HITACHI
Inspire the Next

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

対象製品

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

輸出時の注意

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

商標類

Active Directory は，米国 Microsoft Corporation の，米国およびその他の国における登録商標または商標です。
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。
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 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。
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。
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。
Windows は，米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
Windows NT は，米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
Windows Server は，米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。

発行

2014 年 6 月（第 6 版）K6603839

著作権

目次

図目次

表目次

はじめに

このマニュアルは，シングルノード構成の Hitachi Virtual File Platform / Hitachi Data Ingestor（HVFP/HDI）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

このマニュアルは，シングルノード構成の HVFP/HDI を運用・管理する方（システム管理者）にお読みいただくことを前提に説明しています。

また，次の知識をお持ちであることを前提に説明しています。

- 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
- CIFS に関する基本的な知識
- NFS 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/HDI 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. 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。
B. ネットワークの通信状況の確認方法	ネットワーク設定の問題のため，HVFP/HDI 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。
C. 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。
D. トラブルシューティング事例	GUI，コマンド，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 と HDI でマニュアル体系が異なります。使用している製品に対するマニュアル体系を参照してください。

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

表 はじめに -1 HVFP のマニュアル体系

マニュアル名	内容
Hitachi Virtual File Platform / Hitachi Data Ingestor システム構成ガイド	HVFP を運用するために，最初にお読みいただくマニュアルです。 HVFP の運用を開始する前に理解または検討しておいていただきたいことや，外部サーバの環境設定などについて説明しています。
Hitachi Virtual File Platform セットアップガイド	クラスタ構成の HVFP のセットアップ方法について説明しています。 仮想サーバで HVFP を運用する場合は，「仮想サーバ環境セットアップガイド」をお読みください。
Hitachi Virtual File Platform 仮想サーバ環境セットアップガイド	クラスタ構成の HVFP での Virtual Server のセットアップ方法について説明しています。
Hitachi Virtual File Platform ユーザーズガイド	クラスタ構成の HVFP を運用するために必要な手順や GUI リファレンスなどを説明しています。
Hitachi Virtual File Platform トラブルシューティングガイド	クラスタ構成の HVFP の障害対策を説明しています。
Hitachi Virtual File Platform シングルノード構成セットアップガイド	シングルノード構成の HVFP のセットアップ方法について説明しています。
Hitachi Virtual File Platform / Hitachi Data Ingestor シングルノード構成ユーザーズガイド	シングルノード構成の HVFP を運用するために必要な手順や GUI リファレンスなどを説明しています。
Hitachi Virtual File Platform / Hitachi Data Ingestor シングルノード構成トラブルシューティングガイド（このマニュアル）	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。

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

表 はじめに -2 HDI のマニュアル体系

マニュアル名	内容
Hitachi Data Ingestor セットアップガイド	HDI を管理するために，最初にお読みいただくマニュアルです。 HDI のセットアップ方法について説明しています。
Hitachi Virtual File Platform / Hitachi Data Ingestor システム構成ガイド	HDI の運用を開始する前に理解または検討しておいていただきたいことや，外部サーバの環境設定などについて説明しています。
Hitachi Virtual File Platform / Hitachi Data Ingestor シングルノード構成ユーザーズガイド	HDI を運用するために必要な手順や GUI リファレンスなどを説明しています。

マニュアル名	内容
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（このマニュアル）	HDI の障害対策を説明しています。
Hitachi Virtual File Platform / Hitachi Data Ingestor コマンドリファレンス	HDI で使用できるコマンドの文法について説明しています。
Hitachi Virtual File Platform / Hitachi Data Ingestor メッセージリファレンス	HDI のメッセージについて説明しています。
Hitachi Virtual File Platform / Hitachi Data Ingestor ファイルアクセス（CIFS/NFS）ユーザーズガイド	CIFS または NFS クライアントから，HDI の CIFS サービスまたは NFS サービスを利用するに当たって，事前に知っておいていただきたいことや，注意する必要があることについて説明しています。
Hitachi Data Ingestor 保守取扱説明書	「メッセージリファレンス」や「シングルノード構成トラブルシューティングガイド」などに記載されている，保守員に依頼している作業について，HDI での解決手順を説明しています。

このマニュアルでの表記

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

このマニュアルでの表記	製品名称または意味
Active Directory	Active Directory(R)
ALog ConVerter	ALog ConVerter(R)
Firefox	Mozilla Firefox(R)
HCP	Hitachi Content Platform
HDI	Hitachi Data Ingestor
HVFP	Hitachi Virtual File Platform
Windows	Microsoft(R) Windows(R) Operating System
Windows 8	次の製品を区別する必要がない場合の表記です。 ・ Microsoft(R) Windows(R) 8 32-bit ・ Microsoft(R) Windows(R) 8 64-bit ・ Microsoft(R) Windows(R) 8 Enterprise 32-bit ・ Microsoft(R) Windows(R) 8 Enterprise 64-bit ・ Microsoft(R) Windows(R) 8 Pro 32-bit ・ Microsoft(R) Windows(R) 8 Pro 64-bit ・ Microsoft(R) Windows(R) 8.1 32-bit ・ Microsoft(R) Windows(R) 8.1 64-bit ・ Microsoft(R) Windows(R) 8.1 Enterprise 32-bit ・ Microsoft(R) Windows(R) 8.1 Enterprise 64-bit ・ Microsoft(R) Windows(R) 8.1 Pro 32-bit ・ Microsoft(R) Windows(R) 8.1 Pro 64-bit
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。 ・ Microsoft(R) Windows Server(R) 2003, Datacenter Edition Operating System ・ Microsoft(R) Windows Server(R) 2003, Enterprise Edition Operating System ・ Microsoft(R) Windows Server(R) 2003, Standard Edition Operating System

このマニュアルでの表記	製品名称または意味
	• Microsoft(R) Windows 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。 • Microsoft(R) Windows Server(R) 2012 Datacenter • Microsoft(R) Windows Server(R) 2012 Essentials • Microsoft(R) Windows Server(R) 2012 Foundation • Microsoft(R) Windows Server(R) 2012 Standard

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
＜ ＞	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。

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 すべて半角で指定してください。

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。

1

障害対策の流れ

この章では，Hitachi Virtual File Platform / Hitachi Data Ingestor（HVFP/HDI）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。

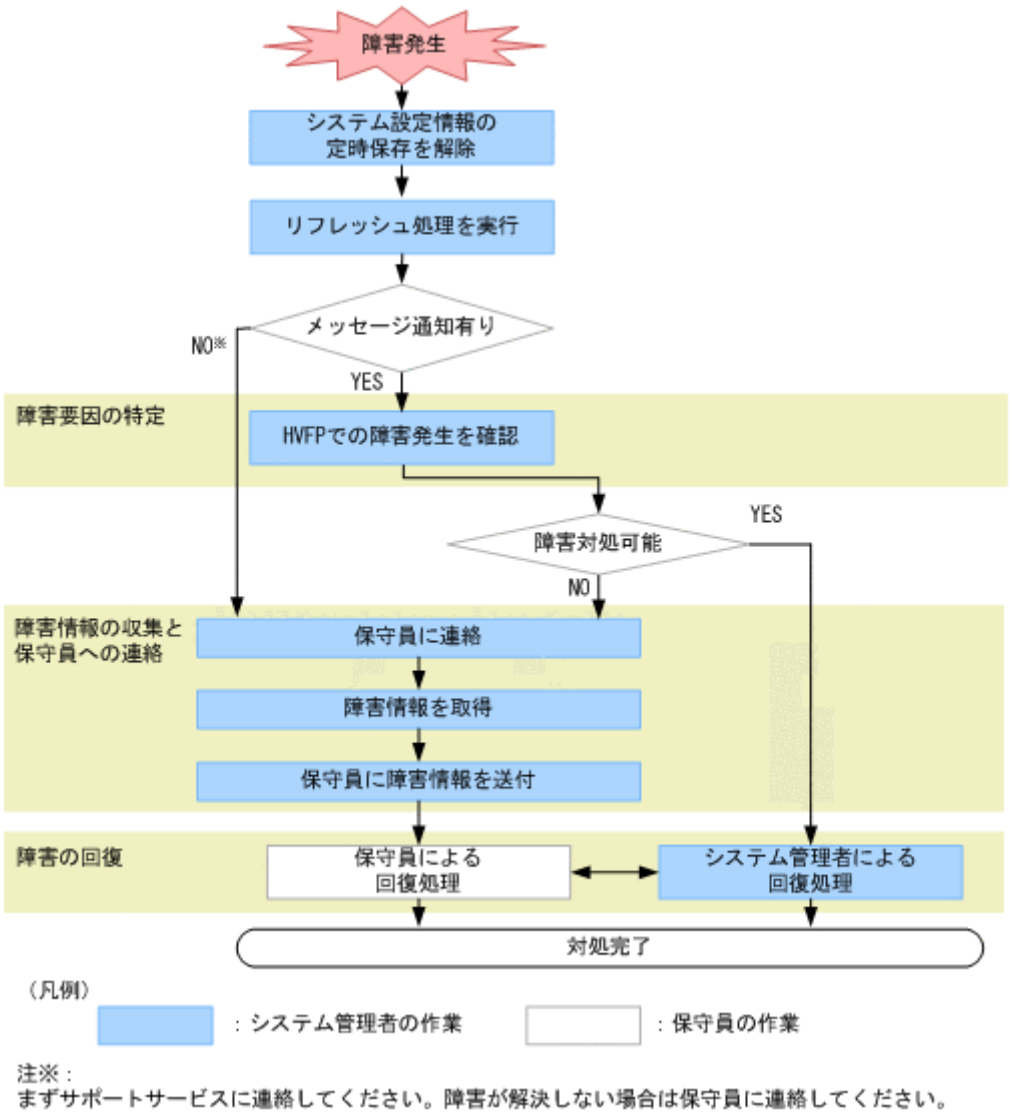
1.1 障害対策の概要

HVFP/HDI 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。その後，GUI の情報をリフレッシュしたら，要因を特定し，障害を回復します。

なお，コマンドを使用する場合は，事前に SSH 環境を設定してください。設定方法については「シングルノード構成ユーザーズガイド」を参照してください。GUI またはコマンドの操作中に発生するおそれがある障害の事例は，「付録 D. トラブルシューティング事例」を参照してください。

障害対策の流れを次に示します。

図 1-1 障害が発生した場合の対策の流れ（HVFP の場合）



HDI で GUI またはコマンドを利用できない場合は，DHCP サーバと HDI との接続に問題が発生し，ノードの IP アドレスに 169.254.1.100，ネットマスクに 255.255.0.0 が暫定的に設定されている可能性があります。169.254.1.100 に接続できるように設定したコンピュータをノードに接続させ，IP アドレスに 169.254.1.100 を指定してノードにアクセスできるかどうかを確認してください。アクセスできた場合，DHCP サーバとの接続に問題があります。必要な対処を実施してください。対処が完了したら，ノードを再起動してください。そのあと，システム設定情報の定時保存を解除してください。

また，HDI の場合，「保守員に連絡してください。」と指示されたときは，「保守取扱説明書」を参照して対処してください。

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。

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 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ったりした場合は，障害情報を収集し，保守員に送付します。

障害の回復

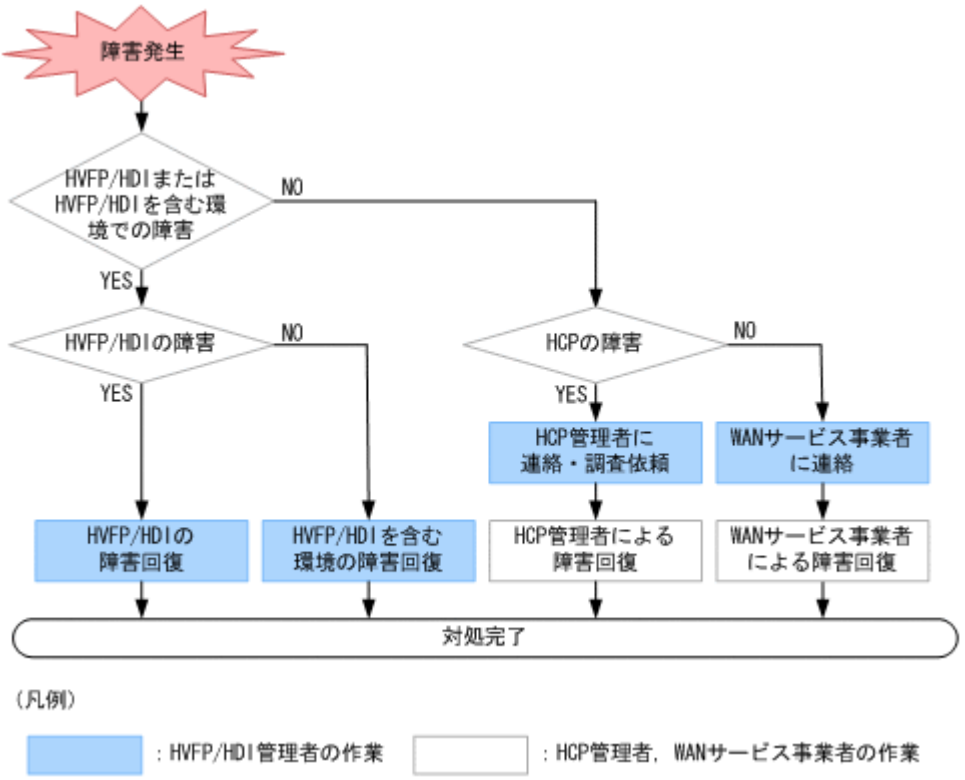
障害要因を特定したら，メッセージに従って障害を回復します。障害の内容によっては，保守員とシステム管理者の間で互いに連絡を取って障害を回復する必要があります。

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

HVFP/HDI で障害が発生していなくても，HCP にアクセスできないために HVFP/HDI のサービスを提供できないことがあります。HCP にアクセスできない障害が発生した場合は，「4.7 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 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ったり，アクセスできなかったりするなど，HVFP/HDI 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，「4.4.1 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. エンドユーザーがファイルシステムにアクセスできない場合は，20 分待ったあと，エンドユーザーに対象のファイルシステム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. 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

   サービス停止した 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ファイルシステムおよび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

   サービス停止した共有のパス名（¥¥＜ノードのホスト名＞¥＜ CIFS 共有名＞¥＜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ファイルシステムおよび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。

3. ノードの電源が入っていることを確認します。

   ノードにストレージシステムを接続している場合は, ストレージシステムの電源が入っていることも確認します。

   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/HDI のサービスを利用できるか，確認してください。

4. ノード上のシステムメッセージを確認します。

   障害のためシステムメッセージを確認できない場合は，「4.18 モニター類を使用して障害を回復する」を参照して対処してください。

5. 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

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。

   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. ファイルシステムウィンドウ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。ファイルシステムウィンドウを参照し，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. ＜ファイルシステム名＞ウィンドウ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，＜ファイルシステム名＞ウィンドウを参照し，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るよう設定されていることを確認してください。HDI で DHCP を使用している場合は，DDNS が正しく動作していることを確認してください。また，次に示すサーバとの接続状態を確認してください。

   - DNS サーバ
   - NIS サーバ
   - WINS サーバ

   各サーバとの接続状態を確認する方法については，「シングルノード構成ユーザーズガイド」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，ネットワークの動作環境に問題がないかどうかを調査します。

   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。ネットワークポートのエラー情報を確認する方法については，「4.14 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態や動作状況を確認してください。

   - DHCP サーバ（HDI の場合）
   - 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態を確認する方法については，「シングルノード構成ユーザーズガイド」を参照してください。HVFP/HDI でのシステム構成およびネットワーク構成については，「シングルノード構成セットアップガイド」（HDI の場合は「セットアップガイド」）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，ノードの IP アドレスとの接続状態を確認します。

    ノード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 で障害が発生していないか確認します。

HCP へのアクセス障害の確認および回復方法については，「4.7 HCP へのアクセス障害を回復する」を参照してください。

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 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

次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。

- Backup Restore
- ファイルスナップショット
- Hitachi File Remote Replicator

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
ノード上のリソースのエラー状態	2.3
ファイルシステムのエラー状態（Backup Restore，Hitachi File Remote Replicator の場合）	2.4
差分格納デバイスのエラー状態	2.5
差分スナップショットのエラー状態（Hitachi File Remote Replicator の場合）	
ノード上のハードウェアの状態（Backup Restore の場合）	2.10
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）	2.14
HFRR ペアの状態（Hitachi File Remote Replicator の場合）	2.15

1.4 メッセージおよび関連マニュアルの参照

HVFP/HDI を運用中に出力されるメッセージや一部の関連マニュアルは，クラスタ構成の HVFP/HDI と共有しているため，シングルノード構成の HVFP/HDI で使用している用語と異なっていたり，使用していない機能について記載されていたりすることがあります。

- 次の用語は，シングルノード構成の HVFP/HDI で使用する用語に読み替えてください。

表 1-2 クラスタ構成の HVFP/HDI で使用している用語の読み替え

メッセージに出力される用語	シングルノード構成で使用する用語
固有 IP アドレス	IP アドレス
システム LU	システムディスク
デバイスファイル	内蔵ハードディスクまたはストレージシステムの LU
ユーザー LU	ユーザーディスク

- 「クラスタ，ノードまたはリソースグループ」や「クラスタまたはリソースグループ」など，「クラスタ」，「ノード」，「リソースグループ」を列挙している説明は，「リソースグループ」の説明だけが該当します。
- シングルノード構成の HVFP/HDI で使用しない機能であるため，「仮想 IP アドレス」，「ハートビートポート」，「フェールオーバー」や「フェールバック」に関する説明は無視してください。
- 「共有 LU」とは，システム設定情報が格納されているディスク領域のことです。
- HDI の場合，対処として「保守員に連絡してください。」と指示されたときは，「保守取扱説明書」を参照して対処してください。

2

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/HDI 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。

なお，HDI の場合，保守員と連携して実施するよう指示されている作業は，「保守取扱説明書」を参照して対処してください。

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

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は，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。

なお，HCP との通信で発生したエラーについてメッセージが表示された場合に，戻り値が表示されていたときは，HCP の管理者に戻り値を連絡し，原因と対処を問い合わせてください。戻り値が表示されていないときは，メッセージに従ってネットワークや外部サーバに問題がないことを確認してください。問題がない場合は HCP の管理者に HCP の状態を確認してください。

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。

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 ＜ X^1X^2 ＞＜ $Y^1Y^2Y^3Y^4Y^5$ ＞-＜ Z ＞

＜ X^1X^2 ＞

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

＜ $Y^1Y^2Y^3Y^4Y^5$ ＞

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

2.3 ノード上のリソースのエラー状態を確認する

ノード上のリソースのエラー状態やエラーが発生する要因を rgstatus コマンドで確認します。rgstatus コマンドを実行すると，ノード上のリソース状態とエラー情報が次の形式で表示されます。

＜リソース状態＞/＜エラー情報＞

リソース状態の確認

リソース状態に表示されている内容を確認します。リソース状態によって必要な対処が異なります。

表 2-1 リソース状態

リソース状態	説明
Online	正常に稼働しています。 エラー情報を確認してください。エラー情報については,「エラー情報の確認」を参照してください。
Online Pending	開始処理中です。
Offline	停止しています。
Offline Pending	停止処理中です。
Partial Online	一部のリソースが閉塞しています。 ハードウェアまたはソフトウェアに障害が発生しています。「リソース状態に「Partial Online」が表示されている場合の対処」に従って対処してください。

エラー情報の確認

ノード上のリソースのエラー情報には，「No error」または「OS error」が表示されます。表示されている内容によってエラー情報が表示される要因が異なります。

「No error」と表示されている場合

ノード上のリソースは正常です。

「OS error」と表示されている場合

ノード上のリソースの起動または停止に失敗しています。ハードウェア障害またはソフトウェア障害が要因の可能性があります。システムメッセージで KAQM35005-E, KAQM35007-E または KAQM35008-E が出力されているか確認し,「表 2-2 エラー情報が「OS error」の場合に確認するメッセージおよび対処」に従って対処してください。

リソース状態に「Partial Online」が表示されている場合の対処

リソース状態に「Partial Online」が表示されている場合は，次のとおり対処してください。

1. システムメッセージ KAQM35003-E の直前に出力されている KAQM35001-E の内容を確認し，閉塞しているリソースを特定します。

   障害リソースのタイプが「LVM_volume」または「Filesystem」の場合，障害が発生しているファイルシステムの状態を確認し，状態に応じて対処します。

   ファイルシステムの状態を確認する方法については「2.4 ファイルシステムのエラー状態を確認する」を参照してください。

2. ノードの状態を確認し，「Online」でない場合は，ノードを再起動します。

   ノードの状態を確認する方法およびノードを再起動する方法については，「シングルノード構成ユーザーズガイド」を参照してください。

   再起動しても回復しない場合は，ログファイルを取得して保守員に連絡してください。

エラー情報に「OS error」が表示されている場合の対処

表 2-2 エラー情報が「OS error」の場合に確認するメッセージおよび対処

メッセージ	直前のメッセージ	2 個前のメッセージ	対処
KAQM35005-E	—	—	ログファイルを取得して保守員に連絡してください。
KAQM35007-E	KAQM35009-E	—	KAQM35009-E の対処に従ってください。
	KAQM35003-E	KAQM35001-E	リソースの状態に「Partial Online」が表示されている場合と同様に対処してください。
			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してください。
		KAQM35002-E	KAQM35002-E の対処に従ってください。
	上記の KAQM35*nnn* 以外	—	ログファイルを取得して保守員に連絡してください。
KAQM35008-E	KAQM35010-E	—	KAQM35010-E の対処に従ってください。
	KAQM35004-E	—	KAQM35004-E の対処に従ってください。
	KAQM35006-E	—	ログファイルを取得して保守員に連絡してください。
	上記の KAQM35*nnn* 以外	—	ログファイルを取得して保守員に連絡してください。

（凡例）—：確認不要

2.4 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，システム管理者はファイルシステムウィンドウでファイルシステムのエラー状態を確認し，障害を回復します。

さらに，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）で確認して，要因を特定します。

2.5 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，＜ファイルシステム名＞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，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中です。

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，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

差分格納デバイスで使用中の容量の割合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。

「4.5.1 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。

「4.5.2 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）」のシングルノード構成の場合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中です。

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に使用しているボリュームグループへのアクセス障害が発生しています。ノード上のリソースが正常に稼働していない場合に表示されることもあります。

rgstatus コマンドでノード上のリソースの状態を確認してください。障害の要因がボリュームグループへのアクセス障害にあると保守員が判断した場合は，「4.5.3 内蔵ハードディスクまたはストレージシステムの LU にアクセス障害が発生した場合」の手順に従って対処してください。

「Offline」が表示された場合

ノード上のリソースが正常に稼働していません。

rgstatus コマンドでリソースの状態を確認して，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に使用しているボリュームグループへのアクセス障害が発生しています。

「4.5.3 内蔵ハードディスクまたはストレージシステムの LU にアクセス障害が発生した場合」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。

障害の要因を特定できない場合は，「3.1 ノード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。

2.6 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 分程度待ってから再度 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。

2.6.1 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，HVFP/HDI に設定されているノード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 HVFP/HDI 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/HDI 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。

  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。

2.6.2 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。

2.6.3 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。

2.7 サーバとの接続に問題がないか確認する

HVFP/HDI 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，ノードの接続に問題が発生していないかを確認します。

- DHCP サーバ（HDI の場合）※
- 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）

DHCP サーバを除いて，各サーバとノードとの接続状況は，Check for Errors ダイアログの List of RAS Information ページ（Server check 表示）で確認できます。ノードと各サーバの接続状態を確認する方法については，「付録 A. ネットワーク情報」を参照してください。DHCP サーバについては，ネットワーク管理者に確認を依頼してください。

注※：ノードとサーバの接続の問題を解決したら，必ずノードを再起動してください。

2.8 ホスト名の名前解決に問題がないか確認する

ノードにログインできる場合，システム管理者は，dig コマンドを使用して，ホスト名の名前解決に問題がないかを確認します。DHCP を使用している場合は，DDNS が正しく動作していることも確認してください。

ホスト名の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，対象のノードにログインします。
2. dig コマンドを実行して，ホスト名の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，ホスト名の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。

上記の手順で問題が特定できないときは，「4.7 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。

2.9 FC パスの状態を確認する

fpstatus コマンドで FC パスに問題が発生していないかを確認します。FC パスに障害が発生している場合は，「4.13 FC パスの障害を回復する」に従って対処してください。

2.10 ハードウェアの状態を確認する

ハードウェアに問題が発生していないかを確認します。GUI でハードウェアの状態を確認する方法については，「シングルノード構成ユーザーズガイド」を参照してください。コマンドを使用する場合は hwstatus 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，「4.17 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。

2.11 HCP との接続状態を確認する

HVFP/HDI 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。

2.12 ネットワークポートの通信を確認する

保守員からネットワークポートの通信の確認を依頼された場合，ネットワークポートに対して 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 2-3 ネットワーク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 2-3 ネットワークポートの通信確認ワークシート

	ネットワークポート
IP アドレス	
実行結果	

ネットワークポートの通信を確認する方法を次に示します。

1. Network & System Configuration ダイアログの List of Interfaces ページで，ネットワークポートの IP アドレスを確認し，ワークシートに記入します。
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ネットワークポートに対して 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 2-4 ネットワークポートの通信確認ワークシートの記入例

	ネットワークポート
IP アドレス	192.168.0.20
実行結果	×

   （凡例）×：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。

2.13 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)」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 サーバと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 サーバとの接続状態を確認する方法については，「シングルノード構成ユーザーズガイド」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」を参照してください。

2.14 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。

2.14.1 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。

2.14.2 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/HDI に添付されている Backup Restore の補足資料を参照してください。

2.14.3 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/HDI に添付されている Backup Restore の補足資料を参照してください。

2.15 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。ファイルシステム編集ダイアログまたは `syncexpand` コマンドで差分格納デバイスを拡張するか，スナップショット削除ダイアログまたは `syncdel` コマンド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。

3

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ったり，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/HDI の障害要因の解析には，次のログファイルが必要です。

- 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

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。

なお，HDI の場合は，障害情報を収集したあと，「保守取扱説明書」を参照して対処してください。

3.1 ノードのログファイルの採取方法

システム管理者は，GUI を利用して，ノード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，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. GUI 左上の設定メニューから，全ログデータのダウンロードを選択します。
2. 全ログデータのダウンロードダイアログでダウンロードボタンをクリックします。
3. 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。
   複数のログファイルが 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。
4. 全ログデータのダウンロードダイアログで OK ボタンをクリックします。

なお，ロググループごとにログファイルを一括ダウンロードする場合は，次の手順に従ってください。

1. 次のどちらかの方法で，Check for Errors ダイアログを表示させます。
   - GUI 左上の設定メニューから起動-エラーチェックを選択します。
   - ＜ホスト名＞ウィンドウの設定エリアで，エラーチェックを選択します。
2. Info. type ドロップダウンリストで Batch-download を選択してから，Display ボタンをクリックします。
3. 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。
4. 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。
5. ダウンロードダイアログの Close ボタンをクリックします。

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。

3.2 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。

なお，コマンドを使用する場合は，あらかじめ「シングルノード構成ユーザーズガイド」を参照して，コマンドを使用するための SSH の環境を設定してください。

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，ノードにログインします。

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 以上のユーザーディスク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：eth0.0010）

   -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 eth1 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 eth1 -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，ユーザーディスク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 M B となります。

3.3 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. ノードにログインします。
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, 全ログデータのダウンロードダイアログで全ログデータ（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，「3.1 ノードのログファイルの採取方法」を参照してください。

4

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，操作してください。

障害を回復する際にノードを操作したり，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。

なお，HDI の場合，保守員と連携して実施するよう指示されている作業は，「保守取扱説明書」を参照して対処してください。

- 4.13 FC パスの障害を回復する
- 4.14 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
- 4.15 リンク結合のエラー情報を確認して障害を回復する
- 4.16 データポートのエラー情報を確認して障害を回復する
- 4.17 ハードウェアの障害を回復する
- 4.18 モニター類を使用して障害を回復する
- 4.19 ほかのファイルサーバからのデータのインポートでの障害を回復する
- 4.20 Backup Restore の機能に関する障害を回復する
- 4.21 Hitachi File Remote Replicator の機能に関する障害を回復する
- 4.22 ファイルスナップショットのタイムアウトの障害を回復する

4.1 GUI の操作ミスを確認して操作し直す

GUI での設定ミスや操作ミスなど，GUI での操作に起因する障害が発生した場合，更新ボタンをクリックして情報を更新したあと，メッセージの指示に従って，操作し直してください。

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 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。

4.4 ファイルシステムの障害を回復する

ここでは，HVFP/HDI 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/HDI 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，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てから，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 の障害またはボリュームグループに割り当てられている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。

- ストレージシステム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，「4.4.4 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場合」に従って対処してください。出力されていない場合は，「4.4.2 OS 障害によってファイルシステムが閉塞している場合」に従って対処してください。

- ストレージシステムを使用していない場合

  OS の障害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。「4.4.2 OS 障害によってファイルシステムが閉塞している場合」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 パスの障害またはボリュームグループに割り当てられているディスクの障害によって，ファイルシステムが閉塞しています。FC パスに障害が発生していないか，ハードウェアウィンドウまたは `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，「4.13 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，「4.4.3 ボリュームグループに割り当てられているディスク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。

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「4.8 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ー HCP の両方に障害が発生した場合，「4.9 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」の手順で回復してください。

4.4.1 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。

注※：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。

4.4.2 OS 障害によってファイルシステムが閉塞している場合

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. 閉塞したファイルシステムを削除します。
2. ノードを再起動します。
3. `fscreate` コマンドでファイルシステムを再構築します。
4. `fsmount` コマンドで再構築したファイルシステムをマウントします。
5. 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。
6. 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では必ず「既存ディレクトリをそのまま使用」を選択してください。

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。

4.4.3 ボリュームグループに割り当てられているディスクの障害によってファイルシステムが閉塞している場合

作成されているボリュームグループの数に応じて，次のどちらかの方法で対処します。

(1) ボリュームグループが 1 つの場合

ファイルシステムおよびボリュームグループを削除します。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，ディスクの障害を取り除き，ノードの OS の再インストールとユーザーディスクの初期化を実施します。
2. システム設定情報とユーザーデータを回復します。
   - 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 から一括で回復します。「4.12 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。
   - HCP にデータをマイグレートしていない場合は，次の手順に従って対処してください。

   a. システム設定情報を回復します。
   b. 閉塞したファイルシステムを削除します。
   c. `vgrdelete` コマンドでボリュームグループを削除します。
   d. `vgrcreate` コマンドでボリュームグループを再作成します。
   e. ファイルシステムを作成します。
   f. 作成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。

(2) ボリュームグループが複数ある場合

障害が発生しているボリュームグループの状態を確認してから必要な対処を実施します。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. ストレージシステム内のボリュームグループに障害が発生した場合は，保守員と連携して，ディスクを交換します。
2. `vgrlist` コマンドで障害が発生しているボリュームグループとディスクを特定します。

   `Total size(GB)` に表示される内容によって，必要な手順が異なります。

   `Total size(GB)` に「-」と表示される場合は，次の手順に従って対処してください。

   a. 障害が発生したボリュームグループを使用するすべてのファイルシステムについて，作成されたすべての差分スナップショットのファイル共有を解除します。
   b. 障害が発生したボリュームグループを使用するすべてのファイルシステムについて，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。
   c. 障害が発生したボリュームグループを使用するすべてのファイルシステムについて，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。
   d. 障害が発生したボリュームグループを使用するすべてのファイルシステムを削除します。
   e. 内蔵ハードディスク内のボリュームグループに障害が発生した場合は，保守員と連携して，ディスクを交換します。
   f. `nasreboot` コマンドでノードを再起動します。
   g. `rgstatus` コマンドでノードの状態を確認します。

      「`Online/No Error`」が表示されない場合は，`-f` オプションを指定して `rgstop` コマンドを実行してください。
   h. `vgrdelete` コマンドで障害が発生したボリュームグループを削除します。

i. -f オプションを指定して rgstop コマンドを実行した場合は，rgstart コマンドを実行します。

j. vgrcreate コマンドでボリュームグループを作成します。

Total size(GB)に容量が表示される場合は，次の手順に従って対処してください。

a. --list オプションを指定して vgrrepair コマンドを実行します。
障害が発生したファイルシステムを記録してください。

b. 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，ファイル共有を解除します。

c. 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。

d. 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。

e. --list オプションを指定して vgrrepair コマンドを実行したときに，「List of unavailable file systems:」に表示されたファイルシステムを削除します。

f. 内蔵ハードディスクのボリュームグループに障害が発生した場合は，保守員と連携して，ディスクを交換します。

g. nasreboot コマンドでノードを再起動します。

h. vgrrepair コマンドでボリュームグループを修復します。

i. vgrexpand コマンドで追加する LU を指定して，ボリュームグループを拡張します。

3. ファイルシステムを削除した場合は，ファイルシステムとファイル共有を再作成します。

4. 差分スナップショットを使用する場合は，作成したファイルシステムに差分格納デバイスを再設定します。

5. ユーザーデータを回復します。

- HCP にデータをマイグレートしている場合は，arcrestore コマンドで HCP からユーザーデータを回復します。
- HCP にデータをマイグレートしていない場合は，ファイルシステムにバックアップデータを回復します。

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。

4.4.4 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場合

プールの容量不足によって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。ストレージシステムの管理者と連携し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。

2. ノードを再起動します。

4.4.5 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。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。

4.5 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。

4.5.1 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。ここでは，`Overflow` 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 `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。スナップショット全削除ダイアログまたは `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」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。

4.5.2 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」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。

4.5.3 内蔵ハードディスクまたはストレージシステムの LU にアクセス障害が発生した場合

内蔵ハードディスクまたはストレージシステムの LU 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

FC パスの障害を回復してください。「4.13 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，ユーザーディスク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 LU 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 LU 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. 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。
5. OS を再起動します。
6. 手順 2 で削除したファイルシステムを再構築します。
7. 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。
8. 差分格納デバイスを再設定します。
9. `lumapctl` コマンドを使用して，ユーザーディスク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. ノードを再起動します。

4.6 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。
   - 「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
     内蔵ハードディスクまたはストレージシステムの LU にアクセス障害が発生しているおそれがあります。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
     ノード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 LU（内蔵ハードディスクまたはストレージシステムの LU）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. OS を再起動します。
4. 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，「4.5.1 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「4.5.2 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。
   - 内蔵ハードディスクまたはストレージシステムの LU にアクセス障害が発生している場合
     「4.5.3 内蔵ハードディスクまたはストレージシステムの LU にアクセス障害が発生した場合」の手順に従って対処してください。

4.7 HCP へのアクセス障害を回復する

次のようなアクセス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

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/HDI 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. 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。また，リモートアクセスの環境（NAT，VPN およびプロキシサーバの設定）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。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，クライアント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。

4.8 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「4.8.1 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「4.8.2 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。

テープ装置にバックアップを取得している場合は，HCP からデータをリストアしたあとで，テープ装置のデータをリストアする必要があります。詳細については，「シングルノード構成ユーザーズガイド」を参照してください。

4.8.1 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/HDI 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 GUI で作成します。

   次のとおり指定してファイルシステムを作成してください。

- 障害が発生したファイルシステムと同じファイルシステム名を指定する
- 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回復されます。

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，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 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。

4.8.2 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/HDI 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 GUI で構築し，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と同じファイルシステム名を指定する
   - 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. arcreplimitset コマンドでファイルシステムのスタブ化閾値を 0GB 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。
   arcreplimitset --rest-size 0g --file-system ＜*ファイルシステム名*＞
3. arcrestore 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，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。

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 arcresidentpolicylist 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. arcresidentpolicyset 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。
   arcresidentpolicyset --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 arcresidentresult 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 em_alertfile 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 `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。

4.9 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/HDI 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/HDI 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. レプリカ HCP 側で運用を開始します。

7. プライマリー HCP が復旧します。
8. 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。
9. 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。
10. 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。
11. 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。

4.10 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/HDI 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/HDI 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 へ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。

4.11 システム設定情報を回復する

ここでは，ノードのシステムディスクで障害が発生し，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に，システム設定情報およびユーザーデータを HCP から一括で回復する手順については，「4.12 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。

なお，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。

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。
4. syslurestore コマンドを使用して，すべてのシステムディスクを回復します。

   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. 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。
6. 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。
7. 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。
8. 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。

4.12 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，ノード上のディスクに障害が発生し，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。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。

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
  - ファイルの作成日時が記録されるかどうか
- マイグレーション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，HFRR 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。

製品によって回復手順が異なります。HVFP の場合は「4.12.1 HVFP の場合」，HDI の場合は「4.12.2 HDI の場合」を参照してください。

4.12.1 HVFP の場合

HVFP でシステム設定情報およびユーザーデータを回復する手順を次に示します。保守員と連携して対処してください。

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，arcproxyset 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，arcsslctl 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ホスト名も--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。

6. 手順 1 で保守員がネットワーク構成を変更した場合は，構成を元に戻します。

7. HVFP に再ログインします。

   手順 5 で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。

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. 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. 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。

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。

4.12.2 HDI の場合

HDI でシステム設定情報およびユーザーデータを回復する方法について説明します。なお，回復にはコマンドを使用します。各コマンドを実行する前に，「コマンドリファレンス」を参照して使用方法を確認してください。

重要

- システム設定情報およびユーザーデータを回復する前に，システム設定ウィザードおよびサービス設定ウィザードを使用してセットアップを実施します（ファイルシステムおよび CIFS ユーザー認証の方式の設定を

除く)。「セットアップガイド」の「セットアップを実施する前に」および「システム回復用ワークシート」を参照して，必要な情報を事前に収集してください。

- サービス設定ウィザードで HCP の情報を設定すると，システム設定情報が HCP に定期的に保存されるように設定されます（デフォルトでは毎日 12:07)。回復が完了する前にシステム設定情報が HCP に保存されると，障害発生前のシステム設定情報が上書きされて回復できなくなります。このため，作業中にシステム設定情報が保存されないように，作業時間を調整してください。システム設定情報およびユーザーデータの回復が完了するまでに（手順 1 から手順 33 まで)，約 4 時間掛かります。デフォルト設定の場合，午前 8:00 までに作業を開始できないときは，12:30 以降に作業を開始してください。
- システム設定情報が HCP に保存される前に障害が発生した場合，ここに示す手順では障害を回復できません。HCP にデータがマイグレートされているときは，HDI を再セットアップしてから，arcrestore コマンドで HCP からユーザーデータを回復してください。セットアップ方法については，「セットアップガイド」を参照してください。

HDI でシステム設定情報およびユーザーデータを回復する手順を次に示します。

1. 管理コンソールから HDI にアクセスします。

   DHCP を使用する場合は，ネットワーク一覧の「その他のデバイス」で，HDI を示すアイコン（HDI-＜製品コード＞-＜製品番号＞）をクリックしてください。

   DHCP を使用しない場合は，WWW ブラウザーのアドレスバーに URL を指定してください。

   https://＜ HDI の IP アドレス＞/admin/

   なお，HDI の IP アドレスの初期設定値は 169.254.1.100 です。
2. ログイン画面でユーザー ID とパスワードを指定して，ログインをクリックします。

   次の情報を指定してください。

   - ユーザー ID：admin
   - パスワード：chang3me!
3. 初回ログイン時に表示されるログインパスワード変更ダイアログでパスワードを変更して，OK をクリックします。

   システム設定ウィザードが起動します。システム設定ウィザードは，GUI 左上の設定メニューから設定ウィザード-システム設定ウィザードを選択しても起動できます。
4. 1. イントロダクションページで次へをクリックします。
5. 2. ライセンスの設定ページでライセンスを設定し，次へをクリックします。
6. 3. 基本的な設定ページで情報を指定し，次へをクリックします。

重要 手順 5 で暗号化機能に対応するライセンス（Hitachi Basic Operating System File Extension for Entry with Data Encryption Feature）を設定した場合は，必ず「ローカルデータの暗号化」の右側のチェックボックスのチェックを外してください。チェックボックスを選択してユーザーデータを暗号化するよう設定すると，システム設定情報の回復に失敗するおそれがあります。手順 31 でシステム設定情報を回復することで，暗号化するかどうかの設定を障害発生前の状態に回復できます。

7. 4. 確認ページで表示された情報を確認し，チェックボックスを選択して適用をクリックします。

   5. 実行ページが表示され，システムのセットアップが実行されます。

   セットアップが完了したら，6. 完了ページが表示されます。

   DHCP を使用しない場合は，管理コンソールの IP アドレスを手順 6 で指定した IP アドレスと同じネットワークに設定してから，HDI および管理コンソールを，障害発生前に接続していたネットワークに接続し直してください。そのあと，以降の手順を実施してください。
8. 6. 完了ページで処理結果を確認して，メッセージに従って再ログインします。
9. ログイン画面でユーザー ID とパスワードを入力して，ログインをクリックします。

   サービス設定ウィザードが起動します。サービス設定ウィザードは，GUI 左上の設定メニューから設定ウィザード-サービス設定ウィザードを選択しても起動できます。
10. 1. イントロダクションページで次へをクリックします。

11. 2. HCP 設定ページでチェックボックスを選択し，情報を指定します。ノードと HCP の通信にプロキシサーバを使用する場合は，プロキシサーバの情報も指定します。
12. 接続テストをクリックします。
13. 次へをクリックします。

    3. リソース設定ページが表示されます。
14. 次へをクリックします。

重要 サービス設定ウィザードの 3. リソース設定ページでは，必ず何も指定しないで「次へ」をクリックしてください。ファイルシステムを作成すると，システム設定情報の回復に失敗するおそれがあります。手順 31 でシステム設定情報を回復することで，ファイルシステムおよび CIFS ユーザー認証の方式の設定を障害発生前の状態に回復できます。

    5. 確認ページが表示されます。
15. 5. 確認ページで表示された情報を確認し，チェックボックスを選択して適用をクリックします。

    6. 実行ページが表示され，サービスのセットアップが実行されます。

    セットアップが完了したら，7. 完了ページが表示されます。
16. 7. 完了ページで処理結果を確認して，完了をクリックします。
17. GUI 左上のダッシュボードタブを選択します。
18. ダッシュボードタブでシステム情報パネルの  をクリックします。
19. ＜ホスト名＞ウィンドウで設定エリアの「ソフトウェア更新」をクリックします。
20. システムソフトウェアインストールダイアログでインストールするソフトウェアのバージョンとチェックボックスを選択し，インストールをクリックします。

    インストール進捗画面が表示され，インストールが開始されます。

    最新ソフトウェアがインストールされていた場合は，ダイアログを閉じて，手順 24 に進んでください。
21. インストール結果を確認して，メッセージに従って再ログインします。
22. ログイン画面でユーザー ID とパスワードを入力して，ログインをクリックします。
23. ダッシュボードタブでシステム情報パネルの  をクリックします。
24. システム設定情報およびユーザーデータを回復するためのコマンドを使用できるように，SSH 環境を設定します。

    PuTTY などの通信ソフトウェアを管理コンソールにインストールしてください。また，鍵作成ツールで秘密鍵および公開鍵（OpenSSH 形式）を作成してください。なお，PuTTY はインストールメディアの次のフォルダに格納されています。

    ＜インストールメディアのドライブ＞:PuTTY¥＜ PuTTY のインストーラファイル＞

    コマンドを実行するときは，SSH 秘密鍵を使用して SSH アカウント（nasroot）で HDI にログインしてください。

    なお，この手順で作成した公開鍵および秘密鍵は，手順 31 でシステム設定情報およびユーザーデータを回復するまでの間，一時的に使用する鍵です。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，これらの鍵は不要となります。以降，この手順で作成した鍵を「公開鍵（一時利用）」および「秘密鍵（一時利用）」と表記します。
25. ＜ホスト名＞ウィンドウで設定エリアの「アクセスプロトコル設定」をクリックします。
26. Access Protocol Configuration ダイアログの List of Services ページで「SSH」を選択して，Modify Configuration をクリックします。
27. Public Key List ページで Add をクリックします。
28. Add Public Key ページで手順 24 で作成した公開鍵（一時利用）のファイルを指定して，Add をクリックします。

SSH アカウント（nasroot）に対して公開鍵（一時利用）が登録されます。

29. ファイルシステムウィンドウでファイルシステム総数に表示されている値を確認します。

30. 手順 28 で登録した公開鍵（一時利用）に対応する秘密鍵（一時利用）を使用し，nasroot でノードにログインします。

手順 29 で確認したファイルシステム総数が 1 以上の場合は，次のとおりコマンドを実行してください。なお，オプションの引数は，手順 6 でシステム設定ウィザードに指定した値と同じになるようにしてください。

DHCP を使用するとき

--host オプションを指定して singleinit コマンドを実行してください。

DHCP を使用しないとき

-a，-n および--host オプションを指定して singleinit コマンドを実行してください。

コマンドを実行するとノードが再起動します。再起動が完了してから，再度，nasroot でノードにログインしてください。

31. 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ホスト名も--system-name オプションで指定してください。

システム設定情報およびユーザーデータを回復すると，障害発生前の HDI に登録されていた公開鍵も復元され，手順 28 で登録した公開鍵（一時利用）は HDI から削除されます。公開鍵（一時利用）の削除に伴い，秘密鍵（一時利用）を使用した HDI へのログインはできなくなります。管理コンソールから公開鍵（一時利用）および秘密鍵（一時利用）を削除してください。以降の手順は，復元された公開鍵に対応する秘密鍵が保存されている管理コンソールから作業してください。

KAQM13187-E メッセージが出力された場合は，システム設定情報ファイルが HCP に保存される前に障害が発生しているため，セットアップ時と同じ手順で再設定してから arcrestore コマンドで HCP からユーザーデータを回復してください。セットアップ手順については，「セットアップガイド」を参照してください。

32. 管理コンソールの IP アドレスを，障害発生前の HDI の IP アドレスと同じネットワークに設定します。

33. 管理コンソールから HDI にアクセスします。

DHCP を使用する場合は，ネットワーク一覧の「その他のデバイス」で，HDI を示すアイコン（HDI-＜製品コード＞-＜製品番号＞）をクリックしてください。

DHCP を使用しない場合は，WWW ブラウザーのアドレスバーに URL を指定してください。

https://＜障害発生前の HDI の IP アドレス＞/admin/

34. 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，次のどれかの画面で確認します。

- 共有ウィンドウ
- ファイルシステムウィンドウ
- Check for Errors ダイアログの List of RAS Information ページ（List of messages 表示）

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。

35. 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。

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. SSH アカウント（nasroot）で HDI にログインします。
   手順 31 で HDI に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。
2. --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。
3. 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 FC パスの障害を回復する

ストレージシステムを使用している場合，FC パスに障害が発生したおそれがあるとき，システム管理者は fpstatus コマンドで FC パスの状態を確認し，障害を回復します。

4.13.1 片方のパスで「Error」が表示されている場合

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，ノードを再起動していない。

(c) FC パスに対応づけられたストレージシステムのホストグループに 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「4.13.5 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. ノード側の FC ポート（HostPort），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

   ノードを再起動します。
2. fpstatus コマンドで対象の FC パスの状態を確認します。

4.13.2 両方のパスで「Online (LU Error)」が表示されている場合

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，ストレージシステムの LU の障害を回復します。
2. fponline コマンドで対象の FC パスをオンラインにするか，または fpstatus コマンドで対象の FC パスの状態を確認します。

3. ノードを再起動します。
4. fpstatus コマンドで対象の FC パスの状態を確認します。

4.13.3 両方のパスで「Error」が表示されている場合

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，ノード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ストレージシステムの 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「4.13.5 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. ノード側の FC ポート（HostPort），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，次の手順に進みます。

   障害が発生していなかった場合

   ノードを再起動し，fpstatus コマンドで FC パスの状態が正しく表示されることを確認します。
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。

   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次の手順に進みます。
4. 保守員と連携して，ストレージシステムの LU の障害を回復します。
5. ノードを再起動します。
6. fpstatus コマンドで対象の FC パスの状態を確認します。

4.13.4 両方のパスで「Configuration Mismatch」が表示されている場合

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 の割り当てが，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. 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。
2. 対象のパスの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。
3. ノードを再起動します。
4. 対象の FC パスの状態を確認します。

4.13.5 両方のパスで「Unknown」が表示されている場合

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 ケーブルの状態を確認します。
4. 対象のパスのホストセキュリティを確認します。
5. 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 を割り当てます。
6. ノードを再起動します。
7. 対象の FC パスの状態を確認します。

4.13.6 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こと考えられます。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. ノードを再起動します。
3. fpstatus コマンドで対象の FC パスの状態を確認します。

4.13.7 片方のパスで「Configuration Mismatch」が表示されている場合

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，「4.13.1 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。

4.13.8 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，ノードの起動時に 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。
3. ノードを再起動します。

4.14 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。

ネットワークポートの IP アドレスの確認

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。

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。

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。

ネットワークポートのネゴシエーションモードの確認

ネットワーク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，ネットワーク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。

4.15 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。

4.15.1 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/HDI 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。

4.15.2 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，HVFP/HDI 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 HVFP/HDI 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。「4.15.1 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。

4.15.3 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。「4.15.1 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。

4.16 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。

4.16.1 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, HVFP/HDI 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/HDI 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。

4.16.2 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，HVFP/HDI 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 HVFP/HDI 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。

4.17 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，Ethernet インターフェースの障害については「4.14 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。

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。

4.18 モニター類を使用して障害を回復する

システム管理者は，障害によってシステムメッセージを確認できない場合に，システム導入時に準備したディスプレイおよびキーボードなどのモニター類を使用して障害を調査し，回復します。モニター類を使用して障害を回復する手順を次に示します。

1. モニター類をノードに接続し，ログインプロンプトが表示されるかどうか確認します。

   ログインプロンプトが表示されない場合は，まず，モニター類の電源が入っているか，モニター類がケーブルで正しく接続されているかなどを確認してください。

   「Copy dump file start:」と表示された場合は，10 分程度待ってから，ログインプロンプトが表示されるかどうか確認してください。

   ログインプロンプトが表示された場合は，システム管理やデータアクセスのために使用するポートに対して ping コマンドを実行してネットワークの状態を確認し，障害が発生している場合は回復してください。障害を回復する手順については「4.16 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。ネットワークに障害が発生していない場合は，手順 4 に進んでください。

   応答がない場合は，次の手順に進んでください。

2. ノードの MAINTENANCE ランプの表示を確認します。

   「00」以外が表示されている場合はエラーが発生しています。保守員に連絡してください。エラーが発生していない場合は次の手順に進んでください。

3. ノードの RESET スイッチを押してノードを再起動します。

   RESET スイッチは，SERVICE ランプスイッチと BUZZER STOP スイッチの間，または SERVICE ランプスイッチと MODE1 ランプの間にあります。ペーパークリップなどを使用して押してください。

   再起動は 10 分程度掛かります。再起動が完了するとログインプロンプトが表示されます。再起動が成功した場合は次の手順に進んでください。失敗した場合は保守員に連絡してください。

4. クライアントからノードのファイルシステムにアクセスできるかどうか確認します。

   アクセスできた場合は障害が回復しています。保守員にダンプ情報を回収するよう依頼してください。アクセスできなかった場合は保守員に連絡してください。

4.19 ほかのファイルサーバからのデータの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データを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。

4.19.1 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/HDI 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 コマンドで，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

ファイルインポートダイアログの接続テストボタンまたは datamigrateaccesstest コマンドで，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

ファイルインポートダイアログまたは datamigrateconflist コマンドで，設定内容に誤りがないか確認します。また，ファイルインポートダイアログの接続テストボタンまたは datamigrateaccesstest コマンドで，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。

4.19.2 HVFP/HDI で I/O 障害が発生した場合

HVFP/HDI 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 4-1 ほかのファイルサーバからのデータインポート時に HVFP/HDI 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。	4.13
ファイルシステムの障害	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。	4.4
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。	4.5

（凡例）－：該当しない

4.19.3 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，ファイルインポートウィンドウ，または--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，ファイルインポートウィンドウまたは datamigratestart コマンドで，インポート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/HDI 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/HDI 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。
3. 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。
4. 手順 3 で DST_NAME に指定したアカウントが未登録の場合，HVFP/HDI または外部サーバにアカウントを登録します。
5. マッピングファイルを HVFP/HDI 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。
6. HVFP/HDI 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。
7. ファイルインポートウィンドウまたは datamigratestart コマンドで，インポートの実行から再度実施します。

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 arcconfedit 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，ファイルインポートウィンドウまたは datamigratestart コマンドで，インポートの実行から再度実施してください。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 arcconfedit 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。

1. 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。

2. 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。

   ```
   [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。

3. 手順 2 で DST_NAME に指定したアカウントが未登録の場合，HVFP/HDI または外部サーバにアカウントを登録します。

4. 作成したマッピングファイルを HVFP/HDI 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。

5. HVFP/HDI 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。

6. ファイルインポートウィンドウまたは datamigratestart コマンドで，インポートの実行から再度実施します。

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 arcconfedit 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，ファイルインポートウィンドウまたは datamigratestart コマンドで，インポートの実行から再度実施してください。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 arcconfedit 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。

4.19.4 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，GUI や 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，再度インポートを実行してください。ファイルが不要な場合，ファイルインポートウィンドウで対象のタスクのインポートを再開し，オンデマンドでのインポートに変更を選択してインポート方法を変更するか，datamigrateconfadd 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。

4.19.5 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，ファイルインポートウィンドウまたは 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，ファイルインポートウィンドウから対象のタスクの設定を編

集するか，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。

4.19.6 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/HDI または外部サーバにアカウントを登録し，ファイルインポートウィンドウから対象のタスクの設定を編集するか，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。

4.20 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ったり，対処できなかったりした場合は，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。

4.20.1 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。

4.20.2 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/HDI に添付されている Backup Restore の補足資料を参照してください。
- /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。
- 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。

4.20.3 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。

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。

4.21 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。

4.21.1 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. ノードの状態を確認します。

   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，それぞれの対策手順に従って対処してください。

   HVFP/HDI 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

   「4.14 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

   「4.15 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

   「4.16 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。

4.21.2 サイト間で HFRR ペアの状態が一致していない場合

HVFP/HDI 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

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。

4.21.3 ノード上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

ノード上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. rgstatus コマンドで「Resource group status」を確認します。
   ノード上のリソースが正しく稼働していないことを確認してください。
2. russervice コマンドを実行して HFRR サービスを停止します。
   HFRR ペアの運用については，「シングルノード構成ユーザーズガイド」を参照してください。
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. russervice 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。

4.21.4 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。

4.21.5 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 でファイルシステムの容量を拡張する方法については，「シング

ルノード構成ユーザーズガイド」を参照してください。fsexpand コマンドでファイルシステムの容量を拡張することもできます。

2. 両サイトで russvrchk 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。

4.21.6 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 で HVFP/HDI のノードの時刻を設定する方法については,「シングルノード構成ユーザーズガイド」を参照してください。timeset コマンドで HVFP/HDI のノードの時刻を設定することもできます。

4.21.7 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 HFRR サービスが停止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。

4.21.8 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ノードを再起動したり 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。

4.21.9 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。

4.22 ファイルスナップショットのタイムアウトの障害を回復する

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。

A

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。

A.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。

A.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
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 A-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。 ＜ノード番号＞(＜ホスト名＞)　＜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 ゲートウェイの IP アドレスが出力されます。 Flags 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。

出力行	出力内容
	U 通常の経路設定であることを示します。 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。 G ゲートウェイが設定されていることを示します。 R 回復される動的な経路の設定であることを示します。 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。 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。 A addrconf によって設定されていることを示します。 C キャッシュのエントリーに設定されていることを示します。 ! 拒否する経路設定であることを示します。 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。 Iface ポート名が出力されます。

A.3 log_ifconfig ファイル

log_ifconfig ファイルの出力例を次に示します。

```
lo        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)

mng0      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

mng0:1    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
          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 A-2 log_ifconfig ファイルに出力される情報

出力項目	出力内容
lo mng ＜番号＞ pm ＜番号＞ agr ＜番号＞ rdn ＜番号＞ eth ＜番号＞ xgbe ＜番号＞	ポート名が出力されます。 ループバックの場合は「lo」と表示されます。 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。 また，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。 0 log_ifconfig ファイルを出力したノードの 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 アドレスのスコープが出力されます。
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ーアドレスが出力されます。

A.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 A-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 A-4
Checking NIS configuration...	NIS サーバとの接続状態が出力されます。	表 A-5
Checking NTP configuration...	NTP サーバとの接続状態が出力されます。	表 A-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 A-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す。	表 A-8

メッセージ	説明	参照先
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す。	表 A-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ます。	表 A-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 A-4 DNS サーバとの接続状態として出力される情報～表 A-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 A-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. No respond servers: ＜HVFP/HDI に設定した DNS サーバの IP アドレス＞	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。 ・ ノードと使用する DNS サーバとの経路上の機器が正常に稼働しているか ・ 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 A-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: ＜HVFP/HDI に設定した NIS サーバの名称または IP アドレス※＞	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。 ・ ノードと使用する NIS サーバとの経路上の機器が正常に稼働しているか ・ 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

出力内容	説明	対処
Warning: The specified NIS server name cannot be resolved. NIS server name: ＜HVFP/HDI に設定した NIS サーバの名称＞	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: ＜HVFP/HDI に設定した NIS サーバの NIS ドメイン名＞	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 A-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。
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: ＜HVFP/HDI に設定した NTP サーバの名称または IP アドレス＞	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。 ・ 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 ・ 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: ＜HVFP/HDI に設定した NTP サーバの名称＞	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 A-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。

出力内容	説明	対処
Error: LDAP server(＜HVFP/HDI に設定した LDAP サーバの IP アドレス＞:＜ポート番号＞) has not been connected.	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。 • 使用する LDAP サーバとノードとの経路上の機器が正常に稼働しているか • 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(＜HVFP/HDI 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.	設定した LDAP サーバとノード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(＜HVFP/HDI 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 size limitation occurred.	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トリー数が制限されているおそれがあります。	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。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.	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。ノードの 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 A-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	ローカル認証を使用しています。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: ＜HVFP/HDI に設定した認証サーバの名称＞	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。 • ノードと使用する 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 • 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

出力内容	説明	対処
Error: timeout. Server: ＜HVFP/HDI に設定した認証サーバの名称＞	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。 ・ ノードと使用する 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 ・ 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: ＜HVFP/HDI 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: ＜HVFP/HDI 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。
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 A-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: ＜HVFP/HDI に設定した KDC サーバの名称＞	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。 ・ ノードと使用する KDC サーバとの経路上の機器が正常に稼働しているか ・ 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: ＜HVFP/HDI に設定した KDC サーバの名称＞	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。 ・ ノードと使用する KDC サーバとの経路上の機器が正常に稼働しているか ・ 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: ＜HVFP/HDI 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。

出力内容	説明	対処
Error: ＜エラー要因＞. Server: ＜HVFP/HDI 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 A-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.	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。 • 使用する LDAP サーバとノードとの経路上の機器が正常に稼働しているか • 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.	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。 • 使用する LDAP サーバとノードとの経路上の機器が正常に稼働しているか • 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 HVFP/HDI 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 HVFP/HDI 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 HVFP/HDI 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.	HVFP/HDI に設定した次のどちらかの情報に誤りがあります。 • ユーザーマッピングアカウントを追加する識別名	Access Protocol Configuration ダイアログの CIFS Service Management ページ（Setting Type：User mapping）で，それ

出力内容	説明	対処
	• LDAP サーバのルート識別名	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.	HVFP/HDI 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。
Error: LDAP server root DN or LDAP administrator DN or LDAP administrator password is invalid.	HVFP/HDI 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=sambaUnixIdPool 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。 • 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=sambaUnixIdPool 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.	ノードの 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.	ノードの OS に障害が発生したため，/enas/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。

B

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/HDI 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，HVFP/HDI のネットワーク設定に問題があるために HVFP/HDI 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。

B.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を確認して，HVFP/HDI 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/HDI 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/HDI 以外のマシンと通信でき，HVFP/HDI とだけ通信できないことを確認します。HVFP/HDI 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。

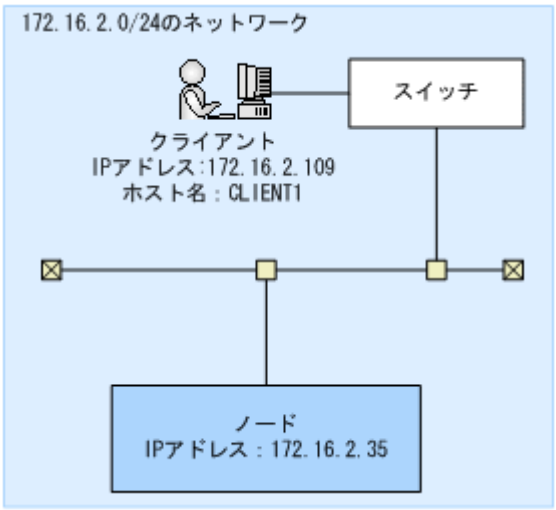
   リンクダウンのメッセージが出力されていた場合，保守員に連絡してください。

B.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を確認する前に，HVFP/HDI 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。

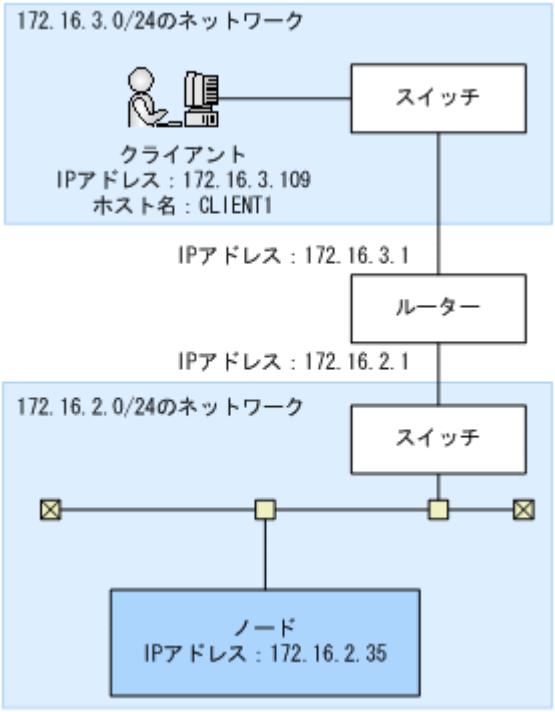
HVFP/HDI とクライアントが同一ネットワークに属している場合の例を次の図に示します。

図 B-1 HVFP/HDI 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/HDI 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 B-2 HVFP/HDI 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



B.2.1 ネットワーク内での通信を確認する

HVFP/HDI 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/HDI 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。

1. 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「B.3.1 IP アドレス，ネットマスクの確認」および「B.3.2 VLAN ID の確認」を参照してください。
2. 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「B.3.3 MTU 値の確認」を参照してください。

B.2.2 異なるネットワーク間の通信を確認する

HVFP/HDI 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/HDI 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「B.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。

B.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。

B.3.1 IP アドレス，ネットマスクの確認

HVFP/HDI 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/HDI

Network & System Configuration ダイアログの List of Interfaces ページで IP アドレスおよび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/HDI 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。

B.3.2 VLAN ID の確認

VLAN を設定している場合は，HVFP/HDI，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/HDI

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/HDI 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/HDI，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。

B.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/HDI，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/HDI

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/HDI 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/HDI 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/HDI 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。

B.3.4 ルーティングの確認

HVFP/HDI，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/HDI

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/HDI 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/HDI 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/HDI，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。

- ノードの再起動
- 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 B-2 HVFP/HDI 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
[IPv4]
Target          Netmask         Gateway         Method Type    MSS   Iface
CLIENT1         -               172.16.2.1      Allow  host    -     eth0
default         0.0.0.0         10.213.16.10    Allow  default -     mng0
```

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
[IPv4]
Target          Netmask         Gateway         Flags   MSS   Iface
172.16.3.109    255.255.255.255 172.16.2.1      UGH     -     eth0
172.16.2.0      255.255.255.0   0.0.0.0         U       -     eth0
10.0.0.0        255.255.255.0   0.0.0.0         U       -     pm0
```

```
10.213.16.0     255.255.255.0   0.0.0.0         U       -     mng0
default         0.0.0.0         10.213.16.10    UG      -     mng0

[IPv6]
Target                    Gateway                 Flags Iface
::1/128                   ::                      Un    lo
fe80::210:18ff:fe75:5780/128 ::                        Un    lo
fe80::210:18ff:fe75:5780/128 ::                        Un    lo
fe80::862b:2bff:fe25:bcc7/128 ::                        Un    lo
fe80::862b:2bff:fe25:bcc7/128 ::                        Un    lo
fe80::/64                 ::                      U     mng0
fe80::/64                 ::                      U     mng0
fe80::/64                 ::                      U     eth0
fe80::/64                 ::                      U     eth0
ff00::/8                  ::                      U     mng0
ff00::/8                  ::                      U     mng0
ff00::/8                  ::                      U     eth0
ff00::/8                  ::                      U     eth0
::/0                      ::                      !n    lo
```

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ノードを再起動すると，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
[IPv4]
Target          Netmask         Gateway         Method Type    MSS
Iface
CLIENT1         -               172.16.2.1      Allow  host    -     eth0
default         0.0.0.0         10.213.16.10    Allow  default -     mng0
```

```
$ sudo routelist -l
[IPv4]
Target          Netmask         Gateway         Flags   MSS   Iface
172.16.2.0      255.255.255.0   0.0.0.0         U       -     eth0
10.0.0.0        255.255.255.0   0.0.0.0         U       -     pm0
10.213.16.0     255.255.255.0   0.0.0.0         U       -     mng0
default         0.0.0.0         10.213.16.10    UG      -     mng0

[IPv6]
Target                  Gateway                 Flags Iface
::1/128                 ::                      Un    lo
fe80::210:18ff:fe75:5780/128 ::                      Un    lo
fe80::210:18ff:fe75:5780/128 ::                      Un    lo
fe80::862b:2bff:fe25:bcc7/128 ::                      Un    lo
fe80::862b:2bff:fe25:bcc7/128 ::                      Un    lo
fe80::/64               ::                      U     mng0
fe80::/64               ::                      U     mng0
fe80::/64               ::                      U     eth0
fe80::/64               ::                      U     eth0
ff00::/8                ::                      U     mng0
ff00::/8                ::                      U     mng0
ff00::/8                ::                      U     eth0
ff00::/8                ::                      U     eth0
::/0                    ::                      !n    lo
```

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 eth0
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 eth0
```

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
[IPv4]
Target          Netmask         Gateway         Method Type    MSS
Iface
default         0.0.0.0         10.213.16.10    Allow  default -     mng0
```

```
$ sudo routelist -l
[IPv4]
Target          Netmask         Gateway         Flags   MSS   Iface
172.16.3.109    255.255.255.255 172.16.2.1      UGH     -     eth0
172.16.2.0      255.255.255.0   0.0.0.0         U       -     eth0
10.0.0.0        255.255.255.0   0.0.0.0         U       -     pm0
10.213.16.0     255.255.255.0   0.0.0.0         U       -     mng0
default         0.0.0.0         10.213.16.10    UG      -     mng0

[IPv6]
Target                  Gateway                 Flags Iface
::1/128                 ::                      Un    lo
fe80::210:18ff:fe75:5780/128 ::                      Un    lo
fe80::210:18ff:fe75:5780/128 ::                      Un    lo
fe80::862b:2bff:fe25:bcc7/128 ::                      Un    lo
fe80::862b:2bff:fe25:bcc7/128 ::                      Un    lo
fe80::/64               ::                      U     mng0
fe80::/64               ::                      U     mng0
fe80::/64               ::                      U     eth0
fe80::/64               ::                      U     eth0
ff00::/8                ::                      U     mng0
ff00::/8                ::                      U     mng0
ff00::/8                ::                      U     eth0
ff00::/8                ::                      U     eth0
::/0                    ::                      !n    lo
```

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：ノードの 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 eth0
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 nasping 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/HDI 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。

B.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。

B.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。

B.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/HDI，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/HDI 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/HDI，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
```

```
10.0.0.0        0.0.0.0         255.255.255.0   U         0 0          0 pm0
192.168.0.0     0.0.0.0         255.255.255.0   U         0 0          0
eth0-br
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」が出力されます。HVFP/HDI 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。

B.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 nastraceroute -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  * * *
$
```

nastraceroute 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確認し，必要に応じて設定を変更します。

C

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。

C.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。

C.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,cccccccc,dddd,eeeeeeee,ffffffff,gggggggg

*** Pair statistical information ***
Date,Pair,Copy request totals,Copy beginning totals,Copy data size
MM DD hh:mm:ss,hh...hh,iiiiiiii,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 C-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/HDI 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みます。
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。

表 C-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みます。
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。

D

トラブルシューティング事例

GUI，コマンド，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。

D.1 GUI に関するトラブルシューティング事例

GUI の操作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 D-1 GUI に関するトラブルシューティング事例

問題発生個所	問題点	要因	対処
全般	Firefox で GUI を使用したとき，ログイン画面でキャンセルボタンをクリックしても画面が閉じない。	Firefox のウィンドウ制御によって発生することがあります。HVFP/HDI の障害ではありません。	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。
	GUI の表示がぼやける。	画面描画の制御によって発生することがあります。HVFP/HDI の障害ではありません。	ウィンドウを閉じ，再度 GUI にログインしてください。
	GUI の表示が処理中の状態から遷移しないため，操作できない。	管理コンソールの制御によって発生することがあります。ノードに処理要求が届いていないため，実行した操作が正常に終了していません。	GUI にログインし直してから，再度実行してください。
	DHCP を使用して HDI のネットワーク情報を設定しているとき，GUI を使用できない。	次の要因が考えられます。 ・ ノードの再起動や dhcpreload コマンドが実行されたため，IP アドレスが変更された可能性があります。 ・ DHCP サーバとの接続で障害が発生したため，IP アドレスが設定されていない可能性があります。	・ WWW ブラウザーのアドレスバーで，ホスト名を指定してください。 ・ ノードの IP アドレスに 169.254.1.100，ネットマスクに 255.255.0.0 が暫定的に設定されている可能性があります。169.254.1.100 に接続できるように設定したコンピュータをノードに接続させ，IP アドレスに 169.254.1.100 を指定してノードにアクセスできるかどうかを確認してください。アクセスできた場合，DHCP サーバとの接続に問題があります。ネットワーク管理者に対処を依頼してください。対処が完了したら，ノードを再起動してください。
	UPnP を使用するとき，管理コンソールのネットワーク一覧に HDI を示すアイコンが表示されない。	次の要因が考えられます。 ・ HDI のノードの電源が入っていない。 ・ 管理コンソールで UPnP を使用できるように設定されていない。 ・ ノードと管理コンソールを接続するネットワークに障害が発生している。	次のとおり対処してください。 1. ノードの電源が入っていることを確認します。 2. 管理コンソールで UPnP を使用できるように設定されていることを確認します。 UPnP を使用するときに必要な管理コンソールの設定については，「セットアップガイド」を参照してください。 3. ネットワークの動作環境を確認します。 ノードと管理コンソールを接続するネットワークの構成や動作環境に問題がないかどうかを確認してください。また，DHCP サーバとの接続状態や動作状況も確認してください。

問題発生個所	問題点	要因	対処
			4. nasreboot コマンドでノードを再起動します。 コマンドが使用できない場合は，ノードの電源を遮断して OS を強制停止させたあと，再度電源を投入して OS を起動してください。
	UPnP を使用するとき，HDI を示すアイコンをクリックしたり，アイコンを右クリックして表示される「デバイスの Web ページの表示」を選択したりしても，GUI が起動しない。	管理コンソールの OS が Windows 8 または Windows Server 2012 の場合，HDI のノードと管理コンソールの間での https 通信が停止されたことによって発生することがあります。	HDI を示すアイコンのプロパティ画面にある「デバイスの Web ページ」に表示されているアドレスをクリックしてください。
システム設定ウィザード	システム設定ウィザードを実行したあと，しばらく待っても画面が再表示されない。	システム管理に使用する IP アドレスを変更する処理でエラーが発生したおそれがあります。	変更前の IP アドレスを使用して再ログインし，入力値を見直して再度実行してください。変更前の IP アドレスを使用しても画面が表示されない場合は，保守員に連絡してください。
	システム設定ウィザードを実行してログインし直したが，設定内容が反映されていない。	システム設定ウィザードでの実行処理中にエラーが発生したおそれがあります。	入力値を見直し，再度実行してください。

D.2 コマンドに関するトラブルシューティング事例

コマンドの操作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 D-2 コマンドに関するトラブルシューティング事例

問題点	要因	対処
DHCP を使用して HDI のネットワーク情報を設定しているとき，ノードにログインできない。	次の要因が考えられます。 ・ ノードの再起動や dhcpreload コマンドが実行されたため，IP アドレスが変更された可能性があります。 ・ DHCP サーバとの接続で障害が発生したため，IP アドレスが設定されていない可能性があります。	・ ホスト名を指定してノードにログインしてください。 ・ ノードの IP アドレスに 169.254.1.100，ネットマスクに 255.255.0.0 が暫定的に設定されている可能性があります。169.254.1.100 に接続できるように設定したコンピュータをノードに接続させ，IP アドレスに 169.254.1.100 を指定してノードにログインできるかどうかを確認してください。ログインできた場合，DHCP サーバとの接続に問題があります。ネットワーク管理者に対処を依頼してください。対処が完了したら，ノードを再起動してください。

D.3 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 D-3 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。	• 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/HDI を連携している場合, 保管期間は HVFP/HDI の WORM 機能で設定してください。 • HVFP/HDI 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。	• 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。
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。インポート完了後に再度マイグレートしてください。

問題点	要因と対処
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て，オンデマンドでのインポートに変更されます。マイグレーション完了後にすべてのファイルのインポートが再開します。
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/HDI 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/HDI 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/HDI 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。	• HVFP/HDI 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 を再起動していないおそれがあります。 • HCP と HVFP/HDI 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，サービス設定ウィザードの 2. 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。	• 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，arcconfedit 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。	• 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。 • 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，転送速度の下限値を見直してください。 • HCP，HVFP/HDI 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。

問題点	要因と対処
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。
ローカルデータの暗号化に使用する共通鍵を HCP から取得できなくなり，ユーザーデータを使用できない。	HCP へのアクセス障害が発生しています。KAQM05258-E～KAQM05264-E のどれかのメッセージが出力されるため，メッセージに従って対処してください。 encdisplaykey コマンドで表示した鍵をシステム外の記録媒体に保存している場合は，HCP へのアクセス障害の回復に時間が掛かる際に，encrecoverkey コマンドで，暗号化に使用する共通鍵を一時的に復旧できます。ただし，暗号化に使用する共通鍵を復旧しても，HCP へのアクセス障害を回復するまでスタブファイルは使用できません。

D.4 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

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 D-4 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

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。	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。 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/HDI 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。 スキャンサーバでの設定が完了したあと，HVFP/HDI で再度リアルタイムスキャンを有効にしてください。
List of Scanner Servers ページの Server status に「Blocked (Time-out)」と表示される。	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。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。