

Hitachi Virtual File Platform

トラブルシューティングガイド

対象製品

Hitachi Virtual File Platform
4.2.2-00 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。

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。

gzip は、米国 FSF(Free Software Foundation)が配布しているソフトウェアです。

InstallShield は、Macrovision Corporation の米国および/または他の国における登録商標または商標です。

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。

Microsoft, Windows, Windows NT および 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。

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.

PuTTY は、Simon Tatham 氏が提供するオープンソースソフトウェア (フリーソフトウェア)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。

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。

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。



発行

2014年3月（第14版）K6603760

著作権

All Rights Reserved. Copyright (C) 2012, 2014, Hitachi, Ltd.

目次

はじめに.....	15
対象読者.....	16
マニュアルの構成.....	16
マニュアル体系.....	16
関連マニュアル.....	17
このマニュアルでの表記.....	18
このマニュアルで使用する記号.....	19
このマニュアルで使用する構文要素.....	19
コマンドの書式で使用する記号.....	19
KB（キロバイト）などの単位表記について.....	20
1. 障害対策の流れ.....	21
1.1 障害対策の概要.....	22
1.2 ファイルシステムを利用できない場合.....	24
1.3 File Services Manager の GUI が正常に動作しない場合.....	26
1.4 Backup Restore ・ ファイルスナップショット ・ Hitachi File Remote Replicator の機能がエラー終了した場合.....	28
2. 障害要因の特定.....	29
2.1 GUI または標準エラー出力に表示されたエラーメッセージを確認する.....	31
2.2 ノード上のシステムメッセージを確認する.....	31
2.3 クラスタおよびノードの状態を確認する.....	32
2.3.1 OS が起動したときに発生した障害の特定.....	33
2.3.2 クラスタを操作しているときに発生した障害の特定.....	34
2.3.3 サービスを利用できない場合の障害の特定.....	35
2.4 リソースグループまたは Virtual Server の状態を確認する.....	35
2.4.1 Virtual Server の起動処理中または停止処理中に発生した障害の特定.....	38
2.4.2 フェールオーバーする契機となった障害の特定.....	39
2.4.3 フェールオーバーが失敗したときの障害の特定.....	39
2.5 ファイルシステムのエラー状態を確認する.....	40
2.6 差分格納デバイスのエラー状態を確認する.....	41
2.7 ユーザーマッピングの情報を確認する.....	43
2.7.1 RID 方式のユーザーマッピングを使用している場合.....	43
2.7.2 LDAP 方式のユーザーマッピングを使用している場合.....	44
2.7.3 Active Directory スキーマ方式のユーザーマッピングを使用している場合.....	44
2.8 管理サーバの稼働状態を確認する.....	45
2.9 サーバとの接続に問題がないか確認する.....	46
2.10 DNS による名前解決に問題がないか確認する.....	47

2.11 FC パスの状態を確認する.....	48
2.12 ハードウェアの状態を確認する.....	48
2.13 HCP との接続状態を確認する.....	48
2.14 管理ポートおよび BMC ポートの通信を確認する.....	48
2.15 NTP による時刻同期に問題がないか確認する.....	49
2.16 バックアップ管理ソフトウェアの状態および設定を確認する.....	50
2.16.1 バックアップサーバおよびメディアサーバでエラーメッセージやログを確認する.....	50
2.16.2 バックアップまたはリストアの実行結果を確認する.....	50
2.16.3 バックアップ管理ソフトウェアの設定内容を確認する.....	50
2.16.4 テープドライブの状態を確認する.....	50
2.17 同じテープ装置を接続しているほかのノードの OS の状態を確認する.....	51
2.18 ノードに SAN で接続されたテープ装置の状態を確認する.....	51
2.19 HFRR ペアの状態を確認する.....	52
3. 障害情報の収集と保守員への連絡.....	53
3.1 管理サーバのログファイルの採取方法.....	54
3.1.1 Windows のメニューから実行する場合.....	54
3.1.2 コマンドを使用する場合.....	54
3.2 ノードおよび Virtual Server のログファイルの採取方法.....	56
3.3 Hitachi File Services Manager のインストーラーのログファイルの採取方法.....	57
3.4 パケットトレースのログファイルの採取方法.....	58
3.5 CIFS サービスの性能解析用ログの採取方法.....	59
4. 障害の回復.....	61
4.1 GUI の操作ミスを確認して操作し直す.....	63
4.2 コマンドの操作ミスを確認して操作し直す.....	63
4.3 管理サーバの認証パスワードを登録し直す.....	63
4.4 システムメッセージを確認して障害を回復する.....	63
4.5 クラスタおよびノードのエラー情報を確認して障害を回復する.....	63
4.5.1 クラスタおよびノードのエラー情報の確認と回復方法の特定.....	63
4.5.2 回復方法 1.....	65
4.5.3 回復方法 2.....	65
4.5.4 回復方法 3.....	65
4.5.5 回復方法 4.....	65
4.5.6 回復方法 5.....	65
4.5.7 回復方法 6.....	66
4.5.8 回復方法 7.....	66
4.5.9 回復方法 8.....	66
4.6 リソースグループまたは Virtual Server のエラー情報を確認して障害を回復する.....	66
4.6.1 リソースグループまたは Virtual Server のエラー情報の確認と回復方法の特定.....	66
4.6.2 回復方法 1.....	70
4.6.3 回復方法 2.....	70
4.6.4 回復方法 3.....	70
4.6.5 回復方法 4.....	70
4.6.6 回復方法 5.....	71
4.6.7 回復方法 6.....	71
4.6.8 回復方法 7.....	71
4.6.9 回復方法 8.....	71
4.6.10 回復方法 9.....	71
4.6.11 回復方法 10.....	71
4.6.12 回復方法 11.....	71

4.6.13 回復方法 12.....	72
4.6.14 回復方法 13.....	72
4.6.15 回復方法 14.....	72
4.6.16 回復方法 15.....	72
4.6.17 回復方法 16.....	72
4.6.18 回復方法 17.....	73
4.6.19 回復方法 18.....	73
4.6.20 回復方法 19.....	73
4.6.21 回復方法 20.....	73
4.6.22 回復方法 21.....	73
4.6.23 回復方法 22.....	74
4.6.24 回復方法 23.....	74
4.6.25 回復方法 24.....	74
4.6.26 回復方法 25.....	74
4.6.27 回復方法 26.....	75
4.6.28 回復方法 27.....	76
4.7 手動でフェールオーバー・フェールバックする.....	77
4.8 ファイルシステムの障害を回復する.....	77
4.8.1 空き容量があってもファイルを作成できない場合.....	78
4.8.2 OS 障害によってファイルシステムが閉塞している場合（自動フェールオーバー機能を設定しているとき）.....	79
4.8.3 OS 障害によってファイルシステムが閉塞している場合（自動フェールオーバー機能を設定していないとき）.....	79
4.8.4 ストレージシステムの障害によってファイルシステムが閉塞している場合.....	80
4.8.5 ファイルシステムを継続使用できない場合.....	81
4.8.6 プールの容量不足によってノード上のファイルシステムが閉塞している場合.....	82
4.8.7 プールの容量不足によって Virtual Server 上のファイルシステムが閉塞している場合.....	83
4.8.8 階層ファイルシステム内の階層で容量が不足している場合.....	83
4.8.9 差分格納デバイスを設定したファイルシステムが閉塞している場合.....	83
4.8.10 プールの容量不足によって差分格納デバイスを設定したファイルシステムが閉塞している場合（Virtual Server 未使用時）.....	84
4.8.11 プールの容量不足によって差分格納デバイスを設定したファイルシステムが閉塞している場合（Virtual Server 使用時）.....	84
4.9 差分格納デバイスの障害を回復する.....	85
4.9.1 差分格納デバイスの容量が不足した場合（状態が Overflow のとき）.....	85
4.9.2 差分格納デバイスの容量が不足した場合（状態が Blocked のとき）.....	86
4.9.3 デバイスファイルにアクセス障害が発生した場合（Virtual Server 未使用時）.....	86
(1) ストレージシステムに障害が発生した場合.....	87
(2) 差分格納デバイスの障害の回復.....	87
4.9.4 デバイスファイルにアクセス障害が発生した場合（Virtual Server 使用時）.....	88
(1) ストレージシステムに障害が発生した場合.....	88
(2) 差分格納デバイスの障害の回復.....	89
4.10 差分スナップショットの障害を回復する.....	89
4.10.1 Virtual Server を使用していない場合.....	90
4.10.2 Virtual Server を使用している場合.....	91
4.11 HCP へのアクセス障害を回復する.....	91
4.12 HCP にデータをマイグレートしていたファイルシステムをリストアする.....	92
4.12.1 ファイルをスタブ化している場合.....	93
4.12.2 ファイルをスタブ化していない場合.....	94
4.13 ファイルシステムおよびプライマリー HCP の障害時にレプリカ HCP からファイルシステムをリストアする.....	95
4.14 マイグレートされたファイルをスタブ化していない場合に HVFP から HCP のデータをリストアする.....	96
4.15 システム設定情報を回復する.....	97
4.15.1 OS ディスクに障害が発生している場合.....	97
4.15.2 共有 LU に障害が発生している場合.....	98

4.15.3 ノードの OS ディスクまたは共有 LU で障害が発生している場合	98
4.15.4 Virtual Server OS LU に障害が発生している場合	99
4.16 システム設定情報およびユーザーデータを一括で回復する	101
4.17 FC パスの障害を回復する	103
4.17.1 同一ターゲットへの片方のパスで「Error」が表示されている場合	103
4.17.2 同一ターゲットへの両方のパスで「Online (LU Error)」が表示されている場合	103
4.17.3 同一ターゲットへの両方のパスで「Error」が表示されている場合	104
4.17.4 同一ターゲットへの両方のパスで「Configuration Mismatch」が表示されている場合	105
4.17.5 同一ターゲットへの両方のパスで「Unknown」が表示されている場合	106
4.17.6 特定の FC パスで「Partially Online」が表示されている場合	106
4.17.7 同一ターゲットへの片方のパスで「Configuration Mismatch」が表示されている場合	106
4.17.8 FC パスの情報が表示されない場合	106
4.18 インターフェースやネットワークのエラー情報を確認して障害を回復する	107
4.18.1 「Unknown」が表示されている場合	107
4.18.2 管理ポートに「Invalid」が表示されている場合	108
4.18.3 データポートに「Invalid」が表示されている場合	108
4.19 リンク結合のエラー情報を確認して障害を回復する	108
4.19.1 [Link status] に「Down」が表示されている場合	108
4.19.2 [LACP] の [Aggregate] に「Not aggregated」が表示されている場合	109
4.19.3 通常稼働させるポートの [Active port] の [Status] に「Standby」が表示されている場合	109
4.20 データポートのエラー情報を確認して障害を回復する	110
4.20.1 [Link status] に「Down」が表示されている場合	110
4.20.2 [Connected status] の [Speed] に誤った通信速度が表示されている場合	110
4.21 ハードウェアの障害を回復する	110
4.22 OS 起動時に LU が認識できない障害を回復する	111
4.23 ほかのファイルサーバからのデータインポートでの障害を回復する	111
4.23.1 インポート元のファイルサーバとの通信に失敗した場合	111
4.23.2 HVFP で I/O 障害が発生した場合	112
4.23.3 一部のファイルのインポートに失敗した場合	112
(1) マッピングが設定済みの場合	112
(2) マッピングが未設定の場合	113
4.23.4 インポートが完了する前にインポートの設定を解除した場合	114
4.23.5 アカウントの名前解決が失敗した場合	114
4.23.6 アカウント名にマルチバイト文字が含まれる場合	114
4.24 Backup Restore の機能に関する障害を回復する	114
4.24.1 オンラインバックアップがエラー終了した場合	115
4.24.2 バックアップサーバまたはメディアサーバと NDMP サーバ間の接続に問題があった場合	115
4.24.3 ジョブの実行状態やテープ装置の状態に問題があった場合	115
4.24.4 テープドライブとノードの接続が閉塞状態になっている場合	116
4.24.5 Backup Restore の処理でタイムアウトが頻発する場合	116
4.24.6 縮退運用中にバックアップまたはリストアを実行する場合	116
(1) 縮退運用中に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	116
(2) 両ノードで同じテープドライブを共有している場合	117
(3) それぞれのノードで異なるテープドライブを使用している場合	117
(4) Virtual Server でテープドライブを使用している場合	117
4.25 Hitachi File Remote Replicator の機能に関する障害を回復する	118
4.25.1 ネットワークに障害が発生した場合	118
4.25.2 サイト間で HFRR ペアの状態が一致していない場合	118
(1) 片方のサイトで nobaseline と表示されるとき	119
(2) 片方のサイトで suspend, cancel-error, restoring, restore-error または disable と表示されるとき	119
(3) 片方のサイトで copy, fullcopy または copy-error と表示されるとき	119
(4) 片方のサイトで cancel と表示されるとき	119
(5) 片方のサイトで--と表示されるとき	119
(6) 片方のサイトで HFRR ペアの情報が消失しているとき	120

4.25.3 フェールオーバーの発生によって処理が中断された場合.....	120
4.25.4 リソースグループまたは Virtual Server のリソースが稼働していない状態で HFRR ペアを解除する場合.....	120
4.25.5 コマンドの処理を途中で終了した場合.....	120
4.25.6 HFRR ペアを構成するファイルシステムの容量拡張に関連する障害が発生した場合.....	120
4.25.7 両サイトの時刻が同期していない場合.....	121
4.25.8 ruspairlist コマンドで Baseline と Copying に同じ差分スナップショット名が表示される場合.....	121
4.25.9 セカンダリーサイトで synclist コマンドに copying と表示される場合.....	121
4.25.10 ruspairdelete コマンドまたは ruspairdisable コマンドで KAQR10760-E メッセージが出力される場合.....	122
4.26 ファイルスナップショットの処理で発生したタイムアウトを回復する.....	123
付録 A インストール履歴.....	125
A.1 ソフトウェアのインストール履歴ログファイルの確認.....	126
付録 B ネットワーク情報.....	127
B.1 ネットワーク情報ログファイルの確認.....	128
B.2 enas_routelist.log ファイル.....	128
B.3 log_ifconfig ファイル.....	129
B.4 log_interfaces_check ファイル.....	131
付録 C ネットワークの通信状況の確認方法.....	139
C.1 ネットワークの通信状況を確認する前に.....	140
C.2 ネットワーク構成ごとの通信の確認.....	140
C.2.1 ネットワーク内での通信を確認する.....	141
C.2.2 異なるネットワーク間の通信を確認する.....	142
C.3 通信できない場合の対処.....	142
C.3.1 IP アドレス、ネットマスクの確認.....	142
C.3.2 VLAN ID の確認.....	142
C.3.3 MTU 値の確認.....	143
C.3.4 ルーティングの確認.....	143
C.3.5 ネゴシエーションモードの確認.....	145
C.4 ネットワークの通信確認の実行例.....	146
C.4.1 nasping コマンドを使用した通信の確認の実行例.....	146
C.4.2 nastraceroute コマンドを使用した通信の確認の実行例.....	147
付録 D Hitachi File Remote Replicator のログの出力内容.....	149
D.1 Hitachi File Remote Replicator ログ.....	150
D.2 Hitachi File Remote Replicator 統計情報ログ.....	150
付録 E トラブルシューティング事例.....	153
E.1 GUI に関するトラブルシューティング事例.....	154
E.2 HCP 連携に関するトラブルシューティング事例.....	162
E.3 ウイルススキャンに関するトラブルシューティング事例.....	164



目次

図 1-1 障害が発生した場合の対策の流れ.....	22
図 1-2 ネットワークを介してリモートの HCP と連携している場合に HCP へのアクセス障害が発生したときの対策の流れ.....	23
図 C-1 HVFP とクライアントが同一ネットワークに属している場合の構成例.....	140
図 C-2 HVFP とクライアントが異なるネットワークに属している場合の構成例.....	141

表目次

表 はじめに -1 HVFP のマニュアル体系.....	17
表 1-1 Backup Restore・ファイルスナップショット・Hitachi File Remote Replicator の機能がエラー終了した際に確認する項目.....	28
表 2-1 クラスタ状態と状態が表示される要因.....	33
表 2-2 ノード状態と状態が表示される要因.....	33
表 2-3 リソースグループ状態と状態が表示される要因.....	35
表 2-4 リソースグループのエラー情報とエラー情報が表示される要因.....	36
表 2-5 Virtual Server 状態と状態が表示される要因.....	37
表 2-6 Virtual Server のエラー情報とエラー情報が表示される要因.....	37
表 2-7 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.....	45
表 2-8 管理サーバ上の統合トレースログファイルおよび Hitachi File Services Manager のメッセージログに出力される情報.....	45
表 2-9 イベントログに出力される情報.....	46
表 2-10 管理ポートおよび BMC ポートの通信確認ワークシート.....	48
表 2-11 管理ポートおよび BMC ポートの通信確認ワークシートの記入例.....	49
表 3-1 種別として指定する値と作成されるアーカイブファイルの関係.....	56
表 3-2 インストールまたはアンインストールがエラー終了したときの状況とログファイルの格納先.....	58
表 4-1 [Browse Cluster Status] ページ ([Cluster / Node status] 表示) で表示されるクラスタ状態に対応した障害の回復方法.....	64
表 4-2 [Browse Cluster Status (Cluster / Node Status)] ページで表示されるノード状態に対応した障害の回復方法.....	64
表 4-3 [Browse Cluster Status] ページ ([Resource group status] 表示) で表示されるリソースグループ状態に対応した障害の回復方法.....	67
表 4-4 [Browse Cluster Status] ページ ([Resource group status] 表示) で表示されるリソースグループのエラー情報に対応した障害の回復方法.....	67
表 4-5 [< Virtual Server >] サブウィンドウで表示される Virtual Server 状態に対応した障害の回復方法.....	68
表 4-6 [< Virtual Server >] サブウィンドウに表示される Virtual Server のエラー情報に対応した障害の回復方法.....	69
表 4-7 Virtual Server の処理が完了していない (コマンドが中断した) 場合の対処および実行可能なコマンド.....	75
表 4-8 ほかのファイルサーバからのデータインポート時に HVFP で I/O 障害が発生した場合のメッセージと対処.....	112
表 A-1 インストール履歴ファイルに出力される情報.....	126
表 B-1 enas_routelist.log ファイルに出力される情報.....	128
表 B-2 log_ifconfig ファイルに出力される情報.....	130
表 B-3 log_interfaces_check ファイルに出力される項目.....	131
表 B-4 DNS サーバとの接続状態として出力される情報.....	131
表 B-5 NIS サーバとの接続状態として出力される情報.....	132
表 B-6 NTP サーバとの接続状態として出力される情報.....	132
表 B-7 ユーザー認証用の LDAP サーバとの接続状態として出力される情報.....	133
表 B-8 CIFS クライアントの認証サーバとの接続状態として出力される情報.....	134

表 B-9 NFS クライアントの認証サーバとの接続状態として出力される情報.....	135
表 B-10 ユーザーマッピング用の LDAP サーバとの接続状態として出力される情報.....	135
表 D-1 Hitachi File Remote Replicator のシステム統計情報として出力される内容.....	150
表 D-2 Hitachi File Remote Replicator のペア統計情報として出力される内容.....	150
表 E-1 GUI に関するトラブルシューティング事例.....	154
表 E-2 HCP 連携に関するトラブルシューティング事例.....	162
表 E-3 ウイルススキャンに関するトラブルシューティング事例.....	164



はじめに

このマニュアルは、Hitachi Virtual File Platform (HVFP) の障害発生時の対応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、次の方にお読みいただくことを前提に説明しています。

- HVFP を運用・管理する方（システム管理者）
- HVFP を利用する方（エンドユーザー）

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. 障害対策の流れ	HVFP に障害が発生したときに、障害の発生元と要因を特定するまでの流れを説明しています。
2. 障害要因の特定	障害情報を確認し、要因を特定する方法について説明しています。
3. 障害情報の収集と保守員への連絡	ログファイルの採取方法について説明しています。
4. 障害の回復	障害を回復する方法について説明しています。
A. インストール履歴	ソフトウェアのインストール履歴のログファイルおよび出力内容について説明しています。
B. ネットワーク情報	ネットワーク情報のログファイルおよび出力内容について説明しています。
C. ネットワークの通信状況の確認方法	File Services Manager のネットワーク設定の問題のため、HVFP とクライアントの間で通信できない場合の対処方法について説明しています。
D. Hitachi File Remote Replicator のログの出力内容	Hitachi File Remote Replicator のログについて説明しています。
E. トラブルシューティング事例	GUI、HCP 連携およびウイルススキャンに関するトラブルシューティングの事例について説明しています。

マニュアル体系

HVFP のマニュアル体系を次に示します。

なお、HVFP 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、運用する構成に応じてお読みいただくマニュアルが異なります。

表 はじめに -1 HVFP のマニュアル体系

マニュアル名	内容
Hitachi Virtual File Platform / Hitachi Data Ingestor システム構成ガイド	HVFP を運用するために、最初にお読みいただくマニュアルです。 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 (このマニュアル)	クラスタ構成の HVFP の障害対策を説明しています。
Hitachi Virtual File Platform シングルノード構成セットアップガイド	シングルノード構成の HVFP のセットアップ方法について説明しています。
Hitachi Virtual File Platform / Hitachi Data Ingestor シングルノード構成ユーザーズガイド	シングルノード構成の HVFP を運用するために必要な手順や GUI リファレンスなどを説明しています。
Hitachi Virtual File Platform / Hitachi Data Ingestor シングルノード構成トラブルシューティングガイド	シングルノード構成の HVFP の障害対策を説明しています。
Hitachi Virtual File Platform / Hitachi Data Ingestor コマンドリファレンス	クラスタ構成およびシングルノード構成の HVFP で使用できるコマンドの文法について説明しています。
Hitachi Virtual File Platform API リファレンス	クラスタ構成およびシングルノード構成の HVFP の API の使用方法について説明しています。
Hitachi Virtual File Platform / Hitachi Data Ingestor メッセージリファレンス	クラスタ構成およびシングルノード構成の HVFP のメッセージについて説明しています。
Hitachi Virtual File Platform / Hitachi Data Ingestor ファイルアクセス (CIFS/NFS) ユーザーズガイド	CIFS または NFS クライアントから、クラスタ構成およびシングルノード構成の HVFP の CIFS サービスまたは NFS サービスを利用するに当たって、事前に知っておいていただきたいことや、注意する必要があることについて説明しています。

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

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)
ALog ConVerter	ALog ConVerter(R)
Device Manager	Hitachi Device Manager Software
Dynamic Provisioning	Hitachi Dynamic Provisioning
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)
HCP	Hitachi Content Platform
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
HVFP	Hitachi Virtual File Platform
Internet Explorer	Windows(R) Internet Explorer(R)
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 • 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 • Microsoft(R) Windows(R) 7 Ultimate x64 Edition
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 NT	Microsoft(R) Windows NT(R) Server Network Operating System
Windows Server 2003	次の製品を区別する必要がない場合の表記です。 <ul style="list-style-type: none"> • Microsoft(R) Windows Server(R) 2003, Datacenter Edition Operating System • Microsoft(R) Windows Server(R) 2003, Enterprise 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, Standard Edition Operating System Microsoft(R) Windows Server(R) 2003, Web Edition Operating System
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

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。

このマニュアルで使用する記号

このマニュアルでは、次に示す記号を使用しています。

記号	意味
[]	画面、メニュー、ボタン、キーボードのキーなどを示します。 (例) [<ファイルシステム>] サブウィンドウ [OK] ボタン [Enter] キー
< >	可変値であることを示します。 (例) <ホスト名>.<ポート番号> 実際のホスト名が「host0」、ポート番号が「1024」の場合、「host0.1024」と指定することを示します。
[] - []	「-」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
英字	A~Z a~z
数字	0~9
英数字	A~Z a~z 0~9

注 すべての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、どれか一つを指定することを示します。 (例 1) [A]

記号	意味
	「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。
...	この記号の直前に示された項目を繰り返して複数指定できます。 (例) A, B, ... 「Aの後ろに、Bを複数指定できる」ことを示します。

KB（キロバイト）などの単位表記について

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

障害対策の流れ

この章では、Hitachi Virtual File Platform (HVFP) に障害が発生したときに、障害の発生元と要因を特定するまでの流れを説明します。

障害要因を特定できなかつたり、障害要因を特定する過程で、フェールオーバーが発生していることを確認したりした場合は、保守員に連絡してください。なお、Virtual Server を使用していない場合は、Virtual Server についての記述は読み飛ばしてください。

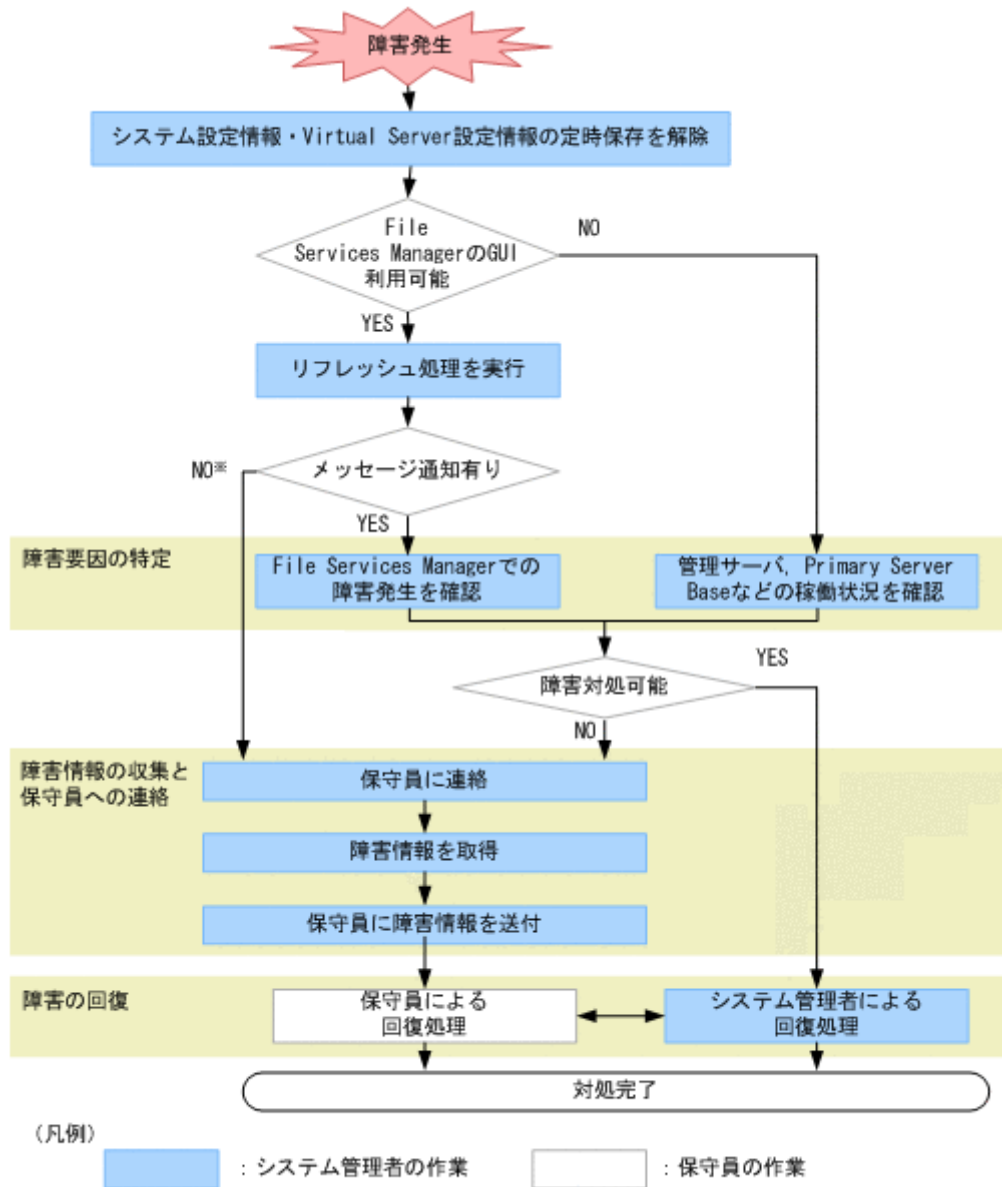
- 1.1 障害対策の概要
- 1.2 ファイルシステムを利用できない場合
- 1.3 File Services Manager の GUI が正常に動作しない場合
- 1.4 Backup Restore ・ ファイルスナップショット ・ Hitachi File Remote Replicator の機能がエラー終了した場合

1.1 障害対策の概要

HVFP で障害が発生していることを確認したら、GUI またはコマンドを利用できる場合には、最初にシステム設定情報の定時保存を解除します。また、Virtual Server を使用している場合は、Virtual Server の設定情報の定時保存を解除します。その後、リフレッシュ処理を実行して管理サーバのデータベースを更新したら、要因を特定し、障害を回復します。

障害対策の流れを次の図に示します。

図 1-1 障害が発生した場合の対策の流れ



※: まずサポートサービスに連絡してください。障害が解決しない場合は保守員に連絡してください。

障害要因の特定

障害情報を確認して、障害要因を特定します。障害が発生してフェールオーバーしている場合は、早急に保守員に連絡してください。

関連項目

- 1.2 ファイルシステムを利用できない場合

- 1.3 File Services Manager の GUI が正常に動作しない場合
- 1.4 Backup Restore ・ ファイルスナップショット ・ Hitachi File Remote Replicator の機能がエラー終了した場合
- 2. 障害要因の特定

障害情報の収集と保守員への連絡

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、保守員に送付します。障害情報を収集する方法については、「3. 障害情報の収集と保守員への連絡」を参照してください。

障害の回復

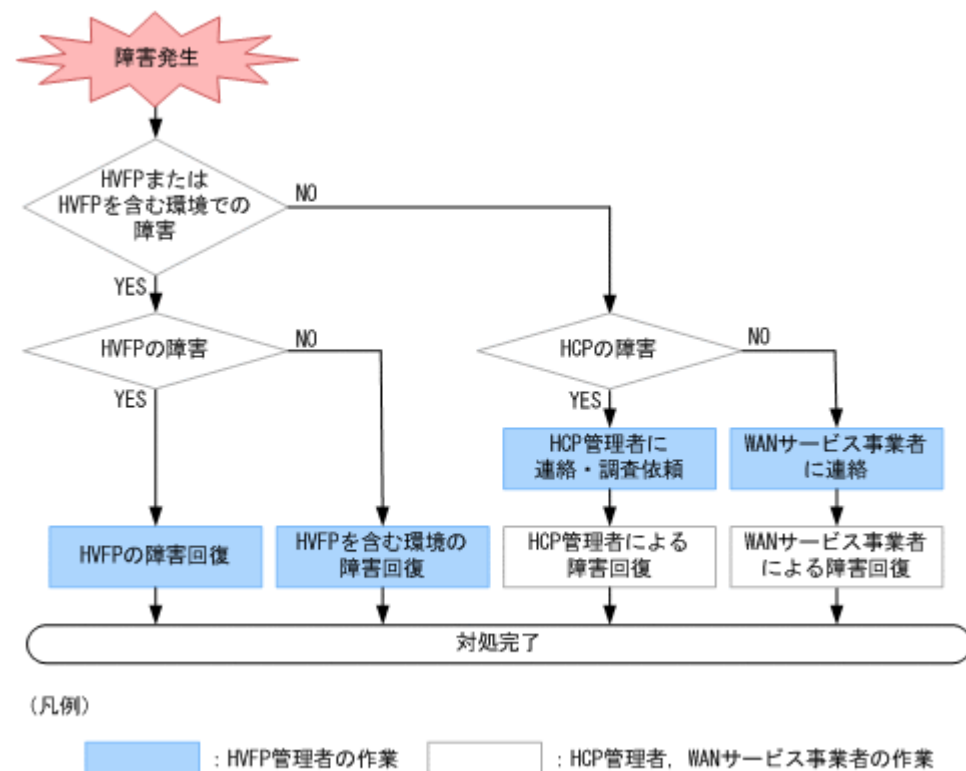
障害要因を特定したら、メッセージに従って障害を回復します。障害の内容によっては、保守員とシステム管理者の間で互いに連絡を取って障害を回復する必要があります。障害を回復する方法については、「4. 障害の回復」を参照してください。

なお、障害回復後は、必要に応じて、システム設定情報および Virtual Server の設定情報の定時保存を有効にしてください。

ネットワークを介してリモートの HCP と連携している場合は、HVFP で障害が発生していても、HCP にアクセスできないために HVFP のサービスを提供できないことがあります。ネットワークを介してリモートの HCP と連携している場合に HCP にアクセスできない障害が発生したときは、「4.11 HCP へのアクセス障害を回復する」に従って対処してください。

HCP にアクセスできない障害が発生したときの障害対策の流れを次の図に示します。

図 1-2 ネットワークを介してリモートの HCP と連携している場合に HCP へのアクセス障害が発生したときの対策の流れ



1.2 ファイルシステムを利用できない場合

エンドユーザーがファイル共有を利用できなかつたり、アクセスできなかつたりするなど、HVFPのサービスを利用できない場合に、システム管理者が障害要因を特定する方法について説明します。

空き容量があってもファイルを作成できない場合は、「[4.8.1 空き容量があってもファイルを作成できない場合](#)」に従って対処してください。

エンドユーザーから連絡を受けて、システム管理者が障害の発生元と要因を特定するまでの手順を次に示します。

1. ファイル共有のサービス停止について、エンドユーザーから通知を受けます。

システム管理者は、エンドユーザーが利用していたファイル共有が NFS 共有か CIFS 共有か確認します。

NFS 共有のサービスが停止した場合

システム管理者はサービス停止した仮想 IP アドレスと共有ディレクトリ名をエンドユーザーに確認し、エンドユーザーが利用しているクラスタ、ノード、リソースグループ、Virtual Server、ファイルシステム、ディレクトリを特定します。

CIFS 共有のサービスが停止した場合

システム管理者はサービス停止した共有のパス名（ $\text{¥¥} < \text{ノードのホスト名または Virtual Server 名} > \text{¥} < \text{CIFS 共有名} > \text{¥} < \text{使用するディレクトリのパス} >$ ）をエンドユーザーに確認し、エンドユーザーが利用しているクラスタ、ノード、リソースグループ、Virtual Server、ファイルシステム、フォルダを特定します。

また、ユーザーマッピングを使用している場合、サービスを利用できないユーザーに対してユーザー ID やグループ ID が正しく割り当てられているか、ユーザーマッピング情報を確認してください。ユーザーマッピング情報を確認する手順については、「[2.7 ユーザーマッピングの情報を確認する](#)」を参照してください。

フェールオーバーやフェールバックによってリソースグループまたは Virtual Server が移動すると、フェールオーバーやフェールバックが成功しても、移動するリソースグループまたは Virtual Server を利用していた CIFS 共有のサービスは強制的に停止されます。CIFS クライアントからファイルシステムを利用する場合の注意事項については、「[システム構成ガイド](#)」を参照してください。

2. ノード、スイッチおよびストレージシステムの電源が入っていることを確認します。

電源が入っていない場合は、電源を入れてから、エンドユーザーが HVFP のサービスを利用できるか、確認してください。

3. ノード上のシステムメッセージを確認します。

4. ファイルシステムに対するアクセスの抑止状況を確認します。

次の操作の処理中は、エンドユーザーからのファイルシステムに対するアクセスが一時的に抑止されます。処理が終了すると抑止が解除されます。

- ファイルシステムの拡張
- 差分格納デバイスの設定、拡張および解除
- 差分スナップショットの作成および削除
- オンラインバックアップの実行
- 仮想 LU の未使用領域の解放

また、Backup Restore のボリュームレプリケーション連携機能を利用している場合は、システム管理者が horcfreeze コマンドを実行して、クライアントからのアクセスを意図的に抑止していることも考えられます。システム管理者は、fsctl コマンドを使用して、エンドユーザーが利用していたファイルシステムに対するアクセスの抑止状況を確認してください。システム

管理者の操作ミスなどによって抑止が解除されていない場合には、`horcunfreeze` コマンドを実行して、抑止を解除してください。

5. [Cluster Management] ダイアログの [Browse Cluster Status] ページで、クラスタ、ノード、リソースグループ、Virtual Server のエラー情報を確認します。
File Services Manager の [Browse Cluster Status] ページで、手順 1 で特定したクラスタの状態を参照し、フェールオーバー機能に障害が発生していないか確認してください。
Virtual Server を使用している場合は、File Services Manager の [< Virtual Server >] サブウィンドウで、手順 1 で特定した Virtual Server の状態を参照し、障害が発生していないか確認してください。
6. [Access Protocol Configuration] ダイアログの [List of Services] ページでサービスの動作状態を確認します。
フェールオーバー機能に障害が認められない場合は、サービスが停止していることがあります。
[Cluster Management] ダイアログの [Browse Cluster Status] ページ ([Resource group status] 表示) にある [Running node] で、エンドユーザーが利用しているリソースグループに割り当てられているノードを確認します。
次に、File Services Manager の [List of Services] ページを参照し、エンドユーザーが利用していたサービスの動作状態を確認します。
7. [< Physical Node >] または [< Virtual Server >] サブウィンドウの [ファイルシステム] タブでファイルシステムのエラー情報を確認します。
エンドユーザーが利用していたサービスが稼働していて、障害が認められない場合は、ファイルシステムに障害が発生していることがあります。File Services Manager の [< Physical Node >] または [< Virtual Server >] サブウィンドウの [ファイルシステム] タブを参照し、操作 1. で特定したファイルシステムの状態を確認します。
8. [< Physical Node >] または [< Virtual Server >] サブウィンドウの [共有] タブでファイル共有の設定を確認します。
ファイルシステムが正常にマウントされていて、障害が認められない場合は、File Services Manager の [< Physical Node >] または [< Virtual Server >] サブウィンドウの [共有] タブを参照し、エンドユーザーが利用していたファイル共有の設定を確認します。
また、ホスト名やネットグループ名を指定して設定した NFS 共有が表示されない場合は、ホスト名の名前解決ができないことや、次に示すサーバとの接続状況に問題があることも要因として考えられます。
 - DNS サーバ
 - NIS サーバ
 - WINS サーバ各サーバとの接続状況を確認する方法については、「[2.9 サーバとの接続に問題がないか確認する](#)」を参照してください。また、NIS サーバおよび DNS サーバの設定を [Network & System Configuration] ダイアログの [DNS, NIS, LDAP Setup] ページで確認してください。
9. ネットワークやクライアントの動作環境を確認します。
ファイル共有が表示されていて、障害が認められない場合は、ネットワークやクライアントの動作環境に問題がないかどうかを調査します。

ネットワークの動作環境

ノードとクライアントを接続するネットワークの構成・動作状態を確認します。

通常はネットワークに接続しているポートがリンクダウンするとフェールオーバーが発生しますが、スイッチやケーブルの障害によって両方のノードが同時にリンクダウンすると、フェールオーバーは抑止されます。ポートのエラー情報を確認する方法については、「[4.18 インターフェースやネットワークのエラー情報を確認して障害を回復する](#)」を参照してください。

このほか、次に示すサーバとの接続状況や動作状況を確認してください。

- DNS サーバ
- NIS サーバ
- ユーザー認証用の LDAP サーバ
- ユーザーマッピング用の LDAP サーバ
- CIFS クライアントの認証サーバ (ドメインコントローラーまたは Windows NT サーバ)
- NFS クライアントの認証サーバ (KDC サーバ)

各サーバとの接続状況を確認する方法については、「[2.9 サーバとの接続に問題がないか確認する](#)」を参照してください。

クライアントの動作環境

クライアントの動作環境が HVFP の提供するファイルシステムを利用する条件に違反している場合、フェールオーバーやフェールバックなどを契機にファイル共有のサービスを受けられなくなることがあります。

HVFP が提供するファイルシステムを利用するクライアントの動作環境については、「システム構成ガイド」を参照してください。

10. サービスを利用できないエンドユーザーのクライアントマシンから、ping コマンドで、ノードまたは Virtual Server の仮想 IP アドレスとの接続状態を確認します。

ノードまたは Virtual Server から応答があった場合

OS に障害が発生しているおそれがあります。保守員に連絡してください。

ノードまたは Virtual Server から応答がない場合

サービスを利用できないエンドユーザーのクライアントマシンからノードまたは Virtual Server までの経路で、ネットワーク障害が発生しているおそれがあります。IP アドレスの設定に問題がないか確認し、ネットワーク管理者に連絡してください。ネットワーク障害が発生していない場合は、保守員に連絡してください。

11. HCP にデータをマイグレートしている場合は、HCP で障害が発生していないか確認します。

HCP で障害が発生している場合は、HCP にマイグレートしているファイルにアクセスするとエラーになることがあります。KAQM37070-E または KAQM37094-E メッセージが出力されていないか確認してください。これらのメッセージが出力されていた場合は、HCP の管理者に障害の回復を依頼してください。

なお、ネットワークを介してリモートの HCP と連携している場合は、「[4.11 HCP へのアクセス障害を回復する](#)」に従って対処してください。

上記の手順で障害要因を特定できなかった場合は、保守員に連絡してください。

1.3 File Services Manager の GUI が正常に動作しない場合

File Services Manager の GUI が正常に動作しない場合は、次の手順に従って障害要因を特定してください。



参考 SNMP または E-mail 通知を利用していない場合、File Services Manager の GUI を利用できない障害が発生すると、障害情報を確認できません。障害情報を確認するために、SNMP または E-mail 通知を併用することを推奨します。

障害要因を特定する手順を次に示します。

1. 管理コンソールで次のことを確認します。

- JavaScript が有効になっているか
- Cookie が有効になっているか

上記の設定に問題がない場合は、「付録 E. トラブルシューティング事例」を参照して対処してください。

2. 管理サーバが正常に稼働しているかを確認します。
マシンおよび OS が正常に稼働していることを確認します。
3. 次の操作を実行して、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。

Windows 7 までの Windows の場合

[スタート] - [プログラム] - [Hitachi Command Suite] - [File Services Manager] - [Status - HFMSM] を選択します。

Windows 8 または Windows Server 2012 の場合

スタート画面のアプリ一覧から [Status - HFMSM] を選択します。

4. `nasping` コマンドでネットワークの接続状態を確認します。
応答エラーになった場合には次のことを確認してください。

- LAN ケーブルが断絶していないか
- ノードに装着ミスがないか
- ノード、スイッチおよびストレージシステムの電源が入っているか
- 管理 LAN およびハートビート LAN の接続が正しいか

このほか、ネットワークの設定に問題があつて応答エラーになることもあります。この場合は、クラスタを構成するノードのうち、GUI が正常に動作するノードで [Network & System Configuration] ダイアログの [List of Interfaces] ページを確認してから障害を回復する必要があります。障害回復の手順については、「4.18 インターフェースやネットワークのエラー情報を確認して障害を回復する」を参照してください。

5. Primary Server Base の稼働状態を確認します。

Primary Server Base の WWW サーバ機能の障害の場合は、一時的なものであることがあります。5 分程度待ったあと、GUI で操作し次の事象が発生しないか確認してください。

- KAQM23101-E※または KAQM23102-E メッセージが表示される
- [< Physical Node >] または [< Virtual Server >] サブウィンドウの [設定] タブからダイアログを起動できない

注※：Virtual Server 上で操作する場合は、事前に [< Virtual Server >] サブウィンドウで、Virtual Server の状態が「Offline」でないことを確認してください。

なお、Primary Server Base の WWW サーバ機能に障害が発生しても、ユーザーに対するファイル共有サービスは停止しません。

6. SNMP を設定している場合は、SNMP マネージャーで、SNMP トラップが出力されていないか確認します。

E-mail 通知を設定している場合は、障害情報の E-mail を受信しているか確認します。

7. 障害の要因を特定できなかった場合は、次のログファイルを採取して、保守員に連絡してください。

- ノードの全ログデータ※
- Virtual Server の全ログデータ※
- 管理サーバのログファイル

注※：障害の状態によってはシステム管理者が採取できないこともあります。

ログファイルの採取方法については「3. 障害情報の収集と保守員への連絡」を参照してください。

1.4 Backup Restore・ファイルスナップショット・Hitachi File Remote Replicator の機能がエラー終了した場合

Backup Restore、ファイルスナップショットまたは Hitachi File Remote Replicator の機能を実行中に処理がエラー終了した場合は、エラー終了する直前にエラーメッセージが出力されていないか確認して、障害が発生したサイトや要因を特定してください。

各機能の実行中に発生したエラーの要因を特定するためには、次の項目を確認します。

表 1-1 Backup Restore・ファイルスナップショット・Hitachi File Remote Replicator の機能がエラー終了した際に確認する項目

確認する項目	参照先
GUI に表示されたエラーメッセージ (Backup Restore, ファイルスナップショットの場合)	2.1
標準エラー出力に表示されたエラーメッセージ	2.1
システムメッセージ (Backup Restore, Hitachi File Remote Replicator の場合)	2.2
クラスタおよびノードのエラー状態	2.3
リソースグループまたは Virtual Server のエラー状態	2.4
ファイルシステムのエラー状態 (Backup Restore, Hitachi File Remote Replicator の場合)	2.5
差分格納デバイスのエラー状態	2.6
差分スナップショットのエラー状態 (Hitachi File Remote Replicator の場合)	
管理サーバの稼働状態 (Backup Restore, ファイルスナップショットの場合)	2.8
ノード上のハードウェアの状態 (Backup Restore の場合)	2.12
バックアップ管理ソフトウェアの状態および設定 (Backup Restore の場合)	2.16
同じテープ装置を接続しているほかのノードの OS の状態 (Backup Restore の場合)	2.17
ノードに SAN で接続されたテープ装置の状態 (Backup Restore の場合)	2.18
HFRR ペアの状態 (Hitachi File Remote Replicator の場合)	2.19

障害要因の特定

この章では、障害情報を確認し、要因を特定する方法について説明します。

システム管理者は、障害が発生したことを認識する前に、エンドユーザーから、HVFP のサービスを利用できないとの連絡を受けることがあります。このとき、障害要因を特定する方法については、「1.2 ファイルシステムを利用できない場合」を参照してください。

障害要因を特定する過程で、フェールオーバーが発生していることを確認した場合は、保守員に連絡してください。

- 2.1 GUI または標準エラー出力に表示されたエラーメッセージを確認する
- 2.2 ノード上のシステムメッセージを確認する
- 2.3 クラスタおよびノードの状態を確認する
- 2.4 リソースグループまたは Virtual Server の状態を確認する
- 2.5 ファイルシステムのエラー状態を確認する
- 2.6 差分格納デバイスのエラー状態を確認する
- 2.7 ユーザーマッピングの情報を確認する
- 2.8 管理サーバの稼働状態を確認する
- 2.9 サーバとの接続に問題がないか確認する
- 2.10 DNS による名前解決に問題がないか確認する
- 2.11 FC パスの状態を確認する
- 2.12 ハードウェアの状態を確認する
- 2.13 HCP との接続状態を確認する
- 2.14 管理ポートおよび BMC ポートの通信を確認する
- 2.15 NTP による時刻同期に問題がないか確認する

- 2.16 バックアップ管理ソフトウェアの状態および設定を確認する
- 2.17 同じテープ装置を接続しているほかのノードの OS の状態を確認する
- 2.18 ノードに SAN で接続されたテープ装置の状態を確認する
- 2.19 HFRR ペアの状態を確認する

2.1 GUI または標準エラー出力に表示されたエラーメッセージを確認する

GUI 操作に起因する障害が発生した場合、GUI にエラーメッセージが表示されます。また、コマンド操作に起因する障害が発生した場合、標準エラー出力にエラーメッセージが表示されます。システム管理者は、表示されたエラーメッセージを確認して要因を特定してください。なお、Hitachi File Remote Replicator の機能に起因するエラーの場合は、プライマリーサイトとセカンダリーサイト両方でエラーメッセージを確認する必要があります。

表示されるエラーメッセージの詳細については、「メッセージリファレンス」を参照してください。

2.2 ノード上のシステムメッセージを確認する

システムメッセージには、ハードウェアやソフトウェアで発生した障害に関する重要メッセージが出力されます。

システム管理者は、障害が発生したら、[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し、障害の発生元と要因を特定します。ノードのシステムメッセージは [< Physical Node >] サブウィンドウから、Virtual Server のシステムメッセージは [< Virtual Server >] サブウィンドウから確認できます。

システム管理者は、システムメッセージのメッセージ ID で障害が発生したプログラムを特定し、メッセージテキストで障害の要因を特定します。

システムメッセージから障害要因を特定できなかった場合や、対処方法として保守員に連絡するよう指示された場合は、障害情報をダウンロードして、保守員に送付してください。

システムメッセージは、メッセージ ID とそれに続くメッセージテキストで構成されています。

メッセージ ID の形式は次のとおりです。

KA < X¹X² > < Y¹Y²Y³Y⁴Y⁵ > - < Z >

< X¹X² >

出力元のプログラムを表す記号です。記号の意味を次に示します。

QB : Backup Restore

QG : File Sharing

QK, QM : File Services Manager

QR : Hitachi File Remote Replicator

QS : File snapshots

QV : Anti-Virus Enabler

< Y¹Y²Y³Y⁴Y⁵ >

メッセージの分類を表す数字です。

< Z >

メッセージレベルを表す記号です。記号の意味を次に示します。

E : エラーレベル

I : 情報レベル

W : 警告レベル

Q : 応答レベル

KAQG70000～KAQG72999 のメッセージ ID の場合、フェールオーバー機能に関連したメッセージが出力されています。

システム管理者は、フェールオーバーが成功したメッセージが出力されていても、フェールオーバーする契機となった障害を回復する必要があります。システムメッセージを確認して障害要因を特定してください。

また、フェールオーバーに失敗したメッセージが出力されていた場合は、フェールオーバーする契機となった障害を回復するほか、フェールオーバーに失敗した原因を特定して回復する必要があります。フェールオーバー機能で障害が発生した場合に障害要因を特定する手順については、「[2.3 クラスタおよびノードの状態を確認する](#)」および「[2.4 リソースグループまたは Virtual Server の状態を確認する](#)」を参照してください。

ノード間のハートビート通信に問題がある場合は、KAQG72012-W または KAQG72013-W が出力されます。この場合、フェールオーバーが失敗したり、クラスタの状態が正しく表示されなかったりするおそれがあります。ハートビートの正の通信路ではハートビートポート、副の通信路では管理ポートを使用します。ハートビートポートまたは管理ポートで障害が発生していないか確認してください。

リソースグループの起動時やフェールオーバー時に、NFS 共有の公開先ホストの名前解決に失敗すると、ノード上のシステムメッセージに KAQG72021-W が出力されます。Virtual Server の起動時やフェールオーバー時に、NFS 共有の公開先ホストの名前解決に失敗すると、Virtual Server のシステムメッセージに KAQM35012-W が出力されます。このとき、名前解決に失敗した公開先を利用するクライアントから HVFP にアクセスできません。

なお、フェールオーバーに失敗し、KAQS11197-E または KAQG72009-E のメッセージがノード上に出力された場合、および Virtual Server の使用時にこれらのメッセージに加えて KAQS11197-E または KAQM35004-E のメッセージが Virtual Server 上に出力された場合、Backup Restore のボリュームレプリケーション連携機能によって、ファイルシステムに対するアクセスが一時的に抑止されているおそれがあります。システム管理者は、fsctl コマンドでファイルシステムに対するアクセスの抑止状況を確認し、horcunfreeze コマンドですべてのファイルシステムの抑止を解除してから、再度フェールオーバーしてください。

2.3 クラスタおよびノードの状態を確認する

クラスタおよびノードのエラー状態を [Cluster Management] ダイアログの [Browse Cluster Status] ページで確認できます。

また、確認したクラスタおよびノードの状態ごとに障害を回復する手順については、「[4.5 クラスタおよびノードのエラー情報を確認して障害を回復する](#)」を参照してください。

システム管理者は、障害が発生した前後のシステムメッセージを確認し、[Browse Cluster Status] ページでエラー状態を確認することで、フェールオーバー機能に発生した障害要因を特定できます。

なお、システムに障害が発生した場合、[Cluster Management] ダイアログの [Browse Cluster Status] ページのクラスタやノードの状態が表示されないことがあります。システム管理者は、[Browse Cluster Status] ページでクラスタやノードの状態を確認できない場合、障害情報を収集して保守員に連絡してください。

クラスタの状態を確認する場合は、[Browse Cluster Status] ページ ([Cluster / Node status] 表示) の [Cluster status] を確認します。[Browse Cluster Status] ページ ([Cluster / Node status] 表示) で表示されるクラスタ状態と状態が表示される要因について次の表に示します。

表 2-1 クラスタ状態と状態が表示される要因

クラスタ状態	説明	状態が表示される要因			
		正常	ハードウェア障害	ソフトウェア障害	誤操作
ACTIVE	正常に稼働しています。	○	—	—	—
INACTIVE	停止しています。	○	—	—	○
UNKNOWN	状態が確認できません。	○	○	○	○
DISABLE	障害によってフェールオーバー機能が無効になっています。	—	○	○	—

(凡例) ○：該当する —：該当しない

ノードの状態を確認する場合は、[Browse Cluster Status] ページ ([Cluster / Node status] 表示) の [Node status] を確認します。[Browse Cluster Status] ページ ([Cluster / Node status] 表示) で表示されるノード状態と状態が表示される要因について次の表に示します。

表 2-2 ノード状態と状態が表示される要因

ノード状態	説明	状態が表示される要因			
		正常	ハードウェア障害	ソフトウェア障害	誤操作
UP	正常に稼働しています。	○	—	—	—
INACTIVE	停止しています。	○	—	—	—
DOWN	OS が異常終了して、ノードが停止しています。	—	○	○	—
UNKNOWN	状態が確認できません。	○	○	○	○

(凡例) ○：該当する —：該当しない

フェールオーバー機能で発生する障害は、次のとおり大別できます。

- ・ OS が起動したときに発生した障害
- ・ クラスタを操作しているときに発生した障害
- ・ フェールオーバーする契機となった障害
- ・ フェールオーバーが失敗したときの障害
- ・ サービスを利用できない障害

障害が発生した状況に応じて、障害要因を特定する手順が異なります。それぞれの対処を次に示します。

2.3.1 OS が起動したときに発生した障害の特定

OS が起動したときに障害が発生し、クラスタを構成するノード間の通信に失敗すると、[Cluster Management] ダイアログの [Browse Cluster Status] ページ ([Cluster / Node status] 表示) にクラスタやノードの状態が「UNKNOWN」と表示され、サービスは開始されません。

OS の起動時に障害が発生すると、ノード上のシステムメッセージに次のメッセージが出力されることがあります。

- ・ KAQG72006-E
- ・ KAQG72007-E

- KAQG72008-E
- KAQG72009-E
- KAQG72018-E

システム管理者は、メッセージを確認して障害要因を特定してください。

OS が起動してサービスが開始されると、すべてのファイルシステムのマウント処理が実行されます。ファイルシステムの数が多いと、OS が起動してサービスが開始されるまでに時間が掛かります。システム管理者は、OS が起動してサービスが開始されるまでの標準時間を事前に計測しておくことで、障害が発生していることを早期に発見できます。

OS が起動したあと、標準時間を超えてもサービスが開始されない場合、[Browse Cluster Status] ページ ([Cluster / Node status] 表示) でクラスタやノードの状態を確認して、障害要因を特定してください。

ノードの電源を遮断して計画的に HVFP を全面停止した場合、再度電源を入れると、自動的にサービスが開始されます。しかし、次の状態でノードを計画停止 (電源遮断) した場合には、再度電源を入れても、サービスは自動的に開始されません。

- クラスタまたはノードが停止している状態
- リソースグループまたは Virtual Server が停止している状態

2.3.2 クラスタを操作しているときに発生した障害の特定

クラスタを操作しているときに障害が発生し、クラスタ操作に失敗すると、[Cluster Management] ダイアログの [Browse Cluster Status] ページのクラスタ・ノードにエラー状態が表示されます。

クラスタが操作される主な契機を次に示します。

- [Browse Cluster Status] ページでクラスタ・ノードの状態を操作したとき
- ファイルシステムを追加・削除したとき
- ファイル共有を追加・解除したとき
- ノード名やクラスタ名を変更したとき
- 仮想 IP アドレスを追加・変更・削除したとき

HVFP では、フェールオーバーしても同じ障害が検出されるためにサービスを継続して提供できないと判断した場合、フェールオーバーしないでサービスを停止します。このとき発生した障害を回復しないで、リソースグループまたは Virtual Server をクラスタ内の別のノードに移動しようとする、クラスタの操作に失敗します。また、マウントしようとしたファイルシステムが、HVFP で利用できないファイルシステムだったり、ファイルシステムの構築に失敗していたりすると、クラスタの操作に失敗します。

クラスタ操作時にサービスが停止した場合、[Browse Cluster Status] ページでクラスタ・ノードの状態を確認して、障害要因を特定してください。

また、クラスタ操作時に障害が発生すると、ノード上のシステムメッセージに次のメッセージが出力されていることがあります。

- KAQG72006-E
- KAQG72007-E
- KAQG72008-E
- KAQG72009-E

システム管理者は、メッセージを確認して障害要因を特定してください。

2.3.3 サービスを利用できない場合の障害の特定

フェールオーバー機能を構成するデーモンは、何らかの要因によって停止した場合でも、自動的に再起動します。各デーモンは、core ファイルを出力して停止することがあります。

サービスを利用できない障害が発生した場合、[Check for Errors] ダイアログの [List of RAS Information] ページ ([List of core files] 表示) を参照して、どのサービスの core ファイルが生成されているか、また同じサービスの core ファイルが複数回生成されているかどうかを確認してください。

2.4 リソースグループまたは Virtual Server の状態を確認する

リソースグループのエラー状態は [Cluster Management] ダイアログの [Browse Cluster Status] ページで、Virtual Server のエラー状態は [< Virtual Server >] サブウィンドウで確認できます。

また、確認したリソースグループまたは Virtual Server の状態ごとに障害を回復する手順については、「4.6 リソースグループまたは Virtual Server のエラー情報を確認して障害を回復する」を参照してください。

システム管理者は、障害が発生した前後のシステムメッセージを確認し、リソースグループは [Browse Cluster Status] ページ、Virtual Server は [< Virtual Server >] サブウィンドウでエラー状態を確認することで、フェールオーバー機能に発生した障害要因を特定できます。

リソースグループの状態を確認する場合は、[Browse Cluster Status] ページ ([Resource group status] 表示) の [Resource group status] を確認します。リソースグループの状態とエラー情報は、次のとおり表示されます。

<リソースグループ状態>/<エラー情報>

[Browse Cluster Status] ページ ([Resource group status] 表示) で表示されるリソースグループ状態と状態が表示される要因について次の表に示します。

表 2-3 リソースグループ状態と状態が表示される要因

リソースグループ状態	説明	状態が表示される要因			
		正常	ハードウェア障害	ソフトウェア障害	誤操作
Online	正常に稼働しています。	△	△	△	△
Online Maintenance	監視機能を解除しているため、障害が発生しても自動的にフェールオーバーできません。	△	△	△	△
Online Pending	開始処理中です。	○	—	—	—
Online Ready [※]	クラスタを起動していないので、リソースグループを起動できません。または、クラスタの停止処理中に障害が発生したのでサービスが正しく稼働していません。 なお、クラスタを起動してもリソースグループ状態が変わらない場合	○	—	○	○

リソースグループ状態	説明	状態が表示される要因			
		正常	ハードウェア障害	ソフトウェア障害	誤操作
	は、「4.5」の回復方法 6 に従って OS を再起動してください。				
Offline※	停止しています。	△	△	△	△
Offline Pending	停止処理中です。	○	—	—	—
Discovery (exclusivity)	開始処理中です。	○	—	—	—
Initializing	開始処理中です。	○	—	—	—
Internal Error	内部エラーを検出しています。保守員に連絡してください。	—	○	○	—

(凡例) ○：該当する —：該当しない △：リソースグループのエラー情報に対応する

注※：クラスタの状態が「DISABLE」の場合にも表示されます。「Online Ready」または「Offline」と表示された場合には、[Browse Cluster Status] ページ ([Cluster / Node status] 表示) でクラスタの状態もあわせて確認してください。

[Browse Cluster Status] ページ ([Resource group status] 表示) で表示されるリソースグループのエラー情報とエラー情報が表示される要因について次の表に示します。

表 2-4 リソースグループのエラー情報とエラー情報が表示される要因

エラー情報	説明	エラー情報が表示される要因			
		正常	ハードウェア障害	ソフトウェア障害	誤操作
No error	エラーは発生していません。	○	—	—	—
Internal error - not recoverable	回復できない内部エラーが発生しています。	—	○	○	—
Monitor activity unknown	監視または監視除外の処理中に障害が発生しています。	—	—	○	—
No available nodes または No available nodes in failure domain after monitor failure	障害が発生しましたが、すでにフェールオーバーしている状態のため、フェールオーバーできません。	○	—	—	○
Node unknown	ノードの [Node status] が「UNKNOWN」のため、リソースグループを起動できません。	—	○	○	○
Split resource group (exclusivity)	クラスタ内で同一のリソースが重複して稼働しています。クラスタを強制停止したあと、両方のノードの OS を再起動してください。	—	—	○	○
srmexec executable error	起動または停止処理中にエラーが発生しています。	—	○	○	—

(凡例) ○：該当する —：該当しない

[< Virtual Server >] サブウィンドウで表示される Virtual Server 状態と状態が表示される要因について次の表に示します。

表 2-5 Virtual Server 状態と状態が表示される要因

Virtual Server 状態	説明	状態が表示される要因			
		正常	ハードウェア障害	ソフトウェア障害	誤操作
Online	正常に稼働しています。	○	—	—	—
Partial online	Virtual Server は稼働状態ですが、一部のサービスが停止しています。	—	△	△	—
Online pending ^{※1}	起動処理中です。	○	—	—	—
Online ready ^{※2}	クラスタを起動していないので、Virtual Server が起動できません。または、クラスタの停止処理中に障害が発生したのでサービスが正しく稼働していません。 なお、クラスタを起動しても Virtual Server 状態が変わらない場合は、「4.5」の回復方法 6 に従って OS を再起動してください。	○	—	○	○
Offline ^{※2}	停止しています。	○	—	—	—
Offline pending	停止処理中です。	○	—	—	—
Dump	Virtual Server の OS に障害が発生しています。	—	△	△	—
Error	エラーが発生している場合に 표시됩니다。エラー情報を参照して対処してください。	—	△	△	△

(凡例) ○ : 該当する — : 該当しない △ : Virtual Server のエラー情報に対応する

注※1: フェールオーバーの開始から終了までの間にも表示されます。Virtual Server の操作中またはフェールオーバー中に OS が障害で停止して、Virtual Server が正常なノード側にフェールオーバーする場合は、通常と比べて 15 分程度長く表示されることがあります。

注※2: クラスタの状態が「DISABLE」の場合にも表示されます。「Online Ready」または「Offline」と表示された場合には、[Browse Cluster Status] ページ ([Cluster / Node status] 表示) でクラスタの状態もあわせて確認してください。

[< Virtual Server >] サブウィンドウで表示される Virtual Server のエラー情報とエラー情報が表示される要因について次の表に示します。

表 2-6 Virtual Server のエラー情報とエラー情報が表示される要因

エラー情報	説明	エラー情報が表示される要因			
		正常	ハードウェア障害	ソフトウェア障害	誤操作
No error	エラーは発生していません。	○	—	—	—
Internal error	回復できない内部エラーが発生しています。	—	○	○	—
Monitor setup error	監視または監視除外の処理中に障害が発生しています。	—	○	○	—
No available nodes	フェールオーバー先のノードの状態が UP でないため、フェールオーバーできません。	—	○	○	○ [※]

エラー情報	説明	エラー情報が表示される要因			
		正常	ハードウェア障害	ソフトウェア障害	誤操作
Node not available	障害が発生しましたが、すでにフェールオーバーしている状態のため、フェールオーバーできません。	—	○	○	—
Node unknown	ノードの状態が UNKNOWN のため、Virtual Server が起動できません。	—	○	○	—
Execution error	起動または停止処理中にエラーが発生しています。	—	○	○	—
OS error	Virtual Server が起動、停止、再起動、またはフェールオーバーできません。	—	○	○	—
Status unknown	情報の取得に失敗しました。	—	○	○	—
Operation incomplete	電源遮断などによって、Virtual Server の処理が完了していません。	—	○	○	—

(凡例) ○：該当する —：該当しない

注※：片方のノードだけでの運用中に、ネットワーク障害によってリンクの Down 状態が検出された場合です。

フェールオーバー機能で発生する障害は、次のとおり大別できます。

- Virtual Server の起動処理中または停止処理中に発生した障害
- フェールオーバーする契機となった障害
- フェールオーバーが失敗したときの障害

障害が発生した状況に応じて、障害要因を特定する手順が異なります。それぞれの対処を次に示します。

2.4.1 Virtual Server の起動処理中または停止処理中に発生した障害の特定

Virtual Server の起動処理中または停止処理中に障害が発生した場合、[< Virtual Server >] サブウィンドウでエラー状態を確認し、ノード上のシステムメッセージおよび Virtual Server のシステムメッセージを確認して、障害要因を特定してください。

Virtual Server の起動処理中または停止処理中に障害が発生すると、ノード上のシステムメッセージに次のメッセージが出力されていることがあります。

- KAQG72018-E
- KAQG72019-E
- KAQG72020-E
- KAQM34nnn

また、Virtual Server のシステムメッセージには、次のメッセージが出力されていることがあります。

- KAQM35nnn

システム管理者は、メッセージを確認して障害要因を特定してください。

OS が起動してサービスが開始されると、すべてのファイルシステムのマウント処理が実行されます。ファイルシステムの数が多いと、OS が起動してサービスが開始されるまでに時間が掛かります。システム管理者は、OS が起動してサービスが開始されるまでの標準時間を事前に計測しておくことで、障害が発生していることを早期に発見できます。

OS が起動したあと、標準時間を超えてもサービスが開始されない場合、[Browse Cluster Status] ページ ([Cluster / Node status] 表示) でクラスタやノードの状態を確認して、障害要因を特定してください。

ノードの電源を遮断して計画的に HVFP を全面停止した場合、再度電源を入れると、自動的にサービスが開始されます。しかし、次の状態でノードを計画停止 (電源遮断) した場合には、再度電源を入れても、サービスは自動的に開始されません。

- クラスタまたはノードが停止している状態
- リソースグループが停止している状態

2.4.2 フェールオーバーする契機となった障害の特定

フェールオーバーが成功した場合でも、障害を回復しないでフェールオーバーしたまま運用を続けると、アクセス性能が低下したり、障害が再発したときにサービスが停止したりします。フェールオーバーする契機となった障害要因を早急に回復して、通常運用に戻す必要があります。

ノード上のシステムメッセージに KAQG70000-E が出力されている場合、フェールオーバーする契機となった要因として、主に次のことが考えられます。

- 管理 LAN またはフロントエンド LAN での障害が発生している
- もう一方のノードの OS が停止するような障害が発生している
- もう一方のノードで電源障害が発生しているか、ハートビート LAN および管理 LAN 両方で障害が発生している

KAQG70000-E が出力されている場合は、前後のメッセージを確認して障害を特定してください。

なお、KAQG72026-E が出力されている場合は、もう一方のノードで電源遮断の障害が発生しているか、ハートビート LAN および管理 LAN 両方で障害が発生しているおそれがあります。この場合、一方のノードで OS が再起動して、リソースグループがもう一方のノードに強制的にフェールオーバーされてサービスを継続しています。保守員に連絡して、障害を回復してください。

2.4.3 フェールオーバーが失敗したときの障害の特定

フェールオーバーで障害が発生すると、フェールオーバーが失敗して、提供しているサービスが停止します。このとき、フェールオーバーで発生した障害を回復する前に、フェールオーバーする契機となった障害を回復してサービスを再開する必要があります。フェールオーバーする契機となった障害の特定については、「2.4.2 フェールオーバーする契機となった障害の特定」を参照してください。

ノード上のシステムメッセージに、フェールオーバーの失敗を通知するメッセージ (KAQG71000-E) が出力されている場合、次のメッセージを確認することで障害要因を特定できます。

- KAQG72000-E
- KAQG72001-E
- KAQG72002-E
- KAQG72003-E
- KAQG72004-E
- KAQG72005-E

さらに、次のメッセージがノード上のシステムメッセージに出力されていることがあります。

- KAGG72006-E
- KAGG72007-E
- KAGG72009-E
- KAGG72018-E
- KAGG72019-E
- KAGG72020-E
- KAGM34nnn

また、Virtual Server のシステムメッセージには、次のメッセージが出力されていることがあります。

- KAGM35nnn

システム管理者は、メッセージを確認して障害要因を特定してください。

2.5 ファイルシステムのエラー状態を確認する

ファイルシステムに障害が発生した場合、システム管理者は [< Physical Node >] または [< Virtual Server >] サブウィンドウの [ファイルシステム] タブでファイルシステムの状態を確認し、必要な対処を実施してください。

ファイルスナップショット機能を運用している場合は、差分スナップショットの状態も表示されません。

「Online (RW)」が表示された場合

読み取りと書き込みが許可された状態でマウントされています。

「Online (RO)」が表示された場合

読み取り専用でマウントされています。

「Unmounted」が表示された場合

アンマウントされています。

「Expanding」が表示された場合

ファイルシステムを拡張する処理を実行中か、処理でエラーが発生しています。しばらくたってから、Processing Node または Virtual Server の情報を更新してください。状態が変わらない場合は、処理でエラーが発生しているおそれがあります。全ログデータを取得して、保守員に連絡してください。

「Reclaiming」が表示された場合

ファイルシステムが使用している仮想 LU の未使用領域を解放中です。

「Data corrupted」が表示された場合

OS の障害またはプールの容量不足によってファイルシステムが閉塞しています。

「4.8 ファイルシステムの障害を回復する」を参照して対処してください。

「Device error」が表示された場合

LU の障害（ドライブの多重障害）によってファイルシステムが閉塞しています。

「4.8 ファイルシステムの障害を回復する」を参照して対処してください。

「File snapshots error」が表示された場合

差分格納デバイスに障害が発生しています。

差分格納デバイスの状態を確認し、「4.9 差分格納デバイスの障害を回復する」を参照して対処してください。

「File snapshots out of capacity」が表示された場合

差分格納デバイスの容量不足によって、差分スナップショットが無効になっています。

差分格納デバイスの状態を確認し、「4.9 差分格納デバイスの障害を回復する」を参照して対処してください。

「Blocked」が表示された場合

差分格納デバイスの容量不足によって、ファイルシステムがブロックされています。

差分格納デバイスの状態を確認し、「4.9 差分格納デバイスの障害を回復する」を参照して対処してください。

「Blocked and ready」が表示された場合

ファイルシステムがブロック状態になってから、差分格納デバイスの空き容量を確保したあとに、OS が再起動されていません。OS を再起動してください。

システム管理者は、障害が発生した前後のシステムメッセージを [Check for Errors] ダイアログの [List of RAS Information] ページ ([List of messages] 表示) で確認し、要因を特定します。要因に応じて、「4.8 ファイルシステムの障害を回復する」に従って対処してください。

2.6 差分格納デバイスのエラー状態を確認する

差分格納デバイスに障害が発生した場合、[差分格納デバイスの状態] を参照して、差分格納デバイスの状態を確認し、必要な対処を実施してください。

「Busy (<進捗>% processed)」が表示された場合

バックグラウンド処理を実行しています。

バックグラウンド処理が完了してから、操作を再度実行してください。

「Purging」が表示された場合

すべての差分スナップショットを削除する処理を実行中か、処理でエラーが発生しています。

しばらくたってから、ファイルスナップショットの情報を更新してください。状態が変わらない場合は、処理でエラーが発生しているおそれがあります。処理でエラーが発生している場合は、すべての差分スナップショットを削除する処理を再実行してください。

「Expanding」が表示された場合

差分格納デバイスを拡張する処理を実行中か、処理でエラーが発生しています。

しばらくたってから、ファイルスナップショットの情報を更新してください。状態が変わらない場合は、処理でエラーが発生しているおそれがあります。処理でエラーが発生している場合は、syncexpand コマンドを実行して、差分格納デバイスの拡張処理のリカバリーを実施してください。

「In processing or error」が表示された場合

差分格納デバイスの設定または解除の処理を実行中か、処理でエラーが発生しています。

しばらくたってから、ファイルスナップショットの情報を更新してください。状態が変わらない場合は、処理でエラーが発生しているおそれがあります。処理でエラーが発生している場合は、差分格納デバイスを解除してください。HFRR ペアとして定義したファイルシステムの場合は、HFRR ペアを解除してから差分格納デバイスを解除してください。

「Warning」が表示された場合

差分格納デバイスの使用量が警告閾値以上になっています。

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、差分格納デバイスの空き容量を確保してください。

「Overflow」が表示された場合

差分格納デバイスの容量が不足したため、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が無効になっています。

「4.9.1 差分格納デバイスの容量が不足した場合（状態が **Overflow** のとき）」の手順に従って対処してください。

「Blocked」が表示された場合

差分格納デバイスの容量が不足したため、差分格納デバイスを設定したファイルシステムがブロックされています。

「4.9.2 差分格納デバイスの容量が不足した場合（状態が **Blocked** のとき）」の手順に従って対処してください。

「Blocked and busy (<進捗>% processed)」が表示された場合

ファイルシステムがブロックされている状態で、バックグラウンド処理を実行しています。バックグラウンド処理が完了してから、操作を再度実行してください。

「Blocked and expanding」が表示された場合

ファイルシステムがブロックされている状態で、差分格納デバイスを拡張する処理を実行中か、処理でエラーが発生しています。

しばらくたってから、ファイルスナップショットの情報を更新してください。状態が変わらない場合は、処理でエラーが発生しているおそれがあります。処理でエラーが発生している場合は、syncexpand コマンドを実行して、差分格納デバイスの拡張処理のリカバリーを実施してください。

「Not available」が表示された場合

ファイルシステムまたは差分格納デバイスの論理ボリュームに障害が発生しています。また、クラスタ、ノード、リソースグループまたは **Virtual Server** が正常に稼働していない場合に、「Not available」が表示されることもあります。

[Cluster Management] ダイアログの [Browse Cluster Status] ページでクラスタ、ノードおよびリソースグループの状態を確認してください。または、[< Virtual Server >] サブウィンドウで **Virtual Server** の状態を確認してください。状態に問題がない場合は、保守員に連絡して、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にアクセス障害が発生していないか確認してください。障害の要因がデバイスファイルのアクセス障害にあると保守員が判断した場合は、「4.9.3 デバイスファイルにアクセス障害が発生した場合 (**Virtual Server** 未使用時)」または「4.9.4 デバイスファイルにアクセス障害が発生した場合 (**Virtual Server** 使用時)」の手順に従って対処してください。

「Offline」が表示された場合

クラスタ、ノードまたはリソースグループが正常に稼働していません。

[Cluster Management] ダイアログの [Browse Cluster Status] ページでクラスタ、ノードおよびリソースグループの状態を確認して、対処してください。

「I/O error」が表示された場合

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に障害が発生しているおそれがあります。

デバイスファイルにアクセス障害が発生しているかどうか保守員に確認してください。障害の要因がデバイスファイルのアクセス障害にあると保守員が判断した場合は、「4.9.3 デバイスファイルにアクセス障害が発生した場合 (**Virtual Server** 未使用時)」または「4.9.4 デバイス

ファイルにアクセス障害が発生した場合 (Virtual Server 使用時)」の手順に従って対処してください。

「System error」が表示された場合

全ログファイルを採取して、保守員に連絡してください。

上記以外の差分格納デバイスの状態については、「ユーザーズガイド」を参照してください。

障害の要因を特定できない場合は、「3.2 ノードおよび Virtual Server のログファイルの採取方法」の手順に従って全ログファイルを一括で採取したあと、保守員に連絡してください。

2.7 ユーザーマッピングの情報を確認する

ユーザーマッピングを使用しているときに、エンドユーザーが CIFS サービスを利用できない場合、ユーザー ID やグループ ID が正しく割り当てられていないおそれがあります。この場合、システム管理者は次のことを確認してください。

- CIFS サービスの構成定義が両ノードで同じである
[Access Protocol Configuration] ダイアログの [CIFS Service Maintenance] ページで、適用されている CIFS サービスの構成定義が両ノードで同じであることを確認します。
- CIFS サービスが正しく稼働している
[Access Protocol Configuration] ダイアログの [List of Services] ページで、CIFS サービスの [Status] に「Running」と表示されていることを確認します。
- ノードまたは Virtual Server がドメインコントローラーに接続されている
[Access Protocol Configuration] ダイアログの [CIFS Service Maintenance] ページで、[DC server connection status] に「Connectable」と表示されていることを確認します。
- ドメイン間に信頼関係が構築されている
登録したドメイン間に信頼関係が構築されているか検証します。例えば、ドメインコントローラーに Windows Server 2003 を使用している場合、Windows の管理ツールで信頼関係を確認できます。
- 最新のユーザー情報が適用されている
ドメインコントローラーで管理しているユーザー情報やグループ情報を変更したあとすぐに、エンドユーザーが CIFS 共有にアクセスすると、古いユーザー情報やグループ情報が適用されることがあります。
ユーザーを再作成するなど、ドメインコントローラーで管理しているユーザー情報やグループ情報を変更した場合は、それらの情報を更新するために、CIFS サービスを再起動するか、5 分経過してから CIFS 共有にアクセスするようエンドユーザーに連絡してください。

特に問題がない場合、システム管理者は次の作業を実施してください。

- [Access Protocol Configuration] ダイアログの [CIFS Service Maintenance] ページで、キャッシュされているユーザーマッピング情報を削除する
- 5 分程度待つてから再度 CIFS 共有にアクセスするよう、エンドユーザーに連絡する

このほか、使用しているユーザーマッピングの方式に応じて、次のことを確認してください。

2.7.1 RID 方式のユーザーマッピングを使用している場合

RID 方式のユーザーマッピングを使用している場合、次のことを確認してください。

- CIFS サービスを利用するユーザーが所属しているドメインが、File Services Manager に設定されている
 ノードまたは Virtual Server が参加しているドメインと直接信頼関係を結んでいるが File Services Manager に設定されていないドメインに所属しているユーザーは、HVFP が提供する CIFS サービスを利用できません。
 [Access Protocol Configuration] ダイアログの [CIFS Service Maintenance] ページの [User mapping information] で、ドメインが設定されていることを確認してください。
- CIFS サービスを利用するユーザーやグループの ID が、ドメインごとに設定したユーザー ID やグループ ID の範囲内にある
 ユーザー ID やグループ ID が [Access Protocol Configuration] ダイアログの [CIFS Service Management] ページ (Setting Type : User mapping) の [User mapping setup] で設定した範囲に含まれないユーザーは、CIFS サービスを利用できません。
 File Services Manager のコマンドを使用して、ユーザーやグループの名称から RID 方式でマッピングされた ID に変換できることを確認してください。

2.7.2 LDAP 方式のユーザーマッピングを使用している場合

LDAP 方式のユーザーマッピングを使用している場合、次のことを確認してください。

- LDAP サーバが正しく稼働している
 [Access Protocol Configuration] ダイアログの [CIFS Service Management] ページ (Setting Type : User mapping) で設定した LDAP サーバが正しく稼働しているか確認します。
- 割り当てられたユーザー ID やグループ ID の最大値が、設定したユーザー ID やグループ ID の範囲内にある (自動的に割り当てている場合)
 [Check for Errors] ダイアログの [List of RAS Information] ページ ([Batch-download] 表示) で、ユーザーマッピング情報ロググループを一括ダウンロードし、CIFS サービスを利用できないエンドユーザーに対してユーザー ID やグループ ID が割り当てられているか確認してください。CIFS サービスを利用できないエンドユーザーに ID が割り当てられていない場合、[Access Protocol Configuration] ダイアログの [CIFS Service Maintenance] ページの [Largest currently used UID] および [Largest currently used GID] に表示されている ID の最大値が、[Range of UIDs] および [Range of GIDs] に表示されている ID の範囲の最大値と同じ値となっていないか確認してください。
- ユーザー ID およびグループ ID が正しく割り当てられている (手動で割り当てている場合)
 [Check for Errors] ダイアログの [List of RAS Information] ページ ([Batch-download] 表示) で、ユーザーマッピング情報ロググループを一括ダウンロードし、CIFS サービスを利用できないエンドユーザーに対して、200~2147483147 の範囲でユーザー ID やグループ ID が割り当てられているか確認してください。

2.7.3 Active Directory スキーマ方式のユーザーマッピングを使用している場合

Active Directory スキーマ方式のユーザーマッピングを使用している場合、次のことを確認してください。

- ドメインコントローラーの Active Directory が正しく稼働している
 冗長化されたものを含む、すべてのドメインコントローラーで使用している Active Directory スキーマおよび設定ファイルが正しいことを確認します。
- ユーザー ID およびグループ ID が正しく割り当てられている
 ドメインコントローラーに、CIFS サービスを利用できないエンドユーザーに対して、200~2147483147 の範囲でユーザー ID やグループ ID が割り当てられているか確認してください。

- ノードが参加しているドメインと信頼関係を結んでいるドメインが定義されている
信頼関係を結んでいるドメインの一覧を確認し、ドメインが表示されていない場合は再定義してください。

2.8 管理サーバの稼働状態を確認する

管理サーバの稼働状態、管理サーバに出力されているログファイル、ネットワークの状態などを確認します。管理サーバで障害が発生している場合は、Hitachi Command Suite 共通コンポーネントおよび Hitachi File Services Manager のログファイルを確認して、要因を特定します。

Hitachi Command Suite 共通コンポーネントおよび Hitachi File Services Manager のログファイルを次に示します。

表 2-7 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

ログファイル	出力先	説明	
Hitachi Command Suite 共通コンポーネントのログ	統合トレースログファイル	<システムドライブ> ¥Program Files¥Hitachi ¥HNTRLib2¥spool¥hntnr2 <n> .log	Hitachi File Services Manager のトレースログのうち、重要度が高いものが出力されます。管理サーバに Hitachi Command Suite 製品がインストールされている場合は、各 Hitachi Command Suite 製品のトレースログも出力されます。
	イベントログ	イベントビューアー	Hitachi File Services Manager のメッセージログのうち、重要度が高いものが出力されます。管理サーバに Hitachi Command Suite 製品がインストールされている場合は、各 Hitachi Command Suite 製品のイベントログも出力されます。
Hitachi File Services Manager のログ	メッセージログ	< Hitachi File Services Manager のインストールフォルダ>¥logs¥HFMS_Message <n> .log	Hitachi File Services Manager のメッセージが出力されます。システム管理者の操作履歴が記録されます。

統合トレースログファイルおよび Hitachi File Services Manager のメッセージログは次の形式で出力されます。

```
<通番> <日付> <時刻> <プログラム名> <プロセス ID> <スレッド ID> <メッセージ ID>
<イベント種別> <メッセージテキスト>
```

統合トレースログファイルおよび Hitachi File Services Manager のメッセージログに出力される情報を次に示します。

表 2-8 管理サーバ上の統合トレースログファイルおよび Hitachi File Services Manager のメッセージログに出力される情報

項目	内容
通番	メッセージログファイル内のメッセージの通番が出力されます。
日付	メッセージが出力された日付が「YYYY/MM/DD」の形式で出力されます。
時刻	メッセージが出力された時刻が「hh:mm:ss.sss」の形式で出力されます。
プログラム名	コンポーネント名やコマンド名が出力されます。 Hitachi File Services Manager に関するログには「FileServicesManager」と出力されます。

項目	内容
プロセス ID	ログを出力したプロセスの ID が 16 進数で出力されます。
スレッド ID	ログを出力したスレッドの ID が 16 進数で出力されます。
メッセージ ID	メッセージ ID が出力されます。
イベント種別	トレース出力の契機となったイベント種別が出力されます。
メッセージテキスト	メッセージの内容が出力されます。

イベントログは次の形式で出力されます。

```
<日付> <時刻> <種類> <ユーザー> <コンピュータ> <ソース> <分類> <イベント ID > <説明>
```

イベントログに出力される情報を次に示します。

表 2-9 イベントログに出力される情報

項目	内容
日付	メッセージが出力された日付が「YYYY/MM/DD」の形式で出力されます。
時刻	メッセージが出力された時刻が「hh:mm」の形式で出力されます。
種類	次の 3 つの種類があります。 <ul style="list-style-type: none"> • 情報 • 警告 • エラー
ユーザー	「N/A」と出力されます。
コンピュータ	コンピュータ名が表示されます。
ソース	「HBase Storage Mgmt Log」と出力されます。
分類	「なし」と出力されます。
イベント ID	「1」と出力されます。
説明	次の形式で出力されます。 HFSM [<プロセス ID >]: <メッセージ ID > <メッセージテキスト>

2.9 サーバとの接続に問題がないか確認する

HVFP で使用している次のサーバの状況やネットワーク構成を確認し、ノードまたは Virtual Server の接続に問題が発生していないかを確認します。

- DNS サーバ※
- NIS サーバ※
- NTP サーバ※
- LDAP サーバ
- CIFS クライアントの認証サーバ（ドメインコントローラーまたは Windows NT サーバ）
- NFS クライアントの認証サーバ（KDC サーバ）

システム管理者は、[Check for Errors] ダイアログの [List of RAS Information] ページ ([Server check] 表示) で、ノードまたは Virtual Server と各サーバとの接続状況を確認してください。ノードまたは Virtual Server と各サーバの接続状態を確認する方法については、「付録 B. ネットワーク情報」を参照してください。

注※：ノードまたは Virtual Server とサーバの接続の問題を解決したら、必ずノードの OS を再起動してください。

2.10 DNS による名前解決に問題がないか確認する

システム管理者は、dig コマンドを使用して、DNS による名前解決に問題がないかを確認します。

DNS による名前解決に問題がないかを確認する手順を次に示します。

1. ssh コマンドを実行して、対象のノードまたは Virtual Server にログインします。
2. dig コマンドを実行して、DNS による名前解決に問題がないか確認します。
dig コマンドは、次に示すオプションを指定して実行してください。ほかのオプションは指定しないでください。

正引きの場合：

```
$ dig +time=5 +tries=2 @<DNSサーバのIPアドレス> <名前解決するホストの名称>
```

逆引きの場合：

```
$ dig +time=5 +tries=2 @<DNSサーバのIPアドレス> -x <名前解決するホストのIPアドレス>
```

dig コマンドの実行例を次に示します。システム管理者は、DNS による名前解決に問題がないか、「ANSWER SECTION」を確認してください。

正引きの場合：

```
$ dig +time=5 +tries=2 @10.208.148.103 win104.temp.local

;<<<>> DiG 9.2.4 <<<>> +time=5 +tries=2 @10.208.148.103 win104.temp.local
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61734
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;win104.temp.local.                IN      A

;; ANSWER SECTION:
win104.temp.local.                3600   IN      A      10.208.148.104

;; Query time: 1 msec
;; SERVER: 10.208.148.103#53(10.208.148.103)
;; WHEN: Mon Jul  6 12:26:40 2009
;; MSG SIZE rcvd: 51
```

逆引きの場合：

```
$ dig +time=5 +tries=2 @10.208.148.103 -x 10.208.148.104

;<<<>> DiG 9.2.4 <<<>> +time=5 +tries=2 @10.208.148.103 -x 10.208.148.104
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9459
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;104.148.208.10.in-addr.arpa.     IN      PTR

;; ANSWER SECTION:
104.148.208.10.in-addr.arpa.     3600   IN      PTR    win104.temp.local.

;; Query time: 0 msec
;; SERVER: 10.208.148.103#53(10.208.148.103)
;; WHEN: Mon Jul  6 12:26:46 2009
;; MSG SIZE rcvd: 76
```

DNS サーバが正常に応答していない場合は、DNS サーバのレコード、ゾーン、再帰の設定などを見直してください。

なお、ネットワークを介してリモートの HCP と連携している場合に、上記の手順で問題が特定できないときは、「4.11 HCP へのアクセス障害を回復する」に従って対処してください。

2.11 FC パスの状態を確認する

GUI で FC パスの状態を確認して、FC パスに問題が発生していないかどうかを確認します。fpstatus コマンドで FC パスの状態を確認することもできます。FC パスに障害が発生している場合は、「4.17 FC パスの障害を回復する」に従って対処してください。

2.12 ハードウェアの状態を確認する

GUI でハードウェアの状態を確認して、ハードウェアに問題が発生していないかどうかを調査します。コマンドを使用する場合は hwstatus コマンドおよび fpstatus コマンドを実行してください。

ハードウェアの状態が正常でない場合は、「4.21 ハードウェアの障害を回復する」に従って対処してください。

2.13 HCP との接続状態を確認する

HVFP からデータをマイグレートしている HCP と接続できるかどうかを確認します。hcpaccesstest コマンドを実行してください。

2.14 管理ポートおよび BMC ポートの通信を確認する

保守員から管理ポートおよび BMC ポートの通信の確認を依頼された場合、管理ポートおよび BMC ポートに対して ping コマンドを実行します。

確認手順を実行する前に、次の「表 2-10 管理ポートおよび BMC ポートの通信確認ワークシート」の様式のワークシートを準備してください。各手順で確認した情報をこのワークシートに記入します。

表 2-10 管理ポートおよび BMC ポートの通信確認ワークシート

	ノード 0		ノード 1	
	管理ポート	BMC ポート	管理ポート	BMC ポート
IP アドレス				
実行結果				

管理ポートおよび BMC ポートの通信を確認する方法を次に示します。

1. 両ノードの管理ポートの IP アドレスおよび BMC ポートの IP アドレスを取得し、ワークシートに記入します。

GUI で管理ポートの IP アドレス（管理 IP アドレス）を確認します。BMC ポートの IP アドレスは bmcctl コマンドで確認します。

2. 手順 1. で取得した IP アドレスを使用して、管理コンソールから両ノードの管理ポートおよび BMC ポートに対して ping コマンドを実行し、結果をワークシートに記入します。

Windows のコマンドプロンプトでの実行結果（成功例および失敗例）を次に示します。

成功例（応答あり）：

```
C:\>ping 192.168.0.20

Pinging 192.168.0.20 with 32 bytes of data:

Reply from 192.168.0.20: bytes=32 time<1ms TTL=128
Reply from 192.168.0.20: bytes=32 time<1ms TTL=128
Reply from 192.168.0.20: bytes=32 time<1ms TTL=128
Reply from 192.168.0.20: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.0.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
```

失敗例（応答なし）：

```
C:\>ping 192.168.0.20

Pinging 192.168.0.20 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.0.20:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

一度でも「Request timed out.」が出力された場合は、一時的に OS に負荷が掛かっていることも考えられるので、再度実行して同じ結果が出力されるかどうか確認してください。また、結果が出力され続けて終了しない場合は、[Ctrl] + [C] キーを押して中断してください。

結果を確認したあと、ワークシートの実行結果のセルに、成功の場合は「○」、失敗の場合は「×」を記入してください。ワークシートの記入例を次に示します。

表 2-11 管理ポートおよび BMC ポートの通信確認ワークシートの記入例

	ノード 0		ノード 1	
	管理ポート	BMC ポート	管理ポート	BMC ポート
IP アドレス	192.168.0.20	192.168.0.22	192.168.0.21	192.168.0.23
実行結果	○	○	×	○

(凡例) ○：成功 ×：失敗

3. 保守員から確認を依頼された場合は、確認結果を連絡します。

2.15 NTP による時刻同期に問題がないか確認する

NTP による時刻同期に問題がないかを確認します。[Check for Errors] ダイアログの [List of RAS Information] ページ ([List of other log files] 表示) で、デーモンログ (/var/log/daemon.log) の出力内容を表示し、「synchronized to <文字列>」というメッセージのうち、最後に出力されたものを確認してください。

<文字列>が NTP サーバの IP アドレスの場合

NTP サーバと時刻同期ができています。

例：Oct 19 13:29:36 D7BQLNBX ntpd[10874]: synchronized to 158.214.125.24, stratum 2

<文字列>が「LOCAL(1)」、「LOCAL(2)」またはもう一方のノードの管理ポートの IP アドレスの場合

NTP サーバと時刻同期ができていません。

```
例: Oct 20 01:20:14 D7BQLNBX ntpd[32302]: synchronized to LOCAL(1),
stratum 13
```

確認後、8時間以上経過しても「synchronized to < NTP サーバの IP アドレス>」というメッセージが出力されない場合は、次のことを確認してください。

- ノードと NTP サーバの接続状態が正常であること
- NTP サーバの環境設定が正しく行われていること

ノードと NTP サーバの接続状態を確認する方法については「付録 B. ネットワーク情報」を参照してください。NTP サーバの環境設定については、「システム構成ガイド (NTP サーバの環境設定)」を参照してください。

2.16 バックアップ管理ソフトウェアの状態および設定を確認する

バックアップまたはリストアを実行できない場合は、障害の要因がバックアップサーバ、メディアサーバ、バックアップ管理ソフトウェアの設定などにあることも考えられます。

バックアップサーバやメディアサーバなどでエラーメッセージやログを確認して、要因を特定してください。バックアップ管理ソフトウェアでエラーメッセージやログを確認する方法については、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。

2.16.1 バックアップサーバおよびメディアサーバでエラーメッセージやログを確認する

バックアップサーバには、Backup Restore とファイルスナップショットのメッセージも通知されます。Backup Restore のメッセージのメッセージ ID は「KAQB」で、ファイルスナップショットのメッセージのメッセージ ID は「KAQS」で始まります。

2.16.2 バックアップまたはリストアの実行結果を確認する

バックアップまたはリストアの実行結果をバックアップ管理ソフトウェアで確認します。詳細については、HVFP に添付されている Backup Restore の補足資料を参照してください。

2.16.3 バックアップ管理ソフトウェアの設定内容を確認する

バックアップサーバおよびメディアサーバに設定した情報が正しいかどうかを確認してください。バックアップサーバおよびメディアサーバの環境設定については、HVFP に添付されている Backup Restore の補足資料を参照してください。

2.16.4 テープドライブの状態を確認する

ノードに SAN で接続されたテープ装置を使用する場合、ネットワークや SAN で障害が発生したり、OS の負荷が高くなったりすると、バックアップ管理ソフトウェアでテープドライブが使用できない状態になることがあります。

このような現象が発生した場合には、負荷を軽減するなど、HVFP の運用を見直してください。テープドライブを使用できる状態にする方法については、HVFP に添付されている Backup Restore の補足資料を参照してください。

2.17 同じテープ装置を接続しているほかのノードの OS の状態を確認する

バックアップまたはリストア処理がエラー終了した場合は、テープ装置を共有しているほかのノードで、OS が起動または再起動されていないことを確認します。

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している場合、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。

ほかのノードで OS が起動または再起動されていた場合は、起動または再起動が完了したあとに、再度バックアップまたはリストアを実行してください。

2.18 ノードに SAN で接続されたテープ装置の状態を確認する

ノードに SAN で接続されたテープ装置を使用している場合は、次の手順でテープドライブの状態を確認します。

1. オプションを指定しないで `tapelist` コマンドを実行します。
テープドライブの登録状況を確認します。

Status の右の項目に「B」と表示された場合

コマンドを実行したノードまたは **Virtual Server** で、テープドライブとノードの接続が閉塞状態になっています。閉塞状態を解消してください。閉塞状態を解消する方法については、「4.24.4 テープドライブとノードの接続が閉塞状態になっている場合」を参照してください。

Status の右の項目に「I」と表示された場合

コマンドを実行したノードまたは **Virtual Server** で、テープドライブの登録情報が無効になっています。 `tapeadd` コマンドでテープドライブの登録情報を有効にしてください。
テープドライブの登録情報を有効に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。

上記以外の場合

バックアップ管理ソフトウェアで、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処理が実行中でないことを確認してから、手順 2. に進みます。

2. `-A`, `-d` および `-t WWN:LUN` オプションを指定して `tapelist` コマンドを実行します。
`WWN:LUN` に指定したテープドライブの接続状況を確認します。

テープドライブの情報が表示されない場合、または Status の左の項目に「N」と表示された場合

次の要因が考えられます。

- テープ装置の電源が入っていない
- ノード、FC スイッチおよびテープ装置が正しく接続されていない
- FC スイッチのゾーニング設定に誤りがある
- FC ケーブルが断線している
- FC スイッチまたはテープ装置が故障している
- コマンドを実行したノードまたは **Virtual Server** 以外で、テープドライブとの接続が閉塞状態になっているノードまたは **Virtual Server** が存在する

システム管理者は、SAN 管理者と連携して、必要な対処をしてください。FC スイッチおよびテープ装置については、それぞれのベンダーから提供されたドキュメントを参照してください。

また、テープドライブとの接続が閉塞状態になっているノードまたは Virtual Server が存在する場合は、「4.24.4 テープドライブとノードの接続が閉塞状態になっている場合」を参照して、閉塞状態を解消してください。

これらの問題がない場合は、ノードの FC ポートまたは OS に障害が発生しているおそれがあります。障害が発生した時点の障害情報を取得して、保守員に連絡してください。

Status に「D,D」と表示された場合

テープドライブが NDMP サーバに登録されていません。-t オプションと WWN:LUN を指定して、テープドライブを個別に NDMP サーバに登録してください。

Model および Type に「Error」と表示された場合

テープ装置に問題があるおそれがあります。ベンダーから提供されたドキュメントを参照し、必要な対処をしてください。

これらの問題がない場合は、一時的な問題のおそれがあるため、再度バックアップまたはリストアを実行してください。問題が解決しない場合は、障害が発生した時点の障害情報を取得して、保守員に連絡してください。

2.19 HFRR ペアの状態を確認する

ruspairlist コマンドで HFRR ペアの状態に問題が発生していないか確認します。

Pair status に cancel-error, copy-error または restore-error と表示された場合は、Hitachi File Remote Replicator の機能で障害が発生しています。[Check for Errors] ダイアログの [List of RAS Information] ページ ([List of other log files] 表示) で、Hitachi File Remote Replicator ログ (/enas/log/rus.log) の出力内容を確認し、要因を特定してください。

Hitachi File Remote Replicator ログ (/enas/log/rus.log) に KAQR20742-E メッセージが出力されている場合、セカンダリーサイトの差分格納デバイスに十分な空き容量がありません。直前の KAQR20750-I メッセージで出力された処理対象の差分データ量を超える空き容量が必要です。[File Snapshots 編集] ダイアログの [ストレージ] タブで差分格納デバイスを拡張するか、[<ファイルシステム>] サブウィンドウの [File Snapshots] タブで不要な差分スナップショットを削除して、処理対象の差分データ量を超える空き容量を確保してください。

障害情報の収集と保守員への連絡

この章では、ログファイルの採取方法について説明します。

システム管理者は、障害の発生元や要因を特定できなかつたり、対処できない障害が発生したりした場合は、障害情報を採取して、保守員へ送付する必要があります。HVFPの障害要因の解析には、次のログファイルが必要です。

- 管理サーバのログファイル
- ノードのログファイル
- ノードの core ファイルおよびダンプファイル
- Virtual Server のログファイル
- Virtual Server の core ファイルおよびダンプファイル

また、Hitachi File Services Manager のインストール時またはアンインストール時に発生した障害の要因を解析するには、インストーラーおよび管理サーバのログファイルが必要です。

このほか、ネットワーク障害の要因を解析するにはパケットトレースのログファイル、CIFS サービスの性能を解析するには CIFS サービスの性能解析用ログファイルが必要です。

- [3.1 管理サーバのログファイルの採取方法](#)
- [3.2 ノードおよび Virtual Server のログファイルの採取方法](#)
- [3.3 Hitachi File Services Manager のインストーラーのログファイルの採取方法](#)
- [3.4 パケットトレースのログファイルの採取方法](#)
- [3.5 CIFS サービスの性能解析用ログの採取方法](#)

3.1 管理サーバのログファイルの採取方法

次のどちらかの方法で、管理サーバ上のログファイルを一括採取できます。

- Windows のメニューから実行する
- コマンドを使用する

注意：

Windows のメニューから実行した場合は、次のログファイルだけが一括採取されます。

- Hitachi Command Suite 共通コンポーネントのログファイル
- Hitachi File Services Manager のログファイル

Device Manager の GUI にログインして HVFP を運用・管理している場合など、Hitachi Command Suite 製品のログファイルが必要なときには、コマンドを使用して一括採取してください。

管理サーバ上のログファイルの採取処理は、同時に複数実行しないでください。

なお、ログファイル採取の結果としてメッセージ KAPM05318-I または KAPM05319-E が出力されない場合、ログファイルの格納先フォルダに十分な空き容量がないため処理が途中で終了しています。ログファイルの格納先フォルダに十分な空き容量を確保したあとで、再度採取してください。

3.1.1 Windows のメニューから実行する場合

Windows のメニューから実行する場合、Hitachi Command Suite 共通コンポーネントおよび Hitachi File Services Manager のログファイルが次のフォルダに格納されます。

<Hitachi File Services Manager のインストールフォルダ>\log_archive

ログファイルは、次の名称でアーカイブされます。

- HiCommand_log.jar
- HiCommand_log.hdb.jar
- HiCommand_log.db.jar
- HiCommand_log.csv.jar

Windows のメニューから実行する場合に、管理サーバ上のログファイルを採取する方法を次に示します。

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] - [Get Logs - 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 [Get Logs - HFSM] を選択します。

コマンドプロンプトに処理経過が表示されます。なお、すでに log_archive ディレクトリが存在していた場合は、削除を確認するメッセージが表示されます。

3. 処理が完了したら、何かキーを押してコマンドプロンプトを閉じます。

3.1.2 コマンドを使用する場合

コマンドを使用した場合は、Hitachi Command Suite 共通コンポーネントと Hitachi File Services Manager のログファイル以外に、管理サーバにインストールされた Hitachi Command Suite 製品のログファイルも採取できます。

コマンドを使用して、管理サーバ上のログファイルを採取する方法を次に示します。

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. 次のとおりコマンドを実行して、ログを採取します。

hcmdsgetlogs コマンドを実行すると、次のアーカイブファイルが作成されます。

- <アーカイブファイル名>.jar
- <アーカイブファイル名>.hdb.jar
- <アーカイブファイル名>.db.jar
- <アーカイブファイル名>.csv.jar

```
< Hitachi Command Suite 共通コンポーネントのインストールフォルダ>%bin
%hcmdsgetlogs /dir <ログファイルの出力先フォルダ> [/types <製品名>[<製品名>
...]] [/arc <アーカイブファイル名>] [/logtypes <ログファイル種別>[<ログファイル種
別>...]]
```

/dir

ログファイルを出力するローカルディスク上のフォルダ（ログファイルの出力先フォルダ）を指定します。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。

ログファイルの出力先フォルダは、/types オプションを省略する場合は 41 バイト以内、/types オプションに FileServicesManager を指定する場合は 33 バイト以内のパスで指定してください。Hitachi Command Suite 製品のログファイルを採取する場合の最大長については、各製品のマニュアルを参照してください。

ログファイルの出力先フォルダに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。パスにスペースが含まれる場合は、パスの前後に引用符 (") を指定してください。パスの区切り文字として、円記号 (¥), コロン (:) および斜線 (/) が使用できます。ただし、文字列の末尾には区切り文字を指定できません。

/types <製品名>[<製品名>…]

障害の発生や格納先の容量を確保できないなどの理由で、特定の製品のログファイルしか採取できない場合に、採取する製品の名称を指定します。Hitachi Command Suite 共通コンポーネントおよび Hitachi File Services Manager のログだけを採取する場合は、FileServicesManager または HFMSM を指定します。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。複数の製品名を指定する場合は、半角スペースで区切ってください。

このオプションを省略すると、Hitachi Command Suite 共通コンポーネントと Hitachi File Services Manager のログファイルに加えて、管理サーバ上のすべての Hitachi Command Suite 製品のログファイルも採取できます。Device Manager の GUI にログインして HVFP を運用・管理している場合は、指定を省略してください。

/arc

アーカイブファイル名を指定します。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。指定を省略した場合には「HiCommand_log」という名称でファイルが出力されます。

コマンドを実行すると、/dir オプションで指定したフォルダの直下にアーカイブファイルが作成されます。

/logtypes <ログファイル種別>[<ログファイル種別>…]

障害や格納先の容量を確保できないなどの理由で、特定の種別のログファイルしか採取できない場合に、採取するログファイルの種別を指定します。複数の種別を指定する場合は、半角スペースで区切ってください。種別として指定する値と作成されるアーカイブファイルの関係の関係を次に示します。

表 3-1 種別として指定する値と作成されるアーカイブファイルの関係

種別として指定する値	作成されるアーカイブファイル
log	.jar および .hdb.jar ファイル
db	.db.jar ファイル
csv	.csv.jar ファイル

このオプションを省略した場合、種別としてすべての値を指定したのと同じ結果になります。なお、/types オプションとともにこのオプションを指定する場合は、種別として指定する値に必ず log を含めてください。

3.2 ノードおよび Virtual Server のログファイルの採取方法

システム管理者は、File Services Manager の GUI を利用して、ノードおよび Virtual Server のログファイルをダウンロードできます。

メッセージや保守員の指示に従い、[Check for Errors] ダイアログの [List of RAS Information] ページで全ログデータ (All log data) をダウンロードして、保守員に送付してください。

システムメッセージ、システムログおよびその他のログファイルを一括ダウンロードする手順を次に示します。

1. メイン画面のエクスプローラメニューで [リソース] - [Processing Node] を選択します。
2. オブジェクトツリーで対象のノードまたは Virtual Server を選択し、表示された画面の [設定] タブの [ベーシック] サブタブで [エラーチェック] をクリックします。
3. [Check for Errors] ダイアログの [List of RAS Information] ページの [Info. type] ドロップダウンリストで [Batch-download] を選択して、[Display] ボタンをクリックします。
4. 一括ダウンロードするロググループをラジオボタンで選択して、[Download] ボタンをクリックします。

注：PSB ロググループを選択した場合は、ダウンロードダイアログが表示される前に、一括ダウンロードを確認するダイアログが表示されます。

5. WWW ブラウザーのダウンロードダイアログで、ダウンロード先を指定します。
選択したロググループに属するログファイルが、tar でアーカイブされ、gzip で圧縮された形式で、指定したダウンロード先にダウンロードされます。
6. ダウンロードダイアログの [Close] ボタンをクリックします。

なお、一括ダウンロードを実行した際、Internet Explorer の「インターネット一時ファイル」の格納先フォルダの容量が不足した場合はデータが欠落します。このとき、Internet Explorer ではエラーにはならず、メッセージも通知されません。

3.3 Hitachi File Services Manager のインストーラーのログファイルの採取方法

次のどちらかの方法で管理サーバ上のログファイルを一括採取することで、Hitachi File Services Manager のインストール時またはアンインストール時に障害が発生した場合に必要なログファイルを採取できます。

- Windows のメニューから実行する
- コマンドを使用する

管理サーバ上のログファイルを一括採取する手順については、「3.1 管理サーバのログファイルの採取方法」を参照してください。

管理サーバ上のログファイルを一括採取できない場合は、次のログファイルを格納先のフォルダから採取して、保守員に送付してください。

Setup.ilg

次のフォルダに格納されます。なお、< ID >は、Hitachi File Services Manager のインストーラーが内部的に付与するプロダクトコードです。

< Windows のシステムドライブ >:\Program Files\InstallShield Installation Information\< ID >

hcmdsist.log

新規インストールの場合は Windows のシステムドライブ、そのほかの場合は Hitachi File Services Manager がインストールされているドライブの直下に格納されます。

hcmdsrtn.inst

新規インストールの場合は Windows のシステムドライブ、そのほかの場合は Hitachi File Services Manager がインストールされているドライブの直下に格納されます。

hcmdsuit.log

新規インストールの場合は Windows のシステムドライブ、そのほかの場合は Hitachi File Services Manager がインストールされているドライブの直下に格納されます。

hcmdsrtn.uit

新規インストールの場合は Windows のシステムドライブ、そのほかの場合は Hitachi File Services Manager がインストールされているドライブの直下に格納されます。

hcmdshdb_result

新規インストールの場合は Windows のシステムドライブ、そのほかの場合は Hitachi File Services Manager がインストールされているドライブの直下に格納されます。

HFSM_<インストール種別>_< YYYY >-< MM >-< DD >_< hh >-< mm >-< ss >.log

<インストール種別>には、ログファイルが出力された状況に応じて、「Install」（インストール時）または「Uninstall」（アンインストール時）が出力されます。

ログファイルの格納先は、障害が発生した時点の状況によって異なります。システム管理者は、インストールまたはアンインストールがエラー終了したときの状況を確認して、障害が発生した前後のログファイルを採取してください。

表 3-2 インストールまたはアンインストールがエラー終了したときの状況とログファイルの格納先

エラー終了時の状況		格納先
インストール	インストール先のフォルダを決定したあとでエラー終了した場合	<インストール先のフォルダ> ¥FileServicesManager¥inst
	インストールフォルダを決定する前にエラー終了した場合	新規インストールの場合 Windows のシステムドライブの直下 そのほかの場合 Hitachi File Services Manager がインストールされているドライブの直下
アンインストール	File Services Manager の inst フォルダが削除されていない場合	<インストール先のフォルダ> ¥FileServicesManager¥inst
	File Services Manager の inst フォルダが削除されている場合	Windows のシステムドライブの直下

3.4 パケットトレースのログファイルの採取方法

システム管理者は、tcpdump コマンドを使用して、ネットワークに障害が発生した場合に必要なパケットトレースのログファイルを採取できます。採取したパケットトレースのログファイルは保守員に送付したあとで削除してください。

システム管理者が UNIX マシンからパケットトレースのログファイルを採取する手順を次に示します。

1. ssh コマンドを実行して、対象のノードまたは Virtual Server にログインします。
2. touch コマンドを実行して、空のログファイルを作成します。

パケットトレースのログファイルの採取先に空のログファイルを作成してください。容量不足によってパケットトレースのログファイルの採取に失敗しないように、空き容量が 1GB 以上のファイルシステムを採取先として指定することを推奨します。事前に空のログファイルを作成しないと、採取したパケットトレースのログファイルが root 権限で作成されるため、削除できなくなります。

3. tcpdump コマンドを実行して、パケットトレースのログファイルを採取します。

tcpdump コマンドは、次に示すオプションを指定して実行してください。ほかのオプションは指定しないでください。

```
$ sudo tcpdump -i インターフェース名 -s サイズ -w パケットトレースのログファイル -n -c 採取パケット数 限定子
```

-i インターフェース名

パケットトレースを採取するインターフェース名を指定します。障害が発生した経路上のインターフェース名を指定します。インターフェース名が不明な場合、またはすべてのインターフェースのパケットトレースを採取する場合は、any を指定します。このオプションは、必ず指定してください。なお、VLAN が設定されているインターフェースの場合、名称は次の形式で指定してください。

<ポート名>.<VLAN ID> (例: eth12.0010)

-s サイズ

採取するパケット内のトレース取得サイズを指定します (単位: バイト)。MTU 値以上のサイズを指定することを推奨します。ただし、ネットワークに負荷が掛かっている場合は、デフォルト値 (96 バイト) を指定してください。

-w パケットトレースのログファイル

パケットトレースログファイルを絶対パスで指定します。このオプションは、必ず指定してください。

-n

名前解決しない場合に指定します。

-c 採取パケット数

トレースを採取するパケット数の上限を指定します。

限定子

次のどちらかの形式で指定します。

host IPアドレス

port ポート番号

限定されたホストまたはポートに対する通信のパケットだけを採取する場合に指定します。特定のホストやポートに対する通信で障害が発生している場合は、このオプションを指定してください。複数の限定子を組み合わせる場合は、and または or で区切って指定します。

システム管理者がパケットトレースのログファイルを採取するときのコマンドの実行例を次に示します。

/mnt/fs1/tcpdump.log にパケットトレースのログファイルを採取する場合

- パケットトレースを採取するインターフェース名は eth12 とする
- トレースを採取するパケット数の上限を 900,000 個とする
- IPアドレスが 10.208.61.8 のホスト、およびポート番号が 139 または 445 のポートに対する通信のパケットを採取する

```
$ ssh -2 nasroot@nas01
$ touch /mnt/fs1/tcpdump.log
$ sudo tcpdump -i eth12 -w /mnt/fs1/tcpdump.log -c 900000 host
10.208.61.8 and port 139 or port 445
```

注意：トレースを採取するパケット数の上限を指定しない場合は、ユーザー LU の空き容量が不足しないよう注意してください。

例えば、採取するパケットトレースのサイズにデフォルト値 (96 バイト) を指定し、トレースを採取するパケット数の上限を指定しない場合に、約 900,000 個のパケットトレースを採取すると、パケットトレースのログファイルサイズは約 100 MB となります。

3.5 CIFS サービスの性能解析用ログの採取方法

CIFS サービスの性能を解析するためにログを採取するように保守員から指示された場合は、次の手順に従って、CIFS サービスの性能解析用ログを採取し、保守員に送付してください。

1. 対象のノードまたは Virtual Server にログインします。
2. cifsinfogetctl コマンドで、CIFS サービスの性能解析用ログを採取するよう設定します。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。
3. ログファイルを取得して、保守員に送付します。

ログの出力先ディレクトリを指定した場合は、指定したディレクトリに CIFS 管理者としてアクセスし、「cifsinfoget_」で始まる名称のディレクトリ内の、すべてのファイルを保守員に送付してください。

ログの出力先ディレクトリの指定を省略した場合は、[Check for Errors] ダイアログの [List of RAS Information] ページで全ログデータ (All log data) をダウンロードして、保守員に送付してください。全ログデータの採取方法は、「[3.2 ノードおよび Virtual Server のログファイルの採取方法](#)」を参照してください。

障害の回復

この章では、障害を回復する方法について説明します。

システム管理者は、エラーメッセージやシステムメッセージなどで障害要因を特定し、メッセージテキストや保守員の指示に従って障害を回復します。

システム管理者が対処できない障害が発生した場合は、保守員の指示に従ってフェールオーバーやフェールバックなどの操作を行ってください。

障害を回復する際にリソースグループやクラスタを操作したり、コマンドを使用したりした場合は、GUI 上に表示されたファイルシステムやファイル共有の情報を更新するために、リフレッシュ処理を実行してください。

- 4.1 GUI の操作ミスを確認して操作し直す
- 4.2 コマンドの操作ミスを確認して操作し直す
- 4.3 管理サーバの認証パスワードを登録し直す
- 4.4 システムメッセージを確認して障害を回復する
- 4.5 クラスタおよびノードのエラー情報を確認して障害を回復する
- 4.6 リソースグループまたは **Virtual Server** のエラー情報を確認して障害を回復する
- 4.7 手動でフェールオーバー・フェールバックする
- 4.8 ファイルシステムの障害を回復する
- 4.9 差分格納デバイスの障害を回復する
- 4.10 差分スナップショットの障害を回復する
- 4.11 HCP へのアクセス障害を回復する
- 4.12 HCP にデータをマイグレートしていたファイルシステムをリストアする
- 4.13 ファイルシステムおよびプライマリー HCP の障害時にレプリカ HCP からファイルシステムをリストアする

- 4.14 マイグレートされたファイルをスタブ化していない場合に HVFP から HCP のデータをリストアする
- 4.15 システム設定情報を回復する
- 4.16 システム設定情報およびユーザーデータを一括で回復する
- 4.17 FC パスの障害を回復する
- 4.18 インターフェースやネットワークのエラー情報を確認して障害を回復する
- 4.19 リンク結合のエラー情報を確認して障害を回復する
- 4.20 データポートのエラー情報を確認して障害を回復する
- 4.21 ハードウェアの障害を回復する
- 4.22 OS 起動時に LU が認識できない障害を回復する
- 4.23 ほかのファイルサーバからのデータインポートでの障害を回復する
- 4.24 Backup Restore の機能に関する障害を回復する
- 4.25 Hitachi File Remote Replicator の機能に関する障害を回復する
- 4.26 ファイルスナップショットの処理で発生したタイムアウトを回復する

4.1 GUI の操作ミスを確認して操作し直す

File Services Manager の GUI での設定ミスや操作ミスなど、File Services Manager の GUI での操作に起因する障害が発生した場合、リフレッシュ処理を実行して管理サーバ上のデータベースを更新したあと、メッセージの指示に従って、操作し直してください。

リフレッシュ処理については、「ユーザズガイド」を参照してください。

4.2 コマンドの操作ミスを確認して操作し直す

コマンドの入力ミスが要因の場合は、標準エラー出力に表示されたメッセージの指示に従って、操作し直してください。

4.3 管理サーバの認証パスワードを登録し直す

Processing Node または Physical Node の稼働状態として「Credential error」と表示された場合、GUI で登録した管理サーバの認証パスワードと、実際にノードに設定されている認証パスワードが不一致になっています。[ノード編集] ダイアログで、ノードに設定した管理サーバの認証パスワードを登録し直してください。

4.4 システムメッセージを確認して障害を回復する

システムメッセージが出力されている場合、システムメッセージのメッセージ ID で障害が発生したプログラムを特定し、メッセージテキストで障害の要因を特定します。

システムメッセージごとの対処方法については、「メッセージリファレンス」を参照してください。該当するメッセージをメッセージ ID から検索し、障害を回復するための対処を確認できます。

メッセージの出力元のプログラムとメッセージ ID の関係については、「2.2 ノード上のシステムメッセージを確認する」を参照してください。

4.5 クラスタおよびノードのエラー情報を確認して障害を回復する

システム管理者は [Cluster Management] ダイアログの [Browse Cluster Status] ページでクラスタ・ノードのエラー状態を確認し、保守員と連携を取って、障害を回復します。

4.5.1 クラスタおよびノードのエラー情報の確認と回復方法の特定

システム管理者は、フェールオーバー機能に発生した障害を特定するために、[Browse Cluster Status] ページで確認したクラスタ・ノードの状態に対応する回復方法を「表 4-1 [Browse Cluster Status] ページ ([Cluster / Node status] 表示) で表示されるクラスタ状態に対応した障害の回復方法」から「表 4-2 [Browse Cluster Status (Cluster / Node Status)] ページで表示されるノード状態に対応した障害の回復方法」で確認します。また、保守員からの指示を確認して、該当する回復方法をこれらの表で特定します。

クラスタの状態を確認する場合は、[Browse Cluster Status] ページ ([Cluster / Node status] 表示) の [Cluster status] を確認します。表示されるクラスタ状態に対応した障害の回復方法について次の表に示します。

表 4-1 [Browse Cluster Status] ページ ([Cluster / Node status] 表示) で表示されるクラスタ状態に対応した障害の回復方法

クラスタ状態	回復方法	
	回復操作	参照先
ACTIVE	正常稼働中のため回復の必要なし。	なし
INACTIVE	停止しているクラスタを起動する。	なし
UNKNOWN※	OS の起動時に発生した障害を回復する。 両方のノードを停止して障害を回復する。 両方のノードを停止してプログラムをリプレースする。	4.5.2
	クラスタを構成する両方のノードの OS を再起動する。	4.5.3
	フェールオーバーによる縮退運用中であるが、クラスタを構成する両方のノードの OS を再起動する。	4.5.3
DISABLE	保守員に連絡する。	なし

注※：ノードの停止、またはノードの強制停止を行ったあと、停止した Physical Node（ノード）で [Browse Cluster Status] ページ ([Cluster / Node status] 表示) を表示すると、クラスタおよびもう一方のノードの状態として「UNKNOWN」が表示されます。この状態では、クラスタおよびもう一方のノードの状態は確認できません。クラスタともう一方のノードの状態は、稼働中の Physical Node（もう一方のノード）で [Browse Cluster Status] ページ ([Cluster / Node status] 表示) を表示して確認してください。

クラスタ起動時にも「UNKNOWN」が表示されます。なお、クラスタ起動時には、クラスタを構成するノード上のすべての OS の起動が完了するまで（最大で 10 分程度）、「UNKNOWN」が表示されます。

ノードの状態を確認する場合は、[Browse Cluster Status] ページ ([Cluster / Node status] 表示) の [Node status] を確認します。表示されるノード状態に対応した障害の回復方法について次の表に示します。

表 4-2 [Browse Cluster Status (Cluster / Node Status)] ページで表示されるノード状態に対応した障害の回復方法

ノード状態	回復方法	
	回復操作	参照先
UP	正常稼働中のため回復の必要なし。	なし
INACTIVE	停止しているノードを起動する。	なし
DOWN	フェールオーバーによる縮退運用を継続しながら、障害が発生したノードの OS を再起動する。	4.5.5
	フェールオーバーによる縮退運用を継続しながら、サービスを停止しないでプログラムをリプレースする。	4.5.6
	両方のノードを停止してプログラムをリプレースする。	4.5.7
UNKNOWN※	両方のノードを停止して障害を回復する。	4.5.7
	フェールオーバーによる縮退運用を継続しながら、障害が発生したノードを停止して回復する。	4.5.4
	フェールオーバーによる縮退運用を継続しながら、障害が発生したノードの OS を再起動する。	4.5.5
	OS の起動時に両方のノードで発生したハードウェアまたはソフトウェア障害を回復する。 両方のノードを停止してプログラムをリプレースする。	4.5.7
	OS の起動時にどちらかのノードで発生したハードウェアまたはソフトウェア障害を回復する。	4.5.8

ノード状態	回復方法	
	回復操作	参照先
	クラスタを構成する両方のノードの OS を再起動する。	4.5.9

注※：クラスタ起動時にも「UNKNOWN」が表示されます。なお、クラスタ起動時には、クラスタを構成するノード上のすべての OS の起動が完了するまで（最大で 10 分程度）、「UNKNOWN」が表示されます。

それぞれの障害に対応した回復方法を次に説明します。

4.5.2 回復方法 1

1. クラスタを強制停止します。
2. クラスタを構成する両方のノードの OS を再起動するよう保守員に依頼します。
障害の回復方法について保守員に相談してから、OS の再起動を依頼してください。保守員は、保守作業を完了してから OS を起動します。
3. クラスタを起動します。

4.5.3 回復方法 2

1. クラスタを強制停止します。
2. クラスタを構成する両方のノードの OS を再起動します。
3. クラスタを起動します。

4.5.4 回復方法 3

1. 保守作業が完了したノードの OS を起動するよう保守員に依頼します。
障害の回復方法について保守員に相談してから、OS の起動を依頼してください。保守員は、保守作業を完了してから OS を起動します。
2. リソースグループを元のノードにフェールバックします。

4.5.5 回復方法 4

1. 障害が発生したノードの OS を再起動します。
2. リソースグループを元のノードにフェールバックします。

4.5.6 回復方法 5

1. 保守作業が完了したノードの OS を起動するよう保守員に依頼します。
障害の回復方法について保守員に相談してから、OS の起動を依頼してください。保守員は、保守作業を完了してから OS を起動します。
2. 両方のリソースグループの実行ノードを変更します。
3. クラスタ内の別のノードの OS を再起動するよう保守員に依頼します。
障害の回復方法について保守員に相談してから、OS の再起動を依頼してください。保守員は、保守作業を完了してから OS を起動します。
4. リソースグループを元のノードにフェールバックします。

4.5.7 回復方法 6

1. クラスタを強制停止します。
2. 両方のノードの OS を再起動します。
3. クラスタを起動します。

4.5.8 回復方法 7

1. 障害が発生したノードを強制停止します。
2. 障害が発生したノードの OS を再起動するよう保守員に依頼します。
障害の回復方法について保守員に相談してから、OS の再起動を依頼してください。保守員は、保守作業を完了してから OS を起動します。
3. 保守作業が完了したノードを起動します。
4. リソースグループを元のノードにフェールバックします。

4.5.9 回復方法 8

1. クラスタを強制停止します。
2. 稼働しているノードの OS をシャットダウンします。
3. クラスタを構成する両方のノードの OS を起動します。
ノード本体の電源を入れます。
4. クラスタの状態が「INACTIVE」の場合にクラスタを起動します。

4.6 リソースグループまたは Virtual Server のエラー情報を確認して障害を回復する

システム管理者は [Cluster Management] ダイアログの [Browse Cluster Status] ページでリソースグループのエラー状態を確認し、[< Virtual Server >] サブウィンドウで Virtual Server のエラー状態を確認し、保守員と連携を取って、障害を回復します。

4.6.1 リソースグループまたは Virtual Server のエラー情報の確認と回復方法の特定

システム管理者は、フェールオーバー機能に発生した障害を特定するために、[Browse Cluster Status] ページで確認したリソースグループの状態、または [< Virtual Server >] サブウィンドウで確認した Virtual Server の状態に対応する回復方法を「表 4-3 [Browse Cluster Status] ページ ([Resource group status] 表示) で表示されるリソースグループ状態に対応した障害の回復方法」から「表 4-6 [< Virtual Server >] サブウィンドウに表示される Virtual Server のエラー情報に対応した障害の回復方法」で確認します。また、保守員からの指示を確認して、該当する回復方法をこれらの表で特定します。

リソースグループの状態を確認する場合は、[Browse Cluster Status] ページ ([Resource group status] 表示) の [Resource group status] を確認します。リソースグループの状態とエラー情報は、次のとおり表示されます。

<リソースグループ状態>/<エラー情報>

表示されるリソースグループ状態に対応した障害の回復方法について次の表に示します。

表 4-3 [Browse Cluster Status] ページ ([Resource group status] 表示) で表示されるリソースグループ状態に対応した障害の回復方法

リソースグループ状態	回復方法	
	回復操作	参照先
Online	リソースグループのエラー情報を参照する。	表 4-4
Online Maintenance	リソースグループのエラー情報を参照する。	表 4-4
Online Pending	開始処理中のため回復の必要なし。 ただし、通常運用時に、リソースグループの起動処理時間を超えて「Online Pending」から状態が遷移しない場合は、次のどちらかの操作を実行してください。 ・ クラスタを再起動する ・ [Running node] に表示されているノードを再起動する	なし
Online Ready	停止しているクラスタまたはノードを起動する。	なし
	OS のシャットダウン時に、クラスタを停止したため、次に起動するときに発生した障害を回復する。	4.6.7
	電源を遮断するときにノードを停止したために、次に起動するときに発生した障害を回復する。 障害が発生したノードだけ、フェールオーバー機能を再起動する。	4.6.8
	障害が発生したノードだけ、再起動する。	4.6.9
	両方のノードの OS を再起動する。	4.6.4
	クラスタが正常に稼働している場合は、リソースグループを起動する。	4.6.20
Offline	リソースグループのエラー情報を参照する。	表 4-4
Offline Pending	停止処理中のため回復の必要なし。	なし
Discovery (exclusivity)	稼働前のオンライン処理中のため回復の必要なし。	なし
Initializing	初期化処理中のため回復の必要なし。	なし
Internal Error	リソースグループのエラー情報を参照する。	表 4-4

表示されるリソースグループのエラー情報に対応した障害の回復方法について次の表に示します。

表 4-4 [Browse Cluster Status] ページ ([Resource group status] 表示) で表示されるリソースグループのエラー情報に対応した障害の回復方法

エラー情報	回復方法	
	回復操作	参照先
No error	正常稼働中のため回復の必要なし。	なし
Internal error · not recoverable	OS の起動時にクラスタ内のノードが起動しない障害を回復する。	4.6.10
	保守員がハードウェアをリプレースする。	4.6.11
	障害が発生したリソースグループを再起動する。	4.6.12
	障害が発生したリソースグループが稼働しているノードを再起動する。	4.6.13
	リソースグループに障害が発生したノードの OS を再起動する。	4.6.14
	障害が発生したノードだけを停止してプログラムをリプレースする。	4.6.15
	両方のノードを停止してプログラムをリプレースする。	4.6.16
Monitor activity unknown	両方のノードを停止してプログラムをリプレースする。	4.6.16
	サービスの再開を優先して障害を回復し、プログラムのリプレースについては後日対応する。	4.6.18

エラー情報	回復方法	
	回復操作	参照先
No available nodes または No available nodes in failure domain after monitor failure	フェールオーバーによって移動してきたリソースグループに障害が発生したとき、同じノード内に、元から稼働していたリソースグループが継続して稼働していた場合に、障害を回復してサービスを再開する。	4.6.11
	フェールオーバーによって移動してきたリソースグループに障害が発生したとき、そのノードで元から稼働していたリソースグループがすでに別のノードに移動していた場合に、障害を回復してサービスを再開する。	4.6.20
Node unknown	障害が発生したリソースグループが稼働しているノードを再起動する。	4.6.13
	リソースグループに障害が発生したノードの OS を再起動する。	4.6.14
	障害が発生したノードだけを停止してプログラムをリプレースする。	4.6.15
	両方のノードを停止してプログラムをリプレースする。 両方のノードを停止して障害を回復する。 OS の起動時に両方のノードに発生したハードウェア障害を回復する。 OS の起動時に障害が発生したノードを停止してプログラムをリプレースする。	4.6.16
Split resource group (exclusivity)	OS の起動時に発生した障害を回復する。 リソースグループで提供しているサービスの再開を優先し、プログラムのリプレースは後日対応する。	4.6.17
	両方のノードを停止してプログラムをリプレースする。	4.6.16
srmd executable error	両方のノードを停止して障害を回復する。	4.6.2
	フェールオーバーによる縮退運用を継続しながら、障害が発生したノードの OS を再起動する。	4.6.3
	OS の起動時に両方のノードで発生したハードウェアまたはソフトウェア障害を回復する。 両方のノードを停止してプログラムをリプレースする。	4.6.4
	OS の起動時にどちらかのノードで発生したハードウェアまたはソフトウェア障害を回復する。	4.6.5
	クラスタを構成する両方のノードの OS を再起動する。	4.6.6
	KAQM05256-E または KAQM05258-E~KAQM05264-E のメッセージ ID のシステムメッセージが出力されているか確認し、各メッセージに従って対処する。	なし

Virtual Server の状態を確認する場合は、[< Virtual Server >] サブウィンドウで確認します。

表示される Virtual Server 状態に対応した障害の回復方法について次の表に示します。

表 4-5 [< Virtual Server >] サブウィンドウで表示される Virtual Server 状態に対応した障害の回復方法

Virtual Server 状態	回復方法	
	回復操作	参照先
Online	正常に稼働しているため、回復の必要なし。	なし
Partial online	正常に稼働しているが、一部のサービスが提供されていない。Virtual Server のシステムメッセージを参照して、KAQMnnnnn メッセージを確認し、対処する。	なし
Online pending	開始処理中のため回復の必要なし。 ただし、通常運用時に、Virtual Server の起動処理時間を超過して「Online Pending」から状態が遷移しない場合は、次のどちらかの操作を実行してください。 ・ クラスタを再起動する	なし

Virtual Server 状態	回復方法	
	回復操作	参照先
	<ul style="list-style-type: none"> 対象の Virtual Server の稼働ノードを再起動する 稼働ノードは、[< Processing Node >] サブウィンドウの [Virtual Servers] タブで参照できます。 	
Online Ready	停止しているクラスタまたはノードを起動する。	なし
	OS のシャットダウン時に、クラスタを停止したため、次に起動するときに発生した障害を回復する。	4.6.2
	電源を遮断するときにノードを停止したために、次に起動するときに発生した障害を回復する。	4.6.8
	障害が発生したノードだけ、再起動する。	4.6.21
	両方のノードの OS を再起動する。	4.6.4
	クラスタが正常に稼働している場合は、Virtual Server を起動する。	なし
Offline	正常に停止しているため、回復の必要なし	なし
Offline Pending	停止処理中のため回復の必要なし。	なし
Error	Virtual Server のエラー情報を参照する。	表 4-6

表示される Virtual Server のエラー情報に対応した障害の回復方法について次の表に示します。

表 4-6 [< Virtual Server >] サブウィンドウに表示される Virtual Server のエラー情報に対応した障害の回復方法

エラー情報	回復方法	
	回復操作	参照先
No error	正常稼働中のため回復の必要なし。	なし
Internal error	ノードおよび Virtual Server のログを取得して保守員に連絡する。	なし
Monitor setup error	監視の再開、または監視除外を再度行う。	4.6.28
	障害が発生したノードの OS を再起動する。	4.6.22
No available nodes	フェールオーバー先のノードを起動する。	4.6.23
	上記の対処を行ったあとも同じエラー状態になる場合は、ノードおよび Virtual Server のログを取得し、保守員に連絡する。	なし
Node not available	フェールオーバーが発生した要因を取り除く。	4.6.24
	上記の対処を行ったあとも同じエラー状態になる場合は、ノードおよび Virtual Server のログを取得し、保守員に連絡する。	なし
Node unknown	両ノードの OS を再起動する。	4.6.25
	上記の対処を行ったあとも同じエラー状態になる場合は、ノードおよび Virtual Server のログを取得し、保守員に連絡する。	なし
Execution error	Virtual Server のシステムメッセージ KAQM35nnn に対処する。	なし
	ノードのシステムメッセージ KAQM34nnn に対処する。	なし
	ノードのシステムメッセージ KAQG72019-E、または KAQG72020-E に対処する。	なし
	KAQM05256-E または KAQM05258-E~KAQM05264-E のメッセージ ID のシステムメッセージが出力されているか確認し、各メッセージに従って対処する。	なし
	Virtual Server が稼働していたノードの OS を再起動する。	4.6.26
	KAQM34nnn, KAQM35nnn, KAQG72019-E, KAQG72020-E がシステムメッセージに含まれない場合、ノードおよび Virtual Server のログを取得し、保守員に連絡する。	なし

エラー情報	回復方法	
	回復操作	参照先
OS error	Virtual Server のシステムメッセージ KAQM35nnn に対処する。	なし
	ノードのシステムメッセージ KAQG72019-E、または KAQG72020-E に対処する。	なし
	KAQM05256-E または KAQM05258-E~KAQM05264-E のメッセージ ID のシステムメッセージが出力されているか確認し、各メッセージに従って対処する。	なし
	Virtual Server が稼働していたノードの OS を再起動する。	4.6.26
	上記の対処をしても、エラー状態になる場合には、ノードおよび Virtual Server のログを取得して保守員に連絡する。	なし
Status unknown	再度、状態の確認を行う。	なし
	再度エラーが発生する場合には、ネットワークの状態を確認し、異常があればそれに対処する。	なし
	ネットワークの状態に異常がなければ、ノードおよび Virtual Server のログを取得して保守員に連絡する。	なし
Operation incomplete	vnaslist コマンドで詳細を確認し、KAQM34070-W メッセージのコマンド情報によって、不整合を解消する。	4.6.27

それぞれの障害に対応した回復方法を次に説明します。各手順での操作方法については、「ユーザーズガイド」を参照してください。なお、以下の回復方法の中で Virtual Server の強制停止後の OS の再起動は、両方のノードのシステムメッセージを確認して KAQG72019-E または KAQG72020-E が出力されている側で行ってください。KAQG72019-E または KAQG72020-E が両方のノードで出力されている場合、より最近にメッセージが出力された側の OS を再起動してください。KAQG72019-E、KAQG72020-E が出力されていない場合、OS の再起動は不要です。

4.6.2 回復方法 1

1. クラスタを強制停止します。
2. クラスタを構成する両方のノードの OS を再起動するよう保守員に依頼します。
障害の回復方法について保守員に相談してから、OS の再起動を依頼してください。保守員は、保守作業を完了してから OS を起動します。
3. クラスタを起動します。

4.6.3 回復方法 2

1. 障害が発生したノードの OS を再起動します。
2. リソースグループを元のノードにフェールバックします。

4.6.4 回復方法 3

1. クラスタを強制停止します。
2. 両方のノードの OS を再起動します。
3. クラスタを起動します。

4.6.5 回復方法 4

1. 障害が発生したノードを強制停止します。
2. 障害が発生したノードの OS を再起動するよう保守員に依頼します。

障害の回復方法について保守員に相談してから、OSの再起動を依頼してください。保守員は、保守作業を完了してからOSを起動します。

3. 保守作業が完了したノードを起動します。
4. リソースグループを元のノードにフェールバックします。

4.6.6 回復方法 5

1. クラスタを強制停止します。
2. 稼働しているノードのOSをシャットダウンします。
3. クラスタを構成する両方のノードのOSを起動します。
ノード本体の電源を入れます。
4. クラスタの状態が「INACTIVE」の場合にクラスタを起動します。

4.6.7 回復方法 6

1. クラスタを起動します。

4.6.8 回復方法 7

1. ノードを起動します。

4.6.9 回復方法 8

1. 障害が発生したノードのOSを起動します。
ノード本体の電源を入れます。

4.6.10 回復方法 9

1. 障害が発生したリソースグループを強制停止します。
2. 障害が発生したノードを停止します。
3. 障害が発生したノードで稼働していたリソースグループを起動します。
4. 保守作業が完了したノードのOSを起動するよう保守員に依頼します。
障害の回復方法について保守員に相談してから、OSの起動を依頼してください。保守員は、保守作業を完了してからOSを起動します。
5. 保守作業が完了したノードを起動します。
6. リソースグループを元のノードにフェールバックします。

4.6.11 回復方法 10

1. 障害が発生したノードで稼働していたリソースグループを強制停止します。
2. 障害が発生したノードのOSを再起動します。
3. リソースグループを起動します。

4.6.12 回復方法 11

1. 障害が発生したリソースグループを強制停止します。
2. リソースグループを起動します。

4.6.13 回復方法 12

1. 障害が発生したリソースグループを強制停止します。
2. ノードを停止します。
3. ノードを起動します。
4. リソースグループを起動します。

4.6.14 回復方法 13

1. 障害が発生したリソースグループを強制停止します。
2. ノードを停止します。
3. 停止したノードの OS を再起動します。
4. ノードを起動します。
5. リソースグループを起動します。

4.6.15 回復方法 14

1. 障害が発生したリソースグループを強制停止します。
2. ノードを停止します。
3. 停止したノードの OS を再起動するよう保守員に依頼します。
障害の回復方法について保守員に相談してから、OS の再起動を依頼してください。保守員は、保守作業を完了してから OS を起動します。
4. ノードを起動します。
5. リソースグループを起動します。
6. クラスタ内の別のリソースグループをフェールオーバーします。
7. クラスタ内の別のノードを停止します。
8. クラスタを構成する別のノードの OS を再起動するよう保守員に依頼します。
保守員は、保守作業を完了してから OS を起動します。
9. クラスタ内の別のノードを起動します。
10. リソースグループを元のノードにフェールバックします。

4.6.16 回復方法 15

1. 障害が発生したリソースグループを強制停止します。
2. クラスタ内の別のリソースグループを停止します。
3. クラスタを停止します。
4. クラスタを構成する両方のノードの OS を再起動するよう保守員に依頼します。
障害の回復方法について保守員に相談してから、OS の再起動を依頼してください。保守員は、保守作業を完了してから OS を起動します。
5. クラスタを起動します。
6. 両方のリソースグループを起動します。

4.6.17 回復方法 16

1. 障害が発生したリソースグループを強制停止します。

2. クラスタ内の別のリソースグループを停止します。
3. クラスタを停止します。
4. クラスタを構成する両方のノードの OS を再起動します。
5. クラスタを起動します。
6. 両方のリソースグループを起動します。

4.6.18 回復方法 17

1. リソースグループを監視します。
2. リソースグループを監視対象から除外します。
3. 1.と 2.の操作を繰り返します。

4.6.19 回復方法 18

1. 障害が発生したリソースグループを強制停止します。
2. フェールバック元のノードを停止します。
3. 停止したノード（フェールオーバー元）の OS を再起動するよう保守員に依頼します。
障害の回復方法について保守員に相談してから、OS の再起動を依頼してください。保守員は、保守作業を完了してから OS を起動します。
4. フェールバック元のノードを起動します。
5. 起動中のリソースグループの実行ノードを変更します。
6. フェールバック先のノードを停止します。
7. 停止したノード（フェールオーバー先）の OS を再起動するよう保守員に依頼します。
保守員は、保守作業を完了してから OS を起動します。
8. フェールバック先のノードを起動します。
9. リソースグループを起動します。

4.6.20 回復方法 19

1. リソースグループを起動します。

4.6.21 回復方法 20

1. ノードの強制停止を行います。
2. OS を停止します。
3. ノードに障害が発生したノードの OS を起動します。
ノード本体の電源を入れます。
4. ノードを起動します。

4.6.22 回復方法 21

1. 障害が発生した Virtual Server を強制的に停止します。
2. 強制的に停止した Virtual Server が稼働していたノードを停止し、そのノードの OS を再起動します。
この操作によって、同一ノード上で正常に稼働していた別の Virtual Server は、ほかのノードにフェールオーバーします。

3. OS を再起動した側のノードを起動します。
4. フェールオーバーした Virtual Server を元のノードにフェールバックします。

4.6.23 回復方法 22

1. 障害が発生した Virtual Server を強制的に停止します。
2. 最初のフェールオーバーが発生した要因をノードおよび Virtual Server のシステムメッセージから特定して取り除きます。
保守員に依頼してください。
3. クラスタを停止します。
4. 強制的に停止した Virtual Server が稼働していたノードの OS を再起動します。
5. もう一方のノードの OS が停止している場合、その OS を起動します。
6. クラスタを起動します。
7. 停止した Virtual Server を起動します。

4.6.24 回復方法 23

1. 障害が発生した Virtual Server を強制的に停止します。
2. 最初のフェールオーバーが発生した要因をノードおよび Virtual Server のシステムメッセージから特定して取り除きます。
保守員に依頼してください。
3. 強制的に停止した Virtual Server が稼働していたノードを停止し、そのノードの OS を再起動します。
この操作によって、同一ノード上で正常に稼働していた別の Virtual Server は、ほかのノードにフェールオーバーします。
4. OS を再起動した側のノードを起動します。
5. フェールオーバーした Virtual Server を元のノードにフェールバックします。
6. 停止した Virtual Server を起動します。

4.6.25 回復方法 24

1. 障害が発生した Virtual Server を強制的に停止します。
2. クラスタを強制停止します。
3. 両方のノードの OS を再起動します。
4. 停止した Virtual Server を起動します。

4.6.26 回復方法 25

1. 障害が発生した Virtual Server を強制的に停止します。
2. Virtual Server が稼働していたノードのシステムメッセージを確認します。

KAQS19002-E が出力されている場合

差分格納デバイスの容量が不足したため、ファイルシステムまたは差分スナップショットがブロックされています。手順 6 に進んでください。なお、差分格納デバイスの容量不足による障害は、手順 7 で Virtual Server を起動したあとに回復してください。

KAQS19002-E が出力されていない場合

手順 3 に進んでください。

3. Virtual Server 起動で発生した要因またはフェールオーバーした要因を、ノードおよび Virtual Server のシステムメッセージから特定して取り除きます。
保守員に依頼してください。
4. 強制的に停止した Virtual Server が稼働していたノードを停止し、そのノードの OS を再起動します。
この操作によって、同一ノード上で正常に稼働していた別の Virtual Server は、ほかのノードにフェールオーバーします。
5. OS を再起動した側のノードを起動します。
6. フェールオーバーした Virtual Server を元のノードにフェールバックします。
7. 停止した Virtual Server を起動します。

4.6.27 回復方法 26

1. KAQM34070-W メッセージ、または KAQM34071-E メッセージの出力内容を基に、表 4-7 Virtual Server の処理が完了していない（コマンドが中断した）場合の対処および実行可能なコマンドに従って、必要に応じて対処します。
2. Virtual Server の状態を vnaslist コマンドで確認し、必要に応じて再設定を行います。
KAQM34070-W メッセージは、エラー情報が「Operation incomplete」と表示された Virtual Server に対して、vnaslist コマンドを実行すると出力されます。vnaslist コマンドの出力結果の例を次に示します。

```
$ sudo vnaslist vs02
ID                : 33
Name              : vs02
Status            : Offline/No error
Monitor           : -
Startup Node      : node0
Active Node       :
KAQM34070-W The virtual server information might not match the system state.
Please correct the cause of the mismatch. (virtual server = vs02, process =
assigning LUs, details = lu0B,lu0C,lu0D,lu0E,lu10,lu11,lu12,lu13)
```

KAQM34070-W メッセージが出力されても、Status に「Online pending」が表示された場合は、Virtual Server の起動処理中のため対処は必要ありません。しばらくしてから vnaslist コマンドを再度実行してください。

KAQM34071-E メッセージは、エラー情報が「Operation incomplete」と表示された Virtual Server に対して、コマンドで処理を行うと出力されます。KAQM34071-E メッセージの出力例を次に示します。

```
$ sudo vnaslurelease lu0B,lu0C,lu0D,lu0E vs02
KAQM34031-Q Are you sure you want to release the specified user LU from the
virtual server? (y/n) y
KAQM34071-E The operation cannot be performed because the virtual server
information might not match the system state. Please correct the cause of
the mismatch, and then retry the operation. (virtual server = vs02, process
= assigning LUs, details = lu0B,lu0C,lu0D,lu0E,lu10,lu11,lu12,lu13)
```

表 4-7 Virtual Server の処理が完了していない（コマンドが中断した）場合の対処および実行可能なコマンド

メッセージ中の「process」の値	対処方法	状態を回復させるコマンド
vnascreate	処理が未完了の Virtual Server をいったん削除し、作成し直す。	vnasdelete
vnasdelete	再実行する。	vnasdelete

メッセージ中の「process」の値	対処方法	状態を回復させるコマンド
vnasedit (-t new-name)	処理が未完了の Virtual Server の Virtual Server 名を設定し直す。このとき、設定し直す Virtual Server 名はメッセージ中の「詳細情報」の値とする。	vnasedit -t n
vnasedit (-t startup-node)	処理が未完了の Virtual Server のデフォルト起動ノードを設定し直す。このとき、設定し直すデフォルト起動ノードはメッセージ中の「詳細情報」の値とする。	vnasedit -t s
vnasluassign	メッセージ中の「詳細情報」の値の LU をいったん解放し、割り当てし直す。※	vnaslurelease
vnaslurelease	メッセージ中の「詳細情報」の値の LU を解放する。※	vnaslurelease
vnasifassign	メッセージ中の「詳細情報」の値の仮想 IP アドレスを割り当てし直す。	vnasifassign
vnasifrelease	メッセージ中の「詳細情報」の値の仮想 IP アドレスを解放する。	vnasifrelease
vnasinit	再実行する。	vnasinit
assigning LUs	GUI の [Virtual Server 編集] ダイアログから、メッセージ中の「詳細情報」に表示されたすべての LU を [選択された LU] に選んだ状態で [OK] ボタンをクリックする。[選択された LU] には、障害発生時の操作のときと同じ状態のすべての LU を選択する。※	なし
preparing for update	処理が未完了の Virtual Server を起動または再起動する。	vnasstart vnasrestart
updating	処理が未完了の Virtual Server を回復する。	vnasinit
unknown	保守員に連絡する。	—

(凡例) — : 該当しない

注意 : Virtual Server OS LU の障害などの要因で、上記の表の対処を実行して問題が解決しない場合は、「4.15.4 Virtual Server OS LU に障害が発生している場合」の手順で、Virtual Server OS LU の回復操作を実行してください。ただし、process に"vnascreate"または"vnasdelete"が出力されている場合は、Virtual Server OS LU の回復のすべての手順は必要ありません。この場合、「4.15.4 Virtual Server OS LU に障害が発生している場合」の手順 3 までを実施して、Virtual Server OS LU の障害を回復させた上で、再び上記の表の対処を実行してください。

注※ : エラー発生時と同じ操作の再実行が必要であるため、メッセージ中の「詳細情報」に表示されたすべての LU を選択して操作を実行してください。

4.6.28 回復方法 27

1. 障害が発生した Virtual Server を強制的に停止します。
2. 強制的に停止した Virtual Server が稼働していたノードを停止し、そのノードの OS を再起動します。
この操作によって、同一ノード上で正常に稼働していた別の Virtual Server は、ほかのノードにフェールオーバーします。
3. OS を再起動した側のノードを起動します。
4. フェールオーバーした Virtual Server を元のノードにフェールバックします。
5. 停止した Virtual Server を起動します。

6. 監視の再開, または監視除外を再度行います。

4.7 手動でフェールオーバー・フェールバックする

システム管理者は, ノードの保守作業や障害回復を行うときに, 保守員の指示に従って, [Cluster Management] ダイアログの [Browse Cluster Status] ページ ([Resource group status] 表示) から手動でフェールオーバー・フェールバックします。保守員の指示を受けてから, サービスが稼働しているリソースグループをフェールオーバーします。また, 保守員の保守作業が完了したことを確認してから, リソースグループを元のノードにフェールバックします。手動でフェールオーバー・フェールバックして障害を回復する手順については, 「4.5 クラスタおよびノードのエラー情報を確認して障害を回復する」を参照してください。

手動でフェールオーバーするためには, 1つのノードに1つのリソースグループが稼働している状態で, リソースグループを別のノードに移動します。この操作は, ノードの保守作業や障害回復を行うときに, リソースグループが提供しているサービスを継続して利用するために行います。

また, 手動でフェールバックするためには, 1つのノードに2つのリソースグループが稼働している状態で, フェールオーバーしたリソースグループを元のノードに移動します。この操作は, フェールオーバーしたリソースグループを障害回復したノードに戻すために行います。

手動でフェールオーバー・フェールバックしているときに障害が発生し, 処理を続行できない場合は, 「4.5 クラスタおよびノードのエラー情報を確認して障害を回復する」を参照してください。

Virtual Server を使用している場合は, システム管理者は, ノードの保守作業や障害回復を行うときに, 保守員の指示に従って, [Virtual Server] タブの [Virtual Server フェールオーバー/フェールバック] ダイアログから手動でフェールオーバー・フェールバックします。保守員の指示を受けてから, サービスが稼働しているリソースグループをフェールオーバーします。また, 保守員の保守作業が完了したことを確認してから, リソースグループを元のノードにフェールバックします。手動でフェールオーバー・フェールバックして障害を回復する手順については, 「4.6 リソースグループまたは Virtual Server のエラー情報を確認して障害を回復する」および「4.5 クラスタおよびノードのエラー情報を確認して障害を回復する」を参照してください。

手動でフェールオーバーするためには, ノード上で稼働している Virtual Server を別のノードに移動します。この操作は, ノードの保守作業や障害回復を行うときに, Virtual Server が提供しているサービスを継続して利用するために行います。

また, 手動でフェールバックするためには, フェールオーバーした Virtual Server を元のノードに移動します。この操作は, フェールオーバーした Virtual Server を障害回復したノードに戻すために行います。

4.8 ファイルシステムの障害を回復する

ここでは, HVFP で運用しているファイルシステムで障害が発生した場合の対処方法について説明します。

HVFP で運用しているファイルシステムに障害が発生した場合, 要因によって回復手順が異なります。GUI の [マウント状態] を参照するか, fslist コマンドを実行して, ファイルシステムの状態を確認し, 対処してください。

GUI の [マウント状態] に「Data corrupted」と表示されている場合, または fslist コマンドの実行結果で [Device Status] に「Normal」, [Mount Status] に「Fatal error」と表示されている場合

OS の障害またはプールの容量不足によってファイルシステムが閉塞しているおそれがあります。仮想 LU を使用しているかどうか、および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よう設定されているかどうかを確認してください。

- ファイルシステムで仮想 LU を使用している場合
ノード上のシステムメッセージに **KAQG90009-E** が出力されているか確認してください。出力されていた場合は、「[4.8.6 プールの容量不足によってノード上のファイルシステムが閉塞している場合](#)」または「[4.8.7 プールの容量不足によって Virtual Server 上のファイルシステムが閉塞している場合](#)」に従って対処してください。
- 自動的にフェールオーバーするよう設定されている場合
「[4.8.2 OS 障害によってファイルシステムが閉塞している場合 \(自動フェールオーバー機能を設定しているとき\)](#)」に従って対処してください。
- 自動的にフェールオーバーする設定になっていない場合
「[4.8.3 OS 障害によってファイルシステムが閉塞している場合 \(自動フェールオーバー機能を設定していないとき\)](#)」に従って対処してください。

GUI の [マウント状態] に「**Device error**」と表示されている場合、または `fslist` コマンドの実行結果で [Device Status] に「**Error**」、[Mount Status] に「**Fatal error**」と表示されている場合

FC パスの障害またはストレージシステムの障害によってファイルシステムが閉塞しています。ファイルシステムで使用している LU のターゲットを [<ファイルシステム>] サブウィンドウで確認したあと、該当するターゲットの FC パスに障害が発生していないか、GUI の [FC パス] サブタブの [状態] または `fpstatus` コマンドで確認してください。

FC パスに障害が発生している場合は、「[4.17 FC パスの障害を回復する](#)」に従って対処してください。

FC パスに障害が発生していない場合は、「[4.8.4 ストレージシステムの障害によってファイルシステムが閉塞している場合](#)」に従って対処してください。

なお、HVFP では、障害に備えてバックアップデータを採取する運用を推奨しています。以降では、ストレージシステムとは別のメディアにファイルシステムのデータをバックアップしてあることを前提とした回復手順を示します。

また、ファイルシステムのデータを HCP にマイグレートしている場合には、各手順でのファイルシステムの再構築およびバックアップデータの回復操作は「[4.12 HCP にデータをマイグレートしていたファイルシステムをリストアする](#)」に従って実行してください。ただし、ファイルシステムおよびプライマリ HCP の両方に障害が発生した場合、「[4.13 ファイルシステムおよびプライマリ HCP の障害時にレプリカ HCP からファイルシステムをリストアする](#)」の手順で回復してください。

階層ファイルシステムに対して **KAQG90004-W** メッセージが出力された場合は、「[4.8.8 階層ファイルシステム内の階層で容量が不足している場合](#)」に従って対処してください。

4.8.1 空き容量があってもファイルを作成できない場合

inode 情報はファイルシステムの先頭 1TB 分の領域に格納されます。inode 情報を格納する領域が満杯の場合、空き容量があってもファイルおよびディレクトリを作成できません。`fsinodespace` コマンドで inode 領域を再構成してください。それでも問題が解決しない場合は次の手順に従って対応してください。

1. ファイルシステムの容量不足が発生した時刻近辺に作成したサイズの大きいファイルを、別のファイルシステムへ移動します。
2. 手順 1 で移動したファイルを元の場所に戻します。

上記の操作を実行しても、ファイルまたはディレクトリを作成できない場合には、移動するファイルを変えて、繰り返してください。

4.8.2 OS 障害によってファイルシステムが閉塞している場合（自動フェールオーバー機能を設定しているとき）

OS 障害によって閉塞したファイルシステムの回復手順を次に示します。

1. リソースグループまたはフェールオーバーしたすべての **Virtual Server** を元のノードにフェールバックします。

2. ファイルシステムを削除します。
閉塞したファイルシステムを削除します。

Virtual Server を使用している場合

手順 3 に進んでください。

Virtual Server を使用していない場合

手順 8 に進んでください。

3. **Virtual Server** の稼働状況とエラー情報を確認します。

稼働状況とエラー情報が **Error/OS error** の場合

手順 4 に進んでください。

稼働状況とエラー情報が **Error/OS error** でない場合

手順 8 に進んでください。

4. **Virtual Server** を強制的に停止します。
5. **Virtual Server** が稼働していたノードの OS を再起動します。
6. フェールオーバーした **Virtual Server** を元のノードにフェールバックします。
7. 停止した **Virtual Server** を起動します。
8. ファイルシステムを再構築します。
9. 再構築したファイルシステムにバックアップデータを回復します。
10. ファイル共有を再作成します。
バックアップデータを使用して回復しているため、[共有追加] ダイアログの [共有ディレクトリの所有者] で、必ず [既存ディレクトリをそのまま使用] を選択してください。
11. **Virtual Server** を使用している場合は、**Virtual Server** の稼働状況を確認し、「Online/No error」でなければ **Virtual Server** を再起動します。

監査ログを出力しているファイルシステムを回復した場合は、**ALog ConVerter** との連携を再設定する必要があります。`alogctl` コマンドで、**ALog ConVerter** との連携を無効にしたあと有効にしてください。両ノードでコマンドを実行してください。

4.8.3 OS 障害によってファイルシステムが閉塞している場合（自動フェールオーバー機能を設定していないとき）

OS 障害によって閉塞したファイルシステムの回復手順を次に示します。次の手順に従って、保守員と連携して対処してください。

1. 保守員に依頼して、障害情報を採取します。
障害情報の採取に伴って、リソースグループまたは **Virtual Server** のフェールオーバーが発生します。

2. リソースグループまたはフェールオーバーしたすべての **Virtual Server** を元のノードにフェールバックします。
3. ファイルシステムを削除します。
閉塞したファイルシステムを削除します。

Virtual Server を使用している場合

手順 4 に進んでください。

Virtual Server を使用していない場合

手順 9 に進んでください。

4. **Virtual Server** の稼働状況とエラー情報を確認します。

稼働状況とエラー情報が **Error/OS error** の場合

手順 5 に進んでください。

稼働状況とエラー情報が **Error/OS error** でない場合

手順 9 に進んでください。

5. **Virtual Server** を強制的に停止します。
6. **Virtual Server** が稼働していたノードの OS を再起動します。
7. フェールオーバーした **Virtual Server** を元のノードにフェールバックします。
8. 停止した **Virtual Server** を起動します。
9. ファイルシステムを再構築します。
10. 再構築したファイルシステムにバックアップデータを回復します。
11. ファイル共有を再作成します。
バックアップデータを使用して回復しているため、[共有追加] ダイアログの [共有ディレクトリの所有者] で、必ず [既存ディレクトリをそのまま使用] を選択してください。
12. **Virtual Server** を使用している場合は、**Virtual Server** の稼働状況を確認し、「Online/No error」でなければ **Virtual Server** を再起動します。

監査ログを出力しているファイルシステムを回復した場合は、**ALog ConVerter** との連携を再設定する必要があります。alogctl コマンドで、**ALog ConVerter** との連携を無効にしたあと有効にしてください。両ノードでコマンドを実行してください。

4.8.4 ストレージシステムの障害によってファイルシステムが閉塞している場合

ストレージシステムの障害によってファイルシステムが閉塞している場合の回復手順を次に示します。次の手順に従って、保守員と連携して対処してください。

1. 閉塞したファイルシステムで使用している LU を確認します。
[<ファイルシステム>] サブウィンドウで次の情報を確認します。
 - LU へのパスが属するターゲット
 - LU が存在するストレージシステムのモデルおよびシリアル番号
 - LU の LDEV 番号
2. ファイルシステムを継続して使用できるか保守員に確認します。
ストレージシステムの障害によってファイルシステムが閉塞しても、ファイルシステムを継続使用できることがあります。

Virtual Server 使用時にファイルシステムを継続使用できる場合

手順 3～5 の操作を実行してください。

Virtual Server 未使用時にファイルシステムを継続使用できる場合
手順 6 に進みます。

ファイルシステムを継続使用できない場合

バックアップデータを使用してファイルシステムを回復します。ここで手順を終了し、続けて「4.8.5 ファイルシステムを継続使用できない場合」に従って対処してください。

3. 障害が発生した LU を使用していない Virtual Server を、手動でフェールオーバーします。
障害が発生した Virtual Server が稼働していたノードで、障害が発生した LU を使用していない Virtual Server をすべてフェールオーバーします。
4. 保守員に依頼して、障害が発生した Virtual Server が稼働しているノードの障害情報を採取します。
障害情報の採取に伴って、Virtual Server のフェールオーバーが発生します。
5. Virtual Server を元のノードにフェールバックします。
これで手順は完了です。以降の手順は読み飛ばしてください。
6. 保守員に依頼して、ストレージシステムの障害を取り除きます。
7. 障害が発生していたリソースグループの状態を確認します。

フェールオーバーしていた場合

手順 9 に進みます。

フェールオーバーしていなかった場合

手順 8 に進みます。

8. ノード上のリソースグループを手動でフェールオーバーします。
9. ノードを停止します。
10. OS を再起動します。
11. ノードを起動します。
12. リソースグループを元のノードにフェールバックします。
13. クラスタ内の別のノードで手順 8～手順 12 の操作を実行します。

4.8.5 ファイルシステムを継続使用できない場合

「4.8.4 ストレージシステムの障害によってファイルシステムが閉塞している場合」で、ファイルシステムを継続使用できない場合、バックアップデータを使用してファイルシステムを回復する必要があります。

バックアップデータを使用してファイルシステムを回復する手順を次に示します。

1. `lumapctl` コマンドを使用して、LU の自動割り当ての設定を保守モードに変更します。
2. 保守員に依頼して、ストレージシステムの障害を取り除きます。
3. ファイルシステムを削除します。
閉塞したファイルシステムを削除します。

Virtual Server を使用している場合

手順 4 に進みます。

Virtual Server を使用していない場合

手順 7 に進みます。

4. 障害が発生した LU を使用していない **Virtual Server** を、手動でフェールオーバーします。
障害が発生した **Virtual Server** が稼働していたノードで、障害が発生した LU を使用していない **Virtual Server** をすべてフェールオーバーします。
5. 保守員に依頼して、障害が発生した **Virtual Server** が稼働しているノードの障害情報を採取します。
障害情報の採取に伴って、**Virtual Server** のフェールオーバーが発生します。
6. **Virtual Server** を元のノードにフェールバックします。
手順 14 に進みます。
7. もう一方のノードで稼働していたリソースグループがフェールオーバーしている場合は、フェールバックします。
8. 操作しているノードのリソースグループがフェールオーバーしていない場合は、手動でフェールオーバーします。
9. フェールオーバー元のノードを停止します。
10. フェールオーバー元のノードの OS を再起動します。
11. フェールオーバー元のノードを起動します。
12. リソースグループを元のノードにフェールバックします。
13. クラスタ内の別のノードで手順 7～手順 12 の操作を実行します。
14. ファイルシステムを再構築します。
15. 再構築したファイルシステムにバックアップデータを回復します。
16. ファイル共有を再作成します。
バックアップデータを使用して回復しているため、[共有追加] ダイアログの [共有ディレクトリの所有者] で、必ず [既存ディレクトリをそのまま使用] を選択してください。
17. `lumapctl` コマンドを使用して、LU の自動割り当ての設定を通常モードに変更します。

監査ログを出力しているファイルシステムを回復した場合は、**ALog ConVerter** との連携を再設定する必要があります。`alogctl` コマンドで、**ALog ConVerter** との連携を無効にしたあと有効にしてください。両ノードでコマンドを実行してください。

4.8.6 プールの容量不足によってノード上のファイルシステムが閉塞している場合

プールの容量不足によってノード上のファイルシステムが閉塞した場合の回復手順を次に示します。

1. ストレージシステムの管理者に依頼して、プールの容量不足を解決します。
ストレージシステム側でプールのフォーマット処理が動作していると、プールに空き容量が残っていても一時的に容量不足となる場合があります。ストレージシステムの管理者にフォーマット処理が完了しているか確認してください。
2. ノード上のリソースグループを手動でフェールオーバーします。
3. ノードを停止します。
4. OS を再起動します。
5. ノードを起動します。
6. リソースグループを元のノードにフェールバックします。
7. クラスタ内の別のノードで手順 2～手順 6 の操作を実行します。

4.8.7 プールの容量不足によって Virtual Server 上のファイルシステムが閉塞している場合

プールの容量不足によって Virtual Server 上のファイルシステムが閉塞した場合の回復手順を次に示します。

1. ストレージシステムの管理者に依頼して、プールの容量不足を解決します。
ストレージシステム側でプールのフォーマット処理が動作していると、プールに空き容量が残っていても一時的に容量不足となる場合があります。ストレージシステムの管理者にフォーマット処理が完了しているか確認してください。
2. Virtual Server を再起動します。

4.8.8 階層ファイルシステム内の階層で容量が不足している場合

階層ファイルシステム内の一階層で容量が不足した場合、クライアントからファイルシステムに空き容量があるように見えていても、書き込めません。

階層ファイルシステム内の一階層で容量が不足した場合の回復手順を次に示します。

1. KAQG90004-W メッセージにファイルシステム名として出力されている文字列を確認します。
文字列がファイルシステム名の場合は Tier 1、「-2」で終わる文字列の場合は Tier 2 の容量が不足しています。
2. 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ます。
不要なファイルを削除する場合は、次のコマンドでファイルの格納先階層を確認してください。
tierfind <ファイルシステム名>
実行結果の例を次に示します。

```
0000000144 -rwxr-x--- -----2- 2011-09-21 04:33:55 ./subdir/file1
0000000139 -rwxr-x--- -----2- 2011-09-21 04:12:01 ./file2
0000000140 -rwxr-x--- ----- 2011-09-21 05:36:01 ./file3
0000000145 -rw-r--r-- ----- 2011-09-21 05:41:46 ./file4
```

各行の3列目の項目で、右から2文字目が「-」であるものが Tier 1にあるファイル（上記の file3, file4）、「2」であるものが Tier 2にあるファイル（上記の file1, file2）です。容量が不足している階層にある不要なファイルを削除してください。

3. Tier 1 の容量が不足していた場合は、arccorrection コマンドを実行します。

4.8.9 差分格納デバイスを設定したファイルシステムが閉塞している場合

障害が発生したファイルシステムに設定された差分格納デバイスを解除したあと、ファイルシステムの障害を回復します。なお、ファイルシステムで仮想 LU を使用している場合は、ノード上のシステムメッセージに KAQG90009-E が出力されているか確認してください。出力されていた場合は、「4.8.10 プールの容量不足によって差分格納デバイスを設定したファイルシステムが閉塞している場合（Virtual Server 未使用時）」に従って対処してください。

次の手順に従って対処してください。

1. ユーザーに、障害が発生したファイルシステムの差分スナップショットにアクセスできる場合は、必要なデータを任意の場所にコピーするように通知します。
ユーザーの作業が完了したら、次の手順に進んでください。
2. 障害が発生した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で、NFS 共有と CIFS 共有を解除します。

3. 障害が発生した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をアンマウントします。
4. 障害が発生したファイルシステムに設定された差分格納デバイスを解除します。
HFRR ペアとして定義したファイルシステムの場合、HFRR ペアを解除してから差分格納デバイスを解除してください。
5. ファイルシステムの障害を回復します。
6. 差分格納デバイスを再設定します。

4.8.10 プールの容量不足によって差分格納デバイスを設定したファイルシステムが閉塞している場合 (Virtual Server 未使用時)

障害が発生したファイルシステムに設定された差分格納デバイスを解除したあと、ファイルシステムの障害を回復します。なお、差分格納デバイスの状態が「Not available」以外の場合は、差分格納デバイスを解除する必要があるため、「4.8.6 プールの容量不足によってノード上のファイルシステムが閉塞している場合」に従って対処してください。

次の手順に従って対処してください。

1. ストレージシステムの管理者に依頼して、プールの容量不足を解決します。
ストレージシステム側でプールのフォーマット処理が動作していると、プールに空き容量が残っていても一時的に容量不足となる場合があります。ストレージシステムの管理者にフォーマット処理が完了しているか確認してください。
2. 障害が発生した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で、NFS 共有と CIFS 共有を解除します。
3. 障害が発生した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をアンマウントします。
4. 障害が発生したファイルシステムに設定された差分格納デバイスを解除します。
HFRR ペアとして定義したファイルシステムの場合、HFRR ペアを解除してから差分格納デバイスを解除してください。
5. ノード上のリソースグループを手動でフェールオーバーします。
6. ノードを停止します。
7. OS を再起動します。
8. ノードを起動します。
9. リソースグループを元のノードにフェールバックします。
10. クラスタ内の別のノードで手順 5～手順 9 の操作を実行します。
11. 差分格納デバイスを再設定します。

4.8.11 プールの容量不足によって差分格納デバイスを設定したファイルシステムが閉塞している場合 (Virtual Server 使用時)

障害が発生したファイルシステムに設定された差分格納デバイスを解除したあと、ファイルシステムの障害を回復します。なお、差分格納デバイスの状態が「Not available」以外の場合は、差分格納デバイスを解除する必要があるため、「4.8.6 プールの容量不足によってノード上のファイルシステムが閉塞している場合」に従って対処してください。

次の手順に従って対処してください。

1. ストレージシステムの管理者に依頼して、プールの容量不足を解決します。

ストレージシステム側でプールのフォーマット処理が動作していると、プールに空き容量が残っていても一時的に容量不足となる場合があります。ストレージシステムの管理者にフォーマット処理が完了しているか確認してください。

2. 障害が発生した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で、NFS 共有と CIFS 共有を解除します。
3. 障害が発生した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をアンマウントします。
4. 障害が発生したファイルシステムに設定された差分格納デバイスを解除します。
HFRR ペアとして定義したファイルシステムの場合、HFRR ペアを解除してから差分格納デバイスを解除してください。
5. Virtual Server を再起動します。
6. 差分格納デバイスを再設定します。

4.9 差分格納デバイスの障害を回復する

ここでは、差分格納デバイスで障害が発生した場合の対処方法について説明します。

4.9.1 差分格納デバイスの容量が不足した場合（状態が Overflow のとき）

差分格納デバイスの容量が不足した場合は、あふれ時の動作の設定によって、差分格納デバイスの状態は Overflow または Blocked になります。

差分格納デバイスの状態が Overflow になると、差分格納デバイスを設定した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。ただし、ファイルシステムはそのまま使用できます。

差分格納デバイスの状態が Overflow になった場合の対処方法を次に示します。

1. 差分スナップショットを利用しているユーザーに、差分スナップショットのデータが失われたことを通知します。
2. Hitachi File Remote Replicator を利用している場合、`ruspairdelete` コマンドに `--delete` オプションを指定して実行し、HFRR ペアを強制解除します。
3. 容量が不足した差分格納デバイスに格納されたすべての差分スナップショットで、NFS 共有と CIFS 共有を解除します。
4. 容量が不足した差分格納デバイスに格納されたすべての差分スナップショットをアンマウントします。
5. 差分格納デバイスの状況に応じて、次のどちらかの方法で対処します。

現在の差分格納デバイスを継続して使用したい場合

設定元の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をまとめて削除します。GUI の [全削除] ボタンまたは `syncdel` コマンドの `-a` オプションを使用してください。

差分格納デバイスの容量を見直したい場合

差分格納デバイスをいったん解除したあと、差分格納デバイスに必要な容量を見直して再設定します。

差分格納デバイスに必要な容量を設計する方法については、「システム構成ガイド（差分格納デバイスの容量の設計）」を参照してください。

6. 差分スナップショットの自動作成スケジュールを使用して運用していた場合は、自動作成スケジュールが有効になるよう設定を変更します。
なお、この手順は、Hitachi File Remote Replicator のセカンダリーサイトの場合には不要です。
7. Hitachi File Remote Replicator を利用している場合、セカンダリーサイトから `ruspairdefine` コマンドを実行して HFRR ペアを再定義し、`ruscopy` コマンドを実行して Hitachi File Remote Replicator の運用を再開します。

4.9.2 差分格納デバイスの容量が不足した場合（状態が Blocked のとき）

差分格納デバイスの容量が不足した場合は、あふれ時の動作の設定によって、差分格納デバイスの状態は Overflow または Blocked になります。ここでは、Blocked になったときの対処について説明します。

差分格納デバイスの状態が Blocked になると、ファイルシステムの使用が一時的に制限されます。ただし、差分スナップショットのデータは無効になりません。

参考：

差分格納デバイスの状態が Blocked になった場合、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は参照できなくなります。下記の手順で回復する前に差分スナップショットを参照するには、差分スナップショットにファイル共有を作成する必要があります。

次の手順に従って対処してください。

1. 差分スナップショットを利用しているユーザーに、ファイルシステムへの書き込みが停止されたことを通知します。
2. 次のどちらかの方法で、差分格納デバイスの使用量が警告閾値を下回るまで空き容量を増やします。
 - 差分格納デバイスを拡張する。
差分格納デバイスに必要な容量を設計し直し、デバイスファイルを追加してください。
差分格納デバイスに必要な容量を設計する方法については、「システム構成ガイド（差分格納デバイスの容量の設計）」を参照してください。
 - 不要な差分スナップショットの NFS 共有および CIFS 共有を解除し、アンマウントしてから削除する。
3. `syncrepair` コマンドでファイルシステムを回復します。
4. 差分スナップショットの自動作成スケジュールを使用して運用していた場合は、自動作成スケジュールが有効になるよう設定を変更します。

4.9.3 デバイスファイルにアクセス障害が発生した場合（Virtual Server 未使用時）

Virtual Server を使用していない場合に、デバイスファイルにアクセス障害が発生したときは、次の手順で障害を回復してください。

1. GUI または `fpstatus` コマンドで FC パスの状態を確認します。

FC パスの状態が正常な場合

ストレージシステムに障害が発生しているかどうか保守員に確認してください。障害が発生していた場合は、「(1) ストレージシステムに障害が発生した場合」の手順を実行してください。

FC パスの状態が正常でない場合

「4.17 FC パスの障害を回復する」に従って対処してください。そのあと、次の手順に進んでください。

2. 差分格納デバイスの状態を確認します。

差分格納デバイスの状態が「Not available」の場合は、「(2) 差分格納デバイスの障害の回復」の手順を実行してください。

(1) ストレージシステムに障害が発生した場合

保守員と連携して次の操作を実行します。

1. lumapctl コマンドを使用して、ユーザー LU の割り当て機能を保守モードに設定します。
2. 障害が発生したデバイスファイルを含むファイルシステムについて、次の操作を実行します。
 - (a) すべての差分スナップショットのファイル共有の解除およびアンマウント
 - (b) 差分格納デバイスの解除
HFRR ペアとして定義したファイルシステムの場合、HFRR ペアを解除してから差分格納デバイスを解除してください。
 - (c) ファイルシステムの削除
3. 障害が発生したデバイスファイルを含む差分格納デバイスについて、次の操作を実行します。
 - (a) すべての差分スナップショットのファイル共有の解除およびアンマウント
 - (b) 差分格納デバイスの解除
HFRR ペアとして定義したファイルシステムの場合、HFRR ペアを解除してから差分格納デバイスを解除してください。
4. クラスタ内の別のノードで手順 2 および手順 3 の操作を実行します。
5. 保守員に依頼して、ストレージシステムの障害を取り除きます。
6. ノード上のリソースグループをクラスタ内の別のノードにフェールオーバー・フェールバックします。
7. ノードを停止します。
8. OS を再起動します。
9. ノードを起動します。
10. ノード上で元から稼働していたリソースグループをフェールバックします。
11. クラスタ内の別のノードで手順 6～手順 10 の操作を実行します。
12. 手順 2 で削除したファイルシステムを再構築します。
13. 再構築したファイルシステムにバックアップデータを回復します。
14. 差分格納デバイスを再設定します。
15. lumapctl コマンドを使用して、ユーザー LU の割り当て機能を通常運用モードに設定します。

(2) 差分格納デバイスの障害の回復

次の手順で差分格納デバイスの障害を回復します。

1. 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で、CIFS 共有を解除します。
2. 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をアンマウントします。
3. 差分格納デバイスを解除します。
HFRR ペアとして定義したファイルシステムの場合、HFRR ペアを解除してから差分格納デバイスを解除してください。

4. ノード上のリソースグループをクラスタ内の別のノードにフェールオーバー・フェールバックします。
5. ノードを停止します。
6. OS を再起動します。
7. ノードを起動します。
8. ノード上で元から稼働していたリソースグループをフェールバックします。
9. クラスタ内の別のノードで手順 4～手順 8 の操作を実行します。

4.9.4 デバイスファイルにアクセス障害が発生した場合（Virtual Server 使用時）

Virtual Server を使用している場合に、デバイスファイルにアクセス障害が発生したときは、次の手順で障害を回復してください。

1. FC パスの状態を確認します。

FC パスの状態が正常な場合

ストレージシステムに障害が発生しているかどうか保守員に確認してください。障害が発生していた場合は、「(1) ストレージシステムに障害が発生した場合」の手順を実行してください。

FC パスの状態が正常でない場合

「4.17 FC パスの障害を回復する」に従って対処してください。そのあと、次の手順に進んでください。

2. 差分格納デバイスの状態を確認します。

差分格納デバイスの状態が「Not available」の場合は、「(2) 差分格納デバイスの障害の回復」の手順を実行してください。

(1) ストレージシステムに障害が発生した場合

保守員と連携して次の操作を実行します。

1. lumapctl コマンドを使用して、ユーザー LU の割り当て機能を保守モードに設定します。
2. 障害が発生したデバイスファイルを含むファイルシステムについて、次の操作を実行します。
 - (a) すべての差分スナップショットのファイル共有の解除およびアンマウント
 - (b) 差分格納デバイスの解除
HFRR ペアとして定義したファイルシステムの場合、HFRR ペアを解除してから差分格納デバイスを解除してください。
 - (c) ファイルシステムの削除
3. 障害が発生したデバイスファイルを含む差分格納デバイスについて、次の操作を実行します。
 - (a) すべての差分スナップショットのファイル共有の解除およびアンマウント
 - (b) 差分格納デバイスの解除
HFRR ペアとして定義したファイルシステムの場合、HFRR ペアを解除してから差分格納デバイスを解除してください。
4. すべての Virtual Server で手順 2 および手順 3 の操作を実行します。
5. 保守員に依頼して、ストレージシステムの障害を取り除きます。
6. 障害が発生した Virtual Server が稼働しているノードに正常な Virtual Server がある場合、フェールオーバーします。
障害が発生した Virtual Server はフェールオーバーできません。

7. 障害が発生した Virtual Server が稼働しているノードの Dump の取得を保守員に依頼します。
8. Virtual Server をフェールバックします。
9. 手順 2 で削除したファイルシステムを再構築します。
10. 再構築したファイルシステムにバックアップデータを回復します。
11. 差分格納デバイスを再設定します。
12. lumapctl コマンドを使用して、ユーザー LU の割り当て機能を通常運用モードに設定します。

(2) 差分格納デバイスの障害の回復

次の手順で差分格納デバイスの障害を回復します。

1. 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で、CIFS 共有を解除します。
2. 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をアンマウントします。
3. 差分格納デバイスを解除します。
HFRR ペアとして定義したファイルシステムの場合、HFRR ペアを解除してから差分格納デバイスを解除してください。
4. 障害が発生した Virtual Server が稼働しているノードに正常な Virtual Server がある場合、フェールオーバーします。
障害が発生した Virtual Server はフェールオーバーできません。
5. 障害が発生した Virtual Server が稼働しているノードの Dump の取得を保守員に依頼します。
6. Virtual Server をフェールバックします。

4.10 差分スナップショットの障害を回復する

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処理の実行中に障害が発生した場合、差分スナップショットが閉塞することがあります。次の手順に従って対処してください。

1. 差分格納デバイスの状態を確認して、障害の要因を特定します。
GUI の [差分格納デバイスの状態] で確認できます。
 - 「Blocked」または「Overflow」が表示されている場合
差分格納デバイスの容量が不足しています。
 - 「I/O error」が表示されている場合
デバイスファイルにアクセス障害が発生しているおそれがあります。デバイスファイルにアクセス障害が発生しているかどうか保守員に確認してください。
 - 「Not available」が表示されている場合
[Cluster Management] ダイアログの [Browse Cluster Status] ページでクラスタ、ノードおよびリソースグループの状態を確認してください。状態に問題がない場合は、保守員に連絡して、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にアクセス障害が発生していないか確認してください。
 - 上記以外が表示されている場合
保守員に障害情報の取得を依頼してください。
2. 差分スナップショットがマウントされている場合は、アンマウントします。
3. リソースグループをフェールオーバーします。
4. ノードを停止します。

5. OS を再起動します。
6. ノードを起動します。
7. リソースグループをフェールバックします。
8. 手順 1 で特定した障害の要因に応じて、必要な対処を実施します。
 - 差分格納デバイスの容量が不足している場合
差分格納デバイスの状態に応じて、「4.9.1 差分格納デバイスの容量が不足した場合（状態が **Overflow** のとき）」または「4.9.2 差分格納デバイスの容量が不足した場合（状態が **Blocked** のとき）」の手順に従って対処してください。
 - デバイスファイルにアクセス障害が発生している場合
「4.9.3 デバイスファイルにアクセス障害が発生した場合（Virtual Server 未使用時）」の手順に従って対処してください。

4.10.1 Virtual Server を使用していない場合

Virtual Server を使用していない場合、次の手順に従って対処してください。

1. 差分格納デバイスの状態を確認して、障害の要因を特定します。
GUI の [差分格納デバイスの状態] で確認できます。
 - 「Blocked」または「Overflow」が表示されている場合
差分格納デバイスの容量が不足しています。
 - 「I/O error」が表示されている場合
デバイスファイルにアクセス障害が発生しているおそれがあります。デバイスファイルにアクセス障害が発生しているかどうか保守員に確認してください。
 - 「Not available」が表示されている場合
[Cluster Management] ダイアログの [Browse Cluster Status] ページでクラスタ、ノードおよびリソースグループの状態を確認してください。状態に問題がない場合は、保守員に連絡して、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にアクセス障害が発生していないか確認してください。
 - 上記以外が表示されている場合
保守員に障害情報の取得を依頼してください。
2. 差分スナップショットがマウントされている場合は、アンマウントします。
3. リソースグループをフェールオーバーします。
4. ノードを停止します。
5. OS を再起動します。
6. ノードを起動します。
7. リソースグループをフェールバックします。
8. 手順 1 で特定した障害の要因に応じて、必要な対処を実施します。
 - 差分格納デバイスの容量が不足している場合
差分格納デバイスの状態に応じて、「4.9.1 差分格納デバイスの容量が不足した場合（状態が **Overflow** のとき）」または「4.9.2 差分格納デバイスの容量が不足した場合（状態が **Blocked** のとき）」の手順に従って対処してください。
 - デバイスファイルにアクセス障害が発生している場合
「4.9.3 デバイスファイルにアクセス障害が発生した場合（Virtual Server 未使用時）」の手順に従って対処してください。

4.10.2 Virtual Server を使用している場合

Virtual Server を使用している場合、次の手順に従って対処してください。

1. 差分格納デバイスの状態を確認して、障害の要因を特定します。
GUI の [差分格納デバイスの状態] で確認できます。
 - 「Blocked」または「Overflow」が表示されている場合
差分格納デバイスの容量が不足しています。
 - 「I/O error」が表示されている場合
デバイスファイルにアクセス障害が発生しているおそれがあります。デバイスファイルにアクセス障害が発生しているかどうか保守員に確認してください。
 - 「Not available」が表示されている場合
[Cluster Management] ダイアログの [Browse Cluster Status] ページでクラスタ、ノードおよびリソースグループの状態を確認してください。または、[< Virtual Server >] サブウィンドウで Virtual Server の状態を確認してください。状態に問題がない場合は、保守員に連絡して、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にアクセス障害が発生していないか確認してください。
 - 上記以外が表示されている場合
保守員に障害情報の取得を依頼してください。
2. 差分スナップショットがマウントされている場合は、アンマウントします。
3. 障害が発生した Virtual Server が稼働しているノードに正常な Virtual Server がある場合、フェールオーバーします。
障害が発生した Virtual Server はフェールオーバーできません。
4. 障害が発生した Virtual Server を強制停止します。
5. 手順 4 で強制停止した Virtual Server を起動します。
6. Virtual Server をフェールバックします。
7. 手順 1 で特定した障害の要因に応じて、必要な対処を実施します。
 - 差分格納デバイスの容量が不足している場合
差分格納デバイスの状態に応じて、「[4.9.1 差分格納デバイスの容量が不足した場合（状態が Overflow のとき）](#)」または「[4.9.2 差分格納デバイスの容量が不足した場合（状態が Blocked のとき）](#)」の手順に従って対処してください。
 - デバイスファイルにアクセス障害が発生している場合
「[4.9.4 デバイスファイルにアクセス障害が発生した場合（Virtual Server 使用時）](#)」の手順に従って対処してください。

4.11 HCP へのアクセス障害を回復する

ネットワークを介してリモートの HCP と連携している場合に、次のような HCP にアクセスできない障害が発生したとき、要因を特定して障害を回復します。

- クライアントが HCP にマイグレートしたファイルにアクセスできない
- マイグレーションが失敗した
- マイグレーションポリシーが登録できない

HCP へのアクセス障害を回復する手順を次に示します。

1. クライアントが HCP にマイグレートしたファイルにアクセスできない場合は、20 分待ったあと、クライアントに対象のファイルに再度アクセスするよう依頼します。
アクセスできた場合は対処の必要はありません。アクセスできなかった場合は次の手順に進んでください。
2. HCP の接続状態および設定を確認します。
hcpaccesstest コマンドで HCP にアクセスできるかを確認します。アクセスできない場合は、archcpget コマンドで HCP の情報が正しく設定されているかを確認します。正しく設定されていない場合は archcpset コマンドで再度設定してください。そのあと、hcpaccesstest コマンドで HCP にアクセスできるかを再度確認してください。
3. エラーメッセージを確認します。
KAQM37070-E または KAQM37094-E メッセージが出力されている場合は、HCP で障害が発生しています。HCP の管理者に障害の回復を依頼してください。
次のどれかのメッセージが出力されている場合は、HCP に負荷が掛かっているか、HVFP と HCP 間のネットワークで障害が発生しているおそれがあります。
KAQM37037-E, KAQM37042-E~KAQM37045-E, KAQM37049-E, KAQM37120-E
HCP へのアクセス障害の要因を調査中であることを HCP 管理者に連絡したあと、手順 4. に進んでください。
上記以外の「KAQM37」で始まるメッセージが出力されていた場合は、メッセージの対処に従ってください。
4. ハードウェアおよびクラスタの状態を確認します。
障害が発生していた場合は保守員に連絡してください。問題がない場合は次の手順に進んでください。
5. NAT, フロントエンド LAN のスイッチおよび DNS サーバの状態を確認します。
障害が発生していた場合は回復してください。問題がない場合は次の手順に進んでください。
6. HCP の管理者に HCP の状態を確認します。
HCP が停止している場合は、HCP の管理者に運用を再開する時刻を確認します。クライアントに、HCP のメンテナンスまたは障害の回復が完了するまで待ってから、アクセスを再開するように連絡してください。
HCP の状態に問題がない場合は、ネットワークの障害です。WAN サービス事業者の保守員に連絡してください。
7. 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利用するエンドユーザーに、ホームディレクトリ下に .conflict ディレクトリが作成されていないかの確認を依頼します。
.conflict ディレクトリがある場合は、.conflict ディレクトリ内のファイルを確認し、必要に応じてホームディレクトリ下の元のファイルに内容を反映するよう、エンドユーザーに依頼してください。

4.12 HCP にデータをマイグレートしていたファイルシステムをリストアする

LU の障害などによって、HCP にデータをマイグレートしていたファイルシステムが無効になったとき、HCP にマイグレートされているデータを使用してファイルシステムをリストアします。リストアする前に、障害を回復しておいてください。

マイグレートされたファイルをスタブ化している場合は「4.12.1 ファイルをスタブ化している場合」、スタブ化していない場合は「4.12.2 ファイルをスタブ化していない場合」の手順を実施してください。

4.12.1 ファイルをスタブ化している場合

マイグレートされたファイルをスタブ化している場合に、HCP から HVFP のファイルシステムにデータをリストアする手順を次に示します。

1. リストアするファイルシステムを構築し、読み書きできる状態でマウントします。
次のとおり指定してファイルシステムを構築してください。
 - 障害が発生したファイルシステム以上の容量にする
 - 障害が発生したファイルシステムと同じ ACL タイプを指定する
 - 障害が発生したファイルシステムで WORM が有効になっていた場合は、WORM を有効にする
 - 障害が発生したファイルシステムでホームディレクトリローミング機能が有効になっていた場合は、ホームディレクトリローミング機能を有効にする
 - 障害が発生したファイルシステムで過去バージョンのファイルをクライアントに公開していた場合は、過去バージョンのファイルをクライアントに公開する
 - 障害が発生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になっていた場合は、CIFS 走査チェックのバイパス機能を有効にする
2. `arcrestore` コマンドを使用して、ファイルシステムをリストアします。



重要

- ・ リストアするファイルシステムにすでにファイルやディレクトリが作成されていると、`arcrestore` コマンドを実行できません。また、`arcrestore` コマンドを実行する前にファイル共有を作成すると、HCP からデータをリストアできないことがあります。
- ・ `KAQM37080-E` メッセージが出力されてリストア処理が中断された場合は、メッセージに従って対処したあと、`--skip` オプションを指定して `arcrestore` コマンドを再度実行してください。

3. ファイルシステムにファイル共有を作成します。
4. マイグレーションポリシーを設定します。

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でリストアされます。

また、手順を実施したあと、すべてのデータがリストアされるまでに時間が掛かるため、リストアされていないデータにクライアントがアクセスすることがあります。このとき、親ディレクトリに大量のデータが格納されていると、ファイル一覧の表示に時間が掛かるため、CIFS クライアントでタイムアウトが発生し、アクセスに失敗するおそれがあります。その場合はしばらく待ってから再度アクセスするようにクライアントに連絡してください。

テープ装置にバックアップを取得している場合は、テープ装置のデータもリストアしてください。

マイグレーション中に障害が発生していた場合、一部のファイルがリストアされないことがあります。その場合は、過去バージョンディレクトリからファイルをリストアしてください。過去バージョンディレクトリからファイルをリストアできないときは、次の手順に従って、ファイルをリストアしてください。

1. `--display` オプションを指定しないで `hcopphanrestore` 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。
2. 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/`

なお、ファイルシステムの運用中でもこの手順を実行できますが、手順を実行中に HCP へのマイグレーションが動作すると、不整合がないファイルも復元されることがあります。復元されたファイルがファイルシステムに存在しないことを確認してからコピーするようにしてください。

4.12.2 ファイルをスタブ化していない場合

マイグレートされたファイルをスタブ化していない場合に、HCP から HVFP のファイルシステムにデータをリストアする手順を次に示します。

1. リストアするファイルシステムを構築し、読み書きできる状態でマウントします。
次のとおり指定してファイルシステムを構築してください。
 - 障害が発生したファイルシステム以上の容量にする
 - 障害が発生したファイルシステムと同じ ACL タイプを指定する
 - 障害が発生したファイルシステムで WORM が有効になっていた場合は、WORM を有効にする
 - 障害が発生したファイルシステムでホームディレクトリローミング機能が有効になっていた場合は、ホームディレクトリローミング機能を有効にする
 - 障害が発生したファイルシステムで過去バージョンのファイルをクライアントに公開していた場合は、過去バージョンのファイルをクライアントに公開する
 - 障害が発生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になっていた場合は、CIFS 走査チェックのバイパス機能を有効にする
2. `arcrcplimitset` コマンドでファイルシステムのスタブ化閾値を `OGB` に設定します。
次のとおりオプションを指定してください。
`arcrcplimitset --rest-size 0g --file-system <ファイルシステム名>`
3. `arcrcstore` コマンドでファイルシステムをリストアします。



重要

- リストアするファイルシステムにすでにファイルやディレクトリが作成されていると、`arcrcstore` コマンドを実行できません。また、`arcrcstore` コマンドを実行する前にファイル共有を作成すると、HCP からデータをリストアできないことがあります。
- `KAQM37080-E` メッセージが出力されてリストア処理が中断された場合は、メッセージに従って対処したあと、`--skip` オプションを指定して `arcrcstore` コマンドを再度実行してください。

4. ファイルシステムにファイル共有を作成します。
5. マイグレーションポリシーを設定します。
6. `--file-system <ファイルシステム名>` オプションを指定して `arcrcresidentpolicylist` コマンドを実行し、キャッシュ常駐ポリシーの設定を確認します。
ファイルシステム上のすべてのオブジェクトが対象になっている場合は、以降の手順は不要です。
7. `arcrcresidentpolicyset` コマンドでファイルシステム上のすべてのオブジェクトを対象に、キャッシュ常駐ポリシーを設定します。
次のとおりオプションを指定してください。
`arcrcresidentpolicyset --policy <ポリシー名> --file-system <ファイルシステム名>`
0 時になると、設定したキャッシュ常駐ポリシーに従いデータがリコールされます。
8. リコール後しばらく待ってから、`--file-system <ファイルシステム名>` オプションを指定して `arcrcresidentresult` コマンドを実行し、キャッシュ常駐ポリシーの実行結果を確認します。
問題なく実行されたこと、また、キャッシュ常駐ポリシーの実行によってシステムメッセージファイルに `KAQM37` メッセージが出力されていないことを確認します。
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でリストアされます。

設定したキャッシュ常駐ポリシーに従いデータがリコールされるまでは、親ディレクトリに大量のデータが格納されていると、ファイル一覧の表示に時間が掛かるため、CIFS クライアントでタイムアウトが発生し、アクセスに失敗するおそれがあります。その場合はしばらく待ってから再度アクセスするようにクライアントに連絡してください。

テープ装置にバックアップを取得している場合は、テープ装置のデータもリストアしてください。

マイグレーション中に障害が発生していた場合、一部のファイルがリストアされないことがあります。その場合は、過去バージョンディレクトリからファイルをリストアしてください。過去バージョンディレクトリからファイルをリストアできないときは、次の手順に従って、ファイルをリストアしてください。

1. `--display` オプションを指定しないで `hccporphanrestore` 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。
2. 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/`

なお、ファイルシステムの運用中でもこの手順を実行できますが、手順を実行中に HCP へのマイグレーションが動作すると、不整合がないファイルも復元されることがあります。復元されたファイルがファイルシステムに存在しないことを確認してからコピーするようにしてください。

4.13 ファイルシステムおよびプライマリー HCP の障害時にレプリカ HCP からファイルシステムをリストアする

ファイルシステムおよびプライマリー HCP に障害が発生した場合、レプリカ HCP から HVFP にファイルシステムをリストアします。

1. レプリカ HCP からフェールオーバーを実行し、レプリカ HCP 側で読み書きできる状態にします。
2. `archcpset` コマンドまたは GUI を使用して、HCP のホスト名にレプリカ HCP のホスト名を設定します。
3. `fscreate` コマンドまたは GUI を使用して、HCP に対してマイグレーション運用を行うファイルシステムを再構築します。

次のとおり指定してファイルシステムを構築してください。

- 障害が発生したファイルシステム以上の容量にする
 - 障害が発生したファイルシステムと同じ ACL タイプを指定する
 - 障害が発生したファイルシステムで WORM が有効になっていた場合は、WORM を有効にする
 - 障害が発生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になっていた場合は、CIFS 走査チェックのバイパス機能を有効にする
4. `arcrestore` コマンドでレプリカ HCP から HVFP にファイルシステムをリストアします。*



重要

- ・ リストアするファイルシステムにすでにファイルやディレクトリが作成されていると、`arcrestore` コマンドを実行できません。また、`arcrestore` コマンドを実行する前にファイル共有を作成すると、HCP からデータをリストアできないことがあります。
- ・ `KAQM37080-E` メッセージが出力されてリストア処理が中断された場合は、メッセージに従って対処したあと、`--skip` オプションを指定して `arcrestore` コマンドを再度実行してください。

5. ファイルシステムにファイル共有を作成します。

6. マイグレーションポリシーを設定します。
7. レプリカ HCP 側で運用を開始します。
8. プライマリー HCP が復旧します。
9. レプリカ HCP からデータリカバリーを実行し、レプリカ HCP のデータをプライマリー HCP にコピーします。
10. プライマリー HCP とレプリカ HCP でデータリカバリーを終了させます。
11. archcpset コマンドまたは GUI を使用して、HCP のホスト名にプライマリー HCP のホスト名を設定し直します。
12. プライマリー HCP 側で運用を開始します。

注意：早急にデータを参照したい場合、手順 2 から手順 5 を実施することでデータを参照できます。ただし、レプリカ HCP が読み取り専用であるため、手順 4 で一部の過去バージョンディレクトリの復元に失敗します。

マイグレーション中に障害が発生していた場合、一部のファイルがリストアされないことがあります。その場合は、過去バージョンディレクトリからファイルをリストアしてください。過去バージョンディレクトリからファイルをリストアできないときは、次の手順に従って、ファイルをリストアしてください。

1. --display オプションを指定しないで hcporphanrestore 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。
2. 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/

なお、ファイルシステムの運用中でもこの手順を実行できますが、手順を実行中に HCP へのマイグレーションが動作すると、不整合がないファイルも復元されることがあります。復元されたファイルがファイルシステムに存在しないことを確認してからコピーするようにしてください。

注※：レプリカ HCP の画面で確認できる「Backlog time」+ 3 時間以内に更新されたファイルは、最新のデータがレプリカ HCP にコピーされていないおそれがあります。

4.14 マイグレートされたファイルをスタブ化していない場合に HVFP から HCP のデータをリストアする

HCP にマイグレートされたファイルをスタブ化していない状態で HCP に障害が発生し、回復時に HCP を初期化した場合に、HVFP から HCP にデータをリストアします。

1. --migrate-info オプションを指定して archcpget コマンドを実行し、マイグレーションの情報を確認します。
ファイルシステムのマイグレーション先ネームスペース、およびシステム設定情報を保存しているネームスペースを確認します。
2. HCP にテナントおよび手順 1 で確認したネームスペースを作成します。
作成したすべてのネームスペースにアクセスする権限をユーザーアカウントに設定してください。
3. --namespace <ネームスペース名> オプションを指定して hcpaccesstest コマンドを実行し、手順 2 で作成したすべてのネームスペースへの接続を確認します。
4. -d trans オプションを指定して syslusave コマンドを実行し、HCP にシステム設定情報を転送します。

5. マイグレーション運用しているすべてのファイルシステムに対して `arccorrection` コマンドを実行し、対象ファイルシステムのデータを HCP にマイグレートする準備をします。

次のとおりオプションを指定してください。

```
arccorrection -t all -V --file-system <ファイルシステム名>
```

実行結果として `KAQM37137-I` および `KAQM37378-I` メッセージのあとに `KAQM37140-E` が出力された場合は、メッセージに従って対処したあと、`arccorrection` コマンドを再度実行してください。`KAQM37137-I` および `KAQM37378-I` が出力されていない場合は、オプションの指定を確認して `arccorrection` コマンドを実行してください。

`arccorrection` コマンドの実行後にマイグレーションタスクが実行されると、対象ファイルシステムのデータが HCP にマイグレートされます。すぐに HCP ヘデータをマイグレートしたい場合は、マイグレーションを即時実行するポリシーを新たに設定してください。

4.15 システム設定情報を回復する

ここでは、ノードの OS ディスク、Virtual Server OS LU または共有 LU で障害が発生し、システム設定情報が無効になった場合の対処方法について説明します。保守員と連携して対処してください。なお、HCP にデータをマイグレートしている場合は、システム設定情報およびユーザーデータを HCP から一括で回復できます。HCP からシステム設定情報およびユーザーデータを一括で回復する場合は、「4.16 システム設定情報およびユーザーデータを一括で回復する」を参照してください。

障害部分によって次のとおり回復手順が異なります。

どちらか一方のノードの OS ディスクに障害が発生した場合

「4.15.1 OS ディスクに障害が発生している場合」を参照してください。

共有 LU に障害が発生した場合

「4.15.2 共有 LU に障害が発生している場合」を参照してください。

両方のノードの OS ディスクおよび共有 LU のうち、複数のディスクに障害が発生した場合

「4.15.3 ノードの OS ディスクまたは共有 LU で障害が発生している場合」を参照してください。

Virtual Server OS LU に障害が発生した場合

「4.15.4 Virtual Server OS LU に障害が発生している場合」を参照してください。

4.15.1 OS ディスクに障害が発生している場合

ノードの OS ディスクに障害が発生し、システム設定情報が無効になった場合、システム管理者は OS ディスクにシステム設定情報を回復します。

ノードの OS ディスクに障害が発生した場合のシステム設定情報の回復手順を次に示します。

1. 保守員にハードウェア障害部分の交換および初期セットアップを依頼します。

2. 管理コンソールに SSH 秘密鍵を用意します。

インストールメディア内の次のファイルに格納されている秘密鍵を使用してください。

PuTTY を使用する場合

```
<インストールメディアのドライブ>:system\ssh\defaultsetupkeyputty.ppk
```

PuTTY 以外の SSH クライアントを使用する場合

```
<インストールメディアのドライブ>:system\ssh\defaultsetupkey
```

この鍵を使用して SSH アカウント (nasroot) で回復対象のノードにログインし、以降の手順のコマンドを実行してください。なお、対応する公開鍵は、手順 4 が完了したあと、ノード上から自動的に削除されます。

3. もう一方のノードの固有 IP アドレスを確認します。
4. `syslurestore` コマンドで、手順 3 で確認した固有 IP アドレスを指定して OS ディスクを回復します。
5. 回復したノードを起動します。
6. 回復したノードにリソースグループをフェールバックします。
7. NDMP サーバを使用していた場合は、NDMP サーバのパスワードを変更します。
NDMP サーバを使用していた場合、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。

4.15.2 共有 LU に障害が発生している場合

共有 LU に障害が発生し、システム設定情報が無効になった場合、システム管理者は共有 LU にシステム設定情報を回復します。

共有 LU に障害が発生した場合のシステム設定情報の回復手順を次に示します。

1. 保守員にハードウェア障害部分の交換を依頼します。
2. `syslurestore` コマンドを使用して共有 LU を回復します。
3. クラスタを再定義します。
4. クラスタおよびすべてのリソースグループまたは **Virtual Server** を起動します。
5. NFS サービスおよび仮想 IP アドレスの情報を再設定するよう促す警告メッセージが出力された場合は、それらの情報を再設定します。

4.15.3 ノードの OS ディスクまたは共有 LU で障害が発生している場合

ノードの OS ディスクまたは共有 LU で障害が発生し、システム設定情報が無効になった場合、システム管理者はノードの OS ディスクおよび共有 LU にすべてのシステム設定情報を回復します。なお、システム設定情報の回復操作を行っても、ノードに登録されている管理サーバの認証パスワードは初期パスワードになっています。必要に応じて下記の手順 8 で変更してください。

`syslurestore` コマンドでシステム設定情報を回復したあと、コマンドを実行するためには、障害発生前にノードに登録されていた SSH 公開鍵に対応する SSH 秘密鍵が必要です。SSH 秘密鍵を確認し、使用できるように用意しておいてください。

ノードの OS ディスクまたは共有 LU に障害が発生した場合のシステム設定情報の回復手順を次に示します。

1. 保守員にハードウェア障害部分の交換および初期セットアップを依頼します。
2. 管理コンソールに SSH 秘密鍵を用意します。
インストールメディア内の次のファイルに格納されている秘密鍵を使用してください。

PuTTY を使用する場合

```
<インストールメディアのドライブ>:system¥ssh¥defaultsetupkeyputty.ppk
```

PuTTY 以外の SSH クライアントを使用する場合

```
<インストールメディアのドライブ>:system¥ssh¥defaultsetupkey
```

この鍵を使用して SSH アカウント (nasroot) でノードにログインし、以降の手順のコマンドを実行してください。なお、対応する公開鍵は、手順 4 が完了したあと、ノード上から自動的に削除されます。

3. ダウンロードしておいたシステム設定情報ファイルをアップロードします。
なお、GUI でアップロードする場合は、管理サーバの初期パスワードを使用してください。
システム設定情報ファイルをアップロードする手順を示します。
 - a. [< Physical Node >] サブウィンドウで [設定] タブの [アドバンスド] サブタブから、[バックアップ設定] をクリックして、[Backup Configuration] ダイアログの [Save System Settings Menu] ページを起動します。
 - b. [Upload Saved Data] ボタンをクリックします。
 - c. [Upload Saved Data] ページの [Upload] ボタンをクリックします。
 - d. [Select Saved Data File] ページの [Saved file] にアップロードするシステム設定情報ファイルのパスを絶対パスで指定して、システム設定情報ファイルをアップロードします。
[Browse] ボタンをクリックすると、ファイル名を参照して指定できます。
4. syslurestore コマンドを使用して、すべてのシステム LU を回復します。
障害発生前に登録されていた公開鍵も復元されます。次回ログイン時には、復元された公開鍵に対応する SSH 秘密鍵を使用してください。
5. クラスタを再定義します。
6. クラスタおよびリソースグループまたは Virtual Server を起動します。
7. 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. ノードおよび File Services Manager に登録されている管理サーバの認証パスワードを変更します。
ノードに登録されている管理サーバの認証パスワードを変更してから、File Services Manager でも同じパスワードを設定します。ノードに登録されている管理サーバの認証パスワードは hnasmpasswd コマンドで変更します。
9. 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ます。
10. アップロードしたシステム設定情報ファイルを削除します。
GUI を使用してアップロードしたシステム設定情報ファイルを削除する手順を示します。
 - a. [< Physical Node >] サブウィンドウで [設定] タブの [アドバンスド] サブタブから、[バックアップ設定] をクリックして、[Backup Configuration] ダイアログの [Save System Settings Menu] ページを起動します。
 - b. [Upload Saved Data] ボタンをクリックします。
 - c. [Upload Saved Data] ページの [Delete] ボタンをクリックして、システム設定情報ファイルを削除します。
11. NDMP サーバを使用していた場合は、NDMP サーバのパスワードを変更します。
NDMP サーバを使用していた場合、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。

4.15.4 Virtual Server OS LU に障害が発生している場合

Virtual Server OS LU に障害が発生し、システム設定情報が無効になった場合、システム管理者は Virtual Server OS LU にシステム設定情報を回復します。

Virtual Server OS LU に障害が発生した場合のシステム設定情報の回復手順を次に示します。

注意：手順 7、手順 8、手順 10 および手順 11 は Virtual Server 上で実行してください。そのほかの手順は Physical Node 上で実行してください。

1. Virtual Server の稼働状況を確認します。
vnaslist コマンドで Virtual Server の稼働状況を確認し「Offline」であれば、手順 3 へ進んでください。
2. Virtual Server を強制的に停止します。
3. ハードウェアに障害が発生し、交換が必要な場合は、保守員に交換および初期セットアップを依頼します。
Virtual Server OS LU に Hitachi AMS2000 シリーズまたは HUS100 シリーズの仮想 LU を使用している場合は、プールの容量が不足しているおそれがあります。ストレージシステムの管理者に依頼して、容量不足を解決してください。そのあと、Virtual Server OS LU について Dynamic Provisioning の全容量割当モードが有効になっているか確認し、無効な場合は有効にするようストレージシステム管理者に依頼してください。
4. vnasinit コマンドを使用して、Virtual Server OS LU を初期化します。
5. Virtual Server を起動します。
6. Virtual Server に管理 IP アドレスを割り当てていず、固有 IP アドレスが未設定の場合、Virtual Server に割り当てているネットワークインターフェースにルーティング情報を追加します。
7. ストレージシステム外に保存しておいた Virtual Server の設定情報ファイルを、Virtual Server にアップロードします。
 - a. [< Virtual Server >] サブウィンドウで [設定] タブの [アドバンスド] サブタブから、[バックアップ設定] をクリックして、[Backup Configuration] ダイアログの [Settings Backup Management] ページを起動します。
 - b. [Restore Settings] ボタンをクリックします。
 - c. [Browse Settings Upload Status] ページの [Upload] ボタンをクリックします。
 - d. [Select Backup File] ページの [Backup file] にアップロードするシステム設定情報ファイルのパスを絶対パスで指定して、システム設定情報ファイルをアップロードします。[Browse] ボタンをクリックすると、ファイル名を参照して指定できます。
HCP に転送した設定情報ファイルを使用する場合は、アップロードは必要ありません。必要に応じて arcproxysset コマンドおよび arcsslct1 コマンドでプロキシサーバおよび SSL の設定をしてください。
8. Virtual Server の設定情報を回復します。
[Settings Backup Management] ダイアログの [Browse Settings Upload Status] ページで、[Restore] ボタンから実行します。
HCP に転送した設定情報ファイルを使用する場合は、--trans オプションを指定して syslurestore コマンドを実行します。1 つのテナント上に複数のシステム設定情報を保存している場合は、システム設定情報を保存したときのホスト名も--system-name オプションで指定してください。
9. Virtual Server を再起動します。
10. アップロードした Virtual Server の設定情報ファイルを Virtual Server 上から削除します。
アップロードした Virtual Server のシステム設定情報ファイルを削除する手順を示します。
 - a. [< Virtual Server >] サブウィンドウで [設定] タブの [アドバンスド] サブタブから、[バックアップ設定] をクリックして、[Backup Configuration] ダイアログの [Settings Backup Management] ページを起動します。
 - b. [Restore Settings] ボタンをクリックします。

- c. [Browse Settings Upload Status] ページの [Delete] ボタンをクリックして、システム設定情報ファイルを削除します。
HCP に転送した設定情報ファイルを使用した場合は、設定情報ファイルを削除する必要はありません。
11. NDMP サーバを使用していた場合は、NDMP サーバのパスワードを変更します。
NDMP サーバを使用していた場合、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。

4.16 システム設定情報およびユーザーデータを一括で回復する

ここでは、HCP にシステム設定情報ファイルを保存し、ユーザーデータをマイグレートしている場合に、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、システム設定情報およびユーザーデータが無効になったときの対処方法について説明します。回復には、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。保守員と連携して対処してください。なお、事前に HCP の情報（ホスト名 (FQDN)、IP アドレス、テナント名およびアカウント情報）を用意しておいてください。

なお、`syslurestore` コマンドでシステム設定情報およびユーザーデータを回復したあと、コマンドを実行するためには、障害発生前にノードに登録されていた SSH 公開鍵に対応する SSH 秘密鍵が必要です。SSH 秘密鍵を確認し、使用できるように用意しておいてください。

ノードの OS ディスク、共有 LU およびユーザー LU で障害が発生した場合のシステム設定情報およびユーザーデータの回復手順を次に示します。

1. 保守員にハードウェア障害部分の交換および初期セットアップを依頼します。
作業完了後、HCP と通信するデータポートの情報（IP アドレス、ネットマスクおよびルーティング）を用意してください。
2. 管理コンソールに SSH 秘密鍵を用意します。
インストールメディア内の次のファイルに格納されている秘密鍵を使用してください。

PuTTY を使用する場合

```
<インストールメディアのドライブ>:system%ssh%defaultsetupkeyputty.ppk
```

PuTTY 以外の SSH クライアントを使用する場合

```
<インストールメディアのドライブ>:system%ssh%defaultsetupkey
```

この鍵を使用して SSH アカウント (nasroot) でノードにログインし、以降の手順のコマンドを実行してください。なお、対応する公開鍵は、手順 5 が完了したあと、ノード上から自動的に削除されます。

3. HCP との通信にプロキシサーバを使用していた場合は、`arcproxysset` コマンドでプロキシサーバを設定します。
システム設定情報を回復するまでホスト名の名前解決ができないため、プロキシサーバの情報は必ず IP アドレスで指定してください。
4. HCP との通信に HTTP を使用していた場合は、`arcsslct1` コマンドで通信方式を HTTP に変更します。
5. `syslurestore` コマンドでシステム設定情報およびユーザーデータを回復します。
`--trans` オプションを指定して `syslurestore` コマンドを実行します。1 つのテナント上に複数のシステム設定情報を保存している場合は、システム設定情報を保存したときのクラスタ名も `--system-name` オプションで指定してください。

障害発生前に登録されていた公開鍵も復元されます。次回ログイン時には、復元された公開鍵に対応する SSH 秘密鍵を使用してください。

なお、KAQM13186-W メッセージが出力された場合、クラスタを再定義したあとに、システムメッセージでエラーの詳細を確認し、ファイルシステムの再構築およびバックアップデータの回復を別途行う必要があります。ファイルシステムの再構築およびバックアップデータを回復する手順については「4.12 HCP にデータをマイグレートしていたファイルシステムをリストアする」を参照してください。

6. クラスタを再定義します。
7. クラスタおよびリソースグループを起動します。
8. 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。
9. ノードおよび File Services Manager に登録されている管理サーバの認証パスワードを変更します。
ノードに登録されている管理サーバの認証パスワードを変更してから、File Services Manager でも同じパスワードを設定します。ノードに登録されている管理サーバの認証パスワードは `hnasmpasswd` コマンドで変更します。
10. 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ます。
11. NDMP サーバを使用していた場合は、NDMP サーバのパスワードを変更します。
NDMP サーバを使用していた場合、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。

なお、次の情報は回復されません。

- 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
 - HCP に格納されたファイルの削除要求を送信するかどうか
 - 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

マウントされていなかったファイルシステムの上記の設定情報には、デフォルト値が設定されています。必要に応じて変更してください。Hitachi File Remote Replicator を使用していた場合は、ペアを再定義してください。このほか、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。

マイグレーション中に障害が発生していた場合、一部のファイルがリストアされないことがあります。その場合は、過去バージョンディレクトリからファイルをリストアしてください。過去バージョンディレクトリからファイルをリストアできないときは、次の手順に従って、ファイルをリストアしてください。

1. `--display` オプションを指定しないで `hccorporphanrestore` 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。
2. 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/`

なお、ファイルシステムの運用中でもこの手順を実行できますが、手順を実行中に HCP へのマイグレーションが動作すると、不整合がないファイルも復元されることがあります。復元されたファイルがファイルシステムに存在しないことを確認してからコピーするようにしてください。

4.17 FC パスの障害を回復する

FC パスに障害が発生したおそれがある場合、システム管理者は [ヘルスマニター] サブウィンドウの [ネットワーク] タブの [FC パス] サブタブ、または `fpstatus` コマンドで FC パスの状態を確認し、障害を回復します。

4.17.1 同一ターゲットへの片方のパスで「Error」が表示されている場合

同一ターゲットへの片方のパスに「Error」が表示されている場合、次のことが考えられます。

- (a) FC ケーブルが外れているなどの要因で、対象の FC パスに障害が発生している。
 - (b) FC パスの変更または削除を実施したあと、OS を再起動していない。
 - (c) FC パスに対応づけられたホストグループに LU が割り当てられていないため、FC パスが設定されていない。
- (a) または (b) の場合は次の手順に従って対処してください。(c) の場合は「4.17.5 同一ターゲットへの両方のパスで「Unknown」が表示されている場合」の手順に従って対処してください。

1. 状態が「Error」となっているパスの情報の、モデル名 (Model) とシリアル番号 (Serial) からストレージシステムを特定します。
2. このパスのノード側の FC ポート (HostPort)、手順 1. で特定したストレージシステムの FC ポート (ArrayPort) に接続された FC ケーブル、および FC スイッチの状態を確認します。

障害が発生していた場合

障害要因を取り除き、対象の FC パスを `fponline` コマンドでオンラインにしてください。

障害が発生していなかった場合

OS を再起動します。

3. `fpstatus` コマンドで対象の FC パスの状態を確認します。

4.17.2 同一ターゲットへの両方のパスで「Online (LU Error)」が表示されている場合

同一ターゲットへの両方のパスに「Online (LU Error)」が表示されている場合、対象のパスでアクセスしている一部の LU に障害が発生していることが考えられます。次の手順に従って対処してください。

1. 保守員と連携して、LU 障害を回復します。

障害が発生した LU がファイルシステムで使用されている場合は、「4.8 ファイルシステムの障害を回復する」のストレージシステムの障害によるファイルシステム閉塞の場合の手順に従っ

て対処してください。障害が発生した LU が差分格納デバイスで使用されている場合は、「4.9 差分格納デバイスの障害を回復する」の手順に従って対処してください。

2. fponline コマンドで対象の FC パスをオンラインにします。
3. fpstatus コマンドで対象の FC パスの状態を確認します。

4.17.3 同一ターゲットへの両方のパスで「Error」が表示されている場合

同一ターゲットへの両方のパスに「Error」が表示されている場合、次のことが考えられます。

(a) 対象の FC パスでアクセスしている全 LU に障害が発生しているか、対象の FC パスに障害が発生している。

(b) FC パスの変更または削除を実施したあと、OS を再起動していない。

(c) FC パスに対応づけられたホストグループに LU が割り当てられていないため、FC パスが設定されていない。

(a) または (b) の場合は次の手順に従って対処してください。(c) の場合は「4.17.5 同一ターゲットへの両方のパスで「Unknown」が表示されている場合」の手順に従って対処してください。

1. 状態が「Error」となっているパスの情報の、モデル名 (Model) とシリアル番号 (Serial) からストレージシステムを特定します。
2. このパスのノード側の FC ポート (HostPort), 手順 1 で特定したストレージシステムの FC ポート (ArrayPort) に接続された FC ケーブル, および FC スイッチの状態を確認します。

障害が発生していた場合

障害要因を取り除き、手順 3 に進みます。

障害が発生していなかった場合

OS を再起動し、FC パスの状態が正しく表示されることを確認します。

3. パス障害が発生していないノードから、パス障害が発生していたノード上で稼働していたリソースグループの状態を確認します。

フェールオーバーしていた場合

手順 5 に進みます。

フェールオーバーしていなかった場合

手順 4 に進みます。

4. パス障害が発生していないノードから、パス障害が発生していたノード上で稼働しているリソースグループを強制停止します。
5. パス障害が発生していないノードから、パス障害が発生していたノードの状態を確認します。

「UP」または「DOWN」の場合

手順 6 に進みます。

「UP」または「DOWN」以外の場合

手順 7 に進みます。

6. パス障害が発生していないノードから、パス障害が発生していたノードを強制停止します。
7. パス障害が発生していたノードで自ノードの OS を再起動します。
--force オプションを指定して nasreboot コマンドを実行してください。
8. パス障害が発生していたノードで自ノードを起動します。

次に実行する手順は、手順 3 で確認したリソースグループの状態によって次のとおり異なります。

パス障害が発生しているノードにリソースグループがフェールオーバーしていた場合
手順 11 に進みます。

パス障害が発生していないノードにリソースグループがフェールオーバーしていた場合
手順 10 に進みます。

フェールオーバーしていなかった場合
手順 9 に進みます。

9. パス障害が発生していたノードで、手順 4 で停止したリソースグループを起動します。
起動が完了したら、手順 11 に進んでください。
10. パス障害が発生していたノードから、パス障害が発生していないノードにフェールオーバーしているリソースグループをフェールバックします。
11. `fpstatus` コマンドで対象の FC パスの状態を確認します。
FC パスの状態が正常な場合は、ここで回復手順は終了です。FC パスに障害が発生している状態のままの場合、または障害を回復した FC パスのファイルシステムが閉塞している場合は手順 12. に進みます。
12. 保守員と連携して、LU 障害を回復します。
障害が発生した LU がファイルシステムで使用されている場合は、「4.8 ファイルシステムの障害を回復する」のストレージシステムの障害によるファイルシステム閉塞の場合の手順に従って対処してください。障害が発生した LU が差分格納デバイスで使用されている場合は、「4.9 差分格納デバイスの障害を回復する」の手順に従って対処してください。障害が発生した LU が共有 LU として使用されている場合は、「4.15 システム設定情報を回復する」を参照してください。障害が発生した LU が Virtual Server OS LU として使用されている場合は、同一ターゲットへの両方のパスに「Error」が表示されているノードの側の OS を再起動してください。
13. 対象の FC パスの状態を確認します。

4.17.4 同一ターゲットへの両方のパスで「Configuration Mismatch」が表示されている場合

同一ターゲットへの両方のパスで「Configuration Mismatch」が表示されている場合、FC パスに対応づけられたホストグループへの LU 割り当てが、交替パスの割り当てと異なることが考えられます。

次の手順に従って対処してください。

1. 状態が「Configuration Mismatch」となっているパスの情報の、モデル名 (Model) とシリアル番号 (Serial) からストレージシステムを特定します。
2. 交替パスが設定されていない場合は、保守員に交替パスを設定するよう依頼します。
3. 対象のパスの、手順 1 で特定したストレージシステムの FC ポート (ArrayPort) に設定された各ホストグループに、同じ LU が割り当てられているかを確認します。
設定が異なる場合は、設定が同じになるように LU を割り当ててください。LU を割り当てる際に LU パスを移動または削除する必要がある場合には、「ユーザズガイド」を参照してください。
4. 対象の FC パスの状態を確認します。

4.17.5 同一ターゲットへの両方のパスで「Unknown」が表示されている場合

同一ターゲットへの両方のパスで「Unknown」が表示されている場合、ホストポートまたはストレージポートを特定できないことが考えられます。この場合および FC パスに対応づけられたホストグループに LU が割り当てられていないため、FC パスが設定されていない場合は、次の手順に従って対処してください。

1. HBA カードが挿入されているか確認します。
2. 対象のパスのストレージシステム側の FC ポート (ArrayPort) が正しいか確認します。
正しくない場合は、保守員に FC パスの再設定を依頼します。
3. 対象のパスのノード側の FC ポート (HostPort)、ストレージシステム側の FC ポート (ArrayPort) に接続された FC ケーブル、および FC スイッチの状態を確認します。
4. SAN 管理者に対象のパスのホストセキュリティを確認します。
5. SAN 管理者に、対象のパスのストレージシステム側の FC ポート (ArrayPort) に設定された各ホストグループに同じ LU を割り当てるよう依頼します。
LU を割り当てる際に LU パスを移動または削除する必要がある場合には、「ユーザズガイド」を参照してください。
6. 対象の FC パスの状態を確認します。

4.17.6 特定の FC パスで「Partially Online」が表示されている場合

特定の FC パスで「Partially Online」が表示されている場合、一部の FC パスが offline になっているため、LU にアクセスできない状態であると考えられます。次の手順に従って対処してください。

1. fponline コマンドで対象の FC パスをオンラインにします。
2. 対象の FC パスの状態を確認します。

4.17.7 同一ターゲットへの片方のパスで「Configuration Mismatch」が表示されている場合

同一ターゲットへの片方のパスで「Configuration Mismatch」が表示され、もう一方のパスには何も情報が表示されていない場合、交替パスが設定されていないことが考えられます。情報が表示されていない方のパスを「Error」と見なして、「4.17.1 同一ターゲットへの片方のパスで「Error」が表示されている場合」に従って対処してください。

4.17.8 FC パスの情報が表示されない場合

接続している FC パスが表示されないときは、OS の起動時に FC パス障害が発生していたことが考えられます。次の手順に従って対処してください。

1. 対象のパスが使用している FC ケーブルや FC スイッチの接続を確認し、障害を取り除きます。
2. FC パスの状態を再度確認します。

4.18 インターフェースやネットワークのエラー情報を確認して障害を回復する

インターフェースやネットワークに障害が発生した場合、システム管理者は [Network & System Configuration] ダイアログの [List of Interfaces] ページでインターフェースやネットワークのエラー状態を確認し、必要に応じて保守員と連携を取って、障害を回復します。

4.18.1 「Unknown」が表示されている場合

[Network & System Configuration] ダイアログの [List of Interfaces] ページで、クラスタを構成するノードのうち、現在アクセスしていないノードの表示項目に「Unknown」が表示されている場合の対処方法を次に示します。

OS の起動の確認

クラスタを構成するノードのうち、アクセスしていないノードの OS が起動しているか確認してください。

OS が起動していない場合は、ノード本体の電源を入れて、OS を起動してください。

OS を起動したあと、再度 [List of Interfaces] ページでインターフェース情報とネットワーク情報を確認してください。

管理ポートの IP アドレスの確認

管理ポートの固有 IP アドレスおよびネットマスクが正しく設定されているか確認してください。設定されている値に誤りがある場合、正しい値を設定してください。

管理ポートの固有 IP アドレスおよびネットマスクは [Edit Interface] ページで設定します。固有 IP アドレスおよびネットマスクを正しく設定したあと、再度 [List of Interfaces] ページでインターフェース情報とネットワーク情報を確認してください。

LAN ケーブルの確認

LAN ケーブルが正しく接続されているか確認してください。LAN ケーブルを再接続したあと、再度 [List of Interfaces] ページでインターフェース情報とネットワーク情報を確認してください。

ハブなどの通信機器の確認

ハブなどの通信機器に問題がないか確認してください。ハブなどの通信機器の問題があった場合、問題を取り除いたあと、再度 [List of Interfaces] ページでインターフェース情報とネットワーク情報を確認してください。

管理ポートのネゴシエーションモードの確認

管理ポートとスイッチのネゴシエーションモードの設定が同じであるか確認してください。設定が異なっている場合は、同じネゴシエーションモードを設定してください。スイッチの種類によっては、互いにオートネゴシエーションモードを設定している場合でも、通信できなくなることがあります。この場合は、管理ポートとスイッチの設定が同じになるように固定のネゴシエーションモードを設定してください。

ネゴシエーションモードは [Negotiation Mode Setup] ページで変更します。

ネゴシエーションモードを設定したあと、再度 [List of Interfaces] ページでインターフェース情報とネットワーク情報を確認してください。

なお、上記の対策を実施しても [List of Interfaces] ページに「Unknown」が表示される場合は、保守員に連絡してください。

4.18.2 管理ポートに「Invalid」が表示されている場合

[Network & System Configuration] ダイアログの [List of Interfaces] ページで、クラスタを構成するノードのうち、現在アクセスしていないノードの管理ポートの表示項目に「Invalid」が表示されている場合、IP アドレスの設定を確認してください。

固有 IP アドレスおよびネットマスクの表示項目に「Invalid」が表示されている場合、固有 IP アドレスおよびネットマスクの設定に誤りがないか確認してください。設定されている値に誤りがある場合、正しい値を設定してください。管理ポートの IP アドレスは [Edit Interface] ページで設定します。

上記の回復作業を実施しても、[List of Interfaces] ページに「Invalid」が表示される場合は、保守員に連絡してください。

4.18.3 データポートに「Invalid」が表示されている場合

[Network & System Configuration] ダイアログの [List of Interfaces] ページで、クラスタを構成するノードのうち、現在アクセスしていないノードのデータポートの表示項目に「Invalid」が表示されている場合、「Invalid」が表示されているすべてのインターフェースを削除し、正しい値を設定してインターフェースを再度追加してください。

上記の回復作業を実施しても、[List of Interfaces] ページに「Invalid」が表示される場合は、保守員に連絡してください。

4.19 リンク結合のエラー情報を確認して障害を回復する

リンク結合の設定に障害が発生した場合、システム管理者は [Network & System Configuration] ダイアログの [List of Trunking Configurations] ページでリンク結合のエラー状態を確認し、障害を回復します。

4.19.1 [Link status] に「Down」が表示されている場合

[Network & System Configuration] ダイアログの [List of Trunking Configurations] ページで、[Link status] に「Down」が表示されている場合、リンクが断絶しているおそれがあります。リンクが断絶している場合の対処方法を次に示します。

使用しているポートにケーブルが接続されているかどうかの確認

使用しているポートにケーブルが接続されているかどうか確認してください。ポートにケーブルが接続されていない場合、ケーブルを正しく接続してください。

ケーブルに障害が発生しているかどうかの確認

ケーブルを正しく接続してもリンクが断絶したままの場合、ケーブルに障害が発生しているおそれがあります。障害のないケーブルに交換してください。

スイッチに障害が発生しているかどうかの確認

ケーブルに障害が発生していない場合、スイッチに障害が発生しているおそれがあります。スイッチの障害を取り除いてください。

ケーブルおよびスイッチに障害が発生していない場合、HVFP のハードウェアに障害が発生しているおそれがあります。保守員に連絡して、障害を回復してください。

4.19.2 [LACP] の [Aggregate] に「Not aggregated」が表示されている場合

[Network & System Configuration] ダイアログの [List of Trunking Configurations] ページで、[LACP] の [Aggregate] に「Not aggregated」が表示されている場合、10 秒以上待ってから [Refresh] をクリックして、ダイアログに表示されている内容を最新情報に更新してください。数回 [Refresh] をクリックしても「Not aggregated」が表示されている場合、ポートがリンク集約に参加できていないおそれがあります。

ポートがリンク集約に参加できていない場合の対処方法を次に示します。

[Link status] に「Up」が表示されている場合

- スイッチが IEEE802.3ad (Dynamic LACP) に対応しているか確認してください。
- ケーブルを接続する個所に誤りがあるおそれがあります。ノードとスイッチの間を接続するケーブルの接続個所を確認してください。接続個所に誤りがある場合、正しく接続してください。
- スイッチの設定に誤りがあるおそれがあります。スイッチ側のリンク集約の設定が、File Services Manager での設定と同じになっているかどうか確認してください。スイッチのリンク集約の設定が File Services Manager での設定と異なっていた場合、スイッチを正しく設定してください。
- スイッチの種類によっては、リンク集約できるポートの組み合わせに制限がある場合があります。スイッチの仕様を確認してください。
- スイッチの種類によっては、互いにオートネゴシエーションモードを設定した場合でも、通信速度が期待値よりも遅くなり、リンク集約に参加できないことがあります。この場合は、互いの設定が同じになるように固定のネゴシエーションモードを設定してください。

[Link status] に「Down」が表示されている場合

リンクが断絶しているおそれがあります。「4.19.1 [Link status] に「Down」が表示されている場合」を参照して対処してください。

4.19.3 通常稼働させるポートの [Active port] の [Status] に「Standby」が表示されている場合

リンク交代を設定している場合、通常稼働させるポート ([Network & System Configuration] ダイアログの [Link Alternation Setup] ページの [Default active port] で選択したポート) の [Active port] の [Status] に「Standby」が表示されているときは、通常稼働させるポートに障害が発生しているおそれがあります。通常稼働させるポートに障害が発生している場合の対処方法を次に示します。

[Link status] に「Up」が表示されている場合

[List of Trunking Configurations] ページでリンク交代ポート (rdn <番号>) を選択し、[Change Active Port Status] ボタンをクリックしてください。[Active port] の [Status] に「Active」が表示され、正常に稼働が開始されます。[Active port] の [Status] が「Active」に変更されない場合、保守員に連絡して、障害を回復してください。

[Link status] に「Down」が表示されている場合

リンクが断絶しているおそれがあります。「4.19.1 [Link status] に「Down」が表示されている場合」を参照して対処してください。

4.20 データポートのエラー情報を確認して障害を回復する

データポートに障害が発生した場合、システム管理者は [Network & System Configuration] ダイアログの [List of Data Ports] ページでデータポートの通信状態を確認し、障害を回復します。

4.20.1 [Link status] に「Down」が表示されている場合

[Network & System Configuration] ダイアログの [List of Data Ports] ページで、[Link status] に「Down」が表示されている場合、リンクが断絶しているおそれがあります。リンクが断絶している場合の対処方法を次に示します。

使用しているポートにケーブルが接続されているかどうかの確認

ポートにケーブルが接続されていない場合、ケーブルを正しく接続してください。

ケーブルに障害が発生しているかどうかの確認

ケーブルを正しく接続してもリンクが断絶したままの場合、ケーブルに障害が発生しているおそれがあります。障害のないケーブルに交換してください。

スイッチの設定に誤りがないかどうかの確認

スイッチ側のネゴシエーションモードの設定が、File Services Manager のネゴシエーションモードの設定と同じになっているかどうか確認してください。

スイッチに障害が発生しているかどうかの確認

ケーブルに障害が発生していない場合、スイッチに障害が発生しているおそれがあります。スイッチの障害を取り除いてください。

ケーブルおよびスイッチに障害が発生していない場合、HVFP のハードウェアに障害が発生しているおそれがあります。保守員に連絡して、障害を回復してください。ポート障害を回復する際に、保守員から指示を受けてフェールオーバーするときは、フロントエンド LAN に設置した管理コンソールから HVFP を管理する運用でも、管理 LAN から操作する必要があります。

4.20.2 [Connected status] の [Speed] に誤った通信速度が表示されている場合

[Network & System Configuration] ダイアログの [List of Data Ports] ページで、[Connected status] の [Speed] に「10Base」が表示されたり、最適な通信速度は 1,000Mbps であるのに「100Base」が表示されたりするなど、スイッチとの通信速度として誤った値（最適でない値）が表示されている場合はスイッチの設定に誤りがあるおそれがあります。スイッチ側のネゴシエーションモードの設定が、File Services Manager での設定と同じになっているかどうか確認してください。スイッチ側のネゴシエーションモードの設定が File Services Manager での設定と異なっていた場合、スイッチを正しく設定してください。

また、スイッチの種類によっては、互いにオートネゴシエーションモードを設定した場合でも通信速度が期待値より遅くなる場合があります。この場合は、互いの設定が同じになるように固定のネゴシエーションモードを設定してください。

4.21 ハードウェアの障害を回復する

システム管理者は、ハードウェアの状態が正常でないことを確認した場合、正常な状態に回復します。GUI でハードウェアの障害を確認した場合、FC パスまたは Ethernet インターフェースの障害については「4.17 FC パスの障害を回復する」または「4.18 インターフェースやネットワークのエ

ラー情報を確認して障害を回復する」に従って対処してください。それ以外の障害については `hwstatus` コマンドを実行してください。 `hwstatus` コマンドで `BMC Information` の `connection` に `failed` が表示された場合は、もう一方のノードの `BMC` のネットワーク状態を確認してください。

上記以外のハードウェアの障害を回復する場合は、保守員に依頼してください。

4.22 OS 起動時に LU が認識できない障害を回復する

OS 起動時に次のどれかの問題があった場合、OS が LU を認識できないため、HVFP を操作できなくなるおそれがあります。

- ストレージシステムへの電源供給が遅れた
- ストレージシステムに電源が供給されていない
- FC ケーブルの接続状態に問題があった

この場合、システムメッセージで `KAQG10104-E` メッセージが通知されます。

対処を次に示します。

1. ノードの電源スイッチを `OFF` にします。
ノードの `Power` ランプスイッチの操作方法については、「システム構成ガイド」を参照してください。
2. ストレージシステムの電源スイッチを確認し、`OFF` になっている場合は `ON` にします。
3. FC ケーブルを確認し、問題がある場合は正しく接続します。
4. ノードの電源スイッチを `ON` にします。
OS が起動されます。

上記の手順を実行しても再度エラーが発生する場合は、保守員に連絡してください。

なお、停電が発生した場合の電源回復時に、OS がストレージシステムより先に起動を完了すると、LU を認識できないことがあります。特別な理由がないかぎり、ノードとストレージシステムには同じ電源を使用してください。

4.23 ほかのファイルサーバからのデータインポートでの障害を回復する

ほかのファイルサーバからのデータインポート中に障害が発生した場合、障害の種類に応じて回復します。

4.23.1 インポート元のファイルサーバとの通信に失敗した場合

インポート元のファイルサーバとの通信に失敗した場合は、次の事項を確認し、問題があった場合は問題を取り除いてください。

HVFP とインポート元のファイルサーバ間のネットワークの状態

`nasping` および `nastraceroute` コマンドを使用して、ネットワークの疎通を確認します。

DNS サーバ、LDAP サーバなどの外部サーバの状態

[`Check for Errors`] ダイアログの [`List of RAS Information`] ページ ([`Server check`] 表示) で、ノードと外部サーバの接続状態を確認します。

インポート元のファイルサーバの稼働状態、ネットワーク設定、共有設定（共有パスの設定）および I/O 状態

`datamigrateaccesstest` コマンドを使用して、設定した内容でインポート元のファイルサーバにアクセスできるか確認します。また、インポート元のファイルサーバのコンソールなどから状態を確認します。

インポートコマンドの実行時に指定したインポート元のファイルサーバのホスト名、IP アドレス、共有名、アカウントおよび共有パス

`datamigrateconflist` コマンドを使用して、設定内容に誤りがないか確認します。また、`datamigrateaccesstest` コマンドを使用して、設定した内容でインポート元のファイルサーバにアクセスできるか確認します。

4.23.2 HVFP で I/O 障害が発生した場合

HVFP で I/O 障害が発生した場合は、出力されたメッセージの内容に応じて対処してください。

表 4-8 ほかのファイルサーバからのデータインポート時に HVFP で I/O 障害が発生した場合のメッセージと対処

メッセージの内容	対処	参照先
ファイルシステムの容量不足	不要なファイルを削除するか、ファイルシステムを拡張して、ファイルシステムに十分な空き容量を確保してください。	—
FC パスの障害	FC パスの障害の回復手順に従って、障害を回復してください。	4.17
LU の障害	ストレージシステムの障害によるファイルシステム閉塞の回復手順に従って、障害を回復してください。	4.8
差分格納デバイスの容量不足	差分格納デバイスの容量が不足した場合の回復手順に従って、障害を回復してください。	4.9
ファイルシステムの閉塞	ファイルシステム閉塞の回復手順に従って、障害を回復してください。	4.8

(凡例) — : 該当しない

4.23.3 一部のファイルのインポートに失敗した場合

データインポートの完了後、`--migfailedlist` オプションを指定して `datamigratestatus` コマンドを実行し、インポート結果を確認します。インポートに失敗したファイルがあった場合は、表示されているエラーメッセージの対処に従って障害を回復してください。障害の回復後、`datamigratestart` コマンドの実行から再度手順を実施してください。なお、ファイルの所有者または ACE に設定されているアカウントが、インポート元のファイルサーバの環境から削除されていたためインポートに失敗した場合は、HVFP でアカウントのマッピングが設定済みかどうかによって対処が異なります。次の「(1) マッピングが設定済みの場合」または「(2) マッピングが未設定の場合」に従って対処してください。

(1) マッピングが設定済みの場合

アカウントのマッピングが設定済みの場合に、アカウントがインポート元のファイルサーバの環境から削除されていたためインポートに失敗したときの対処を次に示します。

1. HVFP で、`--mapdef` オプションを指定して `datamigrateconflist` コマンドを実行し、出力されたマッピング情報をファイルとして保存します。
2. インポート元ファイルサーバ上の対象ファイルのプロパティから、削除されたアカウントの SID を確認します。

SID は、グループ名またはユーザー名の欄に、「S」で始まる半角英数字およびハイフンから成る文字列として表示されます。表示されているすべての SID を記録してください。

- 手順 1 で作成したマッピングファイルの末尾に、手順 2 で取得した SID に対応するマッピングエントリーを追加します。

各項目には次のとおり値を指定してください (SRC_NAME には値を指定しない)。

```
[MAPDEF]
SID=<取得した SID の値>
SRC_NAME=
KIND=< u (ユーザー) または g (グループ) >
DST_NAME=<インポート先アカウント名>
指定例を次に示します。
```

```
[MAPDEF]
SID=S-1-5-21-2348534987-2915341303-3818173629-10003
SRC_NAME=
KIND=u
DST_NAME=usr10003
```

なお、文字コードは UTF-8 にしてください。

- 手順 3 で DST_NAME に指定したアカウントが未登録の場合、HVFP または外部サーバにアカウントを登録します。
- マッピングファイルを HVFP に転送します。
SSH アカウントのホームディレクトリ (/home/nasroot) 以下に転送してください。
- HVFP で、--mapdef オプションおよびマッピングファイル名を指定して、datamigrateconfedit コマンドを実行し、マッピングを再設定します。
- datamigratestart コマンドの実行から再度インポートの手順を実施します。

上記の手順で解決しない場合は、--migrate-replace-owner オプションを指定して arconconfedit コマンドを実行し、削除されたアカウントに割り当てるアカウント名を設定したあと、datamigratestart コマンドの実行から再度インポートの手順を実施してください。インポートの完了後、--migrate-replace-owner オプションに空文字 ("") や "" など) を指定して arconconfedit コマンドを実行し、アカウント割り当ての設定を削除してください。

(2) マッピングが未設定の場合

アカウントのマッピングが未設定の場合に、アカウントがインポート元のファイルサーバの環境から削除されていたためインポートに失敗したときの対処を次に示します。

- インポート元ファイルサーバ上の対象ファイルのプロパティから、削除されたアカウントの SID を確認します。

SID は、グループ名またはユーザー名の欄に、「S」で始まる半角英数字およびハイフンから成る文字列として表示されます。表示されているすべての SID を記録してください。

- 新規にファイルを作成し、手順 1. で取得した SID に対応するマッピングエントリーを追加します。

各項目には次のとおり値を指定してください (SRC_NAME には値を指定しない)。

```
[MAPDEF]
SID=<取得した SID の値>
SRC_NAME=
KIND=< u (ユーザー) または g (グループ) >
DST_NAME=<インポート先アカウント名>
指定例を次に示します。
```

```
[MAPDEF]
SID=S-1-5-21-2348534987-2915341303-3818173629-10003
SRC_NAME=
KIND=u
DST_NAME=usr10003
```

なお、文字コードは UTF-8 にしてください。

- 手順 2. で DST_NAME に指定したアカウントが未登録の場合、HVFP または外部サーバにアカウントを登録します。
- 作成したマッピングファイルを HVFP に転送します。
SSH アカウントのホームディレクトリ (/home/nasroot) 以下に転送してください。
- HVFP で、--mapdef オプションおよびマッピングファイル名を指定して、
datamigrateconfedit コマンドを実行し、マッピングを再設定します。
- datamigratestart コマンドの実行から再度インポートの手順を実施します。

上記の手順で解決しない場合は、--migrate-replace-owner オプションを指定して arconconfedit コマンドを実行し、削除されたアカウントに割り当てるアカウント名を設定したあと、datamigratestart コマンドの実行から再度インポートの手順を実施してください。インポートの完了後、--migrate-replace-owner オプションに空文字 ("") や "" など) を指定して arconconfedit コマンドを実行し、アカウント割り当ての設定を削除してください。

4.23.4 インポートが完了する前にインポートの設定を解除した場合

すべてのファイルのインポートが完了する前に、datamigrateconfdel コマンドを使用してインポートの設定を解除した場合、インポートされていないファイルにクライアントがアクセスするとエラーになります。ファイルが必要な場合は、datamigrateconfadd コマンドの実行から再度手順を実施してください。ファイルが不要な場合は、datamigrateconfdel コマンドを実行し、--type on-demand オプションを指定して datamigratestart コマンドを実行したあと、ファイルを削除してください。

4.23.5 アカウントの名前解決が失敗した場合

アカウントの名前解決が失敗した場合、[Check for Errors] ダイアログの [List of RAS Information] ページ ([Server check] 表示) で、DNS サーバ、LDAP サーバなどの外部サーバに接続できることを確認してください。また、外部サーバにアカウントが登録されていることを確認してください。外部サーバに接続でき、アカウントが登録されている場合は、datamigrateconflist コマンドで、マッピングの内容が正しいことを確認してください。マッピングを設定していない場合は、datamigrateconfedit コマンドでマッピングを設定してください。設定後、インポートの手順を続行してください。

4.23.6 アカウント名にマルチバイト文字が含まれる場合

インポート元のアカウントの名称にマルチバイト文字が含まれる場合、マッピング生成ツール (sidlist.exe) で出力された情報のうち、対象アカウントのインポート先アカウント名 (DST_NAME) を、マルチバイト文字を含まない名称に変更してください。そのあと、HVFP または外部サーバにアカウントを登録し、datamigrateconfedit コマンドでマッピングを再設定してください。再設定後、インポートの手順を続行してください。

4.24 Backup Restore の機能に関する障害を回復する

Backup Restore の機能を使用中に障害が発生した場合のシステム管理者の対応について説明します。障害の要因を特定できなかつたり、対処できなかつたりした場合は、保守員に必ず連絡してください。

エラーメッセージで障害の要因を特定できた場合、対処方法を確認して、障害の要因を取り除いてください。

4.24.1 オンラインバックアップがエラー終了した場合

オンラインバックアップがエラー終了したり、システム管理者が処理を中断したりした場合は、オンラインバックアップ用に作成された差分スナップショットが自動的に削除されないことがあります。GUI または `synclist` コマンドで、作成されている差分スナップショットを確認します。不要な差分スナップショットが残っている場合は、`syncumount` コマンドでアンマウントおよび `syncdel` コマンドで削除してください。

4.24.2 バックアップサーバまたはメディアサーバと NDMP サーバ間の接続に問題があった場合

バックアップサーバまたはメディアサーバと NDMP サーバ間の接続に問題があった場合は、次の方法で接続不良や設定ミスがないかを確認し、必要な処置をしてください。

- ネットワークやルーティングの状態を `nasping` コマンドなどで確認する。
- [Network & System Configuration] ダイアログの [List of Interfaces] ページおよび [List of Routings] ページで、インターフェース情報およびルーティング情報を確認する。
- バックアップサーバに登録されたユーザー名とパスワードが、NDMP サーバおよびメディアサーバに登録されたユーザー名とパスワードと一致しているかどうかをバックアップ管理ソフトウェアで確認する。

各バックアップ管理ソフトウェアでの確認方法については、HVFP に添付されている Backup Restore の補足資料を参照してください。

- [Network & System Configuration] ダイアログの [Edit System File] ページで、`/etc/hosts` ファイルの内容を見直し、登録されているバックアップサーバの情報を修正する。
- [Check for Errors] ダイアログの [List of RAS Information] ページ ([List of other log files] 表示) で、NDMP サーバログ (`/enas/log/ndmpserver.log`) を確認し、出力されたメッセージに従って対処する。

4.24.3 ジョブの実行状態やテープ装置の状態に問題があった場合

ノードに SAN で接続されたテープ装置を使用してバックアップまたはリストアを実行している場合に、フェールオーバーが発生したり、テープ装置との接続やテープ装置に障害が発生したりすると、バックアップまたはリストアのジョブが実行中のままになったり、テープ装置のドライブ内にバックアップメディアが入ったままになったりすることがあります。

この場合は、次の手順でジョブやテープ装置の障害を回復してから運用を再開してください。

1. 実行中のままとなっているジョブや、実行待ちのジョブがないかを確認します。
実行中のままとなっているジョブがある場合は、そのジョブをキャンセルしてください。実行待ちのジョブがある場合には、そのジョブもキャンセルするなどの対応を行い、バックアップまたはリストアが実行されないようにしてください。
2. テープドライブにバックアップメディアが入ったままになっていないか確認します。
テープドライブにバックアップメディアが入ったままになっている場合は、手順 3 および手順 4 を実行してください。
3. テープドライブからバックアップメディアを排出します。
バックアップメディアが入ったままとなっているドライブに対して、ドライブのリセットを実行してください。
4. テープドライブからバックアップメディアが排出されたことを確認します。
バックアップメディアがテープドライブから排出されていない場合は、テープ装置を手動で操作して、バックアップメディアを排出してください。テープ装置の操作方法は、ベンダーのドキュメントを参照してください。

5. テープ装置が正常に稼働していることを確認します。
テープ装置に障害が発生している場合は、ベンダーのドキュメントを参照して、必要な対処をしてください。

これらの操作を実行しても問題が解決しない場合は、保守員に連絡してください。

4.24.4 テープドライブとノードの接続が閉塞状態になっている場合

テープドライブとノードの接続が閉塞状態になっている場合は、次の手順で閉塞状態を解消します。

1. NDMP サーバを停止します。
2. テープ装置に接続されている FC ケーブルを外します。
テープドライブとノードの接続に使用されている FC ケーブルを外してください。
3. テープドライブが接続されていたノードの OS の認識が解除されるのを待ちます。
認識が解除されるまで 30 秒掛かります。
4. テープドライブに障害が発生していないかどうかを確認します。
障害が発生している場合は、ベンダーのドキュメントを参照して、障害を取り除いてください。
5. `-A`, `-d` および `-t WWN:LUN` オプションを指定して `tapelist` コマンドを実行します。
`WWN:LUN` に指定したテープドライブの Status が `N,A` であることを確認します。Status に `N,A` が表示されていない場合は、テープドライブが接続されていたノードの OS を再起動してから、テープドライブの登録情報を有効にしてください。
6. 手順 2 で外した FC ケーブルをテープ装置に接続し直します。
7. NDMP サーバを起動します。

4.24.5 Backup Restore の処理でタイムアウトが頻発する場合

同時刻に、ほかの操作が実行されているおそれがあります。同時刻に複数の操作やスケジュールが実行されていないか確認してください。

`horcfreeze` コマンドを実行して、ファイルシステムに対するアクセスを抑止している場合にも、タイムアウトが発生するおそれがあります。ファイルシステムに対するアクセスの抑止状況は、`fsctl` コマンドで確認できます。

運用を見直しても改善しない場合は、タイムアウトが発生した時点の障害情報を取得して、保守員に連絡してください。

4.24.6 縮退運用中にバックアップまたはリストアを実行する場合

ここでは、縮退運用中にノードに 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を実行する方法を説明します。

(1) 縮退運用中に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

縮退運用中にバックアップまたはリストアを実行する場合は、次の点に注意してください。

- バックアップまたはリストアの処理中にフェールオーバーが発生すると、ジョブが実行中のままになる、バックアップメディアが排出されないなどの問題が発生することがあります。この場合は、「4.24.3 ジョブの実行状態やテープ装置の状態に問題があった場合」に従って対処してから運用を再開してください。
- 縮退運用中にバックアップまたはリストアを実行すると、エラー終了することがあります。「4.5 クラスタおよびノードのエラー情報を確認して障害を回復する」または「4.6 リソースグループ

または **Virtual Server** のエラー情報を確認して障害を回復する」に従って障害を回復してから、バックアップまたはリストアの運用を再開してください。また、必要に応じて、縮退運用中にバックアップが開始されないよう、定期バックアップを一時的に停止してください。

(2) 両ノードで同じテープドライブを共有している場合

両ノードで同じテープドライブを共有している場合の手順を次に示します。

1. バックアップ管理ソフトウェアで、対象のテープドライブが使用できる状態になっていることを確認します。
2. バックアップまたはリストアを実行します。

なお、フェールバックしたあとには、対象のテープドライブが使用できる状態になっていることをバックアップ管理ソフトウェアで確認してください。

(3) それぞれのノードで異なるテープドライブを使用している場合

それぞれのノードで異なるテープドライブを使用している場合の手順を次に示します。

1. `ndmpcontrol` コマンドでフェールオーバー先の NDMP サーバを停止します。
2. フェールオーバー元のノードで使用していたテープドライブをフェールオーバー先の NDMP サーバに登録します。
`tapeadd` コマンドに `-t` オプション、WWN および LUN を指定して、テープドライブを個別に NDMP サーバに登録してください。
3. `ndmpcontrol` コマンドでフェールオーバー先の NDMP サーバを起動します。
4. バックアップ管理ソフトウェアで、対象のテープドライブが使用できる状態になっていることを確認します。
5. バックアップまたはリストアを実行します。

なお、フェールバックしたあとには、バックアップまたはリストア時に登録したテープドライブの情報を次の手順で解除し、対象のテープドライブが使用できる状態になっていることをバックアップ管理ソフトウェアで確認してください。

1. `ndmpcontrol` コマンドで NDMP サーバを停止します。
2. `tapedel` コマンドでバックアップまたはリストア時に登録したテープドライブの登録情報を解除します。
3. `ndmpcontrol` コマンドで NDMP サーバを起動します。
4. バックアップ管理ソフトウェアで、対象のテープドライブが使用できる状態になっていることを確認します。

(4) Virtual Server でテープドライブを使用している場合

Virtual Server でテープドライブを使用している場合の手順を次に示します。

1. `ndmpcontrol` コマンドで稼働ノードが変更になった Virtual Server の NDMP サーバを停止します。
2. `tapeadd` コマンドでテープドライブの登録情報を有効にします。
稼働ノードが変更になった場合、テープドライブの登録情報が無効になるため、無効になったテープドライブを個別に指定してテープドライブの情報を有効にします。
3. `ndmpcontrol` コマンドで Virtual Server 上の NDMP サーバを起動します。
4. バックアップ管理ソフトウェアで、対象のテープドライブが使用できる状態になっていることを確認します。

5. バックアップまたはリストアを実行します。

4.25 Hitachi File Remote Replicator の機能に関する障害を回復する

エラーメッセージで障害の要因を特定できた場合、両サイトのシステム管理者で連携して対処してください。

4.25.1 ネットワークに障害が発生した場合

ネットワークの障害が発生した場合は、次のとおり対処してください。

1. HFRR サービスが正常に稼働していることを確認します。
2. HVFP のノードの状態を確認します。

HVFP のノードの状態を確認し、次の障害が発生していた場合には、参照先の手順に従って対処してください。

HVFP のノードのインターフェースまたはルーティングで障害が発生している場合

「4.18 インターフェースやネットワークのエラー情報を確認して障害を回復する」を参照してください。

リンク結合でエラーが発生している場合

「4.19 リンク結合のエラー情報を確認して障害を回復する」を参照してください。

データポートで障害が発生している場合

「4.20 データポートのエラー情報を確認して障害を回復する」を参照してください。

3. ネットワークの状態を確認します。
ネットワークケーブルやファイアウォール、中継装置などに問題がないか確認します。
russvrchk コマンドや nasping コマンド、nastraceroute コマンドなどを使って、サイト間やネットワーク内の通信状態を確認して、対処してください。
4. HFRR サービスのポート番号と HFRR ペアの定義内容を確認します。
rusportset コマンドと ruspairlist コマンドを使用して、HFRR サービスのポート番号と HFRR ペア定義の HFRR ポート番号が一致していることを確認します。ポート番号が不一致だった場合は、HFRR ペアの定義を見直すなどの対処をしてください。
5. サイトのホスト名と HFRR ペアの定義内容を確認します。
サイトのホスト名と HFRR ペア定義のホスト名が一致していることを確認します。DNS を利用して名前解決をしている場合は、DNS サーバが正常に稼働していることを確認します。ホスト名が不一致だった場合は、HFRR ペアの定義を見直すなどの対処をしてください。

4.25.2 サイト間で HFRR ペアの状態が一致していない場合

HVFP の負荷が高い状態で操作を実行した場合には、状態が更新されるまでに時間が掛かることがあります。また、Hitachi File Remote Replicator がペア状態を更新するときにネットワークに問題が発生した場合、またはコマンド実行中にフェールオーバーが発生した場合にも、HFRR ペアの状態が一致しないことがあります。

プライマリーサイトとセカンダリーサイトで HFRR ペアの状態が一致していなかった場合には、しばらくしてから再度 ruspairlist コマンドを実行して状態を確認してください。

障害が回復している状態にも関わらず、しばらくしても状態が一致しない場合は、以降の手順に従って、両サイトの HFRR ペアの状態を pair または nobaseline にするか、HFRR ペアを再作成してください。

なお、次に示すうちの複数が該当する場合は、(1)から(6)の順序でどの場合に該当するかを確認し、先に該当する方の対処を実行してください。例えば、(2)と(3)が該当する場合は、(2)に示す対処を実行してください。

(1) 片方のサイトで nobaseline と表示されるとき

片方のサイトだけで HFRR ペアの状態が nobaseline の場合は、相手サイトでの HFRR ペアの状態に関係なく、HFRR ペアを再作成してください。

(2) 片方のサイトで suspend, cancel-error, restoring, restore-error または disable と表示されるとき

片方のサイトだけで HFRR ペアの状態が suspend, cancel-error, restoring, restore-error または disable の場合の対応方法を次に示します。

1. 両サイトで--disable オプションを指定して ruspairdisable コマンドを実行し、HFRR ペアをいったん無効にします。
2. ruspairenable コマンドを実行して、HFRR ペアを再度有効にします。

(3) 片方のサイトで copy, fullcopy または copy-error と表示されるとき

片方のサイトだけで HFRR ペアの状態が copy, fullcopy または copy-error の場合の対応方法を次に示します。

1. HFRR ペアの状態が copy または fullcopy となっている場合は、そのサイトで--copycancel オプションを指定して ruscopycancel コマンドを実行し、コピー処理を中断します。
2. HFRR ペアの状態が copy-error となっている場合は、両サイトで--copycancel オプションを指定して ruscopycancel コマンドを実行し、コピー処理を中断します。
3. ruscopy コマンドを実行して、HFRR ペアをコピーします。
4. しばらく待ってから ruspairlist コマンドを実行して、HFRR ペアの状態が pair になることを確認します。

(4) 片方のサイトで cancel と表示されるとき

片方のサイトだけで HFRR ペアの状態が cancel の場合の対応方法を次に示します。

1. --cancel オプションを指定して ruscopycancel コマンドを実行し、コピーを強制的に取り消します。
2. 両サイトで--disable オプションを指定して ruspairdisable コマンドを実行し、HFRR ペアをいったん無効にします。
3. ruspairenable コマンドを実行して、HFRR ペアを再度有効にします。

(5) 片方のサイトで--と表示されるとき

片方のサイトだけで HFRR ペアの状態が--の場合に、--になっているサイトで差分格納デバイスに障害が発生していないときは、HFRR ペアが不正な状態となっているので、HFRR ペアを再作成してください。

(6) 片方のサイトで HFRR ペアの情報が消失しているとき

Virtual Server の強制削除、HFRR ペアの強制解除などによって、HFRR ペアの情報が片方のサイトにだけ残っている場合は、そのサイトで `ruspairdelete` コマンドに `--delete` オプションを指定して実行し、その HFRR ペアを強制解除してください。

4.25.3 フェールオーバーの発生によって処理が中断された場合

フェールオーバーが発生すると、その Virtual Server またはリソースグループに属する HFRR ペアに対する処理が中断されます。フェールオーバー処理が完了したあと、HFRR ペアの状態を `ruspairlist` コマンドで確認してください。また、必要に応じて、フェールオーバー前に実行した操作を再度実行してください。

4.25.4 リソースグループまたは Virtual Server のリソースが稼働していない状態で HFRR ペアを解除する場合

リソースグループが正しく稼働していない状況または Virtual Server のリソースの起動に失敗した状態で HFRR ペアを解除する必要がある場合は、次の手順に従って対処してください。

1. GUI でリソースグループまたは Virtual Server のリソースが正しく稼働していないことを確認します。`rgstatus` コマンドでリソースグループの状態を確認する、または `vnaslist` コマンドで Virtual Server の状態を確認することもできます。
2. `ruservice` コマンドを実行して、対象の HFRR ペアが属するリソースグループまたは Virtual Server の HFRR サービスを停止します。
3. `ruspairlist` コマンドを実行して、対象の HFRR ペアが存在することを確認します。
4. `--delete` オプションを指定して `ruspairdelete` コマンドを実行して、HFRR ペアを強制解除します。
5. `ruspairlist` コマンドを実行して、対象の HFRR ペアが解除されたことを確認します。
6. `ruservice` コマンドを実行して、手順 2 で停止した HFRR サービスを起動します。

4.25.5 コマンドの処理を途中で終了した場合

コマンドの処理を `[Ctrl] + [C]` によって途中で終了した場合は、次に示す対処をして、`error(interrupt)` 状態を解消してください。

- `ruscopycancel` コマンドに `--cancel` オプションを指定して実行した処理（コピーの取り消し）を途中で終了した場合
 `--cancel` オプションを指定して `ruscopycancel` コマンドを再実行してください。または、`ruspairdelete` コマンドもしくは `ruspairdisable` コマンドを実行してください。
- `ruspairdelete` コマンド（HFRR ペアの解除）、`ruspairdisable` コマンド（HFRR ペアの無効化）または `ruspairenable` コマンド（HFRR ペアの有効化）の処理を途中で終了した場合
 同じコマンドを再実行してください。

4.25.6 HFRR ペアを構成するファイルシステムの容量拡張に関連する障害が発生した場合

ここでは、HFRR ペアを構成するファイルシステムの容量拡張に関連する障害が発生した場合の対処について説明します。

ファイルシステムの容量を拡張したあと、HFRR ペアを有効化する際に KAQR10840-E メッセージが出力された場合は、次の手順に従って対処してください。

1. HFRR ペアを構成する両サイトのファイルシステムの容量を確認します。
セカンダリーファイルシステムの容量がプライマリーファイルシステムの容量以上であることを確認してください。この条件を満たしていない場合は、セカンダリーファイルシステムの容量を拡張する必要があります。
ファイルシステムの容量は、`--status` オプションを指定して `rusfspermit` コマンドを実行することで確認できます。GUI または `fsexpand` コマンドでファイルシステムの容量を拡張できます。
2. 両サイトで `rusvrchk` コマンドを実行して、相手サイトの HFRR サービスと通信できることを確認します。
3. どちらかのサイトで `ruspairenable` コマンドを実行して、HFRR ペアを有効化します。

4.25.7 両サイトの時刻が同期していない場合

WORM 対応ファイルシステムの HFRR ペアでは、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。

両サイトの時刻がずれていたためにコピーできなかった場合は、プライマリーサイトまたはセカンダリーサイトの時刻を設定し直して、コピーを再実行してください。両サイトの時刻は一致させておくことをお勧めします。

GUI または `timeset` コマンドで HVFP のノードの時刻を設定できます。

4.25.8 `ruspairlist` コマンドで **Baseline** と **Copying** に同じ差分スナップショット名が表示される場合

コピー処理中にプライマリーサイトでフェールオーバーが発生したり HFRR サービスが停止したりしたときにセカンダリーサイトで `ruspairlist` コマンドを実行すると、**Baseline** と **Copying** に同じ差分スナップショット名が表示されることがあります。この状態ではコピー処理を続行できません。次のとおり対処してください。

全コピー中にこの状態になった場合

- a. `ruspairdefine` コマンドを実行し、HFRR ペアを再作成します。
- b. `ruscopy` コマンドを再実行して、HFRR ペアをコピーします。

差分コピー中にこの状態になった場合

- a. `--cancel` オプションを指定して `ruscopycancel` コマンドを実行し、コピーを強制的に取り消します。
- b. `ruscopy` コマンドを再実行して、HFRR ペアをコピーします。

4.25.9 セカンダリーサイトで `synclist` コマンドに **copying** と表示される場合

コピー処理中にセカンダリーサイトでフェールオーバーが発生したり HFRR サービスが停止したりしたときにセカンダリーサイトで `-v` オプションを指定して `synclist` コマンドを実行すると、`Differential-data snapshot(s)` に **copying** と表示されることがあります。また、KAQR10820-E メッセージが出力されることがあります。この状態ではコピー処理を続行できません。次のとおり対処してください。

1. セカンダリーサイトで `-f` オプションを指定して `syncdel` コマンドを実行し、`-v` オプションを指定して `synclist` コマンドで `Differential-data snapshot(s)` に `copying` と表示された差分スナップショットを削除します。
2. `ruscopy` コマンドを再実行して、**HFRR** ペアをコピーします。

4.25.10 `ruspairdelete` コマンドまたは `ruspairdisable` コマンドで **KAQR10760-E** メッセージが出力される場合

`ruspairdelete` コマンドまたは `ruspairdisable` コマンドを実行した際に、**KAQR10760-E** メッセージが出力された場合の対処について説明します。

`ruspairdelete` コマンドで **KAQR10760-E** メッセージが出力された場合は、次の手順に従って対処してください。

1. 両サイトで `ruspairlist` コマンドを実行し、対象の **HFRR** ペアの状態が `cancel`、`copy` または `fullcopy` でないことを確認します。
`cancel`、`copy` または `fullcopy` の場合は、処理が完了してから、次の操作を実行してください。
2. 対象の **HFRR** ペアに対して、コマンドが実行されていないことを両サイトで確認します。
3. どちらかのサイトで `ruspairdelete` コマンドを実行し、対象の **HFRR** ペアを解除します。
KAQR10760-E メッセージが出力された場合は、次の手順に進んでください。
4. 両サイトで `ruspairlist` コマンドを実行し、すべての **HFRR** ペアの状態が `cancel`、`copy` または `fullcopy` でないことを確認します。
`cancel`、`copy` または `fullcopy` の場合は、処理が完了してから、次の操作を実行してください。
5. すべての **HFRR** ペアに対して、コマンドが実行されていないことを両サイトで確認します。
6. 両サイトで `restart` を指定して `russervice` コマンドを実行し、**HFRR** サービスを再起動します。
7. 両サイトで `--delete` オプションを指定して `ruspairdelete` コマンドを実行し、対象の **HFRR** ペアを強制解除します。
8. 両サイトで `ruspairlist` コマンドを実行し、対象の **HFRR** ペアが解除されていることを確認します。
また、ほかの **HFRR** ペアの状態が一致していることを確認します。

`ruspairdisable` コマンドで **KAQR10760-E** メッセージが出力された場合は、次の手順に従って対処してください。

1. 両サイトで `ruspairlist` コマンドを実行し、対象の **HFRR** ペアの状態が `cancel`、`copy` または `fullcopy` でないことを確認します。
`cancel`、`copy` または `fullcopy` の場合は、処理が完了してから、次の操作を実行してください。
2. 対象の **HFRR** ペアに対して、コマンドが実行されていないことを両サイトで確認します。
3. どちらかのサイトで `ruspairdisable` コマンドを実行し、対象の **HFRR** ペアを無効にします。
KAQR10760-E メッセージが出力された場合は、次の手順に進んでください。
4. プライマリーサイトで差分スナップショットの自動作成スケジュールを参照して、セカンダリーサイトのベースライン差分スナップショットが削除されない設定であることを確認します。
削除される可能性がある場合は、自動作成スケジュールをいったん無効にします。
5. 両サイトで `ruspairlist` コマンドを実行し、すべての **HFRR** ペアの状態が `cancel`、`copy` または `fullcopy` でないことを確認します。

cancel, copy または fullcopy の場合は、処理が完了してから、次の操作を実行してください。

6. すべての HFRR ペアに対して、コマンドが実行されていないことを両サイトで確認します。
7. 両サイトで restart を指定して russervice コマンドを実行し、HFRR サービスを再起動します。
8. 両サイトで --disable オプションを指定して ruspairdisable コマンドを実行し、対象の HFRR ペアをいったん無効にします。
9. 両サイトで ruspairlist コマンドを実行し、対象の HFRR ペアが無効になっていることを確認します。
また、ほかの HFRR ペアの状態が一致していることを確認します。
10. どちらかのサイトで ruspairenable コマンドを実行し、対象の HFRR ペアを有効にします。
11. どちらかのサイトで ruspairdisable コマンドを実行し、対象の HFRR ペアを無効にします。
12. 両サイトで ruspairlist コマンドを実行し、HFRR ペアが無効になっていることを確認します。
13. 手順 4 で自動作成スケジュールを無効にした場合は、自動作成スケジュールを有効にします。

4.26 ファイルスナップショットの処理で発生したタイムアウトを回復する

ファイルスナップショットの処理でタイムアウトが発生した場合、同時刻にほかの操作が実行されているおそれがあります。同時刻に複数の操作やスケジュールが実行されていないか、運用を見直してください。運用を見直しても改善しない場合は、タイムアウトが発生した時点の障害情報を取得して、保守員に送付してください。

インストール履歴

ここでは、ソフトウェアのインストール履歴のログファイルおよび出力内容について説明します。

- A.1 ソフトウェアのインストール履歴ログファイルの確認

A.1 ソフトウェアのインストール履歴ログファイルの確認

[システムソフトウェア] サブウィンドウには最新のインストール情報だけが表示されます。システム管理者は、[Check for Errors] ダイアログの [List of RAS Information] ページ ([Batch-download] 表示) でダウンロードしたソフトウェア情報ロググループのインストール履歴ファイル (/enas/data/pp/history/product_install.log) を利用して、ソフトウェアのインストール履歴を確認できます。

インストール履歴ファイルには、次の形式でインストール情報が出力されます。

```
I, <操作内容>, <プロダクト名称>, <バージョン>, <操作日時>
```

インストール履歴ファイルに出力される情報を次に示します。

表 A-1 インストール履歴ファイルに出力される情報

項目	内容
操作内容	操作内容が出力されます。 「configure」 新規インストールを実行した場合に出力されます。 「upgrade」 更新インストールを実行した場合に出力されます。
プロダクト名称	プロダクトの名称が表示されます。
バージョン	プロダクトのバージョンが出力されます。システム内部で管理しているシステムの正確なバージョンです。GUIなどで表示されるバージョンと異なることがあります。
操作日時	プロダクトを操作した日時が出力されます。

インストール履歴ファイルの出力例を次に示します。

```
I, configure, Hitachi Virtual File Platform, 03-01-00-00-00-00, 2011/06/24 10:15:23 +0000 (UTC)
```

ネットワーク情報

ここでは、ネットワーク情報のログファイルおよび出力内容について説明します。

- B.1 ネットワーク情報ログファイルの確認
- B.2 enas_routelist.log ファイル
- B.3 log_ifconfig ファイル
- B.4 log_interfaces_check ファイル

B.1 ネットワーク情報ログファイルの確認

システム管理者は、[Check for Errors] ダイアログの [List of RAS Information] ページ ([Batch-download] 表示) でダウンロードしたネットワーク情報ロググループの情報を利用して、ルーティングや外部サーバの設定を確認できます。

ネットワーク情報ロググループには次のログファイルが含まれています。

- enas_routelist.log
- log_ifconfig
- log_interfaces_check

VLAN インターフェースの場合は、ポート名は次の形式で出力されます。

<ポート名>.<VLAN ID> (例: eth12.0010)

また、ログファイルには、ノード間の内部通信に使用するインターフェースの情報も出力されます。

log_interfaces_check ファイルは、[List of RAS Information] ページ ([Server check] 表示) の [Results] で参照できます。

B.2 enas_routelist.log ファイル

enas_routelist.log ファイルの出力例を次に示します。

node 0 (D6P67NBX) 2010/01/20 20:57:59					
Target	Netmask	Gateway	Flags	MSS	Iface
10.208.15.1	255.255.255.255	0.0.0.0	UH	-	eth14
172.19.200.0	255.255.255.0	172.19.10.1	UG	400	eth12.1000
172.16.2.0	255.255.255.0	0.0.0.0	U	-	eth14
172.19.10.0	255.255.255.0	0.0.0.0	U	-	eth12.1000
10.0.0.0	255.255.255.0	0.0.0.0	U	-	hb0
192.168.0.0	255.255.255.0	0.0.0.0	U	-	pm0
10.213.88.0	255.255.252.0	0.0.0.0	U	-	mng0
default	0.0.0.0	10.213.88.10	UG	-	mng0

enas_routelist.log ファイルに出力される情報を次に示します。

表 B-1 enas_routelist.log ファイルに出力される情報

出力行	出力内容
1 行目	タイトルが次の形式で出力されます。ログファイルを取得する際に操作した環境によって、出力される情報が異なります。 Physical Node 上で操作した場合 <ノード番号> (<ホスト名>) <出力日時> Virtual Server 上で操作した場合 <Virtual Server 名> <出力日時> なお、出力日時は「YYYY/MM/DD hh:mm:ss」の形式で、2004/11/22 13:14:15 のように出力されます。
2 行目	3 行目以降に出力される内容の項目名です。
3 行目以降	3 行目以降には、それぞれの項目の内容が出力されます。 Target 出力対象のネットワークアドレスが出力されます。デフォルトルートの場合は、default と出力されます。 Netmask 出力対象のネットワークのネットマスクが出力されます。ホストの場合は「255.255.255.255」と出力されます。デフォルトルートの場合、「0.0.0.0」と出力されます。 Gateway

出力行	出力内容
	<p>ゲートウェイの IP アドレスが出力されます。</p> <p>Flags</p> <p>出力対象のネットワークの状態が出力されます。出力されるのは次に示す状態です。</p> <p>U 通常の経路設定であることを示します。</p> <p>H ルーティングの宛先の設定方法がホストであることを示します。</p> <p>G ゲートウェイが設定されていることを示します。</p> <p>R 回復される動的な経路の設定であることを示します。</p> <p>D デーモンまたは置き換えによる動的な設定であることを示します。</p> <p>M 経路制御デーモンまたは置き換えによる動的な設定であることを示します。</p> <p>A addrconf によって設定されていることを示します。</p> <p>C キャッシュのエントリに設定されていることを示します。</p> <p>! 拒否する経路設定であることを示します。</p> <p>MSS この経路での TCP 接続でのデフォルトの最大セグメントが出力されます。ルーティングを追加したときに、この項目が設定されていない場合、「-」が出力されます。</p> <p>Iface ポート名が出力されます。</p>

B.3 log_ifconfig ファイル

log_ifconfig ファイルの出力例を次に示します。

hb0	<pre>Link encap:Ethernet HWaddr 00:26:b9:5b:ed:6b inet addr:10.0.0.21 Bcast:10.0.0.255 Mask:255.255.255.0 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1 RX packets:376753 errors:0 dropped:0 overruns:0 frame:0 TX packets:376655 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:1000 RX bytes:31957682 (30.4 MiB) TX bytes:31818224 (30.3 MiB) Interrupt:36 Memory:d4000000-d4012700</pre>
lo	<pre>Link encap:Local Loopback inet addr:127.0.0.1 Mask:255.0.0.0 UP LOOPBACK RUNNING MTU:16436 Metric:1 RX packets:915538 errors:0 dropped:0 overruns:0 frame:0 TX packets:915538 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:0 RX bytes:81211031 (77.4 MiB) TX bytes:81211031 (77.4 MiB)</pre>
mng0	<pre>Link encap:Ethernet HWaddr 00:26:b9:5b:ed:6f inet addr:10.213.89.117 Bcast:10.213.89.255 Mask:255.255.255.0 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1 RX packets:2980044 errors:0 dropped:0 overruns:0 frame:0 TX packets:2443046 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:1000 RX bytes:1304242346 (1.2 GiB) TX bytes:185251556 (176.6 MiB) Interrupt:32 Memory:d8000000-d8012700</pre>
mng0:1	<pre>Link encap:Ethernet HWaddr 00:26:b9:5b:ed:6f inet addr:10.213.89.118 Bcast:10.213.89.255 Mask:255.255.255.0 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1</pre>

```

Interrupt:32 Memory:d8000000-d8012700

pm0      Link encap:Ethernet  HWaddr 00:26:b9:5b:ed:6d
         inet addr:10.197.181.50  Bcast:10.197.181.255  Mask:255.255.255.0
         UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
         RX packets:0 errors:0 dropped:0 overruns:0 frame:0
         TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:1000
         RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
         Interrupt:48 Memory:d6000000-d6012700

```

log_ifconfig ファイルに出力される情報を次に示します。

表 B-2 log_ifconfig ファイルに出力される情報

出力項目	出力内容
hb0	ポート名が出力されます。
lo	ループバックの場合は「lo」と表示されます。
mng <番号>	VLAN インターフェースの場合は、番号の部分に「<番号>.<VLAN ID>」と表示されます。
pm <番号>	
agr <番号>	また、仮想 IP アドレス※に対しては、番号の部分に「<番号>:<エイリアス番号>」と表示されます。<エイリアス番号>には次の値が出力されます。
rdn <番号>	0
eth <番号>	log_ifconfig ファイルを出力したノードのリソースグループに属している仮想 IP アドレスの場合。
xgbe <番号>	1 もう一方のノードから、log_ifconfig ファイルを出力したノードにフェールオーバーしているリソースグループに属している仮想 IP アドレスの場合。
Link encap	リンクメディアの種類が出力されます。
HWaddr	MAC アドレスが出力されます。
inet addr	IPv4 の場合に、IP アドレスが出力されます。
Bcast	IPv4 の場合に、ブロードキャストアドレスが出力されます。
Mask	IPv4 の場合に、サブネットマスクが出力されます。
inet6 addr	IPv6 の場合に、IP アドレスが出力されます。
Scope	IPv6 の場合に、IP アドレスの範囲が出力されます。
UP	インターフェースが起動している場合に「UP」が出力されます。
BROADCAST	ブロードキャストを使用している場合に「BROADCAST」が出力されます。
RUNNING	インターフェースが準備状態の場合に「RUNNING」が出力されます。
MULTICAST	マルチキャストが有効な場合に「MULTICAST」が出力されます。
MTU	MTU のサイズが出力されます。
Metric	メトリック値が出力されます。
RX, TX	インターフェースの統計値が出力されます。
Interrupt	インターフェースが使用する割り込み番号が出力されます。
Base address	ドライバーモジュールがロードされるベースアドレスが出力されます。
Memory	ドライバーモジュールがロードされるメモリアドレスが出力されます。

注※：リソースグループがフェールオーバーしていたり、停止していたりすると、log_ifconfig ファイルに仮想 IP アドレスの情報が出力されないことや、両ノードの情報が出力されることがあります。例えば、Node-01 ノードと Node-02 ノードでクラスターが構成されている場合は、条件によって、出力される情報が次のように異なります。

Node-01 のリソースグループが停止している場合

Node-01 の仮想 IP アドレスの情報は log_ifconfig ファイルに出力されません。

Node-02 のリソースグループが Node-01 にフェールオーバーしている場合

Node-01 の仮想 IP アドレスの情報として Node-01 と Node-02 の情報が log_ifconfig ファイルに出力されます。

B.4 log_interfaces_check ファイル

log_interfaces_check ファイルに出力される情報を次に示します。

表 B-3 log_interfaces_check ファイルに出力される項目

メッセージ	説明	参照先
Checking DNS configuration...	DNS サーバとの接続状態が出力されます。	表 B-4
Checking NIS configuration...	NIS サーバとの接続状態が出力されます。	表 B-5
Checking NTP configuration...	NTP サーバとの接続状態が出力されます。Virtual Server 上で操作している場合は出力されません。	表 B-6
Checking LDAP configuration (for user authentication)...	ユーザー認証用の LDAP サーバとの接続状態が出力されます。	表 B-7
Checking authentication server configuration (for CIFS)...	CIFS クライアントの認証サーバとの接続状態が出力されま	表 B-8
Checking authentication server configuration (for NFS)...	NFS クライアントの認証サーバとの接続状態が出力されま	表 B-9
Checking LDAP configuration (for user mapping)...	ユーザーマッピング用の LDAP サーバとの接続状態が出力され	表 B-10

注：複数の外部サーバとの接続状態を取得できない場合は、「Aborted: More than 1 errors occurred」と出力され、外部サーバとの接続状態が出力されないことがあります。

log_interfaces_check ファイルに出力される情報について表 B-4 DNS サーバとの接続状態として出力される情報～表 B-10 ユーザーマッピング用の LDAP サーバとの接続状態として出力される情報で説明します。

表 B-4 DNS サーバとの接続状態として出力される情報

出力内容	説明	対処
OK	DNS サーバは正しく設定されています。	なし。
unusing DNS	DNS サーバが File Services Manager に設定されていません。	DNS サーバを使用する場合は、[Network & System Configuration] ダイアログの [DNS, NIS, LDAP Setup] ページで DNS サーバの情報を設定してください。
Warning: DNS server does not respond.	File Services Manager で設定した DNS サーバから応答がありません。	次のことを確認してください。 ・ ノードまたは Virtual Server と使用する DNS サーバとの

出力内容	説明	対処
No respond servers: < File Services Manager で設定した DNS サーバの IP アドレス>		経路上の機器が正常に稼働しているか <ul style="list-style-type: none"> File Services Manager に設定した DNS サーバの IP アドレスが正しいか DNS サーバが正常に稼働しているか
Error: cannot access DNS server. <エラー要因>	そのほかのエラーが発生しました。	保守員に連絡してください。

表 B-5 NIS サーバとの接続状態として出力される情報

出力内容	説明	対処
OK	NIS サーバが正しく設定されています。	なし。
unusing NIS	NIS サーバが設定されていません。	NIS サーバを使用する場合は、[Network & System Configuration] ダイアログの [DNS, NIS, LDAP Setup] ページで NIS サーバの情報を設定してください。
Warning: NIS server does not respond. No respond servers: < File Services Manager に設定した NIS サーバの名称または IP アドレス※>	File Services Manager に設定した NIS サーバから応答がありません。	次のことを確認してください。 <ul style="list-style-type: none"> ノードまたは Virtual Server と使用する NIS サーバとの経路上の機器が正常に稼働しているか File Services Manager に設定した NIS サーバの名称または IP アドレスが正しいか NIS サーバが正常に稼働しているか
Warning: The specified NIS server name cannot be resolved. NIS server name: < File Services Manager に設定した NIS サーバの名称>	File Services Manager に設定した NIS サーバを名前解決できませんでした。	NIS サーバの名称を正しく名前解決できるか確認してください。
Warning: The specified NIS domain is invalid. NIS domain name: < File Services Manager に設定した NIS サーバの NIS ドメイン名>	File Services Manager に設定した NIS ドメイン名に誤りがあります。	NIS ドメイン名が正しく設定されているかを [Network & System Configuration] ダイアログの [DNS, NIS, LDAP Setup] ページで確認してください。
Error: cannot access NIS server. <エラー要因>	そのほかのエラーが発生しました。	保守員に連絡してください。

注※：ブロードキャストを使用している場合は、「Broadcast」と出力されます。

表 B-6 NTP サーバとの接続状態として出力される情報

出力内容	説明	対処
OK	NTP サーバは正しく設定されています。	なし。

出力内容	説明	対処
unusing NTP	NTP サーバが設定されていません。	NTP サーバを使用する場合は、 [Network & System Configuration] ダイアログの [Time Setup] ページで NTP サーバを設定してください。
Warning: NTP server does not respond. No respond servers: < File Services Manager に設定した NTP サーバの名称または IP アドレス>	File Services Manager に設定した NTP サーバから応答がありません。	次のことを確認してください。 <ul style="list-style-type: none"> ・ ノードと使用する NTP サーバとの経路上の機器が正常に稼働しているか ・ File Services Manager に設定した NTP サーバの名称または IP アドレスが正しいか ・ NTP サーバが正常に稼働しているか
Warning: The specified NTP server name cannot be resolved. NTP server name: < File Services Manager に設定した NTP サーバの名称>	File Services Manager に設定した NTP サーバを名前解決できませんでした。	NTP サーバの名称を正しく名前解決できるか確認してください。
Error: cannot access NTP server. <エラー要因>	そのほかのエラーが発生しました。	保守員に連絡してください。

表 B-7 ユーザー認証用の LDAP サーバとの接続状態として出力される情報

出力内容	説明	対処
OK	ユーザー認証用の LDAP サーバは正しく設定されています。	なし。
unusing LDAP	ユーザー認証用の LDAP サーバが設定されていません。	ユーザー認証を LDAP サーバで実施する場合は、[Network & System Configuration] ダイアログの [DNS, NIS, LDAP Setup] ページで LDAP サーバの情報を設定してください。
Error: LDAP server(< File Services Manager に設定した LDAP サーバの IP アドレス>:<ポート番号>) has not been connected.	File Services Manager に設定した LDAP サーバから応答がありません。	次のことを確認してください。 <ul style="list-style-type: none"> ・ 使用する LDAP サーバとノードまたは Virtual Server との経路上の機器が正常に稼働しているか ・ File Services Manager に設定した LDAP サーバの名称または IP アドレスが正しいか ・ LDAP サーバが正常に稼働しているか
Warning: LDAP server(< File Services Manager に設定した LDAP サーバの IP アドレス>:<ポート番号>) has been connected, but the time limitation occurred.	File Services Manager に設定した LDAP サーバとノードまたは Virtual Server との間の接続チェック処理でタイムアウトが発生しました。	[Network & System Configuration] ダイアログの [DNS, NIS, LDAP Setup] ページで、LDAP サーバの情報が正しく設定されていることを確認してください。
Warning: LDAP server(< File Services Manager に設定した LDAP サーバの IP アドレス>:	File Services Manager に設定した LDAP サーバから取得するエントリー数が上限に達しています。LDAP サーバから取得できるエン	[Network & System Configuration] ダイアログの [DNS, NIS, LDAP Setup] ページで、LDAP サーバの情報が正しく

出力内容	説明	対処
<ポート番号>) has been connected, but the size limitation occurred.	トリー数が制限されているおそれがあります。	設定されていることを確認してください。また、LDAP サーバから取得できるエントリー数の設定を確認してください。
Warning: The password of LDAP administrator seems to be invalid.	File Services Manager に設定した LDAP サーバの管理者のパスワードが正しくありません。	LDAP サーバの管理者のパスワードが正しく設定されているか確認してください。
Error: /etc/libnss-ldap.conf is not found.	LDAP サーバの構成定義ファイルが存在しません。OS に障害が発生しているおそれがあります。	保守員に連絡してください。

表 B-8 CIFS クライアントの認証サーバとの接続状態として出力される情報

出力内容	説明	対処
OK	CIFS クライアントの認証サーバは正しく設定されています。	なし。
unusing authentication server	File Services Manager で CIFS クライアントを認証しています。NT サーバ認証, NT ドメイン認証および Active Directory 認証は使用していません。	NT サーバ認証, NT ドメイン認証または Active Directory 認証を使用する場合は, [Access Protocol Configuration] ダイアログの [CIFS Service Management] ページ (Setting Type : Basic) で使用するサーバの情報を設定してください。
Error: rpc error. Server: < File Services Manager に設定した認証サーバの名称 >	File Services Manager に設定した CIFS クライアントの認証サーバから応答がありません。	次のことを確認してください。 <ul style="list-style-type: none"> ・ ノードまたは Virtual Server と使用する CIFS クライアントの認証サーバとの経路上の機器が正常に稼働しているか ・ File Services Manager に設定した CIFS クライアントの認証サーバの名称または IP アドレスが正しいか ・ CIFS クライアントの認証サーバが正常に稼働しているか
Error: timeout. Server: < File Services Manager に設定した認証サーバの名称 >	File Services Manager に設定した CIFS クライアントの認証サーバの接続チェック処理でタイムアウトが発生しました。	次のことを確認してください。 <ul style="list-style-type: none"> ・ ノードまたは Virtual Server と使用する CIFS クライアントの認証サーバとの経路上の機器が正常に稼働しているか ・ File Services Manager に設定した CIFS クライアントの認証サーバの名称または IP アドレスが正しいか ・ CIFS クライアントの認証サーバが正常に稼働しているか
Error: name resolution failure. Server: < File Services Manager に設定した認証サーバの名称 >	CIFS クライアントの認証サーバを名前解決できませんでした。	CIFS サーバの名称を正しく名前解決できるか確認してください。
Error: <エラー要因>. Server: < File Services Manager に設定した認証サーバの名称 >	そのほかのエラーが発生しました。	保守員に連絡してください。

出力内容	説明	対処
Warning: The SRV DNS records might not be created for a domain controller.	DNS サーバに、Active Directory サービスを展開するための SRV レコードが登録されていないおそれがあります。	DNS サーバに、Active Directory サービスを展開するための SRV レコードが登録されているか確認し、登録されていない場合は登録してください。

表 B-9 NFS クライアントの認証サーバとの接続状態として出力される情報

出力内容	説明	対処
OK	KDC サーバは正しく設定されています。	なし。
unusing KDC server	KDC サーバが設定されていません。	Kerberos 認証を使用する場合は、[Access Protocol Configuration] ダイアログの [NFS Service Management] ページで使用する KDC サーバの情報を設定してください。
Error: KDC error. Server: < File Services Manager に設定した KDC サーバの名称 >	File Services Manager に設定した KDC サーバから応答がありません。	次のことを確認してください。 <ul style="list-style-type: none"> ノードまたは Virtual Server と使用する KDC サーバとの経路上の機器が正常に稼働しているか File Services Manager に設定した KDC サーバの名称または IP アドレスが正しいか KDC サーバが正常に稼働しているか
Error: timeout. Server: < File Services Manager に設定した KDC サーバの名称 >	File Services Manager に設定した KDC サーバの接続チェック処理でタイムアウトが発生しました。	次のことを確認してください。 <ul style="list-style-type: none"> ノードまたは Virtual Server と使用する KDC サーバとの経路上の機器が正常に稼働しているか File Services Manager に設定した KDC サーバの名称または IP アドレスが正しいか KDC サーバが正常に稼働しているか
Error: name resolution failure. Server: < File Services Manager に設定した KDC サーバの名称 >	KDC サーバを名前解決できませんでした。	KDC サーバの名称を正しく名前解決できるか確認してください。
Error: <エラー要因>. Server: < File Services Manager に設定した KDC サーバの名称 >	そのほかのエラーが発生しました。	保守員に連絡してください。

表 B-10 ユーザーマッピング用の LDAP サーバとの接続状態として出力される情報

出力内容	説明	対処
OK	ユーザーマッピング用の LDAP サーバは正しく設定されています。	なし。
unusing LDAP	ユーザーマッピング用の LDAP サーバが設定されていません。	LDAP 方式のユーザーマッピングを使用する場合は、[Access Protocol Configuration] ダイアロ

出力内容	説明	対処
		グの [CIFS Service Management] ページ (Setting Type : User mapping) で LDAP サーバの情報を設定してください。
Error: LDAP search timeout.	File Services Manager に設定した LDAP サーバから応答がありません。	次のことを確認してください。 <ul style="list-style-type: none"> 使用する LDAP サーバとノードまたは Virtual Server との経路上の機器が正常に稼働しているか File Services Manager に設定した LDAP サーバの名称または IP アドレスが正しいか LDAP サーバが正常に稼働しているか
Error: LDAP server is down, LDAP server name is invalid, or LDAP server port number is invalid.	File Services Manager に設定した LDAP サーバの名称またはポート番号が誤っているか、サーバが停止しています。	次のことを確認してください。 <ul style="list-style-type: none"> 使用する LDAP サーバとノードまたは Virtual Server との経路上の機器が正常に稼働しているか File Services Manager に設定した LDAP サーバの名称または IP アドレスが正しいか LDAP サーバが正常に稼働しているか
Error: LDAP suffix is not specified.	LDAP サーバのルート識別名が、File Services Manager に設定されていません。	[Access Protocol Configuration] ダイアログの [CIFS Service Management] ページ (Setting Type : User mapping) で LDAP サーバのルート識別名を設定してください。
Error: LDAP administrator DN is not specified.	LDAP サーバの管理者の識別名が、File Services Manager に設定されていません。	[Access Protocol Configuration] ダイアログの [CIFS Service Management] ページ (Setting Type : User mapping) で LDAP サーバの管理者の識別名を設定してください。
Error: LDAP administrator password is not specified.	LDAP サーバの管理者のパスワードが、File Services Manager に設定されていません。	[Access Protocol Configuration] ダイアログの [CIFS Service Management] ページ (Setting Type : User mapping) で LDAP サーバの管理者のパスワードを設定してください。
Error: LDAP user map DN or LDAP server root DN is invalid.	File Services Manager に設定した次のどちらかの情報に誤りがあります。 <ul style="list-style-type: none"> ユーザーマッピングアカウントを追加する識別名 LDAP サーバのルート識別名 	[Access Protocol Configuration] ダイアログの [CIFS Service Management] ページ (Setting Type : User mapping) で、それぞれの識別名が正しく設定されているかを確認してください。
Error: LDAP administrator password is invalid.	File Services Manager に設定した LDAP サーバの管理者のパスワードに誤りがあります。	LDAP サーバに設定されたパスワードを確認して、[Access Protocol Configuration] ダイアログの [CIFS Service Management] ページ (Setting Type : User mapping) で再設定してください。

出力内容	説明	対処
Error: LDAP server root DN or LDAP administrator DN or LDAP administrator password is invalid.	File Services Manager に設定した LDAP サーバのルート識別名, 管理者の識別名, または管理者のパスワードに誤りがあります。	[Access Protocol Configuration] ダイアログの [CIFS Service Management] ページ (Setting Type : User mapping) で, LDAP サーバのルート識別名, 管理者の識別名, および管理者のパスワードが正しく設定されているかを確認してください。
Error: objectClass=sambaUnixIdProl does not exist.	LDAP サーバの初期設定に失敗しました。ユーザーマッピングで使用するエントリーが更新できません。	次のことを確認し, CIFS サービスを再起動してください。 <ul style="list-style-type: none"> 作成した LDAP サーバのスキーマファイルが正しく読み込まれているか ユーザーマッピングで使用するエントリーに, 書き込み権限が設定されているか [Access Protocol Configuration] ダイアログの [CIFS Service Management] ページ (Setting Type : User mapping) で, LDAP サーバの管理者の識別名に設定されたユーザーに管理者権限があるかどうか
Error: objectClass=sambaUnixIdProl is multiple.	LDAP サーバの初期設定に問題があります。	指定された LDAP サーバに LDAP ユーザーマッピングアカウントで使用したエントリーが複数存在します。それらのエントリーのうち, [Access Protocol Configuration] ダイアログの [CIFS Service Management] ページ (Setting Type : User mapping) で指定した LDAP ユーザーマッピングアカウントのエントリー以外は削除してください。
Error: open CIFS.conf failed.	OS に障害が発生したため, /etc/cifs/CIFS.conf ファイルを開けませんでした。	保守員に連絡してください。
Error: open cifs.conf failed.	OS に障害が発生したため, /etc/cifs/conf/cifs.conf ファイルを開けませんでした。	保守員に連絡してください。
Error: cannot access LDAP server. <エラー要因>	そのほかのエラーが発生しました。	保守員に連絡してください。

ネットワークの通信状況の確認方法

システム管理者は、HVFP とクライアントの間のネットワークで通信できるかどうか確認します。ここでは、File Services Manager のネットワーク設定に問題があるために HVFP とクライアントの間で通信できない場合の対処方法について説明します。

- C.1 ネットワークの通信状況を確認する前に
- C.2 ネットワーク構成ごとの通信の確認
- C.3 通信できない場合の対処
- C.4 ネットワークの通信確認の実行例

C.1 ネットワークの通信状況を確認する前に

ネットワークでハードウェア障害やリンク障害が発生していないこと、および HVFP でフェールオーバーが発生していないことを確認して、File Services Manager のネットワーク設定に問題があることを特定します。次の手順で確認してください。

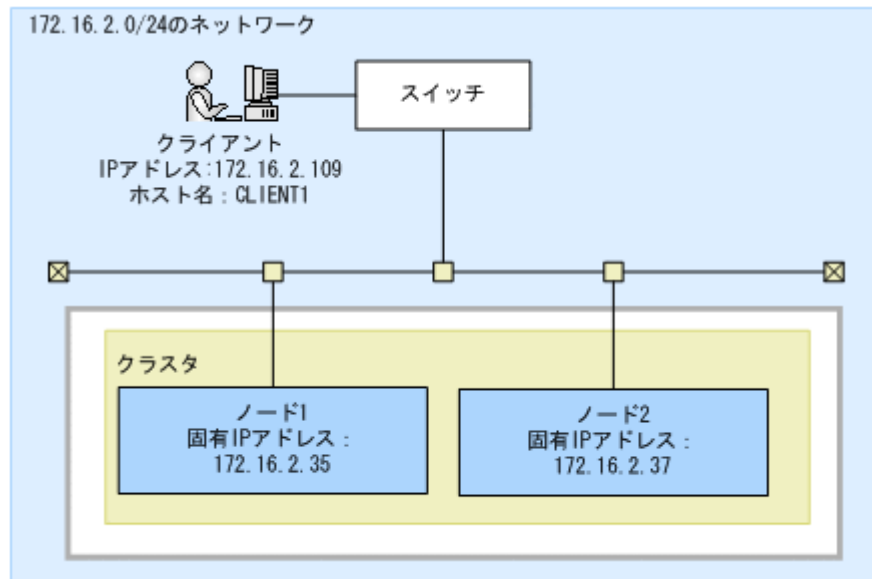
1. HVFP と同じネットワークに属するほかのマシンや、経由するルーターに対してクライアントから ping コマンドを実行します。
クライアントが HVFP 以外のマシンと通信でき、HVFP とだけ通信できないことを確認します。HVFP 以外のマシンと通信できない場合、スイッチ、ルーターなど中継機器の電源が入っているか、ケーブルが抜けていないかなど、中継機器が正常に稼働しているか確認してください。
2. [Check for Errors] ダイアログの [List of RAS Information] ページ ([List of messages] 表示) で、Warning レベルのリンクダウンのメッセージが出力されていないことを確認します。
リンクダウンのメッセージが出力されていた場合、保守員に連絡してください。
3. [List of RAS Information] ページ ([List of messages] 表示) で、KAQG70000-E メッセージが出力されていないこと（フェールオーバーが発生していないこと）を確認します。
フェールオーバーが発生している場合、保守員に連絡してください。

C.2 ネットワーク構成ごとの通信の確認

ネットワークの通信の確認を行う前に、HVFP とクライアントが同一ネットワークに属しているかどうかを確認します。

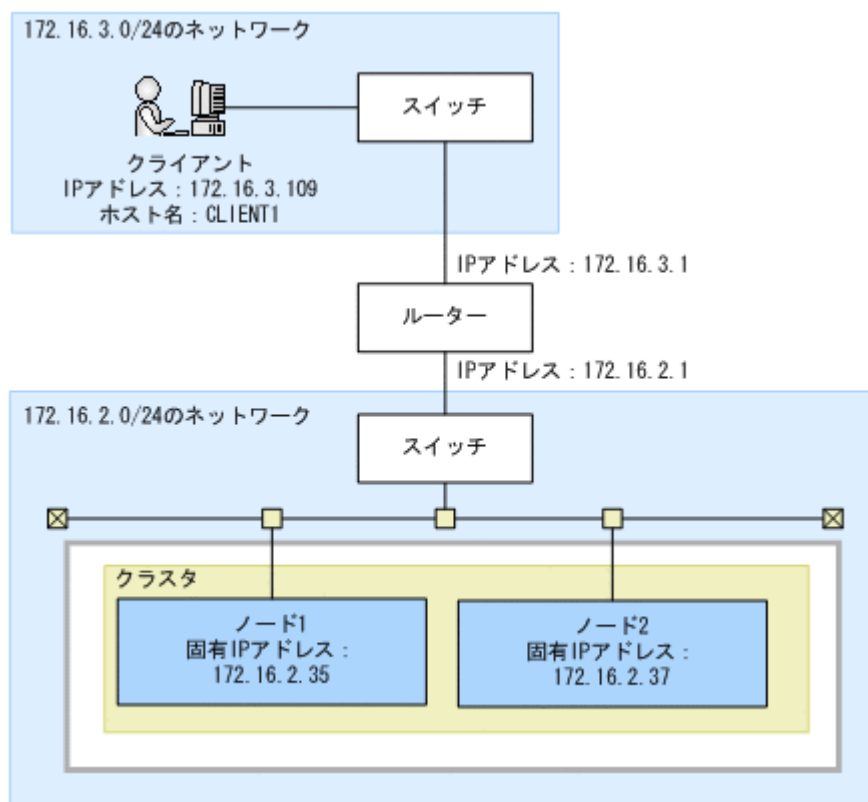
HVFP とクライアントが同一ネットワークに属している場合の例を次の図に示します。

図 C-1 HVFP とクライアントが同一ネットワークに属している場合の構成例



HVFP とクライアントが異なるネットワークに属している場合の例を次の図に示します。

図 C-2 HVFP とクライアントが異なるネットワークに属している場合の構成例



C.2.1 ネットワーク内での通信を確認する

HVFP とクライアントが同一ネットワークに属している場合、次の手順でネットワーク内での通信を確認します。なお、HVFP とクライアントが異なるネットワークに属している場合、ルーターをクライアントと仮定して、次の手順でネットワーク内での通信を確認します。

- 一方のノードから、もう一方のノードの固有 IP アドレスを指定して、`nasping` コマンドを実行します。

通信できない場合、HVFP の IP アドレス、ネットマスクの設定に不正があるか、HVFP またはスイッチの VLAN の設定に不正があります。対処については「[C.3.1 IP アドレス、ネットマスクの確認](#)」および「[C.3.2 VLAN ID の確認](#)」を参照してください。
- 一方のノードから、もう一方のノードに対して、`nasping` コマンドを `-s` オプションを指定して実行します。

通信できない場合、HVFP またはスイッチの MTU 値の設定に不正があります。対処については「[C.3.3 MTU 値の確認](#)」を参照してください。
- クライアントに対して `nasping` コマンドを実行します。

通信できない場合、クライアントの IP アドレス、ネットマスクの設定に不正があるか、スイッチまたはクライアントの VLAN の設定に不正があります。対処については「[C.3.1 IP アドレス、ネットマスクの確認](#)」および「[C.3.2 VLAN ID の確認](#)」を参照してください。
- クライアントに対して、`nasping` コマンドを `-s` オプションを指定して実行します。

通信できない場合、スイッチまたはクライアントの MTU の設定に不正があります。対処については「[C.3.3 MTU 値の確認](#)」を参照してください。

C.2.2 異なるネットワーク間の通信を確認する

HVFP とクライアントが異なるネットワークに属している場合、次の手順で異なるネットワーク間の通信を確認します。

1. クライアント側のネットワークのゲートウェイアドレスを指定して、`nasping` コマンドを実行します。

「Network is unreachable」が出力された場合、HVFP のルーティングの設定に不正があります。また、通信できない場合は、ルーターのルーティングの設定に不正があります。対処については「C.3.4 ルーティングの確認」を参照してください。

2. `nastraceroute` コマンドを `-n` オプション、およびクライアントの IP アドレスを指定して実行します。

通信できない場合、ルーターからクライアントまでのネットワークに異常があります。ルーターからクライアントまでの間を確認してください。

C.3 通信できない場合の対処

ネットワークの疎通を確認した結果、通信できない場合には、設定の内容を確認します。設定に不正があった場合は、正しい設定に変更し、再度動作を確認します。

C.3.1 IP アドレス、ネットマスクの確認

HVFP およびクライアントでネットワークアドレスを確認します。

HVFP

[Network & System Configuration] ダイアログの [List of Interfaces] ページで固有 IP アドレス、仮想 IP アドレス、ネットマスクを確認します。

クライアント

IP アドレスおよびネットマスクの設定を確認します。

HVFP とクライアントのネットワークアドレスが異なる場合は、同じネットワークアドレスになるよう設定を変更してください。

C.3.2 VLAN ID の確認

VLAN を設定している場合は、HVFP、スイッチ、およびクライアントで VLAN の設定を確認します。

HVFP

[Network & System Configuration] ダイアログの [List of Interfaces] ページで VLAN ID を確認します。

スイッチ

HVFP およびクライアントを接続しているポートの VLAN の設定を確認します。複数のスイッチを経由している場合は、スイッチ間を接続しているポートの VLAN の設定を確認します。また、Tagged, Untagged の設定も確認します。

クライアント

Tagged VLAN を設定している場合は、その VLAN ID を確認します。

HVFP, スイッチ, およびクライアントで VLAN ID の設定が異なる場合は, 同じ VLAN ID になるよう設定を変更してください。また, スイッチの Tagged または Untagged の設定に誤りがある場合, 正しく設定してください。

C.3.3 MTU 値の確認

Jumbo Frame を使用する場合など, MTU の設定を変更しているときは, HVFP, スイッチ, およびクライアントの MTU 値の設定を確認します。

HVFP

[Network & System Configuration] ダイアログの [List of Interfaces] ページで MTU 値を確認します。

スイッチ

HVFP およびクライアントを接続しているポートの MTU 値の設定を確認します。複数のスイッチを経由している場合は, スイッチ間を接続しているポートの MTU 値の設定を確認します。

クライアント

MTU 値を確認します。

スイッチの MTU 値が, HVFP およびクライアントに設定されている MTU 値よりも小さい場合, HVFP およびクライアントに設定されている MTU 値よりも大きい値になるよう設定を変更してください。

C.3.4 ルーティングの確認

HVFP, ルーター, スイッチ, およびクライアントに適切なゲートウェイが設定されていることを確認します。

HVFP

[Network & System Configuration] ダイアログの [List of Routings] ページでクライアントに到達できるゲートウェイ (ルーター, スイッチ) が指定されているか確認します。

ルーター, スイッチ

クライアントに到達できるゲートウェイ, および HVFP に到達できるゲートウェイが設定されていることを確認します。

クライアント

HVFP に到達できるゲートウェイが設定されていることを確認します。

HVFP, ルーター, スイッチ, およびクライアントに適切なゲートウェイが設定されていない場合, それぞれのゲートウェイの設定を変更してください。

なお, ルーティング情報を追加する際にホスト名で指定をした場合は, そのホスト名を名前解決ができない状態で次のどれかの操作を実行すると, システム管理者が設定したルーティング情報と, ノードまたは Virtual Server 上で有効になっているルーティング情報とに差異が生じるおそれがあります。

- OS の再起動
- リンク結合の解除
- インターフェースの変更または削除
- ルーティング情報の削除

この場合は, 次の手順に従って対処してください。

ここでは、図 C-2 HVFP とクライアントが異なるネットワークに属している場合の構成例を例に、次のルーティングが設定されていることを想定して説明します。

```
$ sudo routelist
Target      Netmask      Gateway      Method Type  MSS  Iface
CLIENT1    -            172.16.2.1   Allow host  -    eth14
```

有効になっているルーティングの確認

[List of Routings] ページおよび `routelist` コマンドでは、システム管理者が設定したルーティング情報が表示されます。

設定したルーティング情報が有効になっていることを確認するためには、`-l` オプションを指定して `routelist` コマンドで実行する必要があります。

```
$ sudo routelist -l
Target      Netmask      Gateway      Flags  MSS  Iface
172.16.3.109 255.255.255.255 172.16.2.1  UGH   -    eth14
172.16.2.0   255.255.255.0  0.0.0.0    U     -    eth14
10.0.0.0     255.255.255.0  0.0.0.0    U     -    hb0
192.168.0.0  255.255.255.0  0.0.0.0    U     -    pm0
10.213.88.0  255.255.252.0  0.0.0.0    U     -    mng0
```

注：IP アドレス形式で出力されます。また、OS で設定されたルーティングも表示されます。

設定したルーティング情報が有効になっていない場合の対処

ホスト名を使用してルーティング情報を追加したあとに、ホスト名の名前解決ができない状態で OS または Virtual Server を再起動すると、システム管理者が設定したルーティング情報がノード上で有効にならないことがあります。

このような場合の確認・対処手順を次に示します。

- a. システム管理者が設定したルーティング情報と、ノード上で有効になっているルーティング情報を比較します。

```
$ sudo routelist
Target      Netmask      Gateway      Method Type  MSS
Iface
CLIENT1    -            172.16.2.1   Allow host  -
eth14
```

```
$ sudo routelist -l
Target      Netmask      Gateway      Flags  MSS  Iface
172.16.2.0   255.255.255.0  0.0.0.0    U     -    eth14
10.0.0.0     255.255.255.0  0.0.0.0    U     -    hb0
192.168.0.0  255.255.255.0  0.0.0.0    U     -    pm0
10.213.88.0  255.255.252.0  0.0.0.0    U     -    mng0
```

この例では、`routelist` コマンドの結果が、`-l` オプションを指定して実行した `routelist` コマンドの結果に存在しません。

- b. ホスト名 (CLIENT1) を名前解決できる状態にして、ルーティング情報をいったん削除します。

```
$ sudo routedel -d CLIENT1 -g 172.16.2.1 eth14
KAQM05099-Q Do you want to delete the specified routing information? (y/n) y
```

- c. ルーティング情報を再度追加します。

```
$ sudo routeadd -t host -d CLIENT1 -g 172.16.2.1 eth14
```

削除したルーティング情報が有効になっている場合の対処

ホスト名を使用してルーティング情報を追加したあとでそのホスト名に対応する IP アドレスを変更した場合、そのルーティング情報を削除すると、設定ファイルからは削除されますが、ノード上には有効な状態のままルーティング情報が残ってしまうことがあります。

このような場合の確認・対処手順を次に示します。

- a. システム管理者が設定したルーティング情報と、ノード上で有効になっているルーティング情報を比較します。

```
$ sudo routelist
Target          Netmask          Gateway          Method Type     MSS
Iface
```

```
$ sudo routelist -l
Target          Netmask          Gateway          Flags   MSS   Iface
172.16.3.109    255.255.255.255 172.16.2.1      UGH     -     eth14
172.16.2.0      255.255.255.0   0.0.0.0         U       -     eth14
10.0.0.0        255.255.255.0   0.0.0.0         U       -     hb0
192.168.0.0     255.255.255.0   0.0.0.0         U       -     pm0
10.213.88.0     255.255.252.0   0.0.0.0         U       -     mng0
```

この例では、システム管理者が追加したルーティング情報のうち、`routelist` コマンドの結果には存在しないルーティング情報が、`-l` オプションを指定して実行した `routelist` コマンドの結果に存在しています。

- b. ノード上に有効な状態のまま残っているルーティング情報を削除するために、`--nochk` オプションを指定して `routedel` コマンドを実行します。

注意：OS が自動的に設定したルーティング情報は削除しないでください。

```
$ sudo routedel -d 172.16.3.109 -g 172.16.2.1 --nochk eth14
KAQM05099-Q Do you want to delete the specified routing information? (y/n) y
```

疎通対象のホストのネットワークセグメントの送出インターフェースおよびゲートウェイが正しいことを確認します。

ルーティングテーブルを確認し、疎通対象ホストのパケットがどのネットワークインターフェースから送受信されるかを確認します。`routelist -l` コマンドで表示される経路を上から順に調べていき、疎通対象ホストの IP アドレスおよびネットマスクに合致する経路を確認します。経路に設定されているネットワークインターフェースが、宛先ホストと通信できるネットワークインターフェースであることを確認してください。該当経路にゲートウェイが設定されている場合は、そのゲートウェイと通信できることを `nsping` コマンドで確認してください。

なお、疎通対象ホストに合致する経路が複数ある場合は、より上に表示されている経路が送受信に適用されます。HVFP は、送受信に適用されない経路からパケットを受信した場合、パケットを破棄するので注意してください。

`routelist -l` コマンドで同じセグメントの経路が複数表示される場合は、どちらかの経路の設定が誤っているおそれがあります。ルーティング設定を再確認してください。

C.3.5 ネゴシエーションモードの確認

ノードのデータポートとスイッチのネゴシエーションモードの設定が同じであることを確認します。オートネゴシエーションモードが設定されている場合は、通信状態も確認します。

ノードのデータポート

[Network & System Configuration] ダイアログの [List of Data Ports] ページで、ネゴシエーションモードの設定がスイッチ側の設定と同じであるか確認します。オートネゴシエーションモードが設定されている場合は、[Connected status] の [Speed] および [Duplex] に、スイッチとの通信状態として最適な状態が表示されていることを確認します。

スイッチ

ノードのデータポートに接続しているポートのネゴシエーションモードの設定がノード側の設定と同じであるか確認します。

スイッチの種類によっては、互いにオートネゴシエーションモードを設定している場合でも、通信速度が期待値よりも遅くなったり、通信できなくなったりすることがあります。この場合は、ノードとスイッチの設定が同じになるように固定のネゴシエーションモードを設定してください。

C.4 ネットワークの通信確認の実行例

ネットワークの通信を確認するときの例を次に示します。

C.4.1 nasping コマンドを使用した通信の確認の実行例

nasping コマンドを使用して通信を確認する場合の例を次に示します。

成功例

通信が成功した場合の実行例と解説を次に示します。

```
$ sudo nasping -c 3 192.168.0.20
PING 192.168.0.20 (192.168.0.20) 56(84) bytes of data.
64 bytes from 192.168.0.20: icmp_seq=1 ttl=64 time=0.069 ms
64 bytes from 192.168.0.20: icmp_seq=2 ttl=64 time=0.058 ms
64 bytes from 192.168.0.20: icmp_seq=3 ttl=64 time=0.058 ms

--- 192.168.0.20 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
rtt min/avg/max/mdev = 0.058/0.061/0.069/0.010 ms
$ sudo nasping -c 3 -s 9000 192.168.0.20
PING 192.168.0.20 (192.168.0.20) 9000(9028) bytes of data.
9008 bytes from 192.168.0.20: icmp_seq=1 ttl=64 time=5.74 ms
9008 bytes from 192.168.0.20: icmp_seq=2 ttl=64 time=0.981 ms
9008 bytes from 192.168.0.20: icmp_seq=3 ttl=64 time=1.18 ms

--- 192.168.0.20 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2001ms
rtt min/avg/max/mdev = 0.981/2.636/5.742/2.198 ms
$
```

最初の nasping コマンドでは、「192.168.0.20」に 56 バイトの ICMP パケットを 3 回送信して、3 回とも受信しています。つまり、通信が正しく行われていることがわかります。次の nasping コマンドでは、9,000 バイトの ICMP パケットを送信し、パケットの損失は 0% です。こちらも正しく通信できています。

失敗例 1

同じネットワーク内のマシンと通信できない場合の実行例と解説を次に示します。

```
$ sudo nasping -c 3 192.168.0.11
PING 192.168.0.11 (192.168.0.11) 56(84) bytes of data.
From 192.168.0.10 icmp_seq=1 Destination Host Unreachable
From 192.168.0.10 icmp_seq=2 Destination Host Unreachable
From 192.168.0.10 icmp_seq=3 Destination Host Unreachable

--- 192.168.0.11 ping statistics ---
3 packets transmitted, 0 received, +3 errors, 100% packet loss, time
2007ms, pipe 3
$
```

nasping コマンドで「192.168.0.11」に 56 バイトの ICMP パケットを 3 回送信していますが、1 回も受信できていません。このため、指定した IP アドレスを持つマシンと通信できていないことがわかります。HVFP、スイッチおよびクライアントで、IP アドレス、ネットマスクおよび VLAN ID の設定を確認し、必要に応じて変更します。

失敗例 2

スイッチの MTU 値が正しく設定されていない場合の実行例と解説を次に示します。

HVFP のインターフェースでは MTU 値を 9,000 に設定しているが、スイッチでは MTU 値に 9,000 が設定されていない場合の実行例です。

```
$ sudo nasping -c 3 192.168.0.20
PING 192.168.0.20 (192.168.0.20) 56(84) bytes of data.
64 bytes from 192.168.0.20: icmp_seq=1 ttl=64 time=0.074 ms
64 bytes from 192.168.0.20: icmp_seq=2 ttl=64 time=0.060 ms
64 bytes from 192.168.0.20: icmp_seq=3 ttl=64 time=0.070 ms

--- 192.168.0.20 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.060/0.068/0.074/0.005 ms
$ sudo nasping -c 3 -s 9000 192.168.0.20
PING 192.168.0.20 (192.168.0.20) 9000(9028) bytes of data.

--- 192.168.0.20 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2015ms
$
```

最初の nasping コマンドでは「192.168.0.20」に 56 バイトの ICMP パケットを 3 回送信して、3 回とも受信しています。つまり、通信が正しく行われていることがわかります。しかし、次の nasping コマンドでは、9,000 バイトの ICMP パケットを送信していますが、パケットの損失が 100%となっており、通信できていません。HVFP、スイッチ、クライアントの MTU 値の設定を確認し、必要に応じて変更します。

失敗例 3

異なるネットワークのマシンと通信できない場合の実行例と解説を次に示します。別のネットワークのゲートウェイアドレスを指定して、nasping コマンドを実行した場合の実行例です。

```
$ sudo nasping -c 3 192.168.2.2
connect: Network is unreachable
$ sudo nasnetstat -rn
Kernel IP routing table
Destination      Gateway           Genmask           Flags      MSS Window  irtt
Iface
10.0.1.0          0.0.0.0           255.255.255.224  U           0  0        0 hb0
10.208.148.0     0.0.0.0           255.255.255.0   U           0  0        0
eth15-br
10.0.1.0          0.0.0.0           255.255.255.0   U           0  0        0
hb0-br
192.167.0.0      0.0.0.0           255.255.255.0   U           0  0        0
agr0-br
10.197.181.0    0.0.0.0           255.255.255.0   U           0  0        0 pm0
10.213.88.0     0.0.0.0           255.255.252.0   U           0  0        0
mng0-br
$
```

この例では「192.168.2.2」の対象となるゲートウェイが設定されていないこと、およびデフォルトルートも設定されていないことがわかります。指定した IP アドレスに到達するための経路が設定されていないため、「Network is unreachable」が表示されています。HVFP のルーティングの設定を確認して、必要に応じて再設定します。

C.4.2 nastraceroute コマンドを使用した通信の確認の実行例

nastraceroute コマンドを使用して通信を確認する場合の例を次に示します。

成功例

異なるネットワークにあるマシンまでの通信経路が正しく設定されている場合の実行例と解説を次に示します。

```
$ sudo nastraceroute -n 10.213.76.124
traceroute to 10.213.76.124 (10.213.76.124), 30 hops max, 40 byte packets
 1  10.213.88.10  5.580 ms  5.588 ms  5.583 ms
 2  158.214.125.10  7.478 ms  9.683 ms  11.154 ms
```

```
3 10.213.1.3 9.653 ms 9.667 ms 9.982 ms
4 10.213.76.124 9.547 ms 9.560 ms 9.557 ms
$
```

この例では、ルーター「10.213.88.10」、「158.214.125.10」および「10.213.1.3」を経由して、異なるネットワークにあるマシン「10.213.76.124」と通信していることがわかります。

失敗例

ルーターからクライアントまでの経路に異常がある場合の実行例と解説を次に示します。

```
$ sudo nstraceroute -n 10.10.10.10
traceroute to 10.10.10.10 (10.10.10.10), 30 hops max, 40 byte packets
 1 10.213.88.10 5.496 ms 5.490 ms 5.486 ms
 2 158.214.125.10 9.376 ms 9.403 ms 11.644 ms
 3 10.213.1.65 7.238 ms 7.258 ms 7.253 ms
 4 158.214.120.2 7.249 ms 9.324 ms 9.320 ms
 5 133.145.201.2 13.583 ms 15.147 ms 17.309 ms
 6 133.144.227.33 13.551 ms 11.658 ms 10.097 ms
 7 * * *
 8 * * *
...
29 * * *
30 * * *
$
```

nstraceroute コマンドの結果から、「133.144.227.33」のゲートウェイまでは通信できていますが、それ以降は通信できていないことがわかります。ルーターやほかの中継機器、およびクライアントのルーティング設定が正しいかどうかを確認し、必要に応じて設定を変更します。



Hitachi File Remote Replicator のログの出力内容

Hitachi File Remote Replicator ログ (/enas/log/rus.log) および Hitachi File Remote Replicator 統計情報ログ (/enas/log/russtat.log) で、HFRR ペア数やデータ転送バイト量、受信データ量などを確認できます。コマンドの応答速度は正常にも関わらず、処理に時間が掛かる場合には、ログを確認することで、要因を特定できることがあります。

/enas/log/rus.log および /enas/log/russtat.log は、[Check for Errors] ダイアログの [List of RAS Information] ページ ([List of other log files] 表示) からダウンロードできます。

- [D.1 Hitachi File Remote Replicator ログ](#)
- [D.2 Hitachi File Remote Replicator 統計情報ログ](#)

D.1 Hitachi File Remote Replicator ログ

Hitachi File Remote Replicator ログ (/enas/log/rus.log) には、コピー処理の開始・完了の履歴が出力されます。この履歴からコピー処理に掛かった時間やコピープロセス数がわかります。

相手サイトが異なる HFRR ペアのすべてで処理に時間が掛かっている場合は、自サイトの処理速度が遅くなっているおそれがあります。特定の相手サイトと構成している HFRR ペアの処理だけで時間が掛かっている場合は、その相手サイトとの回線に負荷が掛かっているか、相手サイトの処理速度が遅くなっているおそれがあります。

D.2 Hitachi File Remote Replicator 統計情報ログ

Hitachi File Remote Replicator 統計情報ログ (/enas/log/russtat.log) には、システム統計情報とペア統計情報が出力されます。

- ・ システム統計情報
自サイトで発生した HFRR ペアに関する事象の統計情報です。
- ・ ペア統計情報
HFRR ペアごとに発生した事象の統計情報です。

Hitachi File Remote Replicator 統計情報ログは次の形式で出力されます。

```
*** System Statistical information ***
Date,Channel,Process,Process start totals,Pairs,Copies,Copy request totals,Copy
beginning totals
MM DD hh:mm:ss,aa...aa,bbbb,ccccccc,ddd,eeeeeee,fffffff,gggggggg

*** Pair statistical information ***
Date,Pair,Copy request totals,Copy beginning totals,Copy data size
MM DD hh:mm:ss,hh...hh,iiiiiii,jjjjjjjj,kkkkkkkk
...
```

Hitachi File Remote Replicator 統計情報ログに出力される情報を、次の表に示します。

表 D-1 Hitachi File Remote Replicator のシステム統計情報として出力される内容

項目	内容
Date	統計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。
Channel	HVFP のノードのホスト名が出力されます。
Process	現在動作中の処理プロセスの数が出力されます。
Process start totals	統計情報の取得間隔の間に起動された処理プロセスの累計が出力されます。
Pairs	現在の HFRR ペアの数が出力されます。
Copies	現在コピー中の HFRR ペアの数が出力されます。
Copy request totals	統計情報の取得間隔の間に全 HFRR ペアで発生したコピー要求の累計数が出力されます。条件を満たしていないなどで、コピーが実行されなかった数も含まれます。
Copy beginning totals	統計情報の取得間隔の間に全 HFRR ペアで開始されたコピーの累計数が出力されます。条件を満たさなくてコピーが開始されなかった数は含まれません。

表 D-2 Hitachi File Remote Replicator のペア統計情報として出力される内容

項目	内容
Date	統計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。
Pair	HFRR ペアの名称が出力されます。

項目	内容
Copy request totals	統計情報の取得間隔の間に発生したコピー要求の累計数が出力されます。条件を満たしていないなどで、コピーが実行されなかった数も含まれます。
Copy beginning totals	統計情報の取得間隔の間に開始されたコピーの累計数が出力されます。条件を満たしていなくてコピーが開始されなかった数は含みません。
Copy data size	統計情報の取得間隔の間に送受信されたコピーデータ量が出力されます (単位: バイト)。

これらの情報から、単位時間当たりのコピーデータ量の向上が見込めない場合は、高負荷な状態になっていると考えられます。

トラブルシューティング事例

GUI, HCP 連携およびウイルススキャンに関するトラブルシューティングの事例について説明します。

- E.1 GUI に関するトラブルシューティング事例
- E.2 HCP 連携に関するトラブルシューティング事例
- E.3 ウイルススキャンに関するトラブルシューティング事例

E.1 GUI に関するトラブルシューティング事例

GUI 操作に関連して発生した問題のトラブルシューティングの事例を示します。

表 E-1 GUI に関するトラブルシューティング事例

問題発生箇所	問題点	要因と対処
Hitachi File Services Manager のインストール	インストール中に KAQM30001-E が表示される。	管理者権限がないユーザーでインストールを実行しました。 管理者権限があるユーザーで管理サーバにログインし直してから、インストールを再実行してください。
	インストール中に KAQM30002-E または KAQM30007-E が表示される。	Hitachi File Services Manager をインストールする管理サーバの OS または OS のバージョンがサポート対象外です。 サポート対象の OS および OS のバージョンを適用している管理サーバを準備してから、インストールを再実行してください。
	インストール中に KAQM30053-E または KAQM30059-E が表示される。	Hitachi File Services Manager をインストールする管理サーバの空きディスク容量が不足しています。 管理サーバのディスク容量を見直してから、インストールを再実行してください。
	インストール中に KAQM30009-E が表示される。	Hitachi File Services Manager をインストールする管理サーバがマシン要件を満たしていない可能性があります。 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から、インストールを再実行してください。
全般	WWW ブラウザーで Hitachi File Services Manager が表示できない。	Hitachi Command Suite 共通コンポーネントが起動していません。 次の操作を実行して、Hitachi Command Suite 共通コンポーネントを起動してください。 Windows 7 までの Windows の場合 [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 スタート画面のアプリ一覧から [Start - HFSM] を選択します。
		管理サーバのディスク容量が不足しているため、Hitachi Command Suite 共通コンポーネントの起動に失敗しました。 管理サーバのディスク容量を見直してから、次の操作を実行して、Hitachi Command Suite 共通コンポーネントを起動してください。 Windows 7 までの Windows の場合 [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 スタート画面のアプリ一覧から [Start - HFSM] を選択します。
	1 回の操作でダイアログが 2 つ表示された (1 つは白画面, もう 1 つは [閉じる] ボタンが動作しない)	WWW ブラウザーのウィンドウ制御によって発生することがあります。Hitachi File Services Manager の管理対象システムの障害ではありません。 [X] ボタンでこれらのウィンドウを閉じ、ダイアログを表示する操作を再実行してください。

問題発生箇所	問題点	要因と対処
	表示された画面で次の事象が発生する。 <ul style="list-style-type: none"> 一部の画面が正しく表示されない。 ボタンの表示が乱れる（カーソルを合わせたり、離したりしたときにボタン表示が乱れる）。 JavaScript エラーが発生する。 	<p>WWW ブラウザーまたはプロキシサーバのキャッシュに、異なるバージョンの Hitachi File Services Manager の画面の情報が残っているため、画面が正しく表示されないことがあります。この問題は、更新インストールを実行した場合に発生しやすくなります。</p> <p>WWW ブラウザーのキャッシュをクリアし、再実行してください。</p> <p>WWW ブラウザーにプロキシサーバを指定している場合は、「システム構成ガイド」の管理コンソールの環境設定について説明している個所を参照し、プロキシの設定を見直してください。</p>
	ボタンをクリックし、サブウィンドウ表示時に、ウィンドウ上に「ページを表示できない」が表示された。	<p>次の要因が考えられます。</p> <ul style="list-style-type: none"> クライアントマシンとノード間のネットワークに問題がある。 ノードが起動していない。 <p>「1.3」を参照し、対処してください。</p>
		<p>次の要因が考えられます。</p> <ul style="list-style-type: none"> 管理コンソールの OS が管理コンソールのマシン要件を満たしていないおそれがあります。 管理コンソールの OS が、SSL 証明書の検証に失敗しているおそれがあります。 <p>「システム構成ガイド」の管理コンソールの環境設定について説明している個所を参照し、管理コンソールのマシン要件を確認してください。</p>
	実行中のダイアログが、30分以上経過しても結果ダイアログに遷移しない。	<p>WWW ブラウザーのウィンドウ制御によって発生することがあります。Hitachi File Services Manager の管理対象システムの障害ではありません。</p> <p>実行中のダイアログを [X] ボタンで閉じてください。そのあとに、リフレッシュ処理を実行して最新の状態を確認してください。</p>
	Hitachi File Services Manager の操作中に KAPM08201-E が表示される。	<p>画面表示が完了する前に操作をしたおそれがあります。</p> <p>画面表示が完了したあとで、再度操作をしてください。問題が解消されない場合は、管理サーバのログを取得して、保守員に連絡してください。</p>
	実行中のダイアログで KAQM19114-E または KAQM19115-E が表示される。	<p>WWW ブラウザーのウィンドウ制御によって発生することがあります。Hitachi File Services Manager の管理対象システムの障害ではありません。</p> <p>表示されたメッセージに従って対処してください。</p>
	Firefox で Hitachi File Services Manager にログインしたあと、[閉じる] ボタンをクリックしても画面が閉じない。	<p>Firefox のウィンドウ制御によって発生することがあります。Hitachi File Services Manager の管理対象システムの障害ではありません。</p> <p>Firefox の about:config ページで、dom.allow_scripts_to_close_windows に「true」を設定してください。</p>
	操作がエラー終了したときに表示された画面を閉じてしまい、発生したエラーの内容を確認できなかった。	<p>Hitachi File Services Manager のログファイルで問題が発生した日時に出力されたメッセージログを参照し、メッセージ ID およびメッセージテキストからエラーの内容を確認してください。Hitachi File Services Manager のログファイルについては、「2.8」を参照してください。</p>

問題発生箇所	問題点	要因と対処
	CIFS クライアントから共有へのログインに失敗する。	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ないよう設定している可能性があります。 [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。CIFS サービスを再起動する方法については、「ユーザズガイド」を参照してください。
	画面に「500 Internal Server Error」と表示される。	サービスが停止しているか、または開始処理中である可能性があります。 サービスの稼働状態を確認してください。サービスが停止している場合は起動してください。サービスが起動している場合はしばらく待ってから、Hitachi File Services Manager にログインし直してください。
[Processing Node の状態], [Physical Node の状態], または [ハードウェアの状態] の表示内容	[Processing Node の状態] が「Online」以外になっている。	Processing Node を構成する [Physical Node の状態] が「Online」以外になっています。 [Physical Node の状態] に表示される項目に対応して、対処してください。
	[Physical Node の状態] が「Unknown error」と表示される。	管理サーバとノード間のネットワークに問題があります。 ping コマンドを実行するなどしてネットワークを見直してください。
		ノードが起動していません。 ノードを起動してください。
		ノード側で Primary Server Base が動作していません。 全ログデータを取得して、保守員に連絡してください。 Processing Node の追加や編集、または Processing Node の更新操作時に、フェールオーバー中などクラスタの状態遷移が理由で、エラーが返りました。 詳細は、[Cluster Management] ダイアログでノードおよびリソースグループの状態を確認してください。また、[Check for Errors] ダイアログでエラーメッセージが出力されていないか確認してください。 ダイアログを表示できない場合は、「1.3」を参照し、対処してください。対処したあと、Processing Node を更新してください。 改善しない場合は、全ログデータを取得して、保守員に連絡してください。
	[Physical Node の状態] に「Credential error」と表示される。	ノードと Hitachi File Services Manager のパスワードが不一致です。 ノード側のパスワードを変更したあと、Processing Node に関する情報を更新してください (パスワードはクラスタ内のノードで一貫させておく必要があります)。 または、[ノード編集] ダイアログで、Hitachi File Services Manager 側のパスワードを変更してください。
	[Physical Node の状態] に「Maintenance required」と表示される。	ユーザー操作 (クラスタ停止/ノード停止/リソースグループ停止/リソースグループ監視除外) によって次のどれかの状態になっています。 <ul style="list-style-type: none"> フェールオーバー クライアントサービスが停止している

問題発生箇所	問題点	要因と対処
		<ul style="list-style-type: none"> クラスタ未構築 [Cluster Management]ダイアログでノードの状態を確認して、必要であればサービスを起動してください。クラスタ未構築の場合は、クラスタを構築してください。 また、回復操作後に、Processing Node に関する情報を更新してください
	[Physical Node の状態] に「Transitional state」と表示される。	リソースグループが起動中、または停止中の状態です。しばらくすると別の状態に遷移します。ただし、この状態が長く続く場合は障害のおそれがあります。しばらく待って、Processing Node に関する情報を更新すると回復します。回復しない場合は、再実行し、回復するまで待ってください。 長時間待っても回復しない場合は、[Cluster Management] ダイアログでノードの状態を確認してください。
	[Physical Node の状態] に「Ready for failback」と表示される。	該当する Physical Node で稼働する予定のリソースグループがフェールオーバーしている状態です。この状態の場合、相手側のノードでサービスが稼働しています。 [Cluster Management]ダイアログでノードの状態を確認してください。 また、障害要因を取り除いたあと、手でフェールバックしてください。
	[Physical Node の状態] に「Shutdown」が表示される。	Processing Node が停止中の状態になっています。
	[Physical Node の状態] に「Starting」が表示される。	Processing Node が起動中の状態になっています。しばらく待って、Processing Node に関する情報を更新すると回復します。両方の Physical Node の状態が回復したのを確認してください。 複数回、Processing Node の情報を更新しても、状態が回復しない場合、OS の起動中にエラーが発生しているおそれがあります。起動している Physical Node 側の [Cluster Management] ダイアログでノードの状態を確認してください。 両方の Physical Node が起動していない場合は、保守員に連絡してください。
	Processing Node の[ハードウェアの状態]で、状態が「Normal」以外の状態になっている。	Processing Node を構成する Physical Node の[ハードウェアの状態]が「Normal」以外になっています。 [ハードウェアの状態]を構成する要素の中で、「Normal」以外のステータスのものがあります。[設定]タブの [ヘルスマニター] から、状態を確認してください。 それぞれの状態と、障害要因については、「ユーザーズガイド」のハードウェアの情報を参照する方法について説明している箇所を参照してください。 対処方法については「4.21」を参照してください。
[ファイルシステムの状態] の表示内容	[ファイルシステムの状態] に「File snapshots out of capacity」が表示される。	差分格納デバイスの容量が不足している場合に表示されます。 ノード側で、ファイルシステムの [マウント状態] が「Overflow」になっています。 対処方法については、「4.9」を参照してください。
	[ファイルシステムの状態] に「File snapshots error」が表示される。	差分格納デバイスに障害が発生している場合に表示されます。

問題発生箇所	問題点	要因と対処
		ノード側で、ファイルシステムの [マウント状態] が「Not available」になっています。 対処方法については、「4.9」を参照してください。
	[ファイルシステムの状態] に「Data corrupted」が表示される。	OS の障害によってファイルシステムが閉塞している場合に表示されます。 ノード側で、ファイルシステムの [マウント状態] が「Fatal error」になっています。 対処方法については、「4.8」を参照してください。
	[ファイルシステムの状態] に「Device error」が表示される。	LU の障害（ドライブの多重障害）によってファイルシステムが閉塞している場合に表示されます。 ノード側で、ファイルシステムの [Device status] が「Error」になっています。 対処方法については、「4.8」を参照してください。
	[ファイルシステムの状態] に「Blocked」が表示される。	差分格納デバイスの容量不足によって、ファイルシステムがブロックされている場合に表示されます。 [<ファイルシステム>] サブウィンドウの [File Snapshots] タブで差分格納デバイスの状態を確認し、「4.9」を参照して対処してください。
	[ファイルシステムの状態] に「Blocked and ready」が表示される。	ファイルシステムがブロック状態になってから、差分格納デバイスの空き容量を確保したあとに、OS が再起動されていない場合に表示されます。 OS を再起動してください。システム管理者が OS を再起動する方法については、「ユーザズガイド」を参照してください。
	[ファイルシステムの状態] に「Expanding」が表示される。	ファイルシステムを拡張する処理を実行中か、処理でエラーが発生している場合に表示されます。 しばらくたってから、Processing Node または Virtual Server の情報を更新してください。状態が変わらない場合は、処理でエラーが発生しているおそれがあります。 全ログデータを取得して、保守員に連絡してください。
	[ファイルシステムの状態] に「Reclaiming」が表示される。	ファイルシステムに割り当てられている仮想 LU の未使用領域を解放する処理を実行している場合に表示されます。 しばらくたってから、Processing Node の情報を更新してください。状態が変わらない場合は、処理でエラーが発生しているおそれがあります。全ログデータを取得して、保守員に連絡してください。
ファイルスナップショットの [状態] の表示内容	ファイルスナップショットの [状態] に「Purging」と表示される。	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をまとめて削除する処理でエラーが発生しています。 しばらくたってから、ファイルスナップショットの情報を更新してください。状態が変わらない場合は、処理でエラーが発生しているおそれがあります。すべての差分スナップショットをまとめて削除する操作を再実行してください。
	ファイルスナップショットの [状態] に「Expanding」と表示される。	差分格納デバイスを拡張する処理でエラーが発生しています。 しばらくたってから、ファイルスナップショットの情報を更新してください。状態が変わらない場合は、処理でエラーが発生しているおそれがあります。

問題発生箇所	問題点	要因と対処
		「ユーザーズガイド」に記載されている手順に従って、差分格納デバイスの拡張処理のリカバリーを実行してください。
	ファイルスナップショットの [状態] に「In processing or error」と表示される。	差分格納デバイスの設定または解除の処理でエラーが発生しています。 しばらくたってから、ファイルスナップショットの情報を更新してください。状態が変わらない場合は、処理でエラーが発生しているおそれがあります。差分格納デバイスを解除してください。HFRR ペアとして定義したファイルシステムの場合、HFRR ペアを解除してから差分格納デバイスを解除してください。
	ファイルスナップショットの [状態] に「Overflow」と表示される。	差分格納デバイスの容量が不足し、差分スナップショットが無効になっています。 対処方法については、「4.9.1」を参照してください。
	ファイルスナップショットの [状態] に「Blocked」と表示される。	差分格納デバイスの容量が不足し、ファイルシステムがブロックされています。 対処方法については、「4.9.2」を参照してください。
	ファイルスナップショットの [状態] に「Blocked and busy (<進捗>% processed)」と表示される。	ファイルシステムがブロックされている状態で、バックグラウンド処理を実行中です。 バックグラウンド処理が完了してから、次の操作を実行してください。
	ファイルスナップショットの [状態] に「Blocked and expanding」と表示される。	ファイルシステムがブロックされている状態で、差分格納デバイスを拡張する処理を実行中か、処理でエラーが発生しています。 しばらくたってから、ファイルスナップショットの情報を更新してください。状態が変わらない場合は、処理でエラーが発生しているおそれがあります。 対処方法については、「2.6」を参照してください。
	ファイルスナップショットの [状態] に「Not available」と表示される。	次のどれかの場合に表示されます。 <ul style="list-style-type: none"> ファイルシステムまたは差分格納デバイスの論理ボリュームに障害が発生している クラスタ、ノードまたはリソースグループが正常に稼働していない 対処方法については、「2.6」を参照してください。
	ファイルスナップショットの [状態] に「Offline」と表示される。	クラスタ、ノードまたはリソースグループが正常に稼働していません。 クラスタ、ノードおよびリソースグループの状態を確認してください。
	ファイルスナップショットの [状態] に「I/O error」と表示される。	ファイルシステムまたは差分格納デバイスを構成する LU にアクセス障害が発生しています。 対処方法については、「2.6」を参照してください。
	ファイルスナップショットの [状態] に「System error」と表示される。	システムエラーが発生しています。 対処方法については、「2.6」を参照してください。
システムソフトウェアインストールウィザードの表示内容	[インストールの実行] ページの更新インストールのステップで KAQM20046-E が表示される。	管理サーバとノード間のネットワークに問題があるおそれがあります。 ダイアログを表示できない場合は、「1.3」を参照し、対処してください。対処したあと、OS が停止している場合はノード本体のスイッチを押して OS を起動してください。 その後、インストールファイルを再度転送してから更新インストールをやり直してください。繰り返しエラーが発生する場合は全ログデータを取得して、保守員に連絡してください。

問題発生箇所	問題点	要因と対処
		<p>前回の更新インストールが正常に完了していないおそれがあります。</p> <p>インストールファイルを再度転送してから更新インストールをやり直してください。繰り返しエラーが発生する場合は全ログデータを取得して、保守員に連絡してください。</p>
	<p>[確認] ページに表示されるインストール元ディレクトリに、指定していないファイルパス「C:\fakepath\install_files.tar.gz」が表示される。</p>	<p>WWW ブラウザーのセキュリティ機能の影響で、ファイルパスの取得に失敗しているおそれがあります。</p> <p>管理クライアントで使用している WWW ブラウザーで、管理サーバの URL を信頼済みサイトに登録してください。</p>
<p>[HDvM 設定編集] ダイアログ</p>	<p>KAQM23028-E が表示される。</p>	<p>Device Manager の情報が誤っているおそれがあります。</p> <p>[HDvM 設定編集] ダイアログの入力値を見直してください。</p> <p>Device Manager サーバが起動していないおそれがあります。</p> <p>Device Manager サーバが起動しているかどうか確認してください。</p> <p>一時的なネットワークの障害のおそれがあります。</p> <p>Hitachi File Services Manager と Device Manager を別サーバで管理している場合、ネットワークに問題がないか tracert コマンドおよび telnet コマンドを使用して、Hitachi File Services Manager から Device Manager サーバへの接続に問題がないことを確認してください。</p> <p>[例]</p> <pre>tracert < IPアドレス> telnet < IPアドレス> 2001 (2001 は Device Manager サーバのポート番号)</pre> <p>Windows ファイアウォールの設定でアクセスがブロックされているおそれがあります。</p> <p>Windows ファイアウォールのログを確認してください。</p> <p>Device Manager サーバが busy のおそれがあります。</p> <p>繰り返し発生する場合は、[HDvM 設定編集] ダイアログから、通知時刻を変更します。</p> <p>Device Manager サーバで問題が発生しているおそれがあります。</p> <p>Device Manager のマニュアルを参照して、該当するメッセージの詳細を確認してください。</p>
<p>[HDvM 連携管理] ダイアログ</p>	<p>Hitachi File Services Manager から Device Manager へ構成情報が通知されない</p>	<p>管理対象の HVFP が 3.0.0 より前のバージョンのおそれがあります。</p> <p>管理対象の HVFP のバージョンを確認してください。</p>
<p>ダイアログ</p>	<p>KAQM21100-E が表示される。</p>	<p>Hitachi File Services Manager とノードの情報が不一致です。Settings で構成情報変更を実行したあとにリフレッシュを実行していないおそれがあります。</p> <p>または、ほかの Hitachi File Services Manager や CLI でノードの操作が実行されたおそれがあります。</p> <p>[Processing Node 更新] ボタンをクリックして、リフレッシュ処理を実行してください。</p>

問題発生箇所	問題点	要因と対処
[共有追加] ダイアログ [ファイルシステム構築と共有作成]ダイアログ	ローカルユーザや外部サーバに設定したユーザー/グループ名が表示されない。	Hitachi File Services Manager とノードの情報が不一致です。 [ユーザーとグループ更新] ボタンをクリックして、リフレッシュ処理を実行してください。
[ファイルシステム構築と共有作成]ダイアログ	ノードにストレージシステムを登録している場合に、KAQM23537-E が表示される。	RAID グループを作成しましたが、LU を作成するために必要なディスク容量が不足しています。 ディスクを増設するか、使用できる LU のサイズを指定して再実行してください。
[ファイルシステム構築と共有作成]ダイアログ [ファイルシステム構築] ダイアログ [ファイルシステム編集] ダイアログ	[ネームスペースを使用する] の [はい] を選択しても、[テナントハード Quota] および [ストレージ使用量] に値が表示されず、ネームスペースを使用できない。	HCP との通信に障害が発生しています。 HCP の稼働状態を確認してから、設定ウィザードの [6-3. HCP 設定] ページで [接続テスト] ボタンをクリックしてください。HCP と正常に接続できることを確認してから、再実行してください。
[ファイルシステム拡張] ダイアログ	ネームスペースを使用するファイルシステムを拡張するときに、HCP との通信が KAQM26118-E (HTTP リターンコード: 100) で失敗する。	NIS サーバに接続できませんでした。 NIS サーバの設定およびネットワークの状態に問題がないか確認してください。問題を取り除いたあと、再実行してください。
Device Manager 連携	Hitachi File Services Manager から Device Manager への構成情報の通知に失敗する (KAQM23024-E, KAQM23025-E, または KAQM23026-E が表示される)。	[HDvM 設定編集] ダイアログの「KAQM23028-E が表示される。」の要因を参照してください。 [HDvM 設定編集] ダイアログの「KAQM23028-E が表示される。」の要因に対応する対処を参照して対処してください。
	Device Manager の GUI にログインして Hitachi File Services Manager を利用したいが利用できない (KAQM23030-E が表示される)。	Hitachi File Services Manager と Device Manager のユーザーアカウントを管理するサーバの設定が誤っているおそれがあります。 Hitachi File Services Manager と Device Manager を別サーバで管理している場合、ユーザーアカウントを管理するサーバが正しいか確認してください。 詳細は、「システム構成ガイド」を参照してください。
	Device Manager の管理画面に Hitachi File Services Manager で管理しているファイルシステムやマウント情報が表示されない。	HVFP が使用しているストレージシステムが Device Manager に登録されていないおそれがあります。 Device Manager に LUN セキュリティを有効にしたストレージシステムを登録してください。詳しくは Device Manager のマニュアルを参照してください。 HVFP が使用しているストレージシステムを Device Manager に登録したあと、再度 Hitachi File Services Manager の構成情報を通知してください。
設定ウィザード	[6-3. HCP 設定] ページで、HCP との接続テストが KAQM26118-E (HTTP リ	NIS サーバに接続できませんでした。 NIS サーバの設定およびネットワークの状態に問題がないか確認してください。問題を取り除いたあと、再実行してください。

問題発生箇所	問題点	要因と対処
	ターンコード:100) で失敗する。	
	HCP を設定したとき, [8. システムの設定] ページで, HCP との通信が KAQM26118-E (HTTP リターンコード:100) で失敗する。	

E.2 HCP 連携に関するトラブルシューティング事例

HCP との連携で発生した問題に関するトラブルシューティングの事例を示します。

表 E-2 HCP 連携に関するトラブルシューティング事例

問題点	要因と対処
ファイルシステムが作成できない。	作成するネームスペースの容量に対してテナントのハード Quota の値が不足しているおそれがあります。HCP 管理者にハード Quota の値を見直すよう依頼してください。
マイグレーションやリコールが KAQM37037-E, KAQM37066-E または KAQM37094-E (HTTP リターンコード:400) で失敗する。	テナントまたはネームスペースにアクセスするためのユーザーアカウントに, 操作に必要なアクセス権限が与えられていないおそれがあります。HCP 管理者に権限を見直すよう依頼してください。
マイグレーションやリコールが KAQM37037-E, KAQM37066-E または KAQM37094-E (HTTP リターンコード:403) で失敗する。	<ul style="list-style-type: none"> テナントまたはネームスペースにアクセスするためのユーザーアカウントの情報が誤っているおそれがあります。HCP 管理者にユーザー名およびパスワードを確認して, 正しい情報を指定してください。 テナントまたはネームスペースにアクセスするためのユーザーアカウントに, 操作に必要なアクセス権限が与えられていないおそれがあります。HCP 管理者に権限を見直すよう依頼してください。 ネームスペースが存在しないおそれがあります。HCP 管理者に確認してください。 ネームスペースのオブジェクトに対して, カスタムメタデータの追加, 削除および置き換えができるように設定されていないおそれがあります。HCP 管理者にネームスペースの設定を見直すよう依頼してください。 ネームスペースに Retention Class が設定されているおそれがあります。HCP と HVFP を連携している場合, 保管期間は HVFP の WORM 機能で設定してください。 HVFP と HCP の通信プロトコル (HTTP/HTTPS) の設定が一致していないおそれがあります。arcsslctl コマンドで通信プロトコルの設定を見直してください。HCP 管理者に通信プロトコルの設定を見直すよう依頼してください。
マイグレーションやリコールが KAQM37037-E, KAQM37066-E または KAQM37094-E (HTTP リターンコード:409) で失敗する。	<ul style="list-style-type: none"> HCP のほかの処理と競合したおそれがあります。しばらく待ってから, 再度実行してください。 ネームスペースの設定で, バージョン管理が無効になっているおそれがあります。HCP 管理者にバージョン管理を有効にするよう依頼してください。
マイグレーションが KAQM37037-E, KAQM37066-E または KAQM37094-E (HTTP リターンコード:413) で失敗する。	HCP のネームスペースで使用している容量が, ハード Quota の値を超えているおそれがあります。HCP 管理者にハード Quota の値を見直すよう依頼してください。

問題点	要因と対処
マイグレーションやリコールが KAQM37037-E, KAQM37066-E または KAQM37094-E (HTTP リターンコード: 500 または 503) で失敗する。	HCP で内部エラーが発生しているか、HCP が一時的に処理できない状態であるおそれがあります。しばらく待ってから、再度実行してください。
マイグレーションが KAQM37038-E で失敗する。	テナントの設定で、バージョン管理が無効になっているおそれがあります。HCP 管理者にバージョン管理を有効にするよう依頼してください。
ほかのファイルサーバからのデータインポート中に HCP へマイグレートしたファイルが、インポートが終わっても OFFLINE 属性のままである。	ほかのファイルサーバからデータインポート中のファイルを HCP にマイグレートした場合、そのファイルのインポート完了後にマイグレートするまでは OFFLINE 属性のままです。再度マイグレートしてください。
ほかのファイルサーバからのデータインポート中に HCP へのマイグレーションが動作し、データインポートの進捗がなくなった。	ほかのファイルサーバからのデータインポート中に HCP へのマイグレーションが動作すると、すべてのファイルのインポートが一時停止します。マイグレーション完了後に再開します。
マイグレートしたファイルをリストアしたが、リストアされないファイルがある。	HVFP のファイル削除と同期して HCP 側のファイルが削除されます。そのため、リストア前に HVFP 側のファイルを削除した場合は、そのファイルはリストアしても HVFP に戻りません。削除したファイルは、過去バージョンディレクトリから戻してください。
HCP に接続できない。	<ul style="list-style-type: none"> • HVFP に設定されている DNS サーバのアドレスを変更したあとで、OS または Virtual Server を再起動していないおそれがあります。 • HCP と HVFP の間の機器で、HCP に接続するためのポートがブロックされているおそれがあります。HTTP (80) または HTTPS (443)、および MAPI 通信 (9090) のポートが接続できるか見直してください。
HCP との通信が KAQM26110-E (HTTP リターンコード: 302) で失敗する。	プロキシサーバで HCP の管理ポート (9090) の接続が許可されていません。ポート番号 9090 の接続を許可するようにプロキシサーバの設定を変更してから、設定ウィザードの [6-3. HCP 設定] ページで [接続テスト] ボタンをクリックし、HCP と正常に接続できることを確認してください。
ハードリンクが作成できない。	HCP にデータをマイグレートしているファイルシステムは、デフォルトではハードリンク作成が禁止されます。ハードリンクを作成する場合はファイルシステムの設定を変更してください。ただし、ハードリンクのファイルは HCP からリストアできません。
OFFLINE 属性になったファイルが検索できない。	クライアントによっては、OFFLINE 属性のファイルを検索対象外にするものがあります。CIFS 共有の設定を変更することで OFFLINE 属性を無効にできます。ただし、OFFLINE 属性を無効にすることでタイムアウト時間が短くなるなどクライアントの動作が変わるため注意してください。
特定ファイルのマイグレーションが失敗する。	<ul style="list-style-type: none"> • ファイルパスに改行コードを含むファイルはマイグレートされません。ファイル名を変更してください。 • サイズが大きいファイルの場合、タイムアウトエラーになるおそれがあります。タイムアウト値の設定を見直してください。 • 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ます。ファイルがマイグレーション中に更新されていないか見直してください。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。
マイグレーションやリコールがタイムアウトで失敗する。	<ul style="list-style-type: none"> • サイズの大きいファイルのマイグレーションが失敗する場合は、HCP との通信タイムアウト時間が短いおそれがあります。通信タイムアウト時間を見直してください。

問題点	要因と対処
	<ul style="list-style-type: none"> ネットワーク帯域が狭いため、HCP との間の転送速度の下限値を下回ってエラーになっているおそれがあります。ネットワーク帯域に合わせて、転送速度の下限值を見直してください。 HCP, HVFP またはネットワークの負荷が高過ぎるおそれがあります。最大スレッド数を見直してください。 HCP でサービスが実行されているおそれがあります。マイグレーションのスケジュールを見直してください。 ネットワークに問題があるおそれがあります。ネットワークを見直してください。
マイグレーションタスクの状態が「Last time interrupted」になっている。	設定した打ち切り時間までにマイグレーション処理が完了しなかったため、タスクが停止されました。データが HCP にマイグレートされなかったファイルがあるおそれがあります。再度タスクを実行してください。タスクの状態が繰り返し「Last time interrupted」になる場合は、打ち切り時間の設定を見直してください。

E.3 ウィルススキャンに関するトラブルシューティング事例

リアルタイムスキャン機能の使用中に発生した問題に関するトラブルシューティングの事例を示します。

表 E-3 ウィルススキャンに関するトラブルシューティング事例

問題点	要因と対処
[List of Scanner Servers] ページの [Server status] に「Blocked (Access user info. is not registered)」と表示される。	<p>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ません。</p> <p>スキャンサーバで、Hitachi Server Protect Agent Manager の [登録ノード一覧] に対象の HVFP のホスト名があるかを確認してください。対象のホスト名がない場合は、Hitachi Server Protect Agent Manager でノードの情報を指定して [追加] ボタンをクリックしたあと、[OK] ボタンをクリックしてください。対象のホスト名がある場合は、Hitachi Server Protect Agent Manager の [OK] ボタンをクリックしてください。</p> <p>スキャンサーバでの設定が完了したあと、HVFP で再度リアルタイムスキャンを有効にしてください。</p>
[List of Scanner Servers] ページの [Server status] に「Blocked (Timeout)」と表示される。	<p>一定時間が経過してもスキャンサーバからの応答がありませんでした。ネットワークに障害が発生していないか、スキャンサーバが高負荷になっていないかを確認し、問題がある場合は対処してください。</p> <p>また、トレンドマイクロ社のスキャンソフトを使用している場合で、CIFS ユーザーの認証方式にローカル認証以外を選択しているときは、外部認証サーバに障害が発生していないかを確認してください。障害が発生している場合は、障害を回復してください。</p>