア中は、次の操作を実行しないでください。

- ・ ノードまたは Virtual Server 上で tapeadd コマンドを実行する。*
- ・ ノードまたは Virtual Server 上で、-A、-D、または -d オプションを指定して tapelist コマンドを実行する。*
- ・ バックアップ管理ソフトウェアで、テープ装置を管理する画面操作やコマンドを実行する。

注※

コマンドを実行したノードまたは Virtual Server でバックアップやリストアが処理中でない場合も、別のノードまたはノード上の Virtual Server で処理中のバックアップやリストアがエラー終了するおそれがあります。

5.2.10 File Services Manager から操作する場合の注意事項

File Services Manager からの次の操作と、Backup Restore の操作は同時に実行しないでください。

- ・ クラスタの起動または停止
- ・ クラスタの強制停止
- ・ クラスタ構成の定義の変更
- ・ ノードの起動または停止
- ・ ノードの強制停止
- ・ リソースグループの起動または停止
- ・ リソースグループの強制停止
- ・ リソースグループの監視の除外または再開
- ・ リソースグループの実行ノードの変更
- ・ 操作対象のファイルシステムのアンマウント

また、Virtual Server に対する次の操作と、操作対象の Virtual Server 上での Backup Restore の操作を同時に実行しないでください。

- Virtual Server の起動, 停止または再起動
- Virtual Server の強制停止
- Virtual Server の稼働ノードの変更

同時に実行した場合, File Services Manager からの操作または Backup Restore の操作がエラー終了するおそれがあります。

5.2.11 ノード上の OS を起動する場合の注意事項

ノードに SAN で接続されたテープ装置を使用し, ノード間でテープ装置を共有する場合, 一方のノードの OS が起動または再起動されると, もう一方のノードで実行されているバックアップおよびリストアがエラー終了するおそれがあります。バックアップおよびリストアを実行するときは, テープ装置を共有しているほかのノードの OS が起動または再起動されていないことを確認してください。

5.2.12 バックアップ管理ソフトウェアの機能制限

NDMP 機能では, バックアップ管理ソフトウェアの一部の機能を利用できません。バックアップ管理ソフトウェアで提供されている機能と NDMP 機能での利用可否を次の表に示します。

表 5-1 バックアップ管理ソフトウェアで提供されている機能と NDMP 機能での利用可否

機能		利用の可否
バックアップの実行	手動	○
	自動 (スケジュール)	○
バックアップの形式	フルバックアップ	○
	累積インクリメンタル	○※1
	差分インクリメンタル	○※1
バックアップ対象の指定※2	ボリューム	○
	ディレクトリ	○
	ファイル	○
	パスに基づいた履歴※3	○
DAR 機能		○
リストア先の指定	バックアップ対象と同じノード	○
	フェールオーバー先のノード	○
	代替クライアントへのリダイレクトリストア (別のクラスタのノード)	×

(凡例) ○ : 利用できる × : 利用できない

注

バックアップ管理ソフトウェアによって, 提供されている機能には差異があります。バックアップ管理ソフトウェアで提供されている機能の詳細については, 各バックアップ管理ソフトウェアのドキュメントを参照してください。

注※1

HVFP/HDI でのインクリメンタルバックアップは, 内容が変更されたディレクトリとファイルだけが対象になります。

注※2

バックアップまたはリストア時に指定する対象のディレクトリまたはファイルのパスの上限はバックアップ管理ソフトウェアによって異なります。詳細は、HVFP/HDI に添付されている Backup Restore の補足資料を参照してください。

注※3

バックアップ時に、バックアップしたディレクトリおよびファイルのパス名で構成されるファイルヒストリーを NDMP サーバからバックアップ管理ソフトウェアに送信する機能です。

ファイルヒストリーの情報によって、ディレクトリ単位またはファイル単位のリストアができます。

5.2.13 WORM 対応ファイルシステムのバックアップおよびリストアに関する注意事項

WORM 対応ファイルシステムのバックアップまたはリストアを実行する場合の注意事項を説明します。

(1) バックアップを実行する場合

WORM 対応ファイルシステムで自動コミットを有効にしている場合、設定した期間を経過しているにも関わらず、クライアントからのアクセスを受けていないファイルは WORM 化されていません。この状態のファイルをバックアップすると、WORM ファイルとしてバックアップされます。

WORM 対応ファイルシステムをバックアップ対象とする場合、NDMP 機能を使用したオフラインバックアップおよびオンラインバックアップだけを運用できます。

(2) リストアを実行する場合

WORM 対応ファイルシステムのバックアップデータは、バックアップ元のファイルシステムにリストアします。

リストア先のファイルシステムに同じパス名のファイルが存在する場合、ファイルの種類によってリストアできるかどうかが決まります。同じパス名のファイルが存在する場合のリストアの可否を次の表に示します。

表 5-2 同じパス名のファイルが存在する場合のリストアの可否

リストア先のファイルの種類	バックアップデータのファイルの種類	
	WORM 化されていないファイル	WORM ファイル
WORM 化されていないファイル	○	○
WORM ファイル	リテンション期間を経過している	△※1
	リテンション期間を経過していない	×

(凡例) ○：リストアできる △：一部リストアできる ×：リストアできない

注※1

リストア先のファイルに書き込み権限が設定されている場合にリストアできます。

注※2

次の条件をすべて満たす場合にリストアできます。

- リテンション期間、書き込み権限および読み取り専用属性の有無以外のデータが同じである

- 。 バックアップデータのファイルに設定されているリテンション期間が、リストア先のファイルの設定よりも長い

5.2.14 データ集約されているファイルシステムのバックアップ、リストアについて

データ集約による容量節約が有効なファイルシステムをバックアップ、リストアする場合、次の表に示すことに注意してください。なお、データ集約による容量節約が有効なファイルシステムをインクリメンタルバックアップした場合、バックアップ先にはデータ集約が解除された状態のデータが格納されます。

表 5-3 データ集約されたファイルシステムをバックアップ、リストアする場合の注意事項

注意事項	注意を守らなかった場合の動作
データ集約されたファイルシステムのデータをバックアップする場合は、オンラインバックアップを推奨します。 オフラインバックアップする場合は、バックアップ中に容量削減タスクが実行されないようにスケジュールを調整する必要があります。	オフラインバックアップの処理中に容量削減タスクが実行された場合、バックアップデータが不正となり、リストアが失敗することがあります。 バックアップ中にクライアントからのアクセスがあっても同様の問題が発生するため、オフラインバックアップする場合は NFS、CIFS、FTP、SFTP および TFTP サービスを停止してください。 スケジュールは、それぞれの処理に掛かる時間を考慮して、オフラインバックアップの実行日時、容量削減タスクの実行日時と打ち切り時間（容量削減ウィザードの [5. スケジュール] ページで指定する [打ち切り時間]）を適切に設定して調整してください。
データ集約されたファイルシステムのデータをバックアップする場合、バックアップ対象の基点となるディレクトリにはファイルシステムのマウントポイントを指定してください。	バックアップ対象の基点となるディレクトリにマウントポイントより下のディレクトリを指定してバックアップした場合、データ集約が解除された状態でバックアップメディアにデータが格納されるため、バックアップ先の容量不足でバックアップ処理が失敗することがあります。
データ集約されたファイルシステムのデータをリストアする場合、リストア先は新規ファイルシステムのマウントポイント直下としてください。	バックアップ元のファイルシステムにリストアした場合、リストア処理が失敗したり、リストア処理に長時間掛かったりすることがあります。 サブディレクトリにリストアすると、リストア処理が失敗したり、リストアした内容が不正になったりすることがあります。
データ集約されたファイルシステムのデータをリストアする場合、ファイルシステム単位でリストアしてください。	ファイル単位やディレクトリ単位でリストアをすると、リストア処理が失敗したり、リストアした内容が不正になったりすることがあります。
データ集約されたファイルシステムのデータをリストアする場合、リストア先のファイルシステムも内容が重複している複数のファイルのデータを集約する設定（容量節約が有効）になっている必要があります。	リストア処理が失敗します。

5.3 ファイルスナップショット機能の運用について

ここでは、ファイルスナップショット機能を運用するに当たって、システム管理者が知っておいた方がよいことについて説明します。

5.3.1 ファイルスナップショット機能の概要

スナップショットとは、ファイルシステムのデータを任意の時点の状態で複製したものです。ファイルスナップショット機能では、ファイルシステムのデータをそのまま別の領域に保存するのではなく、ファイルシステムが更新されるたびに、更新前のデータ（差分データ）だけを別の領域に退避し、差分データとファイルシステムのデータを使用することでスナップショットを実現します。このスナップショットを差分スナップショットと呼びます。また、差分データを退避させる領域を差分格納デバイスと呼びます。

システム管理者がクライアントに差分スナップショットを公開しておけば、クライアントはシステム管理者を介さずに差分スナップショットのデータを参照できます。このため、ディレクトリやファイルを誤って削除してしまった場合でも、クライアントが差分スナップショットのデータをファイルシステムにコピーすることでデータを回復できます。

なお、ファイルスナップショット機能はファイルシステムレベルでスナップショットを採取するものであり、アプリケーションとの同期を取りません。そのため、クライアントがファイルシステム上のデータをアプリケーションで使用している状態で作成した差分スナップショットについてのアプリケーションレベルでの整合性は保証されません。

5.3.2 ファイルスナップショット機能を運用するための前提条件

ファイルスナップショット機能の各操作を実行するには、クラスタ、ノード、リソースグループおよび Virtual Server の状態が次の条件を満たしている必要があります。

ノード上で実行する場合

- ・ クラスタおよび操作を実行するノードが正常に稼働している
- ・ 操作を実行するノード上で、操作対象のリソースグループが正常に稼働している

Virtual Server 上で実行する場合

- ・ 操作を実行する Virtual Server が正常に稼働している

上記の条件を満たしていない場合、ファイルスナップショット機能の操作がエラー終了するおそれがあります。

5.3.3 ファイルシステムと差分格納デバイスの管理

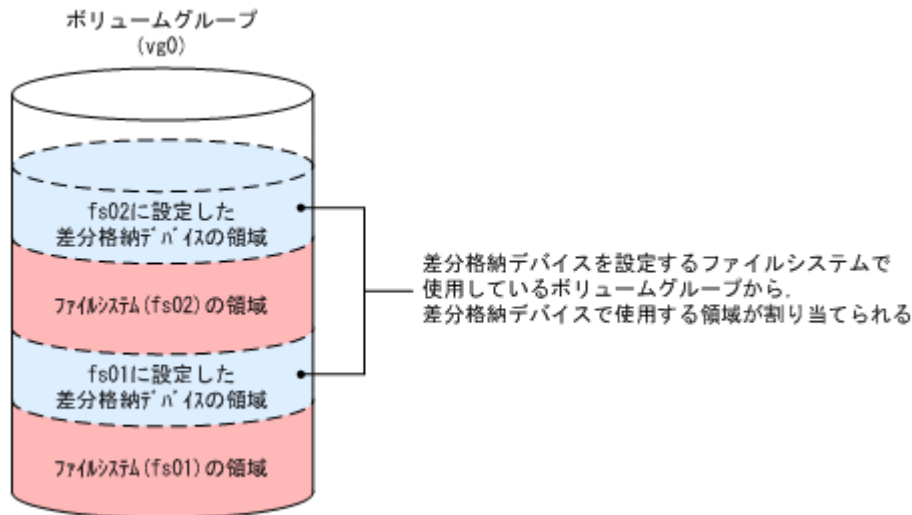
差分格納デバイスは、1つのファイルシステムに対して1つだけ設定できます。差分格納デバイスを設定するファイルシステムは、次の条件を満たしている必要があります。

- ・ ボリュームマネージャー（LVM）を使用して作成されている
- ・ 差分格納デバイスが設定されていない
- ・ 差分スナップショットでない

クラスタ構成の場合は、差分格納デバイスに使用するための、未使用のデバイスファイルを準備してください。差分格納デバイスに使用するデバイスファイルは複数指定できます。

シングルノード構成の場合は、差分格納デバイスを設定するファイルシステムで使用しているボリュームグループを、差分格納デバイスにも使用します。

図 5-4 シングルノード構成の場合の差分格納デバイス



ファイルシステムと差分格納デバイスを管理する際に知っておいた方がよいことについて説明します。

(1) ファイルシステムおよび差分格納デバイス容量の拡張について

ファイルシステムおよび差分格納デバイス容量の拡張上限は、チャンクサイズ、および差分スナップショットの最大予約世代数によって異なります。チャンクサイズは、差分データを退避する単位です。差分スナップショットの最大予約世代数は、拡張できる予約世代数（作成する差分スナップショットの最大数）の上限です。チャンクサイズおよび最大予約世代数は、差分格納デバイスを設定するときに指定します。

チャンクサイズ、および差分スナップショットの最大予約世代数と、ファイルシステムおよび差分格納デバイス容量の拡張上限の関係について、表 5-4 チャンクサイズによるファイルシステムおよび差分格納デバイス容量の拡張上限に示します。

表 5-4 チャンクサイズによるファイルシステムおよび差分格納デバイス容量の拡張上限

チャンクサイズ (KB)	ファイルシステムおよび差分格納デバイス容量の拡張上限			
	最大予約世代数が 124 の場合	最大予約世代数が 248 の場合	最大予約世代数が 496 の場合	最大予約世代数が 992 の場合
64	16TB	-	-	-
128	32TB	16TB	-	-
256	64TB	32TB	16TB	-
512	128TB	64TB	32TB	16TB
1,024	256TB	128TB	64TB	32TB
2,048	512TB	256TB	128TB	64TB
4,096	1PB	512TB	256TB	128TB
8,192	1PB	1PB	512TB	256TB
16,384	1PB	1PB	1PB	512TB
32,768	1PB	1PB	1PB	1PB

(凡例) - : 拡張できない

1TB を超えるサイズにファイルシステムを拡張する場合、inode 領域が再構成されます。このため、ファイルスナップショット機能を使用しているファイルシステムでは、約 10GB の差分データが発生します。

ファイルスナップショット機能を使用しているファイルシステムを拡張するには、差分格納デバイスの空き容量が十分に確保されている必要があります。ファイルシステムを拡張するために必要な空き容量については、「5.7 ファイルスナップショット機能で運用しているファイルシステムの拡張」を参照してください。

(2) 差分格納デバイスに使用するデバイスファイルについて

クラスタ構成の場合、差分格納デバイスに使用するデバイスファイルを決定するときは、デバイスファイルのドライブ種別を考慮する必要があります。SATA ドライブおよび SAS 7.2K ドライブは、FC ドライブ、SAS ドライブおよび SSD とは I/O 性能や処理速度が異なります。このため、差分格納デバイスには、設定元のファイルシステムと同じドライブ種別のデバイスファイルを使用することをお勧めします。

Virtual Storage Platform、Universal Storage Platform V/VM または HUS VM で差分格納デバイスに外部ストレージシステムのデバイスファイルを使用する場合は、次の点に注意してください。

- ・ 外部ストレージシステムが起動していない状態でノードの OS を起動する、自筐体と外部ストレージシステムを接続するケーブルが外れるなど、運用ミスによってデバイスファイルに障害が発生する可能性が、自筐体を使用する場合に比べて高くなります。
- ・ 外部ストレージシステムのデバイスファイルを使用した場合、自筐体のデバイスファイルを使用する場合に比べて、I/O 性能が劣化したり、処理速度が低下したりします。
- ・ 設定元のファイルシステムと同じストレージシステムのデバイスファイルを必ず使用してください。異なるストレージシステムのデバイスファイルを使用した場合、ファイルシステムまたは差分格納デバイスを構成するデバイスファイルの 1 つで障害が発生したときに、すべての差分スナップショットが失われるおそれがあります。差分格納デバイスを設定・拡張する前に、Storage Navigator を使用して、デバイスファイルが実在するストレージシステムを確認してください。
- ・ 差分格納デバイスに仮想 LU を使用する場合は、仮想 LU が属するプールの容量が不足しないように運用する必要があります。

差分格納デバイスに仮想 LU を使用すると、プールの容量が不足した場合に、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無効になります。

また、ファイルシステムおよび差分格納デバイスに仮想 LU を使用していて、両方のプールで容量不足が同時に発生した場合、差分スナップショットが無効になり、ファイルシステムは閉塞します。このとき自動フェールオーバー機能を設定していると、フェールオーバーが発生したあとに両方のノードが停止するおそれがあります。ファイルシステムおよび差分格納デバイスの両方に仮想 LU を使用する場合は、プールの容量不足が同時に発生しないようプールを別々にするか、自動フェールオーバー機能の設定を解除することを推奨します。

(3) 差分格納デバイスの容量の見積もりについて

差分スナップショットの運用中に差分格納デバイスの容量が不足した場合、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すべて無効になったり、ファイルシステムでのサービスが一時的に停止したりします。

システム管理者は、差分スナップショットの運用を開始する前に、差分格納デバイスに十分な容量を割り当ててください。差分格納デバイスに必要な容量は、差分格納デバイスを設定するファイルシステムの容量やデータ更新量、作成する差分スナップショットの数などによって算出できます。ファイルシステムの容量を拡張した場合や、運用方法が変更になった場合は、差分格納デバイスの容量を見積もり直す必要があります。差分格納デバイスに必要な容量の算出方法については、「5.5 差分格納デバイスの容量の設計」を参照してください。

(4) 差分格納デバイスの使用量に関する設定について

差分格納デバイスに十分な容量を見積もって設定しても、見積もり以上の更新が発生するなどの理由で、差分格納デバイスの空き容量が少なくなることがあります。差分格納デバイスの使用量に関する設定を実施することで、差分スナップショットの運用中に差分格納デバイスの容量が不足するおそれを軽減できます。また、差分格納デバイスの容量が不足した場合の動作を選択できます。

差分格納デバイスの使用量に関する設定を実施すると、差分格納デバイスの空き容量が少なくなった場合に、システムメッセージ、SNMP トラップまたは E-mail で通知したり、自動的に差分格納デバイスの空き容量を確保する処理を実行したりできます。また、差分格納デバイスの容量が不足した場合に、ファイルシステムでのサービス提供を継続するか、サービスを停止する代わりに差分スナップショットのデータを保護するかを選択できます。

システム管理者は、ファイルシステムの用途や運用方法を考慮して、設定を検討してください。各設定の詳細については、「5.6 差分格納デバイスの使用量に関する設定」を参照してください。

差分スナップショットの運用を開始したら、システムメッセージ、SNMP トラップまたは E-mail 通知を定期的に参照して、差分格納デバイスの状態を確認してください。差分格納デバイスの容量が不足しそうな場合は、不要な差分スナップショットを削除したり、差分格納デバイスを拡張したりして対処してください。

(5) ファイルシステムへのデータ書き込みについて

ファイルスナップショット機能を使用しているファイルシステムに対して、差分格納デバイスの空き容量を上回るデータの書き込み要求があった場合、差分格納デバイスの容量が不足するおそれがあります。

ファイルスナップショット機能を使用しているファイルシステムに対してリストアを行うときは、一度、差分格納デバイスの設定を解除してください。ファイルスナップショット機能を使用しているファイルシステムに対してリストア操作を行うと、差分格納デバイスへの大量の書き込みが発生して、差分格納デバイスの容量が不足するおそれがあります。その結果、ファイルスナップショット機能の運用が停止したり、ファイルシステムが一時的に使用できなくなったりするおそれがあります。

(6) CIFS サービスの構成定義について

CIFS クライアントからのアクセスが多いファイルシステムで、ファイルスナップショット機能を使用する場合は、事前に CIFS サービスの構成定義の設定を確認してください。

CIFS クライアントからの書き込み要求に対して、一定周期で CIFS 共有フォルダに書き込むよう設定していると、クライアントからのアクセスがタイムアウトしたり、フェールオーバーが失敗したりすることがあります。このため、クローズ要求に同期して CIFS 共有フォルダに書き込むよう設定することをお勧めします。

(7) 仮想 LU の未使用領域の解放について

ファイルスナップショット機能を使用しているファイルシステムでは、差分スナップショットを保持するために、ファイルシステムおよび差分格納デバイスで使用している仮想 LU の未使用領域が使用されます。このため、dpreclaim コマンドを実行しても、仮想 LU の未使用領域を効果的に解放できないことがあります。差分格納デバイスで使用している仮想 LU の未使用領域を解放する場合は、差分スナップショットを削除したり、自動作成の上限数を変更したりして、差分格納デバイスの使用量が減少したときに dpreclaim コマンドを実行してください。

5.3.4 差分スナップショットの管理

差分スナップショットを管理する際に知っておいた方がよいことについて説明します。

(1) 差分スナップショットの予約世代数について

予約世代数は、作成する差分スナップショットの最大数です。予約世代数は、差分格納デバイスを設定したあとに拡張できます。

最大予約世代数は、拡張できる予約世代数の上限であり、指定されている差分スナップショットの予約世代数によって自動的に設定されます。自動的に設定された値よりも大きい最大予約世代数を設定したい場合は、syncstart コマンドを使用してください。

注意：

差分スナップショットの予約世代数には、次の条件式を満たす値を設定してください。

Virtual Server を使用していない場合：

クラスタ内の各ファイルシステムに設定している 予約世代数の合計	≤ 4000
------------------------------------	-------------

Virtual Server を使用している場合：

すべてのVirtual Serverの各ファイルシステムに 設定している予約世代数の合計	≤ 1000
---	-------------

スケジュールを設定して差分スナップショットを自動作成する場合、自動作成の上限数を設定します。自動作成の上限数は、ファイルシステム全体で管理するか、差分スナップショットの自動作成スケジュールの作成間隔ごとに管理するかを選択します。

差分スナップショットの用途や運用方法を考慮して、確保するそれぞれの差分スナップショット数を調整してください。

なお、作成済みの差分スナップショットの世代数は、次に示す差分スナップショットの合計となります。

- ・ 手動で作成した差分スナップショット（作成と削除の同時実行で作成したものを含む）
- ・ スケジュールを設定して自動作成した差分スナップショット
- ・ Backup Restore のオンラインバックアップ機能と連携して作成された差分スナップショット（最大1つ）

(2) 確保できる差分スナップショットの数について

手動で作成する場合は、差分格納デバイスに指定した予約世代数まで差分スナップショットを確保できます。

自動作成する場合は、予約世代数、スケジュールが実行された時点での差分スナップショットの数およびスケジュールを設定する際に指定する自動作成の上限数（または作成間隔ごとに指定する上限数の総和）によって、作成・確保できる差分スナップショットの数が次のとおり異なります。

作成・確保できる差分スナップショットの数

$$G \geq A + B + C$$

$$\text{自動作成して確保できる差分スナップショットの数} = A$$

$$G < A + B + C$$

$$\text{自動作成して確保できる差分スナップショットの数} = G - B - C$$

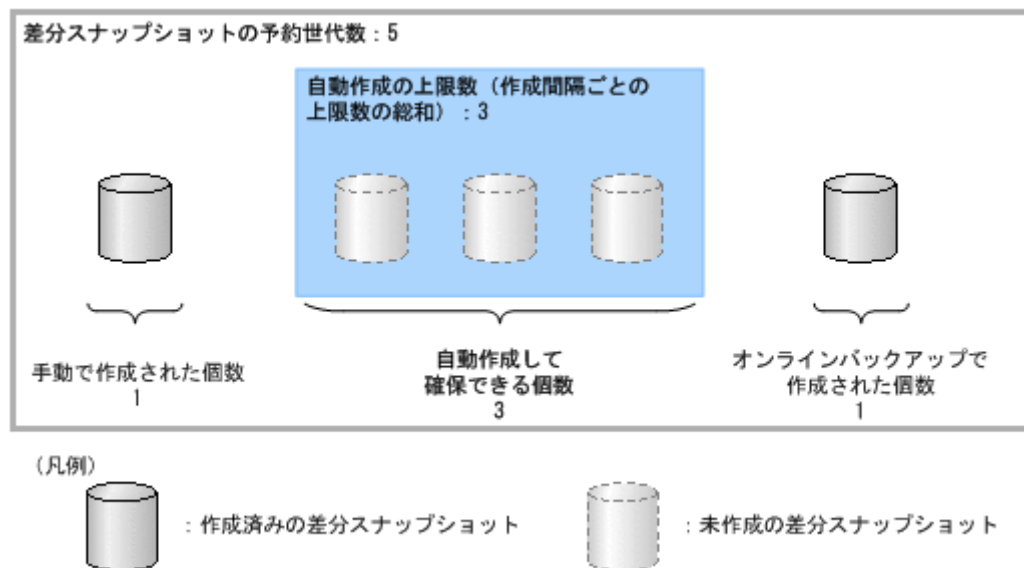
(凡例)

- G : 予約世代数
- A : 自動作成の上限数（作成間隔ごとに管理する場合は、作成間隔ごとの上限数の総和）
- B : 手動で作成された差分スナップショットの個数
- C : オンラインバックアップで作成された差分スナップショットの個数

ここでは、予約世代数を「5」とし、自動作成の上限数を「3」と設定した場合を例に説明します。

自動作成の上限数まで作成・確保できる場合の予約世代数の内訳を次の図に示します。

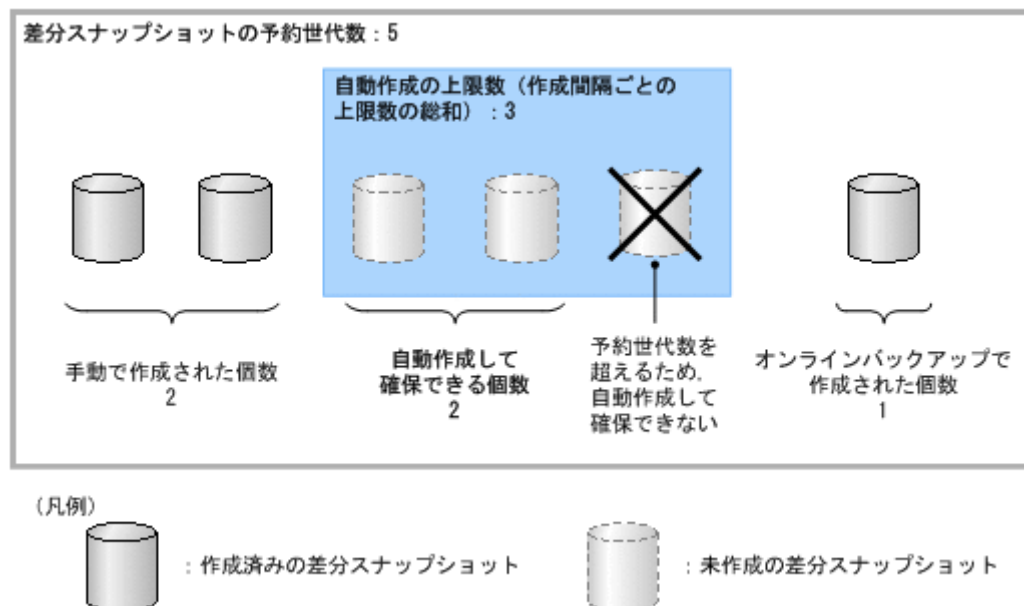
図 5-5 自動作成の上限数まで作成・確保できる場合の予約世代数の内訳



手動で作成された差分スナップショットが1個、オンラインバックアップ機能で作成された差分スナップショットが1個存在する状態では、自動作成して確保できる差分スナップショットの数は上限数と同じ3個です。

自動作成の上限数まで作成・確保できない場合の予約世代数の内訳を次の図に示します。

図 5-6 自動作成の上限数まで作成・確保できない場合の予約世代数の内訳



手動で作成された差分スナップショットが2個、オンラインバックアップ機能で作成された差分スナップショットが1個存在する状態では、上限数に「3」を設定していても、実際に自動作成して確保できる差分スナップショット数は2個になります。

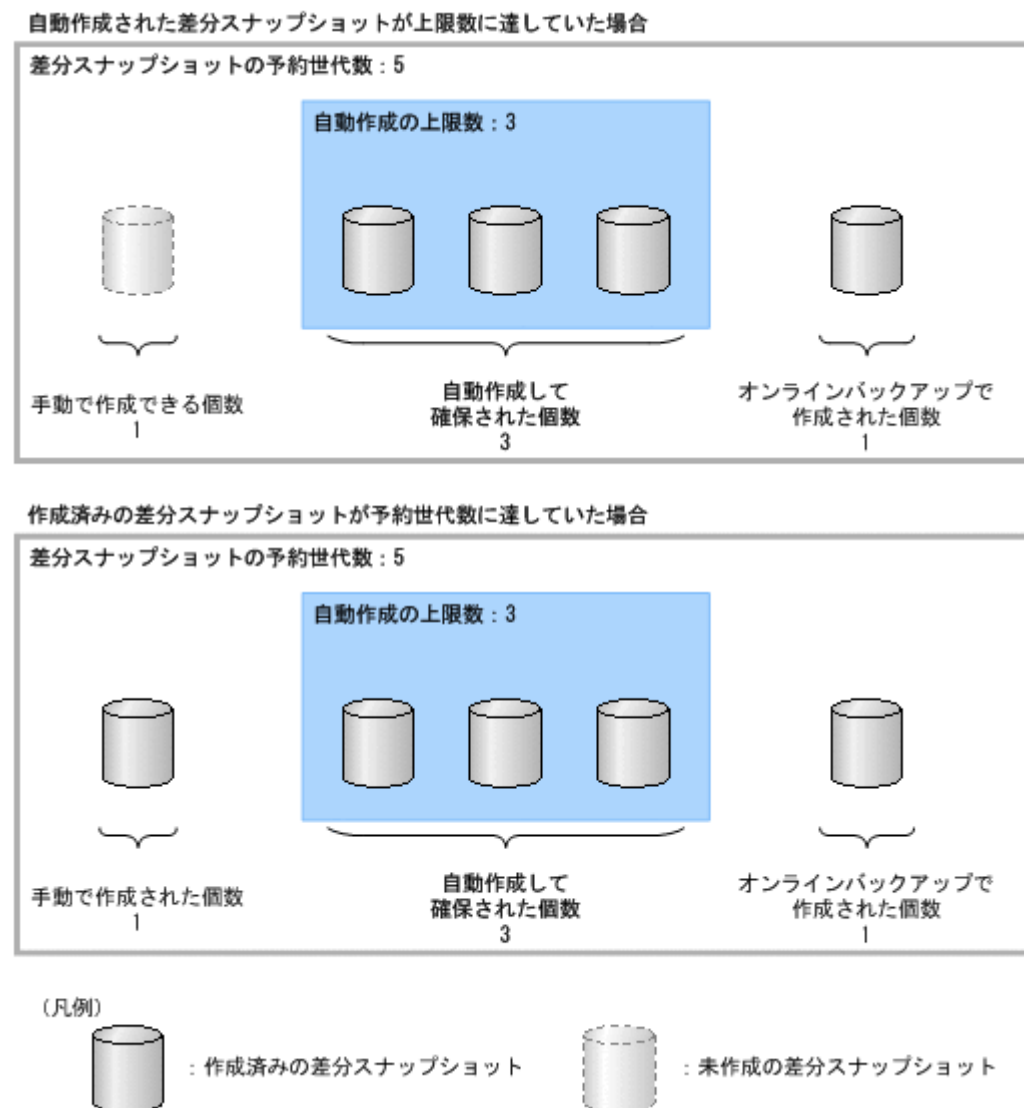
また、スケジュールが実行された際に、自動作成された差分スナップショットが上限数に達していた場合、または作成済みの差分スナップショットの合計数が予約世代数に達していた場合は、自動

作成された差分スナップショットのうち、いちばん古いものが削除され、その上で新しい差分スナップショットが作成されます。

この場合に削除される差分スナップショットは、自動作成の上限数をファイルシステム全体でまとめて管理するように設定しているか、差分スナップショットの自動作成スケジュールの作成間隔ごとに管理するように設定しているかによって異なります。

自動作成の上限数をファイルシステム全体で管理する場合の例を次に示します。

図 5-7 自動作成された差分スナップショットが削除される条件（上限数をファイルシステム全体で管理する場合）



自動作成の上限数をファイルシステム全体で管理する場合、自動作成された差分スナップショットが上限数に達していたとき、または作成済みの差分スナップショットの合計数が予約世代数に達していたときは、ファイルシステムに対して自動作成されたすべての差分スナップショットの中で、作成日付が最も古いものが削除されます。

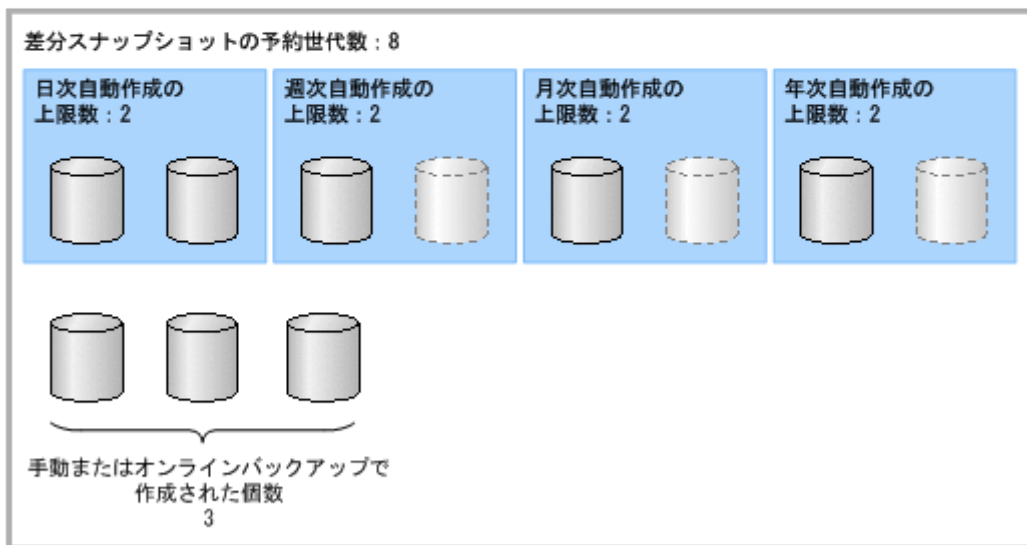
自動作成の上限数を作成間隔ごとに管理する場合の例を次に示します。

図 5-8 自動作成された差分スナップショットが削除される条件（上限数を作成間隔ごとに管理する場合）

自動作成された差分スナップショットのうち、作成間隔ごとの上限数に達しているものがある場合
 (例1)



作成済みの差分スナップショットが予約世代数に達していた場合
 (例2)



(凡例)



：作成済みの差分スナップショット



：未作成の差分スナップショット

自動作成の上限数を作成間隔ごとに管理する場合、実行される自動作成スケジュールの作成間隔ごとに、上限数に達しているかどうか判定されます。図 5-8 自動作成された差分スナップショットが削除される条件（上限数を作成間隔ごとに管理する場合）の例 1 では、日次の自動作成スケジュールが実行された際、日次で自動作成された差分スナップショットのうち、作成日付が最も古いものが削除されます。週次、月次または年次の自動作成スケジュールが実行されたときは、差分スナップショットは削除されず、新たな差分スナップショットが作成されます。

また、図 5-8 自動作成された差分スナップショットが削除される条件（上限数を作成間隔ごとに管理する場合）の例 2 のように作成済みの差分スナップショットが予約世代数に達していたときは、実行される自動作成スケジュールの作成間隔（日次、週次、月次または年次）と同じ作成間隔で作成された差分スナップショットのうち、作成日付が最も古いものが削除されます。

なお、差分スナップショットの運用中に、自動作成された差分スナップショットの総数よりも小さな値に上限数を変更した場合でも、変更前に自動作成された差分スナップショットは削除されません。システム管理者が自動作成された差分スナップショットを削除し、自動作成された差分スナップショットの総数が新たに指定した上限数以下になった時点から、新たな上限数での運用が開始されます。

(3) 差分スナップショットの作成・削除に掛かる時間について

差分スナップショットを作成または削除すると、バックグラウンドで処理が実行されます。バックグラウンド処理が実行されているファイルシステムでは、差分スナップショットを新たに作成・削除できません。

なお、ファイルスナップショット機能を使用しているファイルシステムでは、次の契機でもバックグラウンド処理が実行されます。

- ・ フェールオーバーが発生したとき
- ・ リソースグループを起動したとき
- ・ Virtual Server を起動または再起動したとき
- ・ Backup Restore の horcvmimport コマンドを実行したとき

バックグラウンド処理に掛かる時間は、ファイルシステムの容量、および最大予約世代数に比例して長くなり、チャンクサイズに反比例します。チャンクサイズを大きくすると、バックグラウンド処理に掛かる時間は短くなりますが、ファイルシステムの容量に対して大きくし過ぎると、ファイルシステムの更新量と比べて差分格納デバイスの使用容量が多くなる場合があります。バックグラウンド処理に掛かる時間を考慮した上で、チャンクサイズを小さくして、差分格納デバイスの使用容量が少なくなるようにしてください。差分格納デバイスを設定したあとでチャンクサイズを変更することはできませんので注意してください。

バックグラウンド処理に掛かる時間は、使用するストレージシステムによって異なります。システムの負荷が低く、I/O の競合がない状態の場合に、バックグラウンド処理に掛かる時間の目安を次に示します。なお、ここでは最大予約世代数が 124 の場合の時間の目安を示します。ここで示す時間に対して、最大予約世代数が 248 の場合は 2 倍、496 の場合は 4 倍、992 の場合は 8 倍の時間が目安となります。

表 5-5 バックグラウンド処理に掛かる時間の目安（システム負荷が低く、I/O 競合がない状態の場合）

ファイルシステムの容量	チャンクサイズごとのバックグラウンド処理に掛かる時間の目安（秒）									
	64KB の場合	128KB の場合	256KB の場合	512KB の場合	1MB の場合	2MB の場合	4MB の場合	8MB の場合	16MB の場合	32MB の場合
5TB	1,400	700	350	175	88	44	22	11	6	3
10TB	2,800	1,400	700	350	176	88	44	22	12	6
20TB	-	2,800	1,400	700	352	176	88	44	24	12

(凡例) - : 設定できないチャンクサイズなので目安はない

バックグラウンド処理に掛かる時間は、ファイルシステムへの I/O 量およびシステムの負荷によって変わります。差分スナップショットを自動的に作成する場合は、次のことに注意して、処理に掛かる時間よりも作成間隔が長くなるようにしてください。

- ・ ファイルシステムへの I/O が発生する時間帯に差分スナップショットを作成する場合は、目安時間の 10 倍以上の間隔を空けてください。
- ・ HFRR コピー用として 15 分ごとに自動作成された差分スナップショットをコピー対象とする場合は、バックグラウンド処理が 15 分以内に完了するように、ファイルシステムサイズ、チャンクサイズおよび最大予約世代数を設定してください。
- ・ システムの負荷が低い時間に差分スナップショットを作成してください。
- ・ 同じ時間帯に、複数のファイルシステムに対して、差分スナップショットの作成・削除を実行しないでください。

(4) 差分スナップショットの更新時刻・参照時刻について

差分スナップショットをマウントおよびファイル共有した場合や、クライアントがファイル共有された差分スナップショットを参照した場合でも、差分スナップショットの更新時刻や参照時刻は作成された時刻から変更されません。

5.3.5 同時に実行できない操作

GUI または コマンドを使用した次の操作とファイルスナップショット機能の操作を同時に実行しないでください。

- ・ クラスタの起動・停止
- ・ クラスタの強制停止
- ・ クラスタ構成の定義の変更
- ・ ノードの起動・停止
- ・ ノードの強制停止
- ・ リソースグループの起動・停止
- ・ リソースグループの強制停止
- ・ リソースグループの監視の除外・再開
- ・ リソースグループの実行ノードの変更
- ・ 操作対象のファイルシステムのマウント・アンマウント

また、Virtual Server に対する次の操作と、操作対象の Virtual Server 上でのファイルスナップショット機能の操作を同時に実行しないでください。

- ・ Virtual Server の起動・停止・再起動
- ・ Virtual Server の強制停止
- ・ Virtual Server の稼働ノードの変更

同時に実行した場合、GUI または コマンドでの操作や、ファイルスナップショット機能の操作がエラー終了するおそれがあります。

5.3.6 ファイルスナップショット機能の注意事項

ファイルスナップショット機能を運用する上での注意事項を説明します。

(1) Backup Restore のボリュームレプリケーション連携機能を運用する場合の注意事項

Backup Restore のボリュームレプリケーション連携機能で運用されているファイルシステムに対して、ファイルスナップショット機能の次の操作を実行した場合は、操作後にペアを再構成する必要があります。

- ・ 差分格納デバイスの設定
- ・ 差分格納デバイスの拡張
- ・ 差分格納デバイスの解除

ファイルシステムを構成する LU だけでなく、差分格納デバイスを構成する LU でも、必ずペアを構成してください。

ボリュームレプリケーション連携機能の運用方法の詳細については、「エンタープライズアレイ機能連携ユーザズガイド」または「ミッドレンジアレイ機能連携ユーザズガイド」を参照してください。

(2) Hitachi File Remote Replicator を運用する場合の注意事項

Hitachi File Remote Replicator を運用する場合は、Hitachi File Remote Replicator での運用および制限を考慮して、ファイルスナップショット機能の運用設計および操作を行う必要があります。Hitachi File Remote Replicator については、「5.9 Hitachi File Remote Replicator について」を参照してください。

(3) HCP と連携する場合の注意事項

HCP にデータがマイグレートされるよう設定しているファイルシステムに対して、ファイルスナップショット機能を使用する場合は、次の点に注意してください。

- ・ 差分スナップショット内のスタブファイルには、アクセスできません。
クライアントに差分スナップショットのデータを公開する場合、コマンドでファイルスナップショットを設定するときは、`arcimplimitset` コマンドでスタブ化開始の閾値を `0GB` に設定して、対象のファイルシステム内にスタブファイルが作成されないようにしてください。GUI でファイルスナップショットを設定するときは、スタブ化開始の閾値が自動で `0GB` に設定されます。
なお、ファイルスナップショットの設定を解除し、対象のファイルシステム内のファイルをスタブ化する場合は、`arcimplimitset` コマンドでスタブ化開始の閾値を再設定する必要があります。
- ・ クライアントからのアクセスによって HCP にマイグレートされたデータが HVFP/HDI にリコールされると、ファイルシステムに対して更新要求が発生するため、差分データが差分格納デバイスに退避されます。HCP にデータがマイグレートされるファイルシステムに設定する差分格納デバイスの容量の算出方法については、「5.5 差分格納デバイスの容量の設計」を参照してください。

(4) シングルノード構成で運用する場合の注意事項

内蔵ディスクに障害が発生した場合、内蔵ディスクにある差分スナップショットは復元できません。

5.4 差分スナップショットの運用例

ここでは、差分スナップショットを業務でどのように運用していくかを、例を交えて紹介します。運用例を参考にして、差分スナップショットを運用してください。差分スナップショットの運用方法の検討と設定については、運用している構成に対応する例を参照してください。

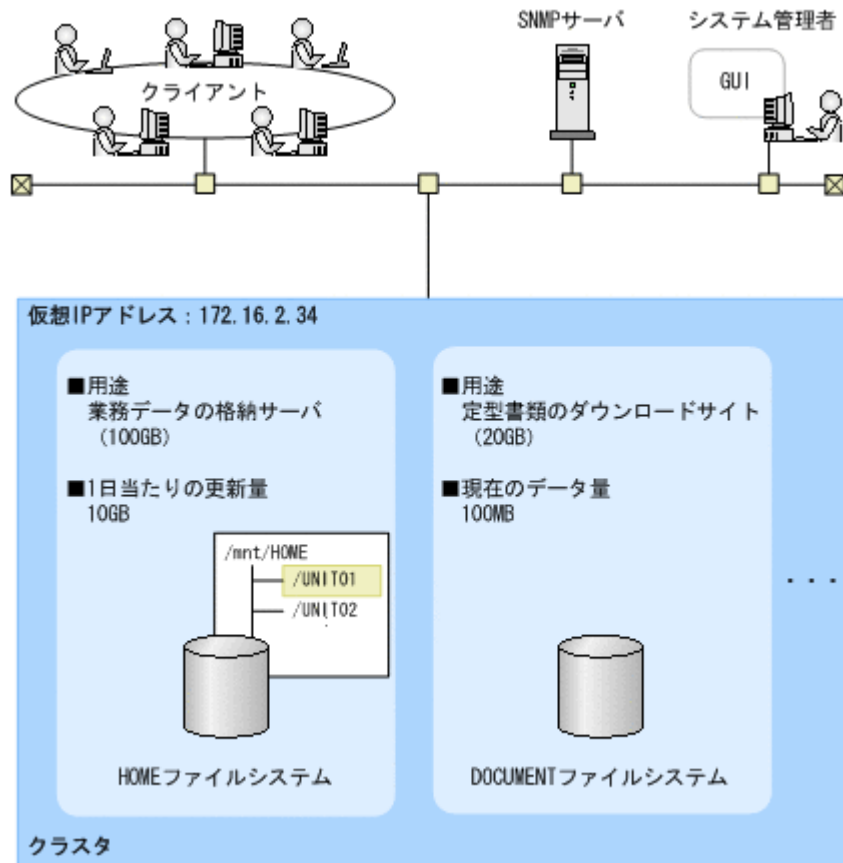
5.4.1 差分スナップショットの運用方法の検討と設定（クラスタ構成の場合）

ここでは、クラスタ構成で差分スナップショットを運用する場合の検討項目、および検討結果に基づいて運用するための設定内容について説明します。

(1) 想定するシステム構成

クラスタ構成の場合の運用例では、次のシステム構成を想定して説明します。

図 5-9 想定するシステム構成

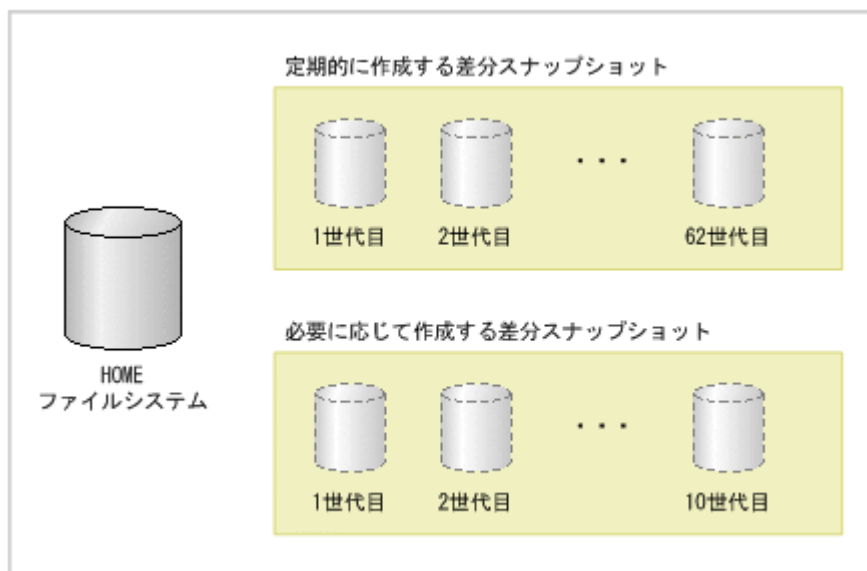


- 仮想 IP アドレスには「172.16.2.34」が設定されている
- クラスタ内にあるファイルシステムのうち、HOME ファイルシステムと DOCUMENT ファイルシステムをファイルスナップショット機能で運用する
- HOME ファイルシステムと DOCUMENT ファイルシステムのデータは、HCP にマイグレートされない
- HOME ファイルシステム（容量：100GB）は業務データの格納サーバとして使用されており、1日当たり平均 10GB のデータ更新が発生している
- HOME ファイルシステムでは、/mnt/HOME/UNIT01 ディレクトリに NFS 共有および CIFS 共有を作成している
- DOCUMENT ファイルシステム（容量：20GB）は申請書や報告書などの定型書類のダウンロードサイトとして使用されており、現在、合計 100MB のデータが格納されている
- HOME ファイルシステム、DOCUMENT ファイルシステムともに、差分格納デバイスを構成するデバイスファイルの数は 1 つである
- 障害情報を SNMP トラップまたは E-mail で通知するように設定している

(2) HOME ファイルシステムでの差分スナップショットの運用

HOME ファイルシステムでは、1 時間当たり平均 427MB の少量のデータ更新が発生すると仮定します。このことを踏まえ、HOME ファイルシステムでは、1 日 2 回、差分スナップショットを定期的に作成し、1 か月間（62 世代）確保する計画を立てます。また、ハードウェアの定期メンテナンス時やユーザーから要求を受けた際に作成する分として、定期的に作成する 62 世代以外に、10 世代を作成・確保できるように予約世代数を設定すると仮定します。

図 5-10 差分スナップショットの運用例 (HOME ファイルシステム)



また、差分格納デバイスの使用量については、次のとおり設定する例とします。

- ・ 差分格納デバイスの使用量が総容量の 75%に達すると、システム管理者にメッセージが通知されるように警告閾値を設定する
- ・ 差分格納デバイスの容量不足を防止する動作を設定しない
- ・ 差分格納デバイスの容量が不足した場合、ファイルシステムの使用を制限し、差分スナップショットのデータを保護するよう設定する

表 5-6 差分格納デバイスの設定内容 (クラスタ構成時の HOME ファイルシステム)

項目	設定内容
予約世代数	72 世代 (62 世代 + 10 世代)
警告閾値	75%
あふれ防止動作	なし
あふれ時の動作	ファイルシステムの使用を制限
チャンクサイズ※1	1,024KB
差分格納デバイスに必要な容量※2	370.1GB

注※1

システムのデフォルト値を使用します。デフォルト値については、表 5-10 デフォルトのチャンクサイズを参照してください。

注※2

差分格納デバイスの容量の見積もり方法については、「5.5 差分格納デバイスの容量の設計」を参照してください。

定期的作成する差分スナップショットは、GUI でスケジュールを設定して自動的に作成します。スケジュールを設定する際には、作成間隔に加えて、マウントポイント名に付与する識別子、マウント数の上限および公開方法を指定します。

ここでは、次のとおり設定する例とします。

- ・ 作成間隔は毎日とし、業務への影響が比較的少ない時間帯を考慮して、作成時刻には 3 : 00 と 17 : 30 を設定する

- ・ クラスタ内に存在する別のファイルシステムや差分スナップショットの運用も考慮し、新しいものから1週間分(14世代)が自動的にマウントおよび公開されるように設定する
- ・ HOME ファイルシステムの差分スナップショットであることを判別できるように、マウントポイント名の識別子には「HOME」を設定する
- ・ 公開方法については、ファイルシステムの共有内に公開するように設定する

表 5-7 自動作成スケジュールの設定内容 (クラスタ構成時の HOME ファイルシステム)

項目	設定内容
上限数の管理方法	ファイルシステム全体で管理する
自動作成の上限数	62 世代
作成日時	<ul style="list-style-type: none"> ・ 毎日 3 : 00 ・ 毎日 17 : 30
自動マウントの上限数	14 世代
識別子	HOME
公開方法	ファイルシステムの共有内に公開する

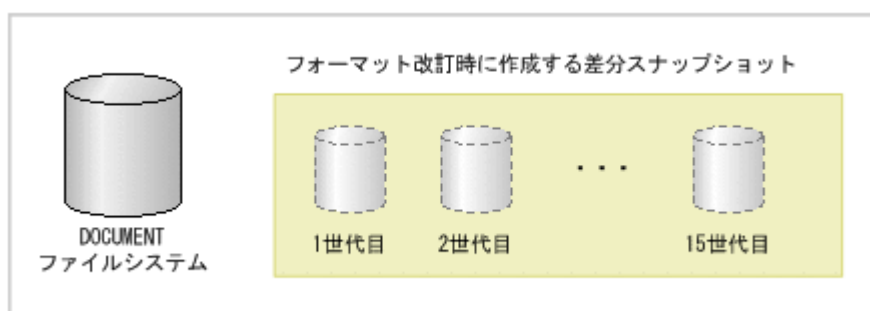
表 5-6 差分格納デバイスの設定内容 (クラスタ構成時の HOME ファイルシステム) および表 5-7 自動作成スケジュールの設定内容 (クラスタ構成時の HOME ファイルシステム) の内容を、[File Snapshots 設定] ダイアログの [ベーシック], [設定] および [スケジュール] タブで設定します。

自動作成された差分スナップショットの名称およびマウントポイントについては、「5.8 差分スナップショットの自動作成の運用」を参照してください。

(3) DOCUMENT ファイルシステムでの差分スナップショットの運用

DOCUMENT ファイルシステムは、各種書類の定型フォーマットが格納されていると仮定します。クライアントの主な利用方法はデータの参照 (ダウンロード) です。規則などの変更に伴い定型書類を改訂しなければならない場合には、業務担当者がデータを更新します。このため、定型書類を改訂する前後に、クライアントからの要求に応じて、システム管理者が手動で差分スナップショットを作成する運用にします。定型書類の改訂は月 1 回程度あると想定し、過去 1 年分を保管できるように、予約世代数には 15 世代を設定すると仮定します。

図 5-11 差分スナップショットの運用例 (DOCUMENT ファイルシステム)



また、差分格納デバイスの使用量については、次のとおり設定する例とします。

- ・ 差分格納デバイスの使用量が総容量の 80%に達すると、システム管理者にメッセージが通知されるように警告閾値を設定する
- ・ 差分格納デバイスの容量不足を防止する動作を設定しない
- ・ 差分格納デバイスの容量が不足した場合、ファイルシステムの使用を制限し、差分スナップショットのデータを保護するよう設定する

表 5-8 差分格納デバイスの設定内容 (DOCUMENT ファイルシステム)

項目	設定内容
予約世代数	15 世代
警告閾値	80%
あふれ防止動作	なし
あふれ時の動作	ファイルシステムの使用を制限
チャンクサイズ※1	1,024KB
差分格納デバイスに必要な容量※2	3.6GB

注※1

システムのデフォルト値を使用します。デフォルト値については、表 5-10 デフォルトのチャンクサイズを参照してください。

注※2

差分格納デバイスの容量の見積もり方法については、「5.5 差分格納デバイスの容量の設計」を参照してください。

表 5-8 差分格納デバイスの設定内容 (DOCUMENT ファイルシステム) の内容を、[File Snapshots 設定] ダイアログの [ベーシック] タブおよび [設定] タブで設定します。

5.4.2 差分スナップショットの運用方法の検討と設定 (シングルノード構成の場合)

シングルノード構成の場合、GUI を使用すると、システムの推奨値に基づいて差分スナップショットの運用を開始できます。差分格納デバイスの容量、差分スナップショットを自動的に作成するときの間隔と識別子については、差分スナップショットの運用方法を検討し、検討結果に基づいて設定してください。コマンドを使用するときは、差分スナップショットの運用方法を検討し、検討結果に基づいて、GUI より詳細に差分スナップショットを設定できます。

ここでは、GUI で差分スナップショットの運用を開始することを想定して、差分スナップショットを運用するときの検討項目、および検討結果に基づいて運用するための設定内容について説明します。

(1) 想定するシステム構成

シングルノード構成の場合の運用例では、次のシステム構成を想定して説明します。

- HOME ファイルシステムをファイルスナップショット機能で運用する
- HOME ファイルシステムのデータは、HCP にマイグレートされない
- HOME ファイルシステム (容量: 100GB) は業務データの格納サーバとして使用されており、1 日当たり平均 10GB のデータ更新が発生している

(2) HOME ファイルシステムでの差分スナップショットの運用と設定

差分格納デバイスの容量、差分スナップショットを自動的に作成する間隔、自動的に作成した差分スナップショットをマウントおよび公開するときの識別子を検討します。

HOME ファイルシステムでは、1 日 2 回、差分スナップショットを自動的に作成する計画を立てます。HOME ファイルシステムの差分スナップショットであることを判別できるように、自動的にマウントおよび公開するときのマウントポイント名の識別子には「HOME」を設定する例とします。

ここでは、差分格納デバイスの容量が不足した場合、ファイルシステムの使用を制限し、差分スナップショットのデータを保護するよう設定する例とします。

ここで示した例で差分スナップショットを運用するときの GUI での設定内容を表 5-9 差分スナップショットの設定内容 (シングルノード構成時の HOME ファイルシステム) に示します。

表 5-9 差分スナップショットの設定内容 (シングルノード構成時の HOME ファイルシステム)

項目	設定内容
差分格納デバイスに必要な容量※	370.1GB
差分スナップショットを自動的に作成する間隔	1日2回 (12時間毎)
識別子	HOME
あふれ時の動作	ファイルシステムの使用を制限

注※

差分格納デバイスの容量の見積もり方法については、「5.5 差分格納デバイスの容量の設計」を参照してください。

自動作成された差分スナップショットの名称およびマウントポイントについては、「5.8 差分スナップショットの自動作成の運用」を参照してください。

5.4.3 運用テストの実施

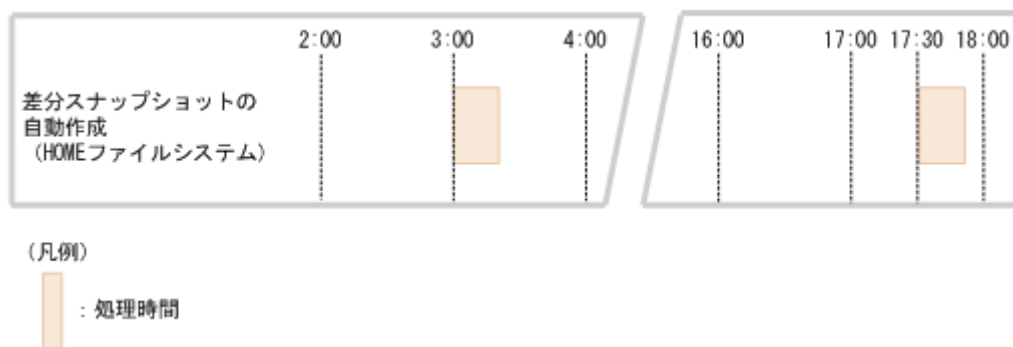
各ファイルシステムに差分格納デバイスを設定したら、運用テストを行います。ここでは、クラスター構成で運用テストを実施する例を説明します。

(1) HOME ファイルシステムの運用テスト

HOME ファイルシステムの差分格納デバイスや自動作成スケジュールを設定したら、クライアントが実際にファイルシステムを利用している環境で、自動作成スケジュールの運用テストを行います。

運用テストでは、ファイルシステムに対するデータの更新量が見積もりどおりになっているか、差分スナップショットが正しく作成されているかなどを確認します。

図 5-12 スケジュールの設定内容



ファイルシステムに対するデータの更新量に関して、見積もりと実際とで差がある場合には、差分格納デバイスの容量を設計し直して再設定または拡張します。

運用テストで問題がないことを確認したら、正式な運用を開始します。

(2) DOCUMENT ファイルシステムの運用テスト

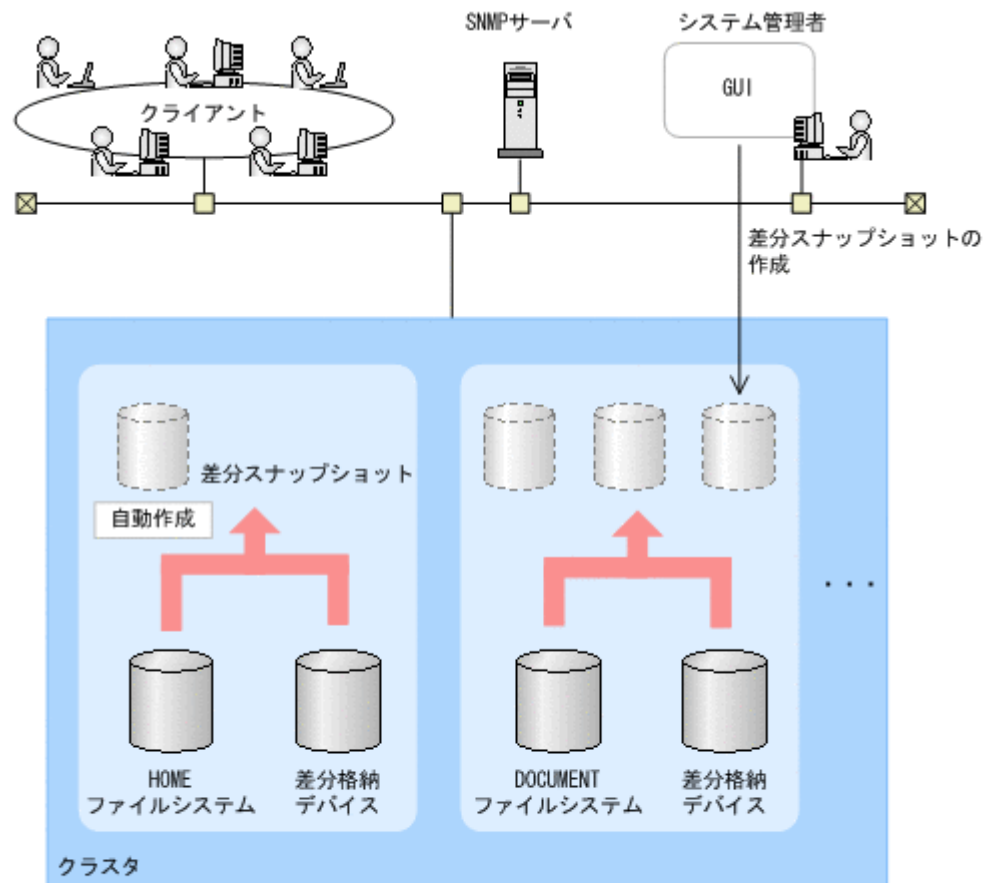
DOCUMENT ファイルシステムの差分格納デバイスを設定したら、差分スナップショットを作成し、正常に作成されているかどうか確認します。

運用テストで問題がないことを確認したら、正式な運用を開始します。

5.4.4 差分スナップショットの運用開始

運用を開始したら、システム管理者は各ファイルシステムの運用方法に応じて作業を行います。ここでは、クラスタ構成の場合の例を説明します。

図 5-13 運用開始後のシステム管理者の作業



(凡例) ———→ : 差分スナップショット作成の操作
 → : 差分スナップショットが作成される際のデータの流れ

(1) HOME ファイルシステムでの作業

HOME ファイルシステムでは、差分スナップショットの作成・公開・削除などの処理は自動的に行われます。

運用開始後に、ファイルシステムでの運用ポリシーが変更になったり、当初の見積もりよりも実際のデータ更新量が多くなったりした場合には、状況に応じて次の操作を実行できます。

- 差分格納デバイスを拡張する
- 差分格納デバイスの警告閾値を変更する
- 差分格納デバイスのあふれ防止動作を変更する
- 差分格納デバイスのあふれ防止動作の動作閾値を変更する
- 差分格納デバイスのあふれ時の動作を変更する
- 差分スナップショットの予約世代数を変更する

- ・ 差分スナップショットの自動作成・マウントの上限数を変更する
- ・ 差分スナップショットの作成間隔を変更する

(2) DOCUMENT ファイルシステムでの作業

システム管理者は、クライアントからの要求に応じて DOCUMENT ファイルシステムの差分スナップショットを手動で作成します。差分スナップショットは、クラスタ構成の場合は [スナップショットの作成または置換]ダイアログまたは `syncadd` コマンド、シングルノード構成の場合は `syncadd` コマンドで作成します。

クライアントが差分スナップショットを参照する必要がある場合は、要求された差分スナップショットを手動でマウントし、差分スナップショットにファイル共有を作成します。クライアントの作業が終了したら、ファイル共有を削除し、差分スナップショットをアンマウントします。

また、不要になった差分スナップショットは定期的に削除します。

運用開始後に、ファイルシステムでの運用ポリシーが変更になったり、当初の見積もりよりも実際のデータ更新量が多くなったりした場合には、状況に応じて次の操作を実行できます。

- ・ 差分格納デバイスを拡張する
- ・ 差分格納デバイスの警告閾値を変更する
- ・ 差分格納デバイスのあふれ防止動作を設定する
- ・ 差分格納デバイスのあふれ防止動作の動作閾値を設定する
- ・ 差分格納デバイスのあふれ時の動作を変更する
- ・ 差分スナップショットの予約世代数を変更する

5.4.5 クライアント側での操作

差分スナップショットは読み取り専用でマウントされます。クライアントは、公開された差分スナップショットにアクセスして、ファイルを参照したり、作成元のファイルシステムやクライアントマシンにファイルをコピーしたりできます。ここでは、クラスタ構成での差分スナップショットの操作例を説明します。

(1) HOME ファイルシステムの差分スナップショットの操作

HOME ファイルシステムの差分スナップショットは、HOME ファイルシステムの共有内に公開されません。クライアントは、差分スナップショット公開用のディレクトリ内の、差分スナップショット作成日時のディレクトリにアクセスすることで参照できます。

ここでは、HOME ファイルシステムに対して 2011 年 11 月 2 日の 3:00 に作成された差分スナップショットをクライアントから参照する例を説明します。

図 5-14 クライアントから差分スナップショットへのアクセス (HOME ファイルシステム)

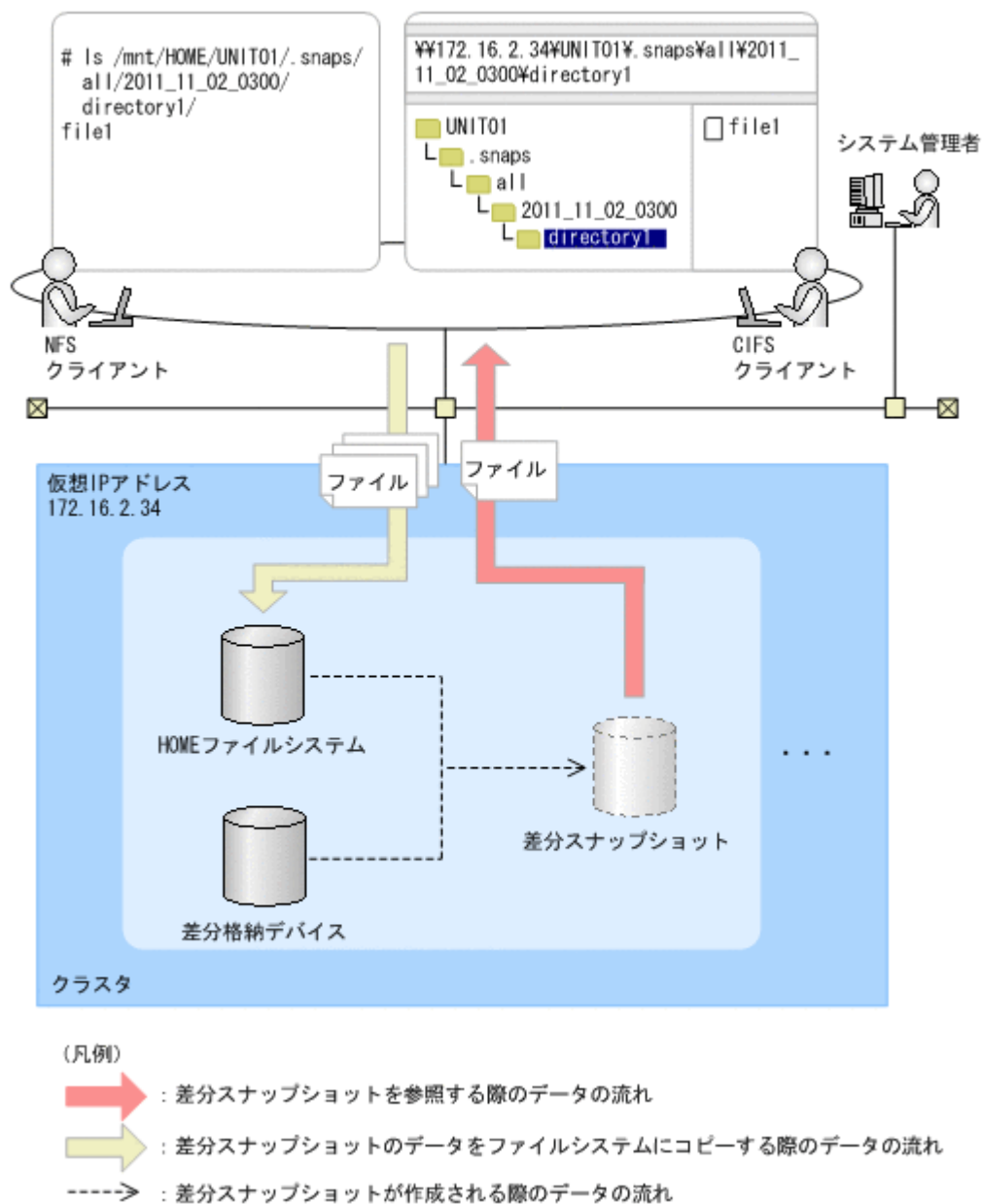


図 5-14 クライアントから差分スナップショットへのアクセス (HOME ファイルシステム) に示す差分スナップショットを参照するには、クライアントは次のディレクトリにアクセスします。

NFS クライアント

```
/mnt/HOME/UNIT01/.snaps/all/2011_11_02_0300
```

CIFS クライアント

```
¥¥172.16.2.34¥UNIT01¥.snaps¥all¥2011_11_02_0300
```

注意： NFSv2 または NFSv3 プロトコルを利用している NFS クライアントが、共有内に公開されている差分スナップショットのデータをファイルシステムにコピーする際には、目的のデータをファイル単位でいったんクライアントマシンにコピーしてから、そのデータをファイルシステムにコピーしてください。そのほかのコピー方法については、「5.8.2 自動作成スケジュールを運用する際の注意事項」を参照してください。

(2) DOCUMENT ファイルシステムの差分スナップショットの操作

DOCUMENT ファイルシステムでは、システム管理者が差分スナップショットにファイル共有を作成することでクライアントに公開します。この場合、NFS クライアントと CIFS クライアントでアクセス方法が次のとおり異なります。

NFS クライアント

対象の共有ディレクトリをクライアントマシン内の既存のディレクトリに NFS マウントすることで、差分スナップショットにアクセスできます。NFS クライアントには、次の形式で差分スナップショットの情報が表示されます。

```
/mnt/<差分スナップショットのマウントポイント名>/<ファイル共有のサブディレクトリ名>
```

作業が完了したら、差分スナップショットをクライアントマシンから NFS アンマウントします。

CIFS クライアント

対象の差分スナップショットが属するリソースグループまたは Virtual Server の仮想 IP アドレスや CIFS 共有名を指定して、差分スナップショットにアクセスします。次のどちらかの形式でパスを指定することで、差分スナップショットのデータにアクセスできます。

```
¥¥<仮想 IP アドレス>¥¥< CIFS 共有名>
```

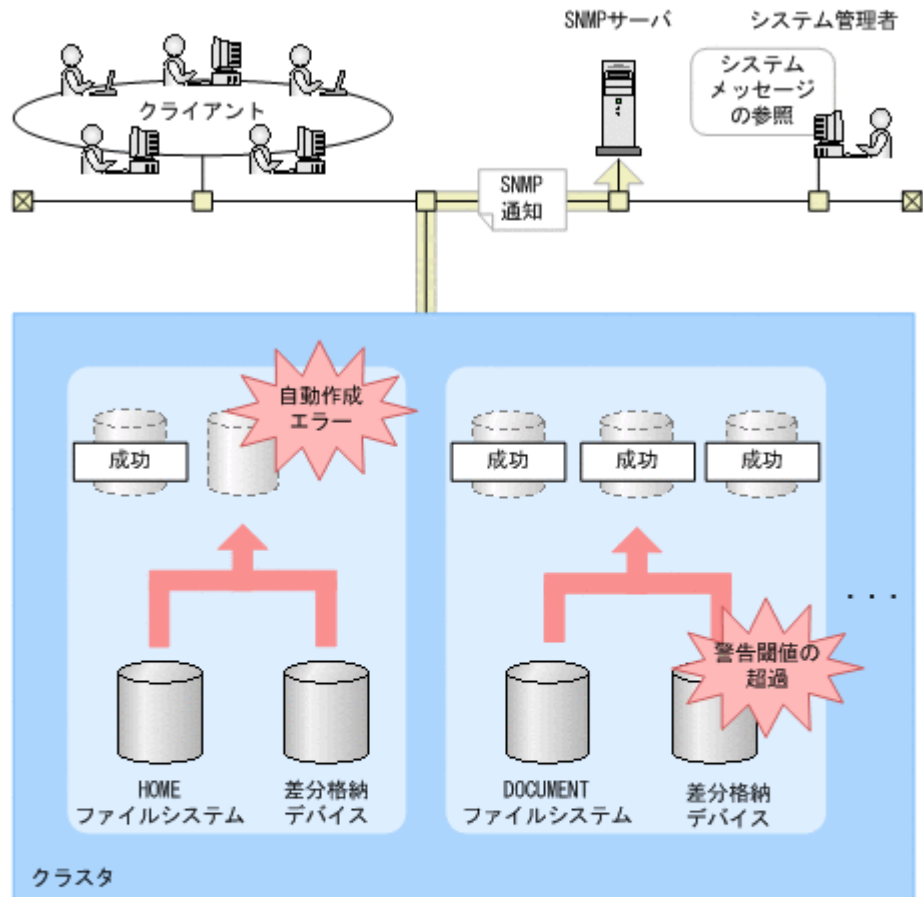
```
¥¥<ノードのホスト名または Virtual Server >¥¥< CIFS 共有名>
```

NFS クライアントおよび CIFS クライアントがファイルシステム内のデータを利用する場合の注意事項については、「4.13 クライアントがファイルシステムの利用を開始する前に」を参照してください。




5.4.6 運用状況の監視

差分スナップショットの運用を開始したら、システム管理者は、差分格納デバイスや差分スナップショットの状況を確認します。また、システムメッセージ (em_alertfile)、SNMP トラップまたは E-mail 通知を定期的に参照して、差分格納デバイスの容量を監視したり、自動作成スケジュールの処理結果を確認したりします。ここでは、クラスタ構成での運用状況の監視例を説明します。

図 5-15 障害の検知方法の例



(凡例)

-  : 差分スナップショットが作成される際のデータの流れ
-  : SNMP通知のデータの流れ
-  : 差分スナップショット

例えば、差分格納デバイスの使用率が警告閾値を超過した場合は、KAQS19001-W メッセージが通知されます。

何らかの通知を受け取った場合や障害が発生した場合は、通知されたメッセージに従って、必要に応じて保守員と連携し、迅速に対処します。

5.4.7 運用完了後の作業

プロジェクトの完了などで、ファイルシステムに対して差分スナップショットを作成・確保する必要がなくなったら、差分格納デバイスを解除します。

差分格納デバイスを解除すると、ファイルシステムに対して確保された差分スナップショットがすべて削除されます。また、ファイルシステムに設定された自動作成スケジュールも解除されます。

5.5 差分格納デバイスの容量の設計

差分格納デバイスを設定する際は、差分格納デバイスに必要な容量を算出する必要があります。ここでは、差分格納デバイスの容量の算出方法について説明します。

システム管理者は、差分格納デバイスを設定・拡張する前に、ファイルシステムの用途や格納するデータの種類の考慮して、そのファイルシステムで想定されるデータの書き込み量を見積もってください。また、差分スナップショットの用途に応じて、作成間隔や確保する世代数を検討してください。

次の2つの値を調べることで、差分格納デバイスに必要なおおよその容量を見積もることができます。

- 設定元のファイルシステムの容量
- 1つの差分スナップショットを作成してから、次の差分スナップショットを作成するまでの間に設定元のファイルシステムに対して発生するデータ更新量

ただし、ファイルシステムのデータがHCPにマイグレートされている場合や、ディスク上でのデータの配置によっては、ファイルシステムに対して更新したデータ量よりも差分格納デバイスに退避したデータ量の方が多くなる場合があります。階層ファイルシステムの場合は、階層間でファイルを移動させるためのポリシーによって階層ごとの更新量や移動量が異なります。第1階層のファイルシステム(Tier 1)から第2階層のファイルシステム(Tier 2)へのファイル移動によって、Tier 2への更新が発生し、差分データの退避が発生します。また、ファイルシステムを更新しても差分格納デバイスにデータが退避されないこともあります。このため、差分格納デバイスの容量は、運用に合った見積もり式で算出される値を目安にして、容量に余裕を持って設定してください(見積もり式では、ファイルシステムに対する更新するデータ量を1時間当たりに換算して計算します)。

- 階層ファイルシステムではないファイルシステムで、HCPにデータがマイグレートされない場合
「5.5.1 HCPにデータがマイグレートされないファイルシステムの場合の見積もり式」を参照してください。
- 階層ファイルシステムではないファイルシステムで、HCPにデータがマイグレートされる場合
「5.5.2 HCPにデータがマイグレートされるファイルシステムの場合の見積もり式」を参照してください。
- 階層ファイルシステムの場合
「5.5.3 階層ファイルシステムの場合の見積もり式」を参照してください。

注意：

「5.5.3 階層ファイルシステムの場合の見積もり式」の見積もり式を使用した差分格納デバイス容量の見積もりが困難な場合は、ファイルシステムの容量と同じ容量を設定してファイルスナップショット機能の運用を開始してください。運用を開始したあと、差分格納デバイスの使用量の増加傾向を考慮しつつ、必要に応じてGUIで差分格納デバイスの容量を追加してください。

差分格納デバイスの容量の上限は、設定されているチャンクサイズによって異なります。設定できる容量の上限については、表 5-4 チャンクサイズによるファイルシステムおよび差分格納デバイス容量の拡張上限を参照してください。

ファイルスナップショット機能を設定するときに差分データを退避する単位として指定するチャンクサイズは、ファイルスナップショット機能のバックグラウンド処理時間および Hitachi File Remote Replicator の運用に影響します。ファイルシステムの容量と、最大予約世代数の組み合わせごとのチャンクサイズのデフォルト値を表 5-10 デフォルトのチャンクサイズに示します。階層ファイルシステムの場合は、各階層のチャンクサイズのデフォルト値のうちの最大値を指定してください。

また、ファイルスナップショット機能のバックグラウンド処理に掛かる時間が、差分スナップショットの作成間隔を超えないように、チャンクサイズを指定してください。バックグラウンド処理に掛かる時間については、表 5-5 バックグラウンド処理に掛かる時間の目安（システム負荷が低く、I/O競合がない状態の場合）を参照してください。

なお、差分格納デバイスを設定したあとは、チャンクサイズを変更できません。ファイルシステムの拡張を計画している場合は、拡張後のファイルシステムの容量を考慮して、チャンクサイズを指定してください。

表 5-10 デフォルトのチャンクサイズ

ファイルシステムの容量	デフォルトのチャンクサイズ (KB) ※			
	最大予約世代数が 124 の場合	最大予約世代数が 248 の場合	最大予約世代数が 496 の場合	最大予約世代数が 992 の場合
32TB 以下	1,024	8,192	16,384	32,768
32TB 超過～128TB 以下	4,096	8,192	16,384	32,768
128TB 超過～256TB 以下	8,192	16,384	32,768	32,768
256TB 超過～512TB 以下	16,384	32,768	32,768	32,768
512TB 超過～1PB 以下	32,768	32,768	32,768	32,768

注※ デフォルトのチャンクサイズを設定する場合、自動作成スケジュールを設定する際に、作成間隔を 2 時間以上空けることを推奨します。デフォルト値を設定すると、差分スナップショットを作成または削除するためのバックグラウンド処理に 15 分以上、最大で 2 時間掛かることがあります。作成間隔を短くしたい場合は、「5.3.4 差分スナップショットの管理」で差分スナップショットの作成・削除に掛かる時間を確認し、ファイルシステムの容量、およびチャンクサイズを変更してください。

5.5.1 HCP にデータがマイグレートされないファイルシステムの場合の見積もり式

階層ファイルシステムの場合は、「5.5.3 階層ファイルシステムの場合の見積もり式」を参照して差分格納デバイスの容量を見積もってください。

HCP にデータがマイグレートされないよう設定している、容量が 256GB 未満のファイルシステムには、次の見積もり式で算出される値を目安にして差分格納デバイスの容量を設定してください。

差分格納デバイスの容量の見積もり式（HCP にデータがマイグレートされない、容量が 256GB 未満のファイルシステムの場合）

差分格納デバイスの容量 (MB)

$$= \frac{A \times K}{2 \times F} + 128 + (B \times C + \frac{F}{1024} \times 3 + 133) \times D + 33 \times E$$

(凡例)

- A : 設定元のファイルシステムの容量 (単位: MB)
- B : ファイルシステムに対して1時間あたりに更新するデータ量 (単位: MB/時間)
- C : 差分スナップショットの作成間隔 (単位: 時間)
- D : 差分スナップショットの予約世代数
- E : 差分格納デバイスを構成するデバイスファイルの数
(シングルノード構成の場合は0を指定)
- F : チャンクサイズ (単位: KB)
- K : 予約世代数に応じた係数
 予約世代数が3～124の場合 : 1
 予約世代数が125～248の場合 : 2
 予約世代数が249～496の場合 : 4
 予約世代数が497～992の場合 : 8

HCP にデータがマイグレートされないよう設定している、容量が 256GB 以上のファイルシステムには、次の見積もり式で算出される値を目安にして差分格納デバイスの容量を設定してください。

差分格納デバイスの容量の見積もり式（HCP にデータがマイグレートされない、容量が 256GB 以上のファイルシステムの場合）

差分格納デバイスの容量 (MB)

$$= \frac{A \times K}{2 \times F} + 128 + \left(B \times C + \frac{F}{1024} \times \frac{A}{131072} + 165 \right) \times D + 33 \times E$$

(凡例)

- A : 設定元のファイルシステムの容量 (単位: MB)
- B : ファイルシステムに対して1時間あたりに更新するデータ量 (単位: MB/時間)
- C : 差分スナップショットの作成間隔 (単位: 時間)
- D : 差分スナップショットの予約世代数
- E : 差分格納デバイスを構成するデバイスファイルの数
(シングルノード構成の場合は0を指定)
- F : チャンクサイズ (単位: KB)
- K : 予約世代数に応じた係数
予約世代数が3~124の場合 : 1
予約世代数が125~248の場合 : 2
予約世代数が249~496の場合 : 4
予約世代数が497~992の場合 : 8

5.5.2 HCP にデータがマイグレートされるファイルシステムの場合の見積もり式

ここで説明する見積もり式は、クライアントに差分スナップショットのデータを公開するために、対象のファイルシステムにスタブファイルが作成されないよう設定していることを前提としています。arcimplimitset コマンドでスタブ化開始の閾値を 0GB に設定しているか確認してください。

HCP にデータがマイグレートされるよう設定している、容量が 256GB 未満のファイルシステムには、次の見積もり式で算出される値を目安にして差分格納デバイスの容量を設定してください。

差分格納デバイスの容量の見積もり式（HCP にデータがマイグレートされる、容量が 256GB 未満のファイルシステムの場合）

差分格納デバイスの容量 (MB)

$$= \frac{A \times K}{2 \times F} + 128 + \left[\left(B + 8 \times G \times \frac{H}{1024^2} \right) \times C + \frac{F}{1024} \times 3 + 133 \right] \times D + 33 \times E$$

(凡例)

- A : 設定元のファイルシステムの容量 (単位: MB)
- B : ファイルシステムに対して1時間あたりに更新するデータ量 (単位: MB/時間)
- C : 差分スナップショットの作成間隔 (単位: 時間)
- D : 差分スナップショットの予約世代数
- E : 差分格納デバイスを構成するデバイスファイルの数
(シングルノード構成の場合は0を指定)
- F : チャンクサイズ (単位: KB)
- G : ファイルシステムに対して1時間あたりに作成されるファイル数
- H : ファイルシステムに対して1時間あたりに作成されるファイルの平均パス長 (単位: バイト)
- K : 予約世代数に応じた係数
予約世代数が3~124の場合 : 1
予約世代数が125~248の場合 : 2
予約世代数が249~496の場合 : 4
予約世代数が497~992の場合 : 8

HCP にデータがマイグレートされるよう設定している、容量が 256GB 以上のファイルシステムには、次の見積もり式で算出される値を目安にして差分格納デバイスの容量を設定してください。

差分格納デバイスの容量の見積もり式（HCP にデータがマイグレートされる、容量が 256GB 以上のファイルシステムの場合）

差分格納デバイスの容量（MB）

$$= \frac{A \times K}{2 \times F} + 128 + \left[\left(B + 8 \times G \times \frac{H}{1024^2} \right) \times C + \frac{F}{1024} \times \frac{A}{131072} + 165 \right] \times D + 33 \times E$$

（凡例）

- A : 設定元のファイルシステムの容量（単位：MB）
- B : ファイルシステムに対して1時間あたりに更新するデータ量（単位：MB/時間）
- C : 差分スナップショットの作成間隔（単位：時間）
- D : 差分スナップショットの予約世代数
- E : 差分格納デバイスを構成するデバイスファイルの数（シングルノード構成の場合は0を指定）
- F : チャンクサイズ（単位：KB）
- G : ファイルシステムに対して1時間あたりに作成されるファイル数
- H : ファイルシステムに対して1時間あたりに作成されるファイルの平均パス長（単位：バイト）
- K : 予約世代数に応じた係数
予約世代数が3～124の場合 : 1
予約世代数が125～248の場合 : 2
予約世代数が249～496の場合 : 4
予約世代数が497～992の場合 : 8

5.5.3 階層ファイルシステムの場合の見積もり式

階層ファイルシステムの場合は、Tier 1 と Tier 2 の両方に対して差分格納デバイスの容量を見積もる必要があります。

(1) Tier 1 の場合の見積もり式

容量が 256GB 未満の Tier 1 には、次の見積もり式で算出される値を目安にして差分格納デバイスの容量を設定してください。

差分格納デバイスの容量の見積もり式（容量が 256GB 未満の Tier 1 の場合）

差分格納デバイスの容量（MB）

$$= \frac{A \times K}{2 \times F} + 128 + \left(B \times C + \frac{F}{1024} \times 3 + 133 \right) \times D + 33 \times E$$

（凡例）

- A : 設定元のファイルシステムの容量（単位：MB）
- B※ : Tier 1 に対して1時間あたりに更新するデータ量（単位：MB/時間）
- C : 差分スナップショットの作成間隔（単位：時間）
- D : 差分スナップショットの予約世代数
- E : 差分格納デバイスを構成するデバイスファイルの数
- F : チャンクサイズ（単位：KB）
- K : 予約世代数に応じた係数
予約世代数が3～124の場合 : 1
予約世代数が125～248の場合 : 2
予約世代数が249～496の場合 : 4
予約世代数が497～992の場合 : 8

注※ Tier 1の更新量には、Tier 2に移動する前のファイルの更新量を含みます。

容量が 256GB 以上の Tier 1 には、次の見積もり式で算出される値を目安にして差分格納デバイスの容量を設定してください。

差分格納デバイスの容量の見積もり式（容量が 256GB 以上の Tier 1 の場合）

差分格納デバイスの容量 (MB)

$$= \frac{A \times K}{2 \times F} + 128 + \left(B \times C + \frac{F}{1024} \times \frac{A}{131072} + 165 \right) \times D + 33 \times E$$

(凡例)

- A : 設定元のファイルシステムの容量 (単位: MB)
- B*: Tier 1 に対して1時間あたりに更新するデータ量 (単位: MB/時間)
- C : 差分スナップショットの作成間隔 (単位: 時間)
- D : 差分スナップショットの予約世代数
- E : 差分格納デバイスを構成するデバイスファイルの数
- F : チャンクサイズ (単位: KB)
- K : 予約世代数に応じた係数
 - 予約世代数が3~124の場合 : 1
 - 予約世代数が125~248の場合 : 2
 - 予約世代数が249~496の場合 : 4
 - 予約世代数が497~992の場合 : 8

注※ Tier 1の更新量には、Tier 2に移動する前のファイルの更新量を含みます。

(2) Tier 2 の場合の見積もり式

容量が 256GB 未満の Tier 2 には、次の見積もり式で算出される値を目安にして差分格納デバイスの容量を設定してください。

差分格納デバイスの容量の見積もり式（容量が 256GB 未満の Tier 2 の場合）

差分格納デバイスの容量 (MB)

$$= \frac{A \times K}{2 \times F} + 128 + \left(B \times C + \frac{F}{1024} \times 3 + 133 \right) \times D + \uparrow \frac{C \times D}{H} \uparrow \times I + 33 \times E$$

(凡例)

- ↑ ↑ : 小数点以下を切り上げる
- A : 設定元のファイルシステムの容量 (単位: MB)
- B : Tier 2 に対して1時間あたりに更新するデータ量 (単位: MB/時間)
- C : 差分スナップショットの作成間隔 (単位: 時間)
- D : 差分スナップショットの予約世代数
- E : 差分格納デバイスを構成するデバイスファイルの数
- F : チャンクサイズ (単位: KB)
- H : Tier 移動の実行間隔 (単位: 時間)
- I : Tier 移動1回当たりの移動量 (単位: MB)
- K : 予約世代数に応じた係数
 - 予約世代数が3~124の場合 : 1
 - 予約世代数が125~248の場合 : 2
 - 予約世代数が249~496の場合 : 4
 - 予約世代数が497~992の場合 : 8

容量が 256GB 以上の Tier 2 には、次の見積もり式で算出される値を目安にして差分格納デバイスの容量を設定してください。

差分格納デバイスの容量の見積もり式（容量が 256GB 以上の Tier 2 の場合）

差分格納デバイスの容量 (MB)

$$= \frac{A \times K}{2 \times F} + 128 + \left(B \times C + \frac{F}{1024} \times \frac{A}{131072} + 165 \right) \times D + \uparrow \frac{C \times D}{H} \uparrow \times I + 33 \times E$$

(凡例)

- ↑ ↑ : 小数点以下を切り上げる
- A : 設定元のファイルシステムの容量 (単位: MB)
- B : Tier 2 に対して1時間あたりに更新するデータ量 (単位: MB/時間)
- C : 差分スナップショットの作成間隔 (単位: 時間)
- D : 差分スナップショットの予約世代数
- E : 差分格納デバイスを構成するデバイスファイルの数
- F : チャンクサイズ (単位: KB)
- H : Tier移動の実行間隔 (単位: 時間)
- I : Tier移動1回当たりの移動量 (単位: MB)
- K : 予約世代数に応じた係数
予約世代数が3~124の場合 : 1
予約世代数が125~248の場合 : 2
予約世代数が249~496の場合 : 4
予約世代数が497~992の場合 : 8

5.5.4 差分格納デバイスを構成するデバイスファイルの前提条件

クラスタ構成の場合は、差分格納デバイスにデバイスファイルを使用します。差分格納デバイスを構成するデバイスファイルの容量は、次の前提条件を満たしている必要があります。

各計算式で使用している A、B または C などの値については、差分格納デバイスの容量の見積もり式 (HCP にデータがマイグレートされない、容量が 256GB 未満のファイルシステムの場合) の凡例を参照してください。ただし、Tier 1 の場合は差分格納デバイスの容量の見積もり式 (容量が 256GB 未満の Tier 1 の場合)、Tier 2 の場合は差分格納デバイスの容量の見積もり式 (容量が 256GB 未満の Tier 2 の場合) の凡例を参照してください。

- 差分格納デバイスを構成するすべてのデバイスファイルがそれぞれ 33MB 以上の容量を持つ
- 各デバイスファイルの容量を 32MB の倍数に切り捨てた容量の合計が、次の計算式で示す容量より大きい

$$33 \text{ (MB)} \times E + A \text{ (MB)} \div (F \text{ (KB)} \div 1024) \times \{(0.5 \text{ (KB)} \div 1024) \times K\} + 5 \text{ (MB)} + (F \text{ (KB)} \div 1024) \times 1024$$

- 1時間当たりのデータ更新量 (B) と差分スナップショットの作成間隔 (C) との積が、設定元のファイルシステムの容量 (A) 以下である

$$B \times C \leq A$$

この条件を満たしていない場合は、1時間当たりのデータ更新量 (B) として適当な値が見積もられているかどうかを確認してください。適当な値である場合は、差分格納デバイスが確実に容量不足を起こさないようにするために、次の見積もり式を使用して算出した安全値以上の容量を差分格納デバイスに割り当ててください。

差分格納デバイスの容量 (MB)

$$= 64 \times E + A \times \left(D + \frac{1}{2 \times F} \right)$$

(凡例)

- A : 設定元のファイルシステムの容量 (単位: MB)
- D : 差分スナップショットの予約世代数
- E : 差分格納デバイスを構成するデバイスファイルの数
- F : チャンクサイズ (単位: KB)

5.5.5 HCP にデータがマイグレートされないファイルシステムの場合の見積もり例

クラスタ構成の場合の、差分格納デバイス容量の見積もり方法を説明します。この例では、次の条件でファイルスナップショット機能を運用することを想定しています。

- ファイルシステムには 100 ユーザーのホームディレクトリを格納する
- 1 ユーザーあたり 5GB のホームディレクトリを割り当てる
- 1 日あたり 1 ユーザーは 10MB のデータを更新する
- 差分スナップショットは 1 日 2 回作成する
- 作成した差分スナップショットは 31 日間保持する
- 同じ容量のデバイスファイルを 3 個使用する

ファイルシステムの容量が 500GB であるため、差分格納デバイスの容量の見積もり式(HCP にデータがマイグレートされない、容量が 256GB 以上のファイルシステムの場合)の見積もり式を使用します。この条件の場合に使用する値は次のとおりです。

差分格納デバイスの容量の見積もり例で使用する値 (HCP にデータがマイグレートされないファイルシステムの場合)

A = 5120 (MB/ユーザー) × 100 (ユーザー) = 512000 (MB)
B = 10 (MB/ユーザー) × 100 (ユーザー) ÷ 24 (時間) = 1000/24 (MB/時間)
C = 24 (時間) ÷ 2 (回) = 12 (時間)
D = 2 (世代/日) × 31 (日) = 62 (世代)
E = 3 (個)
F = 1024 (KB)
K = 1

差分格納デバイスの容量の見積もり例で使用する値 (HCP にデータがマイグレートされないファイルシステムの場合) を使用して見積もり式から算出すると、差分格納デバイスの容量は約 40.9GB になります。

差分格納デバイスを構成するデバイスファイルの容量は、「5.5.4 差分格納デバイスを構成するデバイスファイルの前提条件」の前提条件を満たしている必要があります。前提条件にある計算式について、差分格納デバイスの容量の見積もり例で使用する値 (HCP にデータがマイグレートされないファイルシステムの場合) を当てはめて確認します。

- 各デバイスファイルの容量を 32MB の倍数に切り捨てた容量の合計が、次の計算式で示す容量より大きい

$$\begin{aligned} & 33 \text{ (MB)} \times E + A \text{ (MB)} \div (F \text{ (KB)} \div 1024) \times \{(0.5 \text{ (KB)} \div 1024) \times K\} + 5 \text{ (MB)} + (F \text{ (KB)} \\ & \div 1024) \times 1024 \\ & = 33 \times 3 + 512000 \div (1024 \div 1024) \times \{(0.5 \div 1024) \times 1\} + 5 + (1024 \div 1024) \times 1024 \\ & = 1378 \text{ (MB)} \end{aligned}$$

この例ではデバイスファイルの容量がすべて同じであるため、使用するデバイスファイル 1 個の容量は次のようになります。

$$(40.9 \times 1024) \div 3 = 13960.5 \text{ (MB)}$$

デバイスファイル 1 個の容量を 32MB の倍数に切り捨てると 13,952MB となり、切り捨てた容量の合計は次のとおり 41,856MB となるため、1,378MB より大きくなければならないという前提条件を満たしています。

$$13952 \times 3 = 41856 \text{ (MB)}$$

- 1 時間当たりのデータ更新量 (B) と差分スナップショットの作成間隔 (C) との積が、設定元のファイルシステムの容量 (A) 以下である

$$\begin{aligned}
 & B \times C \\
 & = (1000 \div 24) \times 12 \\
 & = 500 \text{ (MB)} \leq A
 \end{aligned}$$

デバイスファイルの容量が前提条件をすべて満たしているため、各デバイスファイルは 13.9GB 以上の容量が必要ということになります。

5.5.6 HCP にデータがマイグレートされるファイルシステムの場合の見積もり例

クラスタ構成の場合の、差分格納デバイス容量の見積もり方法を説明します。この例では、次の条件でファイルスナップショット機能を運用することを想定しています。

- ・ ファイルシステムには 100 ユーザーのホームディレクトリを格納する
- ・ 1 ユーザー当たり 5GB のホームディレクトリを割り当てる
- ・ 1 日当たり 1 ユーザーは 10MB のデータを更新する
- ・ ファイルシステムに対して 1 日当たりに 50,000 ファイル（ファイルの平均パス長は 100 バイト）を作成する
- ・ 差分スナップショットは 1 日 2 回作成する
- ・ 作成した差分スナップショットは 31 日間保持する
- ・ 同じ容量のデバイスファイルを 3 個使用する

ファイルシステムの容量が 500GB であるため、差分格納デバイスの容量の見積もり式(HCP にデータがマイグレートされる、容量が 256GB 以上のファイルシステムの場合)の見積もり式を使用します。この条件の場合に使用する値は次のとおりです。

差分格納デバイスの容量の見積もり例で使用する値 (HCP にデータがマイグレートされるファイルシステムの場合)

$$\begin{aligned}
 A &= 5120 \text{ (MB/ユーザー)} \times 100 \text{ (ユーザー)} = 512000 \text{ (MB)} \\
 B &= 10 \text{ (MB/ユーザー)} \times 100 \text{ (ユーザー)} \div 24 \text{ (時間)} = 1000/24 \text{ (MB/時間)} \\
 C &= 24 \text{ (時間)} \div 2 \text{ (回)} = 12 \text{ (時間)} \\
 D &= 2 \text{ (世代/日)} \times 31 \text{ (日)} = 62 \text{ (世代)} \\
 E &= 3 \text{ (個)} \\
 F &= 1024 \text{ (KB)} \\
 G &= 50000 \text{ (ファイル)} \\
 H &= 100 \text{ (バイト)} \\
 K &= 1
 \end{aligned}$$

差分格納デバイスの容量の見積もり例で使用する値 (HCP にデータがマイグレートされるファイルシステムの場合) を使用して見積もり式から算出すると、差分格納デバイスの容量は約 68.7GB になります。

差分格納デバイスを構成するデバイスファイルの容量は、「5.5.4 差分格納デバイスを構成するデバイスファイルの前提条件」の前提条件を満たしている必要があります。前提条件にある計算式について、差分格納デバイスの容量の見積もり例で使用する値 (HCP にデータがマイグレートされるファイルシステムの場合) を当てはめて確認します。

- ・ 各デバイスファイルの容量を 32MB の倍数に切り捨てた容量の合計が、次の計算式で示す容量より大きい

$$\begin{aligned}
 & 33 \text{ (MB)} \times E + A \text{ (MB)} \div (F \text{ (KB)} \div 1024) \times \{(0.5 \text{ (KB)} \div 1024) \times K\} + 5 \text{ (MB)} + (F \text{ (KB)} \\
 & \div 1024) \times 1024 \\
 & = 33 \times 3 + 512000 \div (1024 \div 1024) \times \{(0.5 \div 1024) \times 1\} + 5 + (1024 \div 1024) \times 1024 \\
 & = 1378 \text{ (MB)}
 \end{aligned}$$

この例ではデバイスファイルの容量がすべて同じであるため、使用するデバイスファイル1個の容量は次のようになります。

$$(68.7 \times 1024) \div 3 = 23449.6 \text{ (MB)}$$

デバイスファイル1個の容量を32MBの倍数に切り捨てると23,424MBとなり、切り捨てた容量の合計は次のとおり70,272MBとなるため、1,378MBより大きくなければならないという前提条件を満たしています。

$$23424 \times 3 = 70272 \text{ (MB)}$$

- 1時間当たりのデータ更新量 (B) と差分スナップショットの作成間隔 (C) との積が、設定元のファイルシステムの容量 (A) 以下である

$$\begin{aligned} B \times C \\ &= (1000 \div 24) \times 12 \\ &= 500 \text{ (MB)} \leq A \end{aligned}$$

デバイスファイルの容量が前提条件をすべて満たしているため、各デバイスファイルは23.1GB以上の容量が必要ということになります。

5.6 差分格納デバイスの使用量に関する設定

ここでは、差分格納デバイスの使用量に関する設定について説明します。

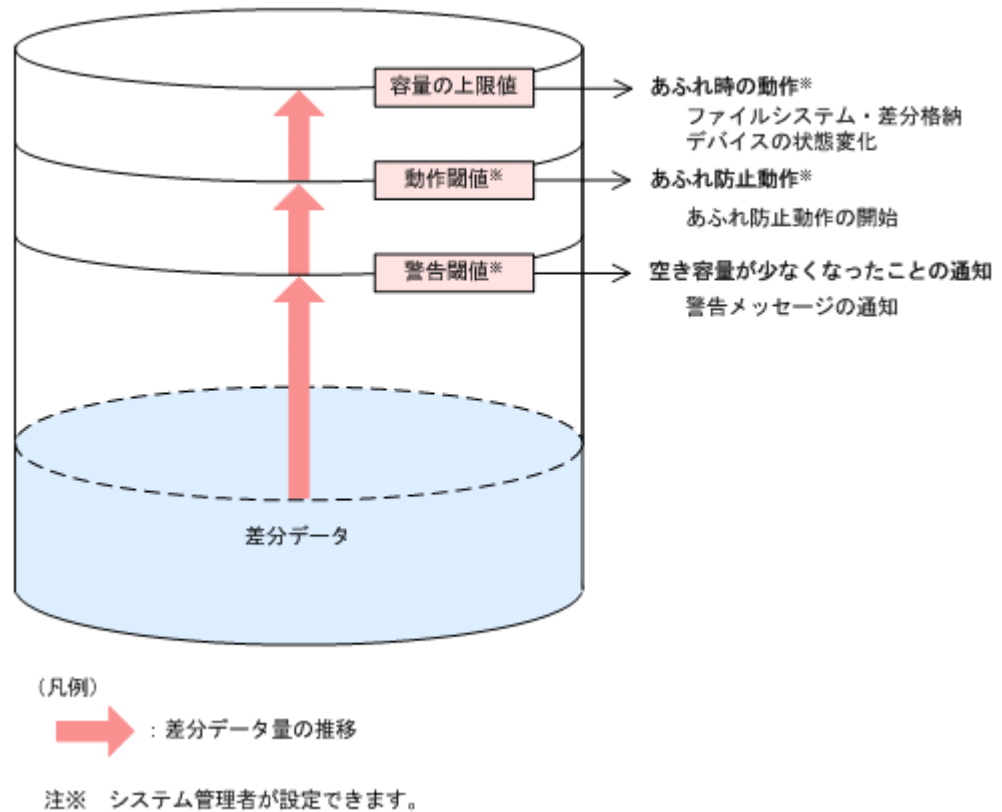
差分格納デバイスの使用量に関して、警告閾値と動作閾値の2段階の閾値を設定できます。これらの閾値を設定することで、差分格納デバイスの使用量が各閾値に達した場合に、差分格納デバイスの空き容量が少なくなったことをシステム管理者に通知したり、差分スナップショットを自動的に削除して空き容量を確保したりできます。これによって、差分格納デバイスの使用量が上限値に達すること（差分格納デバイスのあふれ）を防止できます。

さらに、差分格納デバイスの使用量が上限に達した場合の動作（あふれ時の動作）を設定できます。あふれ時の動作を設定することで、差分格納デバイスの容量が不足した場合に、ファイルシステムの使用を継続するか、ファイルシステムの使用を制限する代わりに差分スナップショットのデータが無効になることを防止するかを選択できます。

システム管理者は、ファイルシステムの用途や運用方法を考慮して、差分格納デバイスの使用量に関する設定を検討してください。また、運用状況を監視して、状況に応じて設定を見直してください。

差分格納デバイスの使用量とシステムの動作の関係を次の図に示します。

図 5-16 差分格納デバイスの使用量とシステムの動作の関係



システム管理者が設定できるそれぞれの項目について、次に説明します。

5.6.1 警告閾値の設定

システム管理者は、差分格納デバイスの空き容量が少なくなったことを事前を知ることで、容量を使い切ってしまうよう対処できます。警告閾値を設定することで、空き容量が少なくなったことのお知らせを受けられます。

警告閾値を設定すると、差分格納デバイスの使用率が警告閾値に達した際、KAQS19001-Wメッセージがシステムメッセージに出力されます。また、事前に設定している場合はSNMPトラップまたはE-mailでも通知されます。

5.6.2 あふれ防止動作および動作閾値の設定

システム管理者は、差分格納デバイスの使用率が警告閾値を超えてもすぐに対処できない場合に備えて、システムが自動的に空き容量を確保するように設定できます。あふれ防止動作およびあふれ防止動作を開始する動作閾値を設定することで、自動的に空き容量を確保できます。

なお、あふれ防止動作を設定する際には、警告閾値に1以上の値を設定しておく必要があります。また、あふれ防止動作を開始する動作閾値には、警告閾値より大きい値を指定します。

あふれ防止動作を設定すると、差分格納デバイスの使用率が動作閾値に達した際、空き容量を確保するために、自動的に差分スナップショットが削除されます。あふれ防止動作では、差分格納デバイスの使用率が警告閾値未満になるまで、差分スナップショットが削除されます。

差分スナップショットの削除は、設定に応じて、作成日付の古い順または新しい順に実行されます。あふれ防止動作の実行結果は、システムメッセージに出力されます。また、事前に設定している場合はSNMPトラップまたはE-mailでも通知されます。

5.6.3 あふれ時の動作の設定

システム管理者が対処できず、あふれ防止動作でも空き容量を確保できなかった場合、差分格納デバイスの容量を上限まで使い切ってしまうことがあります。差分格納デバイスの容量が不足した際のシステムの動作（あふれ時の動作）として、次のどちらかを設定できます。

ファイルシステムの使用を継続する

ファイルシステムの使用を継続する場合、差分格納デバイスの容量が不足した際も、ファイルシステムでのサービス提供は継続できます。ただし、ファイルシステムに対して作成されたすべての差分スナップショットは無効になります。

この設定の場合、差分格納デバイスの容量が不足した際に、KAQS19000-E メッセージが通知されます。

ファイルシステムの使用を制限する

ファイルシステムの使用を制限する場合、差分格納デバイスの容量が不足しても、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のデータは保護されます。ただし、ファイルシステムがブロック状態になり、ファイルシステムへの書き込みができなくなる、ファイルシステムの共有内に公開している差分スナップショットが参照できなくなるなど、使用が一時的に制限されます。

この設定の場合、差分格納デバイスの容量が不足した際に、KAQS19002-E メッセージが通知されます。

あふれ時の動作は、ファイルシステムでのサービス提供と差分スナップショットのデータ保護のどちらを優先するかを検討して選択してください。

5.7 ファイルスナップショット機能で運用しているファイルシステムの拡張

ここでは、ファイルスナップショット機能で運用しているファイルシステムを拡張する際の注意事項について説明します。

ファイルスナップショット機能で運用しているファイルシステムは、次の場合に拡張できます。

- 差分格納デバイスの状態が「Available」、 「Busy」または「Warning」である
- 差分格納デバイスの空き容量が十分にある

ファイルシステムを拡張する前に、差分格納デバイスの状態および空き容量を確認してください。

ファイルシステムの拡張に必要な差分格納デバイスの空き容量は、あふれ防止動作の設定によって、次のとおり異なります。差分格納デバイスの空き容量が次の式で算出した値よりも少ない場合は、差分格納デバイスを拡張するか、不要な差分スナップショットを削除して、空き容量を確保してください。

あふれ防止動作を設定している、かつファイルシステム拡張後の容量が1TB以下の場合

$$\begin{aligned} & \text{必要な差分格納デバイスの空き容量 (KB) =} \\ & (\text{ファイルシステムに追加するデバイスファイルの容量 (KB)} \div \text{チャンクサイズ (KB)} \div 2) \times \\ & \text{最大予約世代数に応じた係数*} + 8192 + \\ & (101 - \text{あふれ防止動作を開始する動作閾値 (\%)}) \div 100 \times \text{差分格納デバイスの容量 (KB)} \end{aligned}$$

あふれ防止動作を設定している、かつファイルシステム拡張後の容量が1TBを超える場合

$$\begin{aligned} & \text{必要な差分格納デバイスの空き容量 (KB) =} \\ & (\text{ファイルシステムに追加するデバイスファイルの容量 (KB)} \div \text{チャンクサイズ (KB)} \div 2) \times \\ & \text{最大予約世代数に応じた係数*} + 8192 + \\ & (101 - \text{あふれ防止動作を開始する動作閾値 (\%)}) \div 100 \times \\ & \text{差分格納デバイスの容量 (KB)} + 10485760 \text{ (KB)} + \\ & \uparrow \text{ファイルシステムに追加するデバイスファイルの容量 (KB)} \div 134217728 \uparrow \times \\ & \text{チャンクサイズ (KB)} \end{aligned}$$

あふれ防止動作を設定していない、かつファイルシステム拡張後の容量が1TB以下の場合

$$\begin{aligned} & \text{必要な差分格納デバイスの空き容量 (KB) =} \\ & (\text{ファイルシステムに追加するデバイスファイルの容量 (KB)} \div \text{チャンクサイズ (KB)} \div 2) \times \\ & \text{最大予約世代数に応じた係数*} + 8192 \end{aligned}$$

あふれ防止動作を設定していない、かつファイルシステム拡張後の容量が1TBを超える場合

$$\begin{aligned} & \text{必要な差分格納デバイスの空き容量 (KB) =} \\ & (\text{ファイルシステムに追加するデバイスファイルの容量 (KB)} \div \text{チャンクサイズ (KB)} \div 2) \times \\ & \text{最大予約世代数に応じた係数*} + 8192 + 10485760 \text{ (KB)} + \\ & \uparrow \text{ファイルシステムに追加するデバイスファイルの容量 (KB)} \div 134217728 \uparrow \times \\ & \text{チャンクサイズ (KB)} \end{aligned}$$

(凡例)

↑ ↑ : 小数点以下を切り上げる

注※

- ・最大予約世代数が124の場合 : 1
- ・最大予約世代数が248の場合 : 2
- ・最大予約世代数が496の場合 : 4
- ・最大予約世代数が992の場合 : 8

5.8 差分スナップショットの自動作成の運用

ここでは、差分スナップショットの自動作成の概要および注意事項について説明します。自動作成には次に示す方法があります。

自動作成スケジュールを設定する

この場合、システム管理者は、毎週1回、毎月1回、特定の日時など差分スナップショットを自動的に作成するスケジュールを、1つのファイルシステムに対して最大で16個設定できます。また、作成と同時に、マウントおよび公開するように設定することもできます。

HFRR コピー用として作成することを設定する

この場合、15分ごとに HFRR コピー用として差分スナップショットが自動的に作成されます。ただし、作成と同時にマウントすることはできません。

なお、自動作成スケジュールの設定と HFRR コピー用として自動作成する設定を重ねて設定できません。

また、差分スナップショット作成のバックグラウンド処理に掛かる時間が15分を超えるおそれがある場合は、HFRR コピー用としてではなく、自動作成スケジュールを設定して自動作成するように

してください。差分スナップショット作成のバックグラウンド処理に掛かる時間については、「5.3.4 差分スナップショットの管理」を参照してください。

5.8.1 自動作成スケジュールの動作

ここでは、差分スナップショットの自動作成スケジュールを実行する際のシステムの動作を説明します。

(1) 差分スナップショットの自動作成の動作

自動作成された差分スナップショットには、次の形式で、自動的に名称が付与されます。

auto-〈作成間隔〉〈自動作成が開始された日時（形式：YYMMDDhhmm）〉

〈作成間隔〉は、スケジュールの設定によって次のとおり付与されます。

D

毎日作成するスケジュールを設定して作成された場合に付与されます。

W

毎週特定の曜日に作成するスケジュールを設定して作成された場合に付与されます。

M

毎月特定の日に作成するスケジュールを設定して作成された場合に付与されます。

A

毎年特定の日に作成するスケジュールを設定して作成された場合に付与されます。

(例) 毎年1月1日の14時00分に作成するスケジュールを設定して作成された差分スナップショットの名称

auto-A0601011400

1つのファイルシステムに対して複数のスケジュールが設定され、そのスケジュールが同時刻に差分スナップショットを作成するように設定された場合、差分スナップショットは1つしか作成されません。また、差分スナップショット名は、スケジュールの中で実行間隔がいちばん長いスケジュールを基に付与されます。

例えば、毎年1月1日14時00分に作成するスケジュールと毎月1日14時00分に作成するスケジュールを設定した場合は、2006年1月1日14時00分には差分スナップショットは1つしか作成されません。また、作成された差分スナップショットには、「auto-A0601011400」という名称が付与されます。

(2) 差分スナップショットの自動マウント・公開の動作

差分スナップショットの作成と同時にマウントおよび公開を行うようスケジュールを設定した場合は、作成された差分スナップショットがマウントされたあと、クライアントに公開されます。

マウントポイントは、設定したスケジュールを基に次の形式で設定されます。

/mnt/〈識別子〉〈作成間隔〉〈自動作成が開始された日時〉

マウントすると、ファイルシステム一覧画面でもマウントポイント名で差分スナップショットの情報を参照できるようになります。ただし、マウントした差分スナップショットに対して、ファイルシステム一覧画面から参照以外の操作はできません。

差分スナップショットはマウントされたあとに公開されます。差分スナップショットをクライアントに公開する方法として、次の方法を選択できます。

- 作成元のファイルシステムの共有内に公開する

- ・ 差分スナップショット自体にファイル共有を作成する
- ・ Volume Shadow Copy Service を使用して CIFS クライアントに公開する

それぞれの動作を次に説明します。

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する動作

ファイルシステムの共有内に差分スナップショットを公開する際に、差分スナップショット公開用のディレクトリ（.snaps）が作成されます。各差分スナップショットは、差分スナップショットの作成日時（形式：YYYY_MM_DD_hhmm）が名称として付与されたサブディレクトリに公開されます。差分スナップショットが公開されている共有内のディレクトリ構造の例を次の図に示します。

図 5-17 差分スナップショットが公開されている共有内のディレクトリ構造



なお、共有ディレクトリ下に .snaps という名称のファイルまたはディレクトリが存在する場合は、自動作成スケジュールの運用を開始する前に削除しておく必要があります。

差分スナップショットにファイル共有を作成する動作

共有ディレクトリ、CIFS 共有のアクセス権および CIFS 共有名以外の共有情報は、作成元のファイルシステムの情報が差分スナップショットに設定されます。CIFS 共有のアクセス権は、常に読み取り専用を設定されます。共有ディレクトリおよび CIFS 共有名は、設定したスケジュールおよび作成元のファイル共有の設定を基に、次の形式で設定されます。

共有ディレクトリ

/mnt/<識別子><作成間隔><自動作成が開始された日時>/<作成元のファイル共有のサブディレクトリ名>

CIFS 共有名

<作成元の CIFS 共有名><作成間隔><自動作成が開始された日時>※

注※ 作成元の CIFS 共有名の末尾がドル記号 (\$) の場合、作成される CIFS 共有名の末尾にドル記号 (\$) が付いた名称になります。

例えば、識別子に「fs01」を設定し、毎年 1 月 1 日の 14 時 00 分に作成するスケジュールを設定して作成された差分スナップショットは、次の設定でマウントおよびファイル共有が行われます。

表 5-11 自動作成された差分スナップショットのマウントおよびファイル共有の設定例

項目	作成元のファイルシステム	作成された差分スナップショット
名称	filesystem01	auto-A0601011400
マウントポイント	/mnt/filesystem01	/mnt/fs01A0601011400

項目	作成元のファイルシステム	作成された差分スナップショット
NFS 共有の共有ディレクトリ	/mnt/filesystem01/dir1_nfs	/mnt/fs01A0601011400/dir1_nfs
CIFS 共有の共有ディレクトリ	/mnt/filesystem01/dir2_cifs	/mnt/fs01A0601011400/dir2_cifs
CIFS 共有名	dir2_cifs	dir2_cifsA0601011400

システム管理者は、差分スナップショットを使用するクライアントに対して、作成される共有ディレクトリ名や CIFS 共有名を通知しておいてください。

差分スナップショットに対して作成されたファイル共有の情報を、File Services Manager で参照および変更できます。必要に応じて、ファイル共有の情報を編集してください。

差分スナップショットを Volume Shadow Copy Service を使用して公開する動作

マウントされている差分スナップショットが、Volume Shadow Copy Service を使用して CIFS クライアントに公開されます。CIFS クライアントが共有内にあるフォルダまたはファイルのプロパティを参照すると、[以前のバージョン] タブ内に差分スナップショットが一覧で表示されます。差分スナップショットをファイル共有内に公開したり、差分スナップショットに共有を作成したりする必要はありません。

Volume Shadow Copy Service を使用して公開する場合は、CIFS サービスの構成定義で Volume Shadow Copy Service を使用するよう設定してください。

特定のファイル共有に対して Volume Shadow Copy Service を使用して公開するかどうかについては、ファイル共有の属性で選択できます。

ただし、セカンダリーサイトの最新差分スナップショットを公開するために使用するファイルシステム（最新差分スナップショット公開用ファイルシステム）の場合は、Volume Shadow Copy Service を使用できません。

(3) 予約世代数または自動作成の上限数に達した場合のシステムの動作

スケジュールを設定・変更するときは、自動作成する差分スナップショットの上限（自動作成の上限数）を設定します。自動作成された差分スナップショットの数が上限に達していた場合、または作成済みの差分スナップショットの合計数が予約世代数に達していた場合には、次の条件を満たす差分スナップショットが削除の候補となります。

- ・ 名称が「auto-」で始まる
- ・ マウントされていないか、自動マウントの際に適用される形式に従ったマウントポイント名でマウントされている
- ・ Hitachi File Remote Replicator で使用されていない

削除候補となる差分スナップショットのうち、実際に削除される差分スナップショットは、自動作成の上限数の管理方法によって次のとおり異なります。

自動作成の上限数をファイルシステム全体で管理する場合

作成間隔に関わらず、作成日付の最も古い差分スナップショットが削除されます。

自動作成の上限数を作成間隔ごとに管理する場合

新たに自動作成される差分スナップショットと同じ作成間隔で、かつ作成日付の最も古い差分スナップショットが削除されます。

例えば、自動作成の上限数をファイルシステム全体で管理する場合に、予約世代数を 5 世代に設定して、自動作成スケジュールを運用すると仮定します。自動作成処理が開始された時点で、確保された差分スナップショットが次の表に示す状態であった場合は、2006 年 1 月 1 日 12 時 00 分に作成された差分スナップショットが削除対象になります。

表 5-12 自動作成処理が開始された時点で削除対象になる差分スナップショットの例（上限数をファイルシステム全体で管理する場合）

作成日時	差分スナップショット名	マウントポイント名	削除対象
2006/01/01 00:00	auto-A0601010000	fs01_autoA0101	対象外
2006/01/01 09:00	snap01	-	対象外
2006/01/01 12:00	auto-D0601011200	fs01D0601011200	対象
2006/01/01 15:00	auto-D0601011500	-	対象外
2006/01/01 18:00	snap02	fs01_snap02	対象外

（凡例） - : マウントされていない

また、自動作成の上限数を作成間隔ごとに管理する場合に、日次自動作成の上限数を 2 個に設定して、自動作成スケジュールを運用すると仮定します。日次のスケジュールによって自動作成処理が開始された時点で、確保された差分スナップショットが次の表に示す状態であった場合は、2009 年 2 月 2 日 9 時 00 分に作成された差分スナップショットが削除対象になります。

表 5-13 自動作成処理が開始された時点で削除対象になる差分スナップショットの例（上限数を作成間隔ごとに管理する場合）

作成日時	差分スナップショット名	マウントポイント名	削除対象
2009/01/01 00:00	auto-A0901010000	-	対象外
2009/01/31 23:45	auto-M0901312345	-	対象外
2009/02/01 00:00	auto-W0902010000	fs02W0902010000	対象外
2009/02/02 09:00	auto-D0902020900	fs02D0902020900	対象
2009/02/03 09:00	auto-D0902030900	fs02D0902030900	対象外

（凡例） - : マウントされていない

削除対象の差分スナップショットは非公開となり、アンマウントされます。なお、削除対象の差分スナップショットにファイル共有が作成されている場合は、手動で作成されたか、自動で作成されたかに関係なく、すべてのファイル共有が削除されます。

このため、重要なデータが格納されている差分スナップショットは、次に示す方法で保護することをお勧めします。

- ・ 手動でマウントしておく
- ・ Backup Restore の NDMP 機能を使用してテープ装置に退避しておく
- ・ Backup Restore のボリュームレプリケーション連携機能または Hitachi File Remote Replicator を使用して別の筐体やノードにコピーしておく

なお、自動作成されたすべての差分スナップショットが、手動でマウントされている場合は、エラーになります。

予約世代数または自動作成の上限数を変更したり、自動作成された差分スナップショットのうちで不要なものをアンマウントしたりして対処してください。

(4) 自動マウントの上限数に達した場合のシステムの動作

作成した差分スナップショットを自動的にマウント・ファイル共有するようにスケジュールを設定する場合は、マウントする差分スナップショットの上限（自動マウントの上限数）を設定します。自動マウントされた差分スナップショット数が上限に達している状態で自動マウントの処理が実行されると、次の条件を満たす差分スナップショットが、アンマウントの候補となります。

- ・ 名称が「auto-」で始まる

- ・ 自動マウントの際に適用される形式に従ったマウントポイント名でマウントされている

アンマウント候補となる差分スナップショットのうち、実際にアンマウントされる差分スナップショットは、自動作成の上限数の管理方法によって次のとおり異なります。

自動作成の上限数をファイルシステム全体で管理する場合

作成間隔に関わらず、作成日付の最も古い差分スナップショットがアンマウントされます。

自動作成の上限数を作成間隔ごとに管理する場合

新たに自動マウントされる差分スナップショットと同じ作成間隔で、かつ作成日付の最も古い差分スナップショットがアンマウントされます。

例えば、自動マウントの上限数をファイルシステム全体で管理する場合に、自動マウントの上限数を「2」に設定して、自動作成スケジュールを運用すると仮定します。自動マウント処理が開始された時点で、次の表に示す状態であった場合は、2006年1月1日12時00分に作成された差分スナップショットがアンマウント対象になります。

表 5-14 自動マウント処理が開始された時点でアンマウント対象になる差分スナップショットの例（上限数をファイルシステム全体で管理する場合）

作成日時	差分スナップショット名	マウントポイント名	アンマウント対象
2006/01/01 00:00	auto-A0601010000	fs01_autoA0101	対象外
2006/01/01 09:00	snap02	fs01_snap02	対象外
2006/01/01 12:00	auto-D0601011200	fs01D0601011200	対象
2006/01/02 21:00	auto-W0601022100	fs01W0601022100	対象外

また、自動マウントの上限数を作成間隔ごとに管理する場合に、日次自動マウントの上限数を「2」に設定して、自動作成スケジュールを運用すると仮定します。日次のスケジュールによって自動マウント処理が開始された時点で、次の表に示す状態であった場合は、2009年2月2日9時00分に作成された差分スナップショットがアンマウント対象になります。

表 5-15 自動マウント処理が開始された時点でアンマウント対象になる差分スナップショットの例（上限数を作成間隔ごとに管理する場合）

作成日時	差分スナップショット名	マウントポイント名	アンマウント対象
2009/02/01 00:00	auto-W0902010000	fs02W0902010000	対象外
2009/02/02 09:00	auto-D0902020900	fs02D0902020900	対象
2009/02/03 09:00	auto-D0902030900	fs02D0902030900	対象外

アンマウント対象の差分スナップショットは非公開になります。なお、アンマウント対象の差分スナップショットにファイル共有が作成されている場合は、手動で作成されたか、自動で作成されたかに関係なく、すべてのファイル共有が削除されます。

自動作成された差分スナップショットを公開し続けたい場合は、自動的にアンマウントされないように、手動でマウントしておくことをお勧めします。

5.8.2 自動作成スケジュールを運用する際の注意事項

差分スナップショットの作成・マウント・公開を自動化する場合は、次の点に注意して運用してください。

(1) スケジュールの設定に関する注意事項

スケジュールに設定する日時によっては、システム管理者が意図した時刻に差分スナップショットが自動作成されないことがあります。次の点に注意して自動作成する日時を設定してください。

- バックグラウンド処理中は、新たに差分スナップショットを作成できません。差分スナップショットの作成・削除の処理時間については、「5.3.4 差分スナップショットの管理」を参照してください。また、作成と同時にマウント・ファイル共有を行う場合は、差分スナップショットの作成の処理時間に加えて、作成するファイル共有の数だけ処理時間が長くなります。これらの処理時間を考慮して、次の条件式を満たすようにスケジュールの間隔を設定してください。

$$\text{自動作成スケジュールの間隔 (単位: 分)} > A + 0.8 \times n + 1$$

(凡例)

A: 差分スナップショットの作成および削除のバックグラウンド処理に掛かる時間
(単位: 分)

n: 作成元のファイルシステムに作成されたNFS共有とCIFS共有の合計数

- 差分スナップショットの自動作成が実行される際に、作成元のファイルシステムで、ほかの処理が行われていたり、オンラインバックアップの処理が行われていたりすると、差分スナップショットの自動作成が失敗するおそれがあります。作成が実行される前後の時間には、ファイルシステムに対して、自動作成以外の操作を実行しないでください。
- 同じ日時に複数のファイルシステムに対して自動作成スケジュールが設定されている場合は、1つの作成処理が完了してから、次の作成処理が開始されます。そのため、システム管理者が設定した時刻に、差分スナップショットの作成処理が開始されないおそれがあります。差分スナップショットの作成処理が同時に複数実行されないように、各ファイルシステムに設定する自動作成スケジュールを調整してください。
- 同じ名称の差分スナップショットがすでに存在した場合や、自動作成スケジュールの運用中にシステム管理者がタイムゾーンを変更したりサマータイムに切り替わったりした場合は、差分スナップショットが自動作成されないおそれがあります。例えば、差分スナップショットを作成するスケジュールがスキップされたり、スケジュールが実行されても名称が重複していることが原因で差分スナップショットの作成に失敗したりすることが想定されます。タイムゾーンを変更する前、またはサマータイムに切り替わる前には、スケジュールを見直して、意図する時刻に差分スナップショットを作成できる設定になっているかどうかを確認してください。

(2) 差分スナップショットを自動マウントする場合の注意事項

差分スナップショットが自動的にマウントされるためには、システムの運用状況が次の条件を満たしている必要があります。

- 作成元のファイルシステムがマウントされている
- クラスタ内 (Virtual Server 使用時は Virtual Server 内) に重複するマウントポイント名が存在しない
- 自動的にマウントされる差分スナップショットを含めて、マウントされる差分スナップショット数、および作成済みのファイルシステム数の合計が、クラスタまたはシングルノード当たり 256 個以下、Virtual Server 当たり 512 個以下である。また、Virtual Server 使用時はシステム全体で 6,144 個以下である

マウント処理を開始する時点で、どれかの条件を満たしていなかった場合は、差分スナップショットの作成処理は正常終了しますが、マウント処理は行われなくて処理が終了します。自動作成スケジュールの運用を開始する前に、運用状況を見直してください。運用開始後は、自動的にマウントされる差分スナップショットの数およびファイルシステムや差分スナップショットなどのマウントポイント名を考慮して、システムを運用してください。

(3) 差分スナップショットをファイルシステムの共有内に自動公開する場合の注意事項

フェールオーバーしたときにタイムアウトが発生するおそれがあるため、共有内に公開する差分スナップショット数を検討する際に次の条件式を満たす必要があります。

共有内に公開する差分スナップショット数を検討する際の条件式

$$\Sigma_1 (A \times B) + \Sigma_2 (A \times C \times D) \leq 4000$$

(凡例)

A: 共有ディレクトリ数*

B: 共有内に公開する差分スナップショット数

C: 過去バージョンのデータの保持期間 (日)

D: 一日当たりのマイグレーションタスクの実行回数 (回/日)

Σ_1 : 共有内に差分スナップショットを公開するファイルシステムでの合計

Σ_2 : 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での合計

注※ NFSプロトコルで複数の公開先を設定している場合は公開先ごとの共有ディレクトリ数 (共有ディレクトリ数×公開先数) となります。

なお、CIFSプロトコルだけを使用している場合は公開先数が1となります。

バージョン管理を利用したファイルの復元については、「6.1.5 バージョン管理を利用したファイルの復元」を参照してください。

検討例を次に示します。

- ・ システムでは、共有内に差分スナップショットを公開するファイルシステムと、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が、それぞれ1つ運用されている
- ・ 共有内に差分スナップショットを公開する共有ディレクトリ数は20
- ・ 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共有ディレクトリ数は10
- ・ NFSプロトコルでの公開先の数は各共有とも5
- ・ 過去バージョンの保持期間は30日
- ・ マイグレーションタスクは1日に1回実行される

このとき、共有内に公開する差分スナップショット数は次を満たす必要があります。

$$(20 \times 5) \times \text{共有内に公開するスナップショット数} + (10 \times 5) \times 30 \times 1 \leq 4000$$
$$\text{共有内に公開するスナップショット数} \leq 25$$

また、CIFSクライアントおよびNFSクライアントについて次の点に注意してください。

CIFSクライアントの注意事項

- 差分スナップショット公開用のディレクトリ (.snaps) には隠しファイル属性が設定されます。CIFSクライアントでは、次のどちらかの方法で参照できます。
 - ・ エクスプローラのリボンメニューで「すべてのファイルとフォルダを表示する」を設定する
 - ・ エクスプローラのアドレスバーに .snaps ディレクトリへのパスを指定する
- .snaps ディレクトリに対して名称変更などの操作は行わないでください。
- CIFS共有にホームドライブを設定している場合でも、クライアントはCIFS共有のトップディレクトリから差分スナップショットにアクセスする必要があります。事前にクライアントに差分スナップショットへのパスを通知しておいてください。

NFSクライアントの注意事項

- 差分スナップショット公開用のディレクトリ (.snaps) には隠しファイル属性が設定されます。NFSクライアントでは、.snaps ディレクトリへのパスを指定して参照します。
- .snaps ディレクトリに対して名称変更などの操作は行わないでください。

- NFSv2 または NFSv3 プロトコルを利用している NFS クライアントから、差分スナップショット内でファイルまたはディレクトリを操作する場合は、絶対パスを指定してください。相対パスを指定すると、意図したものとは異なるファイルまたはディレクトリが操作されるおそれがあります。
- NFSv2 または NFSv3 プロトコルを利用している NFS クライアントから、差分スナップショットのデータを作成元のファイルシステムにコピーする場合は、直接上書きしないでください。コピーが失敗するおそれがあります。次のどちらかの方法で、ファイル単位でコピーしてください。
 - ・差分スナップショットのデータをいったんクライアントマシンにコピーしてから、そのデータをファイルシステムにコピーする
 - ・差分スナップショットのデータをファイルシステムにいったん別名でコピーしてから、必要に応じて名前を変更する
 なお、どうしてもディレクトリ単位でコピーする必要がある場合は、「付録 F. NFS クライアントから共有内の差分スナップショットのデータをディレクトリ単位でコピーする方法」の手順に従ってコピーしてください。
- 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 プロトコルを利用するときは、共有内に公開した差分スナップショットを参照できません。参照する場合は NFSv2 または NFSv3 プロトコルを利用してください。NFSv4 プロトコルを利用する場合は、差分スナップショット自体にファイル共有を作成し、NFS クライアントで差分スナップショットの共有ディレクトリをマウントしてください。

(4) 差分スナップショットにファイル共有を自動作成する場合の注意事項

差分スナップショットにファイル共有を自動作成する場合は、次の点に注意して運用してください。

- ・ CIFS サービスの構成定義で、CIFS 共有の設定を自動的にリロードするよう設定されていることを確認してください。
- ・ 差分スナップショットにファイル共有を自動作成する場合、クラスタ内の NFS 共有および CIFS 共有の上限数はそれぞれ 256 個です。既存のファイル共有数と自動作成されるファイル共有数の合計がこれらの上限を超えないよう、自動作成スケジュールの運用を開始する前に、ファイルシステムや差分スナップショットなどに設定されているファイル共有情報を見直してください。
- ・ 差分スナップショットに NFS 共有が作成されるためには、作成元に設定された NFS 共有の共有ディレクトリの絶対パスが 48 文字以下であることが必要です。
また、CIFS 共有が作成されるためには、次の条件を満たしている必要があります。
 - 作成元の CIFS 共有名が 69 文字以内である
 - 作成元に設定された CIFS 共有の共有ディレクトリの絶対パスが 241 文字以下である
 - 差分スナップショットに設定される CIFS 共有名がノード内で重複していない
 自動作成されるファイル共有の中に上記の条件を満たしていないものがあつた場合は、そのファイル共有は作成されません(差分スナップショットの作成処理およびマウント処理は実行されず)。

(5) Volume Shadow Copy Service を使用して差分スナップショットを公開する場合の注意事項

CIFS クライアントに対してだけ、Volume Shadow Copy Service を使用して差分スナップショットを公開できます。NFS クライアントに差分スナップショットを公開する場合は、ファイルシステムの共有内に公開するか、差分スナップショットに共有を作成してください。

ただし、最新差分スナップショット公開用ファイルシステムの場合は、Volume Shadow Copy Service を使用できません。

(6) スケジュール設定後の注意事項

自動作成スケジュールを設定したあとは、次の点に注意して運用してください。

- 差分スナップショットを作成と同時にマウントおよびファイル共有する場合は、障害発生時に備えて定期的に共有 LU および OS ディスクを保存することをお勧めします。ただし、自動作成スケジュールに設定した日時と、保存時刻が重ならないように注意してください。
なお、Virtual Server を使用している場合は、共有 LU および OS ディスクの代わりに Virtual Server の設定情報を保存してください。
- 自動作成の上限数を、すでに自動作成された差分スナップショットの総数よりも小さな値に変更した場合、変更前に自動作成された差分スナップショットが変更後の上限数まで自動的に削除されることはありません。システム管理者が自動作成された差分スナップショットを手動で削除し、総数が増えた時点から、新たに設定した上限数での運用が開始されます。
- 自動マウントおよび公開を行う設定から行わない設定に変更しても、既存の差分スナップショットの状態は変更されません。また、自動マウントの上限数を、すでに自動マウントされている差分スナップショットの総数よりも小さな値に変更しても、差分スナップショットが変更後の上限数まで自動的にアンマウントされることはありません。システム管理者が自動マウントされた差分スナップショットを手動でアンマウントし、総数が増えた時点から、新たに設定した上限数での運用が開始されます。
- マウントポイントの識別子を変更しても、すでに自動マウントされている差分スナップショットのマウントポイント名は変更されません。次の自動マウントの処理から変更後の識別子がマウントポイント名に適用されます。なお、自動作成された差分スナップショットが上限に達した場合、作成済みの差分スナップショットの合計数が予約世代数に達した場合、または自動マウントされた差分スナップショットが自動マウントの上限に達した場合は、変更前の識別子で自動マウントされている差分スナップショットもアンマウントおよび削除の対象になります。

なお、差分スナップショットの自動作成、マウントおよびファイル共有が正常に行われたかどうかは、システムメッセージおよび SNMP トラップで確認できます。処理が正常に行われたことを示すシステムメッセージおよび SNMP トラップの通知を契機に、自動作成した差分スナップショットをマウント・アンマウントしたり、ファイル共有を作成・削除したりできます。

5.8.3 HFRR コピー用差分スナップショットの自動作成

自動作成スケジュールによって差分スナップショットを作成する場合、プライマリーサイトとセカンダリーサイトの同期間隔は最短で 1 日ですが、HFRR コピー用差分スナップショットの自動作成による方法の場合、同期間隔を 15 分にすることができます。

ここでは、HFRR コピー用の差分スナップショットを自動作成する際のシステムの動作を説明します。

(1) HFRR コピー用差分スナップショット自動作成の動作

HFRR コピー用の差分スナップショットは毎時 15 分ごと（00 分、15 分、30 分、45 分）に作成され、次の形式で、自動的に名称が付与されます。

copy-〈自動作成が開始された日時（形式：YYMMDDhhmm）〉

（例）2012 年 5 月 21 日 14 時 15 分に作成された差分スナップショットの名称

copy-1205211415

HFRR コピー用の差分スナップショットは、自動作成スケジュールによる自動作成の上限数とは無関係に3世代固定でローテートされますが、予約世代数には含まれます。このため、自動作成スケジュールも設定する場合は、自動作成スケジュールによる自動作成の上限数は予約世代数から3を引いた値を指定してください。なお、3世代のHFRR コピー用差分スナップショットが作成される前に予約世代数に達した場合は、KAQS11113-E メッセージが通知されます。また、事前に設定している場合はSNMP トラップまたはE-mailでも通知されます。

HFRR コピー用の差分スナップショットの作成時刻と自動作成スケジュールによる作成時刻が重なった場合は、自動作成スケジュールによって作成されます。これは、自動作成される差分スナップショット名が、スケジュールの中で実行間隔がいちばん長いスケジュールを基に付与されるためです。

例えば、毎日14時15分に作成するスケジュールとHFRR コピー用の差分スナップショットの作成を設定した場合、14時15分には差分スナップショットは1つだけ作成され、「auto-D1205211415」などの名称が付与されます。

フェールオーバーが発生した場合は、自動作成スケジュールによる場合と同様にフェールオーバー先で差分スナップショットが作成されます。ただし、差分スナップショットの作成中にフェールオーバーが発生した場合は、作成されないことがありますが、次回(15分後)作成されます。

(2) HFRR コピー用差分スナップショットのマウント・公開の動作

HFRR コピー用の差分スナップショットは作成と同時に自動マウントすることはできませんが、手動でマウントできます。マウントしたあと差分スナップショットをクライアントに公開する方法は自動作成スケジュールによる作成の場合と同じです。

なお、HFRR コピー用として作成された差分スナップショットをマウントした場合、ローテートの際に作成済み差分スナップショットの共有削除とアンマウントのあと、差分スナップショットが作成されます。

(3) HFRR コピー用差分スナップショットを自動作成する場合の注意事項

HFRR コピー用差分スナップショットを自動作成する場合は、次の点に注意して運用してください。

- 大量にI/Oが発生する運用環境、システムがビジー状態になる運用環境の場合にHFRR コピー用スナップショットを作成するように設定した場合は、15分間隔でスナップショットを作成できないおそれがあります。
- 自動作成スケジュールによる場合と異なり、差分スナップショットの作成に成功した場合、SNMP トラップやE-mailでは通知されず、ログ(/enas/log/syncimage.log)に出力されます。
- HFRR コピー用差分スナップショット自動作成の運用中にシステム管理者がタイムゾーンを変更したりサマータイムに切り替わったりした場合は、自動作成がスキップされたり、自動作成が実行されても名称が重複していることが原因で差分スナップショットの作成に失敗したりすることがあります。タイムゾーンを変更する前、またはサマータイムに切り替わる前には、意図する時刻に差分スナップショットを作成できる設定になっているかどうかを確認してください。
- HFRR コピー用差分スナップショットを自動作成する際、ファイルシステム1個当たり約20秒、排他によってHVFP/HDIのほかの処理を実行できない状態になります。このため、HFRR コピー用差分スナップショットの自動作成を利用するHFRR ペアの数は、サイト当たり(Virtual Serverの場合はVirtual Server 当たり)4以内とすることを推奨します。

5.9 Hitachi File Remote Replicator について

差分スナップショットを別サイトに遠隔バックアップする場合は、Hitachi File Remote Replicator を利用します。ここでは、Hitachi File Remote Replicator の概要、導入するとできること、使用する上でシステム管理者が知っておいた方がよいこと、使用上の注意事項について説明します。

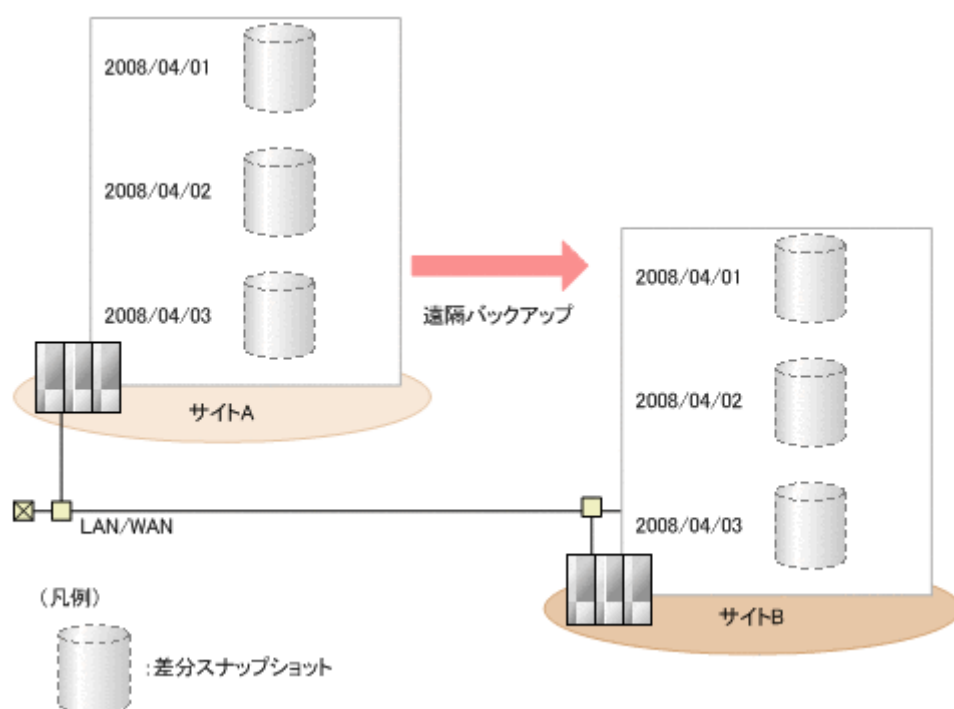
5.9.1 Hitachi File Remote Replicator とは

Hitachi File Remote Replicator は、ファイルスナップショット機能と連携して、あるサイトの差分スナップショットを別のサイトに遠隔バックアップし、複製するプログラムです。

Hitachi File Remote Replicator は、HCP にデータをマイグレートしないファイルシステムまたは階層化しないファイルシステムに対して使用できます。

Hitachi File Remote Replicator の概要を次に示します。

図 5-18 Hitachi File Remote Replicator の概要



Hitachi File Remote Replicator の特長は次のとおりです。

導入コストを削減できます

Hitachi File Remote Replicator では、LAN または WAN 経由でデータをコピーします。

TrueCopy や Universal Replicator などに比べて、安価に遠隔バックアップ環境を整備できます。

必要最小限のデータを遠隔バックアップします

初回のデータ転送以降は、前回のコピー時点と比較した差分データだけをバックアップ先のサイトに転送します。

業務に合わせて自動運用できます

サイト間のデータコピーは、システム管理者が手動で実行する方法以外に、特定の時間帯に自動的に実行する方法もあります。差分スナップショットの自動作成機能と組み合わせて Hitachi File Remote Replicator を運用することで、遠隔バックアップを自動化できるとともに、システム管理者の作業負担を軽減できます。

5.9.2 Hitachi File Remote Replicator でできること

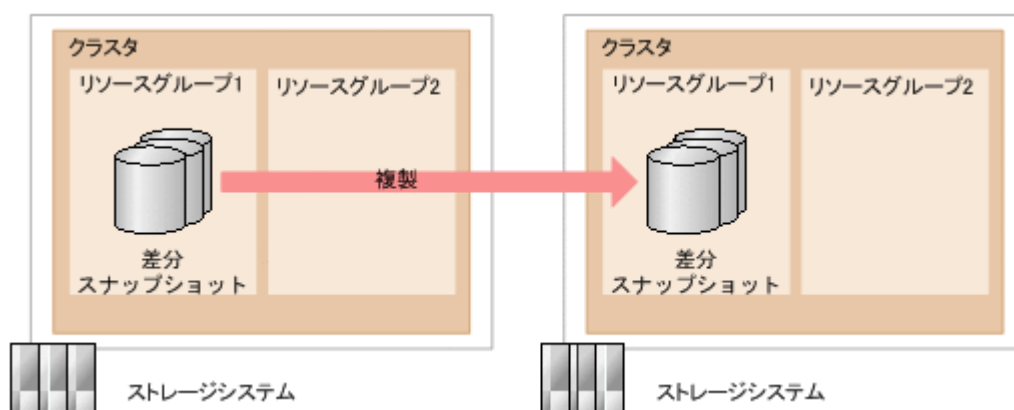
ここでは、Hitachi File Remote Replicator を導入することで実現できる、HVFP/HDI の運用について説明します。

(1) データ保全性の強化

ほかのサイトの HVFP/HDI に差分スナップショットを複製できます。また、複製先のサイトに存在する差分スナップショットでファイルシステムを回復することもできます。

異なるサイトに差分スナップショットを保管しておくことで、ファイルシステムのデータの保全性を高めることができます。WORM 対応ファイルシステムの場合、運用サイトがクラッシュしても、改変および削除を一定期間または無期限に抑止した WORM ファイルのデータを保全できます。

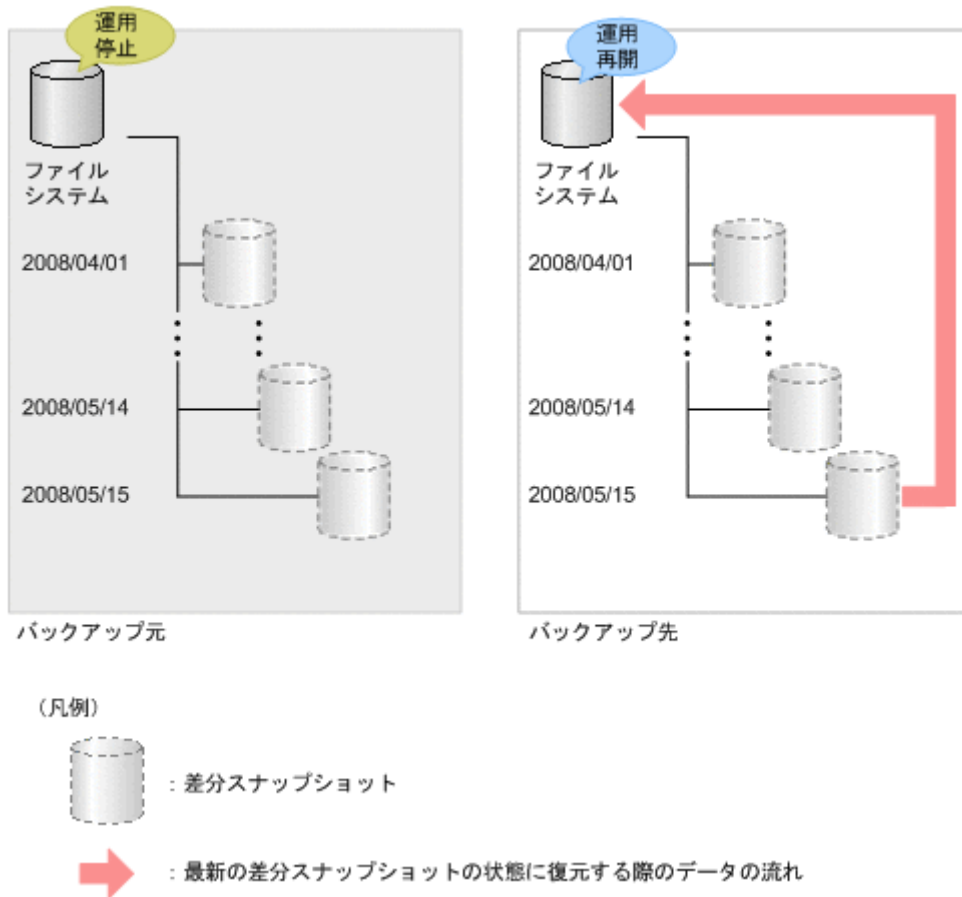
図 5-19 データ保全性の強化



(2) サイトの切り替え

バックアップ先のサイトのファイルシステムに運用を切り替えることができます。バックアップ元のファイルシステムの運用を停止しなければならない場合には、バックアップ先のサイトに存在する最新の差分スナップショットのデータを使って、業務を再開できます。

図 5-20 サイトの切り替え



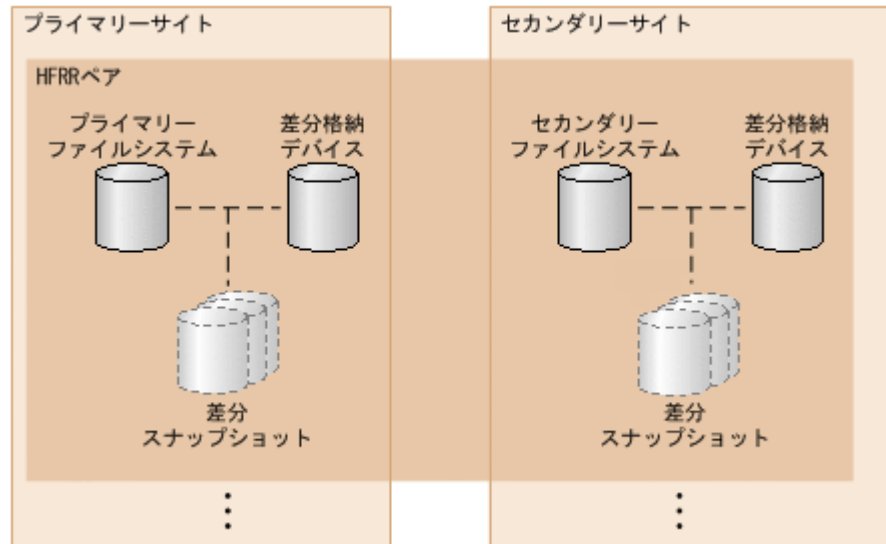
(3) ストレージ資源の有効利用

Hitachi File Remote Replicator を利用できるストレージシステムであれば、異機種ストレージシステムであってもバックアップ先として使用できます。このため、利用頻度の高い差分スナップショットは高性能のストレージシステムに保管し、利用頻度が低くなった差分スナップショットは安価のストレージシステムに保管するなどの DLCM (Data Life Cycle Management) を意識した HVFP/HDI の運用ができます。

5.9.3 ボリューム構成

Hitachi File Remote Replicator でのボリューム構成を次に示します。

図 5-21 ボリューム構成

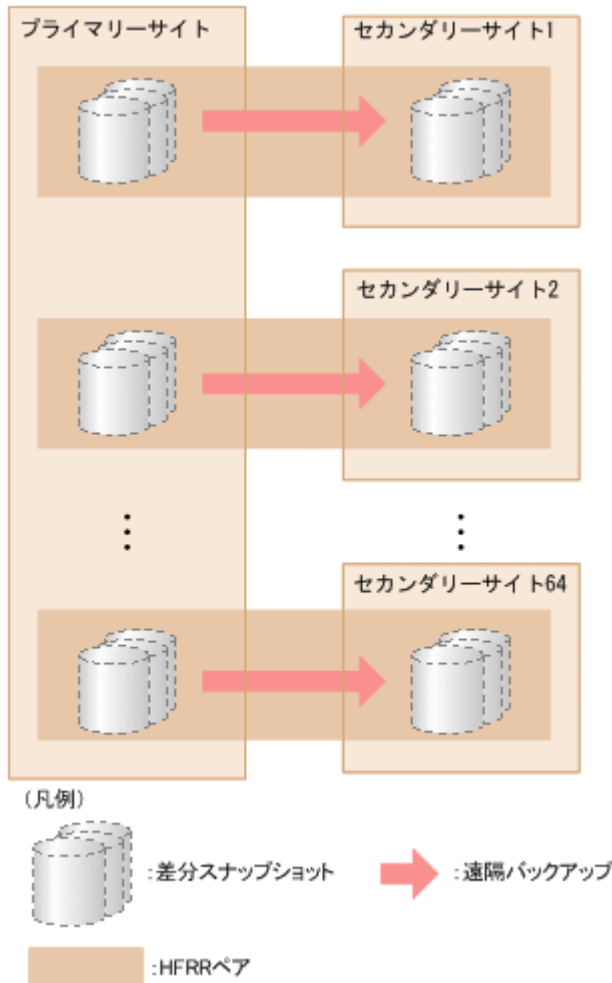


Hitachi File Remote Replicator では、バックアップ元のファイルシステムをプライマリーファイルシステム、バックアップ先のファイルシステムをセカンダリーファイルシステムと呼びます。それぞれのファイルシステムが属するサイトをプライマリーサイト、セカンダリーサイトといいます。

プライマリーファイルシステムとセカンダリーファイルシステムには、それぞれ差分格納デバイスを設定しておきます。差分格納デバイスが設定されたプライマリーファイルシステムと、差分格納デバイスが設定されたセカンダリーファイルシステムをペアとして定義したものを **HFRR ペア** と呼びます。

また、1つのサイトで複数のファイルシステムを運用している場合は、それぞれのファイルシステムの差分スナップショットを別々のサイトに遠隔バックアップすることもできます。Hitachi File Remote Replicator では、1サイト当たり最大で 64 サイト（シングルノード構成の場合は 32 サイト）と HFRR ペアを定義できます。

図 5-22 HFRR ペアの構成



5.9.4 セカンダリーサイトの最新差分スナップショット公開

セカンダリーサイトにコピーされた差分スナップショットをマウントしてファイル共有を設定すると、クライアントから参照できるようになりますが、この場合、目的の差分スナップショットごとにマウントとファイル共有の設定が必要になります。セカンダリーサイトの最新差分スナップショット公開を設定すると、最新差分スナップショット公開用ファイルシステムの常に同じ共有内で最新の差分スナップショット（ベースライン差分スナップショット）を参照できるようになります。セカンダリーサイトの最新差分スナップショット公開を設定する手順については、「ユーザーズガイド」を参照してください。

ここでは、セカンダリーサイトの最新差分スナップショットが公開される動作について説明します。

セカンダリーサイトの最新差分スナップショット公開を設定すると、コピーによって作成された差分スナップショットは、最新差分スナップショット公開用ファイルシステムのファイル共有内のサブディレクトリ（例：/mnt/hfrrmp/secfs1/.snaps/all/2012_05_01_1300）に自動的に公開されて、マウントポイントがシンボリックリンク（例：/mnt/hfrrmp/secfs1/.snaps/latest）されます。

クライアントからこのシンボリックリンクにアクセスすることでセカンダリーサイトの最新の差分スナップショットを常に参照できます。

図 5-23 セカンダリーサイトの最新差分スナップショット公開の概略



セカンダリーサイトの最新差分スナップショット公開を設定する場合の注意事項を次に示します。

- ・ セカンダリーサイトの最新差分スナップショット公開用ファイルシステムでは、Volume Shadow Copy Service を使用できません。
- ・ 最新差分スナップショット公開用ファイルシステムは、このための専用のファイルシステムとして使用してください。
ユーザーデータ用の任意のディレクトリやファイルを作成しないでください。
- ・ 最新差分スナップショット公開用ファイルシステム内にシステムによって作成されるディレクトリ（セカンダリーファイルシステムと同じ名前のディレクトリやその配下の .snaps 以下のディレクトリ）を削除しないでください。
ruspairdisable コマンドで HFRR ペアを無効化したり、ruspairdelete コマンドで HFRR ペアを解除したりすると、最新差分スナップショット公開のための .snaps 以下のディレクトリはいったん削除されます。しかし、ruspairenable コマンドで HFRR ペアを有効化したり、ruspairdefine コマンドで HFRR ペアを再定義したりしたあと HFRR コピーが完了すると、再生成されます。
- ・ クライアントから最新差分スナップショットの同じファイルに 30 分以上継続してアクセスすると、アクセスエラーになることがあります。アクセスエラーになった場合は、ファイルにアクセスし直してください。
- ・ CIFS クライアントが latest フォルダ内をエクスプローラで表示しているときに最新差分スナップショットが更新されても、エクスプローラの表示は自動更新されません。このため、latest フォルダ内のファイル操作に失敗した場合は、CIFS クライアントで [F5] キーを押すなどして、エクスプローラの表示を最新状態にし、操作対象のファイルが存在しているかどうかを確認してください。

5.9.5 サイト間でのデータコピーの仕組み

Hitachi File Remote Replicator では、次のどちらかの形態で、プライマリーサイトの差分スナップショットのデータがセカンダリーファイルシステムに反映されます。

- ・ 全コピー
- ・ 差分コピー

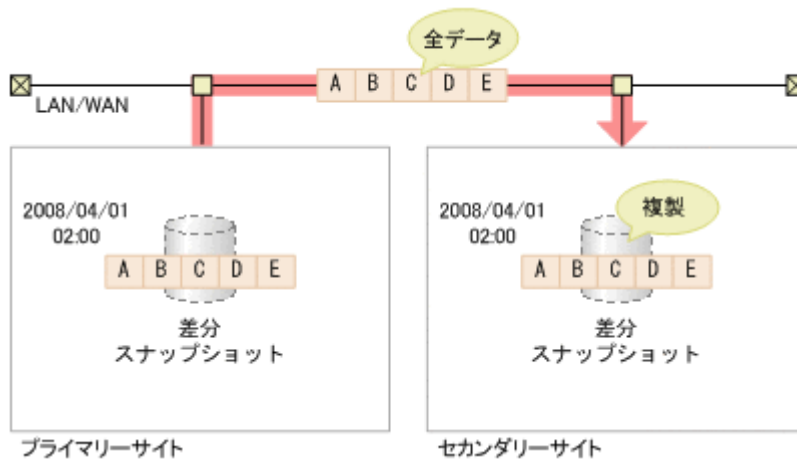
システム管理者は、HFRR ペアを定義したあとに、プライマリーサイトの差分スナップショットをセカンダリーサイトに手動でコピー（全コピー）します。初回のコピー以降は、プライマリーサイトの差分スナップショットのデータをセカンダリーサイトに、自動または手動で定期的にコピー（差分コピー）します。

ここでは、全コピーと差分コピーの仕組みについて説明します。

(1) 全コピーの処理の概略

全コピーの処理の概略を次に示します。

図 5-24 全コピーの処理の概略

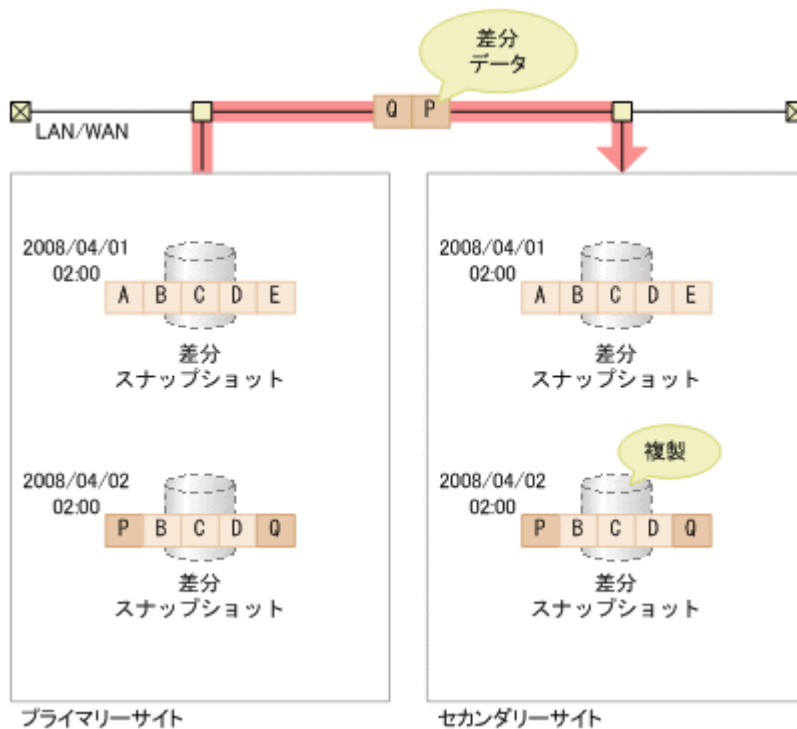


全コピーでは、コピー対象の差分スナップショットの全データがセカンダリーサイトへ転送され、差分スナップショットが複製されます。

(2) 差分コピーの処理の概略

差分コピーの処理の概略を次に示します。

図 5-25 差分コピーの処理の概略



差分コピーでは、直前のコピー処理で対象となった差分スナップショット（ベースライン差分スナップショット）の取得時点から、今回のコピー対象の差分スナップショットの取得までに更新されたデータがセカンダリーサイトに転送されます。

5.9.6 使用上の注意事項

Hitachi File Remote Replicator を使用する上での注意事項を次に示します。

- Hitachi File Remote Replicator は、プライマリーサイトで作成が完了した差分スナップショットを、手動で随時または決まった時間に自動的にセカンダリーサイトにコピーするためのプログラムです。プライマリーサイトのファイルシステムに対する更新を即時にコピーするというものではありません。
- システム管理者は、もう一方のサイトのシステム管理者と連携して、Hitachi File Remote Replicator を運用する必要があります。
- バックアップ先のサイトに切り替えてファイルシステムを運用する場合、バックアップ先のサイトでもバックアップ元のサイトと同様のシステム環境(ファイルシステムにアクセスするクライアントの認証など)を構築する必要があります。

5.10 Hitachi File Remote Replicator を使用する場合の運用設計

システム管理者は、ファイルシステムや差分スナップショットなどの利用形態を踏まえて、Hitachi File Remote Replicator の運用設計を行い、運用環境を構築します。運用環境を構築したら、プライマリーサイトの差分スナップショットのデータをセカンダリーサイトに定期的にコピーします。なお、プライマリーファイルシステムを利用できなくなった場合には、システム管理者はセカンダリーファイルシステムに運用を切り替えることもできます。

ここでは、Hitachi File Remote Replicator の運用を開始するに当たり、システム管理者が実施する作業について説明します。

5.10.1 ファイルシステムの運用設計

システム管理者は、HVFP/HDI の運用方針やセカンダリーサイトの用途などを考慮して、両サイトのファイルシステムを準備します。セカンダリーファイルシステムにはプライマリーファイルシステム以上のブロック容量が必要です。

注意：

プライマリーファイルシステムとセカンダリーファイルシステムのブロック容量の差が大きい場合は、セカンダリーファイルシステムで使用されない領域ができます。このため、ブロック容量が同程度のファイルシステムを用意することをお勧めします。

5.10.2 差合格納デバイスの運用設計

システム管理者は、プライマリーファイルシステムとセカンダリーファイルシステムの両方に差合格納デバイスを設定する必要があります。

(1) セカンダリーファイルシステムの差合格納デバイスの設計

セカンダリーファイルシステムに差分スナップショットがコピーされている間に次に示す状態になると、セカンダリーサイトの差分スナップショットが自動的に削除されます。

セカンダリーサイトの差分スナップショット数がファイルスナップショット機能で設定した予約世代数に達した場合

削除されるのはベースライン差分スナップショット以外のマウントされていない最も古い差分スナップショットです。

セカンダリーサイトの差合格納デバイスに十分な空き容量がなくなった場合

削除されるのはベースライン差分スナップショット以外の差分スナップショットです。コピーに必要な空き容量に達するまで、最も古いものから順に削除対象になります。

なお、削除できなかつたり、十分な空き容量を確保できなかつたりすると、コピー処理がエラーになります。セカンダリーサイトの差分格納デバイスを最大限活用するには、セカンダリーファイルシステムにファイルスナップショットのあふれ防止機能を設定しないでください。また、セカンダリーファイルシステムの差分格納デバイスの容量は、このことを考慮して見積もってください。

差分格納デバイスに必要なおおよその容量は、次の値の積から見積もることができます。

- 予約世代数

セカンダリーサイトに保管する差分スナップショットの数が該当します。

- 1回の差分コピーでセカンダリーサイトに転送されるデータ量 (単位: MB)

Hitachi File Remote Replicator でコピー対象にする差分スナップショット間でのデータ更新量を見積もってください。

1回当たりの差分コピーのデータ量は次の式で計算できます。

1回当たりの差分コピーのデータ量の見積もり式 (ファイルシステムが 256GB 未満の場合)

1回当たりの差分コピーのデータ量 (MB)

$$= (A \times F) \div (2 \times E) + 128 + (B \times C + (E \div 1024) \times 3 + 133) + 33 \times D$$

(凡例)

- A : 設定元のファイルシステムの容量 (単位: MB)
- B : ファイルシステムに対する1時間あたりに更新するデータ量 (単位: MB/時間)
- C : 差分スナップショットの作成間隔 (単位: 時間)
- D : 差分格納デバイスを構成するデバイスファイルの数
(シングルノード構成の場合は0を指定)
- E : チャンクサイズ (単位: KB)
- F : 予約世代数に応じた係数
予約世代数が3~124の場合 : 1
予約世代数が125~248の場合 : 2
予約世代数が249~496の場合 : 4
予約世代数が497~992の場合 : 8

1回当たりの差分コピーのデータ量の見積もり式 (ファイルシステムが 256GB 以上の場合)

1回当たりの差分コピーのデータ量 (MB)

$$= (A \times F) \div (2 \times E) + 128 + (B \times C + (E \div 1024) \times (A \div 131072) + 165) + 33 \times D$$

(凡例)

- A : 設定元のファイルシステムの容量 (単位: MB)
- B : ファイルシステムに対する1時間あたりに更新するデータ量 (単位: MB/時間)
- C : 差分スナップショットの作成間隔 (単位: 時間)
- D : 差分格納デバイスを構成するデバイスファイルの数
(シングルノード構成の場合は0を指定)
- E : チャンクサイズ (単位: KB)
- F : 予約世代数に応じた係数
予約世代数が3~124の場合 : 1
予約世代数が125~248の場合 : 2
予約世代数が249~496の場合 : 4
予約世代数が497~992の場合 : 8

(2) プライマリーファイルシステムの差分格納デバイスの設計

プライマリーファイルシステムの差分格納デバイスのチャンクサイズは、セカンダリーファイルシステムの差分格納デバイスのチャンクサイズと一致させる必要があります。両ファイルシステムのチャンクサイズが一致していない場合、HFRR ペアとして定義できません。

なお、ファイルスナップショットのあふれ防止機能を設定した場合、差分格納デバイスの空き容量があふれ防止動作を開始する閾値に達すると、あふれ防止の警告閾値を下回るまで、プライマリーサイトの差分スナップショットが次に示す順序で削除されます。

1. ベースライン差分スナップショット、コピー中の差分スナップショット以外の差分スナップショット
あふれ防止動作の設定に応じて、作成日付の古い順または新しい順に削除されます。
2. ベースライン差分スナップショット
1の処理をしても警告閾値を下回らない場合に削除されます。
3. コピー中の差分スナップショット
1および2の処理をしても警告閾値を下回らない場合に削除されます。

ベースライン差分スナップショット、コピー中の差分スナップショットが削除された場合、HFRRペアの再作成が必要になります。このため、ベースライン差分スナップショット、コピー中の差分スナップショットが削除されない運用ができるように、プライマリーファイルシステムの差分格納デバイスを見積もってください。

プライマリーファイルシステムの差分格納デバイスの容量の見積もり方法については、「5.5 差分格納デバイスの容量の設計」を参照してください。

5.10.3 Hitachi File Remote Replicator の運用設計

システム管理者は、ファイルシステムや差分格納デバイスの運用設計の結果に基づき、Hitachi File Remote Replicator の運用方針を検討します。

なお、HFRR ペア数の上限は、HVFP/HDI のノードのメモリー量や Virtual Server に割り当てたメモリー量によって異なります。HFRR ペア数の上限を次に示します。

表 5-16 HFRR ペア数の上限（クラスタ構成の場合）

HVFP/HDI のノードのメモリー量	1 サイト当たりの HFRR ペア数の上限
6GB	24
12GB	48
16GB 以上	64

注意：

クラスタ構成のノード上に複数の Virtual Server が存在する場合、全 Virtual Server の HFRR ペア数の合計が、ここに示した 1 サイト当たりの上限を満たす必要があります。

表 5-17 HFRR ペア数の上限（シングルノード構成の場合）

HVFP/HDI のノードのメモリー量	1 サイト当たりの HFRR ペア数の上限
4GB	8
6GB	12
12GB	24
16GB	32

表 5-18 HFRR ペア数の上限（Virtual Server の場合）

HVFP/HDI の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)	Virtual Server 当たりの HFRR ペア数の上限
6GB	2~3 未満	2
	3~4	5

HVFP/HDI のノードの メモリー量	Virtual Server に割り当てた メモリー量 (GB 単位)	Virtual Server 当たりの HFRR ペア数の上限
12GB	2～3 未満	2
	3～4 未満	5
	4～5 未満	8
	5～6 未満	10
	6～8	11
16GB 以上	2～3 未満	2
	3～4 未満	5
	4～5 未満	8
	5～6 未満	10
	6～85*	11

注※

Virtual Server に割り当てることができるメモリー量の上限値はノードのメモリー量によって異なります。Virtual Server に割り当てることができるメモリー量の上限値については、「仮想サーバ環境セットアップガイド」を参照してください。

(1) HFRR ペア名の検討

HFRR ペアには名称を付与する必要があります。ペアとして運用する各サイトで、HFRR ペア名が一意になるように設定してください。

(2) コピー対象の差分スナップショットとコピー時間帯の検討

HVFP/HDI の負荷が高いときには、差分コピーに掛かる時間が長くなることがあります。このため、システム管理者は、次に示すことを考慮して、自動コピーの起動時間帯を検討してください。

- ・ プライマリーサイトで差分スナップショットを自動的に作成する時間帯
- ・ HVFP/HDI 全体に対する負荷
- ・ 差分コピーに掛かる時間（コピー対象となる差分データ量）
- ・ ノード上に複数の Virtual Server が存在する場合は各 Virtual Server での自動コピーの起動時間帯を特定の時間帯に集中させない

(3) セカンダリーサイトでのファイル共有作成のための検討

一時的にサイトを切り替えてファイルシステムの運用を継続する場合、セカンダリーサイトでファイル共有を作成する必要があります。

セカンダリーサイトの状況を次の表に示す条件と照らし合わせて、セカンダリーサイトでのファイル共有作成の運用を決めてください。条件を満たしていれば、プライマリーサイトでバックアップしたファイル共有の情報をセカンダリーサイトにリストアすることで作成できます。満たしていなければ、プライマリーサイトでバックアップしたファイル共有の情報からセカンダリーサイトの環境に合わせたスクリプトファイルを作成して実行することで作成できます。

表 5-19 セカンダリーサイトでのファイル共有作成のための検討項目と条件

項目	条件
CIFS と NFS に共通する項目	ファイルシステム名 セカンダリーファイルシステムがプライマリーファイルシステムと同じ名前である。
CIFS に関する項目	CIFS 共有名 セカンダリーファイルシステムにプライマリーファイルシステムと同じ名前の CIFS 共有を作成できる。

項目		条件
	CIFS 共有に設定するホスト名およびネットワーク名	プライマリーファイルシステムの CIFS 共有に設定されているホスト名およびネットワーク名をセカンダリーサイトで解決できる。
	CIFS 共有に設定するユーザー名およびグループ名	プライマリーファイルシステムの CIFS 共有に設定されているユーザー名およびグループ名をセカンダリーサイトで使用できる。
	CIFS サービスの設定	次に示す項目の内容が両サイトで一致している。 <ul style="list-style-type: none"> • Authentication mode 登録されているサーバが同じ内容の認証情報を保持している。 • CIFS access log • Volume Shadow Copy Service
NFS に関する項目	NFS 共有に設定する公開先ホスト名	プライマリーファイルシステムの NFS 共有に設定されている公開先ホスト名をセカンダリーサイトで解決できる。
	NFS 共有に設定するユーザー ID およびグループ ID	プライマリーファイルシステムの NFS 共有に設定されているユーザー ID およびグループ ID をセカンダリーサイトで使用できる。
	NFS サービスの設定	次に示す項目の内容が両サイトで一致している。 <ul style="list-style-type: none"> • Domain name • KDC server name(s) 登録されているサーバが同じ内容の認証情報を保持している。

これらの項目は、GUI またはコマンドで設定、参照できます。

5.10.4 運用上の注意事項

ここでは、Hitachi File Remote Replicator を運用する上で、ファイルシステムの違いに関係なく考慮することと、WORM 対応ファイルシステムの場合に考慮することを分けて説明します。

(1) ファイルシステムの違いに関係なく考慮すること

システム管理者は次のことを考慮して、両サイトの差分スナップショットを計画的に運用してください。

- HFRR ペアを定義する際のプライマリーサイトおよびセカンダリーサイトのホスト名には、仮想 IP アドレスに接続できるホスト名または IP アドレス (IPv6 の場合は角括弧 ([]) で囲む) を指定してください。
- 両サイトのベースライン差分スナップショットを削除しないでください。
片方のサイトでベースライン差分スナップショットが削除された場合、HFRR ペアを解除したあと、再定義と全コピーを実施する必要があります。
- プライマリーサイトのベースライン差分スナップショットが、常にマウントされているように運用してください。
- コピー処理中は、プライマリーサイトのコピー対象の差分スナップショットに対して、マウント操作は実行できません。
プライマリーサイトでコピー対象の差分スナップショットのデータをクライアントに参照させる場合には、あらかじめマウントしておいてください。
- HFRR ペアが有効な状態では、セカンダリーファイルシステムの差分スナップショットの作成や、有効な自動作成スケジュールの設定など、ファイルスナップショット機能の一部の操作ができなくなります。

HFRR ペアを無効化した状態で、セカンダリーファイルシステムの差分スナップショットを作成した場合、HFRR ペアを再度有効化する際には、セカンダリーサイトの差分スナップショットを削除する必要があります。

- コピー対象の差分スナップショットの名称を確認した上で、コピーしてください。
コピー対象の差分スナップショットと同じ名称の差分スナップショットがセカンダリーサイトに存在すると、コピー処理がエラーになります。
- システムの構成や負荷によっては、コマンドを実行してからコピー処理が開始されるまでに時間が掛かることがあります。コピー処理が開始されると、`ruspairlist` コマンドでその HFRR ペアのコピー状況を参照できます。
- 自動コピーの運用中にシステム管理者がタイムゾーンを変更したりサマータイムに切り替わったりした場合は、コピーされないおそれがあります。タイムゾーンを変更する前、またはサマータイムに切り替わる前には、自動コピー起動時間帯を見直して、意図するコピーが実行される設定になっているかどうかを確認してください。
- HFRR ペアを無効化すると、ペアを構成するファイルシステムの容量を拡張できます。
両サイトのファイルシステムの容量を拡張したあと HFRR ペアを有効化しただけでは、セカンダリーファイルシステムの容量はベースライン差分スナップショットを取得したときのファイルシステムの容量になります。拡張後のファイルシステムの容量にするには、容量を拡張したあとに作成された差分スナップショットを、コピーしてください。なお、コピー前に HFRR ペアを解除すると、セカンダリーファイルシステムの再構築が必要になります。
- Hitachi File Remote Replicator で使用していたファイルシステムは、作成したときよりも容量が小さくなっていることがあります。このため、HFRR ペアを定義する場合は、`rusfspermit` コマンドに `--status` オプションを指定して、HFRR ペアを構成するファイルシステムの容量についての条件を満たしていることを確認するようにしてください。
- セカンダリーサイトには差分スナップショット単位でコピーされます。このため、サイト切り替えの際に、「ユーザーズガイド」に示すプライマリーサイトの計画停止の手順を実行できないと、ベースライン差分スナップショット作成時よりもあとにプライマリーサイトで更新されたファイルは、その差分がセカンダリーサイトに反映されないこととなります。なお、差分スナップショットの作成は、そのバックグラウンド処理に最大 2 時間掛かるおそれがあるため、プライマリーサイトでの差分スナップショットの作成と Hitachi File Remote Replicator によるコピーのスケジュールは、次のように設定することを推奨します。
 - プライマリーサイトでの差分スナップショットの作成は、2 時間おきとなるようにスケジュールする。
 - 常時コピーされるように、自動コピー起動時間帯を 24 時間にします。なお、プライマリーサイトでの差分スナップショット作成のバックグラウンド処理が 15 分以内で完了することが見込める場合は、HFRR コピー用として 15 分ごとに自動作成される差分スナップショットをコピー対象とすることができます。この場合、自動コピー起動時間帯は 24 時間にしてください。差分スナップショット作成のバックグラウンド処理に掛かる時間については、「5.3.4 差分スナップショットの管理」を参照してください。

(2) WORM 対応ファイルシステムの場合に考慮すること

WORM 対応ファイルシステムを Hitachi File Remote Replicator で運用する場合は、次に示すことも考慮して運用してください。

HFRR ペアの定義について

- 一方が WORM 対応ファイルシステムでもう一方が WORM 対応ファイルシステムではない場合、HFRR ペアとして定義できません。
WORM 対応ファイルシステム同士であれば、WORM 属性値が異なっても HFRR ペアとして定義できます。

- **WORM** 対応ファイルシステムで **HFRR** ペアを定義する場合、セカンダリーとするファイルシステムにリテンション期間が残っている **WORM** ファイルが存在していると、**HFRR** ペアとして定義できません。

このため、**WORM** 対応ファイルシステムの **HFRR** ペアを解除した場合、同じファイルシステム同士で再度 **HFRR** ペアを定義することはできません。

WORM 対応ファイルシステムの WORM 属性値について

WORM 属性値が異なっている状態で定義した **HFRR** ペアの場合、コピーが完了すると、セカンダリーファイルシステムの **WORM** 属性値はプライマリーファイルシステムと同じになります。

コピー開始時の両サイトの時刻について

WORM 対応ファイルシステムの **HFRR** ペアの場合、コピー開始時に両サイトの時刻が 1 時間以上ずれていると、コピーできません。自動コピーの開始時に両サイトの時刻が 1 時間以上ずれていると、自動コピーの設定も解除されます。

サイト切り替えについて

WORM 対応ファイルシステムの **HFRR** ペアの場合も、プライマリーファイルシステムでの業務を継続できなくなったときには、サイト切り替えによってセカンダリーファイルシステムで業務を継続できます。なお、サイト切り替え時に無効化したセカンダリーファイルシステムをマウントした場合、プライマリーサイトでの運用再開は必ず、「ユーザズガイド」に示す、計画停止後の運用再開の手順で実行してください。

HFRR ペアとして運用する WORM 対応ファイルシステムの業務での使用について

WORM 対応ファイルシステムの **HFRR** ペアを無効化した場合、業務で使用できるファイルシステムはプライマリーかセカンダリーのどちらか一方だけになります。例えば、セカンダリーファイルシステムをマウントした場合、業務で使用できるのはセカンダリーファイルシステムとなります。なお、**WORM** 対応ファイルシステムの **HFRR** ペアを無効化した場合に、業務で使用できるファイルシステムがどちらなのかは、`-v` オプションを指定して `ruspairlist` コマンドを実行することで確認できます。

HCP と連携して運用を開始する前に

この章では、HCP と連携して HVFP/HDI の運用を開始するに当たり、システム管理者が理解または考慮する必要があることについて説明します。

- 6.1 マイグレーションを管理するための機能
- 6.2 HCP と連携する前に確認すること

6.1 マイグレーションを管理するための機能

HVFP/HDI と HCP を連携することで、システム管理者が設定したポリシーに従って、HVFP/HDI のファイルシステムのデータを HCP のネームスペースにマイグレートできます。システム管理者は、対象のファイルシステムに対するマイグレーションの条件をポリシーとして設定します。設定したポリシーは、マイグレーションタスクとして指定したスケジュールに従って実行されます。また、HCP にマイグレートしたデータをほかの HVFP/HDI と共有することもできます。

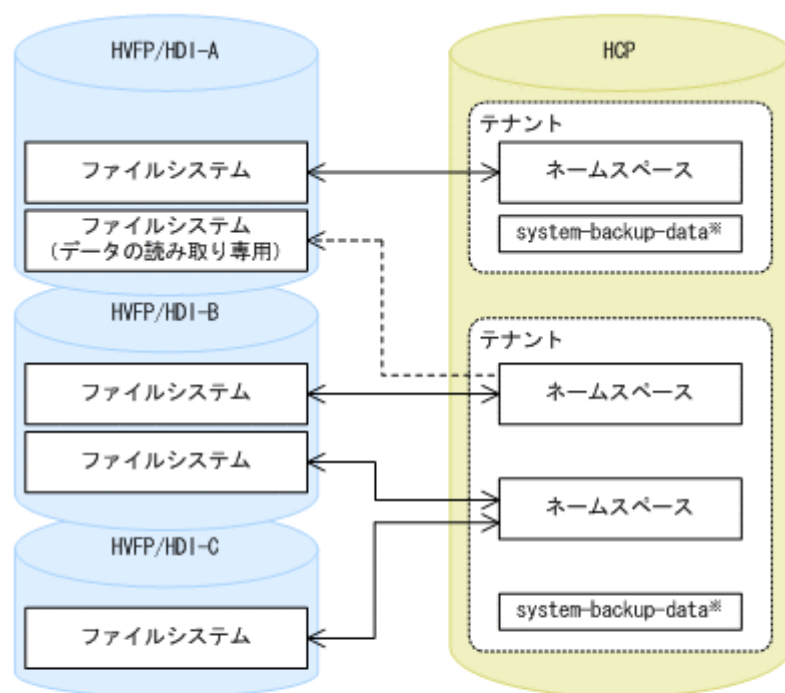
ここでは、HVFP/HDI から HCP へのマイグレーションを管理するための機能について説明します。

6.1.1 ファイルシステムとネームスペースの対応

HVFP/HDI のシステムに対して、HCP の 1 つのテナントを割り当てます。HCP の 1 つのテナントは、複数の HVFP/HDI に割り当てることができます。HCP にマイグレートされたデータをほかの HVFP/HDI と共有するときは、複数の HVFP/HDI からマイグレート先のネームスペースにアクセスできるため、1 つのネームスペースに対して複数のファイルシステムを対応づけられます。

HVFP/HDI のファイルシステムとマイグレート先のネームスペースの対応を次の図に示します。

図 6-1 ファイルシステムとテナントおよびネームスペースの対応



(凡例)

- ↔ : HCP へのマイグレーションおよび HVFP/HDI へのリコールを実行する
- ←--- : ほかの HVFP/HDI からマイグレートされた HCP のデータを読み取り専用で参照する

注※ システム設定情報ファイルを HCP に保存する場合に必要なネームスペースです。同じテナントを複数の HVFP/HDI がデータのマイグレーション先として使用する場合は、システム設定情報の保存先として 1 つのネームスペースを複数の HVFP/HDI で共用します。

6.1.2 ファイルのスタブ化

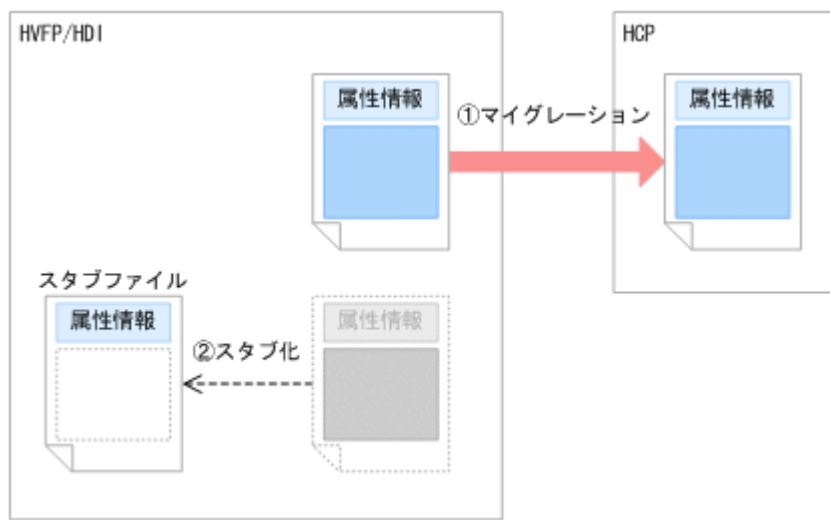
マイグレーションタスクで設定した実行日時になると、マイグレーションポリシーに従って、ファイルシステム内の対象ファイルのデータが HCP にマイグレートされます。

マイグレートされたファイルは、スタブ化されることで属性情報だけが残った状態（スタブファイル）になります。ファイルのスタブ化は、マイグレーションタスクで設定した日時とは別に HVFP/HDI で定期的の実施されます。また、ファイルがスタブ化される際にファイルシステムの残容量が閾値（初期導入時は 10%）より小さければ、アクセス日時の古いファイルから順番に、ファイルシステムの残容量が閾値を上回るまでスタブ化されます。

ただし、HCP でレプリケーション機能を運用していない場合は、`arc replimitset` コマンドで、スタブ化が開始される閾値となるファイルシステムの残容量を `0GB` に設定して、ファイルがスタブ化されないようにしてください。スタブ化が実施されている場合、HCP および HVFP/HDI の両方に障害が発生したときに、スタブ化されているファイルのデータを回復できないおそれがあります。

ファイルのスタブ化について次の図に示します。

図 6-2 ファイルのスタブ化



6.1.3 データ転送前後の内部処理

大量のファイルをマイグレートする場合にも実行時間を短縮できるように、HCP へのデータ転送処理の前後で、対象ファイルの一覧を生成する内部処理が発生します。なお、後処理では、マイグレーションに失敗しているファイルを次回マイグレートするための一覧が生成されます。

対象ファイルの一覧は、ファイルやディレクトリの更新、作成またはリネームなどのイベント情報を基に生成されます。HCP へのデータ転送処理時間は対象のファイルのデータ量やネットワーク環境などに応じて異なりますが、対象ファイルの一覧を生成するときの処理時間はイベント数に応じて異なります。

前処理または後処理の状態は、GUI に表示されるタスクのステータスと同期しないことがあります。例えば、前処理が実行されている状態でマイグレーションタスクを停止しても、対象ファイルの一覧の作成処理が完了するまで前処理は停止しません。また、後処理はバックグラウンドで実行されるため、GUI にはタスクが完了しているステータスが表示されます。

マイグレーションタスクの処理状況と、GUI に表示されるステータスや処理時間の影響因子について次に示します。

表 6-1 タスクの処理状況と、GUI に表示されるステータスや処理時間の影響因子との対応

タスクの処理状況	[タスク管理] ダイアログの [タスクリスト] ページに表示される情報		処理時間の影響因子
	[現在のステータス]	[進捗]	
未実行	「Standby」または「Scheduled」	「-/ (-)」	なし
前処理	「Running」	「calculating」	イベント数
データ転送		<処理済みのファイルおよびディレクトリ数> / <総ファイルおよびディレクトリ数> (<進捗>%)	対象のファイルのデータ量やネットワーク環境など
Quota 情報のバックアップ		「post-command executing」	
後処理	「Standby」または「Scheduled」	「-/ (-)」	イベント数

前処理または後処理中にマイグレーションタスクが実行されると、KAQM37142-E メッセージを出力して失敗します。arctaskstatus コマンドで前処理または後処理の進捗を確認してください。前処理または後処理に時間が掛かる場合は、タスクのスケジュールを設定する際に指定する打ち切り時間を長くするか、タスクを実行する際に初期モードを使用するように arcmodect1 コマンドで設定してください。

6.1.4 HVFP/HDI へのリコール

HVFP/HDI のクライアントからスタブファイルにアクセスすると、HCP にマイグレートされたデータがスタブファイルに書き込まれるため、ファイルを参照または編集できます。

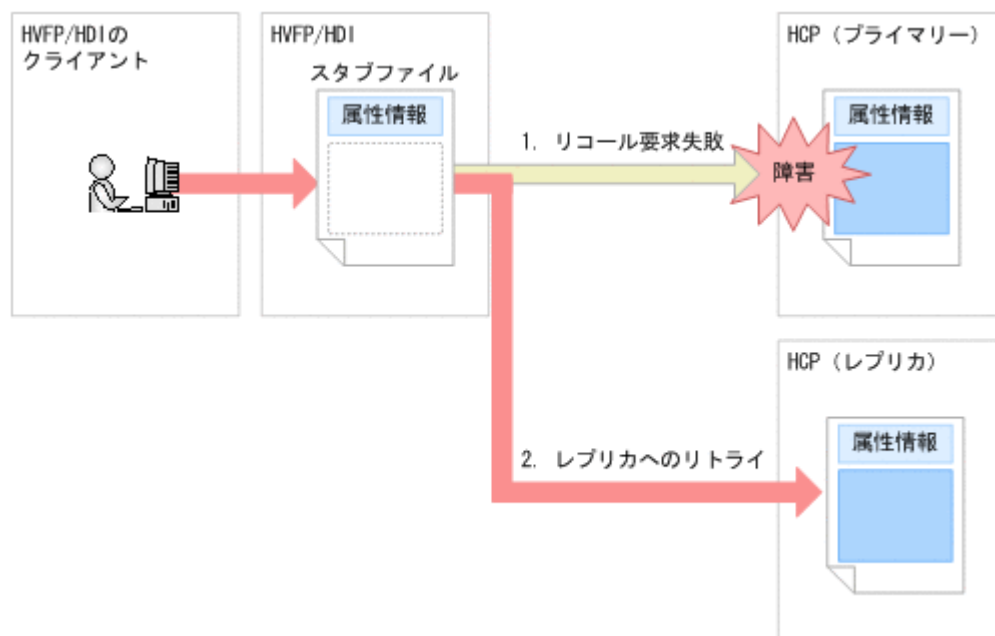
HCP にマイグレートしたデータが HVFP/HDI のスタブファイルに書き込まれることをリコールと呼びます。

スタブファイルへの初回アクセス時は、データがリコールされるため、アクセスに掛かる時間に加えてリコール処理の時間が掛かります。

ファイルのアクセス性能を低下させたくない場合、特定のファイルのデータを常に HVFP/HDI に保持して、ファイルがスタブ化されないように設定することもできます (キャッシュ常駐)。スタブ化されないファイルの条件を設定することで、条件に合致したファイルへのアクセス時にリコール処理の時間がなくなり、スタブファイルの場合よりもアクセス性能が向上します。

HCP でレプリケーション機能を運用する場合は、HVFP/HDI にレプリカのシステムの情報を設定することで、プライマリーシステムの障害によってリコールに失敗すると、自動的にレプリカのシステムに切り替わり、リコール処理を継続できます。

図 6-3 HCP のレプリカのシステムによるリコール処理の継続

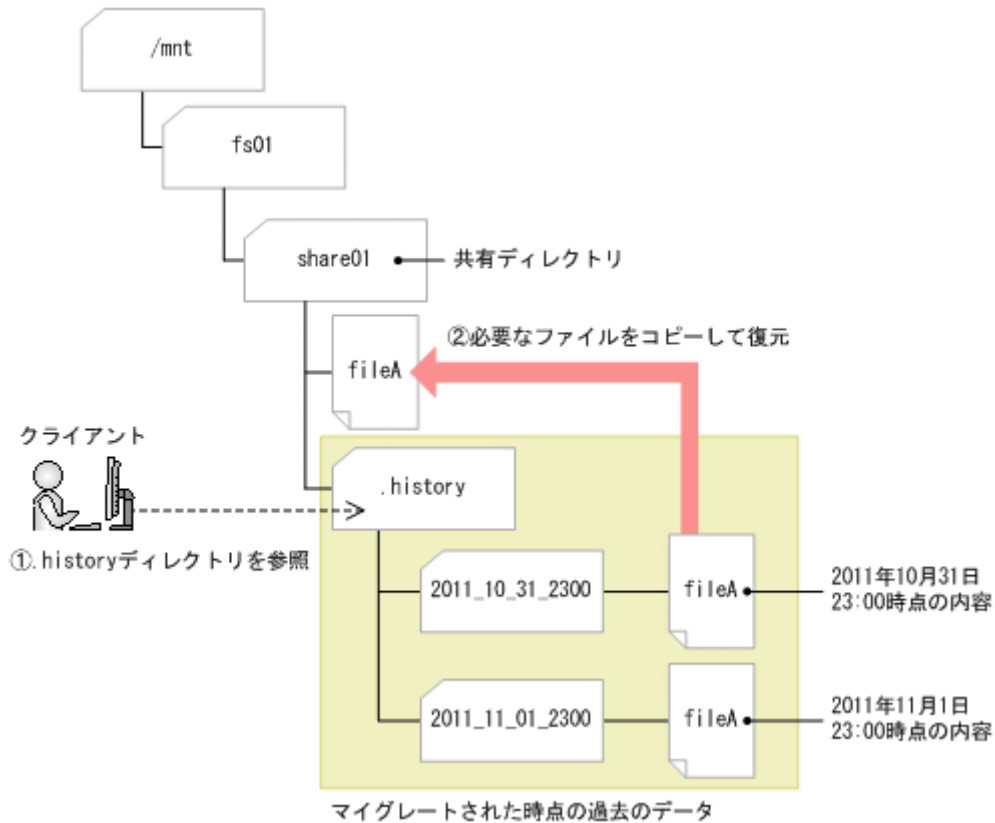


6.1.5 バージョン管理を利用したファイルの復元

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 (ファイルバージョンリストア機能)。

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 6-4 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。
- ・ 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。

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のバージョンをクライアントに公開するかどうかを、GUI またはコマンドで設定します。

6.2 HCP と連携する前に確認すること

HVFP/HDI と HCP を連携する前に確認しておくことを次に示します。

- ・ ファイルシステムに対してマイグレーションポリシーを設定する際、ハードリンクの作成を許可しないよう自動的に設定されます。HVFP/HDI で運用するファイルシステムは、ハードリンクの作成を許可しない設定にしておく必要があります。
- ・ ハードリンクの作成を許可する設定に変更すると、HVFP/HDI のファイルシステムでハードリンクを作成できます。ただし、HVFP/HDI 上のハードリンクが HCP にマイグレートされる際には、1つのファイルとしてマイグレートされます。このため、HCP のデータを HVFP/HDI にリストアするときにハードリンクはリストアされません。

- データを HCP にマイグレートしているファイルシステムで、オフライン属性のファイルを対象とした全文検索などの処理を実施すると、大量のデータが HVFP/HDI にリコールされるため、処理に時間が掛かったり、ファイルシステムの容量が上限に達したりするおそれがあります。
- データを HCP にマイグレートしているファイルシステムで、ファイルやディレクトリの名称を変更すると、マイグレーション対象のファイルを抽出する処理に影響があります。このため、大量にファイル名を変更するとマイグレーションに時間が掛かるおそれがあります。
- ファイルやディレクトリのメタデータを変更すると、メタデータが HCP にマイグレートされます。ACL の変更など、大量のファイルのメタデータを変更する操作を行うと、次回マイグレーションに時間が掛かるおそれがあります。ユーザーに変更があっても影響が少なくなるように、ACL はグループを活用して運用することを推奨します。
- システムバージョン 4.0.0-00 より前から HVFP/HDI と連携して使用しているテナントを複数の HVFP/HDI で共有する構成に変更する場合は、テナントを共有するすべての HVFP/HDI の更新インストールを実施したあとで、複数の HVFP/HDI による使用を開始してください。
- HCP にデータをマイグレートするファイルシステムでは、1 ファイルごとに最大 10KB の管理領域が必要です。ファイルシステムの容量を検討する際に考慮してください。
- HCP にマイグレートされたファイルを HVFP/HDI から削除したときに HCP 上のデータを非同期で削除するように `hcopobjdelset` コマンドで設定している場合でも、ファイルシステムの空き容量が不足すると、ファイルの削除処理と同期して HCP 上のデータが削除されます。このとき、HCP との通信で障害が発生すると、HVFP/HDI からはファイルが削除されますが、HCP 上のデータは削除されません。HSM Core ログ (`hsmarc.log`) を確認し、KAQM37070-E メッセージが出力されている場合は、メッセージの内容を確認して HCP 管理者にデータの削除を依頼してください。
- HCP にマイグレートされたファイルを HVFP/HDI から削除したときに HCP 上のデータを同期して削除するように `hcopobjdelset` コマンドで設定している場合、HCP との通信障害が発生すると、HVFP/HDI でのファイル削除処理もエラーとなります。このため、HCP 上のデータを非同期で削除することを推奨します。
 なお、システムバージョン 4.1 より前の HVFP/HDI から更新インストールを実施すると、HCP 上のデータを同期して削除するように設定されています。必要に応じて設定を変更してください。
- HCP にデータをマイグレートするファイルシステムに対して、ボリュームレプリケーション連携や Hitachi File Remote Replicator の機能は使用できません。
- Hitachi Virtual File Platform Plug-in for VMware vSphere で管理しているファイルシステムのデータは、HCP にマイグレートできません。
- 通常ファイルのほか、ソケットファイルを除くスペシャルファイルやディレクトリがマイグレーションの対象となります。通常ファイル以外のファイルやディレクトリは、マイグレーションポリシーで設定した選択条件に関わらずマイグレートされます。
- マイグレーションポリシーで設定した選択条件に該当するファイルでも、次に示す条件に 1 つでも該当する通常ファイルはマイグレートされません。
 - 一度マイグレートされたあと、データが更新されていない
 - パス長が 4,095 バイトを超える
 - パスに改行コードが含まれている
- ファイルシステムの差分スナップショットを作成している場合は、差分スナップショット（ファイル共有内に公開された差分スナップショットも含む）はマイグレートされません。
- ファイルシステムの差分スナップショットを作成している場合は、差分スナップショット内のスタブファイルにアクセスできません。
- 複数のポリシーでマイグレーションの対象となるファイルは、最初に行われるマイグレーションタスクのポリシーに従ってマイグレートされます。

- ・ フェールオーバーしたときにタイムアウトが発生するおそれがあるため、マイグレーションタスクの実行間隔を検討する際に条件式を満たす必要があります。ただし、arccconfedit コマンドを使用して、一日のうち、最初にマイグレーションが実行されたときにだけ過去バージョンディレクトリが作成されるよう設定した場合は、条件式の「一日当たりのタスクの実行回数」を1にして、設定できる過去バージョンの保持期間を算出できます。使用する条件式については、「共有内に公開する差分スナップショット数を検討する際の条件式」を参照してください。検討例を次に示します。

- システムでは、共有内に差分スナップショットを公開するファイルシステムと、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が、それぞれ1つ運用されている
- 共有内に差分スナップショットを公開する共有ディレクトリ数は20
- 共有内に公開する差分スナップショット数は25
- NFS プロトコルでの公開先の数は各共有とも5
- 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共有ディレクトリ数は10
- 過去バージョンの保持期間は28日

このとき、マイグレーションタスクの実行間隔は次の条件式を満たす必要があります。

$$(20 \times 5) \times 25 + (10 \times 5) \times 28 \times \text{一日当たりのタスクの実行回数} \leq 4000$$

$$\text{一日当たりのタスクの実行回数} \leq 1.07 \text{ (回/日)}$$

$$\text{タスクの実行間隔} \geq 0.93 \text{ (日)}$$

- ・ マイグレーションタスクの実行日時になっても、前回実行された同一ポリシーのマイグレーション処理が終了していない場合は、そのタスクは実行されません。マイグレーションタスクの実行間隔を見直してください。
- ・ 同時に実行できるマイグレーションタスクはリソースグループまたは Virtual Server 当たり 4 つまでです。
- ・ デフォルトでは、マイグレーション中にファイルが更新されると、そのファイルはマイグレートされません。次にマイグレーションが実行されるときにマイグレートされるよう設定されています。マイグレーション中に更新されたファイルを強制的にマイグレートする場合は、arccconfedit コマンドで設定を変更してください。
ただし、連携する HCP のバージョンが 04-10 より前の場合は、マイグレーション中に更新されたファイルはマイグレートされません。次にマイグレーションが実行されるときにマイグレートされます。
- ・ マイグレーション中にフェールオーバーが発生すると、マイグレーション処理を中断します。マイグレートされなかったファイルは、次にマイグレーションが実行されるときにマイグレートされます。
- ・ マイグレーション中にエラーが発生すると、HVFP/HDI から利用されないファイルが HCP 上に残ることがあります。
- ・ NTP サーバの時刻を変更すると HCP が再起動することがあります。HCP の再起動処理中は、マイグレーションおよびリコールの処理が失敗します。
- ・ arcrestore コマンドの実行後やマイグレート中にエラーが発生すると、HVFP/HDI のスタブファイルから参照できる HCP のファイルが最新バージョンでないことがあります。
- ・ ファイルシステムの使用量が上限に達することを防ぐため、ファイルシステムでの1時間当たりのデータの増加量がファイルシステムの残容量を超えないようにスタブ化を開始する閾値を設定する必要があります。
- ・ HCP にマイグレートしたファイルをファイルシステムから削除すると、HCP でもファイルが削除されます。なお、削除したファイルは過去バージョンのデータからリストアできます。

- HCP にマイグレートしたファイルの過去のバージョンをクライアントに公開する場合、マイグレートした時点のファイルと .history ディレクトリ内のファイルとでは、WORM に関する属性、ファイルの最終アクセス日時 (atime) や最終更新日時 (ctime) が異なることがありますが、内容は変更ありません。
- HCP にマイグレートしたファイルの過去のバージョンをクライアントに公開する場合、タイムゾーンを変更すると、ノードの OS を再起動したあとで、.history ディレクトリ下の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の名称が、変更後のタイムゾーンの日に変更されます。
- .history ディレクトリや、HCP を介してデータを参照しているほかのファイルシステムでは、マイグレーションに失敗したファイルおよびディレクトリを参照できません。ファイルやディレクトリが表示されなかったり、0 バイトのファイルや空のディレクトリになったりします。
- HSM Core ログファイル (hsmarc.log) に KAQM37038-E が出力された場合、HCP のバージョン管理 (versioning) を有効にしてから、再度マイグレーションを実行してください。
- マイグレーションポリシーが設定された状態で長期間マイグレーションが実施されていないファイルシステムは、次のマイグレーションに時間が掛かります。マイグレーションポリシーを設定したら、定期的にマイグレーションが実行されるように運用してください。
- マイグレーションの間隔を短くする場合は、HCP でプルーニングまでの保管日数を見直す必要があります。
- 1つのファイルに対して、マイグレーション、ファイル移動、容量削減のタスクのうち、2つ以上の異なるタスクが同時に実行されないようにしてください。なお、同時に実行された場合はエラーが表示されますが、次のタスク実行時に正常に処理されます。
- fsexport コマンドおよび fsimport コマンドは、HCP 連携の設定を引き継ぎません。HCP と連携しているファイルシステムを別のノードに接続させる場合は、ファイルシステムの設定に応じて、次の操作を行ってください。
 - HCP にデータをマイグレートする (ホームディレクトリローミング機能に対応していない) ファイルシステムの場合
[タスク管理] ダイアログでマイグレーションポリシーの設定、および [<ファイルシステム>] サブウィンドウの [ネームスペース] タブでネームスペースの設定を確認してください。そのあと、fsexport コマンドおよび fsimport コマンドを実行し、マイグレーションウィザードでマイグレーションを再設定してください。
 - 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場合
fsexport コマンドおよび fsimport コマンドを実行しないで、ファイルシステムのすべてのデータを HCP にマイグレートし、接続先のノードでファイルシステムを再構築したあと、arcrestore コマンドを実行して、再構築したファイルシステムにデータをリストアしてください。
 - ほかの HVFP/HDI からマイグレートされた HCP のデータを読み取り専用で公開するファイルシステムの場合
fsexport コマンドおよび fsimport コマンドを実行しないで、接続先のノードでファイルシステムを再構築してください。
- 対象のファイルシステムのすべてのファイルがマイグレートされたあとに、ディレクトリがマイグレートされます。ファイルのマイグレーションが完了していても、親ディレクトリのマイグレーションが完了していなければリストアできません。このため、マイグレーション処理が途中で打ち切られると、すべてのファイルをリストアできないおそれがあります。マイグレーションポリシーを設定するときに、余裕を持って打ち切り時間を設定してください。また、サイズの大きいファイルのマイグレーションが完了する前に処理が打ち切られないように、HCP との通信タイムアウトは打ち切り時間よりも十分に短い値を設定してください。
- まだリストアされていないディレクトリへの初回アクセスを契機として、オンデマンドで HCP からデータがリストアされます。ディレクトリ下のファイルやディレクトリの数が多いとデー

タのリストアに時間が掛かるため、クライアント側で使用しているエクスプローラなどがタイムアウトすることがあります。リストアの処理は継続しているため、処理が完了するまでしばらく待ってから、対象のディレクトリに再度アクセスしてください。

- ・ リストアを実施したファイルシステムに対して、全ファイルを対象にした検索のほか、エクスプローラのプロパティ表示、または「フォルダーとデスクトップの説明をポップアップ表示する」機能によるポップアップ表示など、ディレクトリ下を再帰的に走査する処理を実行すると、多数のディレクトリに対してオンデマンドでデータがリストアされるため、時間が掛かります。ディレクトリ下を再帰的に走査する処理は実行しないようにしてください。なお、「フォルダーとデスクトップの説明をポップアップ表示する」機能は、エクスプローラの「フォルダーオプション」で無効にできます。

6.2.1 HVFP/HDI から HCP へアクセスするためのアカウント

HVFP/HDI から HCP のテナントとネームスペースにアクセスするためのアカウントには、データアクセス用の権限とテナント管理用の権限が必要です。データアクセス用の権限では、ネームスペースの作成や編集ができません。また、テナント管理用の権限では、ネームスペースのデータにアクセスできないため、データのマイグレーションやリコールができません。

使用する HCP のバージョンによってアカウントの管理方法が異なります。

(1) HCP のバージョンが 5.0 以降の場合

HVFP/HDI の設定ウィザードで HCP を設定する際、HCP で作成したテナントの管理者情報を指定します。設定ウィザードでの HCP の設定が完了すると、HCP のテナント管理者に対して自動的にデータアクセス用の権限が設定されます。

なお、ほかの HVFP/HDI に対して、HCP にマイグレートされたデータを読み取り専用で公開する場合は、HCP にデータをマイグレートするファイルシステム（コンテンツ共有の設定をオフにする）を GUI で構築または編集する際に、読み取り専用でデータにアクセスする権限を持つユーザーアカウントを作成できます。作成されたアカウントの情報は、ほかの HVFP/HDI からマイグレートされた HCP のデータを読み取り専用で公開するファイルシステム（コンテンツ共有の設定をオンにする）を構築する際に指定します。

(2) HCP のバージョンが 04-10 以前の場合

テナント管理用とデータアクセス用に異なるアカウントが必要となります。

HVFP/HDI の設定ウィザードで HCP を設定する際、HCP で作成したテナントの管理者情報を指定します。設定ウィザードでの HCP の設定が完了すると、HCP のデータアクセスアカウントが自動的に作成されます。

すでに HCP と連携しているため、HCP で作成されたデータアクセスアカウントが HVFP/HDI に設定されているけれども、テナント管理者情報が HVFP/HDI に設定されていない場合、次のどちらかの方法で対応してください。

- ・ テナント管理者のユーザーアカウントを、データアクセスアカウントと同じ名称とパスワードで作成します。
HCP 管理者に依頼するか、使用している HCP のマニュアルを参照してください。
- ・ HCP 管理者から情報を入手し、HVFP/HDI の設定ウィザードでテナント管理者情報を設定します。

なお、ほかの HVFP/HDI に対して、HCP にマイグレートされたデータを読み取り専用で公開する場合は、HCP にデータをマイグレートするファイルシステム（コンテンツ共有の設定をオフにする）を GUI で構築または編集する際に、読み取り専用でデータにアクセスする権限を持つデータアクセスアカウントを作成できます。作成されたアカウントの情報は、ほかの HVFP/HDI からマイ

グレートされた HCP のデータを読み取り専用で公開するファイルシステム（コンテンツ共有の設定をオンにする）を構築する際に指定します。

6.2.2 マイグレート先のネームスペース

GUI を使用して Physical Node 上にファイルシステムを構築する際に、HCP のネームスペースの情報を設定した場合は、自動的にネームスペースが作成されます。Virtual Server 上にファイルシステムを構築する際は、対応するネームスペースを手動で作成する必要があります。

また、HVFP/HDI の設定ウィザードで HCP を設定する際に、システム設定情報の保存先のネームスペース（system-backup-data）が自動的に作成されます。ただし、個々の Virtual Server の設定情報だけを HCP に保存する際は、対応するネームスペースを手動で作成する必要があります。

手動でネームスペースを作成する場合は、HCP の管理者に依頼するか、HCP のマニュアルを参照して作成してください。なお、マイグレート先のネームスペースには Retention Class を設定しないようにしてください。WORM 機能を使用する場合は、HVFP/HDI で設定してください。

ファイルシステムのデータのマイグレート先のネームスペースの容量を検討する際は、次の見積もり式を使用してください。

$$\text{ネームスペースの最大容量} = \text{格納されるユーザーデータの総容量} + \text{1 日間に更新されるファイルの総容量} \times \text{過去バージョンの保持期間}$$

6.2.3 ほかの HVFP/HDI からマイグレートされた HCP のデータを読み取り専用で公開するために

ほかの HVFP/HDI からマイグレートされた HCP のデータを参照し、読み取り専用で公開する場合は、HCP にデータをマイグレートする HVFP/HDI のシステム管理者と、ほかの HVFP/HDI からマイグレートされた HCP のデータを読み取り専用で公開する HVFP/HDI のシステム管理者が連携して作業する必要があります。

ほかの HVFP/HDI からマイグレートされた HCP のデータを読み取り専用で公開するために必要な作業を次に示します。

1. HCP にデータをマイグレートするファイルシステム（コンテンツ共有の設定をオフにする）を構築し、ファイル共有を作成します。
HCP にデータをマイグレートする HVFP/HDI のシステム管理者が実施します。
2. 手順 1 で構築したファイルシステムの HCP へのデータのマイグレーションを実行します。
3. マイグレートされた HCP のデータを読み取り専用で公開します。

ほかの HVFP/HDI からマイグレートされた HCP のデータを読み取り専用で公開するファイルシステム（コンテンツ共有の設定をオンにする）を構築し、ファイル共有を作成します。データがマイグレートされているネームスペースの情報を設定してください。また、手順 1 で構築したファイルシステムと次の設定を同じにしてください。

- ファイルシステムの容量
- ファイルシステムの ACL タイプ
- WORM 機能に関する設定
- スタブ化が開始される閾値
- CIFS 共有および NFS 共有情報

また、読み取りと書き込みを許可してファイルシステムをマウントしてください。

ほかの HVFP/HDI からマイグレートされた HCP のデータを読み取り専用で公開する HVFP/HDI のシステム管理者が実施します。

ほかの HVFP/HDI からマイグレートされた HCP のデータを読み取り専用で公開する手順については、「ユーザーズガイド」を参照してください。

また、ほかの HVFP/HDI からマイグレートされた HCP のデータを読み取り専用で公開するときには、次のことに注意してください。

- Windows のショートカットやシンボリックリンクは作成されたファイルシステムの構成に依存するため、データを参照する各拠点では正しく参照できないことがあります。
- データを共有するすべての拠点で、システムバージョン 03-01-00-00 以降の HVFP/HDI を使用する必要があります。
- ユーザー情報は外部認証サーバで管理し、それぞれの HVFP/HDI で同じユーザー情報を使用してください。
- ほかの HVFP/HDI からマイグレートされた HCP のデータを読み取り専用で公開する前に、公開するデータが HCP にマイグレートされている必要があります。マイグレーションが実行される前に、データを読み取り専用で公開するファイルシステムをマウントした場合、SNMP トラップまたは E-mail で KAQM37250-E が通知されます。KAQM37250-E が通知されたときは、マイグレーションが実行されるまで待つか、すぐにマイグレーションを実行するように、HCP にデータをマイグレートする HVFP/HDI のシステム管理者に依頼してください。
- HCP にデータをマイグレートするファイルシステムでファイル共有の属性を編集したり、ファイル共有を解除したりする場合、HCP にデータをマイグレートする HVFP/HDI のシステム管理者は、ほかの HVFP/HDI からマイグレートされた HCP のデータを読み取り専用で公開する HVFP/HDI のシステム管理者に変更内容を連絡してください。連絡を受けたシステム管理者は、通知された内容に従ってファイル共有の設定を変更してください。

なお、データの公開を中止する場合、HCP にデータをマイグレートする HVFP/HDI のシステム管理者は、ほかの HVFP/HDI からマイグレートされた HCP のデータを読み取り専用で公開する HVFP/HDI のシステム管理者に対して、データの公開の中止を連絡し、ほかの HVFP/HDI からネームスペースにアクセスするために使用したアカウントの設定を変更してください。各 HVFP/HDI のシステム管理者は、ファイルシステムの設定を変更したり、ファイルシステムを削除したりしてください。

6.2.4 マイグレートされた HCP のデータをほかの HVFP/HDI からエンドユーザーごとに使用できるようにするために

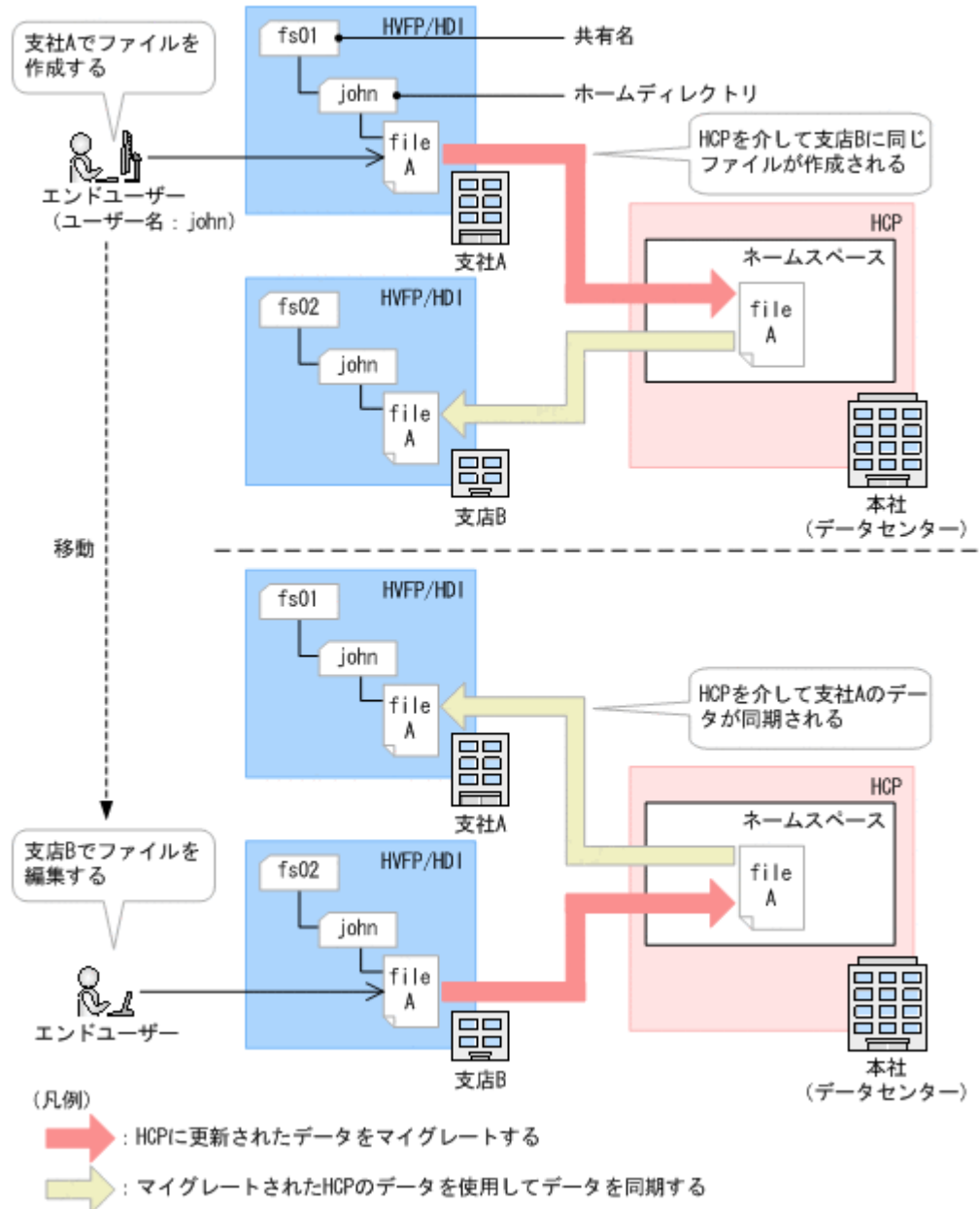
ファイルシステムのデータを HCP にマイグレートする場合、CIFS プロトコルでアクセスするエンドユーザーごとに作成されたホームディレクトリのデータは、エンドユーザーが通常使用している HVFP/HDI とは異なる HVFP/HDI から使用できるように運用できます（ホームディレクトリローミング機能）。ホームディレクトリのデータをほかの HVFP/HDI から使用できるように設定したファイルシステムを「ホームディレクトリローミング対応ファイルシステム」と呼びます。

ホームディレクトリローミング機能を使用する場合は、システムバージョン 4.1.0-00 以降の HVFP/HDI と、バージョン 04-10 以降の HCP を連携して運用してください。

マイグレートされた HCP のデータをほかの HVFP/HDI からエンドユーザーごとに使用する場合のデータの流れを次の図に示します。

図 6-5 マイグレートされた HCP のデータをほかの HVFP/HDI からエンドユーザーごとに使用する
場合のデータの流れ

支社Aのファイルシステム (fs01) と支店Bのファイルシステム (fs02) のデータを共有する場合の例 :



HVFP/HDI 間で共有しているデータは自動的に同期します。エンドユーザーがファイルを編集したあと、HCPにマイグレートされた更新データを使用して、ほかのHVFP/HDIのデータが更新されます。なお、データは1時間ごとにマイグレートされます。

ホームディレクトリローミング対応ファイルシステムには、CIFSクライアントからアクセスしてください。

(1) マイグレートされた HCP のデータをほかの HVFP/HDI からエンドユーザーごとに使用できるようにする場合の注意事項

マイグレートされた HCP のデータをほかの HVFP/HDI からエンドユーザーごとに使用できるようにする場合の注意事項を説明します。

使用する HCP のテナントやネームスペースについては、次のことに注意してください。

- 連携するすべての HVFP/HDI は、マイグレーション先として同一のテナントを指定してください。
- 手動でネームスペースを作成する場合は、使用するネームスペースでプルーニングまでの保管日数を見直す必要があります。HCP の管理者に作業を依頼してください。
- ホームディレクトリローミング機能を使用すると、HCP ではコンプライアンスイベントに関するログメッセージとして次のメッセージが出力されます。通常の処理で出力されるメッセージであるため、問題はありません。

```
Privileged purge succeeded for object /management/hdr/lock/<ユーザー名>.lock, Reason:
unlock_of_homedirectory_resource.. Namespace: <ネームスペース名>
```

HVFP/HDI、ホームディレクトリローミング対応ファイルシステムおよびファイル共有については、次のことに注意してください。

- HCP にマイグレートした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データを読み取り専用で公開することはできません。
- ホームディレクトリローミング対応ファイルシステムに対しては、次の機能は使用できません。
 - ファイルシステムの階層化
 - 複数ファイルのデータ集約
 - WORM 機能
 - サブツリー Quota の管理
 - NDMP 機能
 - ファイルスナップショット機能 (Hitachi File Remote Replicator を含む)
 - ほかのファイルサーバからのインポート
- リアルタイムスキャン機能を利用する場合は、Symantec 社またはマカフィー社のスキャンソフトを使用してください。トレンドマイクロ社のスキャンソフトを使用する場合は、ホームディレクトリローミング対応ファイルシステム内のファイルに対して、リアルタイムスキャンを実施できません。
- マイグレートするファイルの条件に関するマイグレーションポリシーの設定は変更しないでください。ファイルシステム内のすべてのデータが HCP にマイグレートされるよう、ホームディレクトリローミング対応ファイルシステムを構築するときに適切なマイグレーションポリシーがデフォルトで設定されます。
- ホームディレクトリローミング対応ファイルシステムは、HVFP/HDI ごとに 1 個を推奨します。また、ホームディレクトリローミング対応ファイルシステムを構築するときには、1 つのリソースグループまたは Virtual Server 上で同時に実行されるファイル移動タスク、ファイル分析タスク、容量削減タスク、およびマイグレーションタスクの合計が 4 つ以内になるようにしてください。
- ホームディレクトリローミング対応ファイルシステムを使用するエンドユーザー数の上限は 1,000 です。
ホームディレクトリローミング対応ファイルシステムを使用するエンドユーザー数および作成・更新されるファイル数が増加すると、マイグレーションが 1 時間以内に完了しなくなり、ほかの HVFP/HDI でホームディレクトリが読み取り専用になる時間が長くなります。マイグレーションが 1 時間以内に完了するよう、エンドユーザー数やファイル数を調整してください。
- ホームディレクトリにエンドユーザーがアクセスしている間、ほかの HVFP/HDI で同一ユーザーが使用するホームディレクトリは読み取り専用になります。
- メンテナンスのため HVFP/HDI を計画停止する場合、事前に、計画停止する HVFP/HDI からのホームディレクトリへのアクセスを中止するようエンドユーザーに通知し、ホームディレクトリローミング対応ファイルシステム内のすべてのデータを HCP にマイグレートしてください。

HCP にデータをマイグレートしていないと、ほかの HVFP/HDI のホームディレクトリに更新内容が反映されないため、エンドユーザーがほかの HVFP/HDI からホームディレクトリ内の最新のファイルを操作できなくなります。

ホームディレクトリローミング対応ファイルシステムへのアクセスを停止するよう依頼してから、[Access Protocol Configuration] ダイアログで CIFS サービスを停止してください。その後、[タスク管理] ダイアログを使用して、すべてのファイルを HCP にマイグレートしてください。マイグレーションが完了したら、マイグレーションに関するエラーが発生していないことを [Check for Errors] ダイアログで確認してください。エラーが発生しなくなるまで、マイグレーションタスクを実行してください。

クライアントの認証やアカウントについては、次のことに注意してください。

- クライアントの認証には **Active Directory** 認証を使用してください。また、ユーザーマッピングを使用してユーザー ID やグループ ID を割り当ててください。このとき、アカウントに対して HVFP/HDI 間で同じユーザー ID やグループ ID が割り当たるように設定する必要があります。
- アカウントのユーザー名として指定できない名称があります。指定できないユーザー名は、ホームディレクトリの自動作成機能を使用するときに指定できないユーザー名と同じです。ホームディレクトリの自動作成機能を使用するときに指定できないユーザー名については、「ファイルアクセス (CIFS/NFS) ユーザーズガイド」を参照してください。
- アカウントのユーザー名を変更すると、ホームディレクトリのデータにアクセスできなくなります。ユーザー名を変更する必要がある場合は、新規にアカウントを作成してください。

システム管理者は、CIFS 管理者に次の注意事項を連絡してください。

- 共有ディレクトリ直下にファイルやディレクトリを作成しないでください。
- CIFS 管理者として設定されているユーザー、または CIFS 管理者として設定されているグループに属するユーザーのホームディレクトリ以外にはアクセスしないでください。ほかのユーザーのホームディレクトリにアクセスし、データを更新した場合、HVFP/HDI 間でデータの不整合が発生するおそれがあります。
- ホームディレクトリのアクセス権を変更しないでください。
- ホームディレクトリは名称を変更したり削除したりしないでください。すべてのデータを削除する場合は、ホームディレクトリ内のファイルやディレクトリを選択して削除してください。

また、システム管理者は、ホームディレクトリローミング対応ファイルシステムを使用するエンドユーザーに次の注意事項を連絡してください。

- 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共有にネットワークドライブを割り当ててから、アクセスを開始してください。ホスト名だけを指定して HVFP/HDI にアクセスすると、エンドユーザーからホームディレクトリを操作できなくなるおそれがあります。
- HVFP/HDI 間で共通のユーザーアカウントを使用してください。また、ユーザーアカウントはエンドユーザー間で共有しないでください。
- ほかの HVFP/HDI でデータを更新できなくなるおそれがあるため、作業が完了したらクライアントマシンからログオフしてください。
- ホームディレクトリの一時的な現象として、読み取り専用になることがあります。ファイルを更新できなかった場合は、クライアントマシンに保存したあと、しばらくしてからホームディレクトリのファイルを更新してください。更新できない状態が続く場合は、システム管理者に連絡してください。
- ホームディレクトリの一時的な現象として、古いファイルやディレクトリがあったり、空になっていたりすることがあります。また、クライアントからファイルの更新に失敗したりすることもあります。このような問題が発生した場合は、更新に失敗したファイルがあればクライアントマシンにファイルを一時保存した上で、ログオフしたあと 10 分程度待ってから再度アクセスしてください。

ホームディレクトリのファイルは更新されていることがあるため、一時保存したファイルと内容を比較してから、最新の状態にしてください。

- ホームディレクトリ内のファイルに更新した内容が反映されていない場合は、「.conflict」という名称のディレクトリに更新したファイルが格納されていることがあります。.conflict ディレクトリを参照して、更新したファイルがないかを確認してください。.conflict ディレクトリのデータは保持期間を過ぎると自動的に削除されます。.conflict ディレクトリが作成されている場合は、できるだけ早く必要なファイルがないかを確認してください。
- .conflict ディレクトリを参照できるように、すべてのファイルとフォルダが表示されるよう設定してください。
- .conflict ディレクトリ内のファイルは、.conflict ディレクトリ以外のホームディレクトリ内の任意の場所にコピーしてから使用してください。使用するファイルはディレクトリごとコピーしないでください。ディレクトリごとコピーすると、ファイルの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。
- ホームディレクトリのアクセス権を変更するときは、ほかのユーザーに対してデータの更新を許可するアクセス権を設定しないようにしてください。

(2) マイグレートされた HCP のデータをほかの HVFP/HDI からエンドユーザーごとにも使用できるようにするために必要な作業

マイグレートされた HCP のデータをほかの HVFP/HDI からエンドユーザーごとにも使用できるようにするためには、各拠点の HVFP/HDI のシステム管理者が連携して作業する必要があります。

マイグレートされた HCP のデータをほかの HVFP/HDI からエンドユーザーごとにも使用できるようにするときに必要なシステム管理者の作業を次に示します。

1. 各拠点の HVFP/HDI で、ホームディレクトリローミング対応ファイルシステムを構築し、ファイル共有を作成します。

連携するすべての HVFP/HDI で次の設定が同じになるように指定します。

- ノードの時刻
- クライアント認証の設定
- ファイルシステムの設定 (ACL タイプ、過去バージョンの保持期間、または使用する機能など)
- マイグレーション先のネームスペース

GUI でファイルシステムを構築するときにネームスペースを作成した HVFP/HDI のシステム管理者は、ほかの HVFP/HDI のシステム管理者にネームスペース名を連絡してください。

また、HCP の管理者がすべての HVFP/HDI からデータアクセスできるネームスペースを作成する場合は、HCP の管理者から通知された情報を指定してください。

2. 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共有にネットワークドライブを割り当ててからアクセスを開始するようエンドユーザーに連絡します。



重要 HCP との通信障害などが原因で、HVFP/HDI から HCP へのデータのマイグレーションに失敗した場合、ホームディレクトリ下に .conflict という読み取り専用のディレクトリが作成されることがあります。 .conflict ディレクトリ下には、マイグレーションに失敗した日時とその HVFP/HDI を示す名称のディレクトリが作成され、そのディレクトリ内にマイグレーションに失敗したファイルが格納されます。ホームディレクトリ内のファイルに更新内容が反映されていないときは、.conflict ディレクトリを参照するよう、対象のエンドユーザーに依頼してください。 .conflict ディレクトリ内のデータは、次にマイグレーションが実行されるときにマイグレートされるため、各 HVFP/HDI で参照できます。 .conflict ディレクトリにファイルを保持する期間はデフォルトで 4 日間です。保持期間は `arccconfedit` コマンドで変更できます。連携するすべての HVFP/HDI で同じ設定にしてください。

6.2.5 HCP にマイグレートしたデータを使用して HVFP/HDI を回復するために

HVFP/HDI と HCP を連携する場合は、HVFP/HDI のノードの OS ディスク、共有 LU およびユーザー LU で障害が発生したときに、システム設定情報およびユーザーデータを一括で回復できます。すべてのファイルがマイグレーションの対象となっていることと、システム設定情報ファイルが HCP に定時保存されていることを確認してください。システム設定情報ファイルは、HCP 上のシステム設定情報を保存するためのネームスペース (system-backup-data) に、「sysbk_<システムが自動で付与する HVFP/HDI ごとの ID >.1」または「sysbk_<システムが自動で付与する HVFP/HDI ごとの ID >.2」の名称で保存されます。

なお、次の情報は HCP に保存されていないため、回復できません。必要に応じて設定情報を記録しておいてください。

- ・ 情報の保存時にマウントされていなかったファイルシステムの次の設定情報
 - 最大・最小リテンション期間
 - 自動コミットの設定
 - ファイルシステム使用量に関する警告が通知されるかどうか
 - ファイルシステム閉塞時に自動的にフェールオーバーするかどうか
 - ファイルの作成日時が記録されるかどうか
- ・ マイグレーション、ファイル移動および容量削減タスク実行時に使用する初期モードの設定情報
- ・ 差分スナップショット
- ・ Hitachi File Remote Replicator のペア定義およびデータ転送量の設定情報
- ・ HCP にマイグレートされていなかったユーザーデータ

回復されたファイルシステムはハードリンク作成を許可しない設定になります。

このほか、次に示す情報が更新されるたびにシステム外の記録媒体に保管しておく必要があります。

ストレージシステムの設定情報

使用しているストレージシステムが Hitachi AMS2000 シリーズまたは HUS100 シリーズの場合、Hitachi Storage Navigator Modular 2 を使用して、次の設定情報をダウンロードしてください。

- パリティグループおよびロジカルユニットの構成情報ファイル
- ポート情報の構成情報ファイル
- システムパラメーターの構成情報ファイル

Hitachi Storage Navigator Modular 2 の操作手順については、Hitachi Storage Navigator Modular 2 のマニュアルを参照してください。

ファイルシステムの設定情報

対象のファイルシステムが属しているリソースグループが稼働しているノード上で -t および -w オプションを指定して fslist コマンドを実行したときに表示される、ファイルシステムの設定情報を記録してください。

CIFS 共有または NFS 共有情報

cifsbackup コマンドまたは nfsbackup コマンドを使用して、CIFS 共有または NFS 共有の情報をバックアップしてください。ファイルシステムに CIFS 共有と NFS 共有がどちらも設定されている場合は、cifsbackup コマンドおよび nfsbackup コマンドをそれぞれ実行する必要があります。

ファイルシステムとネームスペースの対応

どのファイルシステムとネームスペースが対応するのか記録してください。GUI で **Physical Node** 上にファイルシステムを構築する際に **HCP** のネームスペースの情報を設定した場合は、次の形式でネームスペース名が自動的に付与されます。

<ファイルシステム名>-<システムが自動で付与する HVFP/HDI ごとの ID >

Hitachi File Services Manager のインストールと環境設定

この章では、クラスタ構成の HVFP/HDI を運用する場合に、システム管理者が管理サーバに Hitachi File Services Manager をインストールしたり、環境設定を実施したりするときの操作手順について説明します。

- 7.1 Hitachi File Services Manager をインストール・アンインストールする
- 7.2 Hitachi File Services Manager をインストール・アンインストールする（管理サーバをクラスタ構成で運用する場合）
- 7.3 Hitachi File Services Manager を起動・停止する
- 7.4 システム管理者のアカウントを管理する
- 7.5 Hitachi File Services Manager の環境を設定する
- 7.6 管理サーバのメンテナンス

7.1 Hitachi File Services Manager をインストール・アンインストールする

この節では、Hitachi File Services Manager のインストールおよびアンインストール方法について説明します。

インストールを実施する前に

- 「7.1.5 Hitachi File Services Manager をインストールするときの前提条件」を参照してください。
- 管理サーバをクラスタ構成で運用する場合は、「7.2 Hitachi File Services Manager をインストール・アンインストールする（管理サーバをクラスタ構成で運用する場合）」を参照してください。

7.1.1 Hitachi File Services Manager を新規インストールする

ここでは、Hitachi File Services Manager を新規インストールする方法について説明します。

Hitachi File Services Manager を新規インストールする手順を次に示します。

1. Hitachi File Services Manager のインストールメディアをセットします。
2. エクスプローラでインストールメディアの内容を表示し、HF5Minst.exe を実行します。

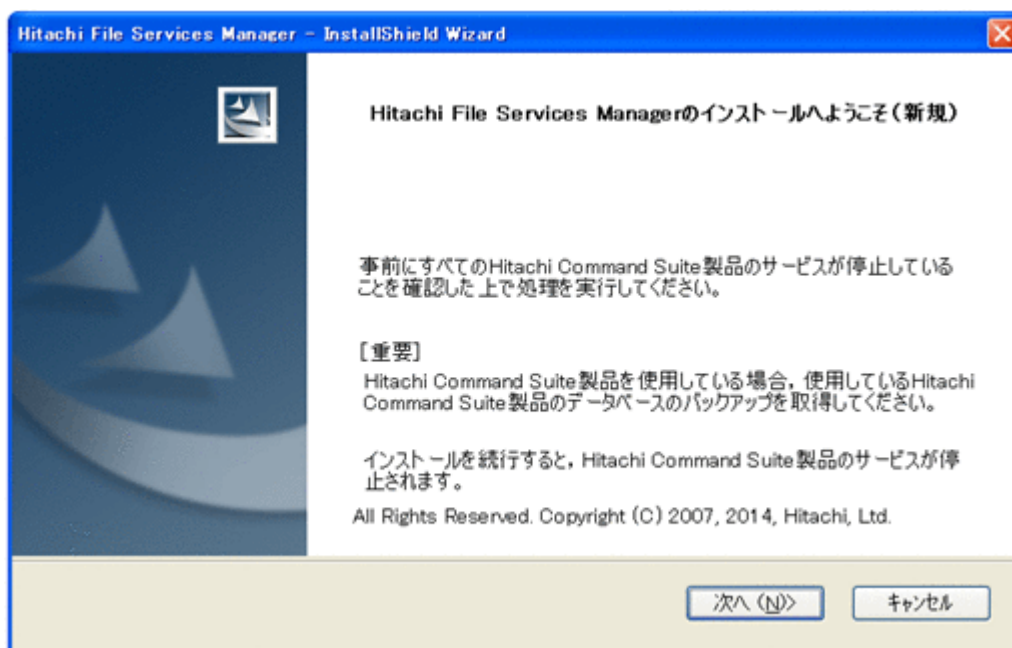
製品使用許諾契約のダイアログが表示されます。

なお、すでに Hitachi Command Suite 製品がドライブ直下にインストールされている場合、インストールが中断されます。この場合は、Hitachi Command Suite 製品をアンインストールするか、ドライブ直下以外にインストールし直してから Hitachi File Services Manager をインストールしてください。

3. 契約の内容を確認して、[はい] ボタンをクリックします。

[Hitachi File Services Manager のインストールへようこそ（新規）] ダイアログが表示されます。

図 7-1 [Hitachi File Services Manager のインストールへようこそ（新規）] ダイアログ



注意：

[次へ] ボタンをクリックした場合、インストーラーが Hitachi Command Suite 共通コンポーネントやほかの Hitachi Command Suite 製品のサービスを停止します。

4. ダイアログの内容を確認して、[次へ] ボタンをクリックします。

Hitachi File Services Manager をインストールするマシンに Hitachi Command Suite 製品がインストールされているかどうかによって、操作が異なります。

Hitachi Command Suite 製品がインストールされている場合

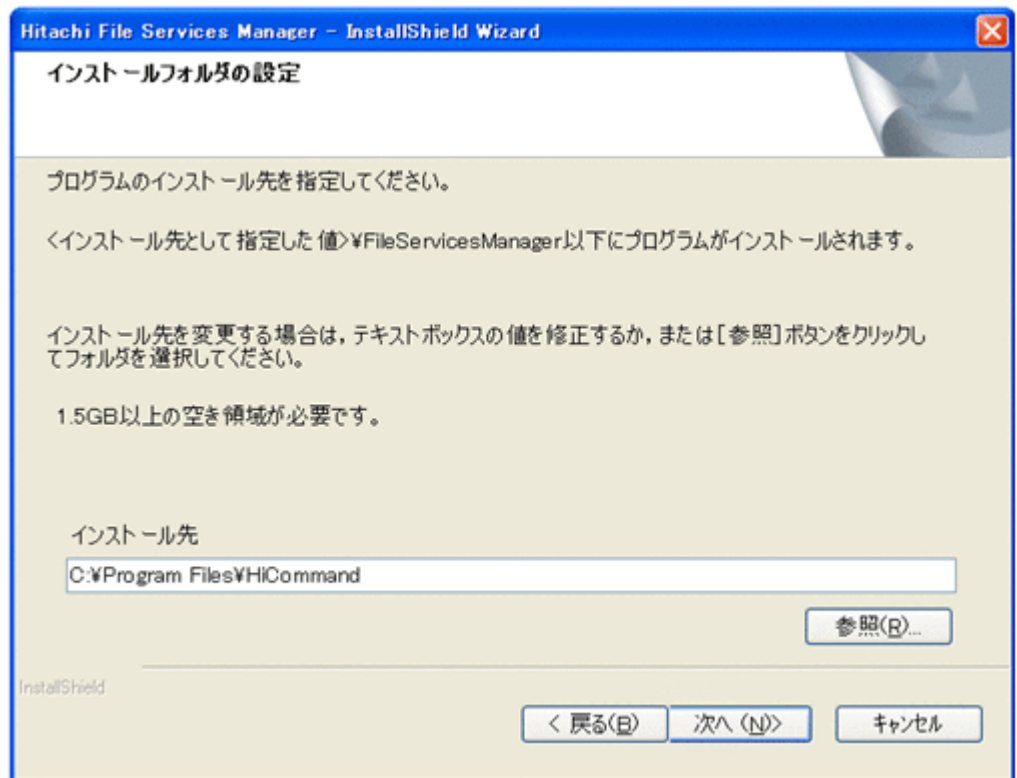
[Hitachi Command Suite 共通コンポーネントデータベースのセットアップ状態の確認] ダイアログが表示されます。

インストール済みの Hitachi Command Suite 製品のセットアップ状態を確認できます。インストール済みの Hitachi Command Suite 製品のセットアップ状態を確認して、[次へ] ボタンをクリックすると、[インストールフォルダの設定] ダイアログが表示されます。

Hitachi Command Suite 製品がインストールされていない場合

[インストールフォルダの設定] ダイアログが表示されます。

図 7-2 [インストールフォルダの設定] ダイアログ



インストール先は、次の条件に従って指定してください。

- インストール先としてドライブ直下 (C:¥, D:¥など) は指定できません。必ずフォルダ名を指定してください。
- 64 バイト以下の絶対パスで指定してください。
- パス名に使用できる文字は英数字、始め丸括弧 ((), 終わり丸括弧 ()), ピリオド (.), アンダーライン (_) およびスペースです。ただし、ピリオド (.) は文字列の先頭および末尾には指定できません。また、スペースは、文字列の先頭および末尾に指定したり、2 つ以上連続して指定したりできません。
- パスの区切り文字として、円記号 (¥) が使用できます。ただし、文字列の末尾には指定できません。

- シンボリックリンクやジャンクションを指定しないでください。

インストール先を指定すると、Hitachi File Services Manager および Hitachi Command Suite 共通コンポーネントは、次のフォルダにインストールされます。

Hitachi File Services Manager のインストール先

<インストール先として指定した絶対パス>¥FileServicesManager¥

Hitachi Command Suite 共通コンポーネントのインストール先

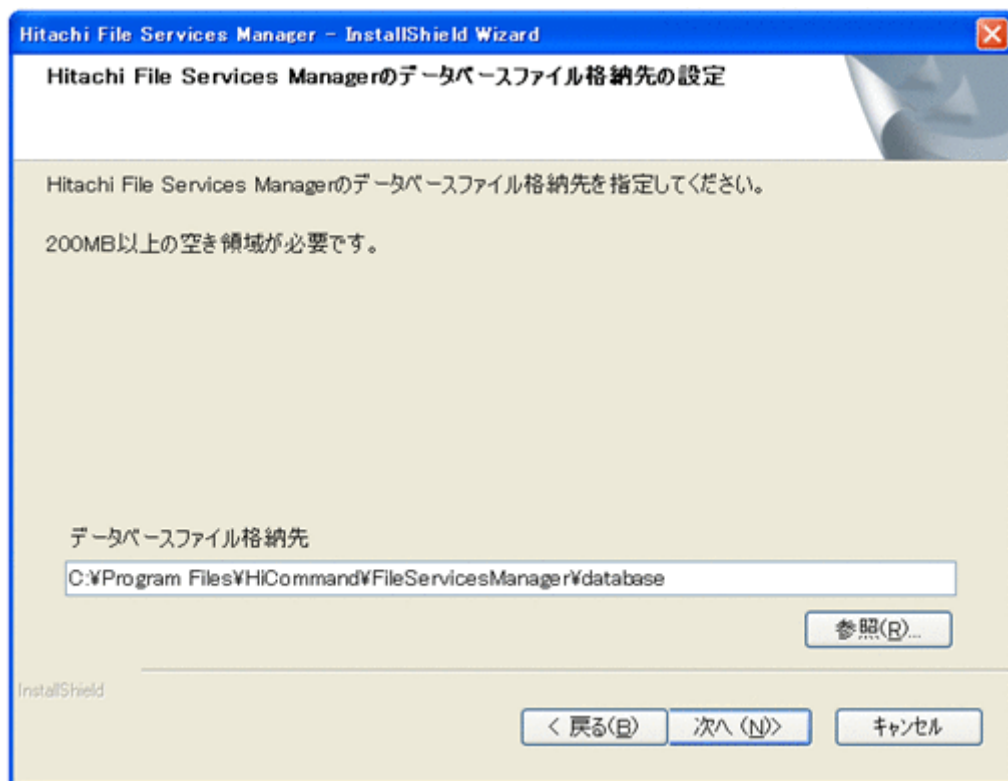
<インストール先として指定した絶対パス>¥Base¥

ただし、Hitachi File Services Manager をインストールするマシンに Hitachi Command Suite 製品がインストールされている場合は、指定したインストール先ではなく、Hitachi Command Suite 共通コンポーネントがインストールされているフォルダに上書きされます。

5. インストール先を指定して、[次へ] ボタンをクリックします。

[Hitachi File Services Manager のデータベースファイル格納先の設定] ダイアログが表示されます。

図 7-3 [Hitachi File Services Manager のデータベースファイル格納先の設定] ダイアログ



データベースファイル格納先のフォルダは、次の条件に従って指定してください。

- 90 バイト以下の絶対パスで指定してください。
 - パス名に使用できる文字は英数字、始め丸括弧 ((), 終わり丸括弧 ()), ピリオド (.), アンダーライン (_) およびスペースです。ただし、ピリオド (.) は文字列の先頭および末尾には指定できません。また、スペースは、文字列の先頭および末尾に指定したり、2 つ以上連続して指定したりできません。
 - パスの区切り文字として、円記号 (¥) が使用できます。ただし、文字列の末尾には指定できません。
6. データベースファイル格納先を指定して、[次へ] ボタンをクリックします。

Windows のファイアウォール機能がインストールされているかどうかによって、操作が異なります。

Windows のファイアウォール機能がインストールされている場合

[Windows ファイアウォール例外登録] ダイアログが表示されます。ダイアログの内容を確認して、[次へ] ボタンをクリックすると、[インストール前の確認] ダイアログが表示されます。

Windows のファイアウォール機能がインストールされていない場合

[インストール前の確認] ダイアログが表示されます。

7. 指定した内容に誤りがないことを確認して、[インストール] ボタンをクリックします。インストールが開始され、処理状況を示すダイアログが表示されます。インストールが正常に完了すると、[インストールの完了] ダイアログが表示されます。

注意：

- [インストール] ボタンをクリックすると、SSL の証明書が次のキーストアファイルに自動的にインポートされます。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %jdk%jre%lib%security%jssecacerts
```

デフォルトパスワードは「changeit」です。インストールが完了したあと、管理サーバで次のとおりコマンドを実行して、パスワードを変更してください。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %bin%hcmdskeytool -storepasswd -keystore < Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %jdk%jre%lib%security%jssecacerts -storepass <現在のパスワード (changeit) > -new <新しいパスワード >
```

- 管理サーバのキーストアファイル (jssecacerts) のパスワードが設定されている場合は、[インストールの完了] ダイアログが表示される前にエラーダイアログが表示されます。ダイアログの内容を確認して [OK] ボタンをクリックし、インストールが完了したあとに、管理サーバに SSL の証明書をインポートしてください。管理サーバに SSL の証明書をインポートする方法については、「7.5.7 管理サーバとノードの通信に必要な SSL の証明書をインポートする」を参照してください。
8. [完了] ボタンをクリックして、インストールを完了します。

非クラスタ構成の管理サーバの場合は、Hitachi Command Suite 共通コンポーネントのサービスが起動し、Hitachi File Services Manager を運用できる状態になります。

クラスタ構成の管理サーバの場合は、クラスタで運用するための設定を続けてください。管理サーバをクラスタ構成で運用する場合に Hitachi File Services Manager をインストールする方法については、「7.2 Hitachi File Services Manager をインストール・アンインストールする (管理サーバをクラスタ構成で運用する場合)」を参照してください。

7.1.2 Hitachi File Services Manager をアップグレード・上書きインストールする

ここでは、Hitachi File Services Manager がインストールされている管理サーバで、Hitachi File Services Manager をアップグレードインストールまたは上書きインストールする方法について説明します。

Hitachi File Services Manager が存在する管理サーバに、新しいバージョンの Hitachi File Services Manager をアップグレードインストールすることで、バージョンを更新できます。Hitachi File Services Manager のインストール後にノードの OS のバージョンを更新した場合は、必ず Hitachi File Services Manager をアップグレードインストールして、最新のバージョンになるようにしてください。

また、同じバージョンの Hitachi File Services Manager を上書きインストールすることで、障害やシステム管理者の誤操作などによって破損した Hitachi File Services Manager の設定ファイルを修復できます。

注意：

- 管理サーバにインストールされている Hitachi File Services Manager より古いバージョンの Hitachi File Services Manager はインストールできません。古いバージョンの Hitachi File Services Manager を利用したい場合は、管理サーバの Hitachi File Services Manager をアンインストールしたあとに、古いバージョンの Hitachi File Services Manager を新規インストールしてください。
- Hitachi File Services Manager をアップグレードインストールした場合は、[ノード編集] ダイアログで、登録済みの Processing Node を管理サーバに再認識させる必要があります。

Hitachi File Services Manager をアップグレードインストールまたは上書きインストールする手順を次に示します。

1. Hitachi File Services Manager のインストールメディアをセットします。
2. エクスプローラでインストールメディアの内容を表示し、HFSMinst.exe を実行します。
製品使用許諾契約のダイアログが表示されます。
3. 契約の内容を確認して、[はい] ボタンをクリックします。

[Hitachi File Services Manager のインストールへようこそ (アップグレード)] ダイアログまたは [Hitachi File Services Manager のインストールへようこそ (上書き)] ダイアログが表示されます。表示されるダイアログの例を次の図に示します。

図 7-4 [Hitachi File Services Manager のインストールへようこそ (上書き)] ダイアログ



注意：

[次へ] ボタンをクリックした場合、インストーラーが Hitachi Command Suite 共通コンポーネントやほかの Hitachi Command Suite 製品のサービスを停止します。

4. ダイアログの内容を確認して、[次へ] ボタンをクリックします。

[Hitachi Command Suite 共通コンポーネントデータベースのセットアップ状態の確認] ダイアログが表示されます。

インストール済みの Hitachi Command Suite 製品のセットアップ状態を確認できます。

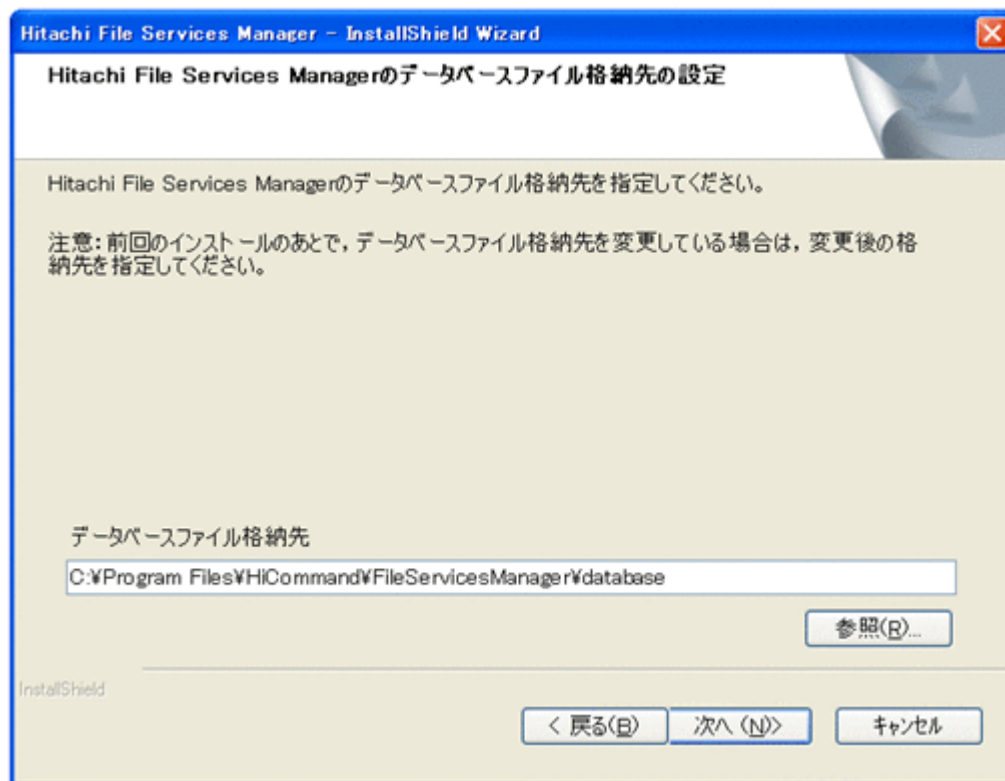
5. セットアップ状態を確認して、[次へ] ボタンをクリックします。

[インストール前の確認] ダイアログが表示されます。

なお、管理サーバに Hitachi File Services Manager のデータベースが存在しない場合は、[インストール前の確認] ダイアログが表示される前に、[Hitachi File Services Manager のデータベースファイル格納先の設定] ダイアログが表示されます。データベースファイル格納先フォルダを指定し、[次へ] ボタンをクリックして、インストール作業を進めてください。

[Hitachi File Services Manager のデータベースファイル格納先の設定] ダイアログを次の図に示します。

図 7-5 [Hitachi File Services Manager のデータベースファイル格納先の設定] ダイアログ (新規インストール以外の場合)



データベースファイル格納先のフォルダは、次の条件に従って指定してください。

- 90 バイト以下の絶対パスで指定してください。
 - パス名に使用できる文字は英数字、始め丸括弧 ((), 終わり丸括弧 ()), ピリオド (.), アンダーライン (_) およびスペースです。ただし、ピリオド (.) は文字列の先頭および末尾には指定できません。また、スペースは、文字列の先頭および末尾に指定したり、2 つ以上連続して指定したりできません。
 - パスの区切り文字として、円記号 (¥) が使用できます。ただし、文字列の末尾には指定できません。
6. 指定した内容に誤りがないことを確認して、[インストール] ボタンをクリックします。

インストールが開始され、処理状況を示すダイアログが表示されます。インストールが正常に完了すると、[インストールの完了] ダイアログが表示されます。

アップグレードインストールおよび上書きインストールでは、Hitachi File Services Manager のデータベースは初期化されません。

また、管理サーバとノードとの間で通信エラーが発生している場合には、アップグレードインストールを行っても、管理サーバ内のデータベースのキャッシュ情報とノード上の情報が不一致に

なっているおそれがあります。この場合には、障害要因を取り除いたあと、リフレッシュ処理を行ってください。

注意：

管理サーバのキーストアファイル (jssecacerts) のパスワードが設定されている場合は、[インストールの完了] ダイアログが表示される前にエラーダイアログが表示されます。ダイアログの内容を確認して [OK] ボタンをクリックし、インストールが完了したあとに、管理サーバに SSL の証明書をインポートしてください。管理サーバに SSL の証明書をインポートする方法については、「7.5.7 管理サーバとノードの通信に必要な SSL の証明書をインポートする」を参照してください。

7. [完了] ボタンをクリックして、インストールを完了します。

非クラスタ構成の管理サーバの場合は、Hitachi Command Suite 共通コンポーネントのサービスが起動し、Hitachi File Services Manager を運用できる状態になります。

クラスタ構成の管理サーバの場合は、クラスタで運用するための設定を続けてください。管理サーバをクラスタ構成で運用する場合に Hitachi File Services Manager をインストールする方法については、「7.2 Hitachi File Services Manager をインストール・アンインストールする (管理サーバをクラスタ構成で運用する場合)」を参照してください。

7.1.3 Hitachi NAS Manager から Hitachi File Services Manager にアップグレードインストールする

ここでは、Hitachi NAS Manager がインストールされている管理サーバで、Hitachi NAS Manager を Hitachi File Services Manager にアップグレードインストールする方法について説明します。

注意：

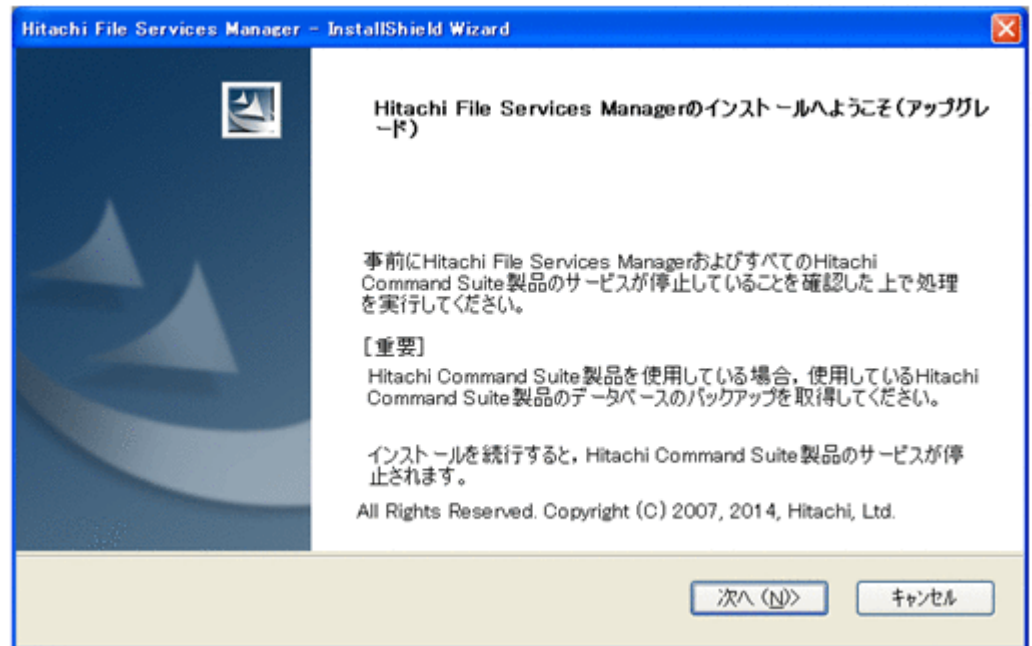
- Hitachi NAS Manager から Hitachi File Services Manager へのアップグレードインストールでは、データベースのデータ移行が完了すると Hitachi NAS Manager はアンインストールされます。
- バージョン 05-00 の Hitachi NAS Manager から Hitachi File Services Manager にアップグレードインストールした場合は、[ノード編集] ダイアログで、登録済みの Processing Node を管理サーバに再認識させる必要があります。
- Hitachi File Services Manager がインストールされている管理サーバに Hitachi NAS Manager はインストールできません。
- Hitachi NAS Manager または Hitachi Command Suite 製品がドライブ直下にインストールされている場合、インストールが中断されます。この場合は、Hitachi NAS Manager および Hitachi Command Suite 製品をドライブ直下以外にインストールし直してから Hitachi File Services Manager をインストールしてください。

Hitachi NAS Manager を Hitachi File Services Manager にアップグレードインストールする手順を次に示します。

1. Hitachi File Services Manager のインストールメディアをセットします。
2. エクスプローラでインストールメディアの内容を表示し、HFSMinst.exe を実行します。
製品使用許諾契約のダイアログが表示されます。
3. 契約の内容を確認して、[はい] ボタンをクリックします。

[Hitachi File Services Manager のインストールへようこそ (アップグレード)] ダイアログが表示されます。

図 7-6 [Hitachi File Services Manager のインストールへようこそ (アップグレード)] ダイアログ



注意：

[次へ] ボタンをクリックした場合、インストーラーが Hitachi Command Suite 共通コンポーネントやほかの Hitachi Command Suite 製品のサービスを停止します。

4. ダイアログの内容を確認して、[次へ] ボタンをクリックします。

[Hitachi Command Suite 共通コンポーネントデータベースのセットアップ状態の確認] ダイアログが表示されます。

インストール済みの Hitachi Command Suite 製品のセットアップ状態を確認できます。

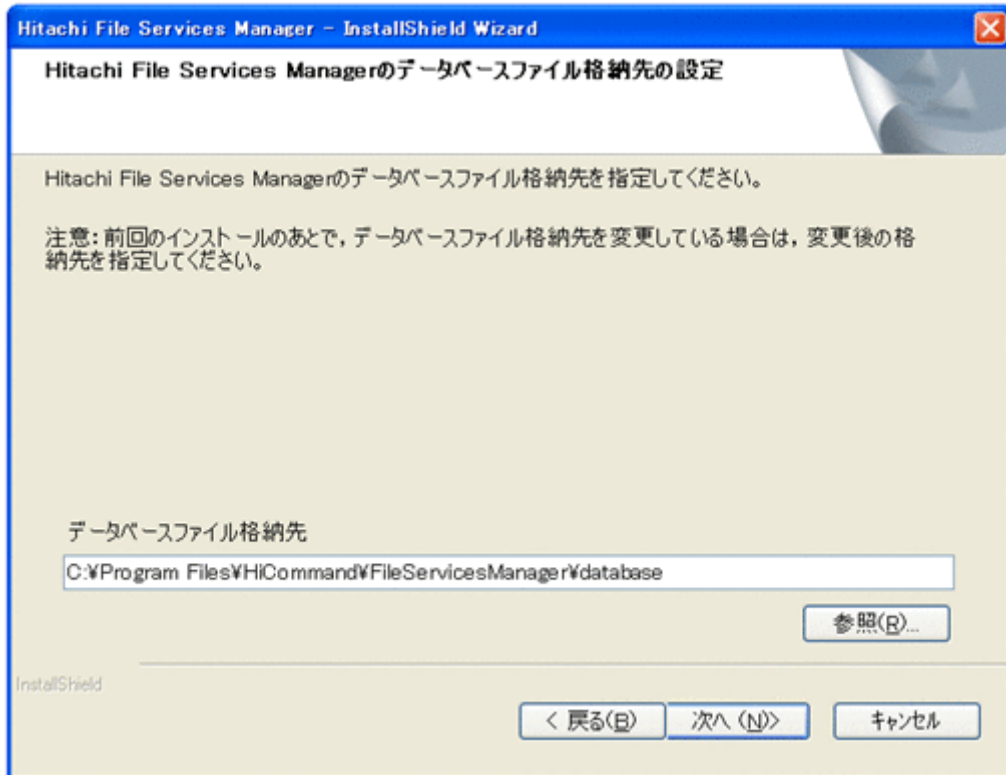
5. セットアップ状態を確認して、[次へ] ボタンをクリックします。

[インストール前の確認] ダイアログが表示されます。

なお、管理サーバに Hitachi NAS Manager のデータベースが存在しない場合は、[インストール前の確認] ダイアログが表示される前に、[Hitachi File Services Manager のデータベースファイル格納先の設定] ダイアログが表示されます。データベースファイル格納先フォルダを指定し、[次へ] ボタンをクリックして、インストール作業を進めてください。

[Hitachi File Services Manager のデータベースファイル格納先の設定] ダイアログ (新規インストール以外の場合) を次の図に示します。

図 7-7 [Hitachi File Services Manager のデータベースファイル格納先の設定] ダイアログ (新規インストール以外の場合)



データベースファイル格納先のフォルダは、次の条件に従って指定してください。

- 90 バイト以下の絶対パスで指定してください。
- パス名に使用できる文字は英数字、始め丸括弧 ()、終わり丸括弧 ()、ピリオド (.), アンダーライン (_) およびスペースです。ただし、ピリオド (.) は文字列の先頭および末尾には指定できません。また、スペースは、文字列の先頭および末尾に指定したり、2 つ以上連続して指定したりできません。
- パスの区切り文字として、円記号 (¥) が使用できます。ただし、文字列の末尾には指定できません。

参考：

Hitachi NAS Manager から Hitachi File Services Manager へのアップグレードインストールの場合、[データベースファイル格納先] には NASManager というフォルダ名を FileServicesManager に置き換えたパスが表示されます。

6. 指定した内容に誤りが無いことを確認して、[インストール] ボタンをクリックします。
インストールが開始され、処理状況を示すダイアログが表示されます。インストールが正常に完了すると、[インストールの完了] ダイアログが表示されます。

なお、Hitachi NAS Manager から Hitachi File Services Manager へのアップグレードインストールでは、Hitachi NAS Manager のデータベースは初期化されずに、データが移行されます。データの移行が完了すると、Hitachi NAS Manager はアンインストールされます。

また、管理サーバとノードとの間で通信エラーが発生している場合には、アップグレードインストールを行っても、管理サーバ内のデータベースのキャッシュ情報とノード上の情報が不一致になっているおそれがあります。この場合には、障害要因を取り除いたあと、リフレッシュ処理を行ってください。

注意：

管理サーバのキーストアファイル (jssecacerts) のパスワードが設定されている場合は、Hitachi NAS Manager がアンインストールされる前にエラーダイアログが表示されません。ダイアログの内容を確認して [OK] ボタンをクリックし、インストールが完了したあとに、管理サーバに SSL の証明書をインポートしてください。管理サーバに SSL の証明書をインポートする方法については、「7.5.7 管理サーバとノードの通信に必要な SSL の証明書をインポートする」を参照してください。

7. [完了] ボタンをクリックして、インストールを完了します。

非クラスタ構成の管理サーバの場合は、Hitachi Command Suite 共通コンポーネントのサービスが起動し、Hitachi File Services Manager を運用できる状態になります。

クラスタ構成の管理サーバの場合は、クラスタで運用するための設定を続けてください。管理サーバをクラスタ構成で運用する場合に Hitachi File Services Manager をインストールする方法については、「7.2 Hitachi File Services Manager をインストール・アンインストールする (管理サーバをクラスタ構成で運用する場合)」を参照してください。

7.1.4 Hitachi File Services Manager をアンインストールする

ここでは、Hitachi File Services Manager をアンインストールする方法について説明します。

注意：

Hitachi NAS Manager から Hitachi File Services Manager にアップグレードインストールした場合など、管理サーバに Microsoft(R) .NET Framework がインストールされているときには、Hitachi File Services Manager をアンインストールしても、Microsoft .NET Framework はアンインストールされません。

(1) アンインストールする前に

Hitachi File Services Manager をアンインストールする前に必要な作業を次に示します。

- Administrator または Administrators グループのユーザーで Windows にログオンしてください。
- Hitachi File Services Manager および Hitachi Command Suite 製品のサービスを停止してください。
- Hitachi File Services Manager および Hitachi Command Suite 製品のデータベースのバックアップを取得してください。
- セキュリティ監視プログラムがインストールされている場合、セキュリティ監視プログラムを停止するか、設定を変更して、Hitachi File Services Manager のアンインストールが妨げられないようにしてください。
- ウイルス検出プログラムがインストールされている場合、ウイルス検出プログラムを停止してから Hitachi File Services Manager をアンインストールすることを推奨します。

Hitachi File Services Manager のアンインストール中にウイルス検出プログラムが稼働していると、アンインストールの速度が低下したり、アンインストールが実行できなかつたり、または正しくアンインストールできなかつたりすることがあります。

- プロセス監視プログラムがインストールされている場合、プロセス監視プログラムを停止するか、設定を変更して、Hitachi File Services Manager と Hitachi Command Suite 共通コンポーネントのサービスまたはプロセスを監視しないようにしてください。

Hitachi File Services Manager のアンインストール中に、プロセス監視プログラムによって、Hitachi File Services Manager と Hitachi Command Suite 共通コンポーネントのサービスまたはプロセスが起動したり停止したりすると、アンインストールに失敗することがあります。

- Windows のサービスを操作するウィンドウをすべて閉じてください。

(2) アンインストールの実行

Hitachi File Services Manager をアンインストールする手順を次に示します。

1. [Hitachi File Services Manager のアンインストール] ダイアログにアクセスします。
次のどちらかの方法でアクセスできます。
 - Windows 7 までの Windows の場合は、[スタート] - [プログラム] - [Hitachi Command Suite] - [File Services Manager] - [Uninstall - HFSM] を選択する
Windows 8 または Windows Server 2012 の場合は、スタート画面のアプリ一覧から [Uninstall - HFSM] を選択します。
 - Windows の [アプリケーションの追加と削除] ※1 ユーティリティから、[Hitachi File Services Manager] を選択して、[変更と削除] ボタン※2 をクリックする
注※1：Windows XP では [プログラムの追加と削除]、Windows Vista 以降は [プログラムと機能] です。
注※2：Windows Vista 以降は [アンインストール] をクリックします。
- [Hitachi File Services Manager のアンインストール] ダイアログが表示されます。

図 7-8 [Hitachi File Services Manager のアンインストール] ダイアログ



2. ダイアログの内容を確認して、[次へ] ボタンをクリックします。
[Hitachi Command Suite 共通コンポーネントデータベースのセットアップ状態の確認] ダイアログが表示されます。
非クラスタ構成の管理サーバ、クラスタ構成の管理サーバの実行系ノードおよび待機系ノードのうち、インストール済みの Hitachi Command Suite 製品のセットアップ状態に応じた内容が表示されます。
3. セットアップ状態を確認して、[次へ] ボタンをクリックします。
[アンインストール前の確認] ダイアログが表示されます。
4. ダイアログに表示されている Hitachi File Services Manager のバージョンおよびインストール先が正しいことを確認して、[アンインストール] ボタンをクリックします。
アンインストールが開始され、処理状況を示すダイアログが表示されます。アンインストールが正常に完了すると、[アンインストールの完了] ダイアログが表示されます。

5. [完了] ボタンをクリックして、Hitachi File Services Manager のアンインストールを完了します。

7.1.5 Hitachi File Services Manager をインストールするときの前提条件

Hitachi File Services Manager をインストールする前に、次のことを確認してください。

Hitachi File Services Manager をインストールするマシンに存在するほかの製品

Hitachi Command Suite 製品のバージョンが、04-00 以降であることを確認してください。また、Large 構成の Tuning Manager が存在しないことを確認してください。

Hitachi File Services Manager をインストールするマシンの環境

- Hitachi File Services Manager をインストールするマシンが、管理サーバのマシン要件を満たしていることを確認してください。
管理サーバのマシン要件については、「[3.2.1 管理サーバのマシン要件](#)」を参照してください。
- 新規インストールする場合は、Hitachi File Services Manager をインストールするための空き容量がディスクドライブにあることを確認してください。
インストールするコンポーネントと必要な空き容量を次の表に示します。

表 7-1 インストールするコンポーネントと必要な空き容量

コンポーネント	必要な空き容量
Hitachi File Services Manager	1.5GB 以上
Hitachi File Services Manager のデータベースファイル	200MB 以上

Hitachi File Services Manager のインストール先と Hitachi File Services Manager のデータベースファイルの格納先には、異なるディスクドライブを指定することもできます。

なお、Hitachi NAS Manager から Hitachi File Services Manager にアップグレードインストールする場合は、表 7-1 インストールするコンポーネントと必要な空き容量に示した空き容量のほかに一時的に 500MB 以上の空き容量が必要です。

- コマンドプロンプトで netstat -a コマンドを実行し、23015～23018、23032 および 45001～49000 のポート番号が Hitachi File Services Manager および Hitachi Command Suite 製品だけで使用されていることを確認してください。

Hitachi File Services Manager および Hitachi Command Suite 製品以外の製品が 23015～23018 および 23032 のポート番号を使用している場合は、使用している製品または Hitachi File Services Manager のどちらかで設定を変更してください。Hitachi File Services Manager でポート番号を変更する方法については「[7.5.5 Hitachi Command Suite 共通コンポーネントのポート番号を変更する](#)」を参照してください。

23015～23018 および 23032 のポート番号の設定が Hitachi Command Suite 製品で変更されている場合は、設定を元に戻す必要はありません。

Hitachi File Services Manager および Hitachi Command Suite 製品以外の製品が 45001～49000 のポート番号を使用している場合は、使用している製品で設定を変更してください。45001～49000 のポート番号は、Hitachi File Services Manager では設定を変更できません。

Hitachi File Services Manager をインストールする前に実施する作業

- Administrator または Administrators グループのユーザーで Windows にログオンしてください。

- Hitachi File Services Manager をインストールするマシン上の Hitachi Command Suite 製品※のサービスを停止してください。
サービスを停止しないでインストールした場合、インストール中に Hitachi Command Suite 共通コンポーネントやほかの Hitachi Command Suite 製品のサービスが停止されます。インストーラーがサービスを停止できなかった場合、インストールは中止されます。
注※
Hitachi Tuning Manager - Agent for SAN Switch がインストールされている場合、Hitachi Command Suite 製品のサービスを停止するコマンド (hcmdssrv /stop コマンド) を実行しても、Hitachi Tuning Manager - Agent for SAN Switch のサービスは停止しません。したがって、この場合は、Hitachi Tuning Manager - Agent for SAN Switch のサービスを事前に停止してから、Hitachi Tuning Manager のサービスを停止する必要があります。Hitachi Tuning Manager - Agent for SAN Switch のサービスの停止方法については、Hitachi Tuning Manager - Agent for SAN Switch のマニュアルを参照してください。
- Hitachi File Services Manager (または Hitachi NAS Manager) および Hitachi Command Suite 製品のデータベースのバックアップを取得してください。
- すでに Hitachi Command Suite 製品がインストールされている場合、HiRDB/EmbeddedEdition_HD0 が起動していることを確認してください。
Hitachi Command Suite 製品は、常に HiRDB/EmbeddedEdition_HD0 が起動している必要があります。Windows の [サービス] ウィンドウの一覧にある HiRDB/EmbeddedEdition_HD0 が起動していることを確認してください。停止していた場合は、HiRDB/EmbeddedEdition_HD0 を起動してください。
- セキュリティ監視プログラムがインストールされている場合、セキュリティ監視プログラムを停止するか、設定を変更して、Hitachi File Services Manager のインストールが妨げられないようにしてください。
- ウイルス検出プログラムがインストールされている場合、ウイルス検出プログラムを停止してから Hitachi File Services Manager をインストールすることを推奨します。
Hitachi File Services Manager のインストール中にウイルス検出プログラムが稼働していると、インストールの速度が低下したり、インストールが実行できなかったり、または正しくインストールできなかったりすることがあります。
- プロセス監視プログラムがインストールされている場合、プロセス監視プログラムを停止するか、設定を変更して、Hitachi File Services Manager と Hitachi Command Suite 共通コンポーネントのサービスまたはプロセスを監視しないようにしてください。
Hitachi File Services Manager のインストール中に、プロセス監視プログラムによって、Hitachi File Services Manager と Hitachi Command Suite 共通コンポーネントのサービスまたはプロセスが起動されたり停止されたりすると、インストールに失敗することがあります。
- Hitachi File Services Manager をインストールするマシンの時刻を調整してください。
マシンの時刻の調整は、Hitachi File Services Manager をインストールする前に実施してください。Hitachi File Services Manager および Hitachi Command Suite 共通コンポーネントのサービスが起動しているときにマシンの時刻を変更すると、Hitachi File Services Manager が正しく動作しなくなるおそれがあります。Hitachi File Services Manager をインストールしたあとで管理サーバの時刻の調整が必要となった場合は、「7.6.5 管理サーバの時刻を調整する」を参照してください。
- Windows のサービスを操作するウィンドウをすべて閉じてください。
- Hitachi File Services Manager をインストールするマシンの OS が Windows Server 2003 SP1 などのデータ実行防止機能 (DEP) を持つ Windows OS で、DEP が有効になっ

ている場合は、Hitachi File Services Manager のインストールメディアをセットし、HFSMinst.exe に対して DEP を解除するよう設定してください。

Device Manager の GUI にログインして Hitachi File Services Manager を使用する際の注意事項

Device Manager と連携する場合、Device Manager の GUI にログインして Hitachi File Services Manager を使用できます。Hitachi File Services Manager と Device Manager のインストール先によって必要な作業が異なります。Device Manager の GUI にログインして Hitachi File Services Manager を使用する場合は、次のことに注意してください。

Hitachi File Services Manager と Device Manager を同一の管理サーバにインストールする場合

- Hitachi File Services Manager のインストール後に、Device Manager を起動してください。Device Manager を起動する方法については、Device Manager のマニュアルを参照してください。また、バージョン 8.0 以降の Device Manager がインストールされた管理サーバにインストールした場合は、Device Manager に接続してユーザーアカウントを管理するように設定を変更します。手順については、「[7.4.7 Device Manager に接続してユーザーアカウントを管理する](#)」を参照してください。
- Hitachi File Services Manager のインストール後に、Device Manager を起動できない場合、ポート番号がほかの製品と重複しているおそれがあります。Device Manager が使用するポート番号を変更してから Device Manager を起動してください。Device Manager が使用するポート番号を変更する方法については、Device Manager のマニュアルを参照してください。
- Device Manager での認証に使用するユーザーアカウントに、Hitachi File Services Manager の Admin 権限を設定してください。
- バージョン 8.0 以降の Device Manager をアンインストールする場合は、Hitachi File Services Manager もアンインストールする必要があります。

Hitachi File Services Manager を Device Manager と異なるマシンにインストールする場合

- Device Manager に接続してユーザーアカウントを管理するように設定を変更します。手順については「[7.4.7 Device Manager に接続してユーザーアカウントを管理する](#)」を参照してください。
- Device Manager での認証に使用するユーザーアカウントに、Hitachi File Services Manager の Admin 権限を設定してください。

7.2 Hitachi File Services Manager をインストール・アンインストールする（管理サーバをクラスタ構成で運用する場合）

この節では、管理サーバをクラスタ構成で運用する場合の Hitachi File Services Manager のインストールおよびアンインストール方法について説明します。ここでは、Windows Server 2003 での操作方法について説明します。Windows Server 2008 または Windows Server 2012 を使用している場合は、Microsoft Cluster Service を Microsoft Failover Cluster に、操作手順に記載している「クラスタアドミニストレータ」を「フェールオーバー クラスタ管理」に読み替えてください。また、各設定項目および設定先も、「フェールオーバー クラスタ管理」についてのドキュメントを参照して、対応する名称に読み替えてください。

クラスタ構成の管理サーバに Hitachi File Services Manager をインストールする前に、次のことを確認してください。

- Hitachi File Services Manager をインストールするマシンが、管理サーバのマシン要件を満たしていること (表 3-2 管理サーバのマシン要件)
- Hitachi File Services Manager をインストールするマシンに、クラスタ構成に必要なソフトウェアがインストールされていること (表 3-5 クラスタ構成で管理サーバを運用する場合の適用 OS とクラスタソフトウェア)
- 実行系ノードと待機系ノードで、インストールを予定している Hitachi File Services Manager のバージョンが同じであること

7.2.1 Hitachi File Services Manager を新規インストールする (管理サーバをクラスタ構成で運用する場合)

ここでは、管理サーバをクラスタ構成で運用する場合に、Hitachi File Services Manager を新規インストールする方法について説明します。

(1) 管理サーバをクラスタ構成にする

Microsoft Cluster Service のクラスタアドミニストレータで、クラスタ管理 IP アドレスおよび共有ディスクを設定していない場合は、次の手順を実行してください。

1. Windows の [スタート] - [設定] - [コントロールパネル] - [管理ツール] - [クラスタアドミニストレータ] を選択して、クラスタアドミニストレータを表示します。
2. [リソースの種類] に [IP アドレス] を選択して、クラスタ管理 IP アドレスをグループに登録します。
3. [リソースの種類] に [ネットワーク名] を選択して、論理ホスト名をグループに登録します。
4. [リソースの種類] に [物理ディスク] を選択して、共有ディスクをグループに登録します。
5. クラスタアドミニストレータで、グループをオンラインにします。

(2) 新規インストールする前に

クラスタ構成の管理サーバに Hitachi File Services Manager を新規インストールする前に、次のことを確認してください。

- 管理サーバの実行系ノード、待機系ノードおよびクラスタ管理 IP アドレスについて、ホスト名から IP アドレスへの名前解決ができることを確認してください。
- クラスタを設定している間は、Hitachi File Services Manager にアクセスしないでください。
- 管理サーバの実行系ノードでのインストールを実施してから、待機系ノードでのインストールを実施してください。

(3) 管理サーバの実行系ノードでの新規インストール

実行系ノードに Hitachi File Services Manager を新規インストールし、クラスタ設定する手順を次に示します。

1. 実行系ノードに Hitachi File Services Manager を新規インストールします。
Hitachi File Services Manager の新規インストール手順については、「[7.1.1 Hitachi File Services Manager を新規インストールする](#)」を参照してください。インストールする際は、Hitachi Command Suite 共通コンポーネント、および Hitachi File Services Manager が使用するデータベースの格納先はデフォルトのままにします。
2. テキストエディターを使って、クラスタ設定ファイルを作成します。

次の項目を指定したファイルを作成してください。

- mode
online と指定します。
- virtualhost
論理ホスト名を指定します。
- onlinehost
実行系ノードのホスト名を指定します。
- standbyhost
待機系ノードのホスト名を指定します。

virtualhost, onlinehost および standbyhost には、IP アドレスは指定できません。
クラスタ設定ファイルの記述例を次に示します。

```
mode = online
virtualhost = hicommand_cluster
onlinehost = hicommand_1
standbyhost = hicommand_2
```

3. クラスタ設定ファイルの名称を cluster.conf として、次のフォルダに格納します。
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > ¥conf¥
4. 管理サーバ上の Device Manager に接続している Tuning Manager のサービスを停止します。
Hitachi Command Suite 製品がインストールされていて、そのうちの Device Manager に接続している Tuning Manager が、Device Manager とは別のマシンにインストールされている場合に必要手順です。Tuning Manager がインストールされているマシンでサービスを停止してください。Tuning Manager のサービスを停止する方法については、インストールされている Tuning Manager のバージョンに対応するマニュアルを参照してください。
5. Hitachi File Services Manager および Hitachi Command Suite 共通コンポーネントが停止しても問題ないことを確認します。
次の手順のコマンドを実行すると、Hitachi File Services Manager および Hitachi Command Suite 共通コンポーネントが自動的に停止します。
6. 次のとおりコマンドを実行して、データベースのバックアップを取得します。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > ¥bin¥hcmdsbackups /
dir <バックアップ先フォルダ> /auto
```

バックアップ先フォルダには、ローカルディスク上のフォルダを絶対パスで指定してください。
実在するフォルダを指定する場合は、空のフォルダであることを確認してください。

指定できる文字は英数字、スペース、感嘆符 (!)、番号記号 (#)、始め丸括弧 ((), 終わり丸括弧 ()), 正符号 (+)、ハイフン (-)、ピリオド (.), 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 (_), 始め波括弧 ({), 終わり波括弧 (}), および波ダッシュ (~) です。また、パスの区切り文字として、斜線 (/), コロン (:) および円記号 (¥) を使用できます。

hcmdsbackups コマンドを実行すると、/dir オプションに指定したバックアップファイルの格納先フォルダに database というフォルダが作成され、データベースのバックアップファイルが backup.hdb というファイル名で格納されます。

/auto オプションを指定した場合でも、Device Manager に接続している Tuning Manager が、Device Manager とは別のマシンにインストールされているときには、Tuning Manager のサービスが自動的に起動および停止されません。

7. 次のとおりコマンドを実行して、データベースを共有ディスクに移行します。

```
<Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%bin
%hcmdsdbcluster /createcluster /databasepath <データベースの再作成先フォルダ>
 /exportpath <データの格納先フォルダ> /auto
```

コマンドの引数は、次の条件に従って指定してください。

- データベースの再作成先フォルダは 92 バイト以下、データの格納先フォルダは 85 バイト以下の絶対パスで指定してください。
- データベースの再作成先フォルダは、共有ディスク上に配置してください。
- データの格納先フォルダは、ローカルディスク上に配置してください。
- データの格納先フォルダに実在するフォルダを指定する場合は、空のフォルダであることを確認してください。
- データベースの再作成先フォルダおよびデータの格納先フォルダに使用できる文字は英数字、始め丸括弧 ()、終わり丸括弧 ()、ピリオド (.), アンダーライン (_) およびスペースです。ただし、ピリオド (.) は文字列の先頭および末尾には指定できません。また、スペースは、文字列の先頭および末尾に指定したり、2 つ以上連続して指定したりできません。
- データベースの再作成先フォルダおよびデータの格納先フォルダには、パスの区切り文字として、円記号 (¥) が使用できます。ただし、文字列の末尾には指定できません。

データベース再作成先フォルダには、次に示す空き容量が必要です。

必要な空き容量 = 2.1GB + ほかの Hitachi Command Suite 製品のデータベース容量
データベース再作成先フォルダの空き容量不足が原因で hcmdsdbcluster /createcluster コマンドの実行に失敗した場合は、データベース再作成先フォルダの空き容量を増やしたあとで、hcmdsdbcluster /createcluster コマンドを再実行してください。

hcmdsdbcluster コマンドが正常終了するまでは、共有ディスクを実行系ノードから切り離さないでください。

hcmdsdbcluster コマンドが異常終了した状態でサーバを再起動すると、共有ディスクの接続先が待機系ノードに切り替わることがあります。

このコマンドを実行すると、HiRDB が使用するポート番号がデフォルト値 (23032) に戻ります。

/auto オプションを指定した場合でも、Device Manager に接続している Tuning Manager が、Device Manager とは別のマシンにインストールされているときには、Tuning Manager のサービスが自動的に起動および停止されません。

8. HiRDB が使用するポート番号をデフォルト値 (23032) から変更して運用する場合は、変更後のポート番号に設定し直してください。

HiRDB が使用するポート番号を変更する方法については、「[7.5.5 Hitachi Command Suite 共通コンポーネントのポート番号を変更する](#)」を参照してください。

9. Hitachi File Services Manager および Hitachi Command Suite 共通コンポーネントが稼働している場合は、次のとおりコマンドを実行して、停止します。

```
<Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%bin%hcmdssrv /stop
```

10. Windows の [サービス] ウィンドウで次のリソースのプロパティを開き、[スタートアップの種類] を [自動] から [手動] に変更します。

- HBase Storage Mgmt Common Service
- HBase Storage Mgmt Web Service
- HiRDB/ClusterService_HD0

11. クラスタアドミニストレータで、次のリソースを登録します。

- HBase Storage Mgmt Common Service

- HBase Storage Mgmt Web Service

- HiRDB/ClusterService_HD0

リソースを登録するには、[新規作成] - [リソース] を選択して、各ダイアログで次の表に示した情報を指定し、[完了] ボタンをクリックします。

表 7-2 HBase Storage Mgmt Common Service をリソースとして登録するための設定

ダイアログ名	設定
新しいリソース	次の項目を指定します。 名前 HBase Storage Mgmt Common Service (任意) リソースの種類 汎用サービス
実行可能な所有者	実行系ノードと待機系ノードが追加されていることを確認します。
依存関係	HiRDB を登録します。
汎用サービスパラメーター	次の項目を指定します。 サービス名 HBaseStgMgmtComService 起動パラメーター なし
レジストリの複製	何も指定しません。

表 7-3 HBase Storage Mgmt Web Service をリソースとして登録するための設定

ダイアログ名	設定
新しいリソース	次の項目を指定します。 名前 HBase Storage Mgmt Web Service (任意) リソースの種類 汎用サービス
実行可能な所有者	実行系ノードと待機系ノードが追加されていることを確認します。
依存関係	HBaseStgMgmtComService を登録します。
汎用サービスパラメーター	次の項目を指定します。 サービス名 HBaseStgMgmtWebService 起動パラメーター なし
レジストリの複製	何も指定しません。

表 7-4 HiRDB をリソースとして登録するための設定

ダイアログ名	設定
新しいリソース	次の項目を指定します。 名前 HiRDB (任意) リソースの種類 汎用サービス
実行可能な所有者	実行系ノードと待機系ノードが追加されていることを確認します。
依存関係	共有ディスクのドライブ、およびネットワーク名を登録します。
汎用サービスパラメーター	次の項目を指定します。 サービス名 HiRDBClusterService_HD0 起動パラメーター

ダイアログ名	設定
	なし
レジストリの複製	何も指定しません。

また、Windows Server 2008 または Windows Server 2012 を使用している場合は、コマンドプロンプトから次のコマンドを実行してください。

```
cluster res "<リソース名>" /priv StartupParameters=""
```

<リソース名>には、HBase Storage Mgmt Web Service の汎用サービスのリソース名を指定します。リソース名は「フェールオーバー クラスタ管理」で確認してください。

(4) 管理サーバの待機系ノードでの新規インストール

待機系ノードに Hitachi File Services Manager を新規インストールし、クラスタ設定する手順を次に示します。

1. 待機系ノードに Hitachi File Services Manager を新規インストールします。

Hitachi File Services Manager の新規インストール手順については、「[7.1.1 Hitachi File Services Manager を新規インストールする](#)」を参照してください。インストールする際は、次の条件に従ってください。

- 実行系ノードと同じインストールフォルダを指定します。
- Hitachi Command Suite 共通コンポーネント、および Hitachi File Services Manager が使用するデータベースの格納先はデフォルトのままにします。

2. テキストエディターを使って、クラスタ設定ファイルを作成します。

次の項目を指定したファイルを作成してください。

- mode
standby と指定します。
- virtualhost
論理ホスト名を指定します。
- onlinehost
実行系ノードのホスト名を指定します。
- standbyhost
待機系ノードのホスト名を指定します。

virtualhost、onlinehost および standbyhost には、IP アドレスは指定できません。クラスタ設定ファイルの記述例を次に示します。

```
mode = standby
virtualhost = hicommand_cluster
onlinehost = hicommand_1
standbyhost = hicommand_2
```

3. クラスタ設定ファイルの名称を cluster.conf として、次のフォルダに格納します。

< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > ¥conf¥

4. 管理サーバ上の Device Manager に接続している Tuning Manager のサービスを停止します。

Hitachi Command Suite 製品がインストールされていて、そのうちの Device Manager に接続している Tuning Manager が、Device Manager とは別のマシンにインストールされている場合に必要手順です。Tuning Manager がインストールされているマシンでサービスを停止してください。Tuning Manager のサービスを停止する方法については、インストールされている Tuning Manager のバージョンに対応するマニュアルを参照してください。

5. Hitachi File Services Manager および Hitachi Command Suite 共通コンポーネントが停止しても問題ないことを確認します。

次の手順のコマンドを実行すると、Hitachi File Services Manager および Hitachi Command Suite 共通コンポーネントが自動的に停止します。

6. 次のとおりコマンドを実行して、共有ディスク上のデータベースを使用するよう設定します。

```
<Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%bin
%hcmsdbclustersetup /createcluster /databasepath <データベースの再作成先フォルダ>
> /exportpath <データの格納先フォルダ> /auto
```

コマンドの引数は、次の条件に従って指定してください。

- データベースの再作成先フォルダには、実行系ノードと同じフォルダを指定してください。
- データの格納先フォルダは、85 バイト以下の絶対パスで指定してください。
- データの格納先フォルダは、ローカルディスク上に配置してください。
- データの格納先フォルダに実在するフォルダを指定する場合は、空のフォルダであることを確認してください。
- データの格納先フォルダに使用できる文字は英数字、始め丸括弧 ()、終わり丸括弧 ()、ピリオド (.), アンダーライン (_) およびスペースです。ただし、ピリオド (.) は文字列の先頭および末尾には指定できません。また、スペースは、文字列の先頭および末尾に指定したり、2 つ以上連続して指定したりできません。
- データの格納先フォルダには、パスの区切り文字として、円記号 (¥) が使用できます。ただし、文字列の末尾には指定できません。

hcmsdbclustersetup コマンドが正常終了するまでは、共有ディスクを実行系ノードから切り離さないでください。

また、hcmsdbclustersetup コマンドが異常終了した状態でサーバを再起動しないでください。

このコマンドを実行すると、HiRDB が使用するポート番号がデフォルト値 (23032) に戻ります。

/auto オプションを指定した場合でも、Device Manager に接続している Tuning Manager が、Device Manager とは別のマシンにインストールされているときには、Tuning Manager のサービスが自動的に起動および停止されません。

7. HiRDB が使用するポート番号をデフォルト値 (23032) から変更して運用する場合は、変更後のポート番号に設定し直してください。

HiRDB が使用するポート番号を変更する方法については、「[7.5.5 Hitachi Command Suite 共通コンポーネントのポート番号を変更する](#)」を参照してください。

8. Hitachi File Services Manager および Hitachi Command Suite 共通コンポーネントが稼働している場合は、次のとおりコマンドを実行して、停止します。

```
<Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%bin%hcmsdssrv /stop
```

9. Windows の [サービス] ウィンドウで次のリソースのプロパティを開き、[スタートアップの種類] を [自動] から [手動] に変更します。

- HBase Storage Mgmt Common Service
- HBase Storage Mgmt Web Service
- HiRDB/ClusterService_HD0

10. クラスタアドミニストレータで、グループをオンラインにします。

7.2.2 Hitachi File Services Manager をアップグレード・上書きインストールする（管理サーバをクラスタ構成で運用する場合）

ここでは、管理サーバをクラスタ構成で運用する場合に、Hitachi File Services Manager をアップグレードインストールまたは上書きインストールする方法について説明します。ただし、管理サーバをクラスタ構成で運用する場合に、Hitachi NAS Manager から Hitachi File Services Manager にアップグレードインストールするときは、「7.2.3 Hitachi File Services Manager を新規・アップグレード・上書きインストールする（Hitachi Command Suite 製品をクラスタ構成で運用している場合）」に記載されている手順に従ってインストールしてください。

管理サーバの実行系ノードでのインストールを実施してから、待機系ノードでのインストールを実施してください。

(1) 管理サーバの実行系ノードでのアップグレード・上書きインストール

実行系ノードに Hitachi File Services Manager をアップグレードインストールまたは上書きインストールし、クラスタ設定する手順を次に示します。

1. Windows の [スタート] - [設定] - [コントロールパネル] - [管理ツール] - [クラスタアドミニストレータ] を選択して、クラスタアドミニストレータを表示します。
2. クラスタアドミニストレータで、次のリソースをオフラインにします。

- HBase Storage Mgmt Common Service
- HBase Storage Mgmt Web Service

3. 次のとおりコマンドを実行して、Hitachi File Services Manager および Hitachi Command Suite 共通コンポーネントを停止します。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ >%bin%\cmdssrv /stop
```

4. クラスタアドミニストレータで、HiRDB/ClusterService_HD0 をオフラインにします。
5. リソースが再起動しないように設定します。クラスタアドミニストレータで次のリソースのプロパティを開き、[詳細設定] - [再開しない] を選択して、[OK] ボタンをクリックします。

- HBase Storage Mgmt Common Service
- HBase Storage Mgmt Web Service
- HiRDB/ClusterService_HD0

6. 次のとおりコマンドを実行して、HiRDB を起動します。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ >%bin%\cmdsdbsrv /start
```

7. 次のとおりコマンドを実行して、データベースのバックアップを取得します。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ >%bin%\cmdsdbackups /dir <バックアップ先フォルダ>
```

バックアップ先フォルダには、ローカルディスク上のフォルダを絶対パスで指定してください。実在するフォルダを指定する場合は、空のフォルダであることを確認してください。

指定できる文字は英数字、スペース、感嘆符 (!)、番号記号 (#)、始め丸括弧 ((), 終わり丸括弧 ()), 正符号 (+)、ハイフン (-)、ピリオド (.), 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 (_), 始め波括弧 ({), 終わり波括弧 (}), および波ダッシュ (~) です。また、パスの区切り文字として、斜線 (/)、コロン (:) および円記号 (¥) を使用できます。

hcmdsbackups コマンドを実行すると、/dir オプションに指定したバックアップファイルの格納先フォルダに database というフォルダが作成され、データベースのバックアップファイルが backup.hdb というファイル名で格納されます。

8. 実行系ノードに Hitachi File Services Manager をアップグレードインストールまたは上書きインストールします。

Hitachi File Services Manager をアップグレードインストールまたは上書きインストールする手順については、「7.1.2 Hitachi File Services Manager をアップグレード・上書きインストールする」を参照してください。

9. 次のとおりコマンドを実行して、Hitachi File Services Manager および Hitachi Command Suite 共通コンポーネントを停止します。

```
<Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%bin%hcmdsrv /stop
```

10. Windows の [サービス] ウィンドウで次のリソースのプロパティを開き、[スタートアップの種類] を [自動] から [手動] に変更します。

- HBase Storage Mgmt Common Service
- HBase Storage Mgmt Web Service

また、Windows Server 2008 または Windows Server 2012 を使用している場合は、コマンドプロンプトから次のコマンドを実行してください。

```
cluster res "<リソース名>" /priv StartupParameters=""
```

<リソース名>には、HBase Storage Mgmt Web Service の汎用サービスのリソース名を指定します。リソース名は「フェールオーバー クラスタ管理」で確認してください。

11. クラスタアドミニストレータで、Hitachi File Services Manager のリソースが登録されているグループを待機系に切り替えます。

待機系に切り替えるために、Hitachi File Services Manager が使用するリソースを登録しているグループを右クリックし、[グループの移動] を選択してください。

(2) 管理サーバの待機系ノードでのアップグレード・上書きインストール

待機系ノードに Hitachi File Services Manager をアップグレードインストールまたは上書きインストールし、クラスタ設定する手順を次に示します。

1. 次のとおりコマンドを実行して、Hitachi File Services Manager および Hitachi Command Suite 共通コンポーネントを停止します。

```
<Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%bin%hcmdsrv /stop
```

2. 次のとおりコマンドを実行して、HiRDB を起動します。

```
<Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%bin%hcmdsbsrv /start
```

3. 次のとおりコマンドを実行して、データベースのバックアップを取得します。

```
<Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%bin%hcmdsbackups /dir <バックアップ先フォルダ>
```

バックアップ先フォルダには、ローカルディスク上のフォルダを絶対パスで指定してください。実在するフォルダを指定する場合は、空のフォルダであることを確認してください。

指定できる文字は英数字、スペース、感嘆符 (!)、番号記号 (#)、始め丸括弧 ((), 終わり丸括弧 ()), 正符号 (+)、ハイフン (-)、ピリオド (.), 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лекс (^)、アンダーライン (_), 始め波括弧 ({), 終わり波括弧 (})

(`{}`), 終わり波括弧 (`}`), および波ダッシュ (`~`) です。また, パスの区切り文字として, 斜線 (`/`), コロン (`:`) および円記号 (`¥`) を使用できます。

`hcmdsbackups` コマンドを実行すると, `/dir` オプションに指定したバックアップファイルの格納先フォルダに `database` というフォルダが作成され, データベースのバックアップファイルが `backup.hdb` というファイル名で格納されます。

4. 待機系ノードに **Hitachi File Services Manager** をアップグレードインストールまたは上書きインストールします。

Hitachi File Services Manager をアップグレードインストールまたは上書きインストールする手順については, 「[7.1.2 Hitachi File Services Manager をアップグレード・上書きインストールする](#)」を参照してください。

5. 次のとおりコマンドを実行して, **Hitachi File Services Manager** および **Hitachi Command Suite** 共通コンポーネントを停止します。

```
<Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%bin%hcmdssrv /stop
```

6. Windows の [サービス] ウィンドウで次のリソースのプロパティを開き, [スタートアップの種類] を [自動] から [手動] に変更します。

- HBase Storage Mgmt Common Service
- HBase Storage Mgmt Web Service

7. クラスタアドミニストレータで, **Hitachi File Services Manager** のリソースが登録されているグループを実行系に切り替えます。

実行系に切り替えるために, **Hitachi File Services Manager** が使用するリソースを登録しているグループを右クリックし, [グループの移動] を選択してください。

8. クラスタアドミニストレータで次のリソースのプロパティを開き, [詳細設定] - [再開する] を選択して, [OK] ボタンをクリックします。

- HBase Storage Mgmt Common Service
- HBase Storage Mgmt Web Service
- HiRDB/ClusterService_HD0

9. クラスタアドミニストレータで, **Hitachi File Services Manager** のリソースを登録しているグループをオンラインにします。

7.2.3 Hitachi File Services Manager を新規・アップグレード・上書きインストールする (Hitachi Command Suite 製品をクラスタ構成で運用している場合)

ここでは, **Hitachi Command Suite** 製品をクラスタ構成で運用している場合に, いったんクラスタ構成を解除し, **Hitachi File Services Manager** をインストールする手順について説明します。

1. **Hitachi Command Suite** 製品のリソースおよびクラスタグループをクラスタの管理対象から外します。

次のとおり操作してください。

- クラスタアドミニストレータで, 管理対象のリソースをオフラインにします。
- クラスタアドミニストレータで, 管理対象のリソースが再起動しないように設定します。リソースのプロパティを開き, [詳細設定] - [再開しない] を選択して, [OK] ボタンをクリックします。対象のリソースが複数ある場合には, この手順を繰り返してください。

2. 実行系ノードおよび待機系ノードで, バージョン 05-70 より古い **HiCommand** 製品のサービスを停止します。

バージョン 05-70 より古い HiCommand 製品がインストールされている場合に必要手順です。サービスを停止する方法については、各製品のマニュアルを参照してください。

3. 実行系ノードおよび待機系ノードで次のとおりコマンドを実行し、Hitachi File Services Manager および Hitachi Command Suite 共通コンポーネントを停止します。

```
<Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%bin%hcmdsdrv /stop
```

4. クラスタドミニストレータで、Hitachi Command Suite 製品のリソースを登録しているグループを待機系に切り替えます。

待機系に切り替えるために、Hitachi Command Suite 製品のリソースを登録しているグループを右クリックし、[グループの移動] を選択してください。

5. 待機系ノードで次のとおりコマンドを実行して、HiRDB を起動します。

```
<Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%bin%hcmdsbsrv /start
```

6. 待機系ノードで次のとおりコマンドを実行して、データベースのバックアップを取得します。

```
<Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%bin%hcmdsbackups /dir <バックアップ先フォルダ>
```

バックアップ先フォルダには、ローカルディスク上のフォルダを絶対パスで指定してください。実在するフォルダを指定する場合は、空のフォルダであることを確認してください。

指定できる文字は英数字、スペース、感嘆符 (!)、番号記号 (#)、始め丸括弧 ((), 終わり丸括弧 ()), 正符号 (+)、ハイフン (-)、ピリオド (.), 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 (_), 始め波括弧 ({), 終わり波括弧 (}), および波ダッシュ (~) です。また、パスの区切り文字として、斜線 (/)、コロ (:) および円記号 (¥) を使用できます。

hcmdsbackups コマンドを実行すると、/dir オプションに指定したバックアップファイルの格納先フォルダに database というフォルダが作成され、データベースのバックアップファイルが backup.hdb というファイル名で格納されます。

7. 待機系ノードで次のとおりコマンドを実行して、データベースをローカルディスクに移行します。

```
<Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%bin%hcmdsdbclustersetup /removecluster /databasepath <データベースの再作成先フォルダ> /exportpath <データの格納先フォルダ>
```

コマンドの引数は、次の条件に従って指定してください。

- データベースの再作成先フォルダは 92 バイト以下、データの格納先フォルダは 85 バイト以下の絶対パスで指定してください。
- データベースの再作成先フォルダおよびデータの格納先フォルダは、ローカルディスク上に配置してください。
- データの格納先フォルダに実在するフォルダを指定する場合は、空のフォルダであることを確認してください。
- データベースの再作成先フォルダおよびデータの格納先フォルダに使用できる文字は英数字、始め丸括弧 ((), 終わり丸括弧 ()), ピリオド (.), アンダーライン (_) およびスペースです。ただし、ピリオド (.) は文字列の先頭および末尾には指定できません。また、スペースは、文字列の先頭および末尾に指定したり、2 つ以上連続して指定したりできません。
- データベースの再作成先フォルダおよびデータの格納先フォルダには、パスの区切り文字として、円記号 (¥) が使用できます。ただし、文字列の末尾には指定できません。

データベース再作成先フォルダには、次に示す空き容量が必要です。

必要な空き容量 = 2.1GB + ほかの Hitachi Command Suite 製品のデータベース容量

データベース再作成先フォルダの空き容量不足が原因で hcmdsdbclustersetup コマンドの実行に失敗した場合は、データベース再作成先フォルダの空き容量を増やしたあとで、hcmdsdbclustersetup コマンドを再実行してください。

hcmdsdbclustersetup コマンドが正常終了するまでは、共有ディスクを実行系ノードから切り離さないでください。

hcmdsdbclustersetup コマンドが異常終了した状態でサーバを再起動すると、共有ディスクの接続先が待機系ノードに切り替わることがあります。

このコマンドを実行すると、HiRDB が使用するポート番号がデフォルト値 (23032) に戻り、Hitachi File Services Manager および Hitachi Command Suite 共通コンポーネントが再起動します。

- HiRDB が使用するポート番号をデフォルト値 (23032) から変更して運用する場合は、変更後のポート番号に設定し直してください。

HiRDB が使用するポート番号を変更する方法については、「[7.5.5 Hitachi Command Suite 共通コンポーネントのポート番号を変更する](#)」を参照してください。

- Hitachi File Services Manager および Hitachi Command Suite 共通コンポーネントが稼働している場合は、次のとおりコマンドを実行して、停止します。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %bin%hcmdssrv /stop
```

- クラスタアドミニストレータで、Hitachi Command Suite 製品のリソースを登録しているグループを実行系に切り替えます。

実行系に切り替えるために、Hitachi Command Suite 製品のリソースを登録しているグループを右クリックし、[グループの移動] を選択してください。

- 実行系ノードで次のとおりコマンドを実行して、HiRDB を起動します。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %bin%hcmdsdsrv /start
```

- 実行系ノードで次のとおりコマンドを実行して、データベースのバックアップを取得します。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %bin%hcmdsbackups /dir <バックアップ先フォルダ >
```

バックアップ先フォルダには、ローカルディスク上のフォルダを絶対パスで指定してください。実在するフォルダを指定する場合は、空のフォルダであることを確認してください。

指定できる文字は英数字、スペース、感嘆符 (!)、番号記号 (#)、始め丸括弧 ((), 終わり丸括弧 ()), 正符号 (+)、ハイフン (-)、ピリオド (.), 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 (_)、始め波括弧 ({), 終わり波括弧 (}), および波ダッシュ (~) です。また、パスの区切り文字として、斜線 (/)、コロン (:) および円記号 (¥) を使用できます。

hcmdsbackups コマンドを実行すると、/dir オプションに指定したバックアップファイルの格納先フォルダに database というフォルダが作成され、データベースのバックアップファイルが backup.hdb というファイル名で格納されます。

- 実行系ノードで次のとおりコマンドを実行して、データベースをローカルディスクに移行します。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %bin%hcmdsdbclustersetup /removecluster /databasepath <データベースの再作成先フォルダ > /exportpath <データの格納先フォルダ >
```

コマンドの引数は、次の条件に従って指定してください。

- データベースの再作成先フォルダは 92 バイト以下、データの格納先フォルダは 85 バイト以下の絶対パスで指定してください。

- データベースの再作成先フォルダおよびデータの格納先フォルダは、ローカルディスク上に配置してください。
- データの格納先フォルダに実在するフォルダを指定する場合は、空のフォルダであることを確認してください。
- データベースの再作成先フォルダおよびデータの格納先フォルダに使用できる文字は英数字、始め丸括弧 ((), 終わり丸括弧 ()), ピリオド (.), アンダーライン (_) およびスペースです。ただし、ピリオド (.) は文字列の先頭および末尾には指定できません。また、スペースは、文字列の先頭および末尾に指定したり、2 つ以上連続して指定したりできません。
- データベースの再作成先フォルダおよびデータの格納先フォルダには、パスの区切り文字として、円記号 (¥) が使用できます。ただし、文字列の末尾には指定できません。

hcmsbdbclustersetup コマンドが正常終了するまでは、共有ディスクを実行系ノードから切り離さないでください。

また、hcmsbdbclustersetup コマンドが異常終了した状態でサーバを再起動しないでください。

このコマンドを実行すると、HiRDB が使用するポート番号がデフォルト値 (23032) に戻り、Hitachi File Services Manager および Hitachi Command Suite 共通コンポーネントが再起動します。

14. HiRDB が使用するポート番号をデフォルト値 (23032) から変更して運用する場合は、変更後のポート番号に設定し直してください。

HiRDB が使用するポート番号を変更する方法については、「[7.5.5 Hitachi Command Suite 共通コンポーネントのポート番号を変更する](#)」を参照してください。

15. Hitachi File Services Manager を新規インストール、アップグレードインストールまたは上書きインストールしたあと、クラスタを構成してください。

Hitachi Command Suite 製品のクラスタ設定については、各製品のマニュアルを参照してください。

7.2.4 Hitachi File Services Manager をアンインストールする（管理サーバをクラスタ構成で運用する場合）

ここでは、管理サーバをクラスタ構成で運用する場合に、Hitachi File Services Manager をアンインストールする方法について説明します。実行系ノード、および待機系ノードで次の手順を実行してください。

実行系ノードでリソースがオンラインになっていない場合は、オンラインにしてからアンインストールしてください。

1. Windows の [スタート] - [設定] - [コントロールパネル] - [管理ツール] - [クラスタアドミニストレータ] を選択して、クラスタアドミニストレータを表示します。
2. クラスタアドミニストレータで、Hitachi File Services Manager のリソースが登録されているグループを実行系に切り替えます。
実行系に切り替えるために、Hitachi File Services Manager が使用するリソースを登録しているグループを右クリックし、[グループの移動] を選択してください。
3. クラスタアドミニストレータで、次のリソースをオフラインにします。

- HBase Storage Mgmt Common Service
- HBase Storage Mgmt Web Service

4. 実行系ノードで次のとおりコマンドを実行し、Hitachi File Services Manager および Hitachi Command Suite 共通コンポーネントを停止します。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %bin%hcmdssrv /stop
```

5. クラスタアドミニストレータで、HiRDB/ClusterService_HD0 をオフラインにします。
6. 次のうち、ほかのアプリケーションによって使用されていないリソースを削除します。
 - HBase Storage Mgmt Common Service
 - HBase Storage Mgmt Web Service
 - HiRDB/ClusterService_HD0
7. クラスタアドミニストレータで、手順 6 で削除しなかったリソースを次のとおり操作します。
リソースのプロパティを開き、[詳細設定] - [再開しない] を選択して、[OK] ボタンをクリックします。
8. 実行系ノードで Hitachi File Services Manager をアンインストールします。
Hitachi File Services Manager のアンインストール手順については、「[7.1.4 Hitachi File Services Manager をアンインストールする](#)」を参照してください。
9. クラスタアドミニストレータで、Hitachi File Services Manager のリソースが登録されているグループを待機系に切り替えます。
待機系に切り替えるために、Hitachi File Services Manager が使用するリソースを登録しているグループを右クリックし、[グループの移動] を選択してください。
10. 待機系ノードで次のとおりコマンドを実行し、Hitachi File Services Manager および Hitachi Command Suite 共通コンポーネントを停止します。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %bin%hcmdssrv /stop
```

11. 待機系ノードで Hitachi File Services Manager をアンインストールします。
Hitachi File Services Manager のアンインストール手順については、「[7.1.4 Hitachi File Services Manager をアンインストールする](#)」を参照してください。
12. 次のうち、ほかのアプリケーションによって使用されていないリソースを、オフラインにした上で削除します。
 - 共有ディスク
 - クラスタの論理 IP アドレス
13. Hitachi File Services Manager のリソースを登録していたグループが不要になった場合は、削除します。
14. クラスタアドミニストレータで、手順 7 で [再開しない] を設定したリソースを次のとおり操作します。
リソースのプロパティを開き、[詳細設定] - [再開する] を選択して、[OK] ボタンをクリックします。
15. クラスタアドミニストレータで、手順 14 で [再開する] を設定したリソースをオンラインにします。

7.3 Hitachi File Services Manager を起動・停止する

システム管理者は、Hitachi Command Suite 共通コンポーネントを起動・停止することで、Hitachi File Services Manager を同時に起動・停止できます。

この節では、Hitachi File Services Manager を起動・停止する方法、および Hitachi File Services Manager の稼働状態を確認する方法について説明します。

7.3.1 常駐プロセス一覧

Hitachi File Services Manager および Hitachi Command Suite 共通コンポーネントの常駐プロセスを次の表に示します。

表 7-5 Hitachi File Services Manager および Hitachi Command Suite 共通コンポーネントの常駐プロセス

プロセス	機能
hcmdssvctl.exe	Hitachi Command Suite サブレットサービスのプロセス
hntr2mon.exe	Hitachi Command Suite 共通トレース情報採取プロセス
hntr2srv.exe	Hitachi Command Suite 共通トレースサービスプロセス
httpsd.exe	Hitachi Command Suite 共通 Web サービスのプロセス

7.3.2 Hitachi File Services Manager を起動する

次のどちらかの方法で、Hitachi File Services Manager を起動できます。

- Windows のメニューから実行する
- コマンドを使用する

ここでは、Hitachi File Services Manager を起動する方法について説明します。Device Manager の GUI にログインして HVFP/HDI を運用・管理している場合は、Device Manager および Hitachi Command Suite 共通コンポーネントを起動する必要があります。Device Manager および Hitachi Command Suite 共通コンポーネントを起動する方法については、Device Manager のマニュアルを参照してください。



参考 05-70 以降の製品の場合、Hitachi Command Suite 共通コンポーネントを起動することで、Device Manager などの Hitachi Command Suite 製品のサービスも、同時に起動されます。

(1) Windows のメニューから実行する場合

Windows のメニューから Hitachi File Services Manager を起動する手順を次に示します。

1. Administrator または Administrators グループのユーザーで Windows にログオンします。
2. Windows 7 までの Windows の場合は、[スタート] - [プログラム] - [Hitachi Command Suite] - [File Services Manager] - [Start - HFSM] を選択します。

Windows 8 または Windows Server 2012 の場合は、スタート画面のアプリ一覧から [Start - HFSM] を選択します。

コマンドプロンプトの画面上に処理の経過が表示されます。

3. 処理が完了したあと、何かキーを押してコマンドプロンプトを終了します。

(2) コマンドを使用する場合

コマンドを使用して、Hitachi File Services Manager を起動する手順を次に示します。

1. 次のとおりコマンドを実行して、Hitachi File Services Manager を起動します。

```
<Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%bin%hcmdssrv / start
```

7.3.3 Hitachi File Services Manager を停止する

次のどちらかの方法で、Hitachi File Services Manager を停止できます。

- Windows のメニューから実行する
- コマンドを使用する

ここでは、Hitachi File Services Manager を停止する方法について説明します。Device Manager の GUI にログインして HVFP/HDI を運用・管理している場合は、Device Manager および Hitachi Command Suite 共通コンポーネントを停止する必要があります。Device Manager および Hitachi Command Suite 共通コンポーネントを停止する方法については、Device Manager のマニュアルを参照してください。



参考 05-70 以降の製品の場合、Hitachi Command Suite 共通コンポーネントを停止することで、Device Manager などの Hitachi Command Suite 製品のサービスも、同時に停止されます。

(1) Windows のメニューから実行する場合

Windows のメニューから Hitachi File Services Manager を停止する手順を次に示します。

1. Administrator または Administrators グループのユーザーで Windows にログオンします。
2. Windows 7 までの Windows の場合は、[スタート] - [プログラム] - [Hitachi Command Suite] - [File Services Manager] - [Stop - HFSM] を選択します。

Windows 8 または Windows Server 2012 の場合は、スタート画面のアプリ一覧から [Stop - HFSM] を選択します。

コマンドプロンプトの画面上に処理の経過が表示されます。

3. 処理が完了したあと、何かキーを押してコマンドプロンプトを終了します。

(2) コマンドを使用する場合

コマンドを使用して、Hitachi File Services Manager を停止する手順を次に示します。

1. 次のとおりコマンドを実行して、Hitachi File Services Manager を停止します。

```
<Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%bin%hcmdssrv /stop
```

7.3.4 Hitachi File Services Manager の稼働状態を確認する

次のどちらかの方法で、Hitachi File Services Manager の稼働状態を確認できます。

- Windows のメニューから実行する
- コマンドを使用する

ここでは、Hitachi File Services Manager の稼働状態を確認する方法について説明します。Device Manager の GUI にログインして HVFP/HDI を運用・管理している場合は、Device Manager および Hitachi Command Suite 共通コンポーネントの稼働状態を確認する必要があります。Device Manager および Hitachi Command Suite 共通コンポーネントの稼働状態を確認する方法については、Device Manager のマニュアルを参照してください。

(1) Windows のメニューから実行する場合

Windows のメニューから Hitachi File Services Manager の稼働状態を確認する手順を次に示します。

1. Administrator または Administrators グループのユーザーで Windows にログオンします。
2. Windows 7 までの Windows の場合は、[スタート] - [プログラム] - [Hitachi Command Suite] - [File Services Manager] - [Status - HFSM] を選択します。

Windows 8 または Windows Server 2012 の場合は、スタート画面のアプリ一覧から [Status - HFSM] を選択します。

コマンドプロンプトの画面上に、Hitachi File Services Manager の稼働状態を示すメッセージが表示されます。Hitachi File Services Manager および Hitachi Command Suite 共通コンポーネントが正常に起動している場合は、次のメッセージが出力されます。

```
KAPM06440-I The HiRDB service has already started.
KAPM05007-I Already started service. service-name= HBase Storage Mgmt Web
Service
KAPM05007-I Already started service. service-name= HBase Storage Mgmt Common
Service
```

3. Hitachi File Services Manager の稼働状態を確認したあと、何かキーを押してコマンドプロンプトを終了します。

(2) コマンドを使用する場合

コマンドを使用して、Hitachi File Services Manager の稼働状態を確認する手順を次に示します。

1. 次のとおりコマンドを実行して、Hitachi File Services Manager の稼働状態を確認します。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %bin%hcmdssrv /
status
```

Hitachi File Services Manager および Hitachi Command Suite 共通コンポーネントが正常に起動している場合は、次のメッセージが出力されます。

```
KAPM06440-I The HiRDB service has already started.
KAPM05007-I Already started service. service-name= HBase Storage Mgmt Web
Service
KAPM05007-I Already started service. service-name= HBase Storage Mgmt Common
Service
```

7.4 システム管理者のアカウントを管理する

システム管理者は、設定ファイルを編集して、システム管理者のアカウントを管理できます。また、Hitachi File Services Manager を Device Manager の GUI からログインして利用する場合は、必要に応じて、Hitachi File Services Manager のユーザーアカウントを管理するサーバを変更できます。

管理サーバをクラスタ構成で運用している場合は、実行系ノードと待機系ノードで同一の設定にしてください。

外部認証サーバでシステム管理者のアカウントを認証する前に

Hitachi File Services Manager では、外部認証サーバと連携してユーザー認証できます。外部認証サーバに登録されているユーザー ID を Hitachi File Services Manager にも登録しておくことで、外部認証サーバに登録されたユーザー ID を使って、Hitachi File Services Manager にログインできます。このため、Hitachi File Services Manager でのログインパスワードの管理やアカウントの制御が不要になります。

また、外部認証サーバと外部認可サーバを併用することで、Hitachi File Services Manager に対するユーザーのアクセス権限を外部認可サーバで制御できます。外部認可サーバとも連携する場合、Hitachi File Services Manager では、ユーザーを外部認可サーバのグループ（認可グループ）ごとに管理するため、Hitachi File Services Manager での個々のユーザーのアカウント管理や権限設定が不要になります。

外部認証サーバとだけ連携する場合と、外部認可サーバとも連携する場合で、外部認証サーバおよび外部認可サーバのマシン要件が異なります。それぞれのマシン要件は、「3.5 LDAP サー

バの環境設定」, 「3.7 KDC サーバの環境設定」または「3.8 RADIUS サーバの環境設定」を参照してください。

注意：

外部認証サーバと連携するための設定で実行するコマンドの引数に、コマンドラインの制御文字が含まれる場合には、コマンドラインの仕様に従い正しくエスケープしてください。

また、円記号 (¥) はコマンドラインでは特殊な扱いとなるため、引数に円記号 (¥) が含まれる場合には注意が必要です。

次の文字が含まれる場合は、引数を引用符 (") で囲むか、1文字ごとにアクサンシルコンプレックス (^) でエスケープしてください。

空白文字 & | ^ < > ()

円記号 (¥) は、次に続く文字によってはエスケープ文字として扱われることがあります。このため、引数に円記号 (¥) と上記の文字が含まれる場合には、引用符 (") で囲まないで、上記文字を1文字ごとにアクサンシルコンプレックス (^) でエスケープしてください。

また、引数の末尾に円記号 (¥) がある場合は、円記号 (¥) でエスケープしてください。

例えば、hcmdsradiussecret コマンドで登録する共有秘密鍵が「secret01¥」の場合は、次のとおりエスケープしてください。

```
hcmdsradiussecret /set secret01¥¥ /name ServerName
```

7.4.1 システム管理者のアカウントに関するセキュリティを設定する

システム管理者は、システム管理者のアカウントのパスワードとして設定できる最小文字数および文字の組み合わせの条件を設定できます。条件を設定することで、システム管理者のパスワードが第三者に利用されるリスクを軽減できます。

また、ログイン失敗時にアカウントが自動的にロックされるよう設定できます。ログインに複数回失敗したアカウントを自動的にロックすることで、不正に GUI にアクセスされるリスクを軽減できます。

注意：

Hitachi Command Suite 共通コンポーネントでは、ユーザーアカウントのロック機能、およびパスワードの複雑性チェック機能が使用できます。これらの機能は、Hitachi File Services Manager および Hitachi Command Suite 製品のユーザーに対して有効になるため、これらの機能が使用できないバージョン 05-00 以前の HiCommand 製品および Hitachi File Services Manager の操作で、次の現象が起こるおそれがあります。

- 正しいユーザー ID とパスワードを指定しても、ログインできない。
アカウントがロックされているおそれがあります。該当するアカウントのロックを解除する、新しいアカウントを登録するなど、適切な対処をしてください。
- パスワードが変更できない、またはユーザーアカウントが追加できない。
指定したパスワードが、パスワードの入力規則に従っていないおそれがあります。出力されるメッセージに従って、適切なパスワードを指定してください。

パスワードの条件や、アカウントの自動ロックに関する設定を行う方法には次の2つの方法があります。

- security.conf ファイルで設定する
- GUI を使用して設定する

ここでは、security.conf ファイルを使用して、パスワードの条件や、アカウントのロックに関する設定を行う方法を説明します。

(1) パスワードの条件を設定する

パスワードの条件は、security.conf ファイルで指定します。security.conf ファイルは、管理サーバの次のフォルダに格納されています。

< Hitachi Command Suite 共通コンポーネントのインストールフォルダ >¥conf¥sec¥

security.conf ファイルでの設定値を変更した場合は、直ちに変更後の値が有効になります。

設定したパスワードの条件は、システム管理者のアカウントを追加するとき、またはシステム管理者のパスワードを変更するときに適用されます。既存のアカウントのパスワードには適用されないため、パスワードが設定した条件を満たしていない場合でも、システム管理者は GUI にログインできます。

security.conf ファイルで指定するパスワードの条件を次に示します。

表 7-6 security.conf ファイルで指定するパスワードの条件

項目	説明
password.min.length	パスワードの最小文字数を指定します。指定できる値の範囲は、1～256です。 デフォルトは「4」です。
password.min.uppercase	パスワードに含める大文字の最小数を指定します。指定できる値の範囲は、0～256です。「0」を指定した場合、大文字の数に制限はなくなります。 デフォルトは「0」です。
password.min.lowercase	パスワードに含める小文字の最小数を指定します。指定できる値の範囲は、0～256です。「0」を指定した場合、小文字の数に制限はなくなります。 デフォルトは「0」です。
password.min.numeric	パスワードに含める数字の最小数を指定します。指定できる値の範囲は、0～256です。「0」を指定した場合、数字の数に制限はなくなります。 デフォルトは「0」です。
password.min.symbol	パスワードに含める記号の最小数を指定します。指定できる値の範囲は、0～256です。「0」を指定した場合、記号の数に制限はなくなります。 デフォルトは「0」です。
password.check.userID	ユーザー ID と同じ文字列をパスワードとして使用することを許可するかどうかを指定します。 true ユーザー ID と同じ文字列をパスワードとして使用すること許可しない場合に選択します。 false ユーザー ID と同じ文字列をパスワードとして使用すること許可する場合に選択します。 デフォルトは「false」です。

security.conf ファイルでの指定例を次に示します。

```
# This is the minimum length of the password
# (minimum: 1 -256characters)
password.min.length=4

# This is the minimum number of uppercase characters included in the password
# (minimum: 0-256 characters, character type: A-Z)
password.min.uppercase=0

# This is the minimum number of lowercase characters included in the password
# (minimum: 0-256 characters, character type: a-z)
password.min.lowercase=0
```

```
# This is the minimum number of numeric characters included in the password
# (minimum: 0-256 characters, character type: 0-9)
password.min.numeric=0

# This is the minimum number of symbolic characters included in the password
# (minimum: 0-256 characters, character type: ! # $ % & ' ( ) * + - . = @ ¥ ^ _
|)
password.min.symbol=0

# This specifies whether the user ID can be used for the password.
# (true = cannot use the user ID, false = can use the user ID)
password.check.userID=false
```

(2) アカウントの自動ロックに関して設定する

アカウントの自動ロックに関する設定は、`security.conf` ファイルで指定します。
`security.conf` ファイルは、管理サーバの次のフォルダに格納されています。
 <Hitachi Command Suite 共通コンポーネントのインストールフォルダ>¥conf¥sec¥
`security.conf` ファイルでの設定値を変更した場合は、直ちに変更後の値が有効になります。

注意：

- 設定した失敗回数の上限は、ログイン認証時に適用されます。
 例えば、失敗回数の設定を 5 回から 2 回に変更した場合、その時点で連続 3 回ログインに失敗しているアカウントはロックされません。次 (4 回目) にパスワードを正しく指定した場合にはログインは許可され、ログインに失敗した場合はアカウントがロックされます。
- ログイン中のシステム管理者のアカウントが自動ロックされた場合、ログアウトするまでは操作を継続できます。

`security.conf` ファイルで指定するアカウントの自動ロックに関する設定を次に示します。

表 7-7 security.conf ファイルで指定するアカウントの自動ロックに関する設定

項目	説明
<code>account.lock.num</code>	ユーザーアカウントが自動的にロックされるまでの、ログインの失敗回数を指定します。 指定できる値の範囲は、0~10 です。「0」を指定した場合、ユーザーがログインに何度失敗しても、ユーザーアカウントはロックされません。 デフォルトは「0」です。

`security.conf` ファイルでの指定例を次に示します。

```
...
# This is the minimum number of login failures before an account is locked
# (minimum: 0-10 times)
account.lock.num=0
...
```

7.4.2 System アカウントのロックに関して設定する

システム管理者は、`user.conf` ファイルを編集して、System アカウントがロックされるよう設定できます。初期導入時には、System アカウントは自動ロックおよび手動ロックの対象にはなっていません。

System アカウントのロックに関する設定を変更するときの手順を次に示します。

- `user.conf` ファイルを編集して、System アカウントのロックに関する設定を変更します。

user.conf ファイルは、管理サーバの次のフォルダに格納されています。user.conf ファイルが存在しない場合は、新規に作成してください。

< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %conf%

2. Hitachi File Services Manager および Hitachi Command Suite 共通コンポーネントをいったん停止したあと、起動し直します。

Hitachi File Services Manager および Hitachi Command Suite 共通コンポーネントを停止・起動する方法については、「7.3 Hitachi File Services Manager を起動・停止する」を参照してください。

System アカウントのロックに関する設定を変更するためのプロパティを次の表に示します。

表 7-8 user.conf ファイルのプロパティ (System アカウントのロックに関する設定の変更)

プロパティ	説明
account.lock.system	System アカウントをロックするかどうかを指定します。 true System アカウントをロックする場合に選択します。この場合、System アカウントを手動でロックできるようになります。 false System アカウントをロックしない場合に選択します。この場合、System アカウントをロックできなくなります。 デフォルトは「false」です。上記以外の文字列を指定した場合は、「false」を指定したものとして処理されます。

user.conf ファイルの記述例を次に示します。

```
...  
account.lock.system=true  
...
```

注意：

バージョン 6.1 以降の Hitachi Command Suite 製品をインストールし、user.conf ファイルに true を設定した場合、すべての Hitachi Command Suite 製品で、System アカウントが自動ロックおよび手動ロックの対象になります。バージョン 06-00 以前の Hitachi Storage Command Suite 製品で、System アカウントでログインできなくなった場合には、アカウントがロックされているおそれがあります。[ユーザー] サブウィンドウでアカウントのロックを解除してください。

7.4.3 システム管理者のアカウントのロックを解除する

ユーザー管理の Admin 権限を持つシステム管理者は、[ユーザー] サブウィンドウでシステム管理者のアカウントのロックを解除できます。また、コマンドを使用することもできます。

コマンドを使用して、システム管理者のアカウントのロックを解除する手順を次に示します。

1. 次のとおりコマンドを実行して、Hitachi Command Suite 共通コンポーネントのサービスが稼働していることを確認します。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %bin%hcmdsdrv /  
status
```

2. 次のとおりコマンドを実行して、ロックを解除します。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %bin%  
%hcmdsunlockaccount /user <ロックを解除するユーザーのユーザー ID > /pass <ロックを解  
除するユーザーのパスワード >
```

7.4.4 LDAP サーバで外部認証する

LDAP サーバでシステム管理者のアカウントを認証するために、Hitachi File Services Manager では次の設定が必要です。

1. LDAP サーバのデータ構造を確認し、Hitachi File Services Manager と連携して認証を行う方法を確認します。
2. 管理サーバの `exauth.properties` ファイルに必要な情報を設定します。
外部認証サーバとだけ連携する場合と、外部認可サーバとも連携する場合で設定が異なります。また、LDAP サーバは、次のどちらかの方法で定義できます。

- `exauth.properties` ファイルに接続先の LDAP サーバの情報を直接指定する
IP アドレスやポート番号などの情報を LDAP サーバごとに `exauth.properties` ファイルに指定します。
- DNS サーバに接続先の LDAP サーバを照会する
LDAP サーバの OS で DNS サーバの環境設定が完了している必要があります。また、DNS サーバの SRV レコードに、LDAP サーバのホスト名やポート番号、ドメイン名などを登録しておく必要があります。

重要：

- 管理サーバと LDAP サーバとの間の通信に StartTLS を使用する場合は、`exauth.properties` ファイルに接続先の LDAP サーバの情報を直接指定する必要があります。
- DNS サーバに接続先の LDAP サーバを照会する場合は、ユーザーがログインする際に処理に時間が掛かることがあります。

3. 次の場合は、LDAP サーバ内のユーザー情報を検索するためのユーザーアカウント（情報検索用のユーザーアカウント）を管理サーバに登録します。

- データ構造が階層モデルのとき
- データ構造がフラットモデルで、かつ外部認可サーバとも連携するとき※

注※

GUI で認可グループを Hitachi File Services Manager に登録する際（手順 5）に、認可グループの **Distinguished Name** が外部認可サーバに登録されているか確認したい場合、System アカウントなど Hitachi File Services Manager に登録されたユーザー ID で操作するためには、情報検索用のユーザーアカウントを管理サーバに登録しておく必要があります。

4. LDAP サーバに、Hitachi File Services Manager を使用するユーザーのアカウントを登録します。

ユーザー ID およびパスワードは、Hitachi File Services Manager で使用できる文字で構成されている必要があります。1 バイト以上 256 バイト以内で次の文字を使用できます。

`A~Z a~z 0~9 ! # $ % & ' () * + - . = @ ¥ ^ _ |`

Hitachi File Services Manager では、ユーザー ID の大文字と小文字の違いは区別されません。また、パスワードの文字種の組み合わせは、外部認証サーバでの設定に従ってください。

5. GUI で、アカウントの登録や権限の設定などを実施します。

外部認証サーバとだけ連携する場合

- ユーザーの登録
- ユーザーの認証方式の変更
既存のユーザーの認証方式を変更する場合に必要な設定です。

- ユーザーグループへのユーザーの登録
- ユーザー管理と Hitachi File Services Manager の操作権限の設定
外部認可サーバとも連携する場合
- 認可グループの登録
- ユーザー管理と Hitachi File Services Manager の操作権限の設定

参考：

登録した認可グループのネストグループに属するユーザーも、認可グループに設定された
ロール（権限）で Hitachi File Services Manager を操作できるようになります。

6. hcmdscheckauth コマンドを使用して、外部認証サーバおよび外部認可サーバに正しく接続できるか確認します。

ここでは、管理サーバで必要な作業について説明します。

(1) データ構造と認証方法の確認

LDAP サーバのデータ構造には次の 2 つがあります。

- 階層構造モデル
- フラットモデル

データ構造によって、exauth.properties ファイルに設定する情報や管理サーバで必要な作業が異なるため、どちらに該当しているかを確認してください。

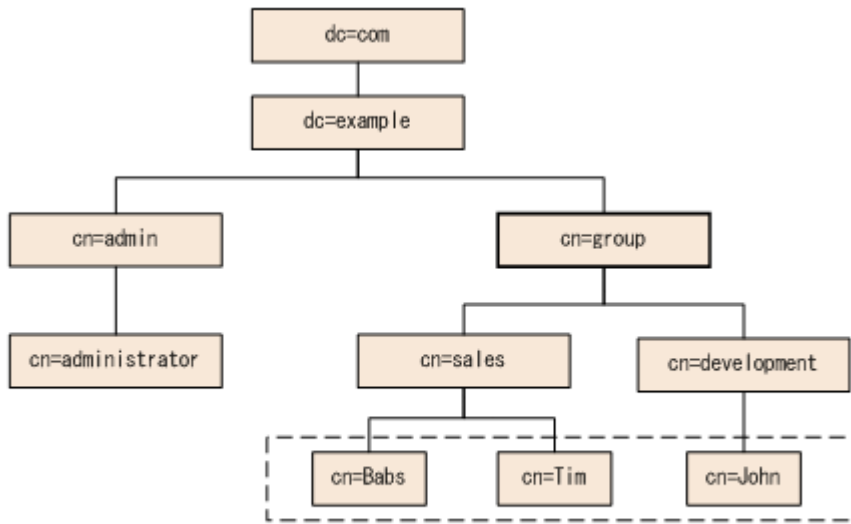
また、認証の際にユーザーを検索する起点となるエントリー（BaseDN）についても確認してください。BaseDN は exauth.properties ファイルの設定で必要な情報です。BaseDN より下の階層のユーザーエントリーが認証の対象となります。Hitachi File Services Manager で認証したいユーザーをすべて含むエントリーであることが必要です。

階層構造モデル

BaseDN より下の階層が分岐していて、かつ別の階層下にユーザーエントリーが登録されているデータ構造の場合は階層構造モデルになります。階層構造モデルの場合は、BaseDN より下のエントリーを対象に、ログイン ID とユーザー属性値が等しいエントリーが検索されます。

次の図に階層構造モデルの例を示します。点線で囲まれた範囲が、認証の対象となるユーザーエントリーです。この例では、対象のユーザーエントリーが「cn=sales」と「cn=development」の 2 つのエントリーにわたって属しているので、BaseDN は「cn=group,dc=example,dc=com」となります。

図 7-9 階層構造モデルの例



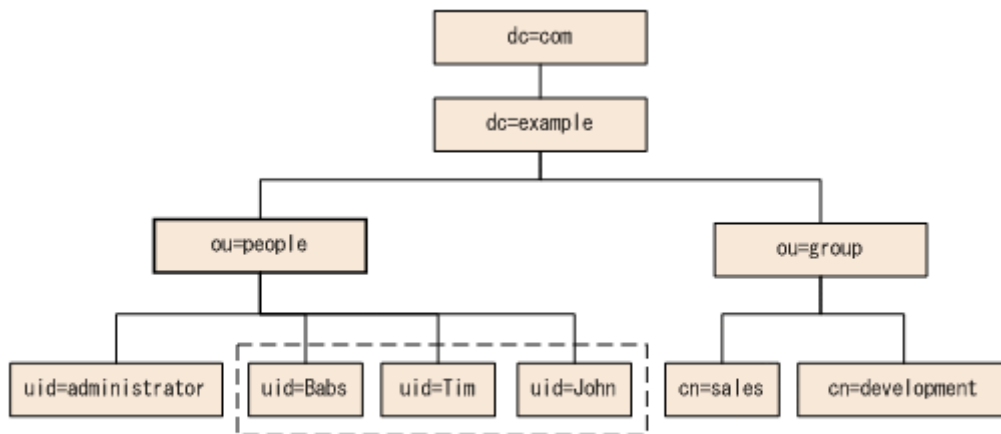
(凡例) []: 認証対象のユーザーエントリー

フラットモデル

BaseDN より下に分岐がなく、かつ直下にユーザーエントリーが登録されているデータ構造の場合はフラットモデルになります。フラットモデルの場合は、BaseDN より下のエントリーを対象に、ログイン ID と BaseDN を組み合わせた DN を持つエントリーが認証されます。

次の図にフラットモデルの例を示します。点線で囲まれた範囲が、認証の対象となるユーザーエントリーです。この例では、認証対象のすべてのユーザーエントリーが「ou=people」の直下に属しているので、BaseDN は「ou=people,dc=example,dc=com」となります。

図 7-10 フラットモデルの例



(凡例) []: 認証対象のユーザーエントリー

ただし、次のどちらかに該当する場合は、データ構造がフラットモデルであっても、階層構造モデルの場合の説明に従って設定してください。

- Hitachi File Services Manager のユーザー ID として、RDN の属性以外のユーザー属性値を使用する
ユーザーエントリーの RDN の属性値以外のユーザー属性値 (Windows のログオン ID など) をユーザー ID として使用する場合には、階層構造モデルの場合の認証方法の設定が必要です。

- ユーザーエントリーの RDN の属性値に、Hitachi File Services Manager のユーザー ID として使用できない文字が使われている

フラットモデルの場合の認証では、ユーザーエントリーの RDN の属性値を Hitachi File Services Manager のユーザー ID として使用します。そのため、Hitachi File Services Manager のユーザー ID として使用できない文字が使われている場合は、フラットモデルの場合の認証を行うことができません。

使用できる RDN の例：

```
uid=John123S
```

```
cn=John_Smith
```

使用できない RDN の例：

```
uid=John:123S (コロン (:)) が使用されている
```

```
cn=John Smith (スペースが使用されている)
```

(2) exauth.properties ファイルの設定 (認証方式が LDAP の場合)

ここでは、LDAP サーバでユーザー認証する場合に exauth.properties ファイルで必要な設定について説明します。

- exauth.properties ファイルで、次のプロパティに値を設定します。

- 共通のプロパティ (表 7-9 LDAP サーバで認証する場合の exauth.properties ファイルの設定項目 (共通項目))
- 外部認証サーバと外部認可サーバのプロパティ

LDAP サーバごとに設定します。

LDAP サーバの情報を直接指定する場合 (「表 7-10 LDAP サーバで認証する場合の exauth.properties ファイルの設定項目 (外部認証サーバの情報を直接指定するとき)」および「表 7-11 LDAP サーバで認証する場合の exauth.properties ファイルの設定項目 (外部認証サーバと StartTLS で通信するとき)」) と、DNS サーバに照会する場合 (表 7-12 LDAP サーバで認証する場合の exauth.properties ファイルの設定項目 (外部認証サーバの情報を DNS サーバに照会するとき)) とで設定する項目が異なります。

exauth.properties ファイルのひな形は次の場所に格納されています。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %sample%conf
¥exauth.properties
```

注意：

設定値の先頭および末尾には空白文字を指定しないでください。また、設定値は引用符 ("") で囲まないでください。指定した場合、値は無視され、デフォルト値が採用されます。

- exauth.properties ファイルを次の場所に格納します。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > ¥conf
¥exauth.properties
```

auth.ocsp.enable プロパティと auth.ocsp.responderURL プロパティの設定値を変更した場合には、Hitachi File Services Manager の再起動が必要です。それ以外のプロパティまたは属性の設定値を変更した場合は、直ちに変更後の値が有効になります。

exauth.properties ファイルの設定項目を「表 7-9 LDAP サーバで認証する場合の exauth.properties ファイルの設定項目 (共通項目)」～「表 7-12 LDAP サーバで認証する場合の exauth.properties ファイルの設定項目 (外部認証サーバの情報を DNS サーバに照会するとき)」に示します。

表 7-9 LDAP サーバで認証する場合の exauth.properties ファイルの設定項目 (共通項目)

プロパティ名	説明
auth.server.type	外部認証サーバの種類です。ldap を指定します。

プロパティ名	説明
	デフォルト値：internal（外部認証サーバと連携しない場合）
auth.server.name	LDAP サーバのサーバ識別名を指定します。接続プロトコルやポート番号などの設定（「表 7-10」および「表 7-12」）を LDAP サーバごとに区別するために付ける任意の名称です。初期値として「ServerName」が設定されています。必ず 1 つ以上のサーバ識別名を指定してください。LDAP サーバを複数指定する場合は、サーバ識別名をコンマ（,）で区切ります。同じサーバ識別名は重複して登録しないでください。 指定できる値：64 バイト以内の次の文字列 0～9 A～Z a～z ! # () + - . = @ [] ^ _ { } ~ デフォルト値：なし
auth.group.mapping	外部認可サーバとも連携するかどうかを指定します。 連携する場合は true を指定します。 連携しない場合は false を指定します。 デフォルト値：false

表 7-10 LDAP サーバで認証する場合の exauth.properties ファイルの設定項目（外部認証サーバの情報を直接指定するとき）

属性	説明
protocol ^{※1}	LDAP サーバ接続のプロトコルです。この項目は必須です。 平文による通信の場合は ldap, StartTLS による通信の場合は tls を指定します。 tls を指定する場合には、LDAP サーバで次のどれかの暗号方式を使用できることを事前に確認してください。 <ul style="list-style-type: none"> • TLS_RSA_WITH_AES_256_CBC_SHA • TLS_RSA_WITH_AES_128_CBC_SHA • SSL_RSA_WITH_3DES_EDE_CBC_SHA 指定できる値：ldap または tls デフォルト値：なし
host ^{※2}	LDAP サーバのホスト名または IP アドレスを指定します。ホスト名を指定する場合、IP アドレスへの名前解決ができることを事前に確認してください。 IP アドレスには、IPv4 アドレスと IPv6 アドレスの両方を使用できます。 IPv6 アドレスは必ず角括弧（[]）で囲んでください。この項目は必須です。 デフォルト値：なし
port	LDAP サーバのポート番号です。指定するポートが、LDAP サーバで待ち受けポート番号として設定されていることを事前に確認してください。 指定できる値：1～65535 デフォルト値：389
timeout	LDAP サーバと接続するときの接続待ち時間です。この値を 0 にした場合、タイムアウトしないで、通信エラーが発生するまで待ち続けます。 指定できる値：0～120（秒） デフォルト値：15
attr	認証で使用するユーザー ID の値が定義されている属性名（Attribute Type）です。 <ul style="list-style-type: none"> • 階層構造モデルの場合 ユーザーを一意に特定できる値が格納されている属性名を指定します。 この属性に格納された値を Hitachi File Services Manager のユーザー ID として使用します。^{※3} 例えば、Active Directory を使用している場合で、Windows のログオン ID をユーザー ID として使用したいときは、Windows のログオン ID が値として定義されている属性名「sAMAccountName」を指定します。 • フラットモデルの場合 ユーザーエントリーの RDN の属性名を指定します。

属性	説明
	<p>例えば、ユーザーの DN が 「uid=John,ou=People,dc=example,dc=com」の場合、RDN 「uid=John」の属性名「uid」を指定します。</p> <p>初期値として「sAMAccountName」が設定されています。この項目は必須です。</p> <p>デフォルト値：なし</p>
basedn	<p>LDAP サーバの情報を検索する際に、起点となるエントリーの DN (BaseDN) です。この DN より下の階層のユーザーエントリーが認証の対象となります。指定した値は LDAP サーバにそのまま渡されるため、BaseDN にエスケープが必要な文字が含まれる場合は、正しくエスケープしてください。</p> <ul style="list-style-type: none"> 階層構造モデルの場合 検索対象のユーザーエントリーをすべて含む階層の DN です。 例えば、「図 7-9」の場合、「cn=group,dc=example,dc=com」を指定します。 フラットモデルの場合 検索対象のユーザーエントリーより 1 つ上の階層の DN です。 例えば、「図 7-10」の場合、「ou=people,dc=example,dc=com」を指定します。 <p>この項目は必須です。DN は RFC4514 の規約に従って指定してください。 例えば、次の文字が DN に含まれる場合は、1 文字ごとに円記号 (¥) でエスケープする必要があります。 空白文字 # + ; , < = > ¥ デフォルト値：なし</p>
retry.interval	<p>LDAP サーバとの通信に失敗した場合のリトライ間隔となる秒数です。</p> <p>指定できる値：1~60 (秒)</p> <p>デフォルト値：1</p>
retry.times	<p>LDAP サーバとの通信に失敗した場合のリトライ回数です。この値を 0 にした場合、リトライされません。</p> <p>指定できる値：0~50</p> <p>デフォルト値：20</p>
domain.name	<p>LDAP サーバが管理するドメインの名称です。外部認可サーバとも連携する場合、この項目は必須です。</p> <p>デフォルト値：なし</p>
dns_lookup	<p>false を指定します。</p> <p>デフォルト値：false</p>

注

各属性は、次のように指定します。

auth.ldap.< auth.server.name に指定した値 > . < 属性 > = < 値 >

注※1

LDAP サーバの接続プロトコルに StartTLS を使用する場合には、Hitachi Command Suite 共通コンポーネントのセキュリティ設定が必要です。StartTLS を使用する場合の設定については、「[7.4.8 Hitachi Command Suite 共通コンポーネントのセキュリティを設定する \(LDAP サーバとの通信\)](#)」を参照してください。

注※2

LDAP サーバの接続プロトコルに StartTLS を使用する場合は、host 属性には LDAP サーバの証明書の CN と同じホスト名を設定してください。IP アドレスは使用できません。

注※3

Hitachi File Services Manager のユーザー ID として使用できない文字列が値に含まれていない属性を指定してください。

表 7-11 LDAP サーバで認証する場合の exauth.properties ファイルの設定項目（外部認証サーバと StartTLS で通信するとき）

プロパティ名	説明
auth.ocsp.enable	LDAP サーバと StartTLS で通信する場合に、OCSP レスポンダーまたは CRL を使用して LDAP サーバの電子署名証明書の有効性を検証するかどうかを指定します。 検証する場合は true を、検証しない場合は false を指定します。 デフォルト値：false
auth.ocsp.responderURL	電子署名証明書の AIA フィールドに記載された OCSP レスポンダー以外の OCSP レスポンダーで電子署名証明書の有効性を検証する場合に、OCSP レスポンダーの URL を指定します。省略した場合は、AIA フィールドに記載された OCSP レスポンダーに問い合わせます。 デフォルト値：なし

表 7-12 LDAP サーバで認証する場合の exauth.properties ファイルの設定項目（外部認証サーバの情報を DNS サーバに照会するとき）

属性	説明
protocol	LDAP サーバ接続のプロトコルです。この項目は必須です。 指定できる値：ldap デフォルト値：なし
port	LDAP サーバのポート番号です。指定するポートが、LDAP サーバで待ち受けポート番号として設定されていることを事前に確認してください。 指定できる値：1～65535 デフォルト値：389
timeout	LDAP サーバと接続するときの接続待ち時間です。この値を 0 にした場合、タイムアウトしないで、通信エラーが発生するまで待ち続けます。 指定できる値：0～120（秒） デフォルト値：15
attr	認証で使用するユーザー ID の値が定義されている属性名（Attribute Type）です。 <ul style="list-style-type: none"> 階層構造モデルの場合 ユーザーを一意に特定できる値が格納されている属性名を指定します。この属性に格納された値を Hitachi File Services Manager のユーザー ID として使用します。※ 例えば、Active Directory を使用している場合で、Windows のログオン ID をユーザー ID として使用したいときは、Windows のログオン ID が値として定義されている属性名「sAMAccountName」を指定します。 フラットモデルの場合 ユーザーエントリーの RDN の属性名を指定します。 例えば、ユーザーの DN が 「uid=John,ou=People,dc=example,dc=com」の場合、RDN 「uid=John」の属性名「uid」を指定します。 初期値として「sAMAccountName」が設定されています。この項目は必須です。 デフォルト値：なし
basedn	LDAP サーバの情報を検索する際に、起点となるエントリーの DN（BaseDN）です。この DN より下の階層のユーザーエントリーが認証の対象となります。指定した値は LDAP サーバにそのまま渡されるため、BaseDN にエスケープが必要な文字が含まれる場合は、正しくエスケープしてください。 <ul style="list-style-type: none"> 階層構造モデルの場合 検索対象のユーザーエントリーをすべて含む階層の DN です。 例えば、「図 7-9」の場合、「cn=group,dc=example,dc=com」を指定します。

属性	説明
	<ul style="list-style-type: none"> フラットモデルの場合 検索対象のユーザーエントリより1つ上の階層のDNです。 例えば、「図 7-10」の場合、「ou=people,dc=example,dc=com」を指定します。 <p>この項目は必須です。DNはRFC4514の規約に従って指定してください。 例えば、次の文字がDNに含まれる場合は、1文字ごとに円記号(¥)でエスケープする必要があります。 空白文字 # + ; , < = > ¥ デフォルト値：なし</p>
retry.interval	LDAPサーバとの通信に失敗した場合のリトライ間隔となる秒数です。 指定できる値：1～60(秒) デフォルト値：1
retry.times	LDAPサーバとの通信に失敗した場合のリトライ回数です。この値を0にした場合、リトライされません。 指定できる値：0～50 デフォルト値：20
domain.name	LDAPサーバが管理するドメインの名称です。この項目は必須です。 デフォルト値：なし
dns_lookup	trueを指定します。 ただし、次の属性に値が設定されている場合は、DNSサーバには照会されず、ユーザーが指定した値を使用してLDAPサーバに接続されます。 <ul style="list-style-type: none"> auth.ldap.<auth.server.nameに指定した値>.host auth.ldap.<auth.server.nameに指定した値>.port デフォルト値：false

注

各属性は、次のように指定します。

auth.ldap.<auth.server.nameに指定した値>.<属性>=<値>

注※

Hitachi File Services ManagerのユーザーIDとして使用できない文字列が値に含まれていない属性を指定してください。

設定例を次に示します。

- LDAPサーバの情報を直接指定する場合(外部認証サーバとだけ連携するとき)

```
auth.server.type=ldap
auth.server.name=ServerName
auth.group.mapping=false
auth.ocsp.enable=false
auth.ocsp.responderURL=
auth.ldap.ServerName.protocol=ldap
auth.ldap.ServerName.host=ldap.example.com
auth.ldap.ServerName.port=389
auth.ldap.ServerName.timeout=15
auth.ldap.ServerName.attr=sAMAccountName
auth.ldap.ServerName.basedn=dc=Example,dc=com
auth.ldap.ServerName.retry.interval=1
auth.ldap.ServerName.retry.times=20
auth.ldap.ServerName.dns_lookup=false
```

- LDAPサーバをDNSサーバに照会する場合(外部認証サーバとだけ連携するとき)

```
auth.server.type=ldap
auth.server.name=ServerName
auth.group.mapping=false
auth.ldap.ServerName.protocol=ldap
auth.ldap.ServerName.timeout=15
auth.ldap.ServerName.attr=sAMAccountName
auth.ldap.ServerName.basedn=dc=Example,dc=com
```

```
auth.ldap.ServerName.retry.interval=1
auth.ldap.ServerName.retry.times=20
auth.ldap.ServerName.domain.name=EXAMPLE.COM
auth.ldap.ServerName.dns_lookup=true
```

- LDAP サーバの情報を直接指定する場合（外部認可サーバとも連携するとき）

```
auth.server.type=ldap
auth.server.name=ServerName
auth.group.mapping=true
auth.ocsp.enable=false
auth.ocsp.responderURL=
auth.ldap.ServerName.protocol=ldap
auth.ldap.ServerName.host=ldap.example.com
auth.ldap.ServerName.port=389
auth.ldap.ServerName.timeout=15
auth.ldap.ServerName.attr=sAMAccountName
auth.ldap.ServerName.basedn=dc=Example,dc=com
auth.ldap.ServerName.retry.interval=1
auth.ldap.ServerName.retry.times=20
auth.ldap.ServerName.domain.name=EXAMPLE.COM
auth.ldap.ServerName.dns_lookup=false
```

- LDAP サーバを DNS サーバに照会する場合（外部認可サーバとも連携するとき）

```
auth.server.type=ldap
auth.server.name=ServerName
auth.group.mapping=true
auth.ldap.ServerName.protocol=ldap
auth.ldap.ServerName.timeout=15
auth.ldap.ServerName.attr=sAMAccountName
auth.ldap.ServerName.basedn=dc=Example,dc=com
auth.ldap.ServerName.retry.interval=1
auth.ldap.ServerName.retry.times=20
auth.ldap.ServerName.domain.name=EXAMPLE.COM
auth.ldap.ServerName.dns_lookup=true
```

(3) 情報検索用のユーザーアカウントの登録（認証方式が LDAP の場合）

hcmdsldapuser コマンドを使用して情報検索用のユーザーアカウントを管理サーバに登録します。登録後は、hcmdsldapuser コマンドで、情報検索用のユーザーアカウントを削除したり、管理サーバに情報検索用のユーザーアカウントを登録済みの LDAP サーバを確認したりできます。

この作業は次の場合に必要です。

- データ構造が階層モデルのとき
- データ構造がフラットモデルで、かつ外部認可サーバとも連携するとき※

注※

GUI で認可グループを Hitachi File Services Manager に登録する際に、認可グループの Distinguished Name が外部認可サーバに登録されているか確認したい場合、System アカウントなど Hitachi File Services Manager に登録されたユーザー ID で操作するためには、情報検索用のユーザーアカウントを管理サーバに登録しておく必要があります。

上記以外の場合は、認証・認可時にユーザー情報の検索を行わないため、この作業は不要です。すでに登録されている場合は、削除してください。

情報検索用のユーザーアカウントを登録する

hcmdsldapuser コマンドで情報検索用のユーザーアカウントを登録します。

情報検索用のユーザーアカウントには、次の条件を満たすユーザーアカウントを登録してください。

- LDAP サーバに登録されていること

- `exauth.properties` ファイルの `auth.ldap.< auth.server.name` に指定した値 `>.basedn` で指定した DN にバインドできること
- `exauth.properties` ファイルの `auth.ldap.< auth.server.name` に指定した値 `>.basedn` で指定した DN 以下のすべてのエントリーに対して属性を検索できること
- `exauth.properties` ファイルの `auth.ldap.< auth.server.name` に指定した値 `>.basedn` で指定した DN を参照できること
- `exauth.properties` ファイルの `auth.ldap.< auth.server.name` に指定した値 `>.basedn` で指定した DN 下にある認可グループを参照できること（外部認可サーバとも連携するとき）
- `exauth.properties` ファイルの `auth.ldap.< auth.server.name` に指定した値 `>.basedn` で指定した DN 下にある認可グループの属性と、認可グループのネストグループの属性を検索できること（外部認可サーバとも連携するとき）

`hcmdsldapuser` コマンドの書式は次のとおりです。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > \bin
\hcmdslapuser /set /dn < 情報検索用ユーザーの DN > [/pass < 情報検索用ユーザーの
パスワード >] /name < サーバ識別名 >
```

- < 情報検索用ユーザーの DN >
DN は RFC4514 の規約に従って指定してください。例えば、次の文字が含まれる場合は、1 文字ごとに円記号 (¥) でエスケープする必要があります。
空白文字 # + , ; < = > ¥
- < 情報検索用ユーザーのパスワード >
大文字と小文字の違いも含めて、LDAP サーバに登録しているパスワードと完全に一致している必要があります。`pass` オプションを省略してコマンドを実行すると、対話形式でパスワードを入力できます（対話形式では入力した文字列が伏せ字で表示されます）。
- < サーバ識別名 >
`exauth.properties` ファイルの `auth.server.name` プロパティに指定したサーバ識別名を指定します。

注意：

LDAP サーバでは DN やパスワードに引用符 (") を使用できますが、管理サーバには DN およびパスワードに引用符 (") が含まれていないユーザーアカウントを登録してください。

「[図 7-9 階層構造モデルの例](#)」のようなデータ構造の場合の実行例を説明します。「[図 7-9 階層構造モデルの例](#)」では、検索の起点となるエントリーの DN は「`cn=group,dc=example,dc=com`」となります。この DN 以下のすべてのユーザー「Babs」「Tim」「John」に対し、属性を検索する権限を持つユーザーが「`administrator`」である場合、`dn` オプションには「`administrator`」の DN「`cn=administrator,cn=admin,dc=example,dc=com`」を指定します。コマンドの実行例を次に示します。「`administrator`」のパスワードは「`administrator_pass`」とします。

```
hcmdsldapuser /set /dn "cn=administrator,cn=admin,dc=example,dc=com" /
pass administrator_pass /name ServerName
```

重要：

- Active Directory を使用している場合は、Active Directory が提供する `dsquery` コマンドでユーザーの DN を確認できます。`dsquery` コマンドを使用して、ユーザー「`administrator`」の DN を確認する場合の実行例と実行結果を次に示します。
`dsquery user -name administrator`
`"CN=administrator,CN=admin,DC=example,DC=com"`
- DN が「`cn=administrator,cn=admin,dc=example,com`」の場合など、DN にコンマ (,) が含まれる場合は次のように指定します。

```
hcmdsldapuser /set /dn "cn=administrator,cn=admin,dc=example
¥,com" /pass administrator_pass /name ServerName
```

情報検索用のユーザーアカウントを削除する

情報検索用のユーザーアカウントを削除するには、次のコマンドを実行してください。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > ¥bin
¥hcmdsldapuser /delete /name <サーバ識別名 >
```

情報検索用ユーザーアカウントを登録済みの LDAP サーバを確認する

どの LDAP サーバの情報検索用ユーザーアカウントが管理サーバに登録されているかを確認する場合は、次のコマンドを実行してください。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > ¥bin
¥hcmdsldapuser /list
```

(4) 外部認証サーバおよび外部認可サーバとの接続確認（認証方式が LDAP の場合）

hcmdscheckauth コマンドを使用して、外部認証サーバおよび外部認可サーバに正しく接続できるか確認します。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > ¥bin
¥hcmdscheckauth [/user <ユーザー ID > /pass <パスワード >] [/summary]
```

- <ユーザー ID >、<パスワード >には、LDAP サーバに登録されているユーザーアカウントのものを指定してください。<ユーザー ID >には、exauth.properties ファイルの auth.ldap.<auth.server.name に指定した値>.attr で指定した属性に格納されている値を指定してください。ただし、<ユーザー ID >、<パスワード >の先頭にスラッシュ (/) が含まれるユーザーアカウントは指定できません。

user オプションおよび pass オプションを省略してコマンドを実行すると、対話形式でユーザー ID およびパスワードを入力できます（対話形式では入力した文字列が伏せ字で表示されます）。

- summary オプションを指定すると、コマンド実行時に表示される確認メッセージが簡略化されます。

hcmdscheckauth コマンドを実行すると、次の 4 フェーズに分けて、exauth.properties ファイルの設定や、外部認証サーバおよび外部認可サーバとの接続状況がチェックされます。フェーズごとにチェック結果が表示されます。

フェーズ 1

exauth.properties ファイルの共通のプロパティ（表 7-9 LDAP サーバで認証する場合の exauth.properties ファイルの設定項目（共通項目））が正しく設定されているかチェックします。

フェーズ 2

exauth.properties ファイルの外部認証サーバと外部認可サーバのプロパティ（「表 7-10 LDAP サーバで認証する場合の exauth.properties ファイルの設定項目（外部認証サーバの情報を直接指定するとき）」～「表 7-12 LDAP サーバで認証する場合の exauth.properties ファイルの設定項目（外部認証サーバの情報を DNS サーバに照会するとき）」）が正しく設定されているかチェックします。

フェーズ 3

外部認証サーバに接続できるかチェックします。

フェーズ 4

外部認可サーバとも連携するよう設定されている場合に、外部認可サーバに接続できるか、および認可グループを検索できるかをチェックします。

各フェーズでの確認が正常に終了した場合、次のメッセージが表示されます。

```
KAPM15004-I The result of the configuration check of Phase <X> was normal.
```

注 <X>にはフェーズ番号が入ります。

- 階層構造モデルの場合の実行例

「[図 7-9 階層構造モデルの例](#)」のユーザー「John」のアカウントを使用して、`hcmdscheckauth` コマンドを実行する例を次に示します。

この例では、`exauth.properties` ファイルの `auth.ldap.<auth.server.name>` に指定した値 `>.attr` に「`sAMAccountName`」が指定されていることとします。LDAP サーバで設定された「John」の `sAMAccountName` 属性の値が「`John_Smith`」であるとき、<ユーザー ID>には「`John_Smith`」を指定します。「John」の、LDAP サーバ上のパスワードが「`John_pass`」であるとき、<パスワード>には「`John_pass`」を指定します。

```
hcmdscheckauth /user John_Smith /pass John_pass
```

- フラットモデルの場合の実行例

「[図 7-10 フラットモデルの例](#)」のユーザー「John」のアカウントを使用して、`hcmdscheckauth` コマンドを実行する例を次に示します。

この例では、`exauth.properties` ファイルの `auth.ldap.<auth.server.name>` に指定した値 `>.attr` に「`uid`」が指定されていることとします。「John」の RDN は「`uid=John`」であるため、<ユーザー ID>には RDN の属性値「`John`」を指定します。「John」の、LDAP サーバ上のパスワードが「`John_pass`」であるとき、<パスワード>には「`John_pass`」を指定します。

```
hcmdscheckauth /user John /pass John_pass
```

7.4.5 RADIUS サーバで外部認証する

RADIUS サーバでシステム管理者のアカウントを認証するために、Hitachi File Services Manager では次の設定が必要です。

1. 管理サーバの `exauth.properties` ファイルに必要な情報を設定します。

外部認証サーバとだけ連携する場合と、外部認可サーバとも連携する場合で設定が異なります。また、外部認可サーバとして使用する LDAP サーバは、次のどちらかの方法で定義できます。

- `exauth.properties` ファイルに接続先の LDAP サーバの情報を直接指定する
IP アドレスやポート番号などの情報を LDAP サーバごとに `exauth.properties` ファイルに指定します。
- DNS サーバに接続先の LDAP サーバを照会する
LDAP サーバの OS で DNS サーバの環境設定が完了している必要があります。また、DNS サーバの SRV レコードに、LDAP サーバのホスト名やポート番号、ドメイン名などを登録しておく必要があります。

重要：

- 管理サーバと LDAP サーバとの間の通信に StartTLS を使用する場合は、`exauth.properties` ファイルに接続先の LDAP サーバの情報を直接指定する必要があります。
- DNS サーバに接続先の LDAP サーバを照会する場合は、ユーザーがログインする際に処理に時間が掛かることがあります。

2. 外部認可サーバとも連携する場合は、LDAP サーバ内のユーザー情報を検索するためのユーザーアカウント（情報検索用のユーザーアカウント）を管理サーバに登録します。
3. RADIUS サーバに、Hitachi File Services Manager を使用するユーザーのアカウントに登録します。

ユーザー ID およびパスワードは、Hitachi File Services Manager で使用できる文字で構成されている必要があります。1 バイト以上 256 バイト以内で次の文字を使用できます。

A~Z a~z 0~9 ! # \$ % & ' () * + - . = @ ¥ ^ _ |

Hitachi File Services Manager では、ユーザー ID の大文字と小文字の違いは区別されません。また、パスワードの文字種の組み合わせは、外部認証サーバでの設定に従ってください。

4. 管理サーバに、RADIUS サーバとの通信用に共有秘密鍵（Shared secret）を設定します。
5. GUI で、アカウントの登録や権限の設定などを実施します。

外部認証サーバとだけ連携する場合

- ユーザーの登録
- ユーザーの認証方式の変更
既存のユーザーの認証方式を変更する場合に必要な設定です。
- ユーザーグループへのユーザーの登録
- ユーザー管理と Hitachi File Services Manager の操作権限の設定

外部認可サーバとも連携する場合

- 認可グループの登録
- ユーザー管理と Hitachi File Services Manager の操作権限の設定

参考：

登録した認可グループのネストグループに属するユーザーも、認可グループに設定されたロール（権限）で Hitachi File Services Manager を操作できるようになります。

6. hcmdscheckauth コマンドを使用して、外部認証サーバおよび外部認可サーバに正しく接続できるか確認します。

ここでは、管理サーバで必要な作業について説明します。

(1) exauth.properties ファイルの設定（認証方式が RADIUS の場合）

ここでは、RADIUS サーバでユーザー認証する場合に exauth.properties ファイルで必要な設定について説明します。

1. exauth.properties ファイルで、次のプロパティに値を設定します。
 - 共通のプロパティ（表 7-13 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目（共通項目））
 - 外部認証サーバのプロパティ（表 7-14 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目（外部認証サーバの設定））
RADIUS サーバごとに設定します。
 - 外部認可サーバのプロパティ
外部認可サーバとも連携する場合に必要な設定です。LDAP サーバの情報をドメインごとに設定します。
LDAP サーバの情報を直接指定する場合（「表 7-15 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目（外部認可サーバの共通設定）」～「表 7-17 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目（外部認可サーバと StartTLS で通信するとき）」）と、DNS サーバに照会する場合（「表 7-15 RADIUS サーバ

で認証する場合の `exauth.properties` ファイルの設定項目（外部認可サーバの共通設定）」および「表 7-18 RADIUS サーバで認証する場合の `exauth.properties` ファイルの設定項目（外部認可サーバの情報を DNS サーバに照会するとき）」とで設定する項目が異なります。

`exauth.properties` ファイルのひな形は次の場所に格納されています。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %sample%conf
%exauth.properties
```

注意：

設定値の先頭および末尾には空白文字を指定しないでください。また、設定値は引用符（"）で囲まないでください。指定した場合、値は無視され、デフォルト値が採用されます。

2. `exauth.properties` ファイルを次の場所に格納します。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %conf
%exauth.properties
```

`auth.ocsp.enable` プロパティと `auth.ocsp.responderURL` プロパティの設定値を変更した場合には、Hitachi File Services Manager の再起動が必要です。それ以外のプロパティまたは属性の設定値を変更した場合は、直ちに変更後の値が有効になります。

`exauth.properties` ファイルの設定項目を「表 7-13 RADIUS サーバで認証する場合の `exauth.properties` ファイルの設定項目（共通項目）」～「表 7-18 RADIUS サーバで認証する場合の `exauth.properties` ファイルの設定項目（外部認可サーバの情報を DNS サーバに照会するとき）」に示します。

表 7-13 RADIUS サーバで認証する場合の `exauth.properties` ファイルの設定項目（共通項目）

プロパティ名	説明
<code>auth.server.type</code>	外部認証サーバの種類です。 <code>radius</code> を指定します。 デフォルト値： <code>internal</code> （外部認証サーバと連携しない場合）
<code>auth.server.name</code>	RADIUS サーバのサーバ識別名を指定します。接続プロトコルやポート番号などの設定（表 7-14）を RADIUS サーバごとに区別するために付ける任意の名称です。初期値として「 <code>ServerName</code> 」が設定されています。必ず 1 つ以上のサーバ識別名を指定してください。RADIUS サーバを複数指定する場合は、サーバ識別名をコンマ（,）で区切ります。サーバ識別名は重複して登録しないでください。 指定できる値：64 バイト以内の次の文字列 0~9 A~Z a~z ! # () + - . = @ [] ^ _ { } ~ デフォルト値：なし
<code>auth.group.mapping</code>	外部認可サーバとも連携するかどうかを指定します。 連携する場合は <code>true</code> を指定します。 連携しない場合は <code>false</code> を指定します。 デフォルト値： <code>false</code>

表 7-14 RADIUS サーバで認証する場合の `exauth.properties` ファイルの設定項目（外部認証サーバの設定）

属性	説明
<code>protocol</code>	RADIUS サーバ認証に使用する認証プロトコルです。この項目は必須です。 指定できる値： <code>PAP</code> または <code>CHAP</code> デフォルト値：なし
<code>host</code> ※1	RADIUS サーバのホスト名または IP アドレスを指定します。ホスト名を指定する場合、IP アドレスへの名前解決ができることを事前に確認してください。IP アドレスには、IPv4 アドレスと IPv6 アドレスの両方を使用できます。IPv6 アドレスは必ず角括弧（[]）で囲んでください。この項目は必須です。 デフォルト値：なし

属性	説明
port	RADIUS サーバの認証用ポート番号です。指定するポートが RADIUS サーバで待ち受けポート番号として設定されていることを事前に確認してください。 指定できる値：1～65535 デフォルト値：1812
timeout	RADIUS サーバと接続するときの接続待ち時間です。 指定できる値：1～65535（秒） デフォルト値：1
retry.times	RADIUS サーバとの通信に失敗した場合のリトライ回数です。この値を 0 にした場合、リトライされません。 指定できる値：0～50 デフォルト値：3
attr.NAS-Identifier ^{※2}	HVFP/HDI の管理サーバのホスト名です。RADIUS サーバが管理サーバを識別するために使用します。初期値として、管理サーバのホスト名が設定されています。 指定できる値：253 バイト以内の次の文字列 0～9 A～Z a～z ! " # \$ % & ' () * + , - . / : ; < = > ? @ [¥] ^ _ ` { } ~ デフォルト値：なし
attr.NAS-IP-Address ^{※2}	HVFP/HDI の管理サーバの IPv4 アドレスです。RADIUS サーバが管理サーバを識別するために使用します。 IPv4 アドレスの形式が不正な場合、この属性は無効です。 デフォルト値：なし
attr.NAS-IPv6-Address ^{※2}	HVFP/HDI の管理サーバの IPv6 アドレスです。RADIUS サーバが管理サーバを識別するために使用します。IPv6 アドレスは必ず角括弧 ([]) で囲んでください。 IPv6 アドレスの形式が不正な場合、この属性は無効です。 デフォルト値：なし

注

各属性は、次のように指定します。

auth.radius.< auth.server.name に指定した値 >.<属性>=<値>

注※1

同一マシンで稼働する外部認可サーバとも連携し、かつ LDAP サーバの接続プロトコルに StartTLS を使用する場合は、host 属性には LDAP サーバの証明書の CN と同じホスト名を設定してください。IP アドレスは使用できません。

注※2

attr.NAS-Identifier, attr.NAS-IP-Address, attr.NAS-IPv6-Address はどれか 1 つを必ず指定してください。

表 7-15 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目（外部認可サーバの共通設定）

属性	説明
domain.name	LDAP サーバが管理するドメインの名称です。外部認可サーバとも連携する場合、この項目は必須です。 デフォルト値：なし
dns_lookup	LDAP サーバの情報を DNS サーバに照会するかどうかです。 exauth.properties ファイルに LDAP サーバの情報を直接指定する場合は false を指定します。 DNS サーバに照会する場合は、true を指定します。

属性	説明
	<p>ただし、次の属性に値が設定されている場合は、DNS サーバには照会されず、ユーザーが指定した値を使用して LDAP サーバに接続されます。</p> <ul style="list-style-type: none"> auth.group.<ドメイン名>.host auth.group.<ドメイン名>.port <p>デフォルト値：false</p>

注

各属性は、次のように指定します。

auth.radius.< auth.server.name に指定した値 > .<属性>=<値 >

表 7-16 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目 (外部認可サーバの情報を直接指定するとき)

属性	説明
protocol ^{※1}	<p>LDAP サーバ接続のプロトコルです。</p> <p>平文による通信の場合は ldap, StartTLS による通信の場合は tls を指定します。</p> <p>tls を指定する場合には、LDAP サーバで次のどれかの暗号方式を使用できることを事前に確認してください。</p> <ul style="list-style-type: none"> TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA SSL_RSA_WITH_3DES_EDE_CBC_SHA <p>指定できる値：ldap または tls デフォルト値：ldap</p>
host ^{※2}	<p>外部認証サーバと外部認可サーバが異なるマシンで稼働している場合に、LDAP サーバのホスト名または IP アドレスを指定します。ホスト名を指定する場合、IP アドレスへの名前解決ができることを事前に確認してください。IP アドレスには、IPv4 アドレスと IPv6 アドレスの両方を使用できます。IPv6 アドレスは必ず角括弧 ([]) で囲んでください。</p> <p>省略した場合は、外部認証サーバと外部認可サーバが同一マシンで稼働しているものと見なされます。</p> <p>デフォルト値：なし</p>
port	<p>LDAP サーバのポート番号です。指定するポートが、LDAP サーバで待ち受けポート番号として設定されていることを事前に確認してください。</p> <p>指定できる値：1～65535 デフォルト値：389</p>
basedn	<p>LDAP サーバの情報を検索する際に、起点となるエントリーの DN (BaseDN) です。この DN より下の階層のユーザーエントリーが認可の対象となります。検索対象のユーザーエントリーをすべて含む階層の DN を指定してください。</p> <p>DN は RFC4514 の規約に従って指定してください。例えば、次の文字が DN に含まれる場合は、1 文字ごとに円記号 (¥) でエスケープする必要があります。</p> <p>空白文字 # + ; , < = > ¥</p> <p>指定した値は LDAP サーバにそのまま渡されるため、BaseDN にエスケープが必要な文字が含まれる場合は、正しくエスケープしてください。</p> <p>省略した場合は、Active Directory の defaultNamingContext 属性に指定されている値が BaseDN と見なされます。</p> <p>デフォルト値：なし</p>
timeout	<p>LDAP サーバと接続するときの接続待ち時間です。この値を 0 にした場合、タイムアウトしないで、通信エラーが発生するまで待ち続けます。</p> <p>指定できる値：0～120 (秒) デフォルト値：15</p>
retry.interval	<p>LDAP サーバとの通信に失敗した場合のリトライ間隔となる秒数です。</p> <p>指定できる値：1～60 (秒)</p>

属性	説明
	デフォルト値: 1
retry.times	LDAP サーバとの通信に失敗した場合のリトライ回数です。この値を 0 にした場合、リトライされません。 指定できる値: 0~50 デフォルト値: 20

注

各属性は、次のように指定します。

auth.group.<ドメイン名>.<属性>=<値>

<ドメイン名>には、auth.radius.<auth.server.name に指定した値>.domain.name の値を指定します。

注※1

LDAP サーバの接続プロトコルに StartTLS を使用する場合には、Hitachi Command Suite 共通コンポーネントのセキュリティ設定が必要です。StartTLS を使用する場合は設定については、「7.4.8 Hitachi Command Suite 共通コンポーネントのセキュリティを設定する (LDAP サーバとの通信)」を参照してください。

注※2

外部認証サーバと外部認可サーバが別のマシンで稼働していて、かつ LDAP サーバの接続プロトコルに StartTLS を使用する場合は、host 属性には LDAP サーバの証明書の CN と同じホスト名を設定してください。IP アドレスは使用できません。

表 7-17 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目 (外部認可サーバと StartTLS で通信するとき)

プロパティ名	説明
auth.ocsp.enable	LDAP サーバと StartTLS で通信する場合に、OCSP レスポンダーまたは CRL を使用して LDAP サーバの電子署名証明書の有効性を検証するかどうかを指定します。 検証する場合は true を、検証しない場合は false を指定します。 デフォルト値: false
auth.ocsp.responderURL	電子署名証明書の AIA フィールドに記載された OCSP レスポンダー以外の OCSP レスポンダーで電子署名証明書の有効性を検証する場合に、OCSP レスポンダーの URL を指定します。省略した場合は、AIA フィールドに記載された OCSP レスポンダーに問い合わせます。 デフォルト値: なし

表 7-18 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目 (外部認可サーバの情報を DNS サーバに照会するとき)

属性	説明
protocol	LDAP サーバ接続のプロトコルです。 指定できる値: ldap デフォルト値: ldap
port	LDAP サーバのポート番号です。指定するポートが、LDAP サーバで待ち受けポート番号として設定されていることを事前に確認してください。 指定できる値: 1~65535 デフォルト値: 389
basedn	LDAP サーバの情報を検索する際に、起点となるエントリーの DN (BaseDN) です。この DN より下の階層のユーザーエントリーが認可の対象となります。検索対象のユーザーエントリーをすべて含む階層の DN を指定してください。

属性	説明
	<p>DN は RFC4514 の規約に従って指定してください。例えば、次の文字が DN に含まれる場合は、1 文字ごとに円記号 (¥) でエスケープする必要があります。</p> <p>空白文字 # + ; , < = > ¥</p> <p>指定した値は LDAP サーバにそのまま渡されるため、BaseDN にエスケープが必要な文字が含まれる場合は、正しくエスケープしてください。</p> <p>省略した場合は、Active Directory の defaultNamingContext 属性に指定されている値が BaseDN と見なされます。</p> <p>デフォルト値：なし</p>
timeout	<p>LDAP サーバと接続するときの接続待ち時間です。この値を 0 にした場合、タイムアウトしないで、通信エラーが発生するまで待ち続けます。</p> <p>指定できる値：0~120 (秒)</p> <p>デフォルト値：15</p>
retry.interval	<p>LDAP サーバとの通信に失敗した場合のリトライ間隔となる秒数です。</p> <p>指定できる値：1~60 (秒)</p> <p>デフォルト値：1</p>
retry.times	<p>LDAP サーバとの通信に失敗した場合のリトライ回数です。この値を 0 にした場合、リトライされません。</p> <p>指定できる値：0~50</p> <p>デフォルト値：20</p>

注

各属性は、次のように指定します。

auth.group.<ドメイン名>.<属性>=<値>

<ドメイン名>には、auth.radius.<auth.server.name に指定した値>.domain.name の値を指定します。

設定例を次に示します。

- 外部認証サーバとだけ連携するとき

```
auth.server.type=radius
auth.server.name=ServerName
auth.group.mapping=false
auth.radius.ServerName.protocol=PAP
auth.radius.ServerName.host=radius.example.com
auth.radius.ServerName.port=1812
auth.radius.ServerName.timeout=1
auth.radius.ServerName.retry.times=3
auth.radius.ServerName.attr.NAS-Identifier=host_A
```

- 外部認可サーバの情報を直接設定するとき

```
auth.server.type=radius
auth.server.name=ServerName
auth.group.mapping=true
auth.ocsp.enable=false
auth.ocsp.responderURL=
auth.radius.ServerName.protocol=PAP
auth.radius.ServerName.host=radius.example.com
auth.radius.ServerName.port=1812
auth.radius.ServerName.timeout=1
auth.radius.ServerName.retry.times=3
auth.radius.ServerName.attr.NAS-Identifier=host_A
auth.radius.ServerName.domain.name=EXAMPLE.COM
auth.radius.ServerName.dns_lookup=false
auth.group.EXAMPLE.COM.protocol=ldap
auth.group.EXAMPLE.COM.host=ldap.example.com
auth.group.EXAMPLE.COM.port=389
auth.group.EXAMPLE.COM.baseDN=dc=Example,dc=com
auth.group.EXAMPLE.COM.timeout=15
auth.group.EXAMPLE.COM.retry.interval=1
auth.group.EXAMPLE.COM.retry.times=20
```

- 外部認可サーバを DNS サーバに照会するとき

```
auth.server.type=radius
auth.server.name=ServerName
auth.group.mapping=true
auth.radius.ServerName.protocol=PAP
auth.radius.ServerName.host=radius.example.com
auth.radius.ServerName.port=1812
auth.radius.ServerName.timeout=1
auth.radius.ServerName.retry.times=3
auth.radius.ServerName.attr.NAS-Identifier=host_A
auth.radius.ServerName.domain.name=EXAMPLE.COM
auth.radius.ServerName.dns_lookup=true
auth.group.EXAMPLE.COM.protocol=ldap
auth.group.EXAMPLE.COM.basedn=dc=Example,dc=com
auth.group.EXAMPLE.COM.timeout=15
auth.group.EXAMPLE.COM.retry.interval=1
auth.group.EXAMPLE.COM.retry.times=20
```

(2) 情報検索用のユーザーアカウントの登録（認証方式が RADIUS の場合）

LDAP サーバを外部認可サーバとして利用する場合に、`hcmsldapuser` コマンドを使用して、情報検索用のユーザーアカウントを管理サーバに登録します。登録後は、`hcmsldapuser` コマンドで、情報検索用のユーザーアカウントを削除したり、管理サーバに情報検索用のユーザーアカウントを登録済みの LDAP サーバを確認したりできます。

情報検索用のユーザーアカウントを登録する

`hcmsldapuser` コマンドで情報検索用のユーザーアカウントを登録します。

情報検索用のユーザーアカウントには、次の条件を満たすユーザーアカウントを登録してください。

- LDAP サーバに登録されていること
- `exauth.properties` ファイルの `auth.group.<ドメイン名>.basedn` で指定した DN にバインドできること
- `exauth.properties` ファイルの `auth.group.<ドメイン名>.basedn` で指定した DN 以下のすべてのエントリーに対して属性を検索できること
- `exauth.properties` ファイルの `auth.group.<ドメイン名>.basedn` で指定した DN を参照できること
- `exauth.properties` ファイルの `auth.group.<ドメイン名>.basedn` で指定した DN 下にある認可グループを参照できること
- `exauth.properties` ファイルの `auth.group.<ドメイン名>.basedn` で指定した DN 下にある認可グループの属性と、認可グループのネストグループの属性を検索できること

`hcmsldapuser` コマンドの書式は次のとおりです。

```
<Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%bin
%hcmsldapuser /set /dn <情報検索用ユーザーの DN> [/pass <情報検索用ユーザーのパスワード>] /name <ドメイン名>
```

- <情報検索用ユーザーの DN>
DN は RFC4514 の規約に従って指定してください。例えば、次の文字が含まれる場合は、1 文字ごとに円記号 (¥) でエスケープする必要があります。
空白文字 # + , ; < = > ¥
- <情報検索用ユーザーのパスワード>
大文字と小文字の違いも含めて、LDAP サーバに登録しているパスワードと完全に一致している必要があります。pass オプションを省略してコマンドを実行すると、対話形式でパスワードを入力できます（対話形式では入力した文字列が伏せ字で表示されます）。
- <ドメイン名>

exauth.properties ファイルの auth.radius.< auth.server.name に指定した値
>.domain.name に指定したドメイン名を指定します。

注意：

LDAP サーバでは DN やパスワードに引用符 (") を使用できますが、管理サーバには DN およびパスワードに引用符 (") が含まれていないユーザーアカウントを登録してください。

重要：

- Active Directory が提供する dsquery コマンドでユーザーの DN を確認できます。dsquery コマンドを使用して、ユーザー「administrator」の DN を確認する場合の実行例と実行結果を次に示します。

```
dsquery user -name administrator
"CN=administrator,CN=admin,DC=example,DC=com"
```

- DN が「cn=administrator,cn=admin,dc=example,com」の場合など、DN にコンマ (,) が含まれる場合は次のように指定します。

```
hcmsldapuser /set /dn "cn=administrator,cn=admin,dc=example
¥,com" /pass administrator_pass /name ServerName
```

情報検索用のユーザーアカウントを削除する

情報検索用のユーザーアカウントを削除するには、次のコマンドを実行してください。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > ¥bin
¥hcmsldapuser /delete /name <ドメイン名>
```

情報検索用ユーザーアカウントを登録済みの LDAP サーバを確認する

どの LDAP サーバの情報検索用ユーザーアカウントが管理サーバに登録されているかを確認する場合は、次のコマンドを実行してください。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > ¥bin
¥hcmsldapuser /list
```

(3) 共有秘密鍵の設定

RADIUS サーバと通信するための共有秘密鍵を、hcmsradiussecret コマンドを使用して管理サーバに設定します。設定後は、hcmsradiussecret コマンドで、共有秘密鍵を削除したり、共有秘密鍵が設定されている外部認証サーバのサーバ識別名を一覧表示したりできます。

共有秘密鍵を設定する

hcmsradiussecret コマンドで共有秘密鍵を設定するには、次のコマンドを実行してください。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > ¥bin
¥hcmsradiussecret [/set <共有秘密鍵>] /name < RADIUS サーバのサーバ識別名 >
```

- set オプションを省略してコマンドを実行すると、対話形式で共有秘密鍵を入力できます（対話形式では入力した文字列が伏せ字で表示されます）。
- < RADIUS サーバのサーバ識別名 > は、exauth.properties ファイルの auth.server.name プロパティに指定するサーバ識別名と一致する必要があります。

共有秘密鍵が「secret01」で、RADIUS サーバのサーバ識別名が「ServerName」の場合の hcmsradiussecret コマンドの実行例を次に示します。

```
hcmsradiussecret /set secret01 /name ServerName
```

共有秘密鍵を削除する

共有秘密鍵を削除するには、次のコマンドを実行してください。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%bin
%hcmdsradiussecret /delete /name < RADIUS サーバのサーバ識別名 >
```

共有秘密鍵が設定されている RADIUS サーバのサーバ識別名を一覧表示する

共有秘密鍵が設定されている RADIUS サーバのサーバ識別名を一覧表示するには、次のコマンドを実行してください。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%bin
%hcmdsradiussecret /list
```

(4) 外部認証サーバおよび外部認可サーバとの接続確認（認証方式が RADIUS の場合）

hcmdscheckauth コマンドを使用して、外部認証サーバおよび外部認可サーバに正しく接続できるか確認します。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%bin
%hcmdscheckauth [/user <ユーザー ID> /pass <パスワード>] [/summary]
```

- ・ <ユーザー ID>、<パスワード>には、RADIUS サーバに登録されているユーザーアカウントのものを指定してください。ただし、<ユーザー ID>、<パスワード>の先頭にスラッシュ (/) が含まれるユーザーアカウントは指定できません。

user オプションおよび pass オプションを省略してコマンドを実行すると、対話形式でユーザー ID およびパスワードを入力できます（対話形式では入力した文字列が伏せ字で表示されます）。

- ・ summary オプションを指定すると、コマンド実行時に表示される確認メッセージが簡略化されます。

hcmdscheckauth コマンドを実行すると、次の 4 フェーズに分けて、exauth.properties ファイルの設定や、外部認証サーバおよび外部認可サーバとの接続状況がチェックされます。フェーズごとにチェック結果が表示されます。

フェーズ 1

exauth.properties ファイルの共通のプロパティ（表 7-13 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目（共通項目））が正しく設定されているかチェックします。

フェーズ 2

exauth.properties ファイルの外部認証サーバのプロパティ（表 7-14 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目（外部認証サーバの設定））と、外部認可サーバのプロパティ（「表 7-15 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目（外部認可サーバの共通設定）」～「表 7-18 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目（外部認可サーバの情報を DNS サーバに照会するとき）」）が正しく設定されているかチェックします。

フェーズ 3

外部認証サーバに接続できるかチェックします。

フェーズ 4

外部認可サーバとも連携するよう設定されている場合に、外部認可サーバに接続できるか、および認可グループを検索できるかをチェックします。

各フェーズでの確認が正常に終了した場合、次のメッセージが表示されます。

```
KAPM15004-I The result of the configuration check of Phase <X> was normal.
```

注 <X>にはフェーズ番号が入ります。

7.4.6 KDC サーバで外部認証する

KDC サーバでシステム管理者のアカウントを認証するために、Hitachi File Services Manager では次の設定が必要です。

1. 管理サーバの `exauth.properties` ファイルに必要な情報を設定します。
外部認証サーバとだけ連携する場合と、外部認可サーバとも連携する場合で設定が異なります。また、外部認証サーバとして使用する KDC サーバは、次のどちらかの方法で定義できます。

- `exauth.properties` ファイルに接続先の KDC サーバの情報を直接指定する
レムごとに、IP アドレスやポート番号などの KDC サーバの情報を `exauth.properties` ファイルに指定します。
- DNS サーバに接続先の KDC サーバを照会する
KDC サーバを管理する DNS サーバの情報を `exauth.properties` ファイルに指定します。また、DNS サーバの SRV レコードに、KDC サーバのホスト名やポート番号、レム名などを登録しておく必要があります。

重要：

- 管理サーバと LDAP サーバとの間の通信に StartTLS を使用する場合は、`exauth.properties` ファイルに接続先の KDC サーバの情報を直接指定する必要があります。
 - DNS サーバに接続先の KDC サーバを照会する場合は、ユーザーがログインする際に処理に時間が掛かることがあります。
2. 外部認可サーバとも連携する場合は、LDAP サーバ内のユーザー情報を検索するためのユーザーアカウント（情報検索用のユーザーアカウント）を管理サーバに登録します。
 3. KDC サーバに、Hitachi File Services Manager を使用するユーザーのアカウントを登録します。

ユーザー ID およびパスワードは、Hitachi File Services Manager で使用できる文字で構成されている必要があります。1 バイト以上 256 バイト以内で次の文字を使用できます。

A~Z a~z 0~9 ! # \$ % & ' () * + - . = @ ¥ ^ _ |

Hitachi File Services Manager では、ユーザー ID の大文字と小文字の違いは区別されません。また、パスワードの文字種の組み合わせは、外部認証サーバでの設定に従ってください。

4. GUI で、アカウントの登録や権限の設定などを実施します。

外部認証サーバとだけ連携する場合

- ユーザーの登録
- ユーザーの認証方式の変更
既存のユーザーの認証方式を変更する場合に必要な設定です。
- ユーザーグループへのユーザーの登録
- ユーザー管理と Hitachi File Services Manager の操作権限の設定

外部認可サーバとも連携する場合

- 認可グループの登録
- ユーザー管理と Hitachi File Services Manager の操作権限の設定

参考：

登録した認可グループのネストグループに属するユーザーも、認可グループに設定されたロール（権限）で Hitachi File Services Manager を操作できるようになります。

5. 管理サーバで `hcmdscheckauth` コマンドを使用して、外部認証サーバおよび外部認可サーバに正しく接続できるか確認します。

ここでは、管理サーバで必要な作業について説明します。

(1) exauth.properties ファイルの設定（認証方式が Kerberos の場合）

ここでは、KDC サーバでユーザー認証する場合に exauth.properties ファイルで必要な設定について説明します。

- exauth.properties ファイルで、必要なプロパティに値を設定します。
 - 共通のプロパティ（表 7-19 KDC サーバで認証する場合の exauth.properties ファイルの設定項目（共通項目））
 - 外部認証サーバのプロパティ
KDC サーバごとに設定します。
KDC サーバの情報を直接指定する場合（表 7-20 KDC サーバで認証する場合の exauth.properties ファイルの設定項目（外部認証サーバの情報を直接指定するとき））と、DNS サーバに照会する場合（表 7-21 KDC サーバで認証する場合の exauth.properties ファイルの設定項目（外部認証サーバの情報を DNS サーバに照会するとき））とで設定する項目が異なります。
 - 外部認可サーバのプロパティ（「表 7-22 KDC サーバで認証する場合の exauth.properties ファイルの設定項目（外部認可サーバの設定）」および「表 7-23 KDC サーバで認証する場合の exauth.properties ファイルの設定項目（外部認可サーバと StartTLS で通信するとき）」）
KDC サーバの情報を直接指定し、かつ外部認可サーバとも連携する場合にだけ必要な設定です。レルムごとに指定します。

exauth.properties ファイルのひな形は次の場所に格納されています。

```
<Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%sample%conf%exauth.properties
```

注意：

設定値の先頭および末尾には空白文字を指定しないでください。また、設定値は引用符（"）で囲まないでください。指定した場合、値は無視され、デフォルト値が採用されます。

- exauth.properties ファイルを次の場所に格納します。

```
<Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%conf%exauth.properties
```

auth.ocsp.enable プロパティと auth.ocsp.responderURL プロパティの設定値を変更した場合には、Hitachi File Services Manager の再起動が必要です。それ以外のプロパティまたは属性の設定値を変更した場合は、直ちに変更後の値が有効になります。

exauth.properties ファイルの設定項目を「表 7-19 KDC サーバで認証する場合の exauth.properties ファイルの設定項目（共通項目）」～「表 7-23 KDC サーバで認証する場合の exauth.properties ファイルの設定項目（外部認可サーバと StartTLS で通信するとき）」に示します。

表 7-19 KDC サーバで認証する場合の exauth.properties ファイルの設定項目（共通項目）

プロパティ名	説明
auth.server.type	外部認証サーバの種類です。kerberos を指定します。 デフォルト値：internal（外部認証サーバと連携しない場合）
auth.group.mapping	外部認可サーバとも連携するかどうかを指定します。 連携する場合は true を指定します。 連携しない場合は false を指定します。 デフォルト値：false

表 7-20 KDC サーバで認証する場合の exauth.properties ファイルの設定項目（外部認証サーバの情報を直接指定するとき）

属性	説明
default_realm	デフォルトのレルム名を指定します。GUI のログイン画面でレルム名を省略してユーザー ID を入力した場合に、この項目で指定したレルムに所属するユーザーとして認証されます。この項目は必須です。 デフォルト値：なし
dns_lookup_kdc	false を指定します。 デフォルト値：false
default_tkt_enctypes	Kerberos 認証に使用する暗号タイプを指定します。このプロパティは、管理サーバの OS が Windows の場合にだけ有効です。 次の暗号タイプを使用できます。 <ul style="list-style-type: none"> • aes128-cts • rc4-hmac • des3-cbc-sha1 • des-cbc-md5 • des-cbc-crc 複数指定する場合は、コンマ (,) で区切ってください。 指定した暗号タイプのうち、管理サーバの OS と KDC サーバの両方でサポートされているものが使用されます。 デフォルト：なし (DES-CBC-MD5 での認証)
clockskew	管理サーバと KDC サーバ間の時刻の差の許容範囲を指定します。この値よりも時刻に差がある場合、認証エラーになります。 指定できる値：0~300 (秒) デフォルト値：300
timeout	KDC サーバと接続するときの接続待ち時間です。この値を 0 にした場合、タイムアウトしないで、通信エラーが発生するまで待ち続けます。 指定できる値：0~120 (秒) デフォルト値：3
realm_name	レルム識別名を指定します。レルムごとに KDC サーバの情報を区別するために付ける任意の名称です。必ず 1 つ以上のレルム識別名を指定してください。レルム識別名を複数指定する場合は、レルム識別名をコンマ (,) で区切ります。同じレルム識別名は重複して登録しないでください。 デフォルト値：なし
< realm_name に指定した値 >.realm	KDC サーバに設定してあるレルム名を指定します。この項目は必須です。 デフォルト値：なし
< realm_name に指定した値 >.kdc	KDC サーバの情報を次の形式で指定します。 <ホスト名または IP アドレス>[:<ポート番号>] この項目は必須です。 <ホスト名または IP アドレス> ホスト名を指定する場合、IP アドレスへの名前解決ができることを事前に確認してください。 IP アドレスは、IPv4 アドレスで指定してください。IPv6 環境では、ホスト名で指定してください。 ただし、ループバックアドレス (localhost または 127.0.0.1) を指定しないでください。 <ポート番号> 指定するポートが KDC サーバで待ち受けポート番号として設定されていることを事前に確認してください。ポート番号を省略した場合、または指定したポート番号が KDC サーバで使用できないポート番号である場合は、「88」を指定したと見なされます。 KDC サーバを複数指定する場合は、次のようにコンマ (,) で区切ります。 <ホスト名または IP アドレス>[:<ポート番号>], <ホスト名または IP アドレス>[:<ポート番号>], ...

注

各属性は、次のように指定します。

auth.kerberos.<属性>=<値>

表 7-21 KDC サーバで認証する場合の exauth.properties ファイルの設定項目（外部認証サーバの情報を DNS サーバに照会するとき）

属性	説明
default_realm	デフォルトのレルム名を指定します。GUI のログイン画面でレルム名を省略してユーザー ID を入力した場合に、この項目で指定したレルムに所属するユーザーとして認証されます。この項目は必須です。 デフォルト値：なし
dns_lookup_kdc	true を指定します。この項目は必須です。 ただし、次のすべての属性に値を設定していると、KDC サーバは DNS サーバに照会されません。 <ul style="list-style-type: none">• realm_name• < realm_name に指定した値 > .realm• < realm_name に指定した値 > .kdc
default_tkt_etypes	Kerberos 認証に使用する暗号タイプを指定します。このプロパティは、管理サーバの OS が Windows の場合にだけ有効です。 次の暗号タイプを使用できます。 <ul style="list-style-type: none">• aes128-cts• rc4-hmac• des3-cbc-sha1• des-cbc-md5• des-cbc-crc 複数指定する場合は、コンマ (,) で区切ってください。 指定した暗号タイプのうち、管理サーバの OS と KDC サーバの両方でサポートされているものが使用されます。 デフォルト：なし (DES-CBC-MD5 での認証)
clockskew	管理サーバと KDC サーバ間の時刻の差の許容範囲を指定します。この値よりも時刻に差がある場合、認証エラーになります。 指定できる値：0~300 (秒) デフォルト値：300
timeout	KDC サーバと接続するときの接続待ち時間です。この値を 0 にした場合、タイムアウトしないで、通信エラーが発生するまで待ち続けます。 指定できる値：0~120 (秒) デフォルト値：3

注

各属性は、次のように指定します。

auth.kerberos.<属性>=<値>

表 7-22 KDC サーバで認証する場合の exauth.properties ファイルの設定項目（外部認可サーバの設定）

属性	説明
protocol*	LDAP サーバ接続のプロトコルです。 平文による通信の場合は ldap, StartTLS による通信の場合は tls を指定します。KDC サーバの情報を直接指定する場合にだけ、StartTLS で通信できます。 tls を指定する場合には、LDAP サーバで次のどれかの暗号方式を使用できることを事前に確認してください。 <ul style="list-style-type: none">• TLS_RSA_WITH_AES_256_CBC_SHA• TLS_RSA_WITH_AES_128_CBC_SHA• SSL_RSA_WITH_3DES_EDE_CBC_SHA

属性	説明
	指定できる値：ldap または tls デフォルト値：ldap
port	LDAP サーバのポート番号です。指定するポートが、LDAP サーバで待ち受けポート番号として設定されていることを事前に確認してください。 指定できる値：1～65535 デフォルト値：389
basedn	LDAP サーバの情報を検索する際に、起点となるエントリーの DN (BaseDN) です。この DN より下の階層のユーザーエントリーが認可の対象となります。検索対象のユーザーエントリーをすべて含む階層の DN を指定してください。 DN は RFC4514 の規約に従って指定してください。例えば、次の文字が DN に含まれる場合は、1 文字ごとに円記号 (¥) でエスケープする必要があります。 空白文字 # + ; , < = > ¥ 指定した値は LDAP サーバにそのまま渡されるため、BaseDN にエスケープが必要な文字が含まれる場合は、正しくエスケープしてください。 省略した場合は、Active Directory の defaultNamingContext 属性に指定されている値が BaseDN と見なされます。 デフォルト値：なし
timeout	LDAP サーバと接続するときの接続待ち時間です。この値を 0 にした場合、タイムアウトしないで、通信エラーが発生するまで待ち続けます。 指定できる値：0～120 (秒) デフォルト値：15
retry.interval	LDAP サーバとの通信に失敗した場合のリトライ間隔となる秒数です。 指定できる値：1～60 (秒) デフォルト値：1
retry.times	LDAP サーバとの通信に失敗した場合のリトライ回数です。この値を 0 にした場合、リトライされません。 指定できる値：0～50 デフォルト値：20

注

各属性は、次のように指定します。

auth.group.<レルム名>.<属性>=<値>

<レルム名>には auth.kerberos.<realm_name に指定した値>.realm の値を指定します。

注※

LDAP サーバの接続プロトコルに StartTLS を使用する場合には、Hitachi Command Suite 共通コンポーネントのセキュリティ設定が必要です。StartTLS を使用する場合の設定については、「7.4.8 Hitachi Command Suite 共通コンポーネントのセキュリティを設定する (LDAP サーバとの通信)」を参照してください。

表 7-23 KDC サーバで認証する場合の exauth.properties ファイルの設定項目 (外部認可サーバと StartTLS で通信するとき)

プロパティ名	説明
auth.ocsp.enable	LDAP サーバと StartTLS で通信する場合に、OCSP レスポンダーまたは CRL を使用して LDAP サーバの電子署名証明書の有効性を検証するかどうかを指定します。 検証する場合は true を、検証しない場合は false を指定します。 デフォルト値：false

プロパティ名	説明
auth.ocsp.responderURL	電子署名証明書の AIA フィールドに記載された OCSP レスポンダー以外の OCSP レスポンダーで電子署名証明書の有効性を検証する場合に、OCSP レスポンダーの URL を指定します。省略した場合は、AIA フィールドに記載された OCSP レスポンダーに問い合わせます。 デフォルト値：なし

設定例を次に示します。

- KDC サーバの情報を直接指定する場合（外部認可サーバと連携しないとき）

```
auth.server.type=kerberos
auth.group.mapping=false
auth.kerberos.default_realm=EXAMPLE.COM
auth.kerberos.dns_lookup_kdc=false
auth.kerberos.clockskew=300
auth.kerberos.timeout=3
auth.kerberos.realm_name=RealmName
auth.kerberos.RealmName.realm=EXAMPLE.COM
auth.kerberos.RealmName.kdc=kerberos.example.com:88
```

- KDC サーバを DNS サーバに照会する場合（外部認可サーバと連携しないとき）

```
auth.server.type=kerberos
auth.group.mapping=false
auth.kerberos.default_realm=EXAMPLE.COM
auth.kerberos.dns_lookup_kdc=true
auth.kerberos.clockskew=300
auth.kerberos.timeout=3
```

- KDC サーバの情報を直接指定する場合（外部認可サーバとも連携するとき）

```
auth.server.type=kerberos
auth.group.mapping=true
auth.ocsp.enable=false
auth.ocsp.responderURL=
auth.kerberos.default_realm=EXAMPLE.COM
auth.kerberos.dns_lookup_kdc=false
auth.kerberos.clockskew=300
auth.kerberos.timeout=3
auth.kerberos.realm_name=RealmName
auth.kerberos.RealmName.realm=EXAMPLE.COM
auth.kerberos.RealmName.kdc=kerberos.example.com:88
auth.group.EXAMPLE.COM.protocol=ldap
auth.group.EXAMPLE.COM.port=389
auth.group.EXAMPLE.COM.basedn=dc=Example,dc=com
auth.group.EXAMPLE.COM.timeout=15
auth.group.EXAMPLE.COM.retry.interval=1
auth.group.EXAMPLE.COM.retry.times=20
```

- KDC サーバを DNS サーバに照会する場合（外部認可サーバとも連携するとき）

```
auth.server.type=kerberos
auth.group.mapping=true
auth.kerberos.default_realm=EXAMPLE.COM
auth.kerberos.dns_lookup_kdc=true
auth.kerberos.clockskew=300
auth.kerberos.timeout=3
```

(2) 情報検索用のユーザーアカウントの登録（認証方式が Kerberos の場合）

LDAP サーバを外部認可サーバとして利用する場合に、hcmdsldapuser コマンドを使用して、情報検索用のユーザーアカウントを管理サーバに登録します。登録後は、hcmdsldapuser コマンドで、情報検索用のユーザーアカウントを削除したり、管理サーバに情報検索用のユーザーアカウントを登録済みの LDAP サーバを確認したりできます。

情報検索用のユーザーアカウントを登録する

hcmdsldapuser コマンドで情報検索用のユーザーアカウントを登録します。

情報検索用のユーザーアカウントには、次の条件を満たすユーザーアカウントを登録してください。

- LDAP サーバに登録されていること
- exauth.properties ファイルの auth.group.<レルム名>.basedn で指定した DN にバインドできること
- exauth.properties ファイルの auth.group.<レルム名>.basedn で指定した DN 以下のすべてのエントリーに対して属性を検索できること
- exauth.properties ファイルの auth.group.<レルム名>.basedn で指定した DN を参照できること
- exauth.properties ファイルの auth.group.<レルム名>.basedn で指定した DN 下にある認可グループを参照できること
- exauth.properties ファイルの auth.group.<レルム名>.basedn で指定した DN 下にある認可グループの属性と、認可グループのネストグループの属性を検索できること

hcmdsldapuser コマンドの書式は次のとおりです。

```
<Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%bin
%hcmdsldapuser /set /dn <情報検索用ユーザーの DN> [/pass <情報検索用ユーザーの
パスワード>] /name <レルム名>
```

- <情報検索用ユーザーの DN >
DN は RFC4514 の規約に従って指定してください。例えば、次の文字が含まれる場合は、1 文字ごとに円記号 (¥) でエスケープする必要があります。
空白文字 # + , ; < = > ¥
- <情報検索用ユーザーのパスワード>
大文字と小文字の違いも含めて、LDAP サーバに登録しているパスワードと完全に一致している必要があります。pass オプションを省略してコマンドを実行すると、対話形式でパスワードを入力できます (対話形式では入力した文字列が伏せ字で表示されます)。
- <レルム名>
exauth.properties ファイルで KDC サーバの情報を直接指定した場合は、auth.kerberos.default_realm の値、または auth.kerberos.<auth.kerberos.realm_name 値>.realm の値を指定します。
exauth.properties ファイルで KDC サーバの情報を DNS サーバに照会するよう設定した場合は、DNS サーバに登録されたレルム名を指定します。

注意：

LDAP サーバでは DN やパスワードに引用符 (") を使用できますが、管理サーバには DN およびパスワードに引用符 (") が含まれていないユーザーアカウントを登録してください。

重要：

- Active Directory が提供する dsquery コマンドでユーザーの DN を確認できます。dsquery コマンドを使用して、ユーザー「administrator」の DN を確認する場合の実行例と実行結果を次に示します。

```
dsquery user -name administrator
"CN=administrator,CN=admin,DC=example,DC=com"
```

- DN が「cn=administrator,cn=admin,dc=example,com」の場合など、DN にコンマ (,) が含まれる場合は次のように指定します。

```
hcmdsldapuser /set /dn "cn=administrator,cn=admin,dc=example
¥,com" /pass administrator_pass /name ServerName
```

情報検索用のユーザーアカウントを削除する

情報検索用のユーザーアカウントを削除するには、次のコマンドを実行してください。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %bin  
%hcmdsldapuser /delete /name <レルム名 >
```

情報検索用ユーザーアカウントを登録済みの LDAP サーバを確認する

どの LDAP サーバの情報検索用ユーザーアカウントが管理サーバに登録されているかを確認する場合は、次のコマンドを実行してください。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %bin  
%hcmdsldapuser /list
```

(3) 外部認証サーバおよび外部認可サーバとの接続確認（認証方式が Kerberos の場合）

hcmdscheckauth コマンドを使用して、外部認証サーバおよび外部認可サーバに正しく接続できるか確認します。exauth.properties ファイルでレルム名を複数指定した場合は、レルムごとに確認してください。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %bin  
%hcmdscheckauth [/user <ユーザー ID > /pass <パスワード >] [/summary]
```

- 外部認証サーバとだけ連携する場合と、外部認可サーバとも連携する場合で、<ユーザー ID >、<パスワード >に指定するユーザーアカウントが異なります。

外部認証サーバとだけ連携する場合：

Hitachi File Services Manager に登録されていて、かつ認証方式が Kerberos のユーザーアカウントを指定してください。

外部認可サーバとも連携する場合：

Hitachi File Services Manager に登録されていないユーザーアカウントを指定してください。

exauth.properties ファイルの default_realm で設定したレルム名とは異なるレルムに所属するユーザーを指定する場合、<ユーザー ID >にはレルム名を含めた文字列を指定してください。exauth.properties ファイルの default_realm で設定したレルムに所属するユーザーを指定する場合は、レルム名を省略して入力できます。また、<ユーザー ID >、<パスワード >の先頭にスラッシュ (/) が含まれるユーザーアカウントは指定できません。

user オプションおよび pass オプションを省略してコマンドを実行すると、対話形式でユーザー ID およびパスワードを入力できます（対話形式では入力した文字列が伏せ字で表示されます）。

- summary オプションを指定すると、コマンド実行時に表示される確認メッセージが簡略化されます。

hcmdscheckauth コマンドを実行すると、次の 4 フェーズに分けて、exauth.properties ファイルの設定や、外部認証サーバおよび外部認可サーバとの接続状況がチェックされます。フェーズごとにチェック結果が表示されます。

フェーズ 1

exauth.properties ファイルの共通のプロパティ（表 7-19 KDC サーバで認証する場合の exauth.properties ファイルの設定項目（共通項目））が正しく設定されているかチェックします。

フェーズ 2

exauth.properties ファイルの外部認証サーバのプロパティ（「表 7-20 KDC サーバで認証する場合の exauth.properties ファイルの設定項目（外部認証サーバの情報を直接指定するとき）」または「表 7-21 KDC サーバで認証する場合の exauth.properties ファイルの設定項目（外部認証サーバの情報を DNS サーバに照会するとき）」）と、外部認可サーバのプロパティ（「表 7-22 KDC サーバで認証する場合の exauth.properties ファイルの設定項目（外部認可サーバの設定）」および「表 7-23 KDC サーバで認証する場合の exauth.properties ファイルの設定項目（外部認可サーバと StartTLS で通信するとき）」）が正しく設定されているかチェックします。

フェーズ 3

外部認証サーバに接続できるかチェックします。

フェーズ 4

外部認可サーバとも連携するよう設定されている場合に、外部認可サーバに接続できるか、および認可グループを検索できるかをチェックします。

各フェーズでの確認が正常に終了した場合、次のメッセージが表示されます。

```
KAPM15004-I The result of the configuration check of Phase <X> was normal.
```

注 <X>にはフェーズ番号が入ります。

(4) Kerberos 認証に使用できる暗号タイプ

Hitachi File Services Manager で、Kerberos 認証に使用できる暗号タイプ（encryption types）は次のとおりです。どれかの暗号タイプを使用できるように KDC サーバを構築してください。

- AES128-CTS-HMAC-SHA1-96
- RC4-HMAC
- DES3-CBC-SHA1
- DES-CBC-CRC
- DES-CBC-MD5

また、外部認証サーバの OS が Windows Server 2008, Windows Server 2008 R2 または Windows Server 2012 の場合、次の両方の条件の満たす環境では、ユーザー認証が正常に動作しないことがあります。

- 外部認証サーバで、ドメイン機能レベルに「Windows Server 2003」または「Windows 2000」が設定されている
- 管理サーバの OS で、暗号タイプに AES128-CTS がサポートされている

例えば、Active Directory のドメイン機能レベルに「Windows Server 2003」または「Windows 2000」で運用している場合でも、次の設定変更をすると、Active Directory でのユーザー認証ができなくなります。

- Active Directory 構築前から存在するユーザーのパスワードを、ドメイン機能レベルが「Windows Server 2003」の Active Directory に移行後に変更したとき
- Windows Server 2003 で構築した Active Directory から、Windows Server 2008 または Windows Server 2012 で構築したドメイン機能レベルが「Windows Server 2003」の Active Directory に移行後、ユーザーのパスワードを変更したとき

この場合は、exauth.properties ファイルの default_tkt_encetypes プロパティの設定を次のとおり変更してください。

7.4.7 Device Manager に接続してユーザーアカウントを管理する

Device Manager と連携する場合、Device Manager に接続してユーザーアカウントを管理する必要があります。Hitachi File Services Manager を、バージョン 8.0 以降の Device Manager がインストールされている管理サーバにインストールしたとき、または Device Manager とは別のマシンにインストールしたときは、Device Manager に接続してユーザーアカウントを管理するように設定を変更してください。

(1) バージョン 8.0 以降の Device Manager がインストールされている管理サーバにインストールしたとき

Device Manager に接続してユーザーアカウントを管理するように設定を変更する手順を次に示します。

1. 管理サーバで次のとおりコマンドを実行して、Device Manager に接続するための情報を設定します。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %bin%hcmdsprmset /  
host < 管理サーバの IP アドレスまたはホスト名 > /port < Device Manager のポート番号 > [/sslport < SSL 接続時の Device Manager のポート番号 >]
```

2. Hitachi File Services Manager および Device Manager を再起動します。

Hitachi File Services Manager を起動・停止する方法については、「[7.3 Hitachi File Services Manager を起動・停止する](#)」を参照してください。Device Manager の再起動については、Device Manager のシステム管理者に依頼してください。

(2) Device Manager とは別のマシンにインストールしたとき

Device Manager に接続してユーザーアカウントを管理するように設定を変更する手順を次に示します。

なお、Hitachi File Services Manager と Device Manager のインストールの順序によって、手順が異なります。

Device Manager の運用開始後に Hitachi File Services Manager をインストールした場合または Hitachi File Services Manager および Device Manager を同時にインストールした場合

1. Hitachi File Services Manager がインストールされている管理サーバで次のとおりコマンドを実行して、Device Manager がインストールされているサーバに接続するための情報を設定します。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %bin%hcmdsprmset /  
host < Device Manager の IP アドレスまたはホスト名 > /port < ポート番号 > [/sslport < SSL 接続時のポート番号 >]
```

2. Hitachi File Services Manager を再起動します。

Hitachi File Services Manager を起動・停止する方法については、「[7.3 Hitachi File Services Manager を起動・停止する](#)」を参照してください。

Hitachi File Services Manager の運用開始後に Device Manager をインストールした場合

1. Hitachi File Services Manager がインストールされている管理サーバで次のとおりコマンドを実行して、Hitachi File Services Manager の認証データを出力します。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%bin
%hcmdsauthmove /export /datapath < Hitachi File Services Manager の認証データを出
力するフォルダの絶対パス>
```

2. Device Manager のシステム管理者に、Hitachi File Services Manager の認証データの移行を依頼します。
3. Hitachi File Services Manager がインストールされている管理サーバで次のとおりコマンドを実行して、Device Manager がインストールされているサーバに接続するための情報を設定します。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%bin%hcmdsprmset /
host < Device Manager の IP アドレスまたはホスト名> /port <ポート番号> [/sslport <
SSL 接続時のポート番号>]
```

4. Hitachi File Services Manager および Device Manager を再起動します。
Hitachi File Services Manager を起動・停止する方法については、「[7.3 Hitachi File Services Manager を起動・停止する](#)」を参照してください。Device Manager の再起動については、Device Manager のシステム管理者に依頼してください。

7.4.8 Hitachi Command Suite 共通コンポーネントのセキュリティを設定する (LDAP サーバとの通信)

Hitachi File Services Manager では、LDAP サーバと連携してユーザー認証・認可を行う場合に、Hitachi File Services Manager と LDAP サーバ間のネットワーク伝送を StartTLS で暗号化できます。管理サーバと LDAP サーバ間の通信を StartTLS で保護するためには次の作業が必要です。

- LDAP サーバの証明書の入手
- トラストストアファイルへの証明書のインポート

なお、Hitachi File Services Manager と LDAP サーバ間のネットワーク伝送を StartTLS で暗号化するためには、`exauth.properties` ファイルの設定も必要です。

注意：

LDAP サーバのサーバ証明書の CN (Subject 欄の CN) は、`exauth.properties` ファイルの次の属性に指定した値と一致している必要があります。

認証方式が LDAP の場合：

```
auth.ldap.< auth.server.name に指定した値>.host
```

認証方式が RADIUS で、外部認可サーバとも連携する場合：

外部認証サーバと外部認可サーバが同一マシンで稼働しているとき：

```
auth.radius.< auth.server.name に指定した値>.host
```

外部認証サーバと外部認可サーバが別のマシンで稼働しているとき：

```
auth.group.<ドメイン名>.host
```

認証方式が Kerberos で、外部認可サーバとも連携する場合：

```
auth.kerberos.< auth.kerberos.realm_name に指定した値>.kdc
```

(1) LDAP サーバの証明書の入手

管理サーバと通信する LDAP サーバのサーバ証明書を入手します。詳細は、利用する LDAP サーバのマニュアルを参照してください。

認証局が発行した電子署名証明書を使用する場合は、サーバ証明書を発行した認証局からルート認証局までのすべての認証局の証明書がチェーンした状態であることを確認してください。電子署名

証明書の有効性を CRL 配布ポイント (CDP) に問い合わせる場合、AIA フィールドおよび CDP フィールドに ldap で始まる URL が含まれない証明書入手する必要があります。

また、著名な CA から LDAP サーバの証明書を取得している場合は、Hitachi Command Suite 共通コンポーネントが参照する標準のトラストストアにすでに CA 証明書が設定されていることがあるので、次のコマンドを実行して確認してください。すでに登録されている CA 証明書によって、LDAP サーバの証明書が認証される場合は、「(2) トラストストアファイルへの証明書のインポート」で説明するトラストストアの設定は不要です。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %bin
%hcmdskeytool -list -v -keystore <トラストストアファイル名> -storepass <トラストストアへのアクセスパスワード>
```

- -keystore <トラストストアファイル名>には、参照するトラストストアファイルを指定します。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %jdk%jre%lib
%security%cacerts
```

- -storepass <トラストストアへのアクセスパスワード>には、トラストストア cacerts を参照するためのパスワードを指定します。デフォルトは「changeit」です。

注意：

トラストストア cacerts は、Hitachi Command Suite 共通コンポーネントをバージョンアップすると更新されるため、cacerts に独自の証明書をインポートして運用することは避けてください。

(2) トラストストアファイルへの証明書のインポート

LDAP サーバの証明書を Hitachi Command Suite 共通コンポーネントで利用するトラストストアにインポートします。LDAP サーバの証明書は ldapcacerts にインポートすることをお勧めします。ほかのプログラムと証明書を共有する場合は jssecacerts にインポートしてもかまいません。トラストストアファイルが存在しない場合は新規に作成してください。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %conf%sec
%ldapcacerts
```

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %jdk%jre%lib
%security%jssecacerts
```

トラストストアファイルの作成、証明書のインポートおよび内容確認には、hcmdskeytool ユーティリティを使用します。

トラストストアファイルの作成、および証明書のインポートには、次のコマンドを実行してください。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %bin
%hcmdskeytool -import -alias <トラストストア内のユニーク名> -file <証明書
ファイル> -keystore <トラストストアファイル名> -storepass <トラストストアへの
アクセスパスワード>
```

- -alias <トラストストア内のユニーク名>には、トラストストア内で証明書を識別するための名称を指定します。
- -file <証明書ファイル>には、証明書ファイルを指定します。
- -keystore <トラストストアファイル名>には、登録・作成するトラストストアファイルを指定します。
- -storepass <トラストストアへのアクセスパスワード>には、トラストストアにアクセスするためのパスワードを指定します。

また、トラストストアの内容を表示するには、次のコマンドを実行してください。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %bin
%hcmdskeytool -list -v -keystore <トラストストアファイル名> -storepass <トラストストアへのアクセスパスワード>
```

- `-keystore` <トラストストアファイル名>には、確認するトラストストアファイルを指定します。
- `-storepass` <トラストストアへのアクセスパスワード>には、トラストストアにアクセスするためのパスワードを指定します。

なお、トラストストアを適用するためには、次の手順で **Hitachi File Services Manager** を再起動する必要があります。

1. **Hitachi File Services Manager** を停止します。
停止方法については、「[7.3.3 Hitachi File Services Manager を停止する](#)」を参照してください。
2. **Hitachi File Services Manager** を起動します。
起動方法については、「[7.3.2 Hitachi File Services Manager を起動する](#)」を参照してください。

注意：

- 証明書ファイルが複数ある場合は、トラストストア内で使用されていない任意のエイリアス名を指定して、インポートしてください。
- `hcmsgkeytool` ユーティリティで、トラストストア内のユニーク名、トラストストアのファイル名、およびパスワードを指定するときには、次の点に注意してください。
 - ファイル名には次の記号を使用しないでください。
: , ; * ? " < > |
 - ファイル名は 255 バイト以内の文字列にしてください。
 - トラストストア内のユニーク名、およびパスワードには引用符 (") を含めないでください。

7.5 Hitachi File Services Manager の環境を設定する

システム管理者は、設定ファイルを編集して、**Hitachi File Services Manager** の環境を設定したり、変更したりできます。

管理サーバをクラスタ構成で運用している場合は、実行系ノードと待機系ノードで同一の設定にしてください。

この節では、システム管理者が、**Hitachi File Services Manager** の環境を設定する方法について説明します。

7.5.1 ログファイルの設定を変更する

システム管理者は、プロパティファイルを編集して、**Hitachi File Services Manager** のメッセージログの最大容量や出力レベルなどの設定を変更できます。

ログファイルの設定を変更する手順を次に示します。

1. プロパティファイル (`user.properties`) を編集して、ログファイルの設定を変更します。
プロパティファイルは、次のフォルダに格納されています。
<Hitachi File Services Manager のインストールフォルダ>\%conf%
2. **Hitachi File Services Manager** および **Hitachi Command Suite** 共通コンポーネントをいったん停止したあと、起動し直します。

Hitachi File Services Manager および **Hitachi Command Suite** 共通コンポーネントを停止・起動する方法については、「[7.3 Hitachi File Services Manager を起動・停止する](#)」を参照してください。

ログファイルの設定を変更するためのプロパティを次の表に示します。

表 7-24 user.properties ファイルのプロパティ（ログファイルの設定）

プロパティ	説明
hnasm.common.logger.loglevel	Hitachi File Services Manager のメッセージログの出力レベルを設定します。 設定できる値※1 -1, 0, 10, 20 および 30 デフォルト値 20 設定できる値以外を指定した場合は、「20」を指定したものととして処理されます。
hnasm.common.logger.syslog.loglevel	Hitachi File Services Manager のイベントログの出力レベルを設定します。 設定できる値※1 -1, 0, 10, 20 および 30 デフォルト値 0 設定できる値以外を指定した場合は、「0」を指定したものととして処理されます。
hnasm.common.logger.maxfilenumber	Hitachi File Services Manager のメッセージログの最大バックアップ数を設定します。 設定できる値※2 1~16 デフォルト値 10 設定できる値以外を指定した場合は、「10」を指定したものととして処理されます。
hnasm.common.logger.maxfilesize	Hitachi File Services Manager のメッセージログの最大容量をバイト単位で設定します。 設定できる値※2 4096~2147483647 デフォルト値 2097152 設定できる値以外を指定した場合は、「2097152」を指定したものととして処理されます。

注※1 値の意味は次のとおりです。ただし、デフォルト値のまま使用することを推奨します。

- -1: 何も出力しない。
- 0: システム情報（起動や停止、重要なエラーなど）を出力する。
- 10: システム情報およびエラー情報を出力する。
- 20: システム情報、エラー情報、および実行履歴情報を出力する。
- 30: デバッグ情報を出力する。

注※2 デフォルト値以上の値を設定することを推奨します。

user.properties ファイルの記述例を次に示します。

```
hnasm.common.logger.loglevel=20
hnasm.common.logger.syslog.loglevel=0
hnasm.common.logger.maxfilenumber=10
hnasm.common.logger.maxfilesize=2097152
```

7.5.2 Hitachi File Services Manager の GUI で Virtual Server を削除する際の動作モードを設定する

システム管理者は、プロパティファイルを編集して、Hitachi File Services Manager の GUI で Virtual Server を削除する際の動作モードを設定できます。

Virtual Server 削除時の動作モードを設定する手順を次に示します。

1. プロパティファイル (user.properties) を編集して、動作モードを設定します。
プロパティファイルは、次のフォルダに格納されています。
< Hitachi File Services Manager のインストールフォルダ > \¥conf¥
2. Hitachi File Services Manager および Hitachi Storage Command Suite 共通コンポーネントをいったん停止したあと、起動し直します。
Hitachi File Services Manager および Hitachi Storage Command Suite 共通コンポーネントを停止・起動する方法については、「7.3 Hitachi File Services Manager を起動・停止する」を参照してください。

動作モードを設定するためのプロパティを次の表に示します。

表 7-25 user.properties ファイルのプロパティ (動作モードの設定)

プロパティ	説明
hnasm.model.deletevnas.mode	Hitachi File Services Manager の GUI で Virtual Server を削除するときの動作モードを指定します。 force 削除対象の Virtual Server にリソースが割り当てられているかどうかに関係なく、強制的に削除する場合に指定します。 このモードの場合、削除対象の Virtual Server にユーザー LU や仮想 IP アドレスが割り当てられていても削除できます。 safe 削除対象の Virtual Server にリソースが割り当てられているかどうかをチェックする場合に指定します。 このモードの場合、ユーザー LU や仮想 IP アドレスが割り当てられている Virtual Server は削除できません。 デフォルトは「force」です。上記以外の文字列を指定した場合は、「force」を指定したもものとして処理されます。

user.properties ファイルの記述例を次に示します。

```
...  
hnasm.model.deletevnas.mode=force  
...
```

7.5.3 ファイルスナップショット機能の情報更新の設定を変更する

システム管理者は、プロパティファイルを編集して、次に示すサブウィンドウでファイルスナップショット機能の情報を表示するたびに自動的に内容を更新するかどうかを設定できます。

- ・ [< ファイルシステム >] サブウィンドウの [File Snapshots] タブ
- ・ [< Physical Node >] サブウィンドウの [ファイルシステム] タブの [File Snapshots] サブタブ
- ・ [< Virtual Server >] サブウィンドウの [ファイルシステム] タブの [File Snapshots] サブタブ

ファイルスナップショット機能の情報更新の設定を変更する手順を次に示します。

1. プロパティファイル (user.properties) を編集して、ファイルスナップショット機能の情報更新の設定を変更します。

プロパティファイルは、次のフォルダに格納されています。

< Hitachi File Services Manager のインストールフォルダ > ¥conf¥

2. Hitachi File Services Manager および Hitachi Command Suite 共通コンポーネントをいったん停止したあと、起動し直します。

Hitachi File Services Manager および Hitachi Command Suite 共通コンポーネントを停止・起動する方法については、「[7.3 Hitachi File Services Manager を起動・停止する](#)」を参照してください。

ファイルスナップショット機能の情報更新の設定を変更するためのプロパティを次の表に示します。

表 7-26 user.properties ファイルのプロパティ (ファイルスナップショット機能の情報更新の設定変更)

プロパティ	説明
hnasm.model.refresh.tab.sync	ファイルスナップショット機能の情報を表示するたびに自動的に内容を更新するかどうかを指定します。 true 自動的に内容を更新する場合に指定します。 false 自動的に内容を更新しない場合に指定します。 デフォルトは「true」です。上記以外の文字列を指定した場合は、「true」を指定したものとして処理されます。

user.properties ファイルの記述例を次に示します。

```
...
hnasm.model.refresh.tab.sync=true
...
```

7.5.4 ライセンスの情報更新の設定を変更する

システム管理者は、プロパティファイルを編集して、[ライセンス設定] サブウィンドウでライセンスの情報を表示するたびに、自動的に内容を更新するかどうかを設定できます。

ライセンスの情報更新の設定を変更する手順を次に示します。

1. プロパティファイル (user.properties) を編集して、ライセンスの情報更新の設定を変更します。

プロパティファイルは、次のフォルダに格納されています。

< Hitachi File Services Manager のインストールフォルダ > ¥conf¥

2. Hitachi File Services Manager および Hitachi Command Suite 共通コンポーネントをいったん停止したあと、起動し直します。

Hitachi File Services Manager および Hitachi Command Suite 共通コンポーネントを停止・起動する方法については、「[7.3 Hitachi File Services Manager を起動・停止する](#)」を参照してください。

ライセンスの情報更新の設定を変更するためのプロパティを次の表に示します。

表 7-27 user.properties ファイルのプロパティ (ライセンスの情報更新の設定変更)

プロパティ	説明
hnasm.model.refresh.screen.license	ライセンスの情報を表示するたびに自動的に内容を更新するかどうかを指定します。 true 自動的に内容を更新する場合に指定します。 false 自動的に内容を更新しない場合に指定します。 デフォルトは「true」です。上記以外の文字列を指定した場合は、「true」を指定したものとして処理されます。

user.properties ファイルの記述例を次に示します。

```

...
hnasm.model.refresh.screen.license=true
...
    
```

7.5.5 Hitachi Command Suite 共通コンポーネントのポート番号を変更する

システム管理者は、設定ファイルを編集して、Hitachi Command Suite 共通コンポーネントによって使用されるポート番号を変更できます。

Hitachi Command Suite 共通コンポーネントによって使用されるポート番号のうち、変更できるものは次の表のとおりです。

表 7-28 Hitachi Command Suite 共通コンポーネントの変更できるポート番号

デフォルトのポート番号	説明
23015/tcp	管理クライアントと通信する際に、HBase Storage Mgmt Web Service へのアクセスで使用されます。SSLを設定している場合でも使用されます。SSL通信だけを許可したい場合は、ファイアウォールを設定してください。
23016/tcp	管理クライアントとSSLで通信する際に、HBase Storage Mgmt Web Service へのアクセスで使用されます。
23017/tcp	Hitachi Command Suite 共通コンポーネントの内部通信 (Web サーバとの通信) で使用されます。
23018/tcp	Hitachi Command Suite 共通コンポーネントの内部通信 (Web サーバからの終了メッセージを受信) で使用されます。
23025/tcp	Hitachi Command Suite 共通コンポーネントの内部通信 (Web サーバとの通信) で使用されます。
23026/tcp	Hitachi Command Suite 共通コンポーネントの内部通信 (Web サーバからの終了メッセージを受信) で使用されます。
23031/tcp	管理サーバの OS が Windows の場合に、Hitachi Command Suite 共通コンポーネントの内部通信 (シングルサインオン) で使用されます。
23032/tcp	Hitachi Command Suite 共通コンポーネントの内部通信 (HiRDB) で使用されます。

Hitachi File Services Manager をインストールしたあとに、Hitachi Command Suite 共通コンポーネントのポート番号を変更する手順を次に示します。

1. バージョン 05-70 より古い HiCommand 製品のサービスを停止します。

バージョン 05-70 より古い HiCommand 製品がインストールされている場合に必要手順です。サービスを停止する方法については、各製品のマニュアルを参照してください。

- Hitachi File Services Manager および Hitachi Command Suite 共通コンポーネントを停止します。

Hitachi File Services Manager および Hitachi Command Suite 共通コンポーネントを停止する方法については、「7.3 Hitachi File Services Manager を起動・停止する」を参照してください。

- Hitachi Command Suite 共通コンポーネントの設定ファイルを編集して、ポート番号を変更します。

変更方法は、ポート番号によって異なります。

表 7-29 Hitachi Command Suite 共通コンポーネントのポート番号設定ファイル

デフォルトのポート番号	設定ファイル	変更場所
23015/tcp	< Hitachi Command Suite 共通コンポーネントのインストールフォルダ >¥httpsd¥conf ¥httpsd.conf	Listen
	< Hitachi Command Suite 共通コンポーネントのインストールフォルダ >¥conf ¥hssso.conf	hssso.hostport
23016/tcp	< Hitachi Command Suite 共通コンポーネントのインストールフォルダ >¥httpsd¥conf ¥httpsd.conf	<ul style="list-style-type: none"> VirtualHost < ホスト名 > : < ポート > Listen*
23017/tcp	< Hitachi Command Suite 共通コンポーネントのインストールフォルダ >¥CC¥web ¥redirector¥workers.properties	worker.worker1.port
	< Hitachi Command Suite 共通コンポーネントのインストールフォルダ >¥CC¥web ¥containers¥HiCommand¥usrconf ¥usrconf.properties	webserver.connector.ajp13.port
23018/tcp	< Hitachi Command Suite 共通コンポーネントのインストールフォルダ >¥CC¥web ¥containers¥HiCommand¥usrconf ¥usrconf.properties	webserver.shutdown.port
23025/tcp	< Hitachi Command Suite 共通コンポーネントのインストールフォルダ >¥CC¥web ¥redirector¥workers.properties	worker.worker5.port
	< Hitachi Command Suite 共通コンポーネントのインストールフォルダ >¥CC¥web ¥containers¥HiCommand¥usrconf ¥usrconf.properties	webserver.connector.ajp13.port
23026/tcp	< Hitachi Command Suite 共通コンポーネントのインストールフォルダ >¥CC¥web ¥containers¥HiCommand¥usrconf ¥usrconf.properties	webserver.shutdown.port
23031/tcp	< Hitachi Command Suite 共通コンポーネントのインストールフォルダ >¥httpsd¥conf ¥hssso_httpsd.conf	Listen 127.0.0.1: <ポート番号>
23032/tcp	< Hitachi Command Suite 共通コンポーネントのインストールフォルダ >¥HDB¥CONF¥emb ¥HiRDB.ini	PDNAMEPORT

デフォルトのポート番号	設定ファイル	変更場所
	< Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%HDB%CONF%pdsys	pd_name_port
	< Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%database%work%def_pdsys	pd_name_port

注※

HBase Storage Mgmt Web Service へのアクセスで SSL を有効にする場合でも、23015/tcp は内部の通信で使用されます。そのため、Listen 23015 行を削除したり、コメント行にしたりしないでください。

- Hitachi File Services Manager および Hitachi Command Suite 共通コンポーネントを起動します。

Hitachi File Services Manager および Hitachi Command Suite 共通コンポーネントを起動する方法については、「[7.3 Hitachi File Services Manager を起動・停止する](#)」を参照してください。

- 手順 1 で停止したサービスがある場合は、起動します。

バージョン 05-70 より古い HiCommand 製品がインストールされている場合に必要手順です。サービスを起動する方法については、各製品のマニュアルを参照してください。

- 次のポート番号を変更した場合には、管理サーバの URL を変更する必要があります。

- 23015/tcp (HBase Storage Mgmt Web Service へのアクセスに使用)

非 SSL で管理サーバと管理クライアント間の通信を行うときには、URL を変更する必要があります。

- 23016/tcp (SSL 対応の HBase Storage Mgmt Web Service へのアクセスに使用)

SSL で管理サーバと管理クライアント間の通信を行うときには、URL を変更する必要があります。

管理サーバの URL を変更する方法については、Device Manager のマニュアルを参照してください。

なお、ファイアウォールが設置されている場合など、管理サーバと管理クライアントとの間のネットワーク環境によっては、URL の変更が不要なこともあります。

7.5.6 SSL を設定する

輸出管理の都合により削除

7.5.7 管理サーバとノードの通信に必要な SSL の証明書をインポートする

輸出管理の都合により削除

7.5.8 警告バナーの設定

システム管理者は、セキュリティ対策の一つとして、Hitachi File Services Manager のログイン画面に任意のメッセージ（警告バナー）を表示できます。不正なアクセスを試みようとする第三者に対し、事前に警告を発することで、データの破壊や情報の漏洩などのリスクを軽減できます。

同じ内容のメッセージをロケールごとに別の言語で登録しておけば、管理コンソールの WWW ブラウザのロケールに合わせて、メッセージを自動的に切り替えられます。

警告バナーの設定方法には次の2つの方法があります。

- コマンドを使用して登録する
- GUIを使用して登録する

ここでは、コマンドを使用して、メッセージを登録・解除する方法を説明します。

(1) メッセージファイルの作成

メッセージファイルには、通常の文字のほか、HTML タグを使用してフォント属性の変更や任意の位置での改行なども設定できます。

指定できる文字は Unicode (UTF-8) です。HTML タグも含めて、最大で 1,000 文字指定できます (指定した改行は文字数にカウントされます)。HTML タグで使用する始め山括弧 (<), 終わり山括弧 (>), アンパサンド (&), アポストロフィ ('') および引用符 (") を表示する場合は、HTML のエスケープシーケンスを使用してください。例えば、アンパサンド (&) をメッセージに表示したい場合は、「&」と記述してください。

メッセージの指定例を次に示します。

```
<center><b>警告</b></center>
これは{会社名}のコンピュータシステムです。このコンピュータシステムは、承認を受けた人だけがその業務のためにのみ使用できます。承認を受けない人からのアクセスや使用があった場合、侵入者として刑事、民事、および行政上の訴訟を提起する場合があります。<br>
犯罪捜査を含む公の目的のために、このコンピュータシステムに対するすべてのアクセスの履歴は、責任者によって傍受、記録、読み取り、複写、および開示される場合があります。アクセスした人に関する私的な機密情報についても機密性とプライバシーの要件に従って暗号化され、アクセス履歴として記録されます。このシステムを使用する人は、承認を受けているかどうかに関係なく、上記の条件に同意したものとみなします。このシステムにおいてプライバシーの権利はありません。
```

なお、メッセージを登録する際、HTML の構文のチェックおよび修正はされません。HTML の構文規則に従って正しく編集してください。メッセージ中の HTML の構文に問題がある場合、ログイン画面に正しく表示されないおそれがあります。

参考：

英語 (bannermsg.txt) と日本語 (bannermsg_ja.txt) のメッセージのサンプルファイルは、管理サーバの次のフォルダに格納されています。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %sample
%resource%
```

このサンプルファイルは、Hitachi Command Suite 共通コンポーネントをインストールするたびに上書きされます。サンプルファイルを使用する場合は、別のフォルダにコピーして使用してください。

(2) メッセージの登録

システム管理者は、作成したメッセージを hcmdsbanner コマンドで登録できます。管理サーバに、警告バナー機能がサポートされた Hitachi Command Suite 製品がインストールされている場合は、その製品のログイン画面にも登録したメッセージが表示されます。

メッセージを登録する際には、Administrator 権限を持つアカウントでログインしておく必要があります。

メッセージを登録する手順を次に示します。

1. 次のとおりコマンドを実行して、メッセージを登録します。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %bin%hcmdsbanner /
add /file <ファイル名> [/locale <ローケール名>]
```

ファイル名

メッセージファイルを絶対パスで指定します。指定できる文字は英数字、スペース、感嘆符 (!)、番号記号 (#)、始め丸括弧 ((), 終わり丸括弧 ()), 正符号 (+)、ハイフン (-)、ピリオド (.), 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 (_), 始め波括弧 ({), 終わり波括弧 (}), および波ダッシュ (~) です。また、パスの区切り文字として、斜線 (/)、コロン (:) および円記号 (¥) が使用できます。

/locale <ロケール名>

メッセージに使用した言語のロケールを指定します。例えば、英語は「en」、日本語は「ja」と指定します。指定したロケールでメッセージがすでに登録されていた場合は、更新されます。

登録するメッセージを GUI で編集する場合は、このオプションを省略してください。

(3) メッセージの削除

システム管理者は、登録したメッセージを hcmdsbanner コマンドで削除できます。メッセージを削除する際には、Administrator 権限を持つアカウントでログインしておく必要があります。

メッセージを削除する手順を次に示します。

1. 次のとおりコマンドを実行して、メッセージを削除します。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %bin% hcmdsbanner / delete [/locale <ロケール名 >]
```

/locale <ロケール名>

メッセージに使用した言語のロケールを指定します。例えば、英語は「en」、日本語は「ja」と指定します。

このオプションを省略すると、hcmdsbanner コマンドで /locale オプションを省略して登録したメッセージが削除されます。

7.5.9 Hitachi File Services Manager の監査ログの採取と確認

システム管理者は、Hitachi Command Suite 共通コンポーネントの環境設定ファイル (auditlog.conf) を編集することで、Hitachi File Services Manager に関するユーザーの操作内容を監査ログとして出力するように設定できます。出力するように設定した場合、Hitachi File Services Manager の監査ログは、Windows のイベントログファイル (アプリケーションログファイル) に出力されます。

監査事象には、重要度 (Severity) が設定されています。重要度によって、出力する監査ログをフィルタリングできます。

Hitachi File Services Manager で出力できる監査ログの種別を次の表に示します。

表 7-30 Hitachi File Services Manager で出力できる監査ログの種別

種別	説明
Authentication	機器、管理者、またはエンドユーザーが接続または認証を試みて成功または失敗したことを示す事象です。 <ul style="list-style-type: none">• FC ログイン• 機器認証 (FC-SP 認証, iSCSI ログイン認証, SSL サーバクライアント認証)• 管理者またはエンドユーザー認証

auditlog.conf ファイルに Authentication を設定することによって、Hitachi File Services Manager の監査ログとして出力される監査事象を次の表に示します。

表 7-31 Hitachi File Services Manager の監査ログとして出力される監査事象

種別の説明	監査事象	Severity	メッセージ ID
管理者またはエンドユーザーの認証	ログインの成功	6	KAPM01124-I
	ログインの成功 (外部認証サーバログイン)	6	KAPM02450-I
	ログインの失敗	6	KAPM01081-E
	ログインの失敗 (権限なし)	6	KAPM01095-E
	ログインの失敗 (ユーザー ID またはパスワードに誤りがある場合)	4	KAPM02291-W
	ログインの失敗 (ロック中のユーザーでログイン)	4	KAPM02291-W
	ログインの失敗 (存在しないユーザーでログイン)	4	KAPM02291-W
	ログインの失敗 (認証失敗)	4	KAPM01125-E
	ログインの失敗 (外部認証サーバ認証失敗)	4	KAPM02451-W
アカウントの自動ロック	アカウントの自動ロック (認証の連続失敗またはアカウントの有効期限切れ)	4	KAPM02292-W

Hitachi File Services Manager の監査ログとして出力される内容については、「[\(2\) Hitachi File Services Manager の監査ログを確認する](#)」を参照してください。

(1) Hitachi File Services Manager の監査ログの採取を設定する

Hitachi File Services Manager の監査ログの採取を設定する手順を次に示します。

- バージョン 05-70 より古い HiCommand 製品のサービスを停止します。
バージョン 05-70 より古い HiCommand 製品が管理サーバと同じマシンにインストールされている場合に必要手順です。サービスを停止する方法については、各製品のマニュアルを参照してください。
- Hitachi File Services Manager および Hitachi Command Suite 共通コンポーネントを停止します。
Hitachi File Services Manager および Hitachi Command Suite 共通コンポーネントを停止する方法については、「[7.3 Hitachi File Services Manager を起動・停止する](#)」を参照してください。
- auditlog.conf ファイルを編集して、Hitachi File Services Manager の監査ログとして出力されるように設定します。

auditlog.conf ファイルは、管理サーバの次のフォルダに格納されています。

< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > \conf\sec\auditlog.conf
auditlog.conf ファイルに設定する項目を次の表に示します。

表 7-32 auditlog.conf ファイルに設定する項目

項目	説明
Log.Event.Category	採取する監査事象の種別を指定します。監査事象の種別が指定されていない場合、監査ログは出力されません。指定できる種別については、「 表 7-30 」を参照してください。大文字、小文字は区別されません。指定できる種別以外を指定した場合は、無視されます。 デフォルト値：指定なし
Log.Level	採取する監査事象の重要度 (Severity) を指定します。指定した値以下の重要度を持つ監査事象が、イベントログファイルに出力されます。 Hitachi File Services Manager の監査ログとして出力される監査事象および監査事象の重要度 (Severity) については、「 表 7-31 」を参照してください。監査事象の重要度 (Severity) とイベントログの種類との対応については、「 表 7-33 」を参照してください。

項目	説明
	次に示す指定できる値以外の数値、または、数値以外の文字を指定した場合は、デフォルト値が仮定されます。 <ul style="list-style-type: none"> 指定できる値：0～7（監査事象の重要度（Severity）） デフォルト値：6

監査事象の重要度（Severity）とイベントログの種類を次の表に示します。

表 7-33 監査事象の重要度（Severity）とイベントログの種類

監査事象の重要度（Severity）	イベントログの種類
0	エラー
1	
2	
3	
4	警告
5	情報
6	
7	

次に auditlog.conf ファイルの設定例を示します。

```
Log.Event.Category Authentication
Log.Level 6
```

この例の場合、監査事象の重要度（Severity）が 0 から 6 の、Authentication の監査事象が出力されます。

- Hitachi File Services Manager および Hitachi Command Suite 共通コンポーネントを起動します。

Hitachi File Services Manager および Hitachi Command Suite 共通コンポーネントを起動する方法については、「7.3 Hitachi File Services Manager を起動・停止する」を参照してください。

- 手順 1 で停止したサービスがある場合は、起動します。

バージョン 05-70 より古い HiCommand 製品がインストールされている場合に必要手順です。サービスを起動する方法については、各製品のマニュアルを参照してください。

(2) Hitachi File Services Manager の監査ログを確認する

Hitachi File Services Manager の監査ログは管理サーバの次に示すイベントログに出力されます。

- Windows XP の場合
 [イベントビューア] - [アプリケーション] で、イベントを開いたときに表示される [説明] の内容
- Windows Server 2003, Windows Server 2003 R2 の場合
 [イベントビューア] - [アプリケーション] で、イベントを開いたときに表示される [イベントのプロパティ] - [説明] の内容
- Windows Vista, Windows 7, Windows 8, Windows Server 2008, Windows Server 2008 R2 または Windows Server 2012 の場合
 [イベントビューア] - [Windows ログ] - [アプリケーション] で、イベントを開いたときに表示される [イベントプロパティ] の [全般] タブの内容

次の形式で出力されます。

<プログラム名> [<プロセス ID>]:<メッセージ部>

<メッセージ部>の出力形式と内容を説明します。



重要 <メッセージ部>には、半角で 953 文字まで表示されます。

<統一識別子>, <統一仕様リビジョン番号>, <通番>, <メッセージ ID>, <日付・時刻>, <検出エンティティ>, <検出場所>, <監査事象の種別>, <監査事象の結果>, <監査事象の結果サブジェクト識別情報>, <ハードウェア識別情報>, <発生場所情報>, <ロケーション識別情報>, <FQDN>, <冗長化識別情報>, <エージェント情報>, <リクエスト送信元ホスト>, <リクエスト送信元ポート番号>, <リクエスト送信先ホスト>, <リクエスト送信先ポート番号>, <一括操作識別子>, <ログ種別情報>, <アプリケーション識別情報>, <予約領域>, <メッセージテキスト>

表 7-34 メッセージ部出力される情報

項目※	内容
統一識別子	「CELFSS」固定
統一仕様リビジョン番号	「1.1」固定
通番	監査ログのメッセージの通番
メッセージ ID	メッセージ ID 詳細については、「表 7-31」を参照してください。
日付・時刻	メッセージが出力された日付と時刻 「yyyy-mm-ddThh:mm:ss.s <タイムゾーン>」の形式で出力されます。
検出エンティティ	コンポーネント名やプロセス名
検出場所	ホスト名
監査事象の種別	事象の種別
監査事象の結果	事象の結果
監査事象の結果サブジェクト識別情報	事象に応じた、アカウント ID、プロセス ID または IP アドレス
ハードウェア識別情報	ハードウェアの型名や製番
発生場所情報	ハードウェアのコンポーネントの識別情報
ロケーション識別情報	ロケーション識別情報
FQDN	完全修飾ドメイン名
冗長化識別情報	冗長化識別情報
エージェント情報	エージェント情報
リクエスト送信元ホスト	リクエストの送信元のホスト名
リクエスト送信元ポート番号	リクエストの送信元のポート番号
リクエスト送信先ホスト	リクエストの送信先のホスト名
リクエスト送信先ポート番号	リクエストの送信先のポート番号
一括操作識別子	プログラム内で操作の通番
ログ種別情報	「BasicLog」または「DetailLog」
アプリケーション識別情報	プログラムの識別情報
予約領域	出力されません。予約領域です。
メッセージテキスト	監査事象に応じた内容

項目※	内容
	発生した監査事象の内容が、文字列で出力されます。表示できない文字は、アスタリスク (*) に置き換えて出力されます。

注※

監査事象によっては、出力されない項目もあります。

監査事象「ログインの成功」で出力されるメッセージ部の例を次に示します。

```
CELFSS,1.1,2,KAPM01124-I,2014-02-06T20:18:42.9+09:00,HBase-SSO,management-
host,Authentication,Success,uid=system,,,,,,,,,,,,BasicLog,,, "The login process
has completed properly."
```

7.6 管理サーバのメンテナンス

この節では、システム管理者が、Hitachi Command Suite 共通コンポーネントのコマンドを実行して、管理サーバのデータベースを管理する方法について説明します。

7.6.1 管理サーバのデータベースをバックアップ・リストアする

ここでは、Hitachi File Services Manager および Hitachi Command Suite 製品のデータベースをバックアップ・リストアする方法について説明します。

Hitachi File Services Manager および Hitachi Command Suite 製品のデータベースは、定期的にバックアップすることを推奨します。

なお、次の操作を実行する場合は、必ず事前にデータベースをバックアップしてください。

- Hitachi File Services Manager をアップグレードインストールまたは上書きインストールする場合
- 管理サーバに、Hitachi Command Suite 製品をインストールする場合
- 管理サーバから、Hitachi Command Suite 製品をアンインストールする場合
- すでに Hitachi Command Suite 製品がインストールされている管理サーバに、Hitachi File Services Manager をインストールする場合
- Hitachi Command Suite 製品がインストールされている管理サーバから、Hitachi File Services Manager をアンインストールする場合

(1) データベースをバックアップする

システム管理者は、コマンドを使用して、Hitachi File Services Manager および Hitachi Command Suite 製品のデータベースをバックアップできます。

Hitachi File Services Manager のデータベースをバックアップするときには、バックアップファイルを格納するフォルダが必要です。バックアップファイルを格納するフォルダには、バックアップコマンドが作成する一時ファイルの分も含めて次の空き容量が必要です。

必要な空き容量：

(<対象となる Hitachi Command Suite 製品のデータベースサイズの総和>) × 2 + 5MB

Hitachi File Services Manager および Hitachi Command Suite 製品のデータベースをバックアップする手順を次に示します。

1. 管理サーバ上の Device Manager に接続している Tuning Manager のサービスを停止します。

Hitachi Command Suite 製品がインストールされていて、そのうちの Device Manager に接続している Tuning Manager が、Device Manager とは別のマシンにインストールされている場合に必要な手順です。Tuning Manager がインストールされているマシンでサービスを停止してください。Tuning Manager のサービスを停止する方法については、インストールされている Tuning Manager のバージョンに対応するマニュアルを参照してください。

- バージョン 05-70 より古い HiCommand 製品のサービスを停止します。

バージョン 05-70 より古い HiCommand 製品が管理サーバと同じマシンにインストールされている場合に必要な手順です。サービスを停止する方法については、各製品のマニュアルを参照してください。

バージョン 05-70 以降の Hitachi Command Suite 製品が管理サーバと同じマシンにインストールされている場合は、Hitachi File Services Manager、Hitachi Command Suite 共通コンポーネントおよびバージョン 05-70 以降の Hitachi Command Suite 製品のサービスが停止しても問題ないことを確認した上で、手順 5 に進んでください。

- 次のとおりコマンドを実行して、Hitachi File Services Manager および Hitachi Command Suite 共通コンポーネントを停止します。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %bin%hcmdssrv /stop
```

- 次のとおりコマンドを実行して、HiRDB を起動します。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %bin%hcmdsdsrv /start
```

- 次のとおりコマンドを実行して、データベースをバックアップします。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %bin%hcmdsbackups /dir <バックアップ先フォルダ> [/auto]
```

バージョン 05-70 以降の Hitachi Command Suite 製品がインストールされている場合は、/auto オプションを指定してください。コマンドのオプションについて次に説明します。

/dir

Hitachi File Services Manager のデータベースのバックアップファイルを格納するローカルディスク上のフォルダ（バックアップ先フォルダ）を絶対パスで指定します。実在するフォルダを指定する場合は、空のフォルダであることを確認してください。

指定できる文字は英数字、スペース、感嘆符 (!)、番号記号 (#)、始め丸括弧 ((), 終わり丸括弧 ()), 正符号 (+)、ハイフン (-)、ピリオド (.), 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 (_), 始め波括弧 ({), 終わり波括弧 (}), および波ダッシュ (~) です。また、パスの区切り文字として、斜線 (/)、コロン (:) および円記号 (¥) を使用できます。

コマンドを実行すると、バックアップ先フォルダに database というフォルダが作成され、データベースのバックアップファイルが backup.hdb というファイル名で格納されます。

/auto

データベースを処理するための準備として、自動的に Hitachi Command Suite 共通コンポーネントおよび 05-70 以降の Hitachi Command Suite 製品のサービスを停止し、HiRDB を起動します。コマンド実行後には、Hitachi Command Suite 共通コンポーネントおよび 05-70 以降の Hitachi Command Suite 製品のサービスが起動されます。05-70 以降の Hitachi Command Suite 製品がインストールされている場合にだけ指定できます。

/auto オプションを指定した場合でも、Device Manager に接続している Tuning Manager が、Device Manager とは別のマシンにインストールされているときには、Tuning Manager のサービスが自動的に起動および停止されません。

- 手順 3 で Hitachi File Services Manager および Hitachi Command Suite 共通コンポーネントを停止している場合は、次のとおりコマンドを実行して、起動します。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%bin%\hcmdsdrv /
start
```

- 手順 2 で停止したサービスがある場合は、起動します。
バージョン 05-70 より古い HiCommand 製品がインストールされている場合に必要手順です。サービスを起動する方法については、各製品のマニュアルを参照してください。
- 手順 1 で Tuning Manager のサービスを停止した場合は、起動します。
Hitachi Command Suite 製品がインストールされていて、そのうちの Device Manager に接続している Tuning Manager が、Device Manager とは別のマシンにインストールされている場合に必要手順です。Tuning Manager がインストールされているマシンでサービスを起動してください。

(2) データベースをリストアする

システム管理者は、コマンドを使用して、バックアップした Hitachi File Services Manager のデータベースをリストアできます。また、Hitachi Command Suite 製品のデータベースも含めて一括リストアすることもできますが、その場合は、Hitachi Command Suite 製品がバックアップ時点の状態に戻っても問題ないことを事前に確認してください。

注意：

管理サーバ上の Hitachi File Services Manager および Hitachi Command Suite 製品をいったんアンインストールし、再度インストールしたあとに Hitachi File Services Manager のデータベースをリストアする場合は、必ず Hitachi Command Suite 製品のデータベースも含めて一括リストアしてください。

データベースをリストアする場合は、バックアップを取得した管理サーバと、リストア先の管理サーバとで、次の点が同じであることが前提です。

- インストールされている Hitachi File Services Manager および Hitachi Command Suite 製品の種類、バージョンおよびリビジョン
- Hitachi File Services Manager, Hitachi Command Suite 製品および Hitachi Command Suite 共通コンポーネントのインストール先
- Hitachi File Services Manager, Hitachi Command Suite 製品および Hitachi Command Suite 共通コンポーネントのデータベース作成先
- IP アドレスとホスト名

また、Hitachi File Services Manager のデータベースをリストアする際、hcmdsdb コマンドを実行すると、バックアップファイルがあるフォルダに一時ファイルが作成されます。フォルダに対して書き込み権限があり、次に示す空き容量があることを確認してください。

必要な空き容量：

(<対象となる Hitachi Command Suite 製品のデータベースサイズの総和>) + 5MB

Hitachi File Services Manager のデータベースをリストアする手順を次に示します。

- 管理サーバ上の Device Manager に接続している Tuning Manager のサービスを停止します。
Hitachi Command Suite 製品がインストールされていて、そのうちの Device Manager に接続している Tuning Manager が、Device Manager とは別のマシンにインストールされている場合に必要手順です。Tuning Manager がインストールされているマシンでサービスを停止してください。Tuning Manager のサービスを停止する方法については、インストールされている Tuning Manager のバージョンに対応するマニュアルを参照してください。
- バージョン 05-70 より古い HiCommand 製品のサービスを停止します。

バージョン 05-70 より古い HiCommand 製品が管理サーバと同じマシンにインストールされている場合に必要手順です。サービスを停止する方法については、各製品のマニュアルを参照してください。

バージョン 05-70 以降の Hitachi Command Suite 製品が管理サーバと同じマシンにインストールされている場合は、Hitachi File Services Manager、Hitachi Command Suite 共通コンポーネントおよびバージョン 05-70 以降の Hitachi Command Suite 製品のサービスが停止しても問題ないことを確認した上で、手順 4 に進んでください。

3. 次のとおりコマンドを実行して、Hitachi File Services Manager および Hitachi Command Suite 共通コンポーネントを停止します。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ >%bin%\hcmdssrv /stop
```

4. 次のとおりコマンドを実行して、データベースをリストアします。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ >%bin%\hcmdssrv /  
restore <バックアップファイル名> /type {FileServicesManager|ALL} [/auto]
```

バージョン 05-70 以降の Hitachi Command Suite 製品がインストールされている場合は、/auto オプションを指定してください。コマンドのオプションについて次に説明します。

/restore

リストアするバックアップファイルの名称（バックアップファイル名）を絶対パスで指定します。

/type

Hitachi File Services Manager のデータベースだけをリストアする場合は、FileServicesManager または HFSM と指定します。

管理サーバにインストールされている Hitachi File Services Manager および Hitachi Command Suite 製品のデータベースをリストアする場合は、ALL と指定します。

/auto

データベースを処理するための準備として、自動的に Hitachi Command Suite 共通コンポーネントおよび 05-70 以降の Hitachi Command Suite 製品のサービスを停止します。コマンド実行後には、Hitachi Command Suite 共通コンポーネントおよび 05-70 以降の Hitachi Command Suite 製品のサービスが停止された状態になります。05-70 以降の Hitachi Command Suite 製品がインストールされている場合にだけ指定できます。

/auto オプションを指定した場合でも、Device Manager に接続している Tuning Manager が、Device Manager とは別のマシンにインストールされているときには、Tuning Manager のサービスが自動的に起動および停止されません。

5. 次のとおりコマンドを実行して、Hitachi File Services Manager および Hitachi Command Suite 共通コンポーネントを起動します。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ >%bin%\hcmdssrv /  
start
```

6. 手順 2 で停止したサービスがある場合は、起動します。

バージョン 05-70 より古い HiCommand 製品がインストールされている場合に必要手順です。サービスを起動する方法については、各製品のマニュアルを参照してください。

7. 手順 1 で Tuning Manager のサービスを停止した場合は、起動します。

Hitachi Command Suite 製品がインストールされていて、そのうちの Device Manager に接続している Tuning Manager が、Device Manager とは別のマシンにインストールされている場合に必要手順です。Tuning Manager がインストールされているマシンでサービスを起動してください。

7.6.2 管理サーバを非クラスタ構成からクラスタ構成に移行する

ここでは、管理サーバを非クラスタ構成からクラスタ構成に移行する手順について説明します。

各手順は、すでに非クラスタ構成で運用を開始している管理サーバを次の前提条件でクラスタ構成に移行することを想定しています。

- すでに非クラスタ構成で運用を開始している管理サーバを実行系ノードとして設定する。
- 実行系ノードにインストールされている Hitachi Command Suite 製品は、待機系ノードにもインストールされており、ライセンスの設定も完了している。

なお、ここでは Windows Server 2003 での操作方法について説明しています。Windows Server 2008 または Windows Server 2012 を使用している場合は、操作手順に記載している「クラスタアドミニストレータ」を「フェールオーバー クラスタ管理」に読み替えてください。また、各設定項目および設定先も、「フェールオーバー クラスタ管理」についてのドキュメントを参照して、対応する名称に読み替えてください。

(1) クラスタ構成に移行する前に

クラスタ構成に移行する前に、次のことを確認してください。

- 実行系ノードおよび待機系ノードが、マシン要件を満たしていること
管理サーバのマシン要件については、「[3.2.1 管理サーバのマシン要件](#)」を参照してください。
- 実行系ノードおよび待機系ノードに、クラスタ構成に必要なソフトウェアがインストールされていること
管理サーバのクラスタ構成に必要なソフトウェアについては、「[3.2.2 管理サーバのクラスタ構成](#)」を参照してください。
- 実行系ノードで共有ディスクが有効になっていること
共有ディスクを有効にする方法については、「[7.2.1 Hitachi File Services Manager を新規インストールする（管理サーバをクラスタ構成で運用する場合）](#)」を参照してください。
- 実行系ノード、待機系ノードおよびクラスタ管理 IP アドレスについて、ホスト名から IP アドレスへの名前解決ができること
- 待機系ノードへのインストールを予定している Hitachi File Services Manager のバージョンが、実行系ノードと同じであること

クラスタの設定作業をしている間は、Hitachi File Services Manager にアクセスしないでください。

管理サーバの実行系ノードでの設定を実施してから、待機系ノードでの設定を実施してください。

(2) 管理サーバの実行系ノードでの設定

管理サーバを非クラスタ構成からクラスタ構成に移行する場合の、実行系ノードでの設定手順を次に示します。

1. データベースのバックアップを取得します。
データベースのバックアップを取得する方法については、「[7.6.1 管理サーバのデータベースをバックアップ・リストアする](#)」を参照してください。
2. テキストエディターを使って、クラスタ設定ファイルを作成します。
次の項目を指定したファイルを作成してください。
 - mode
online と指定します。
 - virtualhost

論理ホスト名を指定します。

- **onlinehost**
実行系ノードのホスト名を指定します。
- **standbyhost**
待機系ノードのホスト名を指定します。

virtualhost, onlinehost および standbyhost には、IP アドレスは指定できません。
クラスタ設定ファイルの記述例を次に示します。

```
mode = online
virtualhost = hicommand_cluster
onlinehost = hicommand_1
standbyhost = hicommand_2
```

3. クラスタ設定ファイルの名称を cluster.conf として、次の場所に格納します。
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > ¥conf¥
4. 管理サーバ上の Device Manager に接続している Tuning Manager のサービスを停止します。
Hitachi Command Suite 製品がインストールされていて、そのうちの Device Manager に接続している Tuning Manager が、Device Manager とは別のマシンにインストールされている場合に必要手順です。Tuning Manager がインストールされているマシンでサービスを停止してください。Tuning Manager のサービスを停止する方法については、インストールされている Tuning Manager のバージョンに対応するマニュアルを参照してください。
5. バージョン 05-70 より古い HiCommand 製品のサービスを停止します。
バージョン 05-70 より古い HiCommand 製品が管理サーバと同じマシンにインストールされている場合に必要手順です。サービスを停止する方法については、各製品のマニュアルを参照してください。
バージョン 05-70 以降の Hitachi Command Suite 製品が管理サーバと同じマシンにインストールされている場合は、Hitachi File Services Manager, Hitachi Command Suite 共通コンポーネントおよびバージョン 05-70 以降の Hitachi Command Suite 製品のサービスが停止しても問題ないことを確認した上で、手順 10 に進んでください。
6. 次のとおりコマンドを実行して、Hitachi File Services Manager および Hitachi Command Suite 共通コンポーネントを停止します。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > ¥bin¥hcmdssrv /stop
```

7. 次のとおりコマンドを実行して、HiRDB を起動します。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > ¥bin¥hcmdsdbsrv /start
```

8. 次のとおりコマンドを実行して、データベースを共有ディスクに移行します。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > ¥bin
¥hcmdsdbclustersetup /createcluster /databasepath <データベースの再作成先フォルダ >
/exportpath <データの格納先フォルダ > [/auto]
```

バージョン 05-70 以降の Hitachi Command Suite 製品がインストールされている場合は、/auto オプションを指定します。コマンドの引数は、次の条件に従って指定してください。

- データベースの再作成先フォルダは 92 バイト以下、データの格納先フォルダは 85 バイト以下の絶対パスで指定してください。
- データベースの再作成先フォルダは、共有ディスク上に配置してください。
- データの格納先フォルダは、ローカルディスク上に配置してください。
- データの格納先フォルダに実在するフォルダを指定する場合は、空のフォルダであることを確認してください。

- データベースの再作成先フォルダおよびデータの格納先フォルダに使用できる文字は英数字、始め丸括弧 ((), 終わり丸括弧 ()), ピリオド (.), アンダーライン (_) およびスペースです。ただし、ピリオド (.) は文字列の先頭および末尾には指定できません。また、スペースは、文字列の先頭および末尾に指定したり、2 つ以上連続して指定したりできません。
- データベースの再作成先フォルダおよびデータの格納先フォルダには、パスの区切り文字として、円記号 (¥) が使用できます。ただし、文字列の末尾には指定できません。

データベース再作成先フォルダには、次に示す空き容量が必要です。

必要な空き容量 = 2.1GB + ほかの Hitachi Command Suite 製品のデータベース容量
データベース再作成先フォルダの空き容量不足が原因で hcmdsdbclustersetup コマンドの実行に失敗した場合は、データベース再作成先フォルダの空き容量を増やしたあとで、hcmdsdbclustersetup コマンドを再実行してください。

hcmdsdbclustersetup コマンドが正常終了するまでは、共有ディスクを実行系ノードから切り離さないでください。

hcmdsdbclustersetup コマンドが異常終了した状態でサーバを再起動すると、共有ディスクの接続先が待機系ノードに切り替わることがあります。

このコマンドを実行すると、HiRDB が使用するポート番号がデフォルト値 (23032) に戻ります。/auto オプションを指定しないでコマンドを実行した場合は、Hitachi File Services Manager および Hitachi Command Suite 共通コンポーネントが再起動します。

/auto オプションを指定した場合でも、Device Manager に接続している Tuning Manager が、Device Manager とは別のマシンにインストールされているときには、Tuning Manager のサービスが自動的に起動および停止されません。

- HiRDB が使用するポート番号をデフォルト値 (23032) から変更して運用する場合は、変更後のポート番号に設定し直してください。

HiRDB が使用するポート番号を変更する方法については、「[7.5.5 Hitachi Command Suite 共通コンポーネントのポート番号を変更する](#)」を参照してください。

- Hitachi File Services Manager および Hitachi Command Suite 共通コンポーネントが稼働している場合は、次のとおりコマンドを実行して、停止します。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %bin%hcmdsdrv /stop
```

- Windows の [サービス] ウィンドウで次のプロパティを開き、[スタートアップの種類] を [自動] から [手動] に変更します。

- Hitachi Command Suite 製品のサービス
- HBase Storage Mgmt Common Service
- HBase Storage Mgmt Web Service
- HiRDB/ClusterService_HD0

- クラスタアドミニストレータで、Hitachi File Services Manager で利用するリソースの登録先のグループに、次のリソースを追加します。

- HBase Storage Mgmt Common Service
- HBase Storage Mgmt Web Service
- HiRDB/ClusterService_HD0
- Hitachi Command Suite 製品のサービス

HBase Storage Mgmt Common Service, HBase Storage Mgmt Web Service および HiRDB/ClusterService_HD0 を追加するには、[新規作成] - [リソース] を選択して、各ダイアログで表 7-35 HBase Storage Mgmt Common Service をリソースとして登録するための設定～表 7-37 HiRDB をリソースとして登録するための設定に示した情報を指定し、[完了] ボタンをクリックします。

Hitachi Command Suite 製品のサービスを追加する方法については、各製品のマニュアルを参照してください。

表 7-35 HBase Storage Mgmt Common Service をリソースとして登録するための設定

ダイアログ名	設定
新しいリソース	次の項目を指定します。 名前 HBase Storage Mgmt Common Service (任意) リソースの種類 汎用サービス
実行可能な所有者	実行系ノードと待機系ノードが追加されていることを確認します。
依存関係	HiRDB を登録します。
汎用サービスパラメーター	次の項目を指定します。 サービス名 HBaseStgMgmtComService 起動パラメーター なし
レジストリの複製	何も指定しません。

表 7-36 HBase Storage Mgmt Web Service をリソースとして登録するための設定

ダイアログ名	設定
新しいリソース	次の項目を指定します。 名前 HBase Storage Mgmt Web Service (任意) リソースの種類 汎用サービス
実行可能な所有者	実行系ノードと待機系ノードが追加されていることを確認します。
依存関係	HBaseStgMgmtComService を登録します。
汎用サービスパラメーター	次の項目を指定します。 サービス名 HBaseStgMgmtWebService 起動パラメーター なし
レジストリの複製	何も指定しません。

表 7-37 HiRDB をリソースとして登録するための設定

ダイアログ名	設定
新しいリソース	次の項目を指定します。 名前 HiRDB (任意) リソースの種類 汎用サービス
実行可能な所有者	実行系ノードと待機系ノードが追加されていることを確認します。
依存関係	共有ディスクのドライブ、およびネットワーク名を登録します。
汎用サービスパラメーター	次の項目を指定します。 サービス名 HiRDBClusterService_HD0 起動パラメーター なし
レジストリの複製	何も指定しません。

また、Windows Server 2008 または Windows Server 2012 を使用している場合は、コマンドプロンプトから次のコマンドを実行してください。

```
cluster res "<リソース名>" /priv StartupParameters=""
```

<リソース名>には、HBase Storage Mgmt Web Service の汎用サービスのリソース名を指定します。リソース名は「フェールオーバー クラスタ管理」で確認してください。

(3) 管理サーバの待機系ノードでの設定

管理サーバを非クラスタ構成からクラスタ構成に移行する場合の、待機系ノードでの設定手順を次に示します。

1. 待機系ノードに、実行系ノードと同じバージョンの Hitachi File Services Manager を新規インストールします。

Hitachi File Services Manager を新規インストールする方法については、「[7.1.1 Hitachi File Services Manager を新規インストールする](#)」を参照してください。インストールする際は、Hitachi Command Suite 共通コンポーネント、および管理サーバが使用するデータベースの格納先にはデフォルト値を指定してください。

2. 管理サーバ上の Device Manager に接続している Tuning Manager のサービスを停止します。

Hitachi Command Suite 製品がインストールされていて、そのうちの Device Manager に接続している Tuning Manager が、Device Manager とは別のマシンにインストールされている場合に必要手順です。Tuning Manager がインストールされているマシンでサービスを停止してください。Tuning Manager のサービスを停止する方法については、インストールされている Tuning Manager のバージョンに対応するマニュアルを参照してください。

3. バージョン 05-70 より古い HiCommand 製品のサービスを停止します。

バージョン 05-70 より古い HiCommand 製品が管理サーバと同じマシンにインストールされている場合に必要手順です。サービスを停止する方法については、各製品のマニュアルを参照してください。

バージョン 05-70 以降の Hitachi Command Suite 製品が管理サーバと同じマシンにインストールされている場合は、Hitachi File Services Manager、Hitachi Command Suite 共通コンポーネントおよびバージョン 05-70 以降の Hitachi Command Suite 製品のサービスが停止しても問題ないことを確認した上で、手順 8 に進んでください。

4. 次のとおりコマンドを実行して、Hitachi File Services Manager および Hitachi Command Suite 共通コンポーネントを停止します。

```
<Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%bin%hcmdssrv /stop
```

5. 次のとおりコマンドを実行して、HiRDB を起動します。

```
<Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%bin%hcmdsbsrv /start
```

6. テキストエディターを使って、クラスタ設定ファイルを作成します。

次の項目を指定したファイルを作成してください。

- mode
standby と指定します。
- virtualhost
論理ホスト名を指定します。
- onlinehost
実行系ノードのホスト名を指定します。
- standbyhost

待機系ノードのホスト名を指定します。

virtualhost, onlinehost および standbyhost には、IP アドレスは指定できません。
クラスタ設定ファイルの記述例を次に示します。

```
mode = standby
virtualhost = hicommand_cluster
onlinehost = hicommand_1
standbyhost = hicommand_2
```

7. クラスタ設定ファイルの名称を cluster.conf とし、次の場所に格納します。

< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > ¥conf¥

8. 次のとおりコマンドを実行して、共有ディスク上のデータベースを使用するよう設定します。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > ¥bin
¥hcmdsdbclustersetup /createcluster /databasepath <データベースの再作成先フォルダ
> /exportpath <データの格納先フォルダ > [/auto]
```

バージョン 05-70 以降の Hitachi Command Suite 製品がインストールされている場合は、/auto オプションを指定します。コマンドの引数は、次の条件に従って指定してください。

- データベースの再作成先フォルダには、実行系ノードと同じフォルダを指定してください。
- データの格納先フォルダは、85 バイト以下の絶対パスで指定してください。
- データの格納先フォルダは、ローカルディスク上に配置してください。
- データの格納先フォルダに実在するフォルダを指定する場合は、空のフォルダであることを確認してください。
- データの格納先フォルダに使用できる文字は英数字、始め丸括弧 (), 終わり丸括弧 (), ピリオド (.), アンダーライン (_) およびスペースです。ただし、ピリオド (.) は文字列の先頭および末尾には指定できません。また、スペースは、文字列の先頭および末尾に指定したり、2 つ以上連続して指定したりできません。
- データの格納先フォルダには、パスの区切り文字として、円記号 (¥) が使用できます。ただし、文字列の末尾には指定できません。

hcmdsdbclustersetup コマンドが正常終了するまでは、共有ディスクを実行系ノードから切り離さないでください。

また、hcmdsdbclustersetup コマンドが異常終了した状態でサーバを再起動しないでください。

このコマンドを実行すると、HiRDB が使用するポート番号がデフォルト値 (23032) に戻ります。/auto オプションを指定しないでコマンドを実行した場合は、Hitachi File Services Manager および Hitachi Command Suite 共通コンポーネントが再起動します。

/auto オプションを指定した場合でも、Device Manager に接続している Tuning Manager が、Device Manager とは別のマシンにインストールされているときには、Tuning Manager のサービスが自動的に起動および停止されません。

9. HiRDB が使用するポート番号をデフォルト値 (23032) から変更して運用する場合は、変更後のポート番号に設定し直してください。

HiRDB が使用するポート番号を変更する方法については、「[7.5.5 Hitachi Command Suite 共通コンポーネントのポート番号を変更する](#)」を参照してください。

10. Hitachi File Services Manager および Hitachi Command Suite 共通コンポーネントが稼働している場合は、次のとおりコマンドを実行して、停止します。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > ¥bin¥hcmdssrv /stop
```

11. Windows の [サービス] ウィンドウで次のプロパティを開き、[スタートアップの種類] を [自動] から [手動] に変更します。

- Hitachi Command Suite 製品のサービス
- HBase Storage Mgmt Common Service
- HBase Storage Mgmt Web Service
- HiRDB/ClusterService_HD0

12. クラスタアドミニストレータで、グループをオンラインにします。

7.6.3 管理サーバのデータベースを移行する

Hitachi File Services Manager および Hitachi Command Suite 製品を長期間使用していると、管理対象となるオブジェクトの増加やバージョンアップなどによって、今までよりも高性能なマシンへのリプレースが必要となることがあります。このような場合、リプレース作業の一つとして、データベースを移行する必要があります。

システム管理者は、Hitachi File Services Manager のインストール先が移行元と移行先で異なる場合や、移行先の Hitachi File Services Manager のバージョンが移行元より新しい場合でもデータベースを移行できます。

ここでは、管理サーバのデータベースを移行する方法について説明します。

(1) データベースを移行する前に

移行先と移行元の Hitachi File Services Manager および Hitachi Command Suite 製品の種類、バージョンおよびユーザー情報についての注意事項を次に示します。

移行先と移行元の Hitachi File Services Manager および Hitachi Command Suite 製品の種類とバージョンについての注意事項

- 移行先には、必要な Hitachi File Services Manager および Hitachi Command Suite 製品を漏れなくインストールしてください。
移行先にインストールされていない Hitachi File Services Manager および Hitachi Command Suite 製品のデータベースは移行できません。
- 移行元と同じバージョンか、または移行元よりも新しいバージョンの Hitachi File Services Manager および Hitachi Command Suite 製品を移行先サーバにインストールしてください。
移行先にインストールされている Hitachi File Services Manager および Hitachi Command Suite 製品のバージョンがどれか1つでも移行元より古い場合、移行はできません。
- Hitachi NAS Manager のデータベースを Hitachi File Services Manager のデータベースに移行する場合は、移行元の Hitachi NAS Manager を Hitachi File Services Manager にアップグレードしてからデータベースを移行してください。
- バージョン 04-20 以前の Replication Monitor のデータベースを移行する場合は、事前に移行元および移行先の Replication Monitor を 5.x のバージョンにアップグレードしてください。
- Replication Monitor のデータベースを Replication Manager のデータベースに移行する場合は、移行元の Replication Monitor を Replication Manager にアップグレードしてからデータベースを移行してください。
- Tuning Manager のデータベースを移行する場合は、データベースが移行できる状態かどうかを確認する必要があります。詳細については、Tuning Manager のマニュアルで、データベースの管理について説明している箇所を参照してください。
- Tuning Manager のバージョンが 6.0 未満の場合、管理対象となるリソース数が管理限界の 70% を超えるときには、同じデータベースの構成には移行できません。

ユーザー情報についての注意事項

- すでに Hitachi File Services Manager および Hitachi Command Suite 製品のユーザー情報がある管理サーバにデータベースを移行しないでください。
移行先にユーザー情報がある場合、そのユーザー情報は移行元のユーザー情報に置き換えられます。
- 移行によってユーザー情報が置き換えられるため、複数の管理サーバで稼働していた Hitachi File Services Manager および Hitachi Command Suite 製品を 1 台の管理サーバに集約するような移行はできません。

データベースを移行する手順を次に示します。

1. 移行先サーバに、データベースを移行する Hitachi File Services Manager および Hitachi Command Suite 製品をインストールします。
Hitachi File Services Manager をインストールする方法については、「[7.1.1 Hitachi File Services Manager を新規インストールする](#)」を参照してください。Hitachi Command Suite 製品をインストールする方法については、各製品のマニュアルを参照してください。
2. 移行元サーバでデータベースをエクスポートします。
移行元サーバでデータベースをエクスポートする方法については、「[\(2\) 移行元サーバでのデータベースのエクスポート](#)」を参照してください。
3. 移行元サーバから移行先サーバへアーカイブファイルを転送します。
4. 移行先サーバでデータベースをインポートします。
移行先サーバでデータベースをインポートする方法については、「[\(3\) 移行先サーバでのデータベースのインポート](#)」を参照してください。

(2) 移行元サーバでのデータベースのエクスポート

Hitachi File Services Manager のデータベースをエクスポートするときには、データベースの情報を一時的に格納するためのフォルダと、アーカイブファイルを格納するフォルダが必要です。それぞれのフォルダには、次に示す 2 つのフォルダの合計サイズと同等の容量を確保してください。

- Hitachi File Services Manager のデータベースの格納先フォルダ
- Hitachi Command Suite 共通コンポーネントのデータベースの格納先フォルダから SYS フォルダ以下を除いたもの

この容量は、Hitachi File Services Manager のデータベースだけがインストールされているときの目安値です。Hitachi Command Suite 製品がインストールされている場合は、それらのデータベースの容量も考慮してください。

データベースの全体容量が 2GB を超えている場合、データベースのエクスポート時に、アーカイブファイルの作成に失敗します。2GB を超えてしまう場合は、アーカイブファイルを使用しない方法で移行します。

データベースを移行元サーバからエクスポートする手順を次に示します。

1. 管理サーバ上の Device Manager に接続している Tuning Manager のサービスを停止します。
Hitachi Command Suite 製品がインストールされていて、そのうちの Device Manager に接続している Tuning Manager が、Device Manager とは別のマシンにインストールされている場合に必要手順です。Tuning Manager がインストールされているマシンでサービスを停止してください。Tuning Manager のサービスを停止する方法については、インストールされている Tuning Manager のバージョンに対応するマニュアルを参照してください。

- バージョン 05-70 より古い HiCommand 製品のサービスを停止します。
バージョン 05-70 より古い HiCommand 製品が管理サーバと同じマシンにインストールされている場合に必要手順です。サービスを停止する方法については、各製品のマニュアルを参照してください。

バージョン 05-70 以降の Hitachi Command Suite 製品が管理サーバと同じマシンにインストールされている場合は、Hitachi File Services Manager、Hitachi Command Suite 共通コンポーネントおよびバージョン 05-70 以降の Hitachi Command Suite 製品のサービスが停止しても問題ないことを確認した上で、手順 5 に進んでください。

- 次のとおりコマンドを実行して、Hitachi File Services Manager および Hitachi Command Suite 共通コンポーネントを停止します。

```
<Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%bin%hcmdssrv /stop
```

- 次のとおりコマンドを実行して、HiRDB を起動します。

```
<Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%bin%hcmdsdbsrv /start
```

- 次のとおりコマンドを実行して、データベースをエクスポートします。

```
<Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%bin%hcmdsdbsrv /export /workpath <作業用フォルダ> /file <アーカイブファイル> [/auto]
```

05-70 以降の Hitachi Command Suite 製品がインストールされている場合は、/auto オプションを指定してください。コマンドのオプションについて次に説明します。

/export

データベースをエクスポートする場合に必ず指定するオプションです。

/workpath

エクスポートしたデータベースの情報を一時的に保存するフォルダ（作業用フォルダ）を絶対パスで指定します。この作業用フォルダは、ローカルディスクにある空のフォルダを指定する必要があります。

/file

データベースのアーカイブファイルを絶対パスで指定します。

/auto

データベースを処理するための準備として、自動的に Hitachi Command Suite 共通コンポーネントおよび 05-70 以降の Hitachi Command Suite 製品のサービスを停止し、HiRDB を起動します。コマンド実行後には、Hitachi Command Suite 共通コンポーネントおよび 05-70 以降の Hitachi Command Suite 製品のサービスが起動されます。05-70 以降の Hitachi Command Suite 製品がインストールされている場合にだけ指定できます。

/auto オプションを指定した場合でも、Device Manager に接続している Tuning Manager が、Device Manager とは別のマシンにインストールされているときには、Tuning Manager のサービスが自動的に起動および停止されません。

- エラーメッセージが出力された場合は、必ずメッセージに従って対処してください。
- 移行先サーバにアーカイブファイルを転送します。
アーカイブファイルを作成できなかった場合、/workpath オプションで指定したフォルダに格納されているファイルをすべて転送してください。このとき、/workpath オプションで指定したフォルダ以下のファイル構成は変更しないでください。

(3) 移行先サーバでのデータベースのインポート

データベースを移行先サーバにインポートする手順を次に示します。

1. 管理サーバ上の Device Manager に接続している Tuning Manager のサービスを停止します。
Hitachi Command Suite 製品がインストールされていて、そのうちの Device Manager に接続している Tuning Manager が、Device Manager とは別のマシンにインストールされている場合に必要な手順です。Tuning Manager がインストールされているマシンでサービスを停止してください。Tuning Manager のサービスを停止する方法については、インストールされている Tuning Manager のバージョンに対応するマニュアルを参照してください。
2. バージョン 05-70 より古い HiCommand 製品のサービスを停止します。
バージョン 05-70 より古い HiCommand 製品が管理サーバと同じマシンにインストールされている場合に必要な手順です。サービスを停止する方法については、各製品のマニュアルを参照してください。
バージョン 05-70 以降の Hitachi Command Suite 製品が管理サーバと同じマシンにインストールされている場合は、Hitachi File Services Manager、Hitachi Command Suite 共通コンポーネントおよびバージョン 05-70 以降の Hitachi Command Suite 製品のサービスが停止しても問題ないことを確認した上で、手順 5 に進んでください。
3. 次のとおりコマンドを実行して、Hitachi File Services Manager および Hitachi Command Suite 共通コンポーネントを停止します。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %bin%hcmdssrv /stop
```

4. 次のとおりコマンドを実行して、HiRDB を起動します。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %bin%hcmdsdsrv /start
```

5. 次のとおりコマンドを実行して、データベースをインポートします。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %bin%hcmdsdbtrans /import /workpath <作業用フォルダ> [/file <アーカイブファイル>] /type {ALL | <移行する Hitachi File Services Manager および Hitachi Command Suite 製品の名称>} [/auto]
```

05-70 以降の Hitachi Command Suite 製品がインストールされている場合は、/auto オプションを指定してください。コマンドのオプションについて次に説明します。

/import

データベースをインポートする場合に必ず指定するオプションです。

/workpath

アーカイブファイルを使用してインポートする場合：

アーカイブファイルを展開するためのフォルダ（作業用フォルダ）を、絶対パスで指定します。この作業用フォルダは、ローカルディスクにある空のフォルダを指定する必要があります。アーカイブファイルを使用する場合、/file オプションは必ず指定します。

アーカイブファイルを使用しないでインポートする場合：

移行元から転送したデータベース情報を格納したフォルダを指定してください。/file オプションは指定しないでください。

/file

移行元サーバから転送したデータベースのアーカイブファイルを絶対パスで指定します。移行元から転送したデータベース情報が、/workpath オプションで指定したフォルダに格納されている場合、/file オプションは省略できます。

/type

移行する Hitachi File Services Manager および Hitachi Command Suite 製品の名称を指定します。Hitachi File Services Manager のデータベースをインポートする場合は、FileServicesManager または HF5M を指定します。

Hitachi File Services Manager のデータベースだけでなく、Hitachi Command Suite 製品のデータベースもインポートする場合は、ALL を指定するか、またはデータベースを移行する Hitachi File Services Manager および Hitachi Command Suite 製品の名称をコマンド (,) で区切って指定します。指定できる Hitachi Command Suite 製品の名称については、各製品のマニュアルを参照してください。

ALL を指定すると、移行元サーバにある Hitachi File Services Manager および Hitachi Command Suite 製品のデータベースの中から、移行先サーバにある Hitachi File Services Manager および Hitachi Command Suite 製品のデータベースが自動的に選択され、インポートされます。

Hitachi File Services Manager および Hitachi Command Suite 製品の名称を指定する場合、指定するすべての製品のデータベースが、アーカイブファイルまたは/workpath オプションに指定するフォルダにあり、かつ、指定するすべての製品が移行先サーバにインストールされていることを確認してください。この条件を満たさない製品が 1 つでもある場合、インポートは中断されます。

/auto

データベースを処理するための準備として、自動的に Hitachi Command Suite 共通コンポーネントおよび 05-70 以降の Hitachi Command Suite 製品のサービスを停止し、HiRDB を起動します。コマンド実行後には、Hitachi Command Suite 共通コンポーネントおよび 05-70 以降の Hitachi Command Suite 製品のサービスが停止された状態になります。05-70 以降の Hitachi Command Suite 製品がインストールされている場合にだけ指定できます。

/auto オプションを指定した場合でも、Device Manager に接続している Tuning Manager が、Device Manager とは別のマシンにインストールされているときには、Tuning Manager のサービスが自動的に起動および停止されません。

- エラーメッセージが出力された場合は、必ずメッセージに従って対処してください。
- 次のとおりコマンドを実行して、Hitachi File Services Manager および Hitachi Command Suite 共通コンポーネントを起動します。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %bin%hcmdssrv / start
```

- 手順 2 で停止したサービスがある場合は、起動します。
バージョン 05-70 より古い HiCommand 製品がインストールされている場合に必要手順です。サービスを起動する方法については、各製品のマニュアルを参照してください。
- 手順 1 で Tuning Manager のサービスを停止した場合は、起動します。
Hitachi Command Suite 製品がインストールされていて、そのうちの Device Manager に接続している Tuning Manager が、Device Manager とは別のマシンにインストールされている場合に必要手順です。Tuning Manager がインストールされているマシンでサービスを起動してください。

7.6.4 管理サーバのホスト名または IP アドレスを変更する

システム管理者は、管理サーバのホスト名または IP アドレスを変更する場合、事前にいくつかの設定ファイルを編集する必要があります。管理サーバをクラスタ構成で運用している場合、実行系ノードと待機系ノードで設定ファイルの情報は同一にしてください。

設定ファイルを編集する前に管理サーバのホスト名または IP アドレスを変更していた場合、hostname コマンドまたは ipconfig /ALL コマンドで変更後のホスト名または IP アドレスを表示し、記録してください。設定ファイルに指定するホスト名は、大文字と小文字の区別も含め、記録したホスト名をそのまま指定してください。

管理サーバのホスト名または IP アドレスを変更する手順を次に示します。手順では、「ホスト名または IP アドレス」のことをホスト名と略します。

- hostname コマンドまたは ipconfig /ALL コマンドを実行して、変更前のホスト名を記録します。
ホスト名の変更によって問題が発生した場合は、記録した変更前のホスト名を使用して元の状態に戻してください。

- バージョン 05-70 より古い HiCommand 製品のサービスを停止します。
バージョン 05-70 より古い HiCommand 製品がインストールされている場合に必要手順です。サービスを停止する方法については、各製品のマニュアルを参照してください。

- 次のとおりコマンドを実行して、Hitachi File Services Manager および Hitachi Command Suite 共通コンポーネントを停止します。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > \bin\hcmdssrv /stop
```

- SSL を設定している場合は、変更後のホスト名を使用して、再度 SSL を設定します。
SSL を設定する方法については、「7.5.6 SSL を設定する」を参照してください。
- 変更後のホスト名を使用して、httpsd.conf ファイルを編集します。
SSL を設定していない場合は、次の表に示す httpsd.conf ファイルにある特定の項目に、変更後のホスト名を指定してください。

表 7-38 ホスト名を変更するための項目 (SSL を設定していない場合)

ファイル名	ファイルの格納先	値を変更する項目
httpsd.conf	< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > \httpsd\conf\	ファイルの先頭にある ServerName

SSL を設定している場合は、さらに次の表に示す httpsd.conf ファイルにある特定の項目に、変更後のホスト名を指定してください。

表 7-39 ホスト名を変更するための項目 (SSL を設定している場合)

ファイル名	ファイルの格納先	値を変更する項目
httpsd.conf	< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > \httpsd\conf\	VirtualHost タグ内の次に示す項目 <ul style="list-style-type: none"> • VirtualHost • ServerName

- pdsys ファイルおよび def_pdsys ファイルを編集します。
次の表に示す pdsys ファイルおよび def_pdsys ファイルにある特定の項目の値を、ループバックアドレス (127.0.0.1) に変更します。

表 7-40 ホスト名を変更するための項目 (pdsys ファイルおよび def_pdsys ファイル)

ファイル名	ファイルの格納先	値を変更する項目
pdsys	< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > \HDB\CONF\	pdunit の-x オプション
def_pdsys	< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > \database\work\	pdunit の-x オプション

- pduatsys ファイルおよび def_pduatsys ファイルを編集します。
次の表に示す pduatsys ファイルおよび def_pduatsys ファイルにある特定の項目の値を、ループバックアドレス (127.0.0.1) に変更します。

表 7-41 ホスト名を変更するための項目 (pdutysys ファイルおよび def_pdutysys ファイル)

ファイル名	ファイルの格納先	値を変更する項目
pdutysys	< Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%HDB%CONF%	pd_hostname (ない場合は追加してください)
def_pdutysys	< Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%database%work%	pd_hostname (ない場合は追加してください)

8. HiRDB.ini ファイルを編集します。

次の表に示す HiRDB.ini ファイルにある特定の項目の値を、ループバックアドレス (127.0.0.1) に変更します。

表 7-42 ホスト名を変更するための項目 (HiRDB.ini ファイル)

ファイル名	ファイルの格納先	値を変更する項目
HiRDB.ini	< Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%HDB%CONF%emb%	PDHOST

9. 必要に応じて、変更後のホスト名を使用して、cluster.conf ファイルを編集します。

管理サーバをクラスタ構成で運用している場合に必要な操作です。

次の表に示す cluster.conf ファイルにある項目のうち、該当するものに変更後のホスト名を指定します。

表 7-43 ホスト名を変更するための項目 (cluster.conf ファイル)

ファイル名	ファイルの格納先	値を変更する項目
cluster.conf	< Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%conf%	論理ホスト名を変更した場合 virtualhost 実行系ノードのホスト名を変更した場合 onlinehost 待機系ノードのホスト名を変更した場合 standbyhost

10. 管理サーバのホスト名を変更し、マシンを再起動します。

すでに管理サーバのホスト名を変更していた場合、マシンの再起動だけを実行してください。

11. 次のとおりコマンドを実行して、Hitachi Command Suite 共通コンポーネントのサービスが稼働していることを確認します。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%bin%hcmdssrv / status
```

12. 管理サーバの URL を変更します。

管理サーバの URL を変更する方法については、Device Manager のマニュアルを参照してください。

13. 次のとおりコマンドを実行して、Hitachi File Services Manager および Hitachi Command Suite 共通コンポーネントを起動します。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%bin%hcmdssrv / start
```

14. 手順 2 で停止したサービスがある場合は、起動します。

バージョン 05-70 より古い HiCommand 製品がインストールされている場合に必要手順です。サービスを起動する方法については、各製品のマニュアルを参照してください。

7.6.5 管理サーバの時刻を調整する

ここでは、Hitachi File Services Manager をインストールしたあとで管理サーバの時刻を調整する方法について説明します。

Hitachi File Services Manager をインストールしたあとで管理サーバの時刻を調整する場合は、時刻を自動的に調整する機能を持つソフトウェアを利用してください。

NTP などで時刻を自動的に修正する機能を使用する場合、マシンの時刻が実際の時刻よりも進んだときに、マシンの時刻をさかのぼらせないで少しずつ時間を掛けて修正する機能を使用してください。機能の中には、時刻のずれ幅が一定時間内であれば少しずつ時刻を修正し、一定時間を超えると時刻をさかのぼらせて修正するものがあります。時刻のずれ幅が、少しずつ修正される範囲を超えないように、使用する機能での時刻調整の頻度を設定してください。

例えば Windows Time サービスを使用した場合、マシンの時刻が実際の時刻よりも進んだ幅が一定時間内であれば、マシンの時刻をさかのぼらせることなく少しずつ時刻を修正できます。Windows Time サービスで少しずつ時刻を修正できる範囲を確認し、マシンの時刻と実際の時刻のずれ幅がその範囲を超えないように、Windows Time サービスでの時刻の調整頻度を設定してください。

時刻を自動的に調整する機能を使用できない場合や、直ちに時刻を変更する必要がある場合、次の手順でマシンの時刻を変更してください。

- バージョン 05-70 より古い HiCommand 製品のサービスを停止します。
バージョン 05-70 より古い HiCommand 製品がインストールされている場合に必要な手順です。サービスを停止する方法については、各製品のマニュアルを参照してください。
- 次のとおりコマンドを実行して、Hitachi File Services Manager および Hitachi Command Suite 共通コンポーネントを停止します。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %bin%hcmdssrv /stop
```

- 管理サーバの時刻を変更します。
- 管理サーバのマシンを再起動します。

7.6.6 管理サーバのネットワークを切断する

NIC の変更やハブのメンテナンスなどのために管理サーバのネットワークを切断する場合は、事前に設定ファイルを編集する必要があります。

管理サーバのネットワークを切断する手順を次に示します。手順 3~5 が設定ファイルを編集する操作に当たります。手順に従って設定ファイルを一度編集すれば、以後ネットワークを切断する場合に編集する必要はありません。

- バージョン 05-70 より古い HiCommand 製品のサービスを停止します。
バージョン 05-70 より古い HiCommand 製品がインストールされている場合に必要な手順です。サービスを停止する方法については、各製品のマニュアルを参照してください。
- 次のとおりコマンドを実行して、Hitachi File Services Manager および Hitachi Command Suite 共通コンポーネントを停止します。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ > %bin%hcmdssrv /stop
```

- pdsys ファイルおよび def_pdsys ファイルを編集します。
次の表に示す pdsys ファイルおよび def_pdsys ファイルにある特定の項目の値を、ループバックアドレス (127.0.0.1) に変更します。

表 7-44 ホスト名を変更するための項目 (pdsys ファイルおよび def_pdsys ファイル)

ファイル名	ファイルの格納先	値を変更する項目
pdsys	< Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%HDB%CONF%	pdunit の-x オプション
def_pdsys	< Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%database%work%	pdunit の-x オプション

4. pdutsys ファイルおよび def_pdutsys ファイルを編集します。

次の表に示す pdutsys ファイルおよび def_pdutsys ファイルにある特定の項目の値をループバックアドレス (127.0.0.1) に変更します。

表 7-45 ホスト名を変更するための項目 (pdutsys ファイルおよび def_pdutsys ファイル)

ファイル名	ファイルの格納先	値を変更する項目
pdutsys	< Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%HDB%CONF%	pd_hostname (ない場合は追加してください)
def_pdutsys	< Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%database%work%	pd_hostname (ない場合は追加してください)

5. HiRDB.ini ファイルを編集します。

次の表に示す HiRDB.ini ファイルにある特定の項目の値をループバックアドレス (127.0.0.1) に変更します。

表 7-46 ホスト名を変更するための項目 (HiRDB.ini ファイル)

ファイル名	ファイルの格納先	値を変更する項目
HiRDB.ini	< Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%HDB%CONF%emb%	PDHOST

6. 管理サーバのマシンを再起動します。
7. 次のとおりコマンドを実行して、Hitachi File Services Manager および Hitachi Command Suite 共通コンポーネントが稼働していることを確認します。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%bin%hcmdssrv / status
```

8. 管理サーバのネットワークを切断して、設定変更やメンテナンスを実施します。
9. 管理サーバのネットワークを使用できる状態にしたあと、次のとおりコマンドを実行して、Hitachi File Services Manager および Hitachi Command Suite 共通コンポーネントを起動します。

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%bin%hcmdssrv / start
```

10. 手順 1 で停止したサービスがある場合は、起動します。

バージョン 05-70 より古い HiCommand 製品がインストールされている場合に必要手順です。サービスを起動する方法については、各製品のマニュアルを参照してください。

7.6.7 JDK を変更する

運用を開始したあと、セキュリティ脆弱性の問題などが理由で Hitachi File Services Manager で使用する JDK を変更するには、hcmdschgjdk コマンドを実行します。Oracle JDK 6 または Oracle JDK 7 に変更できます。

なお、管理サーバがノードと通信するための SSL 証明書は通常、Hitachi File Services Manager のインストールの際に自動でインポートされます。

JDK を変更した場合はキーストアも変更されるため、SSL 証明書を手動でインポートする必要があります。



重要

- 運用を開始したあと、Hitachi File Services Manager で使用する JDK として Oracle JDK を上書きまたはアップグレードインストールした場合は、hcmdschgjdk コマンドで JDK を登録し直してください。
- 運用を開始したあと、Hitachi File Services Manager で使用する JDK を Oracle JDK に変更していて、Oracle JDK をアンインストールすることになった場合は、製品に同梱されていた JDK に戻してください。
- バージョン 7.0 以前の Hitachi Command Suite 製品が管理サーバにインストールされている場合は、Oracle JDK には変更できません。

JDK を変更する手順を次に示します。

1. Hitachi File Services Manager および Hitachi Command Suite 製品のサービスを停止します。停止する方法については、「[7.3.3 Hitachi File Services Manager を停止する](#)」を参照してください。
2. 次のとおりコマンドを実行して、JDK を変更します。

```
<Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%bin%hcmdschgjdk
```

表示された画面で使用する JDK を選択します。

3. Hitachi File Services Manager および Hitachi Command Suite 製品のサービスを起動します。起動する方法については、「[7.3.2 Hitachi File Services Manager を起動する](#)」を参照してください。
4. SSL の証明書を管理サーバのキーストアファイル (jssecacerts) にインポートします。インポートすることで、SSL の証明書の格納場所が、使用する JDK の配下に切り替わります。管理サーバに SSL の証明書をインポートする方法については、「[7.5.7 管理サーバとノードの通信に必要な SSL の証明書をインポートする](#)」を参照してください。
5. Windows ファイアーウォールが有効になっている環境で、Oracle JDK に変更した場合は、Oracle JDK の java.exe ファイルを手動で例外登録します。

Advanced ACL タイプのファイルシステム への移行後に作成される ACL

Classic ACL タイプから Advanced ACL タイプのファイルシステムへの移行時に作成される ACL について説明します。

- [A.1 Advanced ACL タイプのファイルシステムへの移行後に作成される ACL](#)

A.1 Advanced ACL タイプのファイルシステムへの移行後に作成される ACL

HVFP/HDI では、Classic ACL タイプから Advanced ACL タイプのファイルシステムに移行しても、継承関係やアクセス権を継続できるように ACL を作成します。

Classic ACL タイプのファイルシステムで設定されるアクセス権は許可だけですが、継承関係やアクセス権を継続するために、移行後に作成される ACL には拒否の ACE が追加されることもあります。拒否の ACE は、アクセス権の論理和のマスク値に対して、ユーザーやグループのアクセス権のマスク値が不足している差分に応じて作成されます。例えば、あるユーザーのアクセス権が「4 (r--)」、その他 (Everyone) のアクセス権が「6 (rw-)」の場合は、ユーザーに対する「2 (-w-)」の拒否の ACE が作成されます。また、あるユーザーのアクセス権が「4 (r--)」、あるグループのアクセス権が「6 (rw-)」、その他 (Everyone) のアクセス権が「5 (r-x)」の場合は、グループとその他 (Everyone) のアクセス権の論理和のマスク値は「7 (rwx)」となり、ユーザーに対する「3 (-wx)」の拒否の ACE が作成されます。

移行前に Classic ACL タイプのファイルシステムで設定したアクセス権と、移行後に作成される許可のアクセス権との対応について、次の表に示します。

表 A-1 ファイルシステム移行前後のアクセス権の対応

移行前のアクセス権		7 (rwx)	6 (rw-)	5 (r-x)	4 (r--)	3 (-wx)	2 (-w-)	1 (--x)	0 (---)
移行後の アクセス権 (許可)	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) ○ : 許可する × : 許可しない △ : ファイルの所有者に対するアクセス権の場合は許可する

移行前のファイルシステムで、アクセス権の論理和 (OR) のマスク値に対して、ユーザーまたはグループのアクセス権のマスク値が不足している差分に応じて、移行後に拒否のアクセス権も作成されます。

マスク値は、次の式で示されます。

$$\text{マスク値} = r \times 4 + w \times 2 + x \times 1$$

(凡例)

r : 読み出し許可ビット (0 または 1)

w : 書き込み許可ビット (0 または 1)

x : 実行許可ビットまたはディレクトリサーチ許可ビット (0 または 1)

それぞれの許可ビットが 1 の場合に、アクセスが許可されます。

例えば、移行前のファイルシステムでアクセス権の論理和が「7 (rwx)」だった場合、許可ビットの r, w, x はそれぞれ 1 となるため、マスク値は次のとおりとなります。

$$\text{マスク値} = r \times 4 + w \times 2 + x \times 1$$

$$= 1 \times 4 + 1 \times 2 + 1 \times 1$$

$$= 7$$

移行前のファイルシステムで、アクセス権の論理和のマスク値に対して、ユーザーやグループのアクセス権のマスク値が不足している差分と、移行後に作成される拒否のアクセス権との対応について次の表に示します。

表 A-2 移行前のアクセス権の差分と移行後のアクセス権の対応

移行前のアクセス権の差分		7 (rwx)	6 (rw-)	5 (r-x)	4 (r--)	3 (-wx)	2 (-w-)	1 (--x)	0 (---)
移行後の アクセス権 (拒否)	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) ○ : 拒否する × : 拒否しない

ノードの Power ランプスイッチの操作方法

ここでは、保守作業時にクラスタ構成の HVFP/HDI のノードの Power ランプスイッチを操作して、OS を起動または停止する方法を説明します。

- [B.1 OS の起動](#)
- [B.2 OS の強制停止](#)

B.1 OS の起動

ノードの Power ランプスイッチを操作して電源を投入することで OS が起動します。クラスタ内の両ノードの OS を計画停止したあとに起動する場合は、片方のノードの電源を投入したあと、10 分以内にもう片方のノードの電源を投入してください。10 分を超えると、OS を停止しているノードから、OS を起動したノードにフェールオーバーが発生します。

ノードの電源の投入による OS の起動手順を次に示します。

1. ノードに接続している外部サーバが稼働していることを確認します。
2. ノードの前面の Power ランプ (Power ランプスイッチ上の LED) が消灯していることを確認します。
3. ストレージシステムと FC スイッチが稼働していることを確認します。
ストレージシステムと FC スイッチが稼働していない状態で OS を起動すると、FC パスに障害が発生します。
4. 管理 LAN 用の IP スイッチが稼働していることを確認します。
管理 LAN 用の IP スイッチが稼働していないと、ノードから管理サーバまたは管理コンソールに接続できません。
5. ノードの前面の Power ランプスイッチを押します。
6. Power ランプが点灯したことを確認します。

B.2 OS の強制停止

通常、OS の停止には GUI またはコマンドを使用します。GUI またはコマンドを使用しても Power ランプが消灯しない場合、ノードの Power ランプスイッチから OS を強制停止できます。なお、ノードの Power ランプスイッチを操作するときは、保守員の指示に従ってください。

ノードの電源の遮断による OS の強制停止手順を次に示します。

1. ノードの前面の Power ランプスイッチを 5 秒以上押し続けます。
2. Power ランプ (Power ランプスイッチ上の LED) が消灯したことを確認します。

ノード上のポートの配置

ここでは、クラスタ構成の HVFP/HDI で使用するノード上のポートの配置について説明します。

HVFP/HDI のバージョンを更新した場合は、更新前のバージョンのマニュアルを参照して、ポートの配置を確認してください。

□ C.1 ポートの配置

C.1 ポートの配置

使用しているノードの機種によって、ポートの配置が異なります。ポートの配置の例を次の図に示します。

図 C-1 ポートの配置の例 (VFP110 または VFP200N の拡張スロット 1 に GbE カードを搭載しているとき)

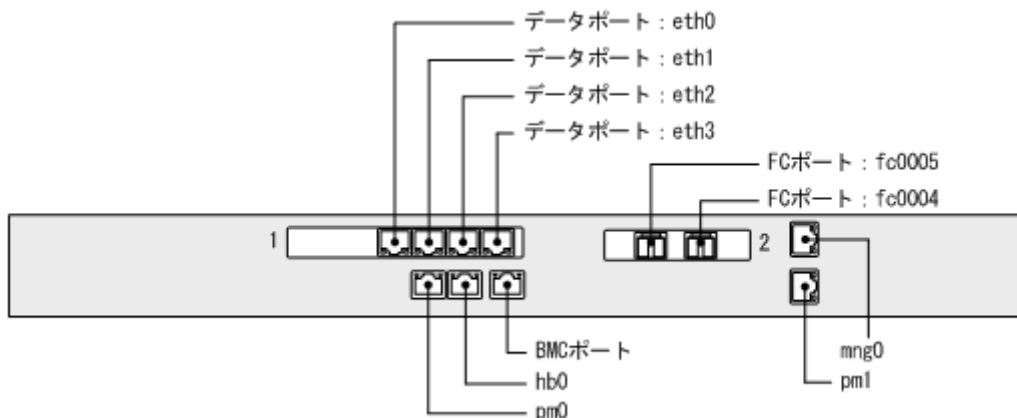


図 C-2 ポートの配置の例 (VFP110 または VFP200N の拡張スロット 1 に 10GbE カードを搭載しているとき)

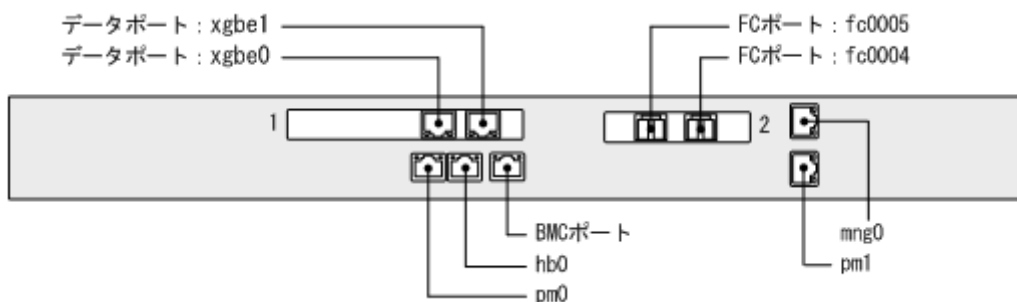


図 C-3 ポートの配置の例 (VFP600N の拡張スロット 1 と 2 に GbE カードを搭載しているとき)

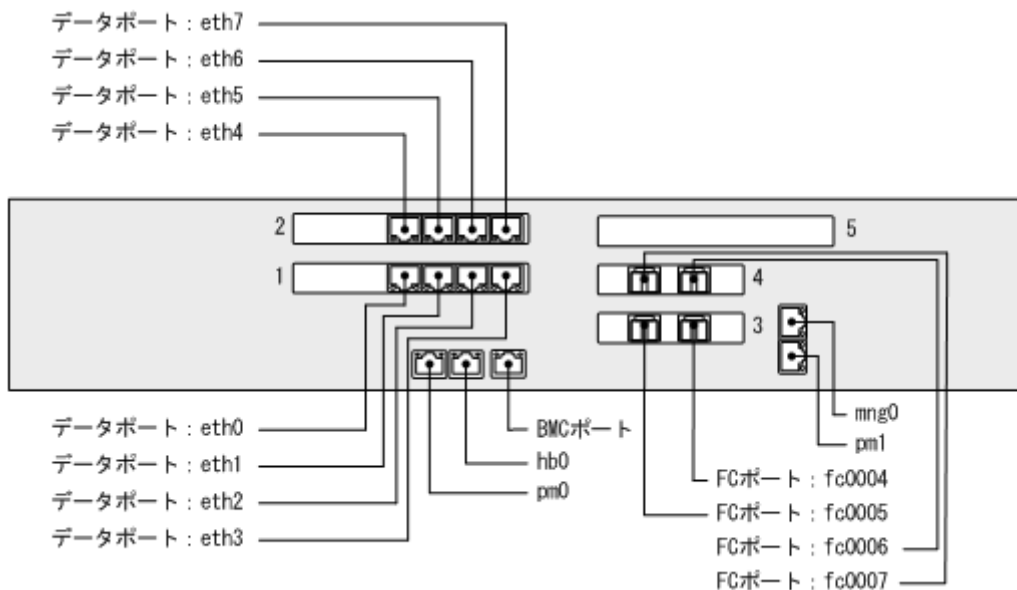
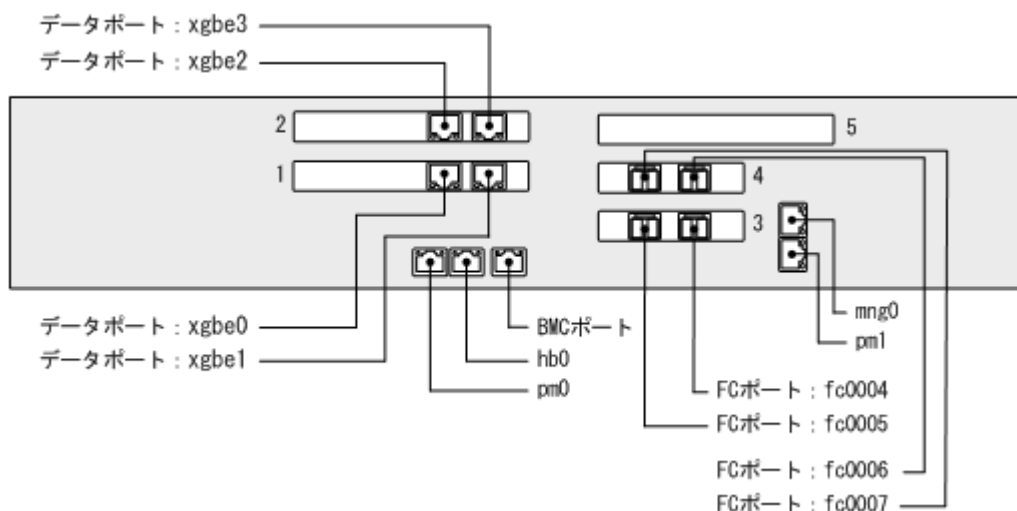


図 C-4 ポートの配置の例 (VFP600N の拡張スロット 1 と 2 に 10GbE カードを搭載しているとき)



拡張スロットには、次に示すオプションカードを搭載できます。

GbE カード

GbE のデータポート (eth <番号>) が 4 ポート配置されています。

10GbE カード

10GbE のデータポート (xgbe <番号>) が 2 ポート配置されています。

FC カード

ストレージシステムやテープ装置に接続するための FC ポートが 2 ポート配置されています。

ノードの機種ごとのポートの配置を次の表に示します。

表 C-1 ポートの配置

ノードの機種とオプションカードの組み合わせ	ポートの名称					
	オンボード	メザニンスロット	拡張スロット 1	拡張スロット 2	拡張スロット 3	拡張スロット 4
図 C-1 の場合	pm0 hb0 BMC ポート	mng0 pm1	eth0 eth1 eth2 eth3	fc0004 fc0005	使用不可	使用不可
図 C-2 の場合	pm0 hb0 BMC ポート	mng0 pm1	xgbe0 xgbe1	fc0004 fc0005	使用不可	使用不可
図 C-3 の場合	pm0 hb0 BMC ポート	mng0 pm1	eth0 eth1 eth2 eth3	eth4 eth5 eth6 eth7	fc0004 fc0005	fc0006 fc0007
図 C-3 の機種で、GbE カードを 2 枚、FC カードを 1 枚搭載する場合	pm0 hb0 BMC ポート	mng0 pm1	eth0 eth1 eth2 eth3	eth4 eth5 eth6 eth7	fc0004 fc0005	未使用
図 C-3 の機種で、GbE カードを 1 枚、FC カードを 2 枚搭載する場合	pm0 hb0 BMC ポート	mng0 pm1	eth0 eth1 eth2 eth3	未使用	fc0004 fc0005	fc0006 fc0007
図 C-3 の機種で、GbE カードと FC	pm0 hb0	mng0 pm1	eth0 eth1	未使用	fc0004 fc0005	未使用

ノードの機種とオプションカードの組み合わせ	ポートの名称					
	オンボード	メザニンスロット	拡張スロット1	拡張スロット2	拡張スロット3	拡張スロット4
カードを1枚ずつ搭載する場合	BMCポート		eth2 eth3			
☒ C-4 の場合	pm0 hb0 BMCポート	mng0 pm1	xgbe0 xgbe1	xgbe2 xgbe3	fc0004 fc0005	fc0006 fc0007
☒ C-4 の機種で、10GbE カードを2枚、FC カードを1枚搭載する場合	pm0 hb0 BMCポート	mng0 pm1	xgbe0 xgbe1	xgbe2 xgbe3	fc0004 fc0005	未使用
☒ C-4 の機種で、10GbE カードおよびGbE カードを1枚ずつ、FC カードを2枚搭載する場合	pm0 hb0 BMCポート	mng0 pm1	xgbe0 xgbe1	eth4 eth5 eth6 eth7	fc0004 fc0005	fc0006 fc0007
☒ C-4 の機種で、10GbE カード、GbE カードおよびFC カードを1枚ずつ搭載する場合	pm0 hb0 BMCポート	mng0 pm1	xgbe0 xgbe1	eth4 eth5 eth6 eth7	fc0004 fc0005	未使用
☒ C-4 の機種で、10GbE カードを1枚、FC カードを2枚搭載する場合	pm0 hb0 BMCポート	mng0 pm1	xgbe0 xgbe1	未使用	fc0004 fc0005	fc0006 fc0007
☒ C-4 の機種で、10GbE カードとFC カードを1枚ずつ搭載する場合	pm0 hb0 BMCポート	mng0 pm1	xgbe0 xgbe1	未使用	fc0004 fc0005	未使用

外部サーバやサービスの IPv6 の対応状況

HVFP/HDI では、IPv4 と IPv6 に対応しています。ここでは、HVFP/HDI の外部サーバや各サービスの IPv6 の対応状況について説明します。

□ D.1 IPv6 で利用できる外部サーバやサービスの一覧

D.1 IPv6 で利用できる外部サーバやサービスの一覧

外部サーバや HVFP/HDI が提供する各サービスの IPv6 の対応状況を次に示します。

表 D-1 外部サーバの IPv6 対応状況

種別	使用可否
管理コンソール, 管理サーバ	○
NTP サーバ	○
SNMP マネージャー	○
バックアップサーバ, メディアサーバ	×
DNS サーバ	○
NIS サーバ	×
KDC サーバ	○※1
ドメインコントローラー	○
LDAP サーバ	○
スキャンサーバ	○※2
システムログの転送先	×
SMTP サーバ	○※3
ALog マネージャーサーバ	×

(凡例) ○ : IPv6 で利用できる × : IPv6 で利用できない

注※1 : CIFS サービスの Kerberos 認証を運用する場合に利用できます。

注※2 : トレンドマイクロ社のスキャンソフトを使用する場合に利用できます。

注※3 : ホスト名を指定する場合に利用できます。

表 D-2 HVFP/HDI が提供するサービスや機能の IPv6 対応状況

種別	使用可否
NFS サービス	○※1
CIFS サービス	○
SSH サービス	○
FTP サービス	○※2
SFTP サービス	○※2
TFTP サービス	×
リアルタイムスキャン機能	○
NDMP 機能	×
Hitachi File Remote Replicator	○
HCP との連携	×
Hitachi Command Suite 製品との連携	○
ほかのファイルサーバからのインポート	○
DHCP サーバとの連携	×

(凡例) ○ : IPv6 で利用できる × : IPv6 で利用できない

注※1 : Kerberos 認証では利用できません。

注※2 : FXP は利用できません。

バックアップおよびリストア対象となるディレクトリやファイルの属性情報

NDMP 機能でメディアにバックアップされる, またはメディアからリストアされるファイルシステムの情報 (Quota 情報), ディレクトリおよびファイルの属性について説明します。

- E.1 バックアップされる属性情報
- E.2 リストアされる属性情報

E.1 バックアップされる属性情報

メディアにバックアップされる Quota 情報, ディレクトリおよびファイルの属性を表 E-1 メディアにバックアップされる Quota 情報および表 E-2 メディアにバックアップされるディレクトリおよびファイルの属性に示します。

表 E-1 メディアにバックアップされる Quota 情報

種別	属性	詳細
ファイルシステムの Quota	<ul style="list-style-type: none"> デフォルト Quota ユーザーの Quota グループの Quota 	<ul style="list-style-type: none"> ブロック使用量のソフトリミット ブロック使用量のハードリミット inode 使用量のソフトリミット inode 使用量のハードリミット
	猶予期間	<ul style="list-style-type: none"> ブロック使用量の猶予期間 inode 使用量の猶予期間
ディレクトリに設定された Quota (サブツリー Quota)	<ul style="list-style-type: none"> ディレクトリに対する Quota デフォルト Quota ユーザーの Quota グループの Quota 	<ul style="list-style-type: none"> ブロック使用量のソフトリミット ブロック使用量のハードリミット inode 使用量のソフトリミット inode 使用量のハードリミット
	猶予期間	<ul style="list-style-type: none"> ブロック使用量の猶予期間 inode 使用量の猶予期間

表 E-2 メディアにバックアップされるディレクトリおよびファイルの属性

属性	詳細	
inode	<ul style="list-style-type: none"> ファイルのパス名 ファイルのモード オーナーのユーザー ID オーナーのグループ ID 最終更新日時 (ctime) 最終編集日時 (mtime) 最終アクセス日時 (atime) ファイルの作成日時 データサイズ ファイル種別 リンクパス名 	
ACL 情報	Classic ACL	アクセス ACL <ul style="list-style-type: none"> アクセス許可 継承属性 デフォルト ACL <ul style="list-style-type: none"> アクセス許可 継承属性
	Advanced ACL	<ul style="list-style-type: none"> ユーザーまたはグループ 所属フラグ 適用先 継承範囲 ACE 種別 アクセス権
ファイル属性	Classic ACL	読み取り属性
	Advanced ACL	<ul style="list-style-type: none"> 読み取り属性 アーカイブ属性 隠しファイル属性 システムファイル属性
WORM	WORM の設定情報	
階層情報	Tier 属性	

属性	詳細
マイグレーション	<ul style="list-style-type: none"> HCP へのマイグレーションの状態 マイグレーション先の HCP 上のデータへのリファレンス

E.2 リストアされる属性情報

メディアからバックアップデータをリストアすると、ファイルシステムには、バックアップ時のデータがリストアされます。また、リストアされるデータをバックアップ時と同じ状態に戻すためには、バックアップ時と同じ状態のファイルシステムにデータをリストアする必要があります。

バックアップデータの ACL タイプとリストア先のファイルシステムの ACL タイプが異なる場合、リストア後には ACL が次のとおり設定されます。

表 E-3 ACL タイプが異なる場合のリストア結果（WORM 機能を使用していないファイルシステムのバックアップデータ）

バックアップデータ	リストア先のファイルシステム※	
	Advanced ACL タイプ	Classic ACL タイプ
Advanced ACL タイプ	バックアップ時の Advanced ACL 情報がリストアされる	ACL 情報はリストアされない
Classic ACL タイプ	バックアップ時の Classic ACL 情報が Advanced ACL 情報に変換されてリストアされる	バックアップ時の Classic ACL 情報がリストアされる

注※

WORM 機能を使用していないファイルシステムと WORM 対応ファイルシステムのどちらも指定できます。

表 E-4 ACL タイプが異なる場合のリストア結果（WORM 対応ファイルシステムのバックアップデータ）

バックアップデータ	リストア先のファイルシステム※	
	Advanced ACL タイプ	Classic ACL タイプ
Advanced ACL タイプ	バックアップ時の Advanced ACL 情報がリストアされる	リストアできない
Classic ACL タイプ	リストアできない	バックアップ時の Classic ACL 情報がリストアされる

注※

WORM 対応ファイルシステムだけをリストア先に指定できます。

システム管理者は、リストアされたデータを確認し、必要に応じて ACL の設定などを変更してください。

NFS クライアントから共有内の差分スナップショットのデータをディレクトリ単位でコピーする方法

ここでは、NFS クライアントから、ファイルシステムの共有内に公開されている差分スナップショットのデータを、ディレクトリ単位でコピーする場合の操作例を説明します。

操作例に記載しているコマンドは、操作できるファイルのサイズや所有者などについて制限されている場合があります。各コマンドの制限事項については、NFS クライアントのプラットフォームのドキュメントを参照してください。なお、手順どおりに操作できない場合は、ファイル単位でコピーしてください。

- F.1 操作例 1 ([find コマンド](#)および [cpio コマンド](#)を使用した例)
- F.2 操作例 2 ([tar コマンド](#)を使用した例)

F.1 操作例 1 (find コマンドおよび cpio コマンドを使用した例)

ここでは、find コマンドおよび cpio コマンドを使用した操作例の手順を説明します。

1. 差分スナップショット内のコピー対象のディレクトリに移動します。
2. find コマンドを実行して、コピー対象のディレクトリに含まれるファイルおよびサブディレクトリへのパスが正しく表示されることを確認します。

```
find .
```

コピー対象のディレクトリの内容と異なるパスが表示される場合は、ディレクトリ単位でのコピーはできません。

3. データをコピーします。
次のコマンドを実行してください。

```
find . | cpio -oB |(cd <コピー先の絶対パス>;cpio -idumBv)
```

<コピー先の絶対パス>には、作成元のファイルシステムのディレクトリを指定できます。

F.2 操作例 2 (tar コマンドを使用した例)

ここでは、tar コマンドを使用した操作例の手順を説明します。

1. 差分スナップショット内のコピー対象のディレクトリに移動します。
2. tar コマンドを実行して、コピー対象のディレクトリに含まれるファイルおよびサブディレクトリへのパスが正しく表示されることを確認します。

```
tar -cvf /dev/null .
```

コピー対象のディレクトリの内容と異なるパスが表示される場合は、ディレクトリ単位でのコピーはできません。

3. データをコピーします。
次のコマンドを実行してください。

```
tar -cvf - . |(cd <コピー先の絶対パス>;tar -xvf -)
```

<コピー先の絶対パス>には、作成元のファイルシステムのディレクトリを指定できます。

障害に備えて予備のシングルノード構成の HVFP を使用したシステムを構築する方法

シングルノード構成の HVFP に障害が発生した場合でも、事前に予備のシングルノード構成の HVFP を用意し、運用中の HVFP のシステム設定情報およびユーザーデータを HCP にマイグレートしておくことで、障害を回復する前に予備の HVFP でファイルシステムの運用を再開できます。シングルノード構成の HVFP に障害が発生すると、通常は障害を回復するまでファイルシステムの運用を停止しますが、障害を回復する前に予備の HVFP で運用を再開すれば、シングルノード構成の HVFP1 台での運用より、障害対策のためにファイルシステムの運用を停止する時間を短縮できます。

ここでは、障害が発生したときに予備の HVFP でファイルシステムの運用を再開できるようにシステムを構築する方法と、障害が発生したときに予備の HVFP でファイルシステムの運用を再開する方法を説明します。

- G.1 事前の準備と注意事項
- G.2 予備のシングルノード構成の HVFP を使用したシステムを構築する
- G.3 障害が発生したときに予備の HVFP で運用を再開する

G.1 事前の準備と注意事項

シングルノード構成の HVFP の障害発生によるファイルシステムの運用停止を短時間に抑えるために、システム管理者は、通常使用する HVFP と障害が発生したときに使用する予備の HVFP を用意して、システムを構築します。システムを構築する前に、次のことを確認してください。

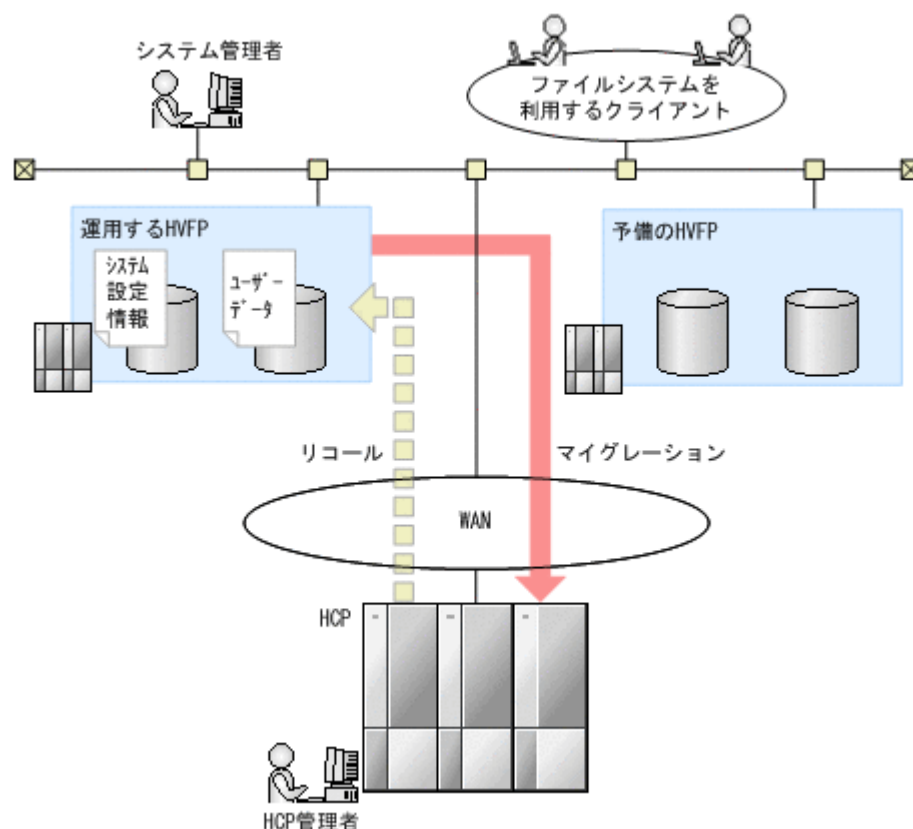
- ファイルシステムにノードの内蔵ハードディスクだけを使用する場合に、このシステムを構築できます。ストレージシステムを使用しないシングルノード構成の HVFP を用意してください。
- システムを構成するすべての HVFP は、ハードウェア構成が同じである必要があります。ノードのメモリー量、ポートの配置、ディスク容量、ドライブ種別などが同じシングルノード構成の HVFP を用意してください。
- 予備の HVFP は障害が発生したときだけに使用してください。通常時のファイルシステムの運用には使用しないでください。
- 障害が発生したときに予備の HVFP でファイルシステムの運用を再開するときには、HCP に保存されているシステム設定情報およびユーザーデータを使用します。このため、システムを構成するすべての HVFP を HCP と連携させ、運用中の HVFP のシステム設定情報ファイルが HCP に定時保存されるように、また、ファイルシステム内のすべてのファイルがマイグレーションの対象となるように設定してください。

なお、一部の情報は HCP に保存されず、HCP に保存されているシステム設定情報およびユーザーデータを予備の HVFP に回復するときに情報が引き継がれません。引き継がれない情報については、「[6.2.5 HCP にマイグレートしたデータを使用して HVFP/HDI を回復するために](#)」を参照してください。

- システムを構築するときや、HCP に保存されているシステム設定情報およびユーザーデータを予備の HVFP に回復するときに障害が発生した場合は、「[トラブルシューティングガイド](#)」を参照して、必要な対処を実施してください。

予備のシングルノード構成の HVFP を使用したシステムの構成を次の図に示します。

図 G-1 予備のシングルノード構成の HVFP を使用したシステムの構成



- ・ ファイルシステムを運用する HVFP と予備の HVFP は、同じネットワークに接続します。障害が発生したときに予備の HVFP で運用を再開する際には、mng0 に接続されている管理コンソールから作業する必要があるため、予備の HVFP は mng0 でネットワークに接続してください。

また、障害が発生した HVFP を回復する際に、管理コンソールを保守ポート (pm0) に接続して使用することがあります。管理コンソールを移動させて保守ポートに接続できるように準備してください。
- ・ 予備の HVFP には、ファイルシステムを運用する HVFP とは異なる IP アドレスやホスト名を設定します。システムを構築するときは、ファイルシステムを運用する HVFP をセットアップする際に必要な情報のほかに、予備の HVFP に設定するための次の情報も準備してください。

 - ホスト名
 - システム管理に使用する IP アドレス
 - ネットマスクまたはプレフィックス長

予備の HVFP ではファイルシステムを運用しないため、ファイルシステムやユーザー認証などに関する情報は設定しません。

シングルノード構成の HVFP のポートの配置については、「シングルノード構成セットアップガイド」を参照してください。

G.2 予備のシングルノード構成の HVFP を使用したシステムを構築する

障害が発生したときに予備の HVFP でファイルシステムの運用を再開できるように、システム管理者は、次の手順に従ってシステムを構築します。

1. システムを構成するすべての HVFP を同じネットワーク（フロントエンド LAN）に接続します。
予備の HVFP は必ず mng0 で接続してください。
IP アドレスやホスト名は、それぞれの HVFP で固有の値を設定してください。
2. 運用を開始するときに使用する HVFP の環境を設定します。
GUI でログインし、システム設定ウィザードおよびサービス設定ウィザードですべての設定を完了してください。HCP と連携し、すべてのファイルがマイグレートされるよう設定してください。
GUI で HVFP の環境を設定する手順については、「シングルノード構成セットアップガイド」を参照してください。
3. 運用を開始するときに使用する HVFP で、[Access Protocol Configuration] ダイアログを使用して SSH アカウント nasroot の公開鍵を登録します。
コマンドを使用するために公開鍵の登録が必要です。公開鍵を登録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。
4. 運用を開始するときに使用する HVFP で、-d trans オプションを指定して syslusave コマンドを実行し、システム設定情報ファイルを HCP に転送します。
5. 障害が発生したときのために用意した予備の HVFP で、ノードの基本的な設定を実施します。
GUI でログインし、システム設定ウィザードで設定を完了してください。
ウィザードの設定が完了すると、ノードの OS が再起動されたあと、ログイン画面が表示されます。
6. 予備の HVFP で、[Access Protocol Configuration] ダイアログで SSH アカウント nasroot の公開鍵を登録します。
運用を開始するときに使用する HVFP と同じ公開鍵を登録してください。
サービス設定ウィザードが起動した場合は、[キャンセル] をクリックしてください。
7. HCP との通信にプロキシサーバを使用している場合は、予備の HVFP で arcproxysset コマンドを実行してプロキシサーバの情報を設定します。
8. HCP との通信に HTTP を使用している場合は、予備の HVFP で arcsslctl コマンドを実行して通信方式を HTTP に変更します。
9. システムを構成するすべての HVFP で、pmctl コマンドを実行して保守ポート（pm0）に設定されている IP アドレスを確認し、記録します。
保守ポートの IP アドレスは障害が発生したときに必要です。HVFP ごとに記録してください。
10. 運用を開始するときに使用する HVFP で、ファイルシステムの運用を開始します。
[タスク管理] ダイアログの [ポリシーの編集] ページで、ファイルシステム内のすべてのファイルがマイグレートされるよう設定されていることを確認してください。
また、[Backup Configuration] ダイアログの [Save All System Settings] ページで、システム設定情報ファイルが HCP に定時保存されるよう設定されていることを確認してください。



重要 ノードのソフトウェアを更新する場合は、システムを構成するすべての HVFP が同じシステムバージョンになるようにしてください。

予備の HVFP のハードウェアに障害が発生した場合に備えて、通常運用時も予備の HVFP の電源を入れておくことを推奨します。また、システムを監視するために、SNMPv2 もしくは v3、または E-mail 通知を使用することを推奨します。システムを監視するために、SNMPv2 もしくは v3、または E-mail 通知を使用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。

G.3 障害が発生したときに予備の HVFP で運用を再開する

ファイルシステムを運用していた HVFP に障害が発生した場合、まず、障害の発生元と要因を特定します。障害対策の流れについては、「トラブルシューティングガイド」を参照してください。

システム管理者が対処できる障害の場合は、障害を回復してください。システム管理者が対処できない障害が発生したり、障害要因を特定できなかつたりした場合は、障害情報を収集し、保守員に連絡します。保守員に連絡したあと、次の手順に従って対処してください。

1. [List of RAS Information] ページで KAQG46040-E および KAQG46041-W を確認し、送信された SIM 障害メッセージの ID として KAQK31500-E, KAQK31530-E または KAQK31531-W が出力されていないかを確認します。

出力されている場合は、障害が発生した HVFP でファイルシステムの運用を再開します。保守員の指示に従って対処してください。

出力されていない場合は、予備の HVFP でファイルシステムの運用を再開します。次の手順に進んでください。

2. 障害が発生した HVFP の管理ポートやデータポートのケーブルを外して、ネットワークから切り離します。

ノードの電源は遮断しないでください。

3. 運用再開に使用する HVFP の電源を投入し、管理コンソールからログインします。

4. 運用再開に使用する HVFP で、`--trans --system-name` オプションを指定して `syslurestore` コマンドを実行し、障害が発生した HVFP のシステム設定情報およびユーザーデータを回復します。

`--system-name` には、障害が発生した HVFP のホスト名を指定してください。また、`syslurestore` コマンドで指定する HCP の情報や HCP との通信に使用するポートの情報を事前に準備してください。`syslurestore` コマンドで指定する情報については、「コマンドリファレンス」を参照してください。

`syslurestore` コマンドを実行したあと、ノードの OS が再起動されます。

なお、外部の機器（ルーターやほかのサーバ）の ARP キャッシュが更新されるまで、通信ができなくなる場合があります。

5. 運用再開に使用する HVFP で `pmctl` コマンドを実行し、保守ポート（`pm0`）の IP アドレスを設定します。

「G.2 予備のシングルノード構成の HVFP を使用したシステムを構築する」の手順 9 で記録しておいた HVFP ごとの IP アドレスを設定してください。

6. `eth0` と `eth1` をリンク結合して管理ポートおよびデータポートとして使用している場合は、運用再開に使用する HVFP のケーブルの接続を変更します。

a. `mng0` のケーブルを外して、ネットワークから切り離します。

b. `eth0` と `eth1` を IP スイッチに接続します。

7. 運用再開に使用する HVFP で、ファイルシステムまたはファイル共有に関するエラーメッセージが出力されていないか確認します。

ファイルシステムまたはファイル共有に関するエラーメッセージが出力されている場合は、システムの接続状態および設定を見直し、エラーメッセージに従って対処してください。対処が完了したら、ファイル共有を再作成します。

8. 運用再開に使用する HVFP で、`hcoporphanrestore` コマンドを実行し、リストアしたファイルに不整合がないか確認します。

9. 不整合があった場合は、復元されたファイルを適切な場所にコピーします。

不整合があったファイルは、次のディレクトリに復元されます。

```
/mnt/<ファイルシステム名>/.lost+found/
```

10. システム設定情報およびユーザーデータを回復させた HVFP でファイルシステムの運用を再開します。

次の作業を実施してください。

 - [タスク管理] ダイアログの [ポリシーの編集] ページで、ファイルシステム内のすべてのファイルがマイグレートされるよう設定されていることを確認してください。

また、[Backup Configuration] ダイアログの [Save All System Settings] ページで、システム設定情報ファイルが HCP に定時保存されるよう設定されていることを確認してください。
 - NFS クライアントにファイル共有を再度マウントするよう依頼してください。
 - NDMP サーバを使用している場合、NDMP サーバのパスワードが初期化されます。不正なアクセスを防止するため、パスワードを変更してください。
 - ファイルシステムが正しく運用できることを確認してください。ファイルシステムが正しく運用できない場合は、ファイルシステムに関する一部の情報が HCP に保存されていないか、おそれがあります。HCP に保存されない情報については、「[6.2.5 HCP にマイグレートしたデータを使用して HVFP/HDI を回復するために](#)」を参照してください。
11. 保守員と連携して、障害が発生した HVFP の障害を回復します。
12. 障害が発生した HVFP で、システムの初期セットアップを実施した場合は、次の作業を実施します。
 - a. ノードの基本的な設定を実施します。

GUI でログインし、システム設定ウィザードで設定を完了してください。
予備の HVFP に使用する IP アドレスを設定してください。
 - b. [Access Protocol Configuration] ダイアログで SSH アカウント `nasroot` の公開鍵を登録します。
 - c. HCP との通信にプロキシサーバを使用している場合は、`arcproxysset` コマンドでプロキシサーバの情報を設定します。
 - d. HCP との通信に HTTP を使用している場合は、`arcsslctl` コマンドで通信方式を HTTP に変更します。
 - e. `pmctl` コマンドで保守ポート (`pm0`) に設定されている IP アドレスを確認し、記録します。
13. 障害が発生した HVFP で、システムの初期セットアップを実施しなかった場合は、次の作業を実施します。
 - a. 保守ポート (`pm0`) に管理コンソールを接続します。
 - b. `singleinit` コマンドで、システム設定情報やユーザーデータなどを削除し、システムを初期化します。

予備の HVFP に使用する IP アドレスを設定してください。
システムを初期化したあと、ノードの OS が再起動されます。
 - c. 保守ポートと管理コンソールとの接続を解除します。
14. 障害を回復した HVFP をネットワークに接続します。

障害を回復した HVFP は、障害が発生したときのために予備の HVFP として待機させます。`eth0` と `eth1` をリンク結合して管理ポートおよびデータポートとして使用する場合でも必ず `mng0` で接続してください。



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](#)

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
DAACL	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
DHCP	Dynamic Host Configuration Protocol
DIMM	dual in-line memory module
DLL	dynamic-link library
DN	distinguished name
DNS	Domain Name System
DOM	Document Object Model
DOS	Disk Operating System
DRAM	dynamic random access memory
DSA	digital signal algorithm

DTD	Document Type Definition
ECC	error-correcting code
EUC	Extended UNIX Code
FC	Fibre Channel
FC-SP	Fibre Channel - Security Protocol
FIB	forwarding information base
FIFO	First In, First Out
FQDN	fully qualified domain name
FTP	File Transfer Protocol
FV	Fixed Volume
FXP	File Exchange Protocol
GbE	Gigabit Ethernet
GID	group identifier
GMT	Greenwich Mean Time
GPL	GNU General Public License
GUI	graphical user interface
HBA	host bus adapter
H-LUN	host logical unit number
HPFS	High Performance File System
HSSO	HiCommand single sign-on
HTML	HyperText Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
I/O	input/output
ICAP	Internet Content Adaptation Protocol
ICMP	Internet Control Message Protocol
ID	identifier
IP	Internet Protocol
IP-SW	IP switch
JDK	Java Development Kit
JIS	Japanese Industrial Standards
JSP	JavaServer Pages
KDC	Key Distribution Center
LACP	Link Aggregation Control Protocol
LAN	local area network
LBA	logical block addressing
LCD	Local Configuration Datastore
LDAP	Lightweight Directory Access Protocol
LDEV	logical device
LDIF	LDAP Data Interchange Format
LDKC	logical disk controller
LED	light-emitting diode
LF	Line Feed
LTS	long term support

LU	logical unit
LUN	logical unit number
LUSE	logical unit size expansion
LVI	Logical Volume Image
LVM	Logical Volume Manager
MAC	Media Access Control
MD5	Message-Digest algorithm 5
MIB	management information base
MMC	Microsoft Management Console
MP	microprocessor
MSS	maximum segment size
MTU	maximum transmission unit
NAS	Network-Attached Storage
NAT	network address translation
NDMP	Network Data Management Protocol
NetBIOS	Network Basic Input/Output System
NFS	Network File System
NIC	network interface card
NIS	Network Information Service
NTFS	New Technology File System
NTP	Network Time Protocol
OID	object identifier
ORB	object request broker
OS	operating system
PAP	Password Authentication Protocol
PC	personal computer
PCI	Peripheral Component Interconnect
PDC	Primary Domain Controller
PDU	protocol data unit
PID	process identifier
POSIX	Portable Operating System Interface for UNIX
PP	program product
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
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

用語解説

ここでは、HVFP/HDI のマニュアルで使用している用語の意味を解説します。

(英字)

ACE

ACL を構成するエントリーです。ディレクトリやファイルに対するアクセス権をユーザーやグループごとに設定します。ACL タイプによって形式が異なります。

ACL

ACE の集まりです。ディレクトリやファイルに対するアクセス権を定義します。

ACL タイプ

使用できる ACL に対応した、ファイルシステムやファイルの種類です。HVFP/HDI で使用できる ACL タイプには、NTFS ACL に準拠した Advanced ACL タイプと POSIX ACL に準拠した Classic ACL タイプがあります。

Anti-Virus Enabler

HVFP/HDI でユーザーに CIFS 共有されているデータのリアルタイムスキャンを実行するためのプログラムです。

Backup Restore

HVFP/HDI で運用されているファイルシステムのデータのバックアップを取得するためのプログラムです。

CIFS

Windows ユーザー向けにファイル共有サービスを提供するためのプロトコルです。

Configuration Manager

HVFP/HDI を効率的にセットアップし、ファイルシステムの運用を管理するためのプログラムです。

Data Control

ノード上の OS を構成するプログラムの一つです。

Device Manager

ストレージシステムのディスクリソースやハードウェア構成を統合管理するためのプログラムです。

Dynamic Provisioning

ストレージシステムの物理容量に依存しない任意の容量のボリュームを仮想的にホストに割り当てる機能です。

Dynamic Tiering

I/O 負荷に応じてデータを自動的に再配置するストレージシステムの機能です。

File Sharing

ノード上の OS を構成するプログラムの一つです。

HBase Storage Mgmt Common Service

Hitachi Command Suite 共通コンポーネントの Web コンテナのサービスです。

HBase Storage Mgmt Web Service

Hitachi Command Suite 共通コンポーネントの WWW サーバのサービスです。

Hitachi Command Suite 共通コンポーネント

Hitachi File Services Manager および Hitachi Command Suite 製品で共通する機能を提供するコンポーネントです。GUI へのログイン、管理サーバの統合ログ出力、Web サービスなどの機能を提供します。

Hitachi Content Platform (HCP)

データを長期保存および管理するためのシステムです。HVFP/HDI で作成したファイルシステムのデータを HCP にマイグレートできます。

Hitachi File Remote Replicator

ファイルスナップショット機能と連携し、あるサイトで作成された差分スナップショットのデータを TCP/IP 経由で別のサイトに遠隔バックアップし、差分スナップショットを複製するプログラムです。

Hitachi File Services Manager

システム管理者が GUI を利用して HVFP/HDI を運用または管理するために必要なプログラムです。

Hitachi Virtual File Platform (HVFP)

ストレージシステムとノードを使用して、ファイル共有サービスを提供するシステムのことで。

LDEV

ストレージシステムのパリティグループ内の記憶領域を論理的に分割して作成される記憶領域です。File Services Manager では「LDEV」と呼ばれますが、Hitachi AMS2000 シリーズまたは HUS100 シリーズでは、「ロジカルユニット (LU)」と呼ばれます。

LU

ストレージシステムのポートに割り当てられた LDEV のことを指します。

LUN

ストレージシステム内の LU に付与される管理番号です。File Services Manager では「LUN」と呼ばれますが、Hitachi AMS2000 シリーズまたは HUS100 シリーズでは「H-LUN」と呼ばれます。

LUN Expansion

複数の LU を 1 つにまとめて、LU の容量を拡張する機能です。

LVM

ボリュームマネージャーの一つです。説明は「ボリュームマネージャー」を参照してください。

NFS

UNIX ユーザー向けにファイル共有サービスを提供するためのプロトコルです。

OS ディスク

OS および OS 上で動作するプログラムが格納される、ノード内の論理的なディスク領域です。

Physical Node

Processing Node を構成する個々のノードのことです。

Primary Server Base

WWW サーバ機能を提供するプログラムです。

Processing Node

ノードで構成される論理的なグループです。ノードをクラスタ構成にしている場合は、クラスタが Processing Node として扱われます。

Quota

ユーザーが使用できるブロック容量や inode 数の制限のことです。HVFP/HDI では、ファイルシステムごと、またはディレクトリごとに設定・管理します。

ShadowImage

ストレージシステム内に、ホストを経由しないでユーザーデータを複製するプログラムです。

TrueCopy

2 台のストレージシステム間で、ホストを経由しないでユーザーデータを複製するプログラムです。

Universal Replicator

2 台のストレージシステム間で、ホストを経由しないで非同期にユーザーデータを複製するプログラムです。

Virtual Server

ノード上に作成できる仮想のファイルサーバ環境です。また、仮想ファイルサーバの複数のリソースを 1 つのグループとして管理する単位を指すこともあります。

WORM

「Write Once, Read Many」の略称で、データが変更できない状態のことです。WORM 化されたファイルを WORM ファイルと呼び、任意のファイルを WORM 化できるファイルシステムを WORM 対応ファイルシステムと呼びます。

(ア行)

インクリメンタルバックアップ

前回のバックアップ以降に内容が変更されたデータを対象とするバックアップ方法です。

(カ行)

外部ストレージシステム

ストレージシステムの外部ストレージ接続機能 (Universal Volume Manager) で接続されたストレージシステムです。

仮想 IP アドレス

リソースグループまたは Virtual Server で稼働しているサービスに接続するときにユーザーが使用する IP アドレスです。仮想 IP アドレスを使用することで、ノードに障害が発生した場合にリソースグループまたは Virtual Server がもう一方の正常稼働しているノードにフェールオーバーしても、ユーザーは継続してサービスを利用できます。

管理 LAN

システム管理者が HVFP/HDI を運用および管理するときに使用する LAN です。

管理コンソール

システム管理者が File Services Manager を操作するために使用するマシンです。

管理サーバ

Hitachi File Services Manager がインストールされたマシンです。管理コンソールとしても使用できます。

共有 LU

ノードに割り当てられた LU のうち、クラスタ構成やファイルシステムなどに関する設定情報が格納される LU のことです。

クラスタ

障害が発生したり、保守作業したりするときのサービスの継続を目的とした冗長構成のことです。

コマンドデバイス

ストレージシステムを制御するコマンドを受け付けるための制御デバイスのことです。

固有 IP アドレス

ノードのインターフェースごとに設定する IP アドレスです。

(サ行)

サブツリー Quota

ディレクトリや、そのディレクトリを利用するユーザーまたはグループに対して設定する Quota です。

差分格納デバイス

差分スナップショットで使用する更新前のファイルシステムのデータを保存しておくための、ストレージシステム内のボリュームです。

差分スナップショット

ファイルスナップショット機能で、ファイルシステムのデータと差分格納デバイスに退避されたデータを使用して、過去のファイルシステムの状態を再現した仮想ボリュームです。

システム LU

OS ディスクと共有 LU の総称です。

システム管理者

HVFP/HDI の運用を管理するユーザーです。システム管理者は、システムをセットアップしたり、システムの稼働状況や障害を監視したりします。

スキャンサーバ

HVFP/HDI で CIFS 共有されているデータのウイルススキャンを LAN 経由で実行するサーバです。

(タ行)

ターゲット

ノードがストレージシステムの LU を一意に識別できるように、複数の LU を 1 つのグループとして管理する単位です。

データポート

フロントエンド LAN に接続するためのノードのポートです。

テープ装置

複数のメディアを収納した装置です。

デバイスファイル

ユーザー LU のことです。説明は「ユーザー LU」を参照してください。

(十行)

ノード

ファイルサーバとして利用するために、ストレージシステムに接続された装置です。2つのノードでクラスタを構成します。

(八行)

ハートビート LAN

クラスタを構成する各ノードが、相互の稼働状況を確認するために使用する LAN です。

バックアップサーバ

バックアップ管理ソフトウェアを使用して、バックアップおよびリストアを管理するサーバです。

ファイルスナップショット機能

HVFP/HDI で運用されているファイルシステムの差分スナップショットを作成するためのプログラムです。

フェールオーバー

ノードで障害が発生したり、保守作業をしたりするときに、HVFP/HDI が提供するサービスを停止しないで運用するために、クラスタ内の別のノードにリソースグループまたは Virtual Server を移すことです。

フェールバック

ノードで発生した障害を回復したり、保守作業が完了したりしてから、クラスタ内の別のノードにフェールオーバーしていたリソースグループまたは Virtual Server を元のノードに戻すことです。

フロントエンド LAN

クライアントがストレージシステム内に格納されたデータにアクセスするときに使用する LAN です。

保守員

HVFP の保守を行う弊社の技術者です。

ボリュームグループ

ボリュームマネージャーを使用して、複数の LU を統合した領域です。1つの LU で構成することもできます。通常のファイルシステムでは、1つのファイルシステムでボリュームグループが構成されます。ファイルスナップショット機能が設定されているファイルシステムでは、ファイルシステム、差分格納デバイスおよび差分スナップショットでボリュームグループが構成されます。

ボリュームマネージャー

ボリュームを管理する機能です。HVFP/HDI では、ボリュームマネージャーとして LVM を使用します。ボリュームマネージャーを使用することで、LU を統合してボリュームグループを作成したり、ボリュームグループを利用して論理ボリュームを作成したりできます。

(マ行)

メディア

バックアップしたデータを格納する磁気テープなどの記録媒体のことです。

メディアサーバ

ストレージシステム外に設置したテープ装置を制御するためのサーバです。

(ヤ行)

ユーザー LU

ノードに割り当てられた LU のうち、ファイルシステムなどユーザーデータを格納するための LU の総称です。「デバイスファイル」または「LU (システム LU を除く)」と呼ばれることもあります。

ユーザー LUN

ユーザー LU に付与される管理番号です。「デバイスファイル番号」と呼ばれることもあります。

ユーザーマッピング

ドメインコントローラーに登録されているユーザーが CIFS 共有にアクセスした際に、ユーザー ID およびグループ ID を割り当てる機能です。

(ラ行)

リソースグループ

複数のリソース (NFS 共有設定, CIFS 共有設定, ファイルシステムの情報, 仮想 IP アドレスの情報など) を 1 つのグループとして管理する単位です。リソースグループごとにサービスを起動, 停止できます。また, 障害発生時にはリソースグループごとにフェールオーバーします。

リンク結合

複数のポートをグループ化して仮想的に 1 つのネットワークインターフェースを構成できる技術です。HVFP/HDI では, リンク結合によって設定した仮想的なネットワークインターフェースを使用してネットワークが構築できます。

論理ボリューム

ボリュームマネージャーを使用して, ボリュームグループを 1 つまたは複数に分割した領域です。HVFP/HDI では, ボリュームマネージャーを使用して構築されたファイルシステムや差分格納デバイス, 差分スナップショットが該当します。

索引

記号

- .snaps ディレクトリ 223
 - コピー方法 (NFS クライアント) 229
 - 参照方法 228
- /etc/hosts ファイル 184

A

- account.lock.num 298
- account.lock.system 299
- ACE 395
- ACL 395
- ACL タイプ 122, 395
- Advanced ACL タイプ
 - 移行 125
- Anti-Virus Enabler 395

B

- Backup Restore 395

C

- CIFS 395
- CIFS アクセスログ 149
- CIFS 共有
 - CIFS アクセスログ 149
 - MMC 連携 149
 - 運用を開始する前に 147
 - 作成する前に 148
 - ネットワーク構成 48
 - ホームドライブの設定 148
- CIFS クライアント
 - ファイルシステムを利用するときの注意事項 174
- CIFS 走査チェックのバイパス 135
- Classic ACL タイプ
 - ACL の設定 149

- Configuration Manager 395

D

- DACL 124
- Data Control 395
- Device Manager 40, 395
- DHCP サーバ 43
 - 環境設定 97
- DNS サーバ 41
 - 環境設定 98
- Dynamic Provisioning 395
- Dynamic Tiering 396

F

- File Sharing 396
- Firefox
 - 設定 76
- FTP クライアント
 - ファイルシステムを利用するときの注意事項 174
- FTP サーバ 42

H

- HBase Storage Mgmt Common Service 396
- HBase Storage Mgmt Web Service 396
- HCP 35, 396
- HFRR ペア 235
- Hitachi Command Suite 共通コンポーネント 41, 396
- Hitachi Content Platform 35, 396
- Hitachi File Remote Replicator 232, 396
 - 運用上の注意事項 243
 - 運用設計 239
 - 使用上の注意事項 239
- Hitachi File Services Manage

インストール (管理サーバをクラスタ構成で運用する場合) 279

Hitachi File Services Manager 40, 396

- アンインストール 266
- アンインストール (管理サーバをクラスタ構成で運用する場合) 279
- インストール 266
- インストール時の前提条件 277
- 環境設定 333
- 起動 292
- 停止 292

Hitachi Storage Navigator Modular 2 41

Hitachi Virtual File Platform 32, 396

- 概要 32

hnasm.common.logger.loglevel 334

hnasm.common.logger.maxfilenumber 334

hnasm.common.logger.maxfilesize 334

hnasm.common.logger.syslog.loglevel 334

hnasm.model.refresh.screen.license 337

hnasm.model.refresh.tab.sync 336

hnasm.model.deletevnas.mode 335

HVFP 32, 396

- システム構成 39
- ネットワーク構成 44
- ハードウェア構成 40

I

Internet Explorer

- 設定 74

K

KDC サーバ 41

- 環境設定 88

L

LDAP サーバ 42

- 環境設定 78
- 注意事項 79

LDEV 396

LU 396

- 作成 114

LUN 396

LUN Expansion 396

LVM 396

M

MMC 連携 149

N

NDMP 機能

- 運用について 178
- オフラインバックアップ 180
- オンラインバックアップ 180
- 概要 179
- 機能制限 186
- 実施時間 182
- 対象データ 182

NDMP サーバ

- アクセス制限 184

NFS 396

NFS 共有

- 運用を開始する前に 147

NFS クライアント

- ファイルシステムを利用するときの注意事項 173

NIS サーバ 41

- 環境設定 78

NTP サーバ 41

- 環境設定 91

O

OS

- 起動 370
- 強制停止 370

OS ディスク 166, 396

P

password.check.userID 297

password.min.length 297

password.min.lowercase 297

password.min.numeric 297

password.min.symbol 297

password.min.uppercase 297

Physical Node 397

Power ランプ 370

Power ランプスイッチ 370

- 操作方法 369

Primary Server Base 397

Processing Node 397

Q

Quota 397

- 運用を開始する前に 136
- サブツリー Quota の管理 143
- 設定情報 137
- ソフトリミット 138
- 注意事項 144

ハードリミット 138
ファイルシステムごとの Quota の管理 142
猶予期間 138

R

RADIUS サーバ 42
環境設定 89
RID 107

S

ShadowImage 397
SID 104
SMTP サーバ 42
環境設定 97
SNMP マネージャー 41
環境設定 89
stdCoreTrap 90
stdEventTrapError 90
stdEventTrapFatalError 90
stdEventTrapInformation 90
stdEventTrapWarning 90
stdQuotaTrapFSDetailSuppress 90
stdQuotaTrapFSLimitExceeded 90
stdQuotaTrapFSSoftLimit 90
stdQuotaTrapFSSubtreeDetailSuppress 90
stdQuotaTrapFSSubtreeLimitExceeded 90
stdQuotaTrapFSSubtreeSoftLimit 90
stdQuotaTrapFSSubtreeSummary 90
stdQuotaTrapFSSummary 90
stdTrapNotice 90
Storage Navigator 40

T

TrueCopy 397

U

Universal Replicator 397
user.conf 298
user.properties
ファイルスナップショット機能の情報更新の設定 336
ライセンスの情報更新の設定 336
ログファイルの設定 333

V

Virtual Server 34, 397
障害情報 167

Virtual Server OS LU 166
VLAN
ネットワーク構成 58
リンク結合を併用したネットワーク構成 60
VLAN ID 59

W

WINS サーバ 41
WORM 397
WORM 対応ファイルシステム 130
注意事項 132
WORM ファイル 130
WWW ブラウザー
管理コンソール 73

あ

アクセス ACL 149
あふれ時の動作 220
あふれ防止動作 219
暗号化
注意事項 116

い

移行
管理サーバの構成 349
管理サーバのデータベース 355
インクリメンタルバックアップ 182, 397
インポート
インポートする前に 168
システム構成 169
注意事項 171

う

運用上の注意事項 100
運用方法の検討
差分スナップショット (クラスタ構成の場合) 199
差分スナップショット (シングルノード構成の場合)
203
運用例
開始 205
完了後の作業 209
クライアント側での操作 206
差分スナップショット 199
システム構成 199
システム構成 (シングルノード構成の場合) 203
状況の監視 208
テスト 204

お

- オフラインバックアップ 180
- オンラインバックアップ 180

か

解除

- システム管理者のアカウントのロック 299
- テープドライブ 96

階層構造モデル 301

階層ファイルシステム 132

- 注意事項 134

外部サーバ 40, 43

外部ストレージシステム 397

外部認可サーバ 295

外部認証サーバ 295

概要

- NDMP 機能 179

- ファイルスナップショット機能 189

仮想 IP アドレス 397

環境設定

- DHCP サーバ 97

- DNS サーバ 98

- KDC サーバ 88

- LDAP サーバ 78

- NIS サーバ 78

- NTP サーバ 91

- RADIUS サーバ 89

- SMTP サーバ 97

- SNMP マネージャ 89

- 管理コンソール 72

- 管理サーバ 67

- スキャンサーバ 92

- ドメインコントローラー 87

- ノードに SAN で接続されたテープ装置 95

管理 LAN 44, 397

管理コンソール 40, 398

- Firefox 76

- Internet Explorer 74

- 環境設定 72

- マシン要件 72

管理サーバ 40, 398

- IP アドレスの変更 359

- 環境設定 67

- 管理者権限でコマンドを実行する 71

- クラスタ構成 70

- 構成の移行 349

- 時刻の調整 362

- 障害情報 167

- データベースの移行 355

- データベースのバックアップ 345

- データベースのリストア 345

- ネットワークの切断 362

- ホスト名の変更 359

- マシン要件 67

- メンテナンス 345

き

- キャッシュ常駐 250

- 共有 LU 166, 398

く

クライアント側での操作

- 運用例 206

- クラスタ 398

け

- 警告閾値 219

検討

- Quota 136

- ファイル共有 147

- ファイルシステム 113

- ユーザーマッピング 104

- リアルタイムスキャン 152

こ

公開

- 自動作成スケジュールで Volume Shadow Copy Service を使用して公開する動作 224

- 自動作成スケジュールで共有内に公開する動作 223

- 自動作成スケジュールでファイル共有を作成する動作 223

- 個別通知モード 139

- コマンドデバイス 398

- 固有 IP アドレス 398

さ

- サブツリー Quota 136, 398

- 差分格納デバイス 189, 398

- HCP と連携しない場合の見積もり式 211

- HCP と連携しない場合の見積もり例 216

- HCP と連携する場合の見積もり式 212

- HCP と連携する場合の見積もり例 217

- 階層ファイルシステムの場合の見積もり式 213

- 使用量に関する設定 218

- 容量の設計 210

- 差分コピー 237

- 差分スナップショット 189, 398

運用方法の検討（シングルノード構成の場合） 203
運用例 199
設定（シングルノード構成の場合） 203
差分スナップショットの自動作成 221
差分データ 189
差分バックアップ 182
サマリー通知モード 139

し

時刻

調整〔管理サーバ〕 362
システム LU 166, 398
システム管理者 398
アカウントのロックの解除 299
システム構成 39
HCP 連携 62
運用例 199
運用例（シングルノード構成の場合） 203
ほかのファイルサーバからのインポート 169
システム設定情報 166
システム設定情報ファイル 166
実行系ノード 70
自動作成スケジュール
公開の動作 222
作成の動作 222
注意事項 226
マウントの動作 222
障害情報
Virtual Server 167
管理サーバ 167
ノード 167

す

スキャンサーバ 42, 398
環境設定 92
スタブファイル 249
ストライピング機能 120
スナップショット 189

せ

セカンダリーサイト 235
セカンダリーファイルシステム 235
設計
差分格納デバイスの容量 210
設定
差分格納デバイス 181
差分スナップショット（クラスタ構成の場合） 199
差分スナップショット（シングルノード構成の場合）
203

全コピー 237
前提条件
差分格納デバイスを構成するデバイスファイル 215
ファイルスナップショット機能 189

そ

増分バックアップ 182
ソフトリミット 138

た

ターゲット 398
待機系ノード 70

ち

注意事項

HCP と連携する場合 199
Hitachi File Remote Replicator 199
LDAP サーバ 79
暗号化 116
階層ファイルシステム 134
自動作成スケジュールで運用する場合 226
シングルノード構成で運用する場合 199
同時に実行できない操作 198
ほかのファイルサーバからのインポート 171
ボリュームレプリケーション連携機能 198

て

データポート 398
テープ装置 43, 399
環境設定 95
テープドライブ
解除 96
登録 95
デバイスファイル 399
デフォルト ACL 149

と

動作閾値 219
登録
テープドライブ 95
ドメインコントローラー 42
環境設定 87

に

認可グループ 295

ね

- ネットワーク構成 44
 - CIFS 共有を利用する場合 48
 - VLAN 58
 - VLAN とリンク結合を併用する場合 60
 - リンク結合 53

の

- ノード 32, 399
 - 障害情報 167

は

- バージョン管理 251
- ハードウェア構成 40
- ハートビート LAN 399
- ハードリミット 138
- バックアップ
 - 管理サーバのデータベース 345
- バックアップ運用
 - 概要 178
- バックアップサーバ 43, 399
- バックグラウンド処理 197

ひ

- 日立固有 MIB オブジェクト
 - 定義ファイルの取得方法 90

ふ

- ファイル共有
 - 運用を開始する前に 147
- ファイルシステム
 - ACL タイプ 122
 - Advanced ACL タイプへの移行 125
 - CIFS 走査チェックのバイパス 135
 - LU の作成 114
 - 運用を開始する前に 113
 - 階層ファイルシステムの運用 132
 - ストライピング機能 120
 - 複数ファイルのデータ集約による容量節約 134
 - ボリュームグループの作成 114
- ファイルシステムの拡張 220
- ファイルスナップショット機能 399
 - 運用 188
 - 概要 189
 - 最大予約世代数 190
 - 処理時間 197
 - 予約世代数 193

- ファイルバージョンリストア機能 251
 - 過去バージョンディレクトリ 251
- フェールオーバー 399
- フェールバック 399
- プライマリーサイト 235
- プライマリーファイルシステム 235
- フラットモデル 302
- プロキシサーバ 42
- フロントエンド LAN 44, 399

へ

- ベースライン差分スナップショット 238
- 変更
 - 管理サーバの IP アドレス 359
 - 管理サーバのホスト名 359

ほ

- ホームディレクトリローミング機能 258
- ホームドライブ
 - 設定 148
- 保守員 399
- ボリュームグループ 113, 399
 - 作成 114
- ボリュームマネージャー 399

ま

- マスク 149

み

- 見積もり
 - バックアップメディアの容量 180
- 見積もり式
 - HCP と連携しない場合の差分格納デバイス 211
 - HCP と連携する場合の差分格納デバイス 212
 - 階層ファイルシステムの場合の差分格納デバイス 213
- 見積もり例
 - HCP と連携しない場合の差分格納デバイス 216
 - HCP と連携する場合の差分格納デバイス 217

め

- メディア 400
 - 容量の見積もり 180
- メディアサーバ 43, 400
- メンテナンス
 - 管理サーバ 345
 - テープ装置の交換 96

ゆ

- ユーザー LU 400
- ユーザー LUN 400
- ユーザーマッピング 104, 400
 - 運用を開始する前に 104
 - ドメインの範囲 104
 - 方式 107
 - 方式の変更 108
- 猶予期間 138

よ

- 用語解説 395

ら

- ライセンス 60

り

- リアルタイムスキャン
 - 運用時の注意事項 153
 - 運用設計 156
 - 運用を開始する前に 152
 - スキャンサーバ登録時の注意事項 156
 - スキャン条件の見直し 164
- リコール 250
- リストア
 - 管理サーバのデータベース 345
- リソースグループ 400
- リテンション期間 130
- リンク結合 400
 - VLAN を併用したネットワーク構成 60
 - ネットワーク構成 53
- リンク交代 53
- リンク集約 53

れ

- 連携
 - ALog ConVerter 149

ろ

- ローカルデータの暗号化 116
- 論理ボリューム 400

