

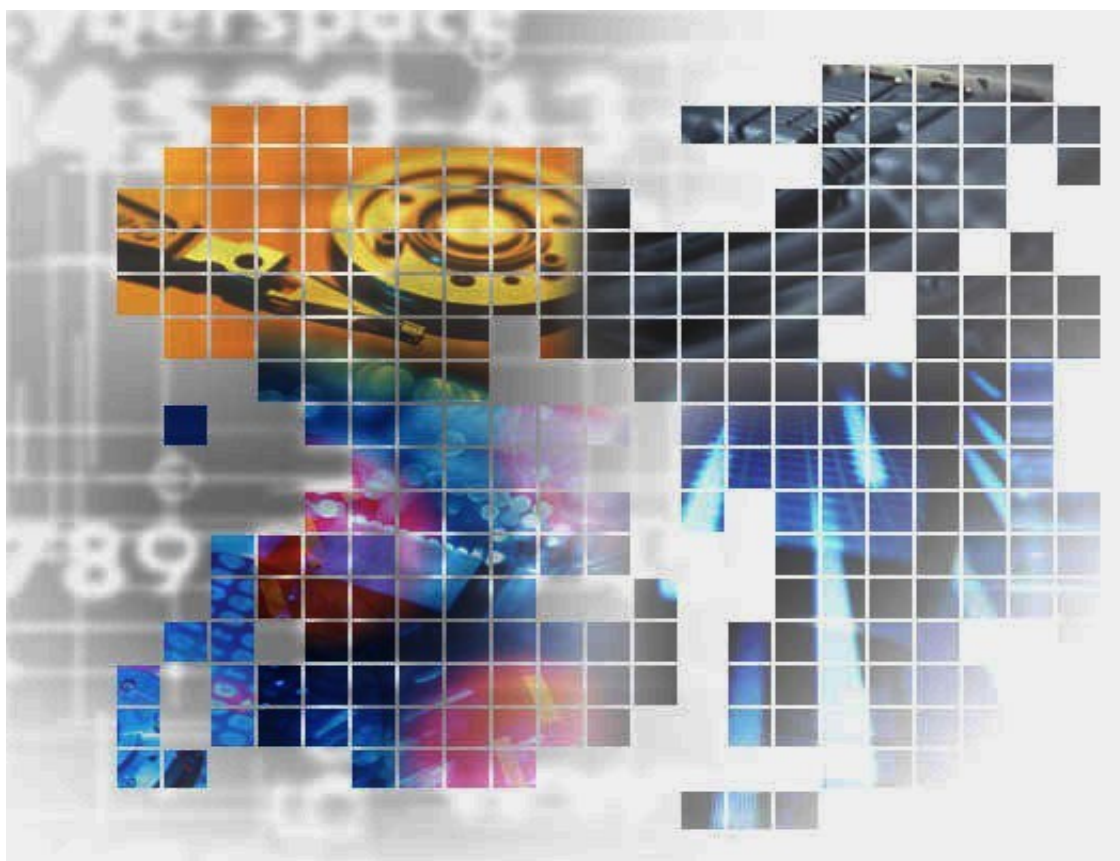
iStorage

Empowered by Innovation

NEC

iStorage HS3/HS8 シリーズ iStorage HS Virtual Appliance

構成設計の手引



IH2404-1-B

輸出する際の注意事項

本製品（ソフトウェアを含む）は、外国為替及び外国貿易法で規定される規制貨物（または役務）に該当することがあります。

その場合、日本国外へ輸出する場合には日本国政府の輸出許可が必要です。

なお、輸出許可申請手続きにあたり資料等が必要な場合には、お買い上げの販売店またはお近くの当社営業拠点にご相談ください。

Copyright © 2026 NEC Corporation. All rights reserved.

このドキュメントの情報は、現状有姿で提供され、予告なしに変更されることがあります。NEC Corporation およびその関連会社は、このドキュメントに誤りがないことの保証は致しかねます。

HYDRAsstor、DataRedux、Distributed Resilient Data (DRD)、ESMPRO は NEC Corporation の日本およびその他の国における登録商標または商標です。

Cohesity、Veritas、Cohesity ロゴ、Veritas ロゴ、Veritas Alta、Cohesity Alta、NetBackup は、Cohesity Inc またはその関連会社の米国およびその他の国における商標または登録商標です。

Commvault は、Commvault Systems, Inc.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。IBM および IBM Spectrum Protect は、IBM 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。

EMC、EMC ロゴおよび NetWorker は、Dell EMC の登録商標または商標です。

Data Protector は、Micro Focus International plc の登録商標または商標です。

UNIX は、The Open Group の米国ならびにその他の国における登録商標です。

Microsoft、Windows、Windows Server、MS-DOS、Active Directory は、米国 Microsoft Corporation の米国およびその他の国における商標または登録商標です。

Linux は、Linus Torvalds 氏の米国およびその他の国における商標または登録商標です。

Ethernet は、米国 XEROX 社の登録商標です。

Intel Xeon は、米国およびその他の国における Intel Corporation またはその子会社の商標または登録商標です。

その他、本通知に登場する会社名、製品名は一般に各社の登録商標または商標です。

iStorage HS シリーズについて

iStorage HS シリーズには、バックアップ/アーカイブ用途の iStorage HS3/HS8/HS Virtual Appliance およびアーカイブ用途の iStorage HS6 があります。

- **iStorage HS3/HS8**

NEC 独自のグリッド・ストレージ技術によるシステムの柔軟な拡張性、分散冗長配置技術による高い信頼性、最先端の重複排除技術による高いデータ圧縮性を持つディスクストレージです。

搭載する重複排除エンジンは、最も効率よく重複を検出できる可変長の知的ブロック分割方式を採用しています。

これにより、複数世代のバックアップデータを効率的に格納し、テープ並みの容量単価を実現した製品です。

- **iStorage HS6**

iStorage HS3/HS8 のコア技術を継承し、システムの柔軟な拡張性、分散冗長配置技術による高い信頼性、および重複排除機能を備えたディスクストレージです。

搭載する重複排除エンジンは、リソースの消費が少ない固定長分割方式を採用しています。これにより入出力処理への影響を抑え低価格を実現しています。

- **iStorage HS Virtual Appliance**

iStorage HS8/HS3 で培われたコア技術をベースとした iStorage HS シリーズの仮想アプライアンス製品です。

一般的なサーバ上の仮想化環境で動作するため、サーバリソースの有効活用を行い、消費電力や運用管理コスト低減を図ることができます。また、すばやく導入することが可能なため、ビジネスや IT 環境の変化に柔軟に対応できます。

iStorage HS Virtual Appliance を使用する場合は、はじめに「iStorage HS Virtual Appliance 導入構成ガイド」をお読みください。

本書について

本書は、ユーザの当面のまたは将来的なデータバックアップおよびデータストレージに関する要求に基づいた各種 iStorage HS 製品構成の設計方法について説明しています。本書は各構成例に必要な製品仕様についても説明しています。詳しい設定内容については「ユーザズガイド」を参照してください。

2026年 9月 初 版

備考

- (1) 本書は、iStorage HS3/iStorage HS8のシステムバージョン7.0.0以降、iStorage HS VirtualApplianceのシステムバージョン6.0.0以降に対応しています。
- (2) 本書では、特にご注意いただく内容を以下で示しております。

シンボル	説明
Note	説明対象の追加情報です。

目次

第1章	製品概要	1
第2章	配備計画	3
Step 1.	設置場所の計画	5
	製品モデルの仕様	5
	増設用製品オプション仕様	12
	製品の構成	13
Step 2.	ネットワークの計画	15
	推奨ネットワークトポロジ	15
	代替ネットワークトポロジ	16
	バックアップネットワークの冗長性	17
	複数のネットワークとの接続	20
	外部ネットワーク通信のフィルタリング設計	21
	アクセラレータノード機能クラスタのためのネットワーク設計	23
	レプリケーション用ネットワークの設計	25
	レプリケーション用ネットワークの接続（スケールアウトモデルの場合）	31
	レプリケーション用ネットワークの接続（シングルノードモデルの場合）	35
Step 3.	ファイルシステムの作成	38
	ファイルシステムの計画	38
	マーカーフィルタリング	40
	WORM (Write Once Read Many)	41
	パリティ	45
	ファイルシステムのエクスポートタイプ	47
	CIFS の認証方式	48
	ファイルシステム参照制限	50
Step 4.	メール通報の設定	51
	イベントレポート	51
	システムレポート	52
Step 5.	NTP サーバの計画	53
	NTP サーバの構成例	53
	Windows サーバを NTP サーバにする場合	55
Step 6.	領域解放の計画	59
Step 7.	ハードウェア障害への対策	63
	アクセラレータノード機能クラスタ	65
Step 8.	レプリケーションの計画	67
	レプリケーションジョブの運用計画	70
	CLI を利用したレプリケーションジョブの運用計画	71
	双方向レプリケーションと領域解放	72
	初期レプリケーションへの計画	73
	レプリケーション負荷の推奨値	74
第3章	システム構成の変更	75
	アクセラレータノード機能を持つノード間の負荷分散	75
	ノードの追加と削除	77
	ハードウェア混在環境でのデータの分散配置	78
第4章	システムの監視	81
	容量の監視	81
	本製品にとっての「容量」とは	81
	重複排除技術（DataRedux）	82
	データ圧縮率	83

GUI を使用して容量を監視するには.....	84
新しいデータ用の容量の見積もり	86
容量予測と容量拡張	88
付録 A ソフトウェア諸元一覧	90
付録 B 電源制御ソフトウェアの設定.....	92
設定手順のフローチャート.....	93
電源制御ソフトウェアの設定手順.....	94
Step 1. IP アドレス確認 (HS3 シリーズ)	94
Step 2. ノード名の設定 (HS3 シリーズ)	96
Step 3. 電源制御端末の設定 (HS3 シリーズ)	97
Step 4. IP アドレス確認 (HS8 シリーズ)	98
Step 5. ノード名の設定 (HS8 シリーズ)	100
Step 6. 電源制御端末の設定 (HS8 シリーズ)	101
Step 7. 電源装置のディスク保護時間の設定.....	102
注意事項	103
索 引	108
付録 C オペレーティングシステムの設定	
付録 D バックアップソフトウェアの設定	

第1章 製品概要

本製品は、ユーザの既存の IT バックアップインフラストラクチャに統合されるディスクベースのデータ保護プラットフォームです。また、バックアップおよびリカバリの性能や信頼性を改善し、画期的なデータ圧縮技術によって、手頃な価格でディスクベースのデータストレージの提供を可能にしました。このデータ圧縮機能は、システム構成の変更前後やシステムのアップグレード後も有効性を失いません。

本製品は、複数のディスク領域全体を有効容量とする、巨大な仮想ディスクとして利用できます。NFS(Network Filesystem)や CIFS(Common Internet Filesystem)ネットワークインタフェース経由で、お客様のバックアップ/リストアシステムから本製品により多くのデータを送信できるという利点があります。また、より低いディスク容量コストで、より高いレベルの冗長性を実現します。本製品は、長期的に必要なストレージ領域を 95%圧縮できます。この結果、一般的に 20:1 の圧縮率を実現できます。

本製品は、標準的なディスクや仮想テープライブラリ(VTL)をベースとするシステムに代わる、信頼性、管理容易性、拡張性に優れたバックアップ/リストアシステムを提供します。

容量/性能の動的拡大

本製品を使用すると、性能とディスク容量の両方を個別に拡張し、アプリケーション要件を満たすことができます。性能用のアクセラレータノード機能を持つノードと容量用のストレージノード機能を持つノードを組み込むことで、従来のコストのかかる「フォークリフト型アップグレード」が不要になります。また、ノードを論理的なプールに追加して管理することにより、ストレージ資源の分断化を抑えることができます。

領域解放機能

本製品の領域解放処理では、保持期間の切れたバックアップデータなどがファイルシステムから削除された後、使用可能な領域を回復できます。本製品では DataRedux（詳細は「[第4章 システムの監視](#)」の「[重複排除技術 \(DataRedux\)](#)」を参照）により、格納されるデータ量を節約するため、格納しようとするデータの中にすでに格納されているデータと同じデータパターンが存在するときは、それが異なるファイルのデータであっても、そのデータパターンは実際には格納されず複数のファイルから論理的に共用されます。削除するファイルが含むデータが、削除されない別のファイルによって使用されている場合は、そのデータは削除されません。領域解放後は、グラフィカルユーザインタフェース(Graphical User Interface: GUI)で表示される容量画面で使用可能な容量の割合を確認できます。

管理インタフェース

本製品のグラフィカルユーザインタフェースを使用すると、システムの機能にすばやく簡単にアクセスできます。このブラウザベースの GUI で実行できる操作の概要は、「ユーザーズガイド」の「第 2 章 グラフィカルユーザインタフェース(GUI)の概要」を参照してください。

第2章 配備計画

本製品を配備する前に、業界トップのストレージ機能と性能を最大限活用するために、慎重に計画を立てる必要があります。

本製品を初めて使用するシステム管理者向けの一般的な配備シナリオの手順を以下に示します。これらの手順を実行すると、本製品の使用を開始できます。

Step 1. 設置場所の計画

ラック、ノード、LAN スイッチなど、付属品を大まかに把握します。本製品を設置するためには、十分な電源供給が可能なインフラストラクチャと、十分なスペースが必要です。

Step 2. ネットワークの計画

システム管理者は、本製品を自社のネットワークに接続する方法を理解する必要があります。

Step 3. ファイルシステムの作成

GUI を使用してバックアップサーバから本製品にアクセスできるようにします。ファイルシステムを作成することで、NFS または CIFS を経由して、本製品のデータへのアクセスが可能になります。

Step 4. メール通報の設定

本製品のメール通報を使用すると、ハードウェア障害を確認でき、故障部品の交換が必要となる時を知ることができます。システムの運用を開始する前に、この機能を有効にしてください。

Step 5. NTP サーバの計画

NTP(Network Time Protocol)を利用すると、本製品の全ノードのシステム時刻を正しく同期させることができます。NTP を利用するためには LAN の中に適切な NTP サーバを構築する必要があります。

Step 6. 領域解放の計画

本製品は、以前削除されたデータパターンを自動的にキャッシュに保存します。領域解放を実施し、それぞれが完了するまでは、ユーザがデータを削除してもそのデータはディスク上から削除されることはありません。システム管理者の責任において領域解放を実行するタイミングを決定してください。

Step 7. ハードウェア障害への対策

バックアップデータを消失することなく、またサービスを止めることなく運用できるように、本製品は様々な機能をサポートしています。システム管理者は、ハードウェア障害のための対策を知っておく必要があります。

Step 8. レプリケーションの計画

本製品は、レプリケーション機能によりデータブロックを別のシステムへ転送し、2つのファイルシステム間で同一のデータコピーを持つことができます。データ転送はバッチジョブとして動作し、ジョブのスケジューリングにはいくつかのオプションが選択できます。

本製品の諸元については、「[付録A ソフトウェア諸元一覧](#)」を参照してください。

Step 1. 設置場所の計画

製品モデルの仕様

使用されている製品モデルの仕様表を参照して、必要な占有スペースなどを把握してください。

- シングルノードモデル(HS3-60) : 表 2-1
- シングルノードモデル(HS3-50S) : 表 2-2
- スケールアウトモデル(HS8-60) : 表 2-3
- スケールアウトモデル(HS8-50S) : 表 2-4
- シングルノードモデル(HS3-50) : 表 2-5
- スケールアウトモデル(HS8-50) : 表 2-6

表 2-1 シングルノードモデル(HS3-60)の仕様

モデル		シングルノードモデル (HS3-60)
搭載ディスク容量(データ)		24TB
搭載ディスク容量(システム)		1.2TB
筐体寸法(WxDxH)(mm) *1		448 x 774 x 87.5
質量(kg)		32
フットプリント(U)		2
電源条件		AC100~240V ± 10%、50/60Hz ± 3Hz 100V ケーブル標準添付 200V ケーブルオプション
ホストインタフェース		1GbE モデル: 1000BASE-T*2 (Copper: RJ-45)
		10GbE モデル: 10GBASE-SR (Optical: LC) + 1000BASE-T*2 (Copper: RJ-45) 10GBASE-T (Copper: RJ-45) + 1000BASE-T*2 (Copper: RJ-45)
ホストポート数		1GbE モデル: 1000BASE-T*2 x 6 ポート
		10GbE モデル: 10GBASE-SR x 2 ポート + 1000BASE-T*2 x 4 ポート 10GBASE-T x 2 ポート + 1000BASE-T*2 x 4 ポート 10GBASE-SR x 4 ポート + 1000BASE-T*2 x 2 ポート 10GBASE-T x 4 ポート + 1000BASE-T*2 x 2 ポート
ディスクドライブ 諸元 (データ用)	ディスクインタフェース	SATA
	容量(回転数)	2TB (7,200rpm)
ディスクドライブ 諸元(シ ステム用)	ディスクインタフェース	SAS
	容量(回転数)	600GB (10,000rpm)
ディスク数		12(データ用) + 2(システム用)
サポートプロトコル		NFS v3 over TCP、CIFS
管理機能		GUI、CLI、メール通報、SNMP

*1: フロントベゼル、スライドレール、および突起物は含みません。

*2: 100BASE-T、10BASE-T を代替で使用可能です。

表 2-2 シングルノードモデル(HS3-50S)の仕様

モデル		シングルノードモデル (HS3-50S)
搭載ディスク容量(データ)		24TB
搭載ディスク容量(システム)		1.2TB
筐体寸法(WxDxH)(mm) *1		448 x 744 x 87.5
質量(kg)		32
フットプリント(U)		2
電源条件		AC100~240V ± 10%、50/60Hz ± 3Hz 100V ケーブル標準添付 200V ケーブルオプション
ホストインタフェース		1GbE モデル: 1000BASE-T*2 (Copper: RJ-45)
		10GbE モデル: 10GBASE-SR (Optical: LC) + 1000BASE-T*2 (Copper: RJ-45) 10GBASE-T (Copper: RJ-45) + 1000BASE-T*2 (Copper: RJ-45)
ホストポート数		1GbE モデル: 1000BASE-T*2 x 6 ポート
		10GbE モデル: 10GBASE-SR x 2 ポート + 1000BASE-T*2 x 4 ポート 10GBASE-T x 2 ポート + 1000BASE-T*2 x 4 ポート 10GBASE-SR x 4 ポート + 1000BASE-T*2 x 2 ポート 10GBASE-T x 4 ポート + 1000BASE-T*2 x 2 ポート
ディスクドライブ 諸元 (データ用)	ディスクインタフェース	SATA
	容量(回転数)	2TB (7,200rpm)
ディスクドライブ 諸元(シ ステム用)	ディスクインタフェース	SAS
	容量(回転数)	600GB (10,000rpm)
ディスク数		12(データ用) + 2(システム用)
サポートプロトコル		NFS v3 over TCP、CIFS
管理機能		GUI、CLI、メール通報、SNMP

*1: フロントベゼル、スライドレール、および突起物は含みません。

*2: 100BASE-T、10BASE-T を代替で使用可能です。

表 2-3 スケールアウトモデル(HS8-60)の仕様

モデル		スケールアウトモデル (HS8-60)			
		1 HN	1 HN + 1 SN	2HN	2HN + 2SN
ノード構成	ハイブリッドノード(HN)	1	1	2	2
	ストレージノード(SN)	0	1	0	2
スイッチ数		0	0	0	2
搭載ディスク容量(データ)		72TB	144TB	144TB	288TB
搭載ディスク容量(システム)		1.8TB	3.0TB	3.6TB	6.0TB
筐体寸法(WxDxH)(mm) *1		448 x 774 x 87.5	448 x 774 x 175	448 x 774 x 175	448 x 774 x 437
質量(kg) *1		44	76	76	150
フットプリント(U) *1		4	6	6	12
電源条件		AC100~240V ± 10%、50/60Hz ± 3Hz 100V ケーブル標準添付 200V ケーブルオプション			
ホストインタフェース		1GbE モデル: 1000BASE-T (Copper: RJ-45)			
		10GbE モデル: 10GBASE-SR (Optical: LC) + 1000BASE-T (Copper: RJ-45) 10GBASE-T (Copper: RJ-45) + 1000BASE-T (Copper: RJ-45)			
ホストポート数 (ハイブリッドノード 1 台あたり)		1GbE モデル: 1000BASE-T x 6 ポート			
		10GbE モデル: 10GBASE-SR x 2 ポート + 1000BASE-T x 4 ポート 10GBASE-T x 2 ポート + 1000BASE-T x 4 ポート 10GBASE-SR x 4 ポート + 1000BASE-T x 2 ポート 10GBASE-T x 4 ポート + 1000BASE-T x 2 ポート			
ディスクドライブ諸元(データ用)	ディスクインタフェース	SATA			
	容量(回転数)	6TB (7,200rpm)			
ディスクドライブ諸元(システム用)	ディスクインタフェース	SAS			
	容量(回転数)	HN: 900GB (10,000rpm), SN: 600GB (10,000rpm)			
ディスク数		ハイブリッドノード 1 台あたり: 12(データ用) + 2(システム用) ストレージノード 1 台あたり: 12(データ用) + 2(システム用)			
サポートプロトコル		NFS v3 over TCP、CIFS			
管理機能		GUI、CLI、メール通報、SNMP			

* 1: フロントベゼル、スライドレール、および突起物は含みません。推奨オプションである保守 PC のフットプリントを 2U、重量を 12kg (ベゼル、ケーブル込)として算出した値になります。

Note 表 2-3 に記載されていない装置の構成については、担当営業または担当 SE にお問い合わせください。

表 2-4 スケールアウトモデル(HS8-50S)の仕様

モデル		スケールアウトモデル (HS8-50S)			
		1 HN	1 HN + 1 SN	2HN	2HN + 2SN
ノード構成	ハイブリッドノード(HN)	1	1	2	2
	ストレージノード(SN)	0	1	0	2
スイッチ数		0	0	0	2
搭載ディスク容量(データ)		72TB	144TB	144TB	288TB
搭載ディスク容量(システム)		1.8TB	3.0TB	3.6TB	6.0TB
筐体寸法(WxDxH)(mm) *1		448 x 744 x 87.5	448 x 744 x 175	448 x 744 x 175	448 x 744 x 437
質量(kg) *1		44	76	76	150
フットプリント(U) *1		4	6	6	12
電源条件		AC100~240V ± 10%、50/60Hz ± 3Hz 100V ケーブル標準添付 200V ケーブルオプション			
ホストインタフェース		1GbE モデル: 1000BASE-T (Copper: RJ-45)			
		10GbE モデル: 10GBASE-SR (Optical: LC) + 1000BASE-T (Copper: RJ-45) 10GBASE-T (Copper: RJ-45) + 1000BASE-T (Copper: RJ-45)			
ホストポート数 (ハイブリッドノード 1 台あたり)		1GbE モデル: 1000BASE-T x 6 ポート			
		10GbE モデル: 10GBASE-SR x 2 ポート + 1000BASE-T x 4 ポート 10GBASE-T x 2 ポート + 1000BASE-T x 4 ポート 10GBASE-SR x 4 ポート + 1000BASE-T x 2 ポート 10GBASE-T x 4 ポート + 1000BASE-T x 2 ポート			
ディスクドライブ諸 元(データ用)	ディスクインタフェース	SATA			
	容量(回転数)	6TB (7,200rpm)			
ディスクドライブ諸 元(システム用)	ディスクインタフェース	SAS			
	容量(回転数)	HN: 900GB (10,000rpm), SN: 600GB (10,000rpm)			
ディスク数		ハイブリッドノード 1 台あたり: 12(データ用) + 2(システム用) ストレージノード 1 台あたり: 12(データ用) + 2(システム用)			
サポートプロトコル		NFS v3 over TCP、CIFS			
管理機能		GUI、CLI、メール通報、SNMP			

* 1: フロントベゼル、スライドレール、および突起物は含みません。推奨オプションである保守 PC のフットプリントを 2U、重量を 12kg (ベゼル、ケーブル込)として算出した値になります。

Note 表 2-4 に記載されていない装置の構成については、担当営業または担当 SE にお問い合わせください。

表 2-5 シングルノードモデル(HS3-50)の仕様

モデル		シングルノードモデル (HS3-50)
搭載ディスク容量(データ)		24TB
搭載ディスク容量(システム)		1.2TB
筐体寸法(WxDxH)(mm)*1		448 x 684 x 87
質量(kg)		32
フットプリント(U)		2
電源条件		AC100~240V ± 10%、50/60Hz ± 3Hz 100V ケーブル標準添付 200V ケーブルオプション
ホストインタフェース		1000 / 100BASE-T (Copper: RJ-45)
ホストポート数		6 ポート
ディスクドライブ諸元 (データ用)	ディスクインタフェース	SATA
	容量(回転数)	2TB (7,200rpm)
ディスクドライブ諸元 (システム用)	ディスクインタフェース	SAS
	容量(回転数)	600GB (10,000rpm)
ディスク数		12(データ用) + 2(システム用)
サポートプロトコル		NFS v3 over TCP、CIFS
管理機能		GUI、CLI、メール通報、SNMP

* 1: フロントベゼル、スライドレール、および突起物は含みません。

表 2-6 スケールアウトモデル(HS8-50)の仕様

モデル		スケールアウトモデル (HS8-50)			
		1 HN	1 HN + 1 SN	2HN	2HN + 2SN
ノード構成	ハイブリッドノード(HN)	1	1	2	2
	ストレージノード(SN)	0	1	0	2
スイッチ数		0	0	0	2
搭載ディスク容量(データ)		48TB	96TB	96TB	192TB
搭載ディスク容量(システム)		1.8TB	3.0TB	3.6TB	6.0TB
筐体寸法(WxDxH)(mm) *1		448 x 684 x 176	448 x 684 x 276	448 x 684 x 276	448 x 684 x 534
質量(kg) *1		44	76	76	152
フットプリント(U) *1		4	6	6	12
電源条件		AC100~240V ± 10%、50/60Hz ± 3Hz 100V ケーブル標準添付 200V ケーブルオプション			
ホストインタフェース		1GbE モデル: 1000 / 100BASE-T (Copper: RJ-45)			
		10GbE モデル: 10GBASE-SR (Optical: LC)または 10GBASE-T(Copper: RJ-45)と 1000 / 100BASE-T (Copper: RJ-45)			
ホストポート数 (ハイブリッドノード 1 台あたり)		1GbE モデル: 6 ポート(1000 / 100BASE-T)			
		10GbE モデル: 2 または 4 ポート(10GBASE-SR または 10GBASE-T)と 2 ポート(1000 / 100BASE-T)			
ディスクドライブ諸 元(データ用)	ディスクインタフェース	SATA			
	容量(回転数)	4TB (7,200rpm)			
ディスクドライブ諸 元(システム用)	ディスクインタフェース	SAS			
	容量(回転数)	HN: 900GB (10,000rpm), SN: 600GB (10,000rpm)			
ディスク数		ハイブリッドノード 1 台あたり: 12(データ用) + 2(システム用) ストレージノード 1 台あたり: 12(データ用) + 2(システム用)			
サポートプロトコル		NFS v3 over TCP、CIFS			
管理機能		GUI、CLI、メール通報、SNMP			

*1: フロントベゼル、スライドレール、および突起物は含みません。必須オプションである保守 PC のフットプリントを 2U、重量を 12kg(ベゼル、ケーブル込)として算出した値になります。

Note 表 2-6 に記載されていない装置の構成については、担当営業または担当 SE にお問い合わせください。

● iStorage HS Virtual Appliance

iStorage HS Virtual Appliance は、仮想マシン上で動作する NEC iStorage HS のソフトウェアバージョンです (この仮想マシンの機能は、物理システムとほぼ変わりません)。この仮想システムは VMware ESXi 5.5、6.0 および Microsoft Hyper-V で動作します。配備・構成を実行後、グラフィカルユーザインターフェイス (GUI) またはコマンドラインインターフェイス (CLI) を使用して、そのサービスを管理することができます。iStorage HS 仮想システムの詳細については、「iStorage HS Virtual Appliance 導入構成ガイド」の「第 1 章 iStorage HS Virtual Appliance の概要」を参照してください。

増設用製品オプション仕様

ラックモデル、ラックレスモデルまたはスケールアウトモデルの場合、本製品はノードを追加することによって、システムを拡張することができます。表 2-7、表 2-8、表 2-9 に、ノードを拡張するための増設製品を示します。システムにラックを追加する場合には、拡張ラックと LAN スイッチの増設が必要です。

表 2-7 HS8-60 の増設用製品オプション一覧（ノード）

製品オプション	HS8-60 HN	HS8-60 SN
ホストポート数	表 2-3 「ホストポート数」を参照	-
質量(kg)	32	32
筐体寸法(W x D x H)(mm)	448 x 744 x 87.5	448 x 744 x 87.5
搭載ディスク容量(データ)	72TB	72TB
搭載ディスク容量(システム)	1.8TB	1.2TB
搭載ディスク数	12(データ用) + 2(システム用)	12(データ用) + 2(システム用)

表 2-8 HS8-50S の増設用製品オプション一覧（ノード）

製品オプション	HS8-50S HN	HS8-50S SN
ホストポート数	表 2-3 「ホストポート数」を参照	-
質量(kg)	32	32
筐体寸法(W x D x H)(mm)	448 x 744 x 87.5	448 x 744 x 87.5
搭載ディスク容量(データ)	72TB	72TB
搭載ディスク容量(システム)	1.8TB	1.2TB
搭載ディスク数	12(データ用) + 2(システム用)	12(データ用) + 2(システム用)

表 2-9 HS8-50 の増設用製品オプション一覧（ノード）

製品オプション	HS8-50 HN	HS8-50 SN
ホストポート数	表 2-5 「ホストポート数」を参照	-
質量(kg)	32	32
筐体寸法(W x D x H)(mm)	448 x 684 x 87	448 x 684 x 87
搭載ディスク容量(データ)	48TB	48TB
搭載ディスク容量(システム)	1.8TB	1.2TB
搭載ディスク数	12(データ用) + 2(システム用)	12(データ用) + 2(システム用)

製品の構成

本製品は、複数のノードまたは単体のノードで構成されます。本製品のノードには、アクセラレータノード、ストレージノードとハイブリッドノードの3種類があります。

- **アクセラレータノード(AN)**

アクセラレータノード機能のみが動作する物理ノードです。

- **ストレージノード(SN)**

ストレージノード機能のみが動作する物理ノードです。

- **ハイブリッドノード(HN)**

アクセラレータノード機能とストレージノード機能の両者の機能を持った物理ノードです。

ノードの詳細については、「ユーザズガイド」の「第1章 概要」を参照してください。

本製品のノード構成には以下の3種類があります。

- (1) アクセラレータノード機能を持つノードが2台以上あるモデル（図 2-1 を参照）
- (2) アクセラレータノード機能を持つノードが1台のみのモデル（図 2-2 を参照）
- (3) シングルノードモデル（図 2-3 を参照）

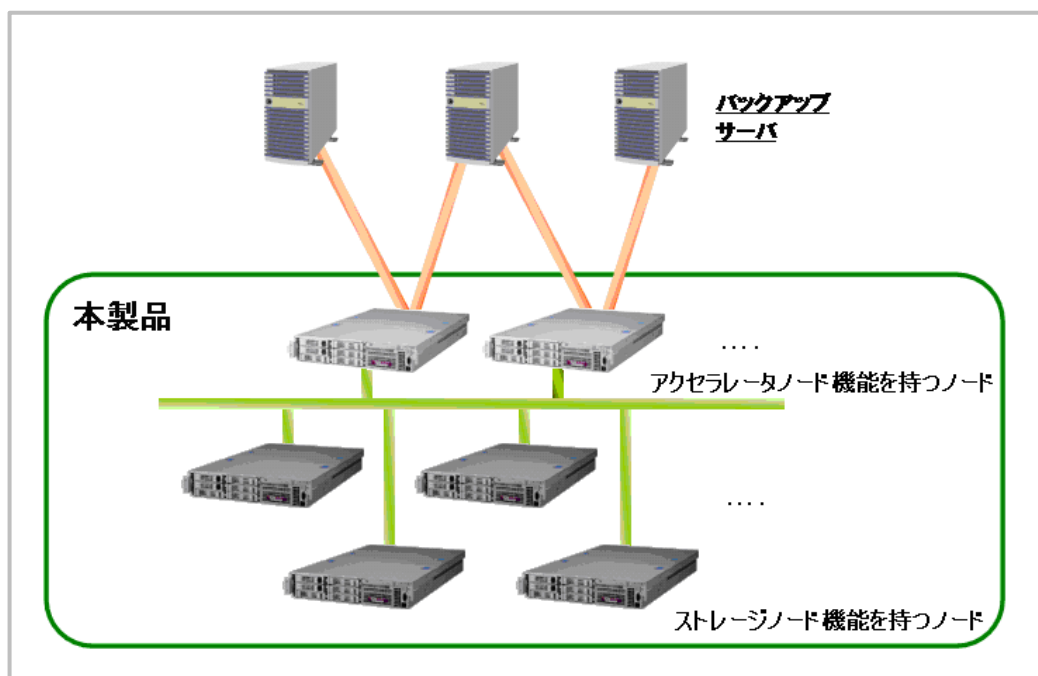


図 2-1 アクセラレータノード機能を持つノードが2台以上ある構成

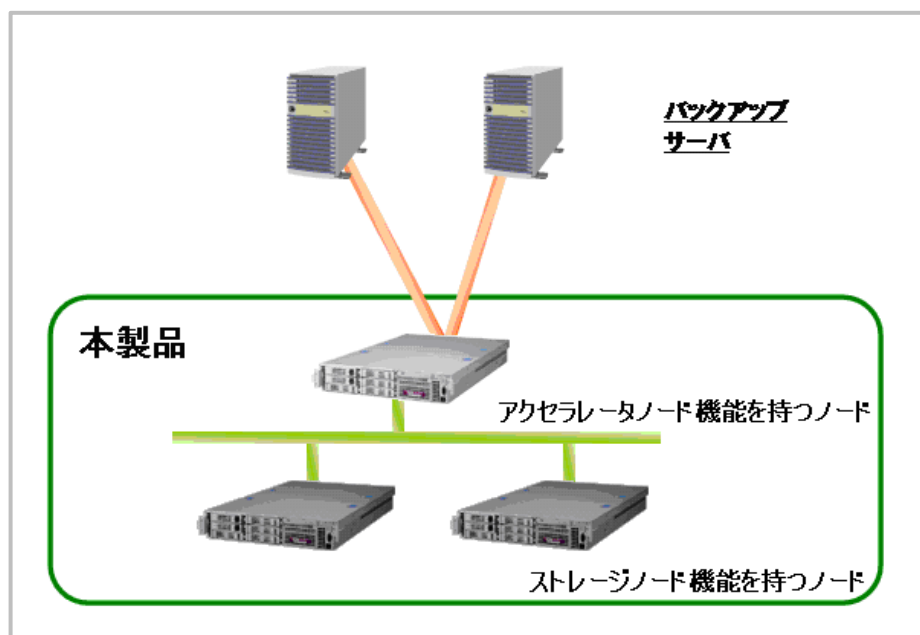


図 2-2 アクセラレータノード機能を持つノードが1台のみの構成

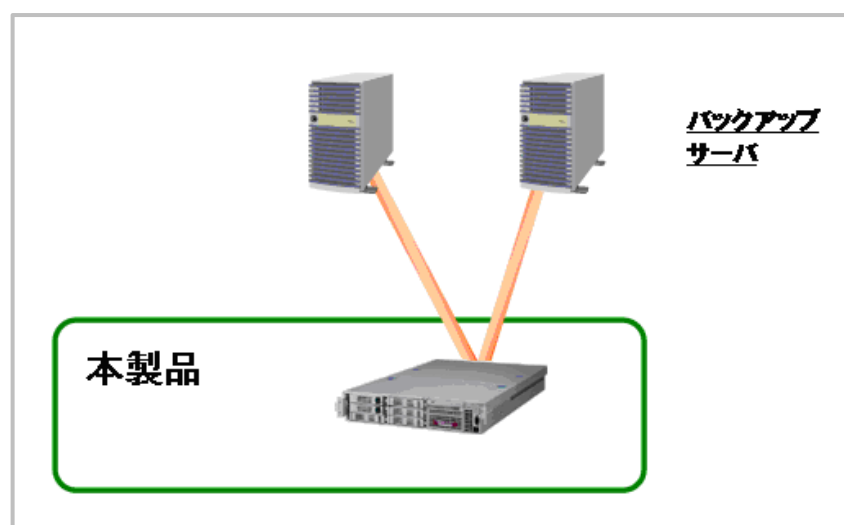


図 2-3 シングルノードモデルの構成

アクセラレータノード機能を持つノードがある構成では、本製品の操作および制御は、アクセラレータノード機能を持つノードを通して行います。

シングルノードモデルの場合、ハードウェアとしてはノード1台のみの構成となります。このノードが、ストレージノードとアクセラレータノードの両方の役割を務めます。

Step 2. ネットワークの計画

推奨ネットワークトポロジ

本製品を導入する際には、専用のバックアップネットワークの利用を推奨します。バックアップネットワークを専用とすることで、バックアップ用の帯域幅が他の通信により減少することを防ぐことができます。本製品の高性能ネットワークを最大限に活用するには、9,000バイト以下のジャンボフレームの利用も推奨します。

Note ジャンボフレームを利用する場合、本製品の設定だけでなく、本製品を接続する機器およびバックアップサーバもジャンボフレームの設定を行う必要があります。

本製品の推奨ネットワークトポロジを図 2-4 に示します。このトポロジではバックアップサーバは、2つのネットワークインタフェースによりそれぞれユーザネットワークとバックアップネットワークに接続することで、ネットワークを有効に分割しバックアップ帯域幅とセキュリティを確保しています。ここで、バックアップサーバのオペレーティングシステムは、マルチホーム環境においても性能劣化やルーティングなどの問題なく動作する必要があります。

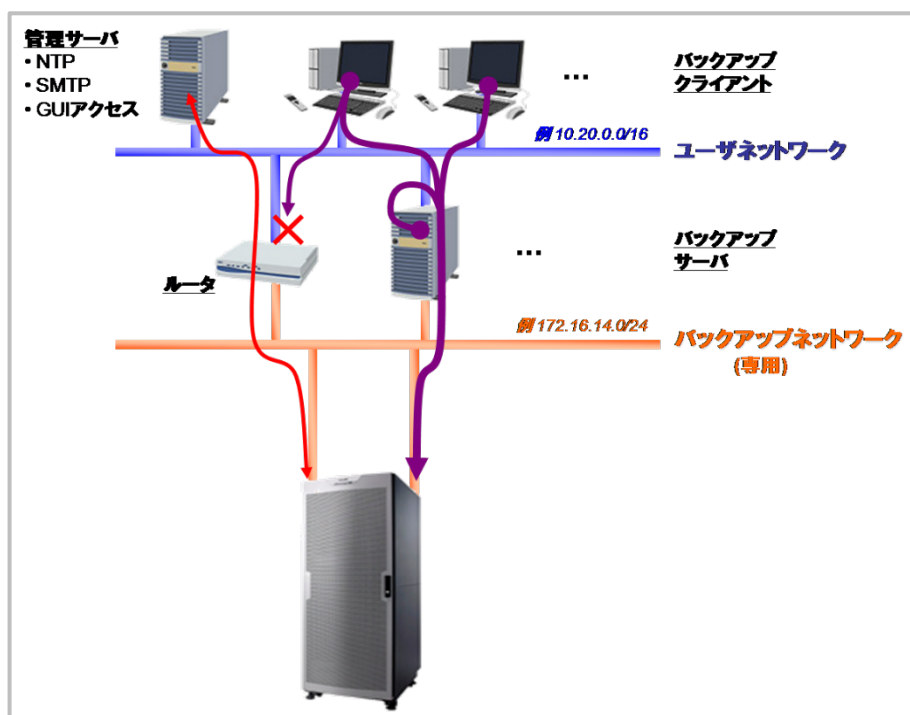


図 2-4 ネットワークの計画 - 推奨ネットワークトポロジ

代替ネットワークトポロジ

代替ネットワークトポロジでは、ルータ（L3 スイッチ）を使用して、バックアップサーバのトラフィックをバックアップネットワークに転送します。この場合、マルチホーム環境のバックアップサーバは不要で、バックアップサーバでは 1 つのネットワークインタフェースしか必要ありません。推奨ネットワークトポロジを使用する場合と同様にルータを設定することで、不要なトラフィックを拒否しセキュリティを確保することができます。この代替ネットワークトポロジではルータを通るトラフィックの一部は、MAC アドレスによる負荷分散ポリシーを備える機器を経由する場合、理想的に負荷分散できない場合があるため注意が必要です。代替ネットワークを図 2-5 に示します。

Note 代替ネットワークトポロジでジャンボフレームを利用する場合、本製品とバックアップサーバ間の経路にあるすべての機器（ルータ）にジャンボフレームの設定を行う必要があります。

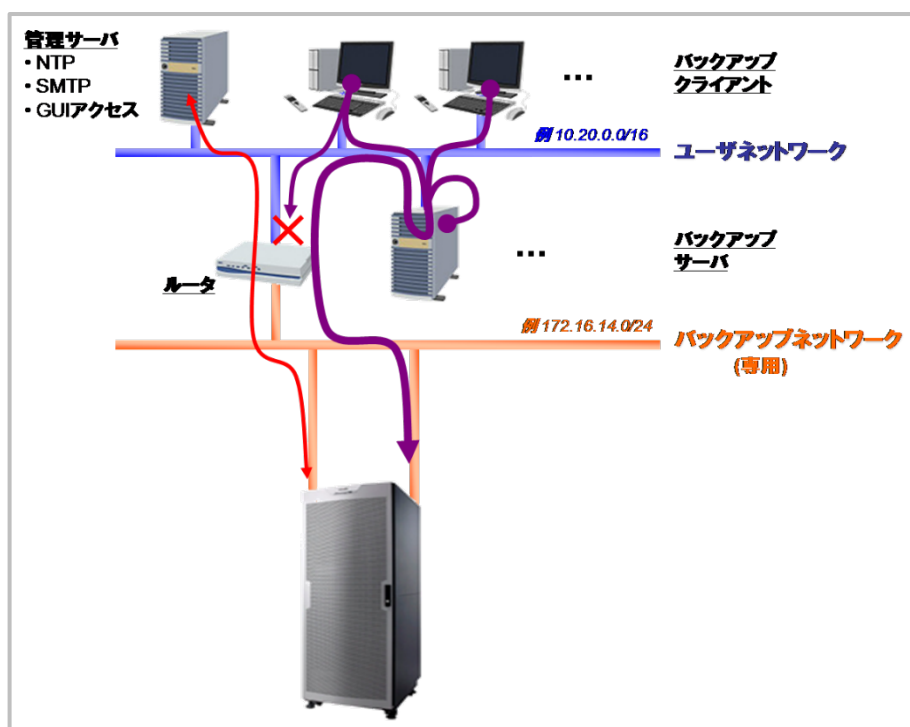


図 2-5 代替ネットワークトポロジ

バックアップネットワークの冗長性

本製品は、バックアップネットワーク内で、バックアップサーバとの間に冗長ネットワークリンクを確立するために、bonding という冗長化機能を持っています。bonding ポートは、複数のネットワークインタフェースを束ね、通信帯域を増大させるとともに NIC やスイッチの故障時には通信可能なインタフェースを用いて、次の 4 種類の動作モードをサポートしています。本製品では通信帯域を有効利用できる balance-alb モードの設定を推奨します。

Note iStorage HS Virtual Appliance での bond 作成はサポートしていません。ネットワークの冗長化には、基盤となるホストサーバでの bond 使用を推奨します。
ストレージネットワーク冗長化のイメージを図 2-6 に示します。

表 2-10 bonding の動作モード

動作モード	説明	10GbE NIC のサポート状況
802.3ad	802.3ad はネットワークスイッチなどでも一般的に普及している標準規格(IEEE802.3ad)に準拠したモードです。802.3ad により、2 つ以上の Gigabit Ethernet 接続をグループ化し、高帯域幅ネットワーク接続向けに、より大きな冗長性を実現できます。条件として、すべてのリンクが同じ速度と同じ通信方式（全二重または半二重）である必要があります。また、LAN スイッチが IEEE802.3ad をサポートしている必要があります、多くの場合スイッチに 802.3ad を有効にする設定が必要になります。 スイッチの装置を跨って 802.3ad を構成する場合は、一般的にスイッチがスタッキング構成をサポートする必要があります。非スタック構成で 사용되는場合は、LAN スイッチが「単一障害点」になる場合があります。 本製品からの送信負荷分散は次の 2 種類の送信ポート選択ポリシーに従って決定されます。 - レイヤ 2 (MAC アドレス) : 通信先の MAC アドレスに基づいて選択されます。 - レイヤ 3+4 (IP アドレス+ポート番号) : 通信先の IP アドレスと TCP/UDP ポート番号に基づいて選択されます。 この送信ポート選択ポリシーは GUI から設定可能です。受信側の負荷分散は接続されているスイッチの負荷分散ポリシーに依存します(※)。負荷分散ポリシーやスイッチの設定方法についてはスイッチのベンダに問い合わせてください。 ※スイッチの負荷分散ポリシー、IP アドレス、MAC アドレスの組み合わせによっては、受信ポートの偏りが発生します。このモードは耐障害性と負荷分散を提供します。	○

動作モード	説明	10GbE NIC のサポート状況
balance-alb	本製品と接続するスイッチが IEEE802.3ad をサポートしていない場合、balance-alb を使用することを推奨します。このモードでは、送信ポートおよび受信ポートを通信負荷状況により分散します。受信ポートの分散は、通信相手ごとに各スレーブの異なる MAC アドレスを ARP によって通知することで実現しています。そのため、ルータを越える別サブネットからの通信相手が存在する場合、均等に負荷分散しない場合があります。 balance-alb モードでは、特別なスイッチを必要とせず、速度や通信方式が異なる L2 スイッチ間で動作可能です。1 つの IP アドレスに複数の MAC アドレスを用いるため、ネットワーク監視ソフトウェアが IP アドレス重複のアラートを発生させる場合があります。 このモードは耐障害性と負荷分散を提供します。	○
active-backup	active-backup では、1 つのインタフェースのみが有効となり、残りのインタフェースは待機状態となります。有効なインタフェースがダウンすると、待機状態の 1 つが有効なインタフェースとして新たに使用されます。本モードは接続するスイッチに特別な機能を必要としません。 スイッチの設定によってはインタフェース切り替え時にリンクアップの検出に時間を要して切り替え後に通信可能となるまで時間がかかる場合があります。この現象は、bonding ポートの設定で updelay に適切な値(※)を指定することで回避できます。 ※通常は 5 秒程度の値を設定することで回避できますが、スイッチに Spanning Tree を設定している場合は、30 秒以上の値を設定してください。 このモードは耐障害性のみ提供します。	○
balance-rr	利用可能なスレーブを順番に使用して送信します。受信ポートは接続されるスイッチの転送ポリシに依存します。 環境（特に遅延のある WAN 環境）によってはパケット順序の入れ替わりにより性能劣化が発生する場合があります。性能劣化が認められる場合、他モードの利用を検討してください。また、スイッチによってはポートのグルーピングが必要になる場合があります。詳細はスイッチのベンダに問い合わせてください。 このモードは耐障害性と負荷分散を提供します。	×

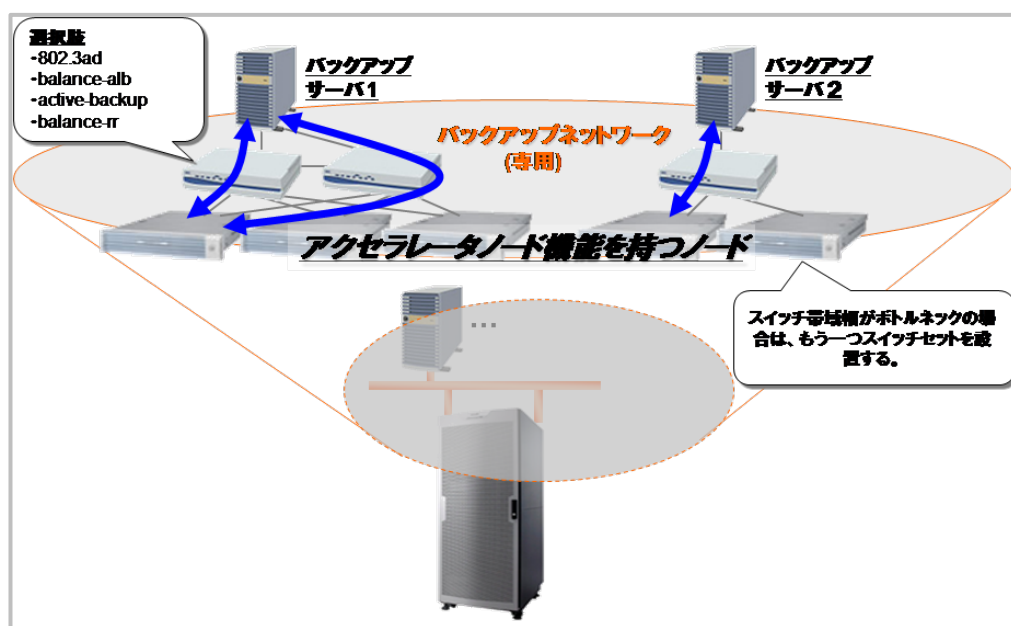


図 2-6 バックアップネットワークの冗長性

複数のネットワークとの接続

本製品は、複数のネットワークから接続するために VLAN Tagging(IEEE802.1Q)をサポートしています。

VLAN Tagging は、1 つの物理 LAN を複数の仮想 LAN(VLAN)で共有するための機能です。VLAN はネットワークを構成する上で物理的な束縛を受けないことから、ネットワーク構成の変更や端末の移動を容易に行うことができます。

また、bonding と組み合わせることで高帯域幅を複数の VLAN で有効利用することができます。

VLAN Tagging の設定方法については、「コマンドリファレンス」の「第II編 リファレンス」の「第2章 コマンド」の「vlan」を参照してください。

VLAN Tagging の接続イメージを図 2-7 に示します。

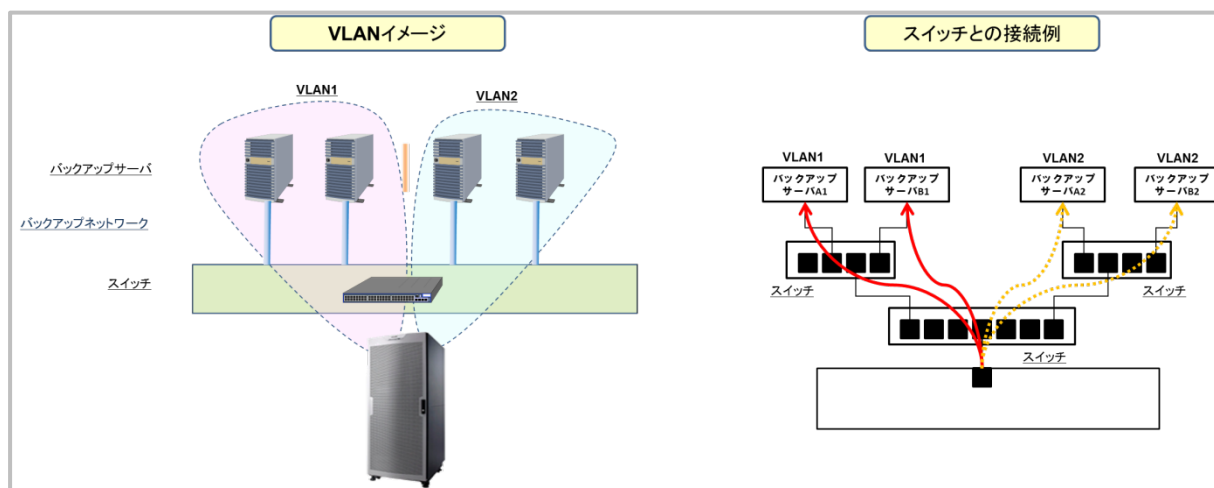


図 2-7 VLAN Tagging の接続イメージ

外部ネットワーク通信のフィルタリング設計

本製品は TCP/IP パケットのフィルタリング機能を有し、外部ネットワークとの通信でシステムに必要なパケットとそうでないパケットの判別を行います。設定を追加したい場合、CLI(netfirewall)を使用してフィルタリングルールを追加することができます。高いセキュリティを維持する必要があり、下記に記載するサービスをブロックしたい場合設定を検討して下さい。

表 2-11 サービスと対応ポート

サービス名	使用ポート/プロトコル *1
CLI (telnet) *2	23
CLI (rsh) *3	514/tcp
CLI (ssh)	22
GUI (HTTP)	8585, 9595
GUI (HTTPS)	8282, 9292
ftp	21
sftp	115
rsync	873
NFS (nfs, sunrpc)	111/tcp udp portmapper, 2049/tcp nfsd, 61001/tcp udp mountd, 61002/tcp udp lockd, 61003/tcp udp statd
CIFS (NetBIOS, SMB)	137, 138, 139, 445

* 1: プロトコルの記載がない場合 TCP,UDP ともに使用

* 2: システムバージョン 5.7.1 以降はデフォルトでブロック

* 3: システムバージョン 7.0.0 以降はデフォルトでブロック

図 2-8 フィルタリング機能の概念図に本製品のフィルタリング機能の概念図を示します。外部ネットワーク用の I/F (elan I/F) がパケットを受信すると、フィルタリング機能が受信可否を判断します。まずユーザが追加定義したフィルタリングルールに基づき受信可否を判断します。ルールに該当しなかった場合はシステムが備えるフィルタリングルールで判定を行います。フィルタリング機能が受信可能と判断したら各サービスへパケットが届けられ通信が可能になります。先にユーザ定義のルールで判断しているため、誤った設定をすると通信できなくなります。十分な検討を行った上でルールを追加して下さい。ユーザ定義フィルタリングルールに追加するには CLI (netfirewall) を使用して下さい。

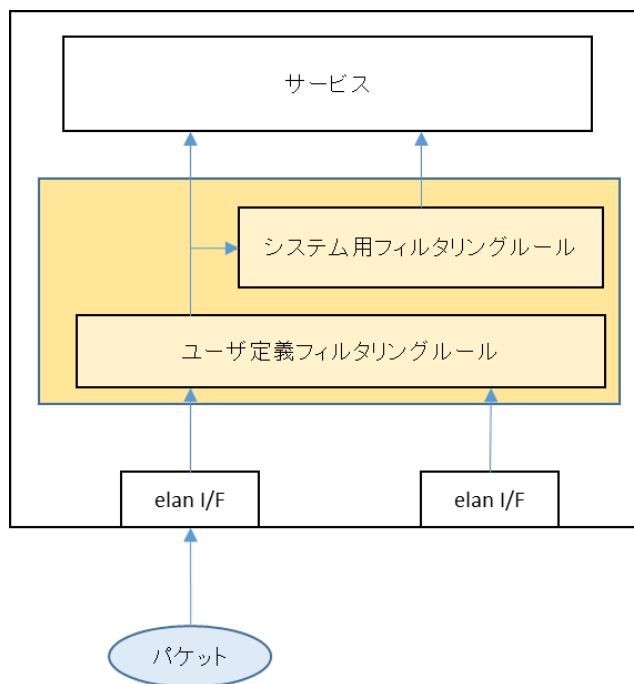


図 2-8 フィルタリング機能の概念図

Note netfirewall CLI で設定を実機に反映する際にわずかな間(数秒程度)ユーザ定義フィルタリングルールが解除されます。極めてセキュリティレベルが高い環境下で運用されている場合、クローズドのネットワーク内で設定するなど外部から物理的に隔離した環境で設定してください。

設定例 1 :

192.0.2.0/24 のネットワークからの telnet(23)の通信を許可する。

```
netfirewall add source-address=192.0.2.0/24 protocol=tcp port-number=23 action=accept
netfirewall add source-address=192.0.2.0/24 protocol=udp port-number=23 action=accept
netfirewall reflect
```

設定例 2 :

192.0.2.0/24 のネットワーク以外からの rsh(514/tcp)の通信をブロックする。

```
netfirewall add source-address=192.0.2.0/24 protocol=tcp port-number=514 action=accept
netfirewall add protocol=tcp port-number=514 action=drop
netfirewall reflect
```

※rsh はシステムバージョン 7.0.0 以降ではデフォルトでブロックしています。

Note フィルタリング機能は先に登録したルールから順に合致しているか判定を行い、最初に合致したルールを実行すると終了します。登録順に留意して下さい。

Note netfirewall CLI は reflect オプションを実行するまで設定が反映されません。追加したルールに問題がなければ netfirewall reflect オプションを実行して下さい。

アクセラレータノード機能クラスタのためのネットワーク設計

ラックモデル、ラックレスモデルまたはスケールアウトモデルの場合、本製品はアクセラレータノード機能を持つノードの障害の発生時に別のアクセラレータノード機能を持つノードに IP アドレスとファイルシステムを自動的に引き継ぎ、サービスの停止時間を短縮することができます。この機能をアクセラレータノード機能クラスタと呼び、障害が発生したノードのリソースを移動する動作を「フェイルオーバー」と呼びます。

2つのノードを互いにフェイルオーバーするよう関連付ける場合、両者のネットワーク構成は同等である必要があります。同等なネットワーク構成とは、以下の設定内容がノード間で同一であることを示します。

- インタフェース名（冗長リンクを用いる場合は、両ノード共冗長リンクを用いる必要あり）
- ネットワークアドレスとサブネットマスク
- ゲートウェイ設定（デフォルトゲートウェイと静的ルーティング設定内容）
- DNS 設定

これらのネットワーク設定が異なる場合、フェイルオーバー動作自体は正常に終了することがありますが、クライアントから移動後のリソースへは到達不能になります。

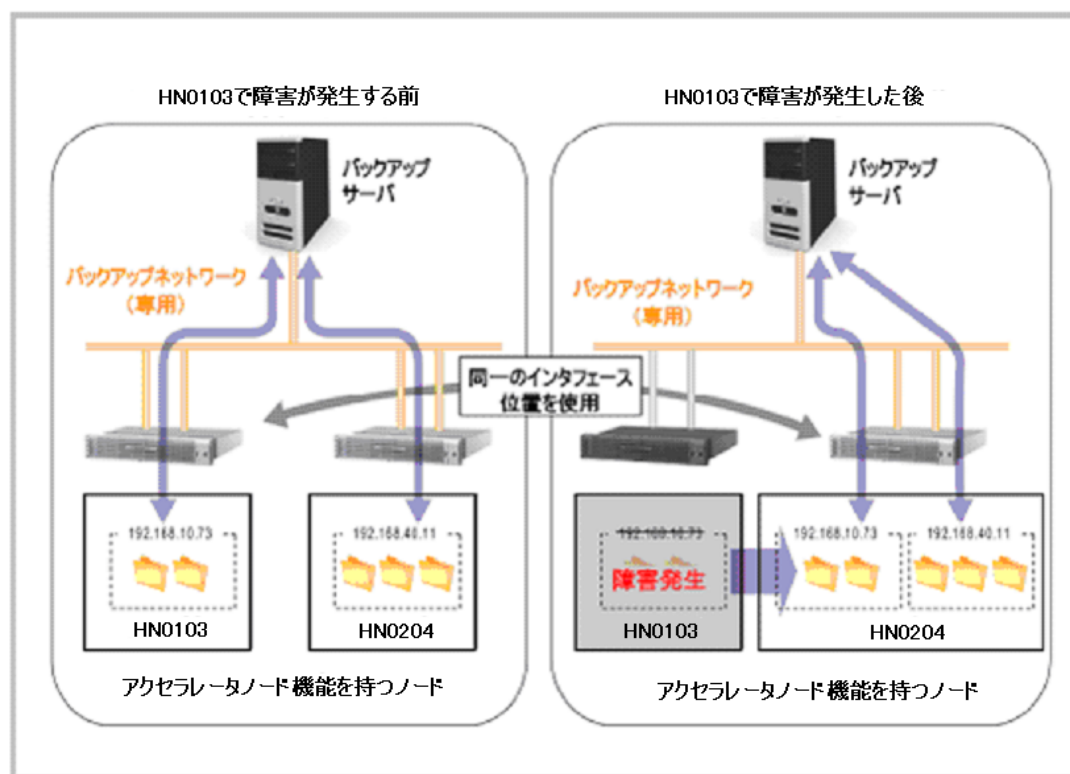


図 2-9 アクセラレータノード機能クラスタ動作イメージ

図 2-9 の例では HN0103 と HN0204 が互いにフェイルオーバー先として構成されており、HN0204 は HN0103 の故障時にその IP アドレスとファイルシステムを引き継ぎます。バックアップサーバは HN0103 の故障後しばらくすると、HN0103 が動作しているかのようにそのファイルシステムにアクセスすることができます。詳細は「[Step 7. ハードウェア障害への対策](#)」 「[アクセラレータノード機能クラスタ](#)」を参照してください。

レプリケーション用ネットワークの設計

リモートサイト¹⁾の本製品へ接続するためのレプリケーション用ネットワークには、IP ネットワーク（通常は WAN(VPN)）を使用します。本製品によるリモートサイトへの転送データの暗号化を設定していないときは、データ暗号化機能を備えた VPN の利用を推奨します。レプリケーションを行うネットワーク経路で VPN を使用する際に、レプリケーションがエラーとなる場合があります。レプリケーションがエラーとなる場合は、コマンドラインインタフェース(CLI)の `net` コマンド（サブコマンド名 `test`）を使用し、本製品のポートの MTU の設定に問題がないことを確認してください。問題がある場合は、MTU を変更してください。net コマンドの使用方法は、「コマンドリファレンス」の「第 II 編 リファレンス」、「第2章 コマンド」の「net」を参照してください。また、MTU の変更方法は、「ユーザーズガイド」の「第5章 システム設定」の「アクセラレータノード機能を持つノードの外部ネットワーク設定を有効にする」を参照してください。

リモートサイトの本製品が別のサブネットに属する場合はルータが必要となるので、アクセラレータノード機能を持つノードにゲートウェイを設定してください。

レプリケーションを行うネットワーク経路にファイアウォールを設置する場合は、以下を参考に設定してください。

用途	送信元 IP アドレス	送信先	
		IP アドレス	TCP ポート番号
制御用	マスタ側の FIP*	レプリカ側の FIP*	30001, 30027
	レプリカ側の FIP*	マスタ側の FIP*	30001, 30027
データ転送用	レプリカ側レプリケーションセットのデータ転送ポートの IP アドレス	マスタ側レプリケーションセットのデータ転送ポートの IP アドレス	30010, 30027~30035
	マスタ側レプリケーションセットのデータ転送ポートの IP アドレス	レプリカ側レプリケーションセットのデータ転送ポートの IP アドレス	30010, 30027~30035

* : FIP はフローティング IP アドレスを意味します。レプリケーション用 FIP を設定している場合、FIP はレプリケーション用 FIP、設定していない場合、FIP は GUI 管理用 FIP です。シングルノードモデルの場合、FIP をレプリケーション IP アドレスに読み替えてください。

OST の高速コピー機能を使用する場合、レプリケーションを利用してデータの転送を行います。その間 NetBackup メディアサーバはレプリカ側 iStorage HS と通信を継続する必要があります。高速コピーを行うネットワーク経路にファイアウォールを設置する場合は、レプリケーションの設定に加えて、以下を参考に設定してください。

用途	送信元 IP アドレス	送信先	
		IP アドレス	TCP ポート番号
制御用	NetBackup メディアサーバの IP アドレス	レプリカ側 iStorage HS の外部 IP アドレス	64006~64010, 64020

¹⁾iStorage HS 設置場所のことを「サイト」、遠隔の iStorage HS 設置場所を「リモートサイト」と呼びます。リモートサイトに対して、近隣の iStorage HS 設置場所を「ローカルサイト」と呼びます。

IP アドレスは NAT などにより変換して通信することはできません。

スケールアウトモデルの場合は、フローティング IP アドレスがレプリケーション用ネットワーク上に存在している必要があります。詳細については、「[ユーザーズガイド](#)」の「[第9章 レプリケーション \(GUI 操作\)](#)」を参照してください。

以下の2つは代表的なネットワーク構成例です。

バックアップとレプリケーションで冗長リンクを共有する構成

複数のネットワークインタフェースを冗長化し、バックアップとレプリケーションに利用します。図 2-10 と図 2-11 はこのネットワーク構成の例です。この場合、遠隔の本製品へパケット転送するため、2つのネットワーク間にルータが必要になり、アクセラレータノード機能を持つノードにゲートウェイの設定が正しく行われている必要があります。

表 2-12 バックアップとレプリケーションで冗長リンクを共有する構成の長所と注意点

長所	注意点
- 耐障害性が高い - 帯域が広い	レプリケーションの通信がバックアップ性能を阻害する可能性がある

Note レプリケーションには、使用する帯域を制限するオプションがあります。ジョブレベル、システムレベルまたはノードレベルで帯域制限を設定することができます。

- スケールアウトモデルの場合

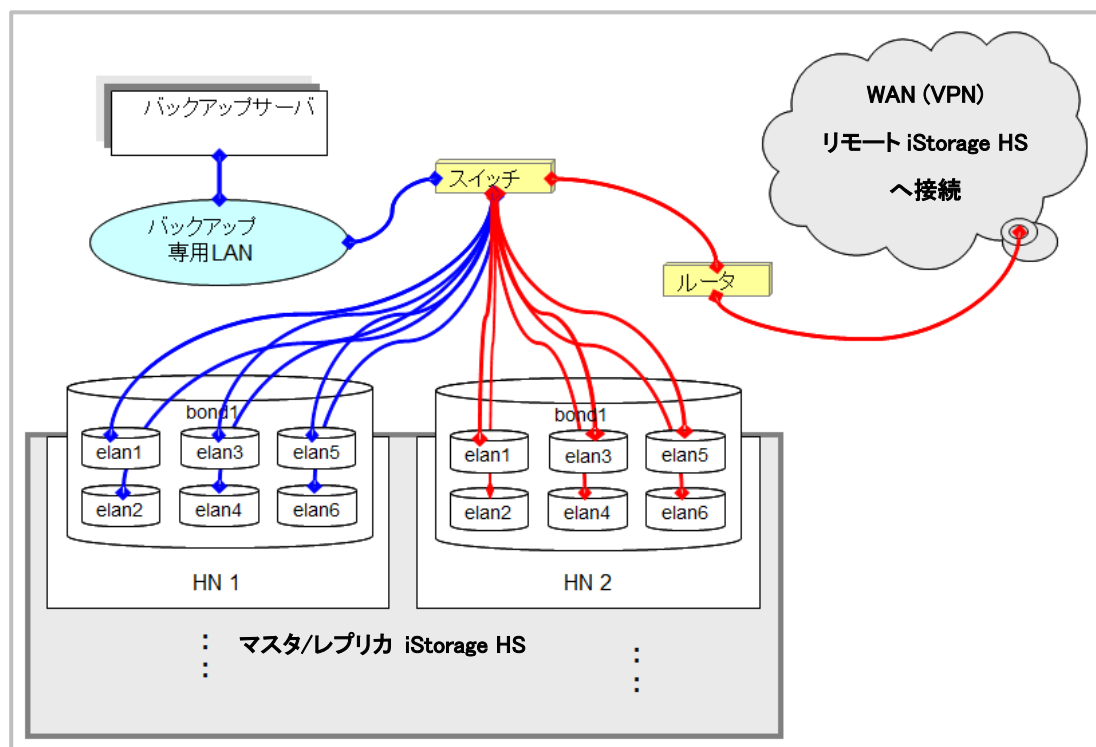


図 2-10 バックアップとレプリケーションで冗長リンクを共有する構成
(スケールアウトモデル)

- シングルノードモデルの場合

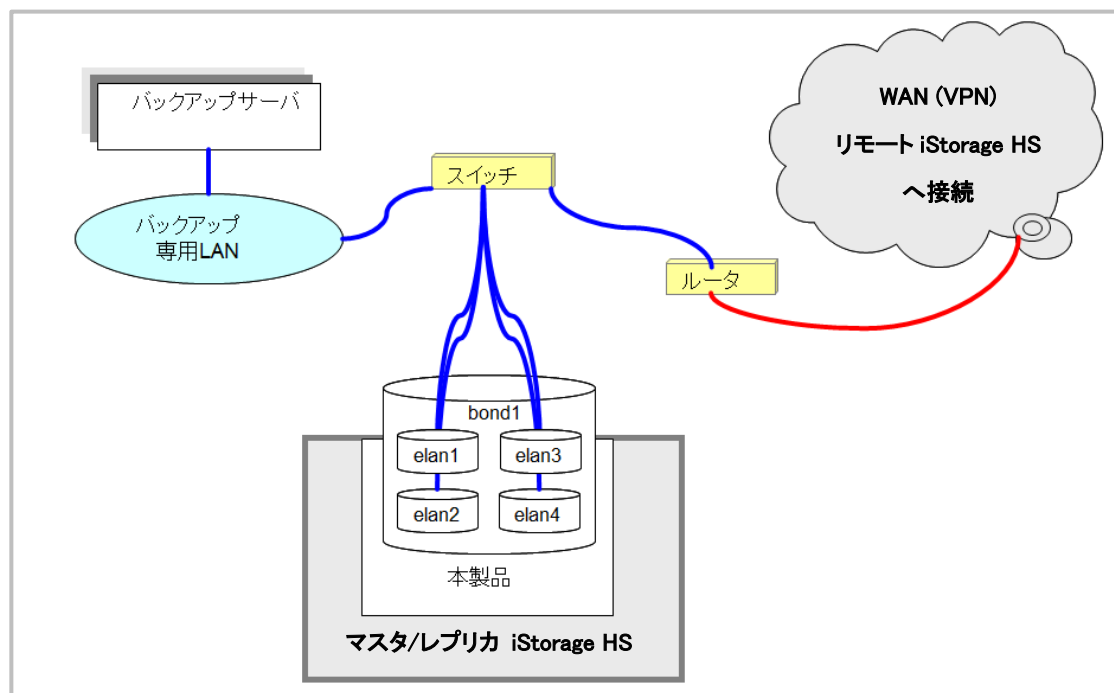


図 2-11 バックアップとレプリケーションで冗長リンクを共有する構成
(シングルノードモデル)

バックアップとレプリケーションで冗長リンクを分ける構成

図 2-12 と図 2-13 のネットワーク構成例は、1 つの冗長リンクをレプリケーション専用にご利用します。

表 2-13 バックアップとレプリケーションで冗長リンクを分ける構成の長所と注意点

長所	注意点
バックアップで使用するネットワークとレプリケーションで使用するネットワークが独立しているため、他の業務に影響を及ぼさない	- 通信帯域が前例（バックアップとレプリケーションで冗長リンクを共有する構成）と比べて小さい - 冗長リンクを使用しない場合、ネットワークインタフェースの耐障害性はない

- スケールアウトモデルの場合

レプリケーションネットワークである bond2 にフローティング IP アドレスが設定されている必要があります。

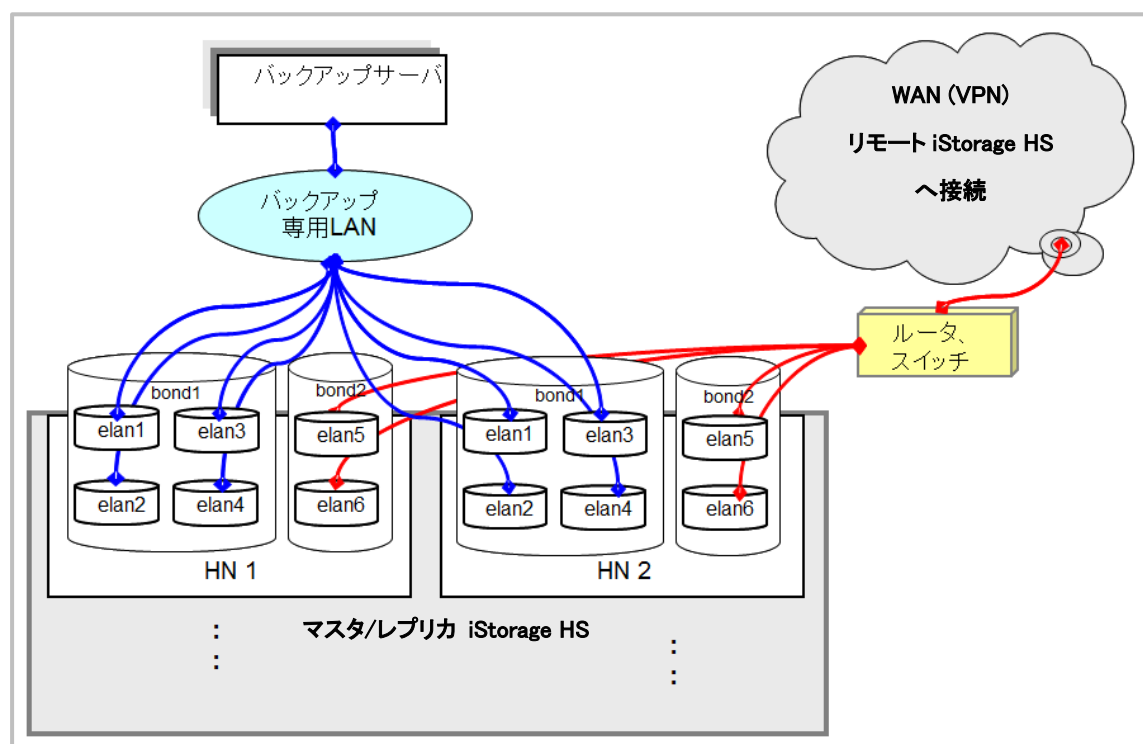


図 2-12 バックアップとレプリケーションで冗長リンクを分ける構成
(スケールアウトモデル)

- シングルノードモデルの場合

レプリケーションネットワークである bond2 がレプリケーション用ポートとして設定されている必要があります。

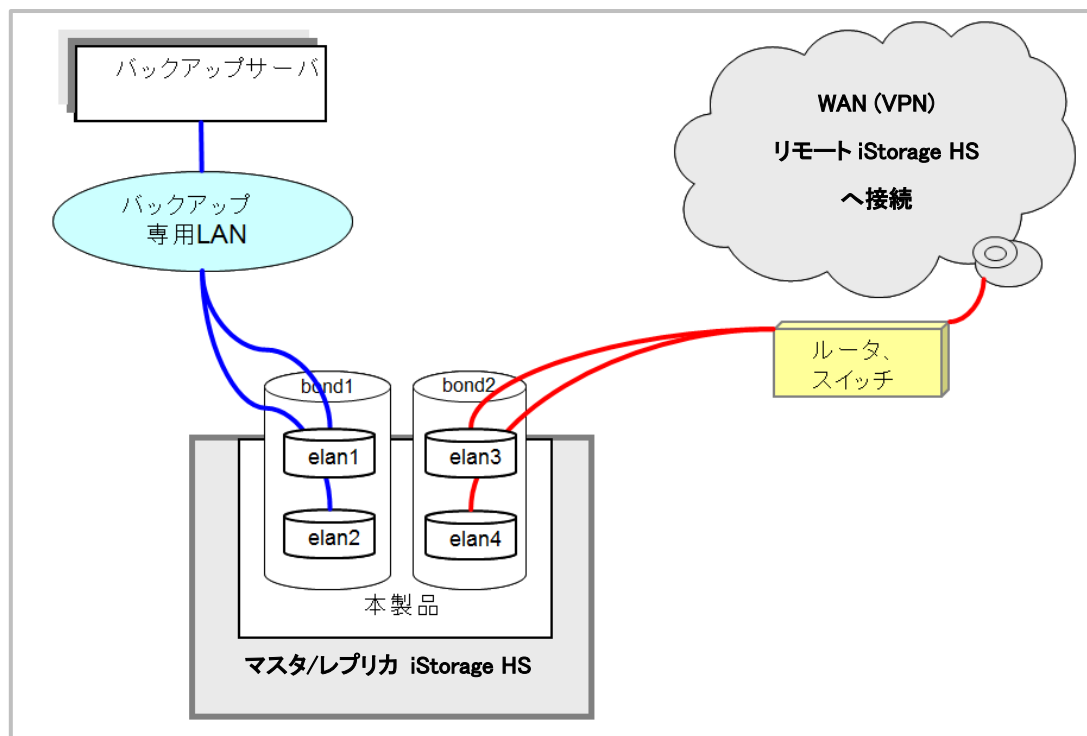


図 2-13 バックアップとレプリケーションで冗長リンクを分ける構成
(シングルノードモデル)

レプリケーション用ネットワークの接続（スケールアウトモデルの場合）

本製品は、GUI 操作用の管理 LAN とレプリケーション制御通信用のレプリケーション制御 LAN(WAN)を、異なるネットワークとして接続することができます。そのため、データセンタなどの管理 LAN が分離された環境においてもレプリケーションが利用可能です(図 2-14)。シングルノードモデルについては「[レプリケーション用ネットワークの接続（シングルノードモデル）](#)」を参照してください。

管理 LAN とレプリケーション制御 LAN(WAN)のネットワークを分離するには、ローカルシステムに、GUI 用の外部フローティング IP アドレスとは別に、レプリケーション用の外部フローティング IP アドレスを設定します。また、リモートサイトのシステムに本機の情報を登録（リモートシステム登録）する際、そのレプリケーション用外部フローティング IP アドレスを登録します（

図 2-15）。

GUI 用とレプリケーション用の外部フローティング IP アドレスは、システムの外部ネットワーク画面から設定できます。

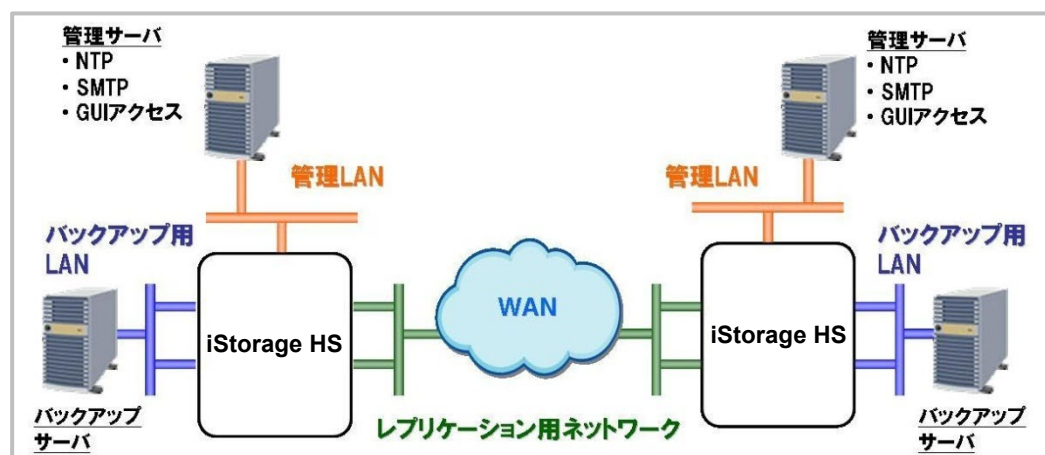


図 2-14 GUI とレプリケーションのネットワークを分離する場合
(スケールアウトモデル)

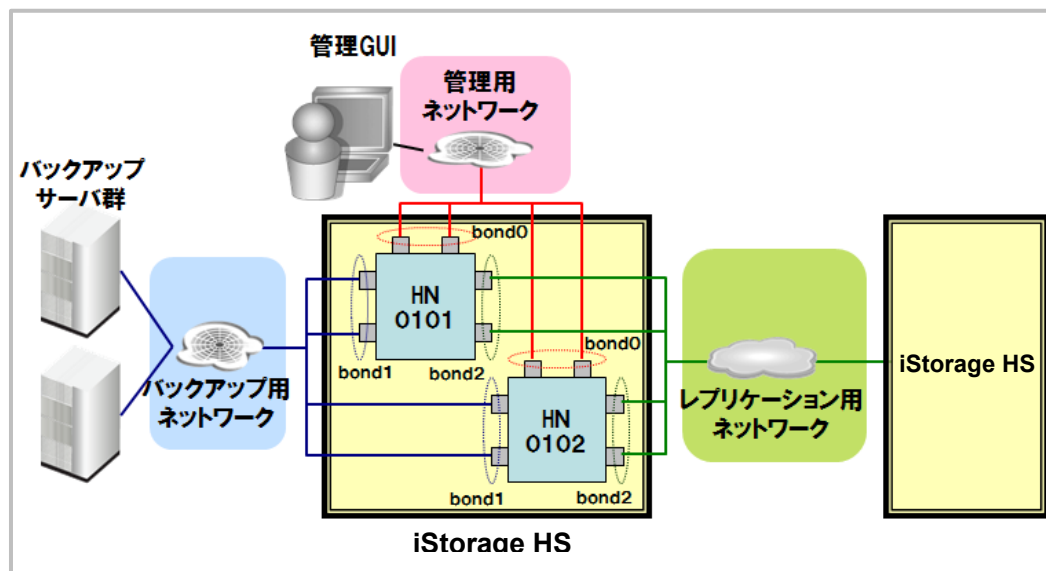


図 2-15 ネットワーク分離例（スケールアウトモデル）

物理ポート数が不足した場合などは、管理 LAN とレプリケーション制御 LAN(WAN)を共用することができます。管理 LAN とレプリケーション制御 LAN(WAN)を共用してバックアップ用の LAN を分離するといったように、ネットワークすべてを共用せずに一部を分離することもできます。

ネットワークを共用する場合は、ローカルシステムに GUI 用の外部フローティング IP アドレスのみ設定します。レプリケーション用の外部フローティング IP アドレスは設定しないでください。また、リモートサイトのシステムに本機情報を登録(リモートシステム登録)する際、GUI 用の外部フローティング IP アドレスを登録します(図 2-16、図 2-17、図 2-18)。

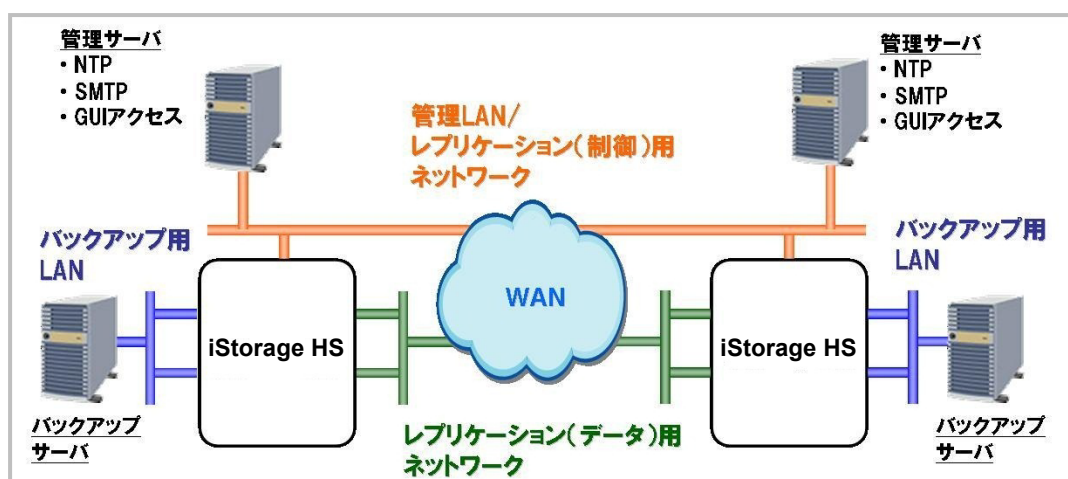


図 2-16 GUI とレプリケーションのネットワークを共用する場合
(スケールアウトモデル)

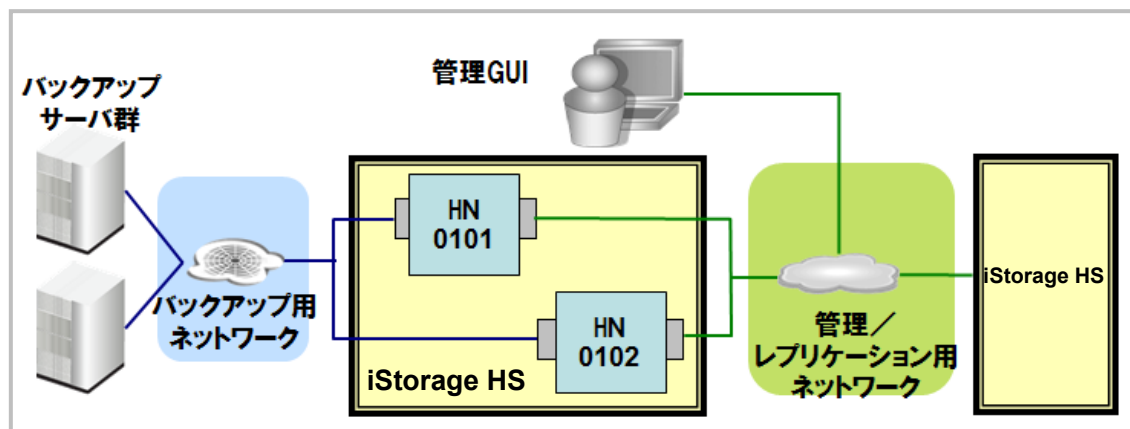


図 2-17 管理/レプリケーション用ネットワークの共用例
(スケールアウトモデル)

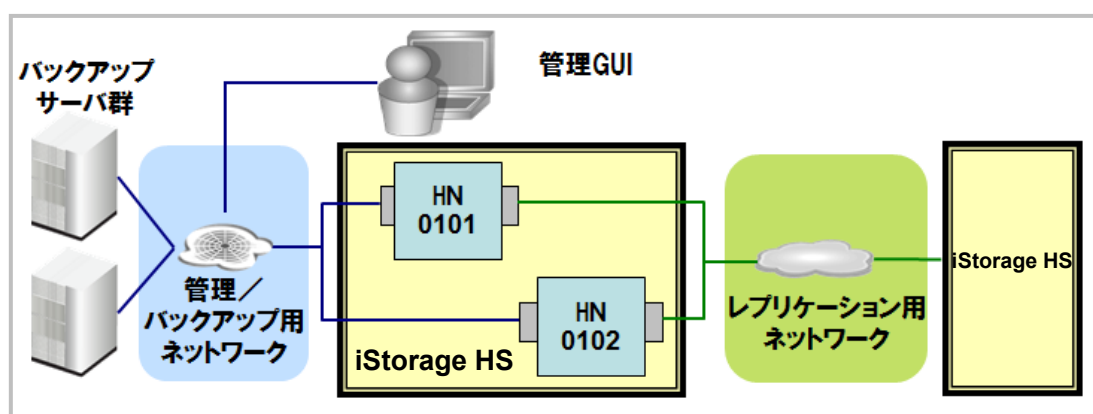


図 2-18 管理/バックアップ用ネットワークの共用例
(スケールアウトモデル)

管理 LAN とレプリケーション制御 LAN(WAN)のネットワークを分離した場合、管理 LAN（図 2-19 の HN0101 の管理用ネットワークへの接続ポート）またはレプリケーション制御 LAN(WAN)（図 2-19 の HN0101 のレプリケーション用ネットワークへの接続ポート）のどちらかに障害が起きると、管理ノードから代替ノードへフェイルオーバーします。管理 LAN とレプリケーション制御 LAN(WAN)の両方に障害が起きたときは、管理 LAN を優先したフェイルオーバー動作となります（図 2-19）。

GUI の詳細については「ユーザズガイド」の「第6章 システムの操作と状態の監視」と「第9章 レプリケーション (GUI 操作)」を参照してください。

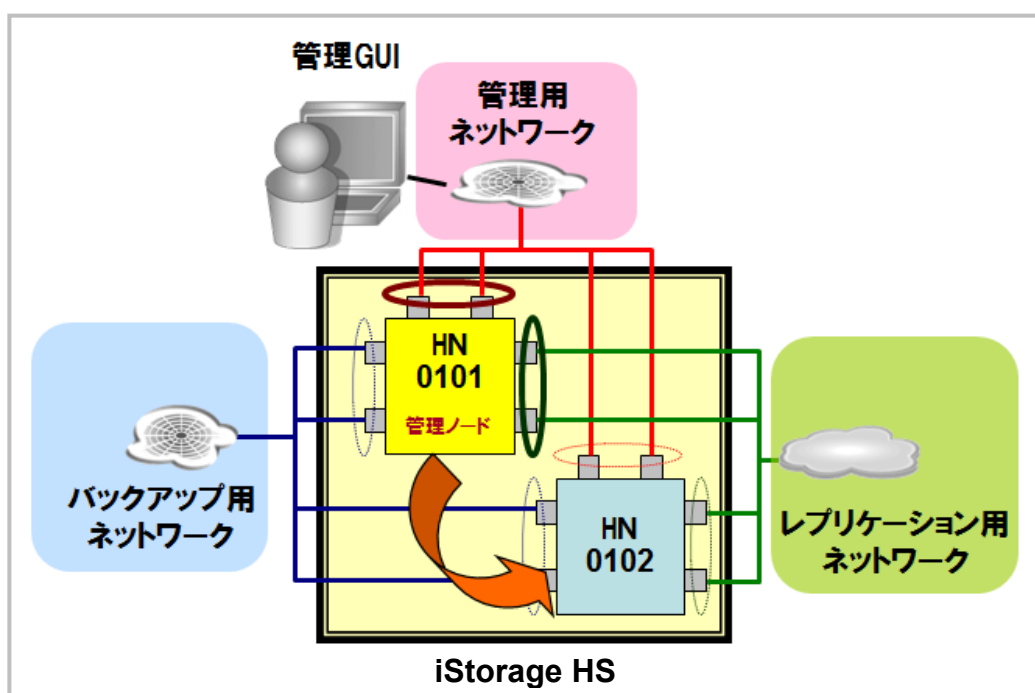


図 2-19 ネットワーク分離時の障害動作
(スケールアウトモデル)

Note ローカルサイトとリモートサイトのシステム間でレプリケーション制御通信を行うアクセラレータノード機能を持つノードに障害が発生した場合、代替ノードによって通信可能とするため、レプリケーション用外部フローティング IP アドレスを使用してシステム間の通信を行います。

レプリケーション用ネットワークの接続（シングルノードモデルの場合）

本製品は、GUI 操作用の管理 LAN とレプリケーション制御通信用のレプリケーション制御 LAN(WAN)を、異なるネットワークとして接続することができます。そのため、データセンタなどの管理 LAN が分離された環境においてもレプリケーションが利用可能です(図 2-20)。

管理 LAN とレプリケーション制御 LAN(WAN)のネットワークを分離するには、ローカルシステムに GUI 操作用のポートとレプリケーション用のポートを準備し、それぞれのポートには外部 IP アドレスを設定します。「レプリケーション用ポート」にはレプリケーション用の外部 IP アドレスを設定したポートを選択します。また、リモートサイトのシステムに本機情報を登録（リモートシステム登録）する際は、「レプリケーション用ポート」に設定したポートの外部 IP アドレスを登録します（図 2-21）。

外部 IP アドレスや「レプリケーション用ポート」の設定は、システムの**外部ネットワーク**画面から設定できます。

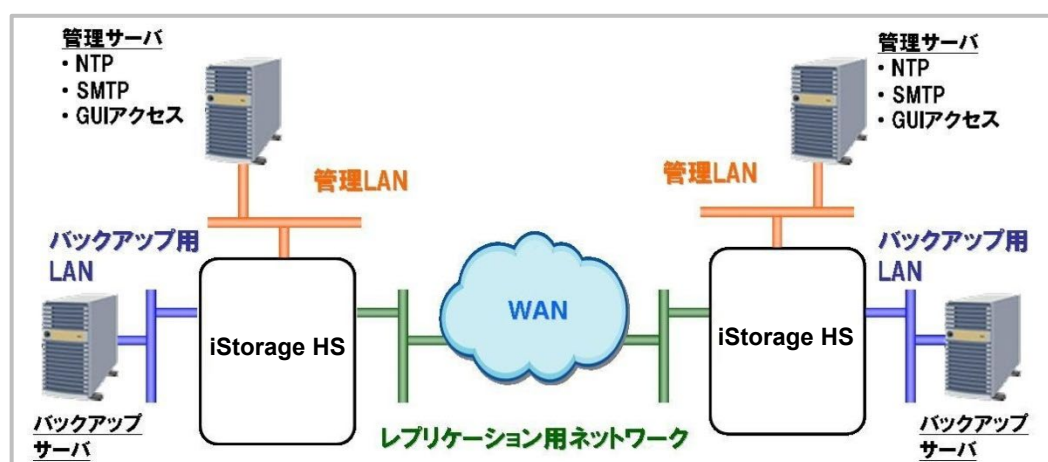


図 2-20 GUI とレプリケーションのネットワークを分離する場合（シングルノードモデル）

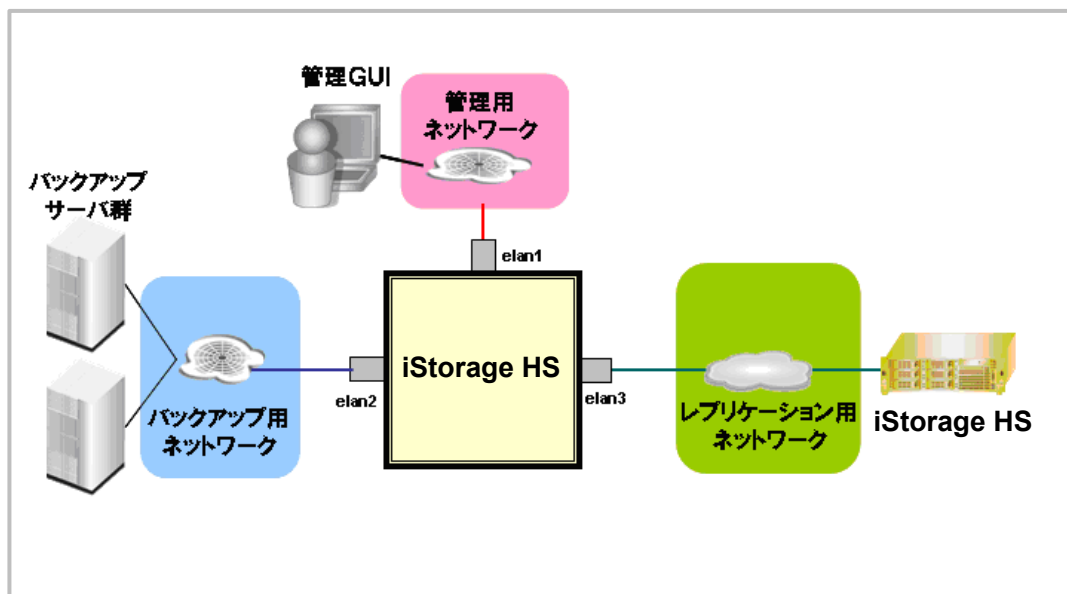


図 2-21 ネットワーク分離例（シングルノードモデル）

物理ポート数が不足した場合などは、管理 LAN とレプリケーション制御 LAN(WAN)を共用することができます。管理 LAN とレプリケーション制御 LAN(WAN)を共用してバックアップ用の LAN を分離するといったように、ネットワークすべてを共用せずに一部を分離することもできます。

管理 LAN とレプリケーション制御 LAN(WAN)を共用する場合は、ローカルシステムに GUI 操作用のポートを準備し、「レプリケーション用ポート」には GUI 操作用のポートを選択します。また、リモートサイトのシステムに本機を登録（リモートシステム登録）する際は、「レプリケーション用ポート」に設定したポートの外部 IP アドレスを登録します（図 2-22、図 2-23）。

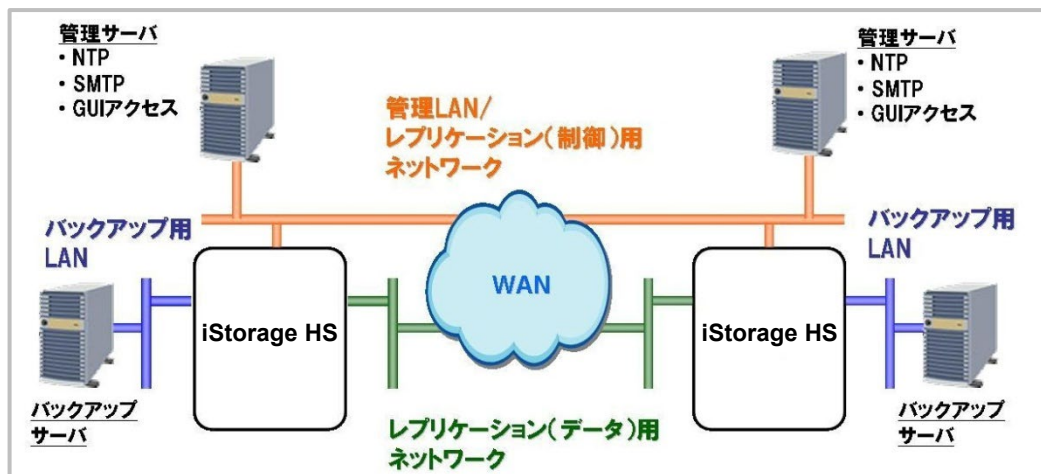


図 2-22 GUI とレプリケーションのネットワークを共用する場合（シングルノードモデル）

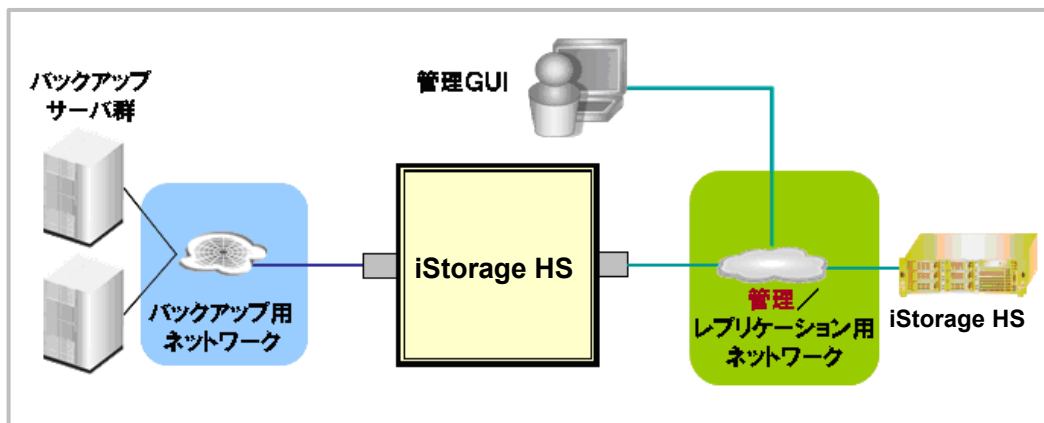


図 2-23 管理/レプリケーション用ネットワークの共用例（シングルノードモデル）

また、図 2-24 のように管理/バックアップ用のネットワークを共有し、レプリケーション用ネットワークを分離することも可能です。

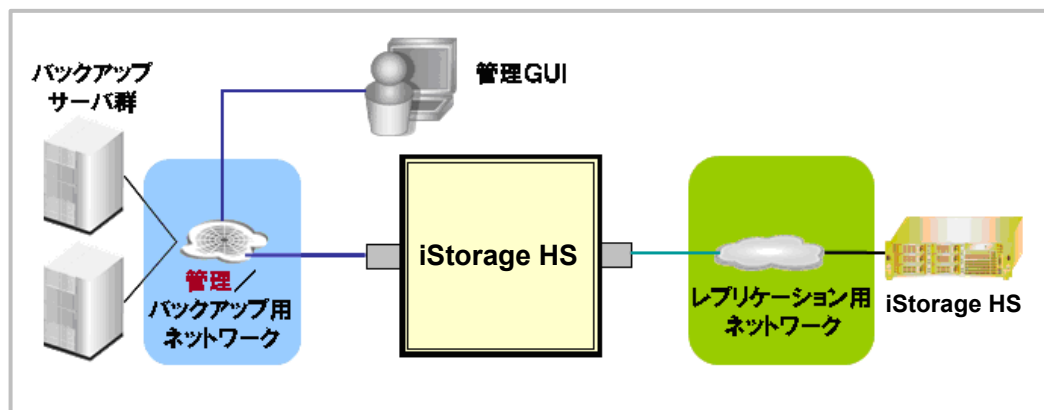


図 2-24 管理/バックアップ用ネットワークの共用例（シングルノードモデル）

Step 3. ファイルシステムの作成

ファイルシステムではこのステップで説明しているマーカーフィルタリング、WORM(Write Once Read Many)、パリティのほかに、クォータ、暗号化、非同期モードなど様々なオプションが利用可能です。ファイルシステムを作成する際には、用途に合わせた適切なオプションを利用してください。これらのオプションを利用する場合は、事前に「ユーザーズガイド」の「第4章 ファイルシステム設定の管理」および「コマンドリファレンス」の「第II編 リファレンス」の「第2章 コマンド」の「fs」を参照し、使用方法や注意事項を十分に確認してください。

ファイルシステムの計画

本製品の主な利点の1つは、ファイルシステムの作成を準備する際に、前もってファイルシステムの容量を決める必要がないということです。本製品は、容量パーティショニングの計画を立てる必要はありません。ファイルシステムが管理ユニットとしての役割を果たし、バックアップサーバを本製品にマッピングします。(アクセラレータノード機能を持つノードがある場合は、アクセラレータノード機能を持つノードにマッピングします。) ファイルシステムの作成および使用方法を最大限活用するには、以下のガイドラインに従ってください。一般的な構成は図 2-25 のようになります。

なお、アクセラレータノード機能を持つノードが2台以上あるモデルでは、協調アクセスグリッド機能を利用することで、複数のノードから同一のファイルシステムにアクセスすることが可能です。協調アクセスグリッド機能についての概要および詳細な設定方法は「協調アクセスグリッドユーザーズガイド」を参照してください。

バックアップポリシーやバックアップサーバに基づいてファイルシステムを作成します。そうすることで、データバックアップサーバが各ファイルシステムにデータを格納するタイミングや格納するデータの量を観察できます。

アクセラレータノード機能を持つノードが2台以上あるモデルでは、以下の2点についても注意してください。

- すべてのアクセラレータノード機能を持つノード間でネットワーク負荷が同じになるように、ファイルシステムをアクセラレータノード機能を持つノード間に分散させてください。1台のアクセラレータノード機能を持つノード上では、時間が異なるバックアップを組み合わせることを推奨します。この方法で、より効率的にアクセラレータノード機能を持つノードの空き時間を使用できます。

- アクセラレータノード機能を持つノード間の負荷分散を適切に設計するためには、ファイルシステムごとの使用状況を管理する必要があります。アクセラレータノード機能を持つノード間の負荷分散の設計を複雑にしないために、過大なファイルシステムを作成することは避けてください。ファイルシステムの数は一ノードあたり10個以下にしてください。

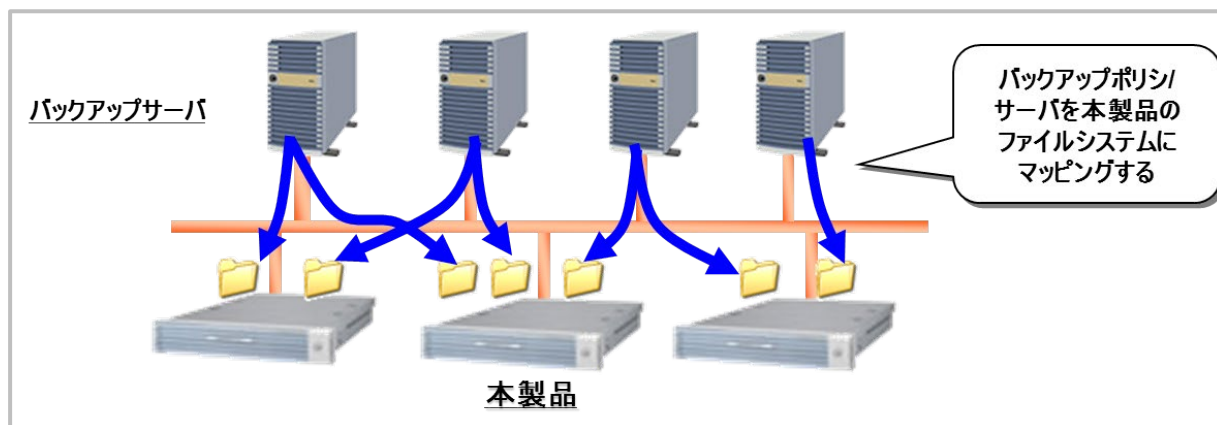


図 2-25 ファイルシステムのマッピング

ラックモデルまたはラックレスモデルで、1回のバックアップをできるだけ迅速に完了する必要がある場合は、図 2-26 のようにバックアップ用に複数のアクセラレータノード機能を持つノードを割り当てることができます。ただし、この構成は、一部のバックアップソフトウェアではサポートされていません。

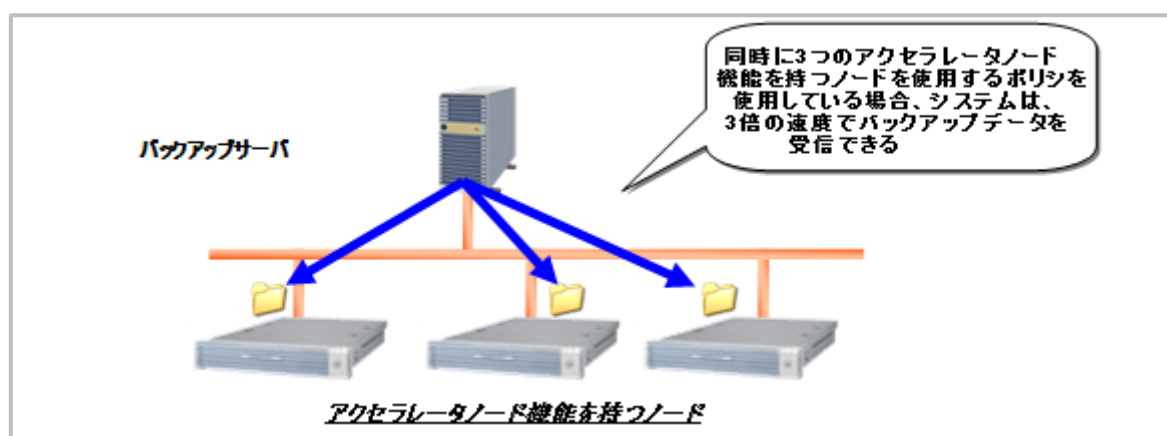


図 2-26 ファイルシステムの計画 - 性能集約型の場合

マーカーフィルタリング

バックアップソフトウェアによっては、マーカーと呼ばれるメタデータをバックアップデータに挿入します。挿入されたマーカーは、本装置に保存されるバックアップデータの圧縮率を低下させます。ファイルシステムのマーカーフィルタリングオプションは、マーカータイプに合わせて、バックアップデータ中に存在するマーカーのフィルタリングを行い、データ保存時のデータ圧縮を最適化するオプションです。マーカーフィルタリングオプションを使用する場合は、ファイルシステムの作成時にマーカーフィルタリングオプションを有効に設定し、使用するバックアップソフトウェアに対応するマーカータイプを選択します。サポートしているマーカータイプは表 2-19 の通りです。

Note ファイルシステムの作成後は、マーカーフィルタリングの設定を変更することはできません。

Note 使用するバックアップソフトウェアに対応するマーカータイプを選択しなかった場合、圧縮率は向上しません。また、マーカーフィルタリングを使用しないファイルシステムに比べ、性能が低下します。

Note レプリケーションを使用する場合、レプリカのファイルシステムには、マスタのファイルシステムと同じマーカーフィルタリングの設定が使用されます。

表 2-14 サポートするバックアップソフトウェア

マーカータイプ	バックアップソフトウェア
NBU1	Veritas NetBackup
CVS1	Commvault
TSM1	IBM Spectrum Protect
NW1	EMC NetWorker
DP1	Data Protector
RM1	Oracle Recovery Manager
SSR1	Veritas System Recovery
ARC1	Arcserve Backup

バックアップソフトウェア側の設定を、本製品との組み合わせに適した設定に変更することで、よりマーカーフィルタリングの効果を高めることができます。各バックアップソフトウェアの設定については、「[付録 D バックアップソフトウェアの設定](#)」を参照してください。

WORM (Write Once Read Many)

法令や運用規則により、ファイルが一定期間確実に保持されるよう、ファイルを WORM メディアに保存する場合があります。そのような場合は、改ざん防止機能が提供する WORM 対応ファイルシステムにファイルを保存してください。WORM 対応ファイルシステムは、ファイルを、一定期間改ざんや削除から保護します。

WORM 対応ファイルシステムは、従来のファイルシステムと同様に、NFS クライアントや CIFS クライアントからアクセスできます。

Note ユーザや WORM 機能に対応したアプリケーションは、WORM 対応ファイルシステム上のファイルをクライアントから操作することで、ファイルの保護を開始できます。この操作を実行するには、「ユーザズガイド」の「第14章 WORM (Write Once Read Many)」を参照してください。

WORM に対応したアーカイブソフトウェアで、ファイルをアーカイブし、一定期間保護する場合は、アーカイブ先に本製品の WORM 対応ファイルシステムを指定してください。アーカイブソフトウェアが自動的に、ファイルの保護を開始します。

ユーザによる直接操作で、ファイルをアーカイブする場合は、ファイルを WORM 対応ファイルシステムにコピーしてから、保護を開始してください。この操作を実行するには、「ユーザズガイド」の「第14章 WORM (Write Once Read Many)」を参照してください。

意図せずファイルが保護されないよう、以下の設定を推奨します。

- WORM 機能に対応したバックアップソフトウェアやアーカイブソフトウェアの WORM データの保存先に、WORM 対応ファイルシステムを指定してください。それ以外のデータや、WORM に対応していないアプリケーションのデータの保存先に、WORM 対応ファイルシステムを指定しないでください。
- WORM 対応ファイルシステムを、ユーザが直接操作する場合、WORM 対応ファイルシステムは、アーカイブ用途に限定してください。業務で使用しているファイルシステムから、WORM 対応ファイルシステムにファイルをコピーし、保護を開始する運用を推奨します。

- WORM 対応ファイルシステムを複数のクライアントで同時にアクセスする場合、WORM 対応ファイルシステムは、読み取り専用のモードでエクスポートしてください。データを保存するために、1 クライアントからアクセスする場合のみ、読み書きのモードでエクスポートすることを推奨します。

Note WORM 対応ファイルシステム上のファイルを、複数の CIFS クライアントから同時に更新すると、一部の操作は実際には失敗しているにもかかわらず、成功のステータスで終了することがあります。その結果、該当のファイルのリストアが正常に行われな可能性がります。

Note バックアップソフトウェアが生成したファイルを WORM 対応ファイルシステムにコピーする場合、ファイルシステム作成時に、バックアップソフトに応じたマーカーフィルターを設定することを推奨します。

WORM 対応ファイルシステムは、表 2-20 の属性を設定することで、作成可能です。WORM の属性は、法令や運用規則に従い決定します。

表 2-15 WORM 属性

属性	説明
WORM タイプ	Compliance と Enterprise の 2 種類があります。WORM ファイルシステム作成時にどちらかを選択します。
デフォルト保護期間	WORM ファイルのデフォルト保護期間です。保護期間が設定されていないファイルは、保護開始時にデフォルト保護期間が設定されます。この属性は、WORM 対応ファイルシステム作成時に必ず指定します。
最小保護期間	WORM ファイルの最小保護期間です。最小保護期間より保護期間が短くならないように、ファイルの保護開始時に、保護期限が補正されます。最小保護期間を指定していない場合の保護期間は 1 日です。
最大保護期間	WORM ファイルの最大保護期間です。最大保護期間より保護期間が長くならないように、ファイルの保護開始時に、保護期限が補正されます。最大保護期間を指定していない場合の保護期限は、2100 年(GMT)までとなります。

WORM には、Compliance と Enterprise の 2 種類のタイプがあります。各タイプの特徴は表 2-21 の通りです。法令や運用規則に従い、どちらかを選択してください。

表 2-16 WORM タイプ

WORM タイプ	説明
Compliance	保護期間中の WORM ファイルが存在する間、ファイルシステムは削除できません。法令により厳しく規制された環境では、 Compliance を指定してください。
Enterprise	保護期間中の WORM ファイルが存在する場合でも、特権管理者ロールがコマンドラインインタフェース(CLI)を実行することで、ファイルシステムを削除できます。詳細は「コマンドリファレンス」の「第II編 リファレンス」の「第2章 コマンド」の「fs」を参照してください。保護期間内のファイルが削除できる環境では、 Enterprise を指定してください。法令により厳しく規制された環境では、 Compliance を指定してください。

WORM 対応ファイルシステム上のファイルは、それぞれ一定期間保護されます。本製品は、1 日から 100 年の保護期間を設定可能です。

WORM 属性の最小/最大保護期間を設定することで、保護期間の有効範囲を制限できます。詳細は、図 2-27 を参照してください。

デフォルト/最小/最大保護期間は、WORM 対応ファイルシステム作成後も変更可能です。変更後の保護期間は、次の保護開始時に有効となります。

WORM 対応ファイルシステム上のファイルを、ユーザによる直接操作で保護を開始する場合、誤った保護期間を設定しないよう、最小/最大保護期間を設定することを推奨します。

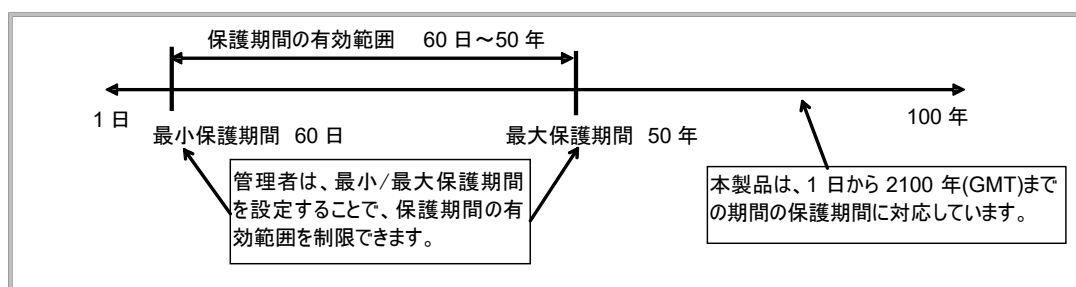


図 2-27 ファイルの保護期間の有効範囲

Note ファイルシステムの保護期間は 100 年まで設定可能ですが、実際の保護期間は 2100 年(GMT)までです。そのため、2100 年を超える保護期限を設定しても、2100/12/31 23:59:59 GMT と設定されます。

WORM 対応ファイルシステム上のファイルには、それぞれ、保護期間満了日時となる保護期限を設定できます。保護期限が設定されていないファイルは、保護開始時に、WORM 対応ファイルシステムに設定されているデフォルト保護期間から計算した保護期限が付与されます。ファイルの保護期限の設定手順は、「ユーザズガイド」の「第14章 WORM (Write Once Read Many)」を参照してください。

法令や運用規則により保護期間が異なるファイルを保管し、ユーザが直接操作でファイルを保護する運用の場合、各法令や運用規則に準拠するデフォルト保護期間の WORM 対応ファイルシステムを作成し、ファイルを保管する運用を推奨します。

WORM に対応したアプリケーションでの運用の場合は、アプリケーションの説明書に従い、WORM 対応ファイルシステムを作成してください。

パリティ

パリティ数は格納データの冗長性をあらわす指標です。一般的に一度に失うことのできるディスクの数を指します。たとえば、パリティ数が3の場合、格納データの欠損なしに3個のディスクまで失うことができます。各パリティ数がどれだけの数の障害に耐えることができるかは、表 2-22、表 2-23、表 2-24 を参照してください。一方、パリティ数を増やすと、同じデータを格納するのに必要となるディスク領域は増えてしまいます。格納データ全体に対して、冗長性を持たせるためにシステムが付与したデータの割合が、**オーバーヘッド**です。各パリティ数がどれだけのオーバーヘッドを有するかは、表 2-23、表 2-24 を参照してください。表 2-23、表 2-24 を参照し、運用方針に適したパリティ数を選択してください。

- iStorage HS Virtual Appliance

iStorage HS Virtual Appliance では、ファイルシステムのパリティ数は0です。

データのパリティ数を目的として、ハードウェア RAID 構成を有する物理ディスクを作成することを推奨します。

- 1 ノード構成、複数ノード構成

表 2-23 および表 2-24 を参照してください。

表 2-17 パリティ数、オーバーヘッドと耐障害性の相関 (2/3)

レベル	パリティ数	オーバーヘッド	1 ノード構成	2 ノード構成	
			ディスク障害の数	SN/HN 障害の数	ディスク障害の数
高 ↑ ↓ 低	6	50%	6	1	6
	5	42%	5	0	5
	4	33%	4	0	4
	3	25%	3	0	3
	2	17%	2	0	2
	1	8%	1	0	1

表 2-18 パリティ数、オーバーヘッドと耐障害性の相関 (3/3)

レベル	パリティ数	オーバーヘッド	4 ノード構成		10 ノード構成		20 ノード構成	
			SN/HN 障害の数	ディスク 障害の数	SN/HN 障害の数	ディスク 障害の数	SN/HN 障害の数	ディスク 障害の数
高 ↑ ↓ 低	6	50%	2	6	4	6	6	6
	5	42%	1	5	3	5	5	5
	4	33%	1	4	2	4	4	4
	3	25%	1	3	1	3	3	3
	2	17%	0	2	1	2	2	2
	1	8%	0	1	0	1	1	1

Note 表 2-23、表 2-24 に記載されていない構成に関しては、担当営業または担当 SE にお問い合わせください。

なお、ノード障害やディスク障害が発生すると、表 2-23、表 2-24 の耐障害性の範囲内でも必ず数分間の無応答時間が発生しますので注意してください。この間は書き込みや読み込みの応答が無くなるため、ジョブのタイムアウト値が小さい場合、タイムアウトを引き起こす可能性があります。ほとんどのケースでは無応答時間は 1～2 分ですが（3 分を超えることはほとんどありません）、パリティ数が 6 の場合に限界数のノード障害が同時に発生すると、最大で 7～8 分の無応答時間が発生する場合があります。

また、ノード障害時は通常時に比べて少ない台数で処理するため、書き込み性能が最大 50%（ノード数および重複率に依存）低下します。なおかつ、ノード障害発生からリカバリ処理（処理量は格納データ量に依存）が無くなるまでの間は、さらに最大 25%（ノード数およびパリティ数に依存）低下します。この一時的な性能低下により、9 時間／日以上運用を行っている場合、その日の運用が終わらなくなる可能性があります。

ファイルシステムのエクスポートタイプ

本製品は、ファイルシステムのエクスポートタイプとして、CIFS、NFS、OST の3種類をサポートしています。

- CIFS

iStorage HS のファイルシステムに CIFS 経由でアクセスします。CIFS を利用する場合は、認証方式を選択できます。本製品でサポートしている CIFS の認証方式は、ワークグループ（共有）、Active Directory、ワークグループ(LDAP)の3種類です。詳細は「[CIFS の認証方式](#)」を参照してください。

- NFS

iStorage HS のファイルシステムに NFS 経由でアクセスします。

- OST

OST ファイルシステムは、Veritas NetBackup の OST (OpenStorage)機能を使用する場合に作成します。詳細は「*OpenStorage(OST) ユーザーズガイド*」を参照してください。

CIFS の認証方式

CIFS 経由でファイルシステムにアクセスするユーザにどの認証方式を適用するかを決めます。本製品は以下の認証方式をサポートしています。

- ワークグループ（共有）
iStorage HS に設定したパスワードを知っているユーザが対象です。
- Active Directory
Active Directory に登録および認証されたユーザが対象です。

Note 本製品は、NTFS 相当のアクセス制御リスト（Access Control List、以降 ACL）をサポートしています。ACL を使用する場合は Active Directory を使用してください。なお、ファイルやフォルダへのアクセス履歴をログに記録する監査機能についてはサポートしていません。

次に、各認証方式のネットワーク構成について説明します。

認証方式としてワークグループ（共有）を使用する場合のネットワーク構成は図 2-28 のようになります。

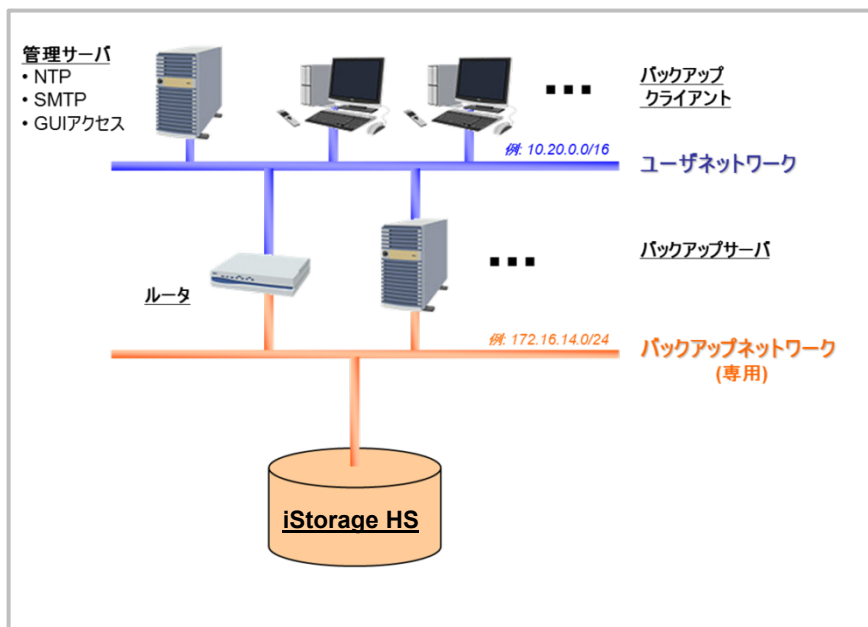


図 2-28 ネットワーク構成(1/2)

認証方式として Active Directory を使用する場合のネットワーク構成は図 2-29 のようになります。

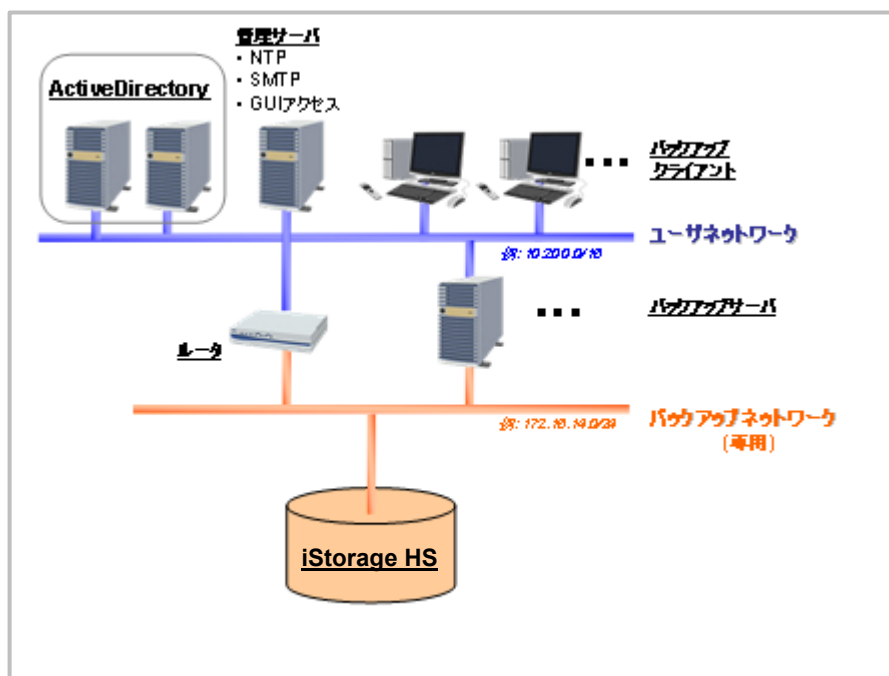


図 2-29 ネットワーク構成(2/2)

ファイルシステム参照制限

本製品はアクセス権がないクライアントがファイルシステムの存在を認識できない（参照できない、アクセスできない）ようにする機能を提供しています。

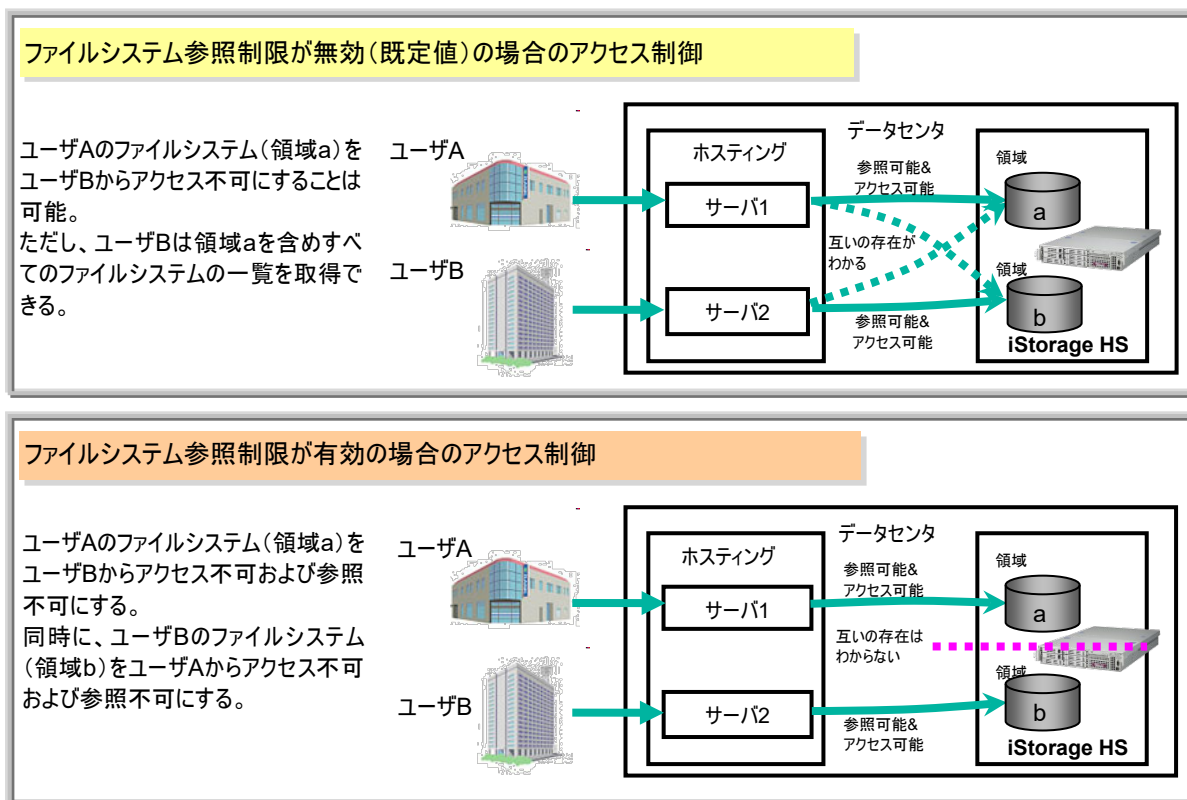


図 2-30 ファイルシステム参照制限

Note CIFS の場合、ファイルシステム参照制限は認証方式がワークグループ（共有）のみ使用可能です。

Step 4. メール通報の設定

本製品は、イベントメッセージやサービス統計情報をメールで送信する機能をサポートしています。この機能をそれぞれイベントレポート、システムレポートと呼びます。

なお、イベントレポートとシステムレポートを使用するためには、メールサーバの設定が必要となります。メールサーバに SMTP 認証を使用することも可能です。

Note 詳細な設定手順は「ユーザズガイド」の「第5章 システム設定」を参照してください。

イベントレポート

イベントレポートは、運用中のシステムで発生したイベントを即座にユーザにメールで知らせる機能です。この機能により、システムの状態をリアルタイムで監視することができます。本製品では、イベントメッセージには、Emergency、Alert、Warning、Information の4つのレベルがあります。詳細は表 2-25 を参照してください。

表 2-19 イベントメッセージのレベル

レベル	種類	状態
↑ ↓	Emergency	重大な問題が発生したため、システムが停止しました。緊急に対処が必要ですので、すぐにテクニカルサポートに連絡してください。
	Alert	問題が発生したため、システムの一部が停止しました。対処が必要ですので、テクニカルサポートに連絡してください。
	Warning	問題が発生しましたが、システムは機能しています。対処方法に従って、対処を実施してください。問題が解決できない場合は、テクニカルサポートに連絡してください。
	Information	各種情報イベントです。対処は必要ありません。本イベントは、各種操作をした場合やシステムに変更があった場合などに通知されます。

また、宛先ごとにどのレベルのイベントメッセージを送信するかを指定するために、送信レベルが設定できます。イベントレポートは、送信レベルとして指定されたレベル以上のイベントメッセージを送信します。送信レベルについての詳細は表 2-26 を参照してください。

表 2-20 イベントレポートの送信レベル

送信レベル	送信するイベントメッセージ	予想されるユーザの役割
Information or above	以下の 4 種類のイベントメッセージすべて - Emergency - Alert - Warning - Information	サービスがインストールされる前、たとえば、システムテスト時のシステムインテグレータ
Warning or above	Warning レベル以上のイベントメッセージ - Emergency - Alert - Warning	予防保守を計画するために、システムの性能低下を把握する必要があるマネージャや管理者
Alert or above	Alert レベル以上のイベントメッセージ - Emergency - Alert	システムの可用性を把握する必要がある IT 部門の上級マネージャ
Emergency	以下のイベントメッセージ Emergency	

システムレポート

本製品は、過去のイベントメッセージ、性能情報、システム構成情報、メンテナンス情報を採取してシステムレポートを作成し、送信することができます。また、曜日と時間帯を指定して、自動的に毎週のシステムレポートを作成、送信することも可能です。

Step 5. NTP サーバの計画

本製品を正しく運用するためには、本製品を構成するすべてのノードの時刻を同期させる必要があります。ノードの時刻を正確に同期させるためには、以下の構成を推奨します。

- 複数(3 台)の NTP サーバを構成し、冗長性を持たせること
- 上位のタイムソースは共通とし、信頼のおけるものであること

詳細は「ユーザズガイド」の「第5 章 システム設定」の「NTP サーバを設定する」を参照してください。

Note NTP サーバの設定を変更（追加/削除/変更）した場合は、設定を反映するためにシステムを再起動してください。

Note NTP サーバ側で UDP の 123 番ポートに対する送受信を許可するように設定してください。

Note Windows サーバを NTP サーバにする場合は、Windows タイムサービスを NTP サーバとして設定してください。SNTP サーバとして設定した場合、同期しません。設定例については、「[Windows サーバを NTP サーバにする場合](#)」を参照してください。

Note 仮想マシンを NTP サーバとして使う場合に、本製品と NTP サーバとの時刻同期ができない場合があるため、仮想マシンの NTP サーバを利用しないでください。

AN クラスタを構成している場合は、GUI 操作の管理ノードから到達できるネットワーク上に NTP サーバを構成することを推奨します。

Note この構成を取らないと、アクセラレータノード機能を持つノードがフェイルオーバーした場合に、本製品と NTP サーバとの時刻の同期ができなくなる場合があります。ただし、その場合でも本製品のノード間の時刻の同期は維持されます。

Note NTP サーバを仮想システム上に構成しないでください。

Note システム上に DNS が構成されていて、NTP サーバをホスト名で指定する場合、複数 IP アドレスを持つホスト名を使用しないでください。

NTP サーバの構成例

本製品における NTP サーバの計画について、以下 3 つのケースを例に説明します。環境に応じていずれかの構成を設計してください。

1. LAN/Active Directory(AD)ドメインの外部にある信頼のおけるタイムソースが利用できる場合
2. LAN/AD ドメインの中に信頼のおけるタイムソースを構築する場合
3. NTP サーバの冗長構成ができない場合

ケース 1: LAN/AD ドメインの外部にある信頼のおけるタイムソースが利用できる場合

LAN/AD ドメインの外部にある信頼のおけるタイムソースが利用できる場合、そのタイムソースと同期している NTP サーバを構成してください（図 2-31）。

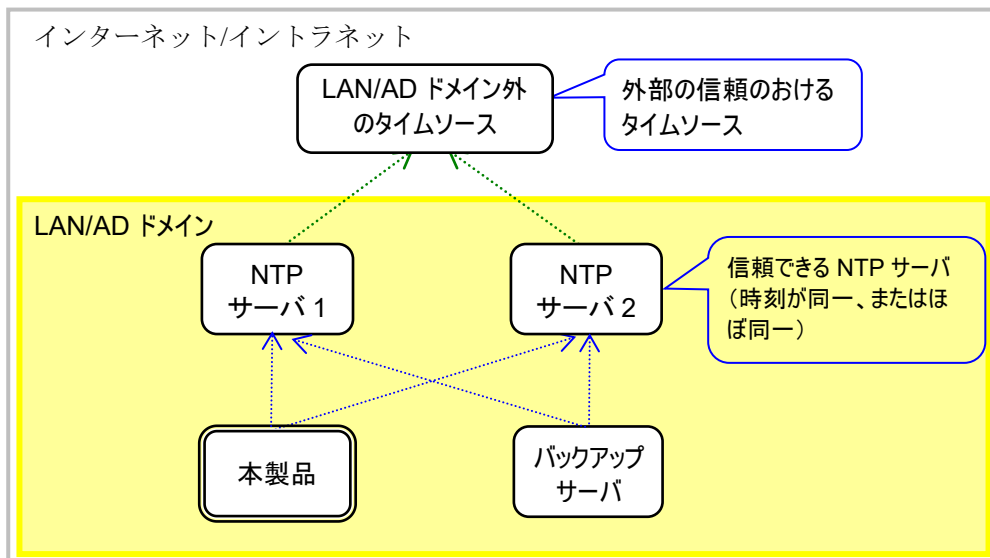


図 2-31 サーバの構成例（ケース 1）

ケース 2: LAN/AD ドメインの中に信頼のおけるタイムソースを構築する場合

外部の信頼のおけるタイムソースが利用できない場合は、LAN/AD ドメインの中に信頼のおけるタイムソースを 1 台用意します。このタイムソースと同期する NTP サーバを構成してください（図 2-32）。

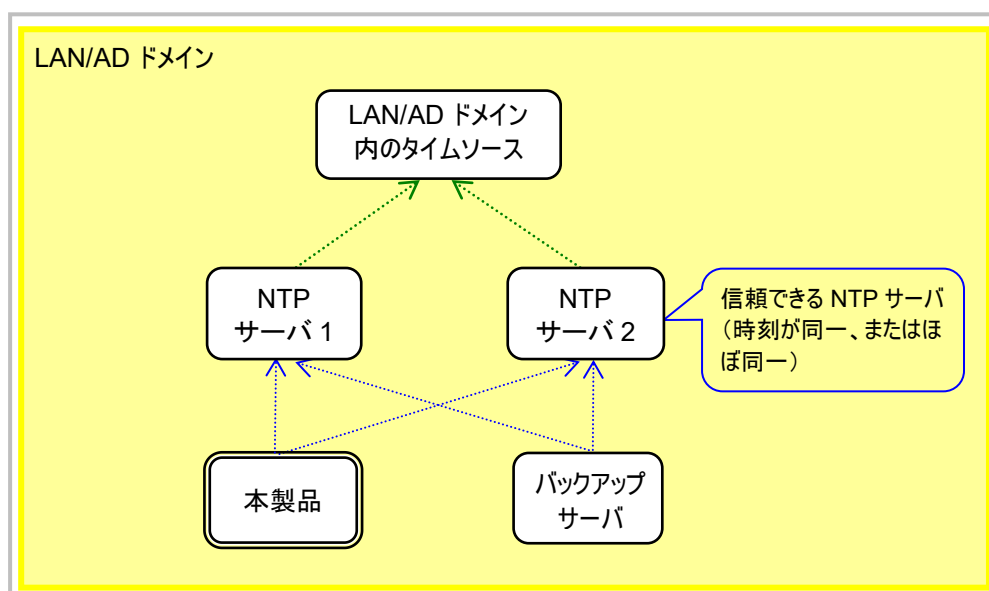


図 2-32 サーバの構成例（ケース 2）

ケース 3: NTP サーバの冗長構成ができない場合

LAN/AD ドメインの中に信頼のおけるタイムソースを構築するが、ケース 2 のように NTP サーバの冗長構成ができない場合は、LAN/AD ドメイン内の NTP サーバのシステム時刻と同期する構成を設計します（図 2-33）。

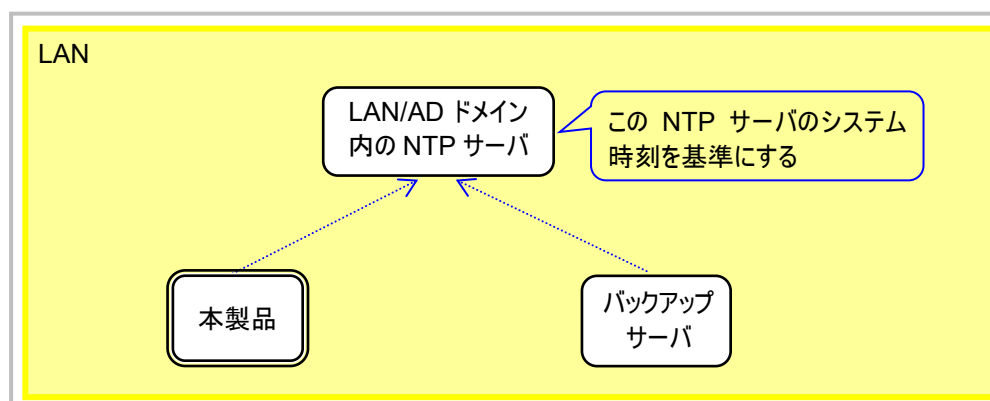


図 2-33 サーバの構成例（ケース 3）

図 2-33 のような構成にするには、LAN 内の NTP サーバの `server`、`fudge` パラメータを図 2-34 のように設定してください。

```
(/etc/ntp.conf の設定内容（抜粋）)
:
server 127.127.1.1
fudge 127.127.1.1 stratum 1
:
```

図 2-34 LAN/AD ドメイン内の NTP サーバの設定例

すでに `server 127.127.1.0` が設定されている場合、上記設定に**変更**してください。
`server 127.127.1.0` が設定されていない場合、上記設定を**追加**してください。

Windows サーバを NTP サーバにする場合

Windows タイムサービスのグループ・ポリシー・オブジェクト(GPO)の使用の有無により、2 通りの設定方法があります。以下の 1.または 2.のいずれかの手順で設定を行ってください。

Note 本製品では、Windows Server 2003 以降のバージョンの Windows Server を NTP サーバとして使用することができます。

Note 本節の操作は Administrator 権限のアカウントで実施してください。

1. Windows タイムサービスの GPO を使用していない場合

w32tm コマンドとレジストリエディタを使用して、以下の(1)～(3)の手順で NTP サーバを構成します。

(1) Windows タイムサービスのパラメータ設定（タイムソース別）

使用するタイムソースに応じて、以下のいずれかを設定します。

ケース 1: AD ドメイン外部の NTP サーバから時刻情報を取得する場合

- ① コマンドプロンプトから以下を実行します。

```
w32tm /config /syncfromflags:MANUAL /manualpeerlist:<NTP サーバ>,0x1
```

<NTP サーバ> にはドメイン外部の NTP サーバのホスト名か IP アドレスを指定します。また、末尾に“,0x1”を付与してください。

- ② レジストリエディタを使って以下のレジストリ値を 900 に設定します。

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders\NtpClient\SpecialPollInterval
```

ケース 2: AD ドメイン階層に従ってタイムソースから時刻情報を取得する場合

コマンドプロンプトから以下を実行します。

```
w32tm /config /syncfromflags:DOMHIER
```

ケース 3: NTP サーバの冗長構成ができない場合

レジストリエディタを使って以下のレジストリ値を 0 に設定します。

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders\NtpClient\Enabled
```

(2) Windows タイムサービスのパラメータ設定（タイムソース共通）

(1)に続けて、以下の①②を実行します。

- ① コマンドプロンプトから以下を実行します。

```
w32tm /config /reliable:YES /LocalClockDispersion:0 /update
```

- ② レジストリエディタを使って以下のレジストリ値を 1 に設定します。

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders\NtpServer\Enabled
```

(3) Windows タイム サービスの再起動とタイムソースへの即時同期

コマンドプロンプトから以下を順次実行します。

```
net stop w32time && net start w32time  
w32tm /resync
```

2. Windows タイム サービスの GPO を使用している場合

グループ・ポリシー・オブジェクト・エディタ(gpedit.msc)を使用して、以下の(1)～(3)の手順で NTP サーバを構成します。

Note Windows タイムサービスの GPO は以下の場所にあります。

[ローカルコンピュータポリシー]－[コンピュータの構成]－[管理用テンプレート]－[システム]－[Windows タイム サービス]

Note グループ・ポリシーを階層化して管理している場合、[ローカルコンピュータポリシー]よりも優先される階層の GPO を変更する必要があります。

Active Directory の管理者に確認して、適切な階層の GPO を変更してください。

(1) Windows タイムサービスのパラメータ設定（タイムソース別）

使用するタイムソースに応じて、以下のいずれかを設定します。

ケース 1: AD ドメイン外部の NTP サーバから時刻情報を取得する場合

[タイムプロバイダ]－[Windows NTP クライアントを構成する]を開き、構成を「有効」にし、以下のパラメータを設定します。

NtpServer: <NTP サーバ>, 0x1

種類: NTP

SpecialPollInterval: 900

<NTP サーバ> にはドメイン外部の NTP サーバのホスト名か IP アドレスを指定します。

また、末尾に“, 0x1”を付与してください。

ケース 2: AD ドメイン階層に従ってタイムソースから時刻情報を取得する場合

① [タイム プロバイダ]－[Windows NTP クライアントを構成する]を開き、構成を「有効」にし、以下のパラメータを設定します。

種類: NT5DS

ケース 3: NTP サーバの冗長構成ができない場合

[タイム プロバイダ]－[Windows NTP クライアントを有効にする]を開き、構成を「無効」にします。

(2) Windows タイムサービスのパラメータ設定（タイムソース共通）

(1)に続けて、以下の①②を設定します。

- ① [グローバル構成設定]を開き、構成を「**有効**」にし、以下のパラメータを設定します。

AnnounceFlags: 5

LocalClockDispersion: 0

- ② [タイム プロバイダ]－[Windows NTP サーバーを有効にする]を開き、構成を「**有効**」にします。

(3) Windows タイムサービスの設定反映、再起動とタイムソースへの即時同期

コマンドプロンプトから以下を順次実行します。

```
gpupdate /Target:Computer
```

```
net stop w32time && net start w32time
```

```
w32tm /resync
```

Step 6. 領域解放の計画

本製品にマウントされたファイルシステム上のデータを削除しても（あるいは書き込まれたデータの保存期間が過ぎても）、本製品に格納されているデータ量がただちに減少するとは限りません。格納されているデータを削除するためには、領域解放を行う必要があります。領域解放に関する操作方法は、「ユーザーズガイド」の「第7章 システムの容量と性能」の「領域解放」および「コマンドリファレンス」の「第II編 リファレンス」の「第2章 コマンド」の「*reclamation*」を参照してください。

領域解放は、特定段階と解放段階の2段階で行われます。特定段階では、解放が可能な**解放可能領域**を特定しますが、解放はしません。解放段階で**解放可能領域**を**空き領域**として使用できるように解放します。

また、領域解放には、FG（フォアグラウンド）モードとBG（バックグラウンド）モードの2種のモードがあり、選択できます。各モードの特徴は表 2-27 を参照してください。

表 2-21 領域解放のモード

モード	説明	長所	短所
FG	特定段階中は、領域は読み取り専用になる。	最少の時間で領域を特定できる。	特定段階中は、書き込みやファイルシステムの操作ができない。
BG	特定段階中も、領域は読み書き可能。	特定段階中も、書き込みやファイルシステムの操作が可能。	特定段階中の書き込みや読み込み、ファイルシステムの操作は通常時より遅くなることがある。また、書き込みや読み込みを領域解放中に実行すると、領域解放に時間がかかることがある。

BG モードでは、領域解放の「優先度」で、領域解放が優先的に使用するリソースの割合が設定できます。領域解放の特定段階に要する時間と、領域解放の特定段階中に行われる書き込みと読み込みの性能は、「優先度」で設定した値によって変化します。

領域解放の特定段階にかかる時間を長くする原因として、以下のことが考えられます。

- 前回の特定段階完了から今回の特定段階開始までに書き込まれたデータ量が多い
- 前回の特定段階完了から今回の特定段階開始までに論理的に削除されたデータ量が多い
- 領域解放開始時のデータ量が多い
- BG モードで同時に書き込みを行っているとき、その帯域が大きく、圧縮率が小さい
- BG モードで同時に読み込みを行っているとき、その帯域が多い
- 障害などが発生した後でデータを復旧中のとき、復旧しようとするデータ量が多い
- 障害から回復した後やノードを追加した後にデータを移動中のとき、移動しようとするデータ量が多い
- BG モードで領域解放の「優先度」を設定している場合、「優先度」が低い

定期的に領域解放を自動実行させることにより、領域解放の運用管理にかかる負担を軽減できます。本製品の初期インストール時には、推奨されるスケジュールが表 2-28 のようにあらかじめ設定されています。（アップデート時には、アップデート前のスケジュールが引き継がれます。）

表 2-22 あらかじめ設定されているスケジュール

項目	設定値		
頻度	毎週	毎週	毎週
曜日	月	水	金
開始時刻	14:00	14:00	14:00
終了期限	20:00	20:00	20:00
優先度	50%	50%	50%

領域解放を行わないと不要になったデータや管理データが削除されないため、すぐに容量が枯渇します。また、領域解放を行わない期間が長くなると、次の領域解放にかかる時間が長くなります。このような事態を防ぎ、円滑な運用を行うために、領域解放のスケジュール機能を利用してください。スケジュールが未登録の場合は、画面に警告メッセージが表示され、イベントログが出力されます。

また、本製品のスケジュール機能を利用しなくても、外部のスケジューラから CLI の `reclamation` コマンドを呼び出すことで、領域解放の実行を自動化することができます。この場合は、**領域解放画面でスケジュール未登録時に警告しない**チェックボックスを選択してください。こうすることで、本製品のスケジュールが未登録でも、警告メッセージの表示も、イベントログの出力もありません。

領域解放のスケジュール作成時には、開始日時のほか、終了期限や優先度をあらかじめ設定することもできます。前述のように、データ量や圧縮率などのデータの特徴によって領域解放の特定段階にかかる時間が変動しますので、運用状況に合わせて適宜スケジュールを見直すことをお勧めします。また、あまり短い間隔で領域解放を行うと、解放段階に割り当てる時間が無くなり、1回あたりの領域解放の効果が小さくなります。領域解放を実行する頻度は1日1回にしてください。

Note 領域解放の終了期限と次の領域解放の開始時間は30分以上の間隔をあけてください。領域解放がスケジュールの終了期限を過ぎた場合はキャンセルされますが、完全にキャンセルされるまで数秒から数分のタイムラグがあり、この間は次の領域解放を開始できません。

解放段階の進行状況は、**領域解放画面**ではなく、**状態画面**で**システム名**をクリックすると表示される**システム状態画面**で監視できます。CLIを使用する場合は、`reclamation` コマンドではなく、`system status show` コマンドで監視できます。バックグラウンドタスクの領域解放タスクとして、残りの処理対象データ量が表示されます。操作方法および画面の確認方法については、「**ユーザーズガイド**」の「**第6章 システムの操作と状態の監視**」の「**iStorage HS システムの状態を監視する**」および「**コマンドリファレンス**」の「**第II編 リファレンス**」の「**第2章 コマンド**」の「`system status`」を参照してください。

また、解放段階の進行状況は、**容量画面**の**解放中領域**を参照することでも監視できます（図2-35）。CLIを使用する場合は、`system capacity show` コマンドで監視できます。

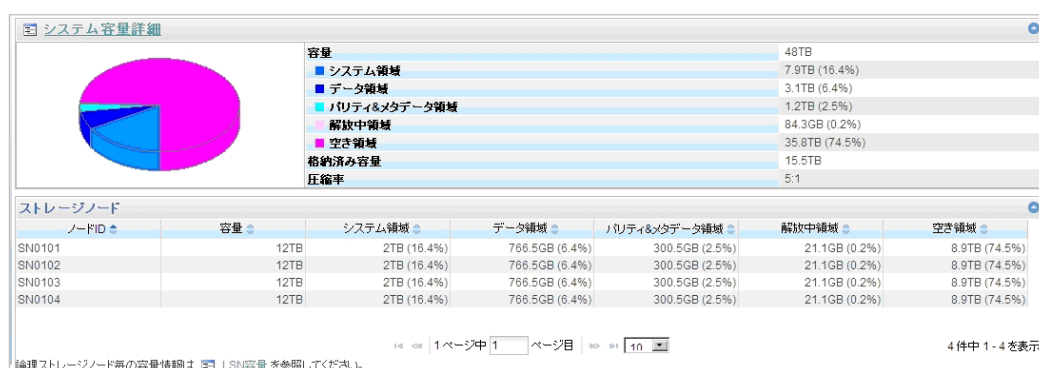


図 2-35 容量画面の解放中領域

特定段階で特定された**解放可能領域**は、特定段階までにファイルシステム上から削除したデータ量とは一致しません。一致しない原因は以下の通りです。

- **解放可能領域**にはデータに伴って解放されるパリティやメタデータも含まれる。
- **解放可能領域**に含まれるデータは、ファイルシステムに書き込まれたあと、本製品内部で圧縮されている。
- 論理的に削除対象となったデータでも、本製品内部で他のデータと重複している場合は**解放可能領域**に含まれない。

容量の監視、予測については、「[第4章 システムの監視](#)」の「[容量の監視](#)」を参照してください。

Step 7. ハードウェア障害への対策

バックアップデータを消失することなく、またサービスを止めることなく運用をするためには、障害対策が必要となります。以下に、運用中の代表的な障害と本製品の対障害用機能の対応を示します。

Note このステップは、iStorage HS Virtual Appliance には適用されません。この障害は、基盤となるホストサーバの構成によって対処する必要があります。

- **ネットワーク障害**

ネットワーク障害の対策には、ポートの **bonding** という冗長化機能を利用してください。bonding により、アクセラレータノード機能とバックアップサーバ間に冗長ネットワークリンクを確立することができます。詳細は「[Step 2. ネットワークの計画](#)」の「[バックアップネットワークの冗長性](#)」を参照してください。

- **HDD 障害**

HDD 障害が発生した場合でも、ストレージノード障害と同様に自動的にバックアップデータを再生成します。HDD 障害時の性能は、HDD 縮退と再生成による負荷の影響で、正常時と比較して複数ノード構成の場合で 62.5%程度、シングルノードモデルと 1HN 構成の場合で 50%程度まで低下する可能性があります。

- **装置の全壊**

運用中に自然災害などにより装置が全壊し、復旧が不可能になる可能性があります。この対策には、レプリケーション機能を利用してください。レプリケーション機能を利用することで、物理的に離れた本製品のシステム同士で、ファイルシステムの論理イメージのコピーが可能になり、装置が全壊して復旧が不可能になっても、バックアップデータの消失を防ぐことができます。詳細は「[Step 8. レプリケーションの計画](#)」を参照してください。

また、ラックモデル、ラックレスモデルの場合は、以下の障害の対策も利用が可能です。

- **アクセラレータノード機能を持つノードの障害**

アクセラレータノード機能を持つノードに障害が発生した場合、そのノードが所有するサービスが停止します。この障害に対する対策として、アクセラレータノード機能クラスタ機能を使用してください。アクセラレータノード機能クラスタを利用すると、ノードに障害が発生した場合でも、IP アドレスとファイルシステムを別のノードに引き継ぎ、サービスの停止時間を短縮することができます。

- **ストレージノード機能を持つノードの障害**

本製品は、バックアップデータに特殊なパリティを付与して、複数のストレージノード機能を持つノードに分散配置します。これにより、ノード障害が発生した場合でも、自動的にバックアップデータを再生成します。ストレージノード機能を持つノード障害時の性能は、ストレージノード機能を持つノードの台数を n とした場合、ノード縮退と再生成による負荷の影響で、正常時と比較して $(n-1)/n \times 75\%$ 程度まで低下する可能性があります。

Note 障害が発生した場合は、ただちに復旧処理を行ってください。

アクセラレータノード機能クラスタ

この節では、アクセラレータノード機能を持つノード障害の対策手段であるアクセラレータノード機能クラスタの設計について詳しく説明します。なお、アクセラレータノード機能クラスタは、アクセラレータノード機能を持つノードが2台以上あるモデルの場合のみ利用できます。

本製品は、アクセラレータノード機能を持つノード障害が発生した時、IPアドレスとファイルシステムを別のアクセラレータノード機能を持つノードに引き継ぎ、サービスの停止時間を短縮することができます。この機能をアクセラレータノード機能クラスタ（ANクラスタ）と呼び、障害が発生したノードのリソースを移動する動作を「フェイルオーバー」と呼びます。

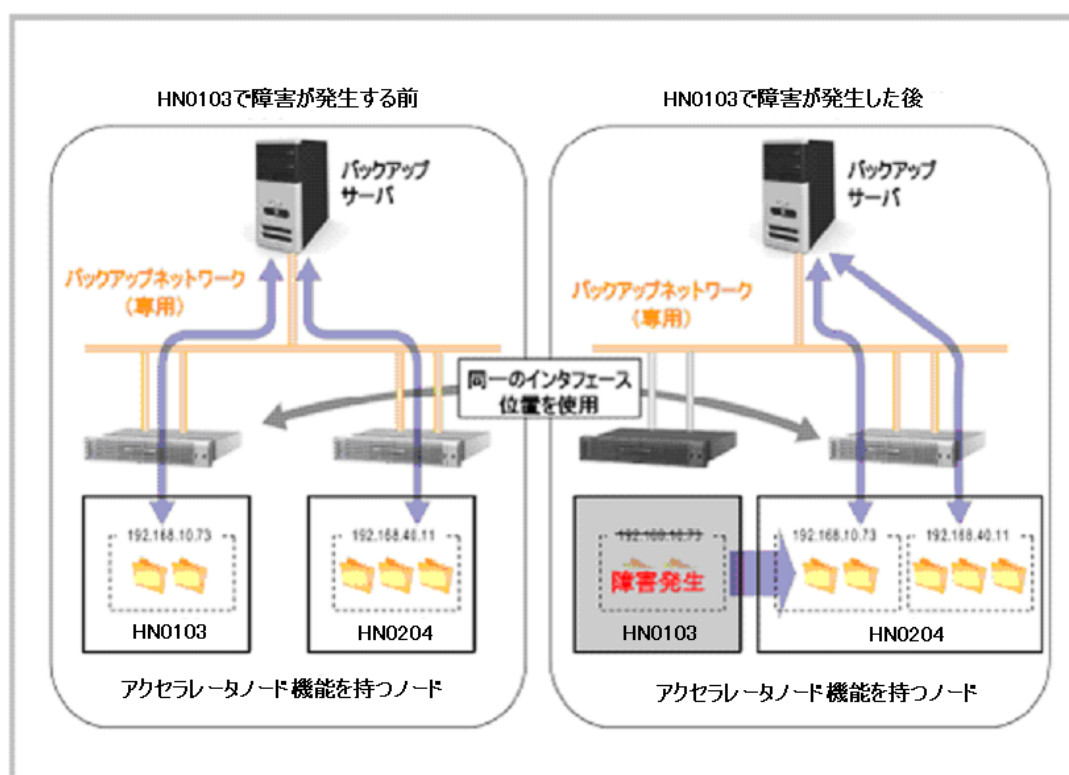


図 2-36 アクセラレータノード機能クラスタ動作イメージ

図 2-36 の例では HN0103 と HN0204 が互いにフェイルオーバー先として構成されており、HN0204 は HN0103 の故障時にその IP アドレスとファイルシステムを引き継ぎます。バックアップサーバは HN0103 の故障後しばらくすると、HN0103 が動作しているかのようにそのファイルシステムにアクセスすることができます。

AN クラスタを有効にするには、複数のアクセラレータノード機能を持つノードで構成されたグループを作成する必要があります。このグループをノードグループと呼びます。AN クラスタはノードグループ単位で機能するようになっており、各ノードのフェイルオーバーの規則はノードグループのポリシーに依存します。本製品では、ノードグループのポリシーとしてペア、N:1、サイクリック、カスタムの 4 種類をサポートしています。

表 2-23 ノードグループのポリシー

ポリシー	特徴	ノードグループの構成
ペア	2 台のノードでノードグループを構成し、互いにフェイルオーバーするように関係付けます。	ノード 2 台
N:1	ノードグループ内の任意のノードが、あらかじめ定めたフェイルオーバー先の 1 台のノードにフェイルオーバーするように関係付けます。	ノード 2 台以上
サイクリック	3 台以上のノードで構成される場合、フェイルオーバー先のノードを動的に変更するため、管理が容易で、特定のノードにフェイルオーバー先が集中することがありません。	ノード 2 台以上
カスタム	ノードごとに任意のフェイルオーバー先のノードを 1 台指定することができます。	ノード 2 台以上

上記を参照し、運用方針に適したポリシーを選択してください。なお、運用の途中にノードグループのポリシーを変えたい場合でも、運用を止めることなくポリシーの変更が可能です。ただし、フェイルオーバーしているノードがある場合、ポリシーの変更はできません。

また、フェイルオーバーを正しく動作させるには、フェイルオーバー元のノードとフェイルオーバー先のノードのネットワーク構成が同等でなければいけないことにも注意が必要です。

詳細は「[Step 2. ネットワークの計画](#)」の「[アクセラレータノード機能クラスタのためのネットワーク設計](#)」を参照してください。

前述のように、フェイルオーバーをすると、ノードのリソース（IP アドレスとファイルシステム）が別のノードに移動します。これにより、フェイルオーバー先のノードにすべてのリソースが集中し、ノードの負荷が高くなってしまうことが考えられます。したがって、AN クラスタを設計する時は、各ノード間の負荷分散についても考慮してください。

Step 8. レプリケーションの計画

本製品のレプリケーション機能は、物理的に離れた2つのシステム同士で、ファイルシステムの論理イメージをコピーできます。本製品では、以下の双方向レプリケーショントポロジをサポートしています。

- 1対1トポロジ (図 2-37)
2台のシステム間で複数のファイルシステムのレプリケーションを可能とするトポロジです。
- N対Mトポロジ (図 2-38)
複数のシステム間で複数のファイルシステムのレプリケーションを可能にするトポロジです。NとMは、スケールアウトモデルではそれぞれ50台、シングルノードモデルではそれぞれ16台まで指定できます。
- チェーントポロジ (図 2-39)
1台目のシステムから2台目のシステムへのレプリケーション、2台目のシステムから3台目のシステムへのレプリケーションを可能とするトポロジです。この構成で複数台のシステムを次々と接続することができます。

各トポロジについては、図 2-37、図 2-38、図 2-39 を参照してください。

なお、各図で示されている HN1、HN2 はアクセラレータノード機能を持つノードを示します。(シングルノードモデルの場合は、HN1 と HN2 を1つのノードとみなしてください。)
システム(A)の HN1 とシステム(B)の HN2 のように、対称でないアクセラレータノード機能を持つノード同士でもレプリケーションすることができます (図 2-37、図 2-38)。
また、シングルノードモデルと、スケールアウトモデルを組み合わせた構成でもレプリケーションが可能です。

レプリケーションは、バッチジョブとして実行されます。「レプリケーションセット」はマスタ側とレプリカ側の2つのファイルシステムを関連付け、「レプリケーションセット」単位でデータ転送スケジュールを定義します。ファイルシステムの論理イメージは、ジョブ開始時のイメージがコピーされます。この時、マスタ側(コピー元)のシステム固有のデータのみが、レプリカ側(コピー先)のシステムに送信されます。同じデータが2回送信されることがないため、レプリケーション処理は非常に効率的です。

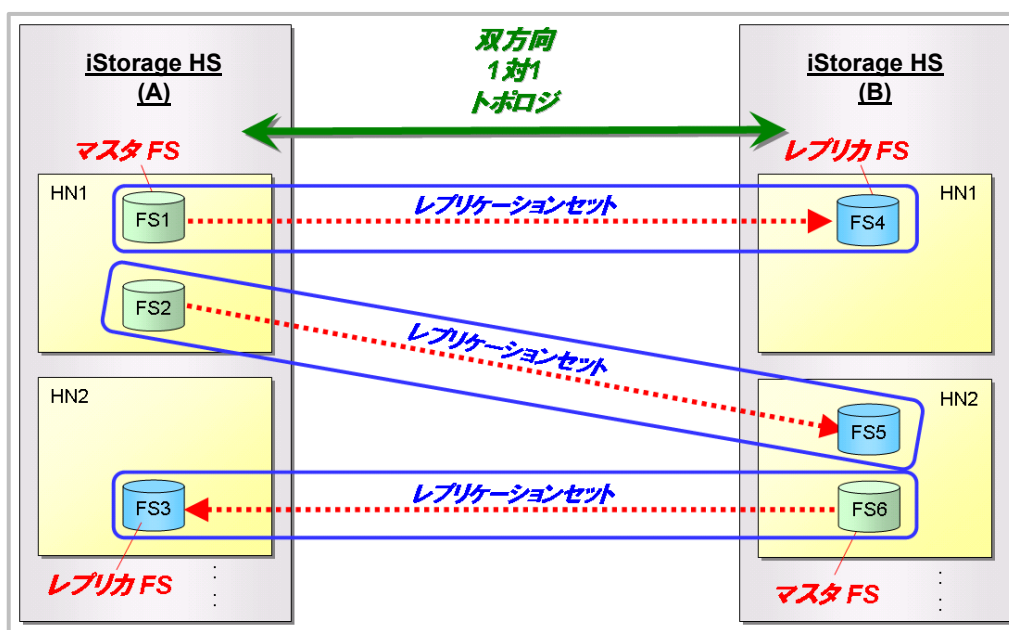


図 2-37 レプリケーショントポロジ (1 対 1)

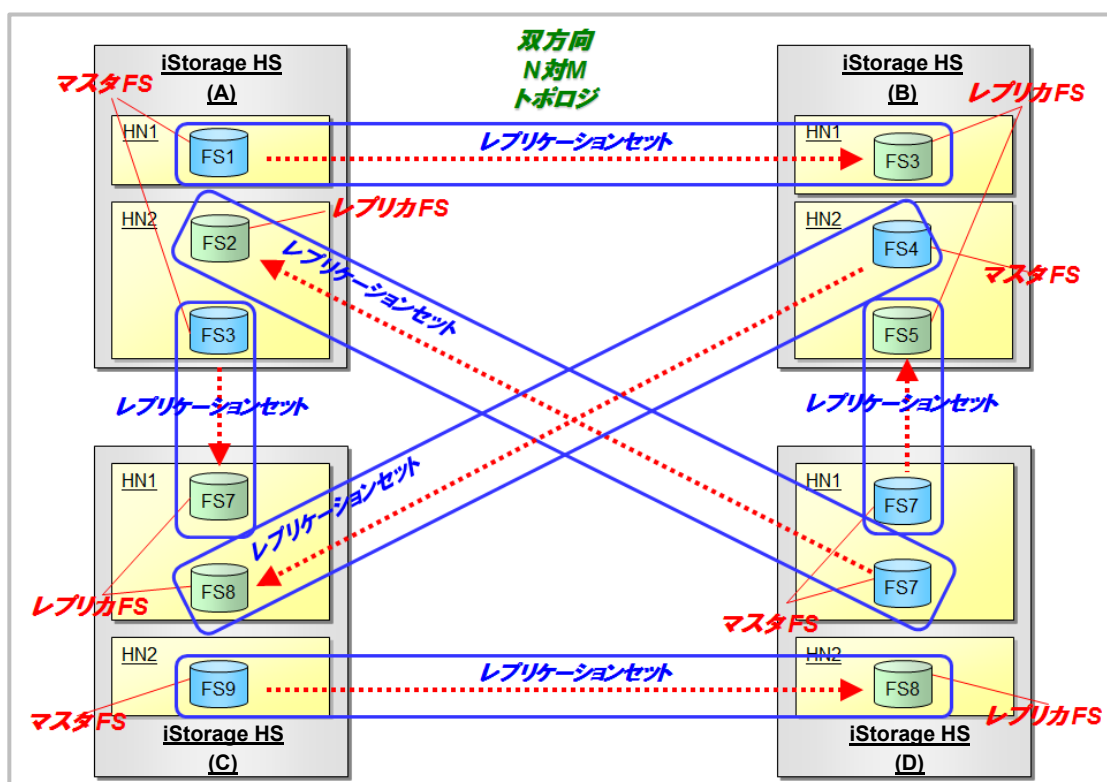


図 2-38 レプリケーショントポロジ (N 対 M)

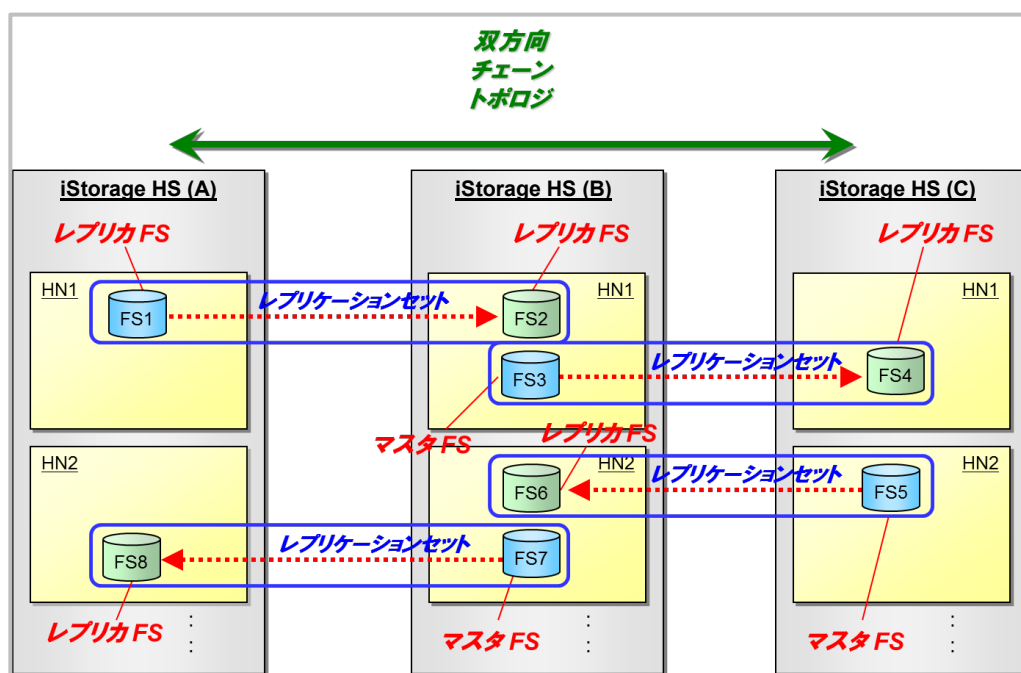


図 2-39 レプリケーショントポロジ (チェーン)

本製品のレプリケーション機能では、以下の操作が可能です。

- リモートの本製品のシステムを登録できます。
- リモートシステムごとにマスタからレプリカへのデータ転送を暗号化するかどうかを設定できます。
- 「レプリケーションセット」を定義し、論理イメージを同期する2つのファイルシステムに関連付けできます。レプリケーションセットは、レプリケーションのジョブ実行スケジュールや利用可能な帯域幅を設定することもできます。
- レプリケーションのジョブを手動実行、またはキャンセルできます。
- レプリケーションの帯域を、ノードレベルまたはシステムレベルで制御できます。
- レプリケーションに関するノードごとの統計情報を表示できます。

レプリケーションジョブの運用計画

レプリケーションジョブは、バックアップが完了した直後にスケジュール実行することを推奨します。可能であれば、レプリケーション時間も含めたバックアップウィンドウを計画してください（図 2-40 の推奨スケジュール 1）。

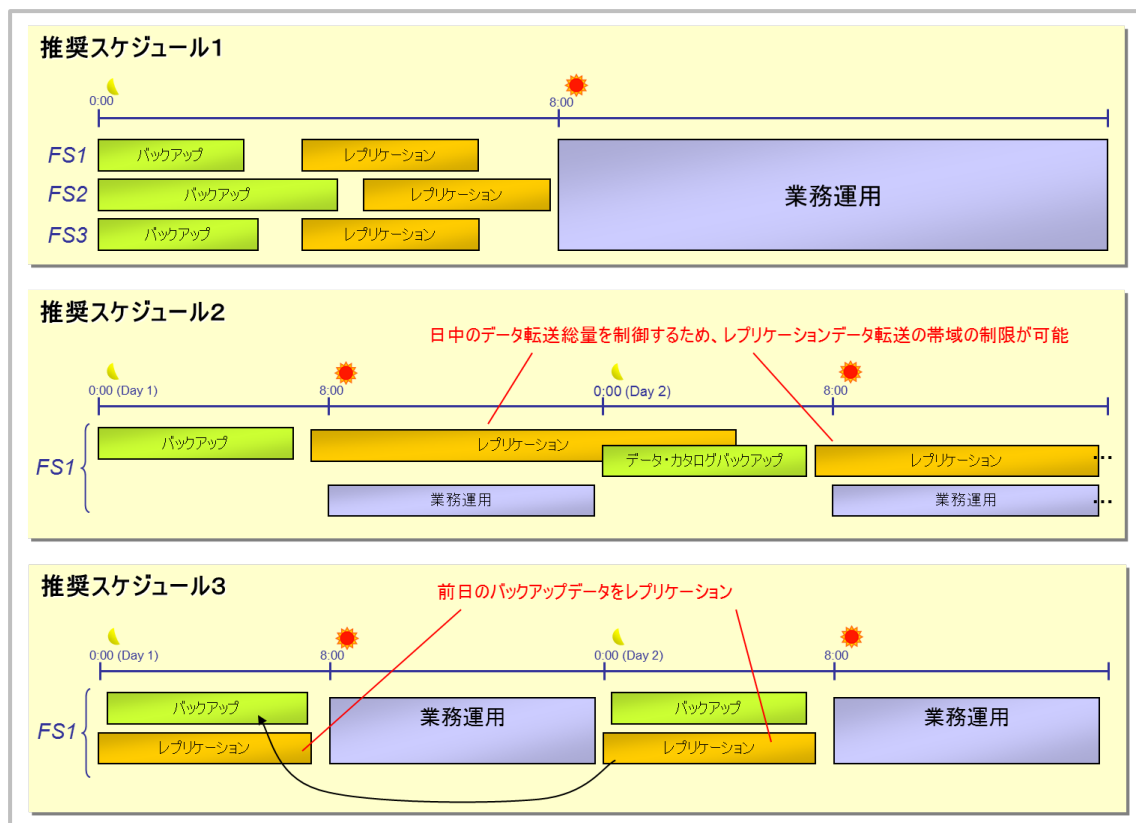


図 2-40 レプリケーションジョブの運用計画

サイト間の回線幅が十分でないなどの理由でレプリケーションが長時間にわたる場合、昼間のビジネスタイムにレプリケーションを実行することも考えられます（図 2-40 の推奨スケジュール 2）。次回のバックアップイメージに対するレプリケーションを開始するまで、レプリケーションジョブは 24 時間継続することが可能です。なお、昼間の WAN ルータへの負荷が問題になる場合は、帯域制限を設定してください。

昼間のレプリケーションが現実的でない場合、当日のバックアップデータの代わりに、前日のバックアップデータをレプリケートする運用が考えられます（図 2-40 の推奨スケジュール 3）。レプリケーションを開始してからバックアップを開始することでバックアップウィンドウとレプリケーションウィンドウを完全にオーバーラップすることが可能です。

CLI を利用したレプリケーションジョブの運用計画

レプリケーションジョブは、バックアップが完了した直後に実行することを推奨します。CLI を使用することで、バックアップ直後にレプリケーションを開始することができます（図 2-41）。

Step 1. Script の準備

バックアップ後にレプリケーションを実行する Script をバックアップサーバに準備してください。

Step 2. Script の実行

準備した Script を実行してください。リモート接続により、データのバックアップ後、続けてレプリケーションが実行されます。また、レプリケーションジョブの終了を待ち合わせ、ジョブ終了後に他の CLI（領域解放など）を実行する運用も可能です。

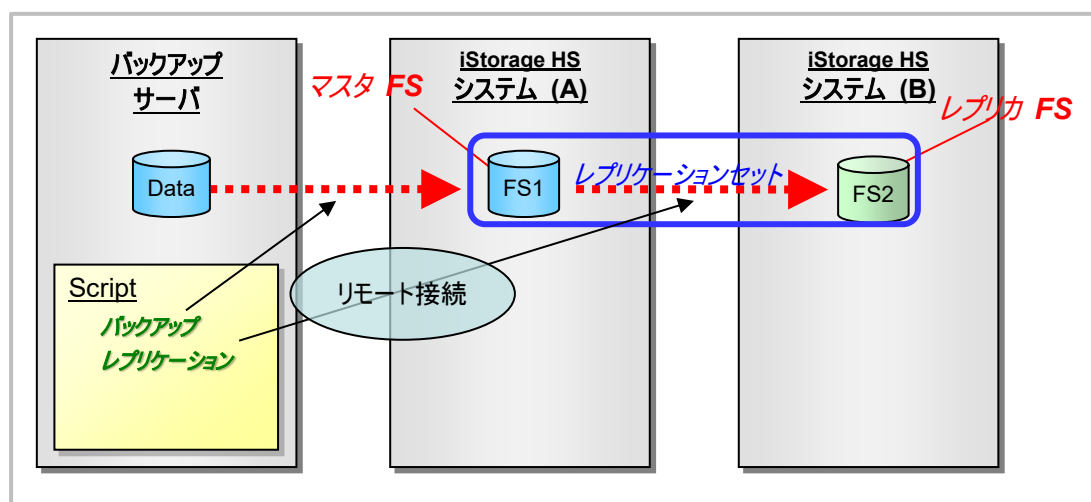


図 2-41 CLI を利用したレプリケーションジョブの運用計画

双方向レプリケーションと領域解放

BG（バックグラウンド）モードの領域解放を行っている場合は、レプリケーションジョブを開始できますが、FG（フォアグラウンド）モードの領域解放の特定段階では、レプリケーションジョブを開始できません。FG（フォアグラウンド）モードの領域解放とレプリケーションは別々のタイミングで行い、マスタ側システムとレプリカ側システムは、同じタイミングで領域解放を実施してください。マスタファイルシステムですでに開始したレプリケーションジョブは、特定段階が開始してもレプリケーションジョブを継続できます。双方向レプリケーションでレプリケーション専用のウィンドウの確保が難しい場合、この特性を利用することで問題解決できる場合があります。マスタファイルシステムのレプリケーション中に領域解放を実施してください。領域解放を BG モードで運用する場合は、これらの制約はありません。

Note 領域解放とレプリケーションを同時に実施すると、業務運用時間をより多く確保できます（図 2-42）。

Note マスタ側、レプリカ側のレプリケーションが同時に実行されている場合は、いずれかのシステムにおいても、マスタファイルシステム、レプリカファイルシステムの双方の役割でレプリケーションが動作します。このため、この場合は FG（フォアグラウンド）モードの領域解放とレプリケーションを同時に実施することはできません。

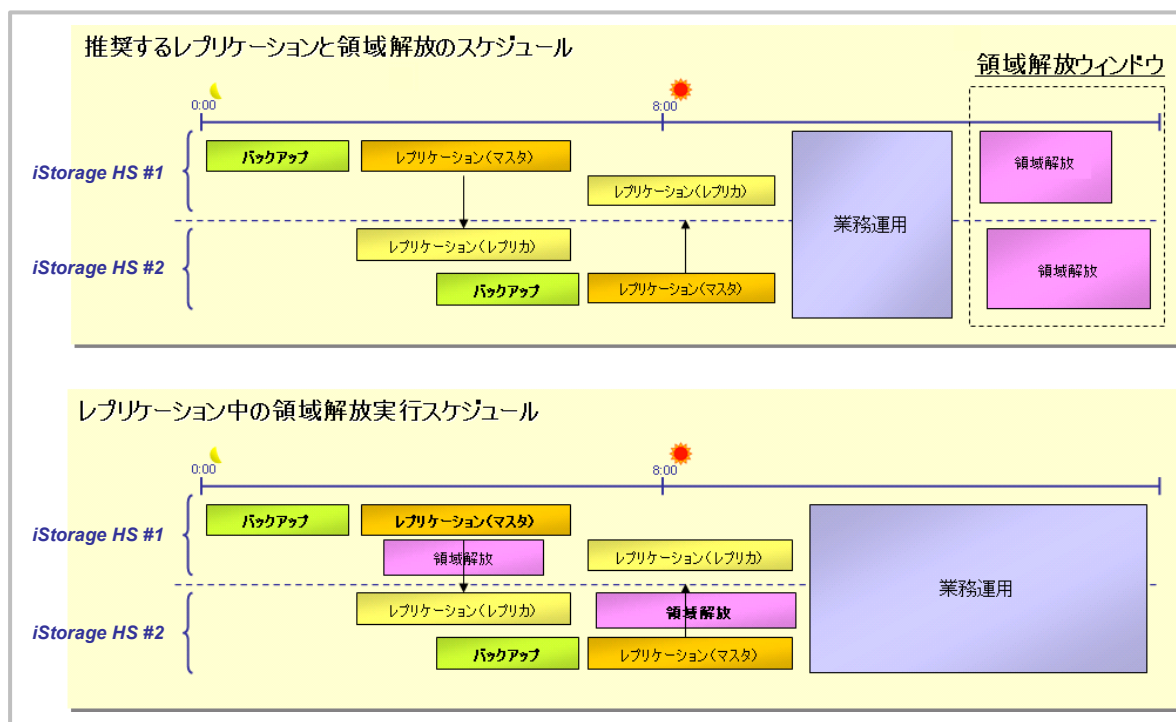


図 2-42 レプリケーションと領域解放のスケジュール

初期レプリケーションへの計画

本製品のレプリケーション機能は、日々の同期データの転送量を可能な限り削減します。しかし、1 回目のレプリケーションジョブではすべての固有なデータが転送されるので、WAN を利用する場合など、条件などを考慮の上、適切な計画を立ててください。

代表的な計画の例として、4 つのケースを説明します。

ケース 1: 一時的に 2 つのシステムを同じ場所に構築できる場合

最初に、2 つのシステムを同じ場所で構築します。レプリケーションを設定し、LAN 上で初期レプリケーションを実施してください。その後、片方のシステムをリモートサイトに移動してください。そして、WAN 経由の運用を開始してください。これによりレプリケーション時間を短縮することができます。

ケース 2: すでにシステムが遠隔地にある場合

すでに本システムを遠隔地に構築しているなどの理由で、2 台のシステムを同じ場所で運用できない場合は、初期レプリケーションを WAN で実施することも可能です。初期レプリケーションに必要な時間は、マスタファイルシステムが参照しているデータパターンの量と WAN の帯域幅に大きく依存します。十分な時間的余裕を持って、運用を開始してください。

ケース 3: すでにシステムが遠隔地にあり、レプリケーションを行うデータが大量にある場合

2 台のシステムを同じ場所で運用できず、また WAN 経由の初期レプリケーションも時間的に現実的ではない場合、データを物理的に移動させる方法が考えられます。

まず、マスタ側のローカルサイトで本製品に格納しているデータをテープにコピーしてください。次に、テープをリモートサイトへ移動します。リモートサイトの本製品では作業用ファイルシステムを作成し、テープからデータを書き込みます。その後、レプリケーションを開始すると、本製品はテープから書き込まれたデータを活用して WAN 経由のデータ転送を大幅に削減します。その結果、初期レプリケーションを短時間で完了することが可能です。

ケース 4: システムが遠隔地にあり、すでに両サイトで同じデータを保持している場合

双方向のレプリケーション運用で類似データを互いにコピーしあう場合、本製品は自身に格納されたデータを使ってリモートサイトのコピーを生成できます。そのため、初期レプリケーションは短時間で完了できる可能性があります。たとえば、ローカルサイトとリモートサイトで同じ種類のクライアント OS をバックアップしている場合、すでに多くの同一データを両サイトで保持しているため、WAN 経由のデータ転送は大幅に少なくなることが期待できます。

レプリケーション負荷の推奨値

レプリケーションでは、高負荷によるジョブの失敗や性能問題を回避するため、ジョブの開始頻度と同時実行ジョブ数を低く抑えることを推奨します。具体的な推奨値は、以下の通りです。

表 2-24 レプリケーションのジョブ開始頻度の推奨値

項目	推奨値	
同時開始ジョブ数	アクセラレータノード機能を持つノードあたり: 5 ジョブ以下 合計: 150 ジョブ以下	
ジョブの開始間隔	開始間隔を 5 分以上空ける	
一時間あたりの開始ジョブ数	アクセラレータノード機能を持つノードあたり: 60 ジョブ以下 合計: 360 ジョブ以下	
スケジュールによって開始し、協調アクセスグリッドを利用するジョブの同時開始ジョブ数	ノードグループに属するノードの数が 6 ノード以下の場合	合計: 75 ジョブ以下
	同 7 ノードの場合	合計: 38 ジョブ以下
	同 8 ノード以上の場合	合計: 4 ジョブ以下

表 2-25 レプリケーションの同時実行ジョブ数の推奨値

項目	推奨値	
同時実行ジョブ数 (ある時点で実行中のジョブ数)	シングルノードモデル、または Virtual Appliance の場合	4 ジョブ以下
	グリッドモデルの場合	アクセラレータノード機能を持つノードあたり: 16 ジョブ以下 合計: 75 ジョブ以下

Note アクセラレータノード機能クラスタを設定している環境で、アクセラレータノード機能を持つノードの障害が発生した場合、実行中のジョブは失敗し、別のアクセラレータノード機能を持つノードが障害の発生したノードのレプリケーションセットを引き継ぎます。そのため、他ノードのレプリケーションセットを引き継いだ状態では、障害以前と比較してレプリケーションセット数、および実行ジョブ数が増加します。また、レプリケーションセットを引き継ぐ際にアクセラレータノード機能を持つノード 1 台あたりのレプリケーションセットの最大数を超えた場合、フェイルオーバーは失敗します。アクセラレータノード機能クラスタを設定する際は、障害発生時にレプリケーションセットを引き継いだ場合に、アクセラレータノード機能を持つノード 1 台あたりのレプリケーションセットの最大数、およびジョブの推奨値を超えないように留意してください。

第3章 システム構成の変更

ラックモデル、ラックレスモデルおよびスケールアウトモデルでは、アクセラレータノード機能を持つノードやストレージノード機能を持つノードの追加または削除、またシステムの構成を変更することができます。

アクセラレータノード機能を持つノード間の負荷分散

本製品では、アクセラレータノード機能を持つノード間で簡単に負荷を分散できます。あるノードで負荷が偏っている場合は、ファイルシステムを他のノードに移動して、バックアップサーバとその特定のノードの関係を変更できます。GUI の**性能**画面 (図 3-1) を参照して、負荷が最も高いノードと最も低いノードを把握します。この際、すべてのノードと各ノードのネットワークスループットを必ず確認してください。負荷分散が必要なノードを特定した後、そのノードに関係するバックアップサーバ上でファイルシステムをアンマウントします。アンマウントしたファイルシステムを他のノードに移動します。次に、移動したファイルシステムがあるノードの IP アドレスでファイルシステムをマウントし、バックアップ操作を再開します。

このプロセスでは、バックアップサーバでファイルシステムをアンマウントする必要があります。この処理自体は短時間で行われますが、バックアップを中断してしまわないように事前に計画を立ててください。

ファイルシステムの移動方法については「ユーザズガイド」の以下の説明を参照してください。

第4章 ファイルシステム設定の管理

- ファイルシステムの移動

第7章 システムの容量と性能

- システム全体の性能を監視する
- ノードの性能を監視する

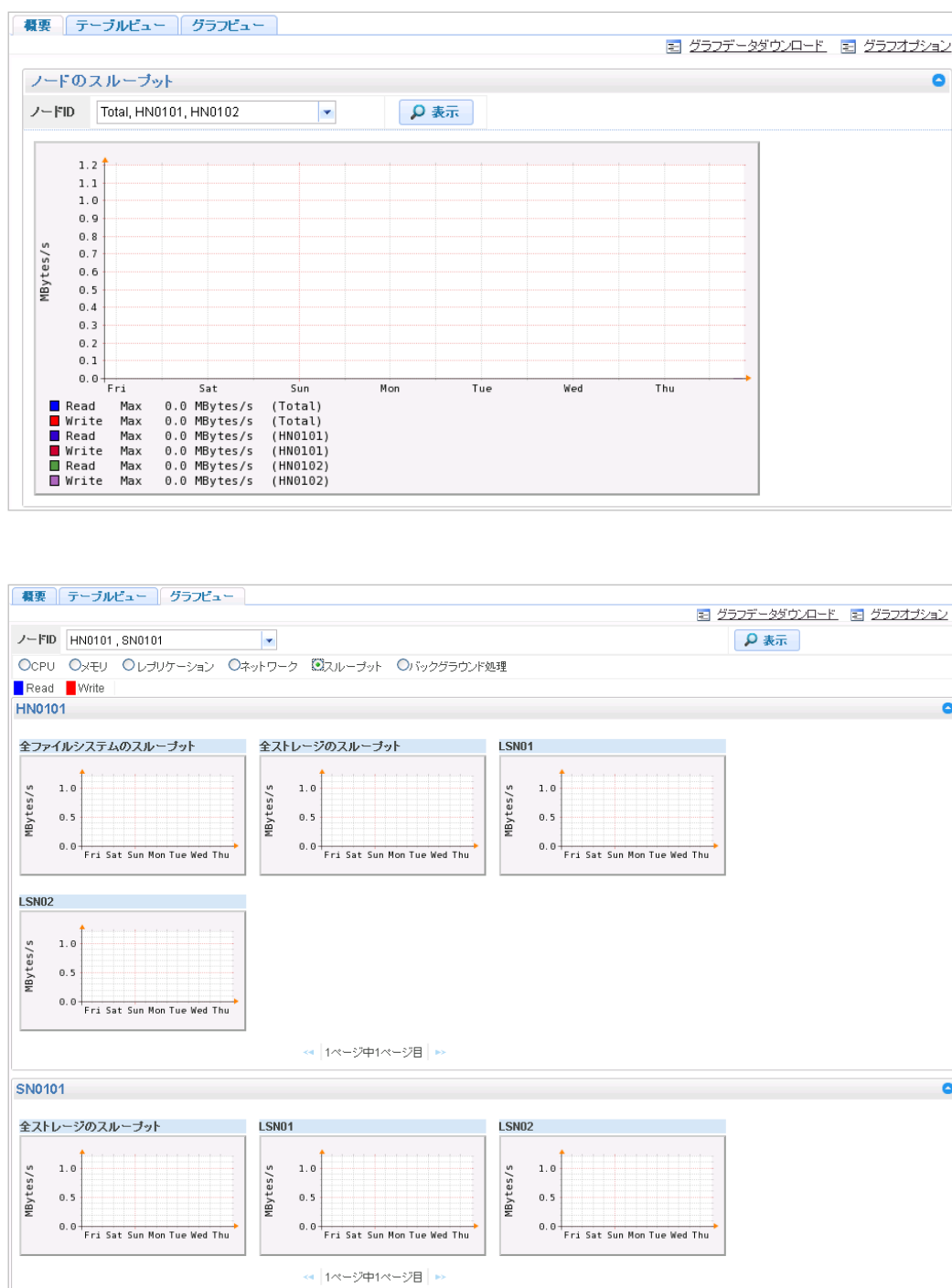


図 3-1 アクセラレータノード機能を持つノードの負荷分散

各ノードのスループットは、GUI の性能グラフで表示できます。このグラフでは、各ノードのスループットを比較できます。特定のノードのグラフ線が他よりも大幅に高い場合は、将来、本製品でボトルネックが発生し、大幅に高いグラフ線を持つノードで性能に関する問題が生じます。この場合は、ボトルネックを持つノードから、使用可能な帯域幅がより多い別のノードにファイルシステムを移動するようにします。ファイルシステムの移動方法については、「ユーザーズガイド」の「第4章 ファイルシステム設定の管理」を参照してください。

ノードの追加と削除

本製品では、ノードを追加または削除して、システム規模を拡大/縮小できます。考えられるノード数の変更ワークフローは以下の通りです。

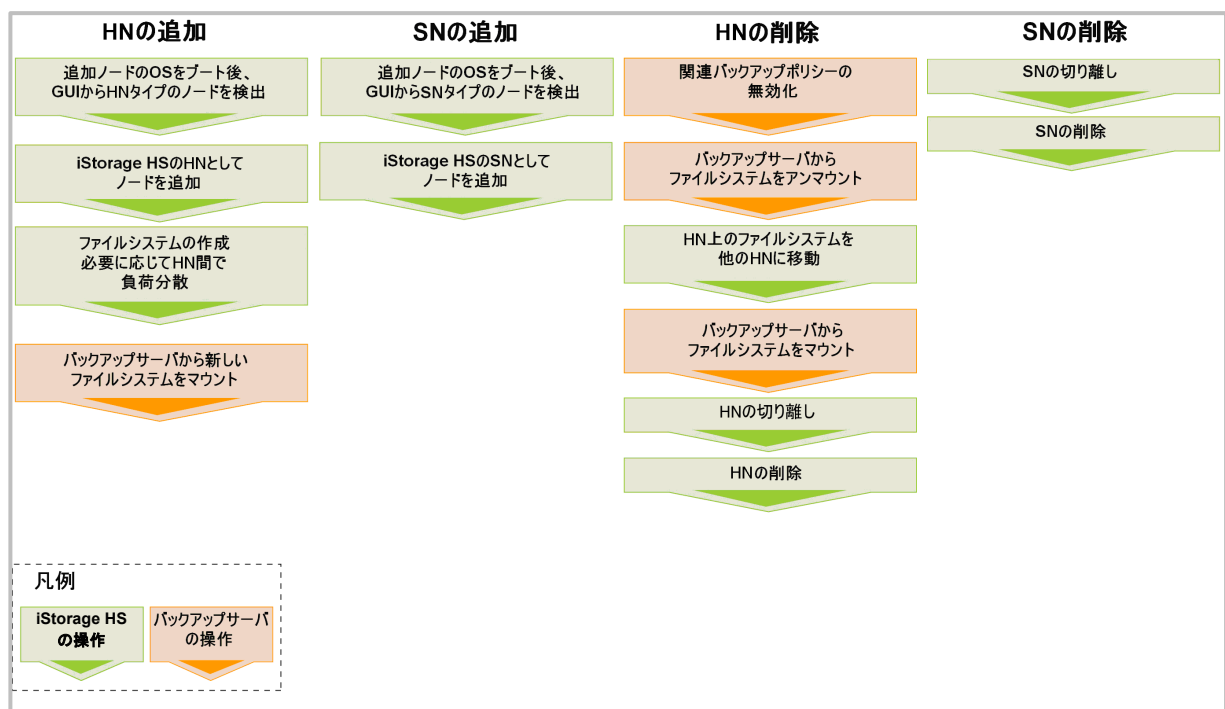


図 3-2 ノードの追加と削除

ハードウェア混在環境でのデータの分散配置

本製品では、同一システム内に複数世代のストレージノード機能を持つノードが存在できます。HS8-50S と HS8-50、または、HS8-60 と HS8-50 の混在環境では、ノードの容量が異なるため、システムの冗長性と容量を考慮し、格納されたデータをノード間にどのように分散配置するかを選択する必要があります。

分散配置方法の選択は、以下で説明するモードを変更することにより可能になります。モードの変更は CLI から `administrator` ロールで実行できます。既定のモードは「冗長モード」です。モードの変更を行った場合、データの再配置はバックグラウンドで穏やかに行われます。

冗長モード： 特定のノードが障害となった場合でも、パリティ 3 以上のファイルシステム上のデータは失われないように、各ノードにデータを分散配置します。パリティ 3 は、ファイルシステムのパリティ数の既定値になります。

容量モード： 各ノードの容量を効率的に使用するように、各ノードの容量に応じて、データを分散配置します。

これらのモードは、容量効率とノード障害に対する耐障害性の面で動作に違いがあります。例として、2 ノード構成の HS8-50 に対して、2 台の HS8-50S のストレージノードを追加したシステムを想定します。冗長モードでは、データは各ノードに同じ割合で分散配置されます。一方、容量モードでは、HS8-50S のノードの容量は HS8-50 に比べて約 1.5 倍となるため、データはおおよそ 2:2:3:3 の割合で分散配置されます。

容量効率：

前述したシステムを冗長モードで使用する場合、HS8-50 のノードが容量フル状態となったとき、HS8-50S のノードでは容量は全体の 2/3 までしか使用されません。しかし、あるノードが容量フル状態となった場合、システムとしても容量フル状態とみなされるため、HS8-50S のノードに残っている空き容量は使用することができません。

一方、容量モードでは、各ノードの容量に応じてデータを分散配置します。そのため、各ノードの容量を効率よく使用することができます。

ノード障害に対する耐障害性：

冗長モードは、容量モードに比べ、ノード障害に対し耐障害性が高くなります。

冗長モードでは、1 台の HS8-50S のノードで障害が発生した場合でも、パリティが 3 以上のファイルシステムに格納されているデータは失われることはありません。

一方、前述したシステムを容量モードで使用する場合、HS8-50S の 1 台のノード障害でデータを失わないためには、パリティ数が 4 以上のファイルシステムに格納する必要があります。

表 3-1 冗長モードと容量モードの比較

	メリット	デメリット
冗長モード	ノード障害に対する高い耐障害性	低い容量効率
容量モード	高い容量効率	ノード障害に対する低い耐障害性

各構成での容量効率

冗長モードで HS8-50S/HS8-60 のノードが使用可能な容量を示します。赤色で示す組み合わせで HS8-50S/HS8-60 のノードの使用可能な容量は、それぞれ以下になります。

その他組み合わせでは、HS8-50S/HS8-60 の容量は 100%使用可能です。

表 3-2 冗長モードでの使用可能な HS8-50S の容量

		HS8-50 ノード数				
		1	2	3	4	5
HS8-50S /HS8-60 ノード数	1	67%	67%	67%	89%	
	2	67%	67%			
	3	67%				
	4					

各構成でのノード障害に対する耐障害性

冗長モードでは、パリティ 3 以上のファイルシステム上のデータは失われないように、各ノードにデータを分散配置します。したがって、HS8-50S/HS8-60 でノード障害が起きると、パリティ数が 3 未満のファイルシステムの読み込みができなくなります。

容量モードの場合、各構成のノード障害に対する耐障害性は、以下のようになります。HS8-50S/HS8-60 でノード障害が起きると、“✓”で示される組み合わせでは、当該パリティ数のファイルシステムの読み込みができなくなります。

表 3-3 パリティ数 3 のファイルシステムのノード障害への耐障害性

		HS8-50 ノード数				
		1	2	3	4	5
HS8-50S /HS8-60 ノード数	1	✓	✓	✓	✓	
	2	✓	✓			
	3	✓				
	4					

表 3-4 パリティ数 4 のファイルシステムのノード障害への耐障害性

		HS8-50 ノード数				
		1	2	3	4	5
HS8-50S /HS8-60 ノード数	1	✓	✓			
	2	✓				
	3					
	4					

Note 表 3-3、表 3-4 に記載されていない構成、またはパリティ数に関しては、担当営業または担当 SE にお問い合わせください。

第4章 システムの監視

容量の監視

本製品にとっての「容量」とは

すべてのサーバからのデータは、分割、重複排除、圧縮され、ストレージノード機能を持つノードに均一に分散されます。このようなストレージシステムは、「ストレージグリッド」と呼ばれます。

圧縮される前のクライアントのデータ量は、**格納済み容量**として定義されます。格納済み容量は、ファイルシステム上のサイズを示します。圧縮の実行後は、GUI の**容量**画面（図 4-2）の**データ領域**として参照できます。**パリティ&メタデータ領域**の値は、冗長フラグメントとデータに付随するメタデータの合計を示します。

重複排除技術（DataRedux）

DataRedux は本製品独自の重複排除技術です。DataRedux は、本製品に書き込むデータが、すでに書き込まれているデータと重複していないか確認し、重複している場合は書き込みを中止します。これにより、データの格納効率を高め、高性能と高コストパフォーマンスを実現します。

DataRedux にはデータを可変長のサイズに分割するという高度な方法があります。これにより、固定長のデータ分割方法では検出できなかったデータの重複も検出できるようになりました（図 4-1）。

バックアップの場合、ディスク消費量が実際のバックアップデータ量の 1/20 から 1/50 と大幅に圧縮されることが実証されています。また、バックアップの場合は重複するデータを繰り返し保存するので、バックアップを重ねるごとにデータの圧縮効果が大きくなります。

この重複排除技術により、ディスクへのデータの転送量と、データを保存するのに必要な実際の物理ディスク容量が大幅に削減されます。その結果、ディスクバックアップを高速かつ低コストで実現できます。また、この技術をリモートレプリケーションに応用すると、従来、更新差分までしか圧縮できなかった転送データをさらに圧縮できます。これにより、リモートサイトへのデータ転送量を飛躍的に小さくでき、帯域の小さな低速回線を使用したリモートレプリケーションが可能です。



図 4-1 重複排除(DataRedux)

データ圧縮率

データ圧縮率は、**格納済み容量**を**データ領域**で割って計算します（図 4-2）。圧縮率は、格納するデータの特徴によって異なります。たとえば、バックアップデータがシンクライアントの数百の OS イメージの場合、2 つの OS イメージ間の違いは小さいので、優れた合計圧縮率となります。しかし、格納データが一意で圧縮できない完全にランダムなデータの場合、合計圧縮率は 1 という低い値になることもあります。これらは極端な例で、通常のバックアップデータは、このデータ例のおおよそ中間の圧縮合計率になります。また、バックアップに関して以下の点に注意してください。

- バックアップサーバのデータを圧縮すると、重複データを検出できる可能性が低くなります。本製品の機能がデータ圧縮を提供しているので、バックアップサーバ自体にデータ圧縮をさせないようにしてください。
- 画像ファイル(PNG、JPEG、TIFF)など、すでに圧縮されているデータをさらに圧縮することはできません。このような種類のファイルの場合、圧縮率が 1 まで低くなる場合があります。
- 暗号化は、圧縮と同様に本製品のデータ重複排除に影響を与える場合があるので、バックアップサーバでは使用しないでください。

GUI を使用して容量を監視するには

本製品は、容量の使用傾向を監視するために、以下の 2 つの画面（図 4-2、図 4-3）を提供しています。

図 4-2 の GUI の**容量**画面を利用して、システムの総容量を監視できます。

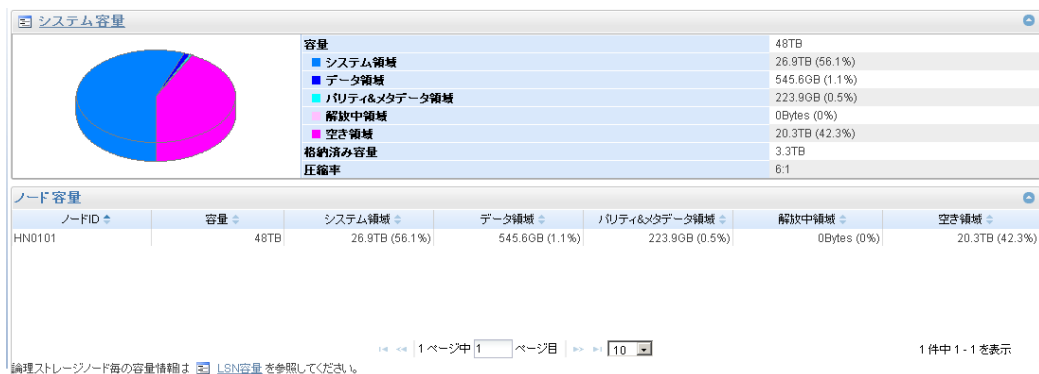


図 4-2 容量画面

図 4-3 の**システム容量**画面の使用領域グラフに重複排除やデータ圧縮後、サーバからデータを格納するために使用される領域の量を示します。この値はデータ、パリティ、メタデータで構成されています。圧縮率グラフに重複排除やデータ圧縮のデータ圧縮率を示します。

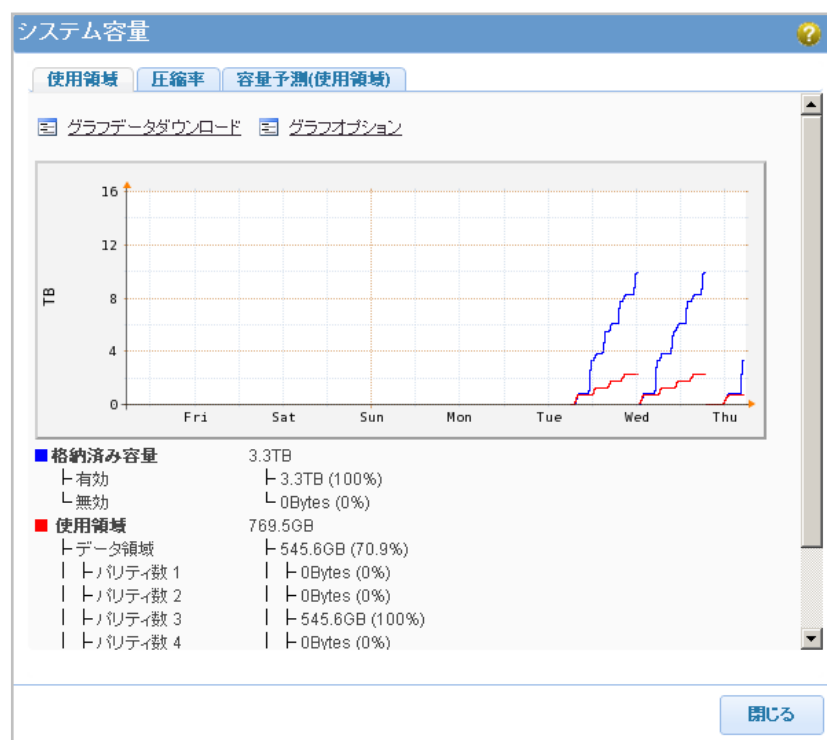


図 4-3 システム容量画面

新しいデータ用の容量の見積もり

本製品の GUI を使用すると、将来必要となる容量を予測できます。この画面（図 4-4、図 4-5）には、**格納済み容量とデータ圧縮率**の履歴が表示されます。書き込みを予定しているデータとよく似たデータが格納されているファイルシステムのデータ圧縮率を、新しく格納するデータの圧縮率と仮定することで、格納する予定のデータ量からディスクの使用量を予測できます。



The screenshot shows a window titled 'fsHN0101_1' with a help icon. It has two tabs: '圧縮状況(日次)' (Compression Status (Daily)) and '格納済み容量' (Stored Capacity). The '格納済み容量' tab is active, displaying a table with the following data:

日付	書き込みデータ	圧縮率	重複排除	データ圧縮
2012/11/01	401.8GB	6.6:1	4.3:1	1.5:1
2012/10/31	10.5GB	1.5:1	1:1	1.5:1

Below the table, there is a pagination control showing '1 ページ中 1 | ページ目' and a dropdown for '10'. To the right, it says '2 件中 1 - 2 を表示'. A '閉じる' (Close) button is at the bottom right.

図 4-4 新しいデータ用の容量の見積 (1/2)

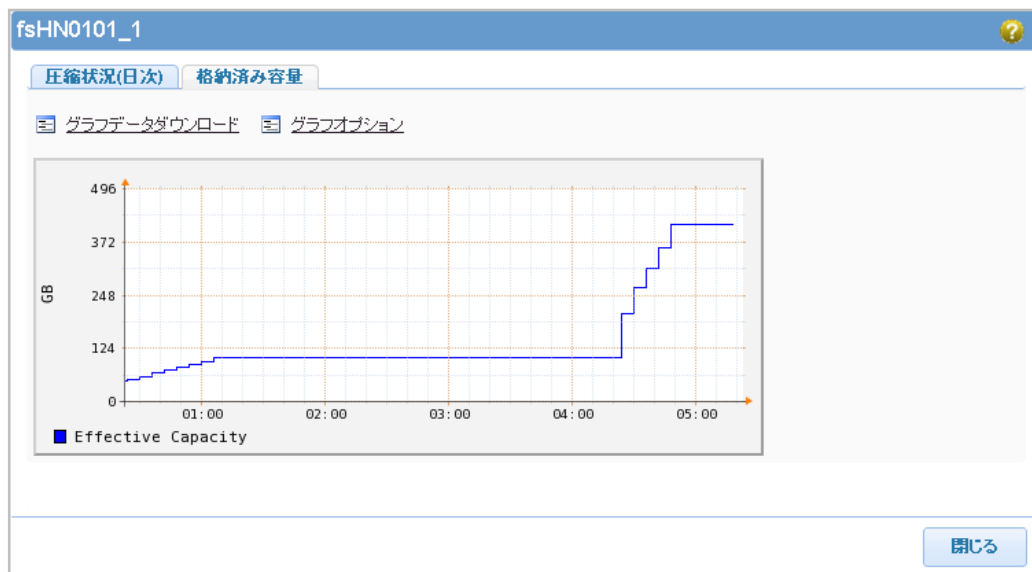


図 4-5 新しいデータ用の容量の見積(2/2)

たとえば、本製品の1つのファイルシステムに、100台のクライアントPCからの書き込みデータがあり、その格納済み容量は12TBで、圧縮率はおよそ24だとします。

このとき、本製品では、 $12\text{TB} / 24 = 500\text{GB}$ のディスクスペースがデータとして実際に使用されていることになります。

クライアントPCの数が100台から5倍の500台に増加することが予測される場合、格納済み容量の増加量は、12TBの5倍の60TBと予測できます。

書き込みデータの種類が変わらなければ、圧縮率はおよそ24のまま変わらないと推測できます。したがって、実際に使用されるディスクスペースは $60\text{TB} / 24 = 2.5\text{TB}$ と予測されます。

容量予測と容量拡張

容量予測は、将来必要となる容量を推定するために役立ちます。本製品では、同時に故障することが許されるノードの数はパリティ 3 の場合で全体の 25%です。（パリティ 3 以外の場合は、表 2-22、表 2-23、表 2-24 を参照）25%のストレージノード機能を持つノードが同時に故障すると、失われたデータは残りの 75%のストレージノード機能を持つノードでリカバリされます。リカバリが完了すると、全体のデータ量はストレージ機能を持つノードが故障する前と等しくなります。言い換えると、すべてのデータをリカバリするには、全体の 75%のストレージ機能を持つノードだけで全データを格納できなければならず、25%の空き容量が必要ということになります。以上の理由により、リカバリ限界をシステムのディスクの限界の 75%に設定してください。このリカバリ限界に達する前に、システムの拡張を計画してください。リカバリ限界に達する予測日とディスクの限界に達する予測日は図 4-6 のように、それぞれ、リカバリ限界となる容量、ディスクの限界となる容量から特定することができます。

システム容量詳細画面にある容量予測（使用領域）



図 4-6 容量の拡張タイミングの決定

Note 高圧縮率のデータを書き込んだ場合、ディスクの限界に到達する前に、システムが内部的に持つ論理使用領域の限界に達することがあります。

容量予測（図 4-7）を使用すると、拡張するストレージの台数を見積もることができます。これは、現在のデータ増加傾向が、予測期間中も変化しないことを前提としています。

システム容量画面にある容量予測（使用領域）

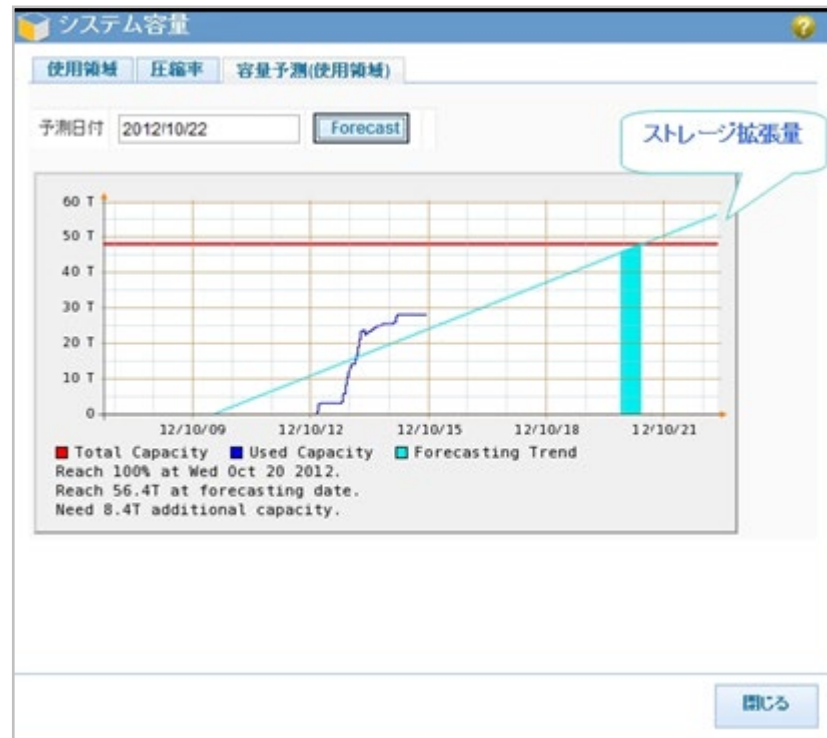


図 4-7 必要な容量拡大量の決定

付録 A ソフトウェア諸元一覧

カテゴリ	項目	値
ネットワーク	設定可能な VLAN ID	1～4083、4094
	FIP に割り当て可能な VLAN ID	1～4083、4094
	MTU	576～9000
	アクセラレータノード機能を持つノード 1 台あたりのルーティングの最大数	31 個
	ノード毎に設定可能なフィルタリングルール数	100
ファイルシステム	アクセラレータノード機能を持つノード 1 台あたりのファイルシステムの最大数	250 個 ^{*1*2}
	システム 1 台あたりのファイルシステムの最大数	250 個 x アクセラレータノード機能を持つノード数 ^{*3*13}
	ファイルシステム名の最大長	64 文字 (1 バイト文字)
	ファイルシステムの最大サイズ	256PB
	最大ファイルサイズ	512TB-1B
	1 ディレクトリに作成可能なオブジェクト (ファイル、ディレクトリ) の最大数	400,000 個 ^{*4*5}
	1 ファイルシステムに作成可能なオブジェクト (ファイル、ディレクトリ) の最大数	1,000,000,000 個 ^{*6}
メール通報	設定可能なメールサーバの最大数	5 台
	設定可能なシステム管理者の E-mail アドレスの最大数	1 個
	設定可能なシステムレポートの E-mail アドレスの最大数	32 個
	設定可能なイベントレポートの E-mail アドレスの最大数	32 個
NTP	設定可能な NTP サーバの最大数	3 台
領域解放	領域解放の自動スケジュールの最大数	31 個
	領域解放の自動スケジュールの終了期限	15 分～9999 分
	領域解放の履歴の最大保存件数	30 個
レプリケーション	アクセラレータノード機能を持つノード 1 台あたりのレプリケーションジョブの最大同時実行数	125 個 ^{*7*14}
	アクセラレータノード機能を持つノード 1 台あたりのレプリケーションセットの最大数	125 個
	レプリケーションセット 1 個あたりのスケジュールの最大数	10 個
	システム 1 台あたりの設定可能なリモートシステムの最大数	50 個 ^{*8}
SNMP	設定可能なトラップサーバの最大数	5 台 ^{*9}

GUI/CLI 利用ユーザ	同時ログイン可能なユーザ数(システム監視員)	30
	同時ログイン可能なユーザ数(システム管理者)	1
NFS	パス名の最大長	4095 文字 (1 バイト文字) *10
	ファイル名の最大長	255 文字 (1 バイト文字) *10
	接続数 (推奨)	1000 未満*12
CIFS	パス名の最大長	4095 文字 (1 バイト文字) *10 *11
	ファイル名の最大長	255 文字 (1 バイト文字) *10*11
	最大ファイルサイズ	16TB
	アクセラレータノード機能を持つノード 1 台あたりの 1 クライアントから同時にオープンできるファイルの最大数	3000 (iStorage HS8) または 2000 (iStorage HS3) *15
	アクセラレータノード機能を持つノード 1 台あたりの接続数 (推奨)	200 未満*12*16
バックアップ/ リストア	アクセラレータノード機能を持つノード 1 台あたりの同時バックアップ/リストアジョブの最大数 (推奨)	20 (iStorage HS8) または 8 (iStorage HS3 および iStorage HS Virtual Appliance)
	同時バックアップジョブの最大数 (推奨) *17	4
	同時リストアジョブの最大数 (推奨) *17	4

* 1: AN クラスタ構成時にはフェイルオーバー後のファイルシステムが 250 個以内である必要があります。

* 2: 協調ノードグループを構成するノードの場合、ノード 1 台あたりのファイルシステムの最大数は協調グリッドファイルシステムの数も含めた数値になります。

* 3: 協調グリッドファイルシステムが存在する場合は、システム 1 台あたりのファイルシステム最大数は減少します。

* 4: CLI の system config コマンドにより、最大 1,300,000 個まで拡張することができます。

* 5: 1 ディレクトリに作成するオブジェクト数は、以下の値を下回るようにすることを推奨します。

- CIFS 経由の場合: 3000 個
- NFS 経由の場合: 30000 個

この値を超えてオブジェクトを作成した場合、性能に影響を与える可能性があります。

また、CIFS 経由で協調グリッドファイルシステムを使用している場合、ディレクトリ階層が深くなると、性能に影響を与える可能性があります。この場合、協調グリッドファイルシステムのディレクトリ属性キャッシュを有効にすることで、性能への影響を軽減できます。設定は CLI の system config コマンド(パラメータ名 fs_dir_attr_cache_time)により行います。

* 6: マーカーフィルタリング使用時は約 1/3 となります。

* 7: シングルノードモデルの場合、32 個です。

* 8: シングルノードモデルと iStorage HS Virtual Appliance の場合、16 個です。

* 9: 最初の SNMP トラップサーバのみ GUI から設定が可能です。SNMP トラップサーバを 5 つまで設定する場合は CLI を使用してください。

* 10: マルチバイト文字を使用している場合は、1 文字のバイト数に応じて文字数の最大長は短くなります。

ファイル名やディレクトリ名のバイト長は使用する文字コードによって異なるため、以下に注意してください。

- CIFS 経由の場合、ファイル名やディレクトリ名の文字コードは UTF-8 を使用します。
- NFS 経由の場合、ファイル名やディレクトリ名の文字コードは変換されません。NFS クライアント(バックアップサーバ)やクライアントアプリケーション(バックアップソフトなど)が設定している文字コードを使用します。

* 11: Windows のアプリケーションによっては、ファイル名やディレクトリ名の文字数の最大長が本製品の諸元より短い場合があります。代表的なアプリケーションとしてエクスプローラがあります。

* 12: I/O 負荷状況や他プロトコルの同時利用により、同時にアクセス可能なクライアント数は変動します。

* 13: iStorage HS Virtual Appliance の場合、この値は 250 です。

* 14: iStorage HS Virtual Appliance の場合、この値は 16 です。

Note iStorage Virtual Appliance の場合、推奨値は 2 です。

* 15: iStorage HS Virtual Appliance の場合、この値は 1000 です。

* 16: iStorage HS Virtual Appliance の場合、この値は 50 未満です。

* 17: この項目は、iStorage HS Virtual Appliance にのみ適用されます。

付録 B 電源制御ソフトウェアの設定

ここでは、iStorage HS シリーズで電源制御ソフトウェア機能を使用するために必要な設定手順について説明します。

本機能を使用するためには、本機能を使用するシステムの全ノードに対して、別途ライセンスが必要になります。ライセンスについては、担当営業または担当 SE にお問い合わせください。

本機能を使用するためには、電源制御端末に下記のソフトウェアが必要となりますので、あらかじめご準備ください。

- Windows OS 利用時
ESMPRO/AutomaticRunningController V5.1 以降
ESMPRO/AC Enterprise V5.1 以降
または、SigmaSystemCenter/電源管理基本パック Ver2.1

上記以外のバージョンについてはテクニカルサポートにご確認ください。

- Linux OS 利用時
ESMPRO/AutomaticRunningController for Linux V4.0 以降

ここで使用する用語について説明します。システム構成の概要は図 C-1 を参照してください。

電源制御端末：

電源制御端末用ソフトウェアと組み合わせることにより、UPS 装置を含めたシステム全体の電源を制御する端末装置。

連動端末：

電源制御端末によって電源制御される端末装置。ここでは iStorage HS を指します。

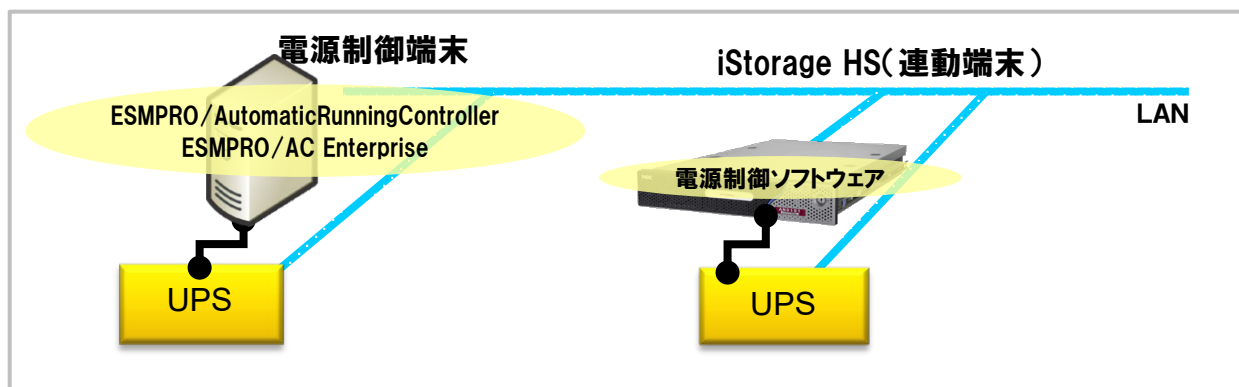


図 C-1 電源制御構成図

設定手順のフローチャート

電源制御ソフトウェア機能を使用するための設定手順は、iStorage HS のモデルごとに異なります。設定手順のフローチャート（図 C-2）に従って設定を行ってください。

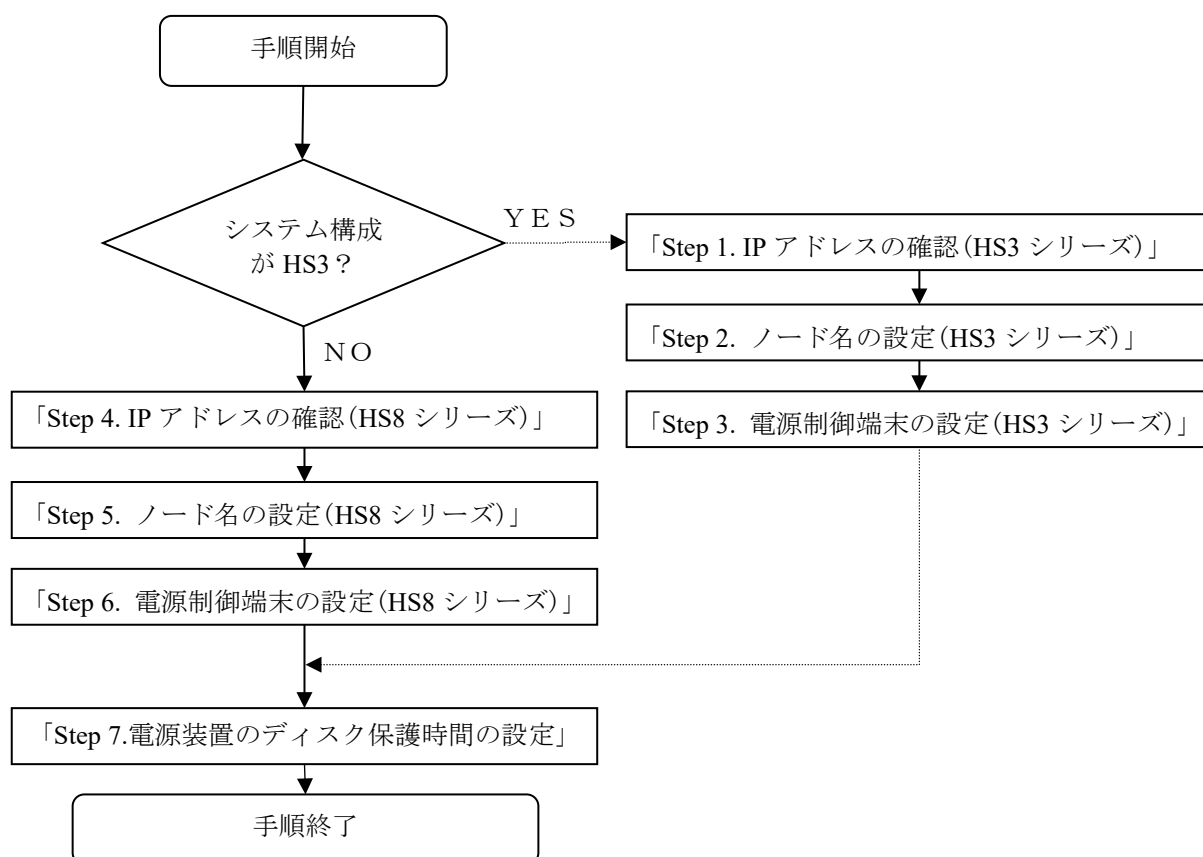


図 C-2 設定手順のフローチャート

電源制御ソフトウェアの設定手順

電源制御ソフトウェア機能を使用するためには、電源制御端末に iStorage HS を登録する必要があります。

電源制御端末への登録に際して、電源制御の対象となるコンピュータを特定するための、コンピュータ名（ノード名）と IP アドレスが必要となりますので、以降の手順を実行してください。

すでに、iStorage HS のシステムバージョン 4.1.0 以降で電源制御ソフトウェアを使用されている場合、今回アップグレードを行ったとしても、iStorage HS、電源制御サーバのどちらに対しても再設定は不要となり、以降の手順は不要です。

新たに電源制御ソフトウェアを導入する場合や、すでに iStorage HS で電源制御ソフトウェアを使用されているが、アップグレードを契機に電源制御端末に任意の名称を登録されたい場合に以降の手順を実行してください。

Step 1. IP アドレス確認 (HS3 シリーズ)

ここでは電源制御端末にシステムを登録するために必要な IP アドレスの設定確認方法について説明します。

下記の手順を実施してください。

- ① GUI にログイン後、メイン画面（図 C-3）で**ネットワーク**をクリックします。

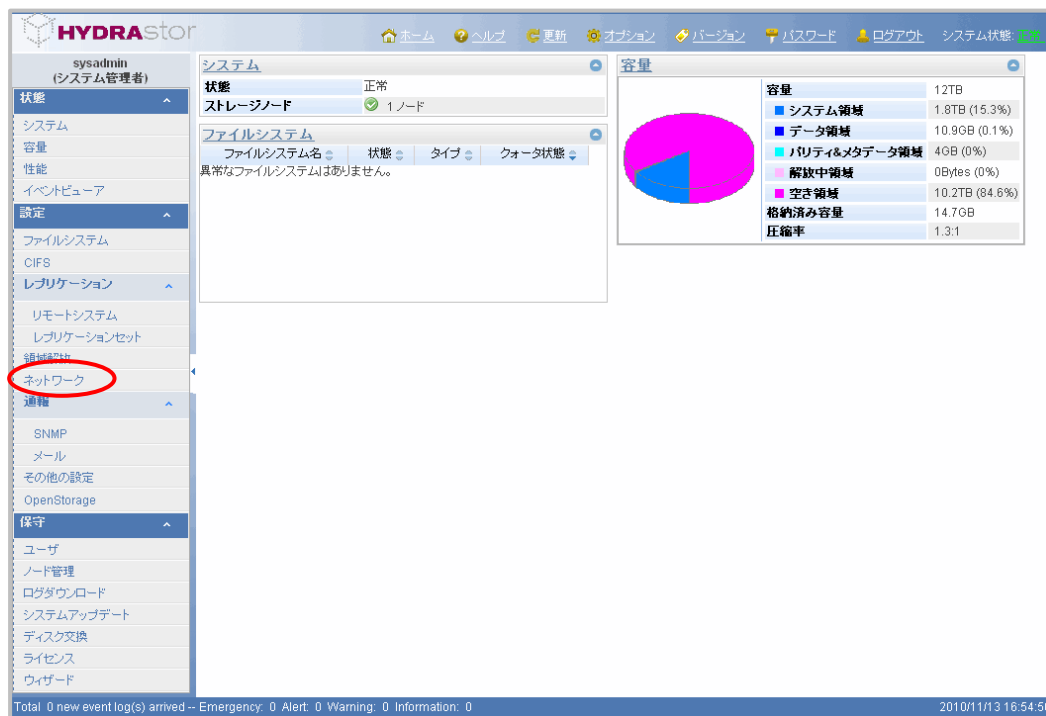


図 C-3 メイン画面

- ② ネットワーク画面（図 C-4）で表示される外部 IP アドレスのうち、電源制御サーバと接続可能な外部 IP アドレスを確認します。外部 IP アドレスは bonding ポートも設定可能です。

ここで確認した外部 IP アドレスは「Step 3. 電源制御端末の設定 (HS3 シリーズ)」で使用します。

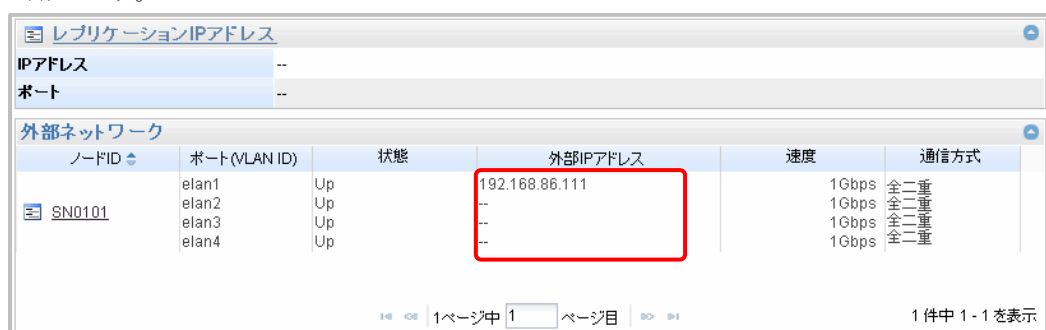


図 C-4 ネットワーク画面

Step 2. ノード名の設定 (HS3 シリーズ)

ここでは電源制御端末に iStorage HS を登録するために必要な名称（ノード名）を、現在設定されているノード名から変更する場合に、iStorage HS に設定する方法について説明します。

下記の手順を実施してください。

powercontrol コマンドの詳細は、「コマンドリファレンス」の「第 II 編 リファレンス」の「第 2 章 コマンド」の「powercontrol」を参照してください。

- ノード名確認手順

- ① ssh または telnet を使い、CLI にログインしてください。
- ② 下記のコマンドを実行して、対象ノードのノード名を確認してください。

```
powercontrol show
```

- ③ CLI からログアウトしてください。

- ノード名設定手順

- ① あらかじめ電源制御端末に登録する iStorage HS の名称を決定しておいてください。名称は最大 15 文字の英数字です。
- ② ssh または telnet を使い、管理者権限のあるアカウントで CLI にログインしてください。
- ③ 下記のコマンドを実行して、対象のノードに名称を設定してください。

```
powercontrol set node=<対象ノード名> name=<名称>
node=<対象ノード名>
  ※対象ノードのノード名
  例) node=SN0101
name=<名称>
  ※対象ノードに指定したい任意の名称（15 文字以内の英数字）
  例) name=HYDRAsystem1
```

- ④ 下記のコマンドを実行して、対象のノードに名称が正しく設定されているか確認してください。設定が間違っていた場合は再度③の手順を実行してください。

```
powercontrol show
```

- ⑤ CLI からログアウトしてください。

Step 3. 電源制御端末の設定 (HS3 シリーズ)

iStorage HSを電源制御端末から制御するために、ESMPRO/AC EnterpriseのAC Management Consoleを起動後、連動端末設定画面（図C-5）で、①～③の設定をしてください。

これらの設定を誤ると、電源制御端末からiStorage HSを認識できず、電源制御ソフトウェア機能が有効にならないため、注意してください。

連動端末設定画面以外の設定については、電源制御端末用ソフトウェアのマニュアルを参照してください。

- ① 名称：「Step 2. ノード名の設定 (HS3シリーズ)」で対象のノードに設定した名称
- ② IP address：「Step 1. IPアドレス確認 (HS3シリーズ)」で確認した外部ネットワークのIPアドレス
- ③ Linux：チェックボックスにチェックを入れてください。

連動端末(サーバ)

「ESMPRO/AC Enterprise マルチサーバオプション」か、「ESMPRO/AC Blade マルチサーバオプション」、「ESMPRO/AC Advance マルチサーバオプション」をセットアップしたサーバを登録します。

① 名称 (コンピュータ名: 15文字まで。Linuxの場合は大/小文字を区別する必要あり)

☒ コンピュータ名を大文字に自動変換する。(Linuxの場合は無効)

② IP address (例: 172.16.1.10)

説明

③ ☒ Linux

ブラウザ設定

☐ Advance option mode

リモート起動用 MAC address

リモート起動用 IP address

リモート起動用 ネットマスク

OK

キャンセル

図 C-5 連動端末設定画面

Step 4. IP アドレス確認 (HS8 シリーズ)

ここでは電源制御端末にシステムを登録するために必要な IP アドレスの設定確認方法について説明します。

以降、デフォルトの管理ノードを **HN0101**、代替ノードを **HN0102** として説明します。これらのノード名は HS8-30 の場合、**AN0101** や **AN0102** などになります。お客様システムのノード名で読み替えてください。

対象となるシステムの下記のノードに対して、下記の手順を実施してください。

- 対象ノード

アクセラレータノード機能を持つノードが 1 ノードの場合 : **HN0101**

アクセラレータノード機能を持つノードが 2 ノード以上の場合 : **HN0101** と **HN0102**

- 手順

① GUI にログイン後、メイン画面（図 C-6）で**ネットワーク**をクリックします。

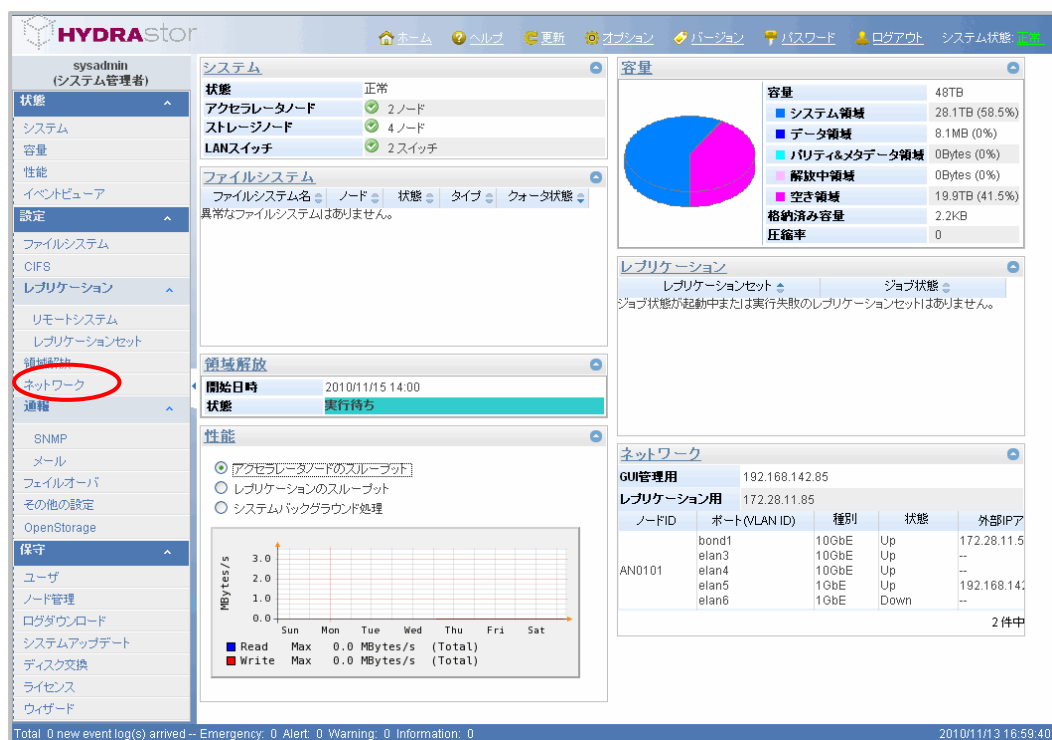


図 C-6 メイン画面

- ② ネットワーク画面（図 C-7）で表示される外部 IP アドレスのうち、電源制御サーバと接続可能な外部 IP アドレスを確認します。外部 IP アドレスは bonding ポートも設定可能です。

ここで確認した外部 IP アドレスは「Step 6. 電源制御端末の設定(HS8 シリーズ)」で使います。

フローティングIPアドレス

外部フローティングIPアドレス

GUI管理用

レプリケーション用

192.168.14.23

192.168.14.23

外部ネットワーク

ノードID	ポート(VLAN ID)	種別	状態	外部IPアドレス	帯域幅	通信方式	フェイルオーバー	監視
AN0101	elan1	10GbE	Up	192.168.14.24	100Mbps	全二重	対象	対象
	elan2	10GbE	Up	--	100Mbps	全二重	--	--
	elan3	10GbE	Up	--	100Mbps	全二重	--	--
	elan4	10GbE	Up	--	1Gbps	全二重	--	--
	elan5	1GbE	Up	--	1Gbps	全二重	--	--
	elan6	1GbE	Up	--	1Gbps	全二重	--	--

1ページ中 1 ページ目 2件中 1-2を表示

内部ネットワーク

ノードID	ノードタイプ	ポート	内部IPアドレス	ネットマスク	帯域幅	bondingスレーブ
AN0101	アクセラレータノード	bond0	169.254.1.11	255.255.255.0	3Gbps	ilan1(Up),ilan2(Up),ilan3(Up),ilan4(Up)
AN0102	アクセラレータノード	bond0	169.254.1.12	255.255.255.0	4Gbps	ilan1(Up),ilan2(Up),ilan3(Up),ilan4(Up)
SN0101	ストレージノード	bond0	169.254.1.31	255.255.255.0	4Gbps	ilan1(Up),ilan2(Up),ilan3(Up),ilan4(Up)
SN0102	ストレージノード	bond0	169.254.1.32	255.255.255.0	4Gbps	ilan1(Up),ilan2(Up),ilan3(Up),ilan4(Up)
SN0103	ストレージノード	bond0	169.254.1.33	255.255.255.0	4Gbps	ilan1(Up),ilan2(Up),ilan3(Up),ilan4(Up)
SN0104	ストレージノード	bond0	169.254.1.34	255.255.255.0	4Gbps	ilan1(Up),ilan2(Up),ilan3(Up),ilan4(Up)

1ページ中 1 ページ目 6件中 1-6を表示

Step 5. ノード名の設定 (HS8 シリーズ)

ここでは電源制御端末に iStorage HS を登録するために必要な名称（ノード名）を、現在設定されているノード名から変更する場合に、iStorage HS に設定する方法について説明します。

対象となる iStorage HS の下記のノードに対して、下記の手順を実施してください。

powercontrol コマンドの詳細は、「コマンドリファレンス」の「第 II 編 リファレンス」の「第 2 章 コマンド」の「powercontrol」を参照してください。

- 対象ノード

アクセラレータノード機能を持つノードが 1 ノードの場合 : **HN0101**

アクセラレータノード機能を持つノードが 2 ノード以上の場合 : **HN0101** と **HN0102**

- ノード名確認手順

- ① ssh または telnet を使い、CLI にログインしてください。
- ② 下記のコマンドを実行して、対象ノードのノード名を確認してください。

```
powercontrol show
```

- ③ CLI からログアウトしてください。

- ノード名設定手順

- ① あらかじめ電源制御端末に登録する iStorage HS の名称を決定しておいてください。名称は最大 15 文字の英数字です。
- ② ssh または telnet を使い、管理者権限のあるアカウントで CLI にログインしてください。
- ③ 下記のコマンドを実行して、対象のノードに名称を設定してください。

```
powercontrol set node=<対象ノード名> name=<名称>
node=<対象ノード名>
  ※対象ノードのノード名
  例) node=HN0101
name=<名称>
  ※対象ノードに指定したい任意の名称 (15 文字以内の英数字)
  例) name=Mysystem1
```

- ④ 下記のコマンドを実行して、対象のノードに名称が正しく設定されているか確認してください。設定が間違っていた場合は再度③の手順を実行してください。

```
powercontrol show
```

- ⑤ CLI からログアウトしてください。

Step 6. 電源制御端末の設定 (HS8 シリーズ)

iStorage HSを電源制御端末から制御するために、ESMPRO/AC EnterpriseのAC Management Consoleを起動後、連動端末設定画面（図C-8）で、下記のノードそれぞれに対して、①～③の設定をしてください。

これらの設定を誤ると、電源制御端末からiStorage HSを認識できず、電源制御ソフトウェア機能が有効にならないため、注意してください。

アクセラレータノード機能を持つノードが 1 ノードの場合 : **HN0101**

アクセラレータノード機能を持つノードが 2 ノード以上の場合 : **HN0101** と **HN0102**

連動端末設定画面以外の設定については、電源制御端末用ソフトウェアのマニュアルを参照してください。

- ① 名称 : 「Step 5. iStorage HSノード名の設定」で対象のノードに設定した名称
- ② IP address : 「Step 4.iStorage HSのIPアドレス確認」で確認した外部ネットワークのIPアドレス
- ③ Linux : チェックボックスにチェックを入れてください。

連動端末(サーバ)

「ESMPRO/AC Enterprise マルチサーバオプション」か、「ESMPRO/ACBlade マルチサーバオプション」、「ESMPRO/AC Advance マルチサーバオプション」を、セットアップしたサーバを登録します。

① 名称 (コンピュータ名: 15文字まで。Linuxの場合は大/小文字を区別する必要あり)

☒ コンピュータ名を大文字に自動変換する。(Linuxの場合は無効)

② IP address (例: 172.16.1.10)

説明

③ ☒ Linux

ブラウザ設定

☐ Advance option mode

リモート起動用 MAC address

リモート起動用 IP address

リモート起動用 ネットマスク

OK

キャンセル

図 C-8 連動端末設定画面

Step 7. 電源装置のディスク保護時間の設定

停電後の復電が短時間で行われた場合、iStorage HSが自動起動しない場合があるため、以下の設定を行ってください。

ESMPRO/AC EnterpriseのAC Management Consoleを起動後、電源装置設定画面（図C-9）で、「Disk保護時間」として、「120 sec」以上の値を設定してください。

なお、停電後の復電に際して、「Disk保護時間」経過後に、iStorage HSが自動起動します。

The screenshot shows the '電源装置' (Power Device) management interface. The '電源装置管理情報' (Power Device Management Information) section includes fields for 'サーバの電源' (Server Power) set to '冗長なし' (No Redundancy), 'IP address' set to '192.168.136.240', and 'SNMP コミュニティ名' (SNMP Community Name) set to 'public'. The '電源異常' (Power Abnormality) section shows '電源異常確認時間' (Power Abnormality Confirmation Time) at 60 seconds and 'Warm-UP 順位' (Warm-UP Order) as a dropdown. Three radio buttons are present: '電源異常回復時にリポートしない' (Do not report when power abnormality recovers), '電源異常回復時にリポートする (UPSによるリポート)' (Report when power abnormality recovers (by UPS report)) - which is selected, and '電源異常回復時にリポートする (制御端末からリポートする)' (Report when power abnormality recovers (from control terminal)). The 'Warm-UP 時間' (Warm-UP Time) is 0 seconds. 'バッテリー温度監視' (Battery Temperature Monitoring) is set to 55 °C for the upper limit and 0 °C for the lower limit. The 'SNMP設定情報' (SNMP Settings Information) section shows '名称' (Name) as 'UPS_IDEN', '電源切断予告時間' (Power Disconnection Advance Time) as 360 seconds, and 'Disk保護時間' (Disk Protection Time) as 120 seconds, which is circled in red. Other settings include '許容電圧(上限)' (Allowable Voltage (Upper Limit)) at 225 V, '許容電圧(下限)' (Allowable Voltage (Lower Limit)) at 182 V, '電源異常検出感度' (Power Abnormality Detection Sensitivity) at 2, '異常発生時のブザータイミング' (Buzzer Timing when abnormality occurs) at 1, '異常検出時のブザータイマ' (Buzzer Timer when abnormality is detected) at 0 seconds, and '自動バッテリーテストパターン' (Automatic Battery Test Pattern) at 2. On the right, there are buttons for 'OK', 'キャンセル' (Cancel), 'UPS レポート' (UPS Report), 'バッテリー交換日' (Battery Replacement Date), '冗長構成設定' (Redundancy Configuration Setting), and 'iStorage連携' (iStorage Linkage). A '情報の上書きをSNMPで実行(S)' (Execute overwrite with SNMP) button is also present.

図 C-9 電源装置設定画面

注意事項

本製品を使用する際は、以下の点にも注意してください。

1. UPS について

- (1) iStorage HS の冗長電源ユニットは異なる UPS 装置に接続しないでください。
- (2) iStorage HS に接続する UPS は、1 ノードの場合は 1500VA、2 ノードの場合は 3000VA の UPS を選択してください。
- (3) iStorage HS のシャットダウン完了までには、最長 5 分かかる可能性があります。
表 C-1、表 C-2 を参考に、バッテリーバックアップ時間に十分余裕がある UPS 装置を選定してください。

表 C-1 構成ごとの皮相電力と有効電力 (HS3 シリーズ)

型名 ※x は数字	製品名	ノード数	最大皮相電力 (VA)	最大有効電力 (W)
NF7158-SBT60x	iStorage HS3-60	1	726	718
NF7158-SBT61x	iStorage HS3-60+10GbE-SR 2PORT	1	733	725
NF7158-SBT62x	iStorage HS3-60+10GbE-SR 4PORT	1	756	748
NF7158-SBT63x	iStorage HS3-60+10GbE-T 2PORT	1	736	728
NF7158-SBT64x	iStorage HS3-60+10GbE-T 4PORT	1	765	757
NF7159-SBT50x NF7159-SBT50xH NF7159-SBT50xD NF7159-SBT50xG	iStorage HS3-50S	1	500	498
NF7159-SBT51x NF7159-SBT51xC NF7159-SBT51xH NF7159-SBT51xJ NF7159-SBT51xD NF7159-SBT51xG	iStorage HS3-50S+10GbE-SR 2PORT	1	505	503
NF7159-SBT52x NF7159-SBT52xC NF7159-SBT52xH NF7159-SBT52xJ NF7159-SBT52xD NF7159-SBT52xG	iStorage HS3-50S+10GbE-SR 4PORT	1	514	513
NF7159-SBT53x NF7159-SBT53xH NF7159-SBT53xD NF7159-SBT53xG	iStorage HS3-50S+10GbE-T 2PORT	1	506	504
NF7159-SBT54x NF7159-SBT54xH NF7159-SBT54xD NF7159-SBT54xG	iStorage HS3-50S+10GbE-T 4PORT	1	518	515
NF7158-SBT50x	iStorage HS3-50	1	480	476
-	iStorage HS3-50+10GbE-SR 2PORT	1	491	486
-	iStorage HS3-50+10GbE-SR 4PORT	1	493	488
-	iStorage HS3-50+10GbE-T 2PORT	1	500	495
-	iStorage HS3-50+10GbE-T 4PORT	1	511	506

表 C-2 構成ごとの皮相電力と有効電力 (HS8 シリーズ)

型名 ※x は数字	製品名	HN	SN	L2 スイ ッチ	最大 皮相電力 (VA)	最大 有効電力 (W)
NF7158-SBS61x	iStorage HS8-60	1	0	0	809	806
NF7158-SBS620	iStorage HS8-60	1	1	0	1583	1578
NF7158-SBS62x	iStorage HS8-60	2	0	0	1618	1612
NF7158-SBS640	iStorage HS8-60	2	2	2	3402	3294
NF7158-SAS600	iStorage HS8-60 増設用ハイブリッドノード(72TB)	1	0	0	809	806
NF7158-SSS600	iStorage HS8-60 増設用ストレージノード(72TB)	0	1	0	774	772
-	iStorage HS8-60 の HN1 台に 10GbNIC (10GBASE-SR)x1 枚増設	1	0	0	816	813
-	iStorage HS8-60 の HN1 台に 10GbNIC (10GBASE-SR)x2 枚増設	1	0	0	814	811
-	iStorage HS8-60 の HN1 台に 10GbNIC (10GBASE-T)x1 枚増設	1	0	0	819	816
-	iStorage HS8-60 の HN1 台に 10GbNIC (10GBASE-T)x2 枚増設	1	0	0	820	817
NF7158-SWS600	iStorage HS8-60	0	0	1	118	69
NF7159-SBS51x NF7159-SBS51xH NF7159-SBS51xD NF7159-SBS51xG	iStorage HS8-50S	1	0	0	692	691
NF7159-SBS520 NF7159-SBS520H NF7159-SBS520D NF7159-SBS520G	iStorage HS8-50S	1	1	0	1368	1366
NF7159-SBS52x NF7159-SBS52xH NF7159-SBS52xD NF7159-SBS52xG	iStorage HS8-50S	2	0	0	1384	1382
NF7159-SBS540 NF7159-SBS540A NF7159-SBS540H NF7159-SBS540D NF7159-SBS540G	iStorage HS8-50S	2	2	2	2896	2892
NF7159-SAS500 NF7159-SAS500H NF7159-SAS500D NF7159-SAS500G	iStorage HS8-50S 増設用ハイブリッドノード(72TB)	1	0	0	692	691
NF7159-SSS500 NF7159-SSS500H NF7159-SSS500D NF7159-SSS500G	iStorage HS8-50S 増設用ストレージノード(72TB)	0	1	0	676	675
-	iStorage HS8-50S の HN1 台に 10GbNIC (10GBASE-SR)x1 枚増設	1	0	0	702	701
-	iStorage HS8-50S の HN1 台に 10GbNIC (10GBASE-SR)x2 枚増設	1	0	0	704	703
-	iStorage HS8-50S の HN1 台に 10GbNIC (10GBASE-T)x1 枚増設	1	0	0	703	702

型名 ※x は数字	製品名	HN	SN	L2 スイ ッチ	最大 皮相電力 (VA)	最大 有効電力 (W)
-	iStorage HS8-50S の HN1 台に 10GbNIC (10GBASE-T)x2 枚増設	1	0	0	706	705
NF7158-SBS51x	iStorage HS8-50	1	0	0	647	641
NF7158-SBS520	iStorage HS8-50	1	1	0	1145	1135
NF7158-SBS52x	iStorage HS8-50	2	0	0	1294	1282
NF7158-SBS540 NF7158-SBS540A	iStorage HS8-50	2	2	2	2466	2430
NF7158-SAS500	iStorage HS8-50 増設用ハイブリッドノード(48TB)	1	0	0	647	641
NF7158-SSS500	iStorage HS8-50 増設用ストレージノード(48TB)	0	1	0	498	494
-	iStorage HS8-50 の HN1 台に 10GbNIC (10GBASE-SR)x1 枚増設	1	0	0	653	646
-	iStorage HS8-50 の HN1 台に 10GbNIC (10GBASE-SR)x2 枚増設	1	0	0	663	656
-	iStorage HS8-50 の HN1 台に 10GbNIC (10GBASE-T)x1 枚増設	1	0	0	662	655
-	iStorage HS8-50 の HN1 台に 10GbNIC (10GBASE-T)x2 枚増設	1	0	0	681	674

2. 提供機能について

- (1) ESMPRO/AutomaticRunningController や ESMPRO/AC Enterprise が提供するスケジュール運転機能には対応していません。
- (2) Management Console などを用いて、直接 iStorage HS にログインすることはできません。
- (3) ESMPRO/AC Enterprise の AC Management Console から「指定サーバのシャットダウン」を選択して、iStorage HS の電源 OFF やリブートを実行しないでください。iStorage HS システムのノードの停止や再起動は、iStorage HS の GUI から実施してください。

3. ネットワークポートについて

- (1) iStorage HS は、電源制御端末との間で udp のポート : 6000 を使用して双方向で通信を行います。このポートをファイアウォールなどで閉じている場合は開放してください。

解放の対象は下記となります。

- 対象ポート : udp 6000
- 対象 IP アドレス
- iStorage HS の IP アドレス
アクセラレータノード機能を持つノードの外部 IP アドレス（実 IP アドレス）
※外部フローティング IP アドレスではありません。
- 電源制御端末の IP アドレス

4. 復電時の iStorage HS の自動起動について

以下の作業を実施した場合は、作業完了後 10 分以上経過してからシステムを再起動してください。

- iStorage HS 電源制御ソフトウェアのライセンス解除
- 管理機能の移動
- 管理ノードまたは代替ノードの交換（保守員作業）

これらの作業の完了後、復電時の自動起動に必要な設定が非同期に行われ、設定完了まで最大で 10 分程度かかります。

作業完了後 10 分以上経過してからシステムを再起動することで、復電時の自動起動設定が有効になり、復電時に iStorage HS が自動起動できるようになります。

索引

C

Command Line Interface (CLI) 71
Common Internet Filesystem (CIFS)..... 1

N

Network Filesystem (NFS) 1

V

VLAN Tagging..... 20

W

WORM (Write Once Read Many) 41

あ

アクセラレータノード機能クラスタ 23

て

ディスク容量
拡張可能..... 1

に

認証方式 47

は

パーティショニング 38
バックアップサーバ 16
バックアップネットワーク 15, 16
パリティ 45

ふ

フェイルオーバー 23

ま

マーカータイプ 40
マーカーフィルタリング 40

ら

ラックレスモデル 13

り

リモートサイト 25
領域解放 1

る

ルータ 16

れ

レプリケーション 25

付録 C オペレーティングシステムの設定

ここでは、本製品とオペレーティングシステムとの組み合わせで推奨する設定について説明します。ただし、オペレーティングシステムのベンダから提供されている説明書やホワイトペーパーを代替する説明ではありません。詳細は各ベンダのマニュアルを参照してください。ここで説明している内容を確認し、必要に応じて適用することを推奨します。

本付録は以下の構成となっています。

[1. iStorage HSの構成](#)

[2. Windows クライアント](#)

[3. Solarisクライアント](#)

[4. HP-UXクライアント](#)

[5. AIXクライアント](#)

[6. Red Hat Enterprise Linux\(RHEL\)クライアント](#)

1. iStorage HSの構成

iStorage HSは、複数のノードまたは単体のノードで構成されます。本製品のノードには、スケールアウトモデルとしてアクセラレータノード、ストレージノードとハイブリッドノードの3種類、シングルノードモデルとして1種類があります。

- アクセラレータノード(AN)
アクセラレータノード機能のみが動作する物理ノードです
- ストレージノード(SN)
ストレージノード機能のみが動作する物理ノードです
- ハイブリッドノード(HN)
アクセラレータノード機能とストレージノード機能の両者の機能を持った物理ノードです
- シングルノード
アクセラレータノード機能とストレージノード機能の両者の機能を持った物理ノードです
HNと異なり、他のノードと組み合わせてグリッド構成をとることはできません

複数のストレージノード機能が連携して巨大な一つの仮想ディスクを構成し、アクセラレータ機能を持つノードとお客様のバックアップ/リストアシステムを、CIFS(Common Internet FileSystem)またはNFS(Network File system)経由で接続することでiStorage HSへのバックアップ/リストアが可能になります。

(本書はCIFSまたはNFS経由でiStorage HSにバックアップ/リストアを行う環境を想定しています。ユニバーサル高速I/Oを利用する場合は「iStorage HSシリーズ ユニバーサル高速I/Oユーザーズガイド」を参照してください。)

バックアップソフトウェアを設定する際には、iStorage HSをバックアップデータの格納先ストレージデバイスとしてください。

以下にバックアップソフトウェアとiStorage HSの一般的な構成図を示します。

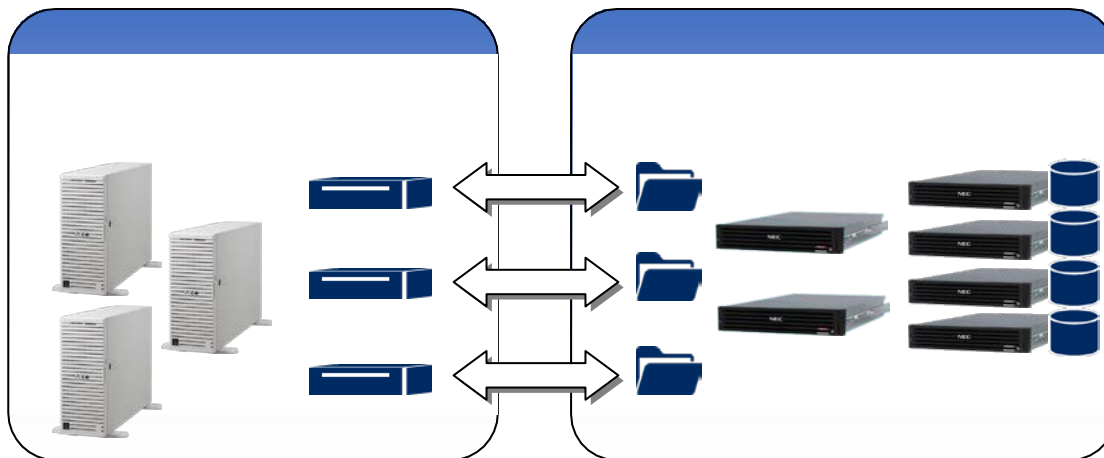


図 1: iStorage HS 構成図

1-1 推奨MTUの設定

バックアップサーバとiStorage HS間のネットワークがジャンボフレームに対応している場合は、MTUの設定を変更することで性能が向上する可能性があります。

GUIまたはCLIでMTUの設定を 9000 に変更してください。

設定方法については「iStorage HS シリーズ ユーザーズガイド」、または「iStorage HS シリーズ コマンドリファレンス」を参照してください。

バックアップサーバのMTUを変更する手順はご利用のOSのマニュアルを参照してください。

その他 iStorage HSご利用時のネットワークの構成については「第2章 配備計画 Step 2. ネットワークの計画」を参照してください。

1-2 NFSのポート設定

iStorage HSのNFS機能で使用するポートは以下です。このため、ファイアウォールにおいて、以下のポートが開放されている必要があります。

```
tcp/udp 111  
tcp/udp 2049  
tcp/udp 61001  
tcp/udp 61002  
tcp/udp 61003
```

また、NFSクライアント側では、以下のポートが開放されている必要があります。
なお、ポート番号はNFSクライアントのマニュアルを参照してください。

```
portmap  
nlm(nlockmgr)  
nsm(status)
```

2. Windows クライアント

2-1 TCPパラメータの設定

Windows 2008、Windows 2008 R2をご利用の場合、複数台のWindowsクライアントを用いて書き込みを行うと、パケットロスが発生し、iStorage HSの性能が向上しないことがあります。

本現象は、ウィンドウ自動チューニング・レベルの受信機能を無効にすることで解決する可能性があります。コマンドプロンプト(cmd.exe)を起動し、以下のコマンドを実行して、ウィンドウ自動チューニング・レベルの受信機能を無効にしてください。

```
netsh interface tcp set global autotuninglevel=disabled
```

Windows 2008、Windows 2008 R2以外をご利用の場合、TCP受信/送信バッファ等をチューニングする必要はありません。

2-2 TSO/LSOの設定

TSO(TCPセグメンテーションオフロード)はネットワークカード(NIC)が持つ機能の一つで、TCPパケット転送処理の一部をCPUに変わってNICが実行する機能です。NICによってはLSO(ラージセンドオフロード)あるいは、大量送信オフロードと呼ばれることがあります。WindowsクライアントのCPUリソースに余力がある場合、TSO/LSOを無効にすることで、通信性能が改善される場合があります。

TSO/LSOを無効にする方法は、通常はデバイスマネージャからNICのプロパティを開いて詳細設定のタブで設定をします。ただし、詳細な設定方法はNIC毎に異なるため、ご利用のNICのマニュアルを確認してください。

2-3 セッションタイムアウト値の設定

使用しているアプリケーションの書き込みジョブ等がWindowsのセッションタイムアウトにより失敗するのを防ぐため、セッションタイムアウト値を変更します。

レジストリエディタ(REGEDT32.EXE)を起動し、以下の場所に移動します。

```
HKEY_LOCAL_MACHINE
  SYSTEM
    CurrentControlSet
      Services
        LanmanWorkstation
          Parameters
```

「SessTimeout」レジストリパラメータを10分に設定します。タイプと値は以下のとおりです。

名前: SessTimeout
 タイプ: REG_DWORD
 データ: 00000258 (16 進数)
 (デフォルト値は 45 (秒))

2-4 CIFSの認証方式としてActiveDirectoryを使用する場合

CIFSの認証方式としてActiveDirectoryを使用する場合、クライアントは以下のどちらかのドメインに参加している必要があります。

- iStorage HS の所属するドメインと同じドメイン
- iStorage HS の所属するドメインと信頼関係が結ばれている信頼関係先ドメイン

上記のドメインへ参加していない場合、iStorage HSへのアクセスが失敗します。

2-5 SNPの設定

SNP(Scalable Networking Pack)は、ネットワークのスループットを向上する機能であり、Windows OSとネットワークドライバ、およびネットワークアダプタが連携して実現される機能です。しかし、SNPを有効にした場合に、ネットワークのパフォーマンス低下が発生する事例などが報告されており、安定した技術ではないことも確認されています。このため、ネットワーク性能にネックがある場合には、SNP機能が有効になっていないか確認をしてください。SNP機能が有効となっている場合には、SNP機能を無効に設定してご利用されることを推奨します。

Expressシリーズにおいては、以下の注意事項を参照して、SNP無効化の設定をしてください。

- Scalable Networking Pack(SNP)の使用上の注意事項について
<http://support.express.nec.co.jp/care/techinfo/snp.html>

2-6 推奨MTUの設定

MTU(Maximum transmission unit)とはネットワークで転送可能な最大パケットサイズです。MTU が大きすぎると、経路上のルータなどが処理できず通信できなくなります。MTUが小さすぎる場合、TCP のオーバーヘッドが大きくなり性能が低下します。以下に Windows OSでMTUを変更し、ジャンボパケットに対応させる手順を示します。いずれかの方法で設定を行ってください。

コマンドで設定する場合

1. 現在のMTUの設定を確認(以下の例では1500が設定されています)

```
C:\>netsh interface ipv4 show subinterfaces
```

MTU	MediaSenseState	受信バイト	送信バイト	インターフェース
4294967295		1	0	1576 Loopback
Pseudo-Interface 1				
1500		5	0	0 Ethernet
1500		1	42762674596	121789270695 Ethernet 2

```
C:\>
```

2. MTU を9000に変更

```
netsh interface ipv4 set subinterface "Ethernet 2" mtu=9000store=persistent
```

ドライバ設定から変更する場合

ドライバ設定からMTUを変更する手順はご利用のNICのマニュアルを参照してください。以下はIntel社製のNICでMTU 変更する場合の例です。

1. コントロールパネルで「ネットワークと共有センター」を選択
2. 「アダプターの設定の変更」を選択
3. NICを右クリックし、「プロパティ」を選択
4. 「構成(C)」ボタンを押下
5. 「詳細設定」タブを選択
6. 「ジャンボ パケット」を選択して値を「9014バイト」に変更

3. Solarisクライアント

3-1 TCPパラメータの設定

/etc/rc3.d/S90hsファイルを作成します。ファイルに以下の2行を入力し、TCPパラメータを設定します。

```
ndd -set /dev/tcp tcp_recv_hiwat 131072
(デフォルトの受信ウィンドウサイズをバイト単位で設定します。)

ndd -set /dev/tcp tcp_xmit_hiwat 131072
(デフォルトの送信ウィンドウサイズをバイト単位で設定します。)
```

3-2 NFSパラメータの設定

/etc/system.dディレクトリに任意のファイル名で以下を記述したファイルを追加します。(*1) (*2)

```
set nfs:nfs3_bsize=131072
(NFSクライアントによって使用される論理ブロックサイズを設定します。)

set nfs:nfs3_max_transfer_size=131072
(NFSのデータ転送サイズの最大値を設定します。)

set nfs:nfs3_max_threads=16
(NFSクライアントに対し非同期入出力を実行するカーネルスレッドの数を設定します。)
```

(*1) 指定された値は、ブート時に読み込まれ適用されます。上記ファイルを修正後、ファイルに対する変更を有効にするためシステムをリブートしてください。

(*2) Solaris10以前のバージョンでは/etc/system.dディレクトリが存在しないため、/etc/systemファイルに設定を追加してください。

通常、上記設定を行えば iStorage HSへの書き込み性能は向上します。

上記設定を行っても、Solarisクライアントからcommit要求が高頻度で発行されることで、iStorage HSへの書き込み性能が低下している場合は、以下のパラメータの値を調整することで改善できる可能性があります。以下のパラメータを4～8程度に変更して、効果を検証の上、利用してください。

```
nfs:nfs3_async_clusters(デフォルト 1)
(NFSクライアントによって生成される非同期要求の組み合わせを制御します。)
```

3-3 NFSマウント時の設定

ファイルシステムのマウント時、iStorage HSのデータ転送サイズの推奨値は読み込み131072バイト、書き込み32768バイトです。
マウントオプションの例を以下に示します。

```
# mount -F nfs -o  
hard,intr,proto=tcp,vers=3,rsz=131072,wsz=32768,bg  
HYDRAstor_AN01:/export/fs1 /HYDRAstor/fs1
```

3-4 MTUの設定

MTU(Maximum transmission unit)とはネットワークで転送可能な最大パケットサイズです。MTU が大きすぎると、経路上のルータなどが処理できず通信できなくなります。MTUが小さすぎる場合、TCP のオーバーヘッドが大きくなり性能が低下します。MTUの設定変更についてはSolarisのドキュメントを参照してください。

4. HP-UXクライアント

4-1 TCPパラメータの設定

以下の2つのコマンドを実行して、TCPの送受信サイズを設定し、NFSを再マウントして値を有効にします。

```
# ndd -set /dev/tcp tcp_recv_hiwater_def 262144
# ndd -set /dev/tcp tcp_xmit_hiwater_def 262144
```

nddコマンドを発行すると、変更が直ちに反映されます。リブートの必要はありません。この設定値は、リブート後はデフォルトに戻ります。リブート後に毎回この値が設定されるようにするには/etc/rc.config.d/nddconf ファイルに以下の要領で記述します。

```
TRANSPORT_NAME[num]=tcp
NDD_NAME[num]=tcp_recv_hiwater_def
NDD_VALUE[num]=262144

TRANSPORT_NAME[num + 1]=tcp
NDD_NAME[num + 1]=tcp_xmit_hiwater_def
NDD_VALUE[num + 1]=262144
```

numは0から順に1ずつ増やしていく必要があります。

/etc/rc.config.d/nddconfに既に定義がある場合は、numが0から順に振られているはずですので、その次の値をnumとして定義を行ってください。定義が一つもない場合はnumを0として定義してください。

4-2 NFSパラメータの設定

HP-UX 11i v3,v2をご利用の場合、NFSのデータ転送サイズの最大値を設定してください。HP-UX 11i v1をご利用の場合、設定の必要はありません。

HP-UX 11i v3をご利用の場合、以下のコマンドを実行してください。

```
# kctune nfs3 bsize=131072
```

HP-UX 11i v2をご利用の場合、以下の2つのコマンドを実行してください。

```
# kctune nfs3_max_transfer_size=65536
# kctune nfs3 max transfer size cots=65536
```

4-3 NFSマウント時の設定

ファイルシステムのマウント時、iStorage HSのデータ転送サイズの推奨値はHP-UX 11i v3では読み込み131072バイト、書き込み32768バイト、HP-UX 11i v2では読み込み65536バイト、書き込み32768バイト、HP-UX 11i v1では読み込み、書き込みともに32768バイトです。

マウントオプションの例を以下に示します。

HP-UX 11i v3

```
# mount -F nfs -o
  hard,intr,proto=tcp,vers=3,rsiz=131072,wsiz=32768,bg
HYDRAsor_AN01:/export/fs1 /HYDRAsor/fs1
```

HP-UX 11i v2

```
# mount -F nfs -o
  hard,intr,proto=tcp,vers=3,rsiz=65536,wsiz=32768,bg
HYDRAsor_AN01:/export/fs1 /HYDRAsor/fs1
```

HP-UX 11i v1

```
# mount -F nfs -o
  hard,intr,proto=tcp,vers=3,rsiz=32768,wsiz=32768,bg
HYDRAsor_AN01:/export/fs1 /HYDRAsor/fs1
```

4-4 NFSの性能向上に関する推奨設定

HP-UXをクライアントとして使用する際、NFSの性能を向上させるための推奨パラメータ、推奨パッチ等を示します。

4-4.1 HP-UX 11i v3の推奨設定

HP-UX 11i v3使用時の推奨メモリサイズ

HP-UX 11i v3では、メモリのサイズが小さい場合、`nfscommit`要求が高頻度で発行されるため、iStorage HSへの書き込み性能に大きな影響を及ぼします。
iStorage HSとの組み合わせでご利用いただく場合は、**8GB以上のメモリ**を搭載して下さい。

HP-UX 11i v3使用時の推奨パッチ(プロダクト)

HP-UX 11i v3のNFSに関する修正や機能拡張は、パッチリリースによる対応ではなく、ONCplusプロダクトのバージョンアップが必要となります。ONCplusプロダクトはB.11.31.09以降を適用してください。
適用方法に関しては、HP社から提供されている情報を参考にしてください。

HP-UX 11i v3使用時の推奨パラメータ値

`nfs_enable_write_behind=1`

以下のコマンドを実行し、パラメータに値を設定します。パラメータに値を設定後、システムをリブートし、値を有効にします。

```
# kctune nfs_enable_write_behind=1
# shutdown -r
```

その他、推奨するカーネルパラメータを下表に示します。

パラメータ	変更コマンド
nfs_enable_enhanced_commit(default: 0)	kctune nfs_enable_enhanced_commit=1
nfs3_max_threads(default: 8)	kctune nfs3_max_threads=16
nfs3_bsize	kctune nfs3_bsize=262144
fcache_fb_policy	kctune fcache_fb_policy=1
lcpu_attr	kctune lcpu_attr=1
nfs_enable_write_behind	kctune nfs_enable_write_behind=1 (リブートが必要)
fs_async	kctune fs_async=1
nfs3_max_transfer_size	kctune nfs3_max_transfer_size=4194304

4-4.2 HP-UX 11i v2の推奨設定

HP-UX 11i v2使用時の推奨パッチ(プロダクト)(2010 年 9 月時点)

PHNE_38503: s700_800 11.23 Core NFS cumulative patch
 PHNE_40953: s700_800 11.23 Kernel RPC cumulative patch
 PHNE_40955: s700_800 11.23 NFS cumulative patch
 PHNE_36981: s700_800 11.23 RPC commands and daemons cumulative patch
 PHNE_38905: s700_800 11.23 Lock Manager cumulative patch
 HP-UX BalancedFreelist 1.0 for HP-UX 11i version 2

HP-UX 11i v2使用時の推奨パラメータ値

nfs_fine_grain_fs_lock=2
 nfs_async_read_avoidance_enabled=1
 nfs_clnt_avoid_write_copy=1
 nfs_wakeup_one=1
 nfs3_adaptive_cache_validate=1

以下のコマンドを実行し、パラメータに値を設定します。パラメータに値を設定後、システムをリブートし、値を有効にします。

```
# kctune nfs_fine_grain_fs_lock=2
# kctune nfs_async_read_avoidance_enabled=1
# kctune nfs_clnt_avoid_write_copy=1
# kctune nfs_wakeup_one=1
# kctune nfs3_adaptive_cache_validate=1
# shutdown -r
```

/etc/rc.config.d/nfsconf ファイルに定義されている以下のパラメータを変更します。

```
NUM_NFSIOD=0
```

4-4.3 HP-UX 11i v1の推奨設定

HP-UX 11i v1 使用時の推奨パッチ

PHNE_41023:	s700_800 11.11 ONC/NFS General Release/Performance Patch
PHKL_30398:	s700_800 11.11 KI FSS ID and KI_rfscall
PHKL_34595:	s700_800 11.11 VM NFS umount fix
PHKL_41041:	s700_800 11.11 nfs clinet hang
PHKL_38736:	s700_800 11.11 select_enh tunable;Buffer Cache Perf
PHKL_36133:	s700_800 11.11 Cumulative VM, Psets, Preemption, PRM, MRG
PHKL_39133:	s700_800 11.11 SPP fragmentation;AIO;EVP;ufalloc;dup2 race
PHCO_27957:	s700_800 11.11 umount(1M) cumulative patch
PHCO_33205:	s700_800 11.11 mountall, Dev IDs enabler, iSCSI support

HP-UX 11i v1使用時の推奨パラメータ値

```
nfs_wakeup_one=1
nfs3_adaptive_cache_validate=1
```

以下のコマンドを実行し、パラメータに値を設定します。パラメータに値を設定後、システムをリブートし、値を有効にします。

```
# echo 'nfs_wakeup_one?W 0x1' | adb -w -k /stand/vmunix
/dev/kmem
# echo 'nfs3_adaptive_cache_validate?W 0x1' | adb -w
-k/stand/vmunix/dev/kmem
# shutdown -r
```

/etc/rc.config.d/nfsconfファイルに定義されている以下のパラメータを変更します。

```
NUM_NFSIOD=0
```

4-5 Bondingに関する注意事項

HP-UXクライアントを使用される場合は、**balance-rr**以外の**bonding**モードを選択することを推奨します。

iStorage HSの外部ネットワーク接続で**bonding**モードとして**balance-rr**を使用した場合、ネットワーク性能が低速化する場合があります。

4-6 MTUの設定

MTU(Maximum transmission unit)とはネットワークで転送可能な最大パケットサイズです。MTUが大きすぎると、経路上のルータなどが処理できず通信できなくなります。MTUが小さすぎる場合、TCP のオーバーヘッドが大きくなり性能が低下します。MTUの設定変更についてはHP-UXのドキュメントを参照してください。

5. AIXクライアント

5-1 TCPパラメータの設定

AIXではメモリが動的に割り当てられるので、AIXクライアントはTCP受信/送信バッファ等をチューニングする必要はありません。

5-2 NFSパラメータの設定

iStorage HSの使用するNFS用のポートにアクセス許可を与えるために、ファイルシステムをマウントする前に以下のいずれかを実施して下さい。

なお、本書では信頼性確保のため、前者の設定方法を推奨します。

- (1) `nfs_use_reserved_ports`に1を設定する。

```
# nfsd -o nfs use reserved ports=1
```

- (2) ファイルシステムの「1024番以上のポートからのアクセスを拒否する。(secure)」オプションを無効にする。

上記オプションが有効になっているとiStorage HSのファイルシステムをAIXクライアントからマウントできません。

上記オプションの設定は、ファイルシステム単位に iStorage HSGUI/CLIから行えます。以下にGUI から上記オプションを無効にする手順を示します。

CLI から設定する場合は、「iStorage HS シリーズ コマンドリファレンス」を参照してください。

ファイルシステム作成時に上記オプションを無効にする場合

ファイルシステム作成時に「1024番以上のポートからのアクセスを拒否する。(secure)」チェックボックスを外して下さい。

ファイルシステム作成

ファイルシステムオプション

ファイルシステム名: fs1

ノード: AN 01 01

エクスポートタイプ: ☒ NFS ☐ CIFS

容量: ファイルシステムの容量: 256 PB

☐ ハードクォータを有効にする

☐ ソフトクォータを有効にする ソフトリミット: 90 %

パリティ数: 3 (オーバーヘッド: 25%)

説明:

エクスポートオプション

エクスポート名: /export/fs1

接続許可クライアント: *

① エントリを分けるには半角スペースを使用します。

アクセス権限: ☒ 読み書き ☐ 読み取り専用

ユーザアクセス: 全てのユーザを匿名ユーザとしてアクセスさせる。(all_squash)

① 匿名ユーザ: UID=1000, GID=1000

その他のオプション: ☐ 1024番以上のポートからのアクセスを拒否する。(secure)

OK キャンセル

既存のファイルシステムの上記オプションを無効にする場合

ファイルシステムを選択し、ファイルシステム変更画面で「1024番以上のポートからのアクセスを拒否する。(secure)」チェックボックスを外して下さい。

ファイルシステム変更(fs1)

容量: ファイルシステムの容量: 256 PB

☐ ハードクォータを有効にする

☐ ソフトクォータを有効にする ソフトリミット: %

格納済み容量: 1.1KB

パリティ数: 3

オーバーヘッド: 25%

説明:

作成日時: 2011/03/17 10:23:56

① 上記のファイルシステムの容量と格納済み容量は2のべき乗に基づく単位で表示しています。(GB = 1024 × 1024 × 1024)

エクスポートオプション

エクスポート名: /export/fs1

接続許可クライアント: *

① エントリを分けるには半角スペースを使用します。

アクセス権限: ☒ 読み書き ☐ 読み取り専用

ユーザアクセス: 全てのユーザを匿名ユーザとしてアクセスさせる。(all_squash)

① 匿名ユーザ: UID=1000, GID=1000

その他のオプション: ☐ 1024番以上のポートからのアクセスを拒否する。(secure)

OK キャンセル

5-3 Virtual Memory Manager(VMM)の設定

AIX 5.3使用時の推奨VMMパラメータ値を以下に示します。AIX 6.1において推奨値はデフォルトの値と同じになるため、下記パラメータを設定する必要はありません。

```
minperm% = 5
maxperm% = 90
maxclient% = 90
lru_file_repage = 0
page_steal_method = 1
```

設定例を示します。(*1)(*2)

```
# vmo -r -o minperm%=5
# vmo -r -o maxperm%=90
# vmo -r -o maxclient%=90
# vmo -r -o lru_file_repage=0
# vmo -r -o page_steal_method=1
```

- (*1) `page_steal_method`パラメータ変更時には、`bosboot`が必要になります。上記コマンド実行時に、“Run bosboot now?”と表示されるので、“yes”と入力して、`bosboot`を実行してください。
- (*2) 上記設定例で変更されたパラメータは、システム再起動後に有効になります。設定後に必ずシステム再起動を行ってください。

5-4 NFSマウント時の設定

ファイルシステムのマウント時、iStorage HSのデータ転送サイズの推奨値は読み込み65536バイト、書き込み32768バイトです。
マウントオプションの例を以下に示します。

```
# mount -V nfs -o llock,intr,hard,rsz=65536,wsz=32768,
proto=tcp,timeo=600,retrans=2
HYDRAstor_AN01:/export/fs1 /HYDRAstor/fs1
```

5-5 MTUの設定

MTU(Maximum transmission unit)とはネットワークで転送可能な最大パケットサイズです。MTUが大きすぎると、経路上のルータなどが処理できず通信できなくなります。MTUが小さすぎる場合、TCP のオーバーヘッドが大きくなり性能が低下します。MTUの設定変更についてはAIXのドキュメントを参照してください。

6. Red Hat Enterprise Linux(RHEL)クライアント

6-1 TCPパラメータの設定

TCP受信/送信バッファ等をチューニングする必要はありません。

6-2 NFSマウント時の設定

ファイルシステムのマウント時、iStorage HSのデータ転送サイズの推奨値はRHELでは読み込み131072バイト、書き込み32768バイトです。
マウントオプションの例を以下に示します。

RHEL

```
# mount -t nfs -o  
hard,intr,nfsvers=3,tcp,rsz=131072,wsz=32768,bg  
HYDRAsor_AN01:/export/fs1 /HYDRAsor/fs1
```

6-3 MTUの設定

MTU(Maximum transmission unit)とはネットワークで転送可能な最大パケットサイズです。
MTU が大きすぎると、経路上のルータなどが処理できず通信できなくなります。MTUが小さすぎる場合、TCP のオーバーヘッドが大きくなり性能が低下します。MTUの設定変更についてはRHELのドキュメントを参照してください。

6-4 ユニバーサル高速 I/Oの利用

RHELではメモリ不足時に大量の同期書き込みが発生し、バックアップが大幅に遅延する現象が発生することがあります。ユニバーサル高速I/Oを利用するとこの問題を回避することが可能です。バックアップサーバのOSとしてRHELを使用する場合はユニバーサル高速I/Oの利用を推奨します。

付録 D バックアップソフトウェアの設定

ここでは、本製品とバックアップソフトウェアとの組み合わせで推奨する設定について説明します。ただし、バックアップソフトウェアのベンダから提供されている説明書やホワイトペーパーを代替する説明ではありません。詳細は各ベンダのマニュアルを参照してください。ここで説明している内容を確認し、必要に応じて適用することを推奨します。

本付録は以下の構成となっています。

[Arcserve Backup](#)

[Backup Exec](#)

[Commvault](#)

[Data Protector](#)

[Veritas NetBackup](#)

[NetVault Backup](#)

[NetWorker](#)

[Oracle Exadata Database Machine](#)

[Spectrum Protect](#)

[Veritas System Recovery](#)

Arcserve Backup

1. iStorage HSの設定

1-1 バックアップ先ファイルシステム名の文字数に関する注意点

iStorage HSのファイルシステムをArcserve Backupのリモートファイルシステムデバイスとして設定する場合、リモートファイルシステムデバイスを指定するファイルシステム名の合計の文字数が32文字以上になると、バックアップ/リストア性能の低下が発生する場合があります。もし、このような現象が発生した場合には、リモートファイルシステムデバイスに指定するバックアップ先ファイルシステム名を、UNC パス形式で合計の文字数が 31 文字以下になるように設定してください。

例えば、iStorage HSに作成したファイルシステムの直下に「ディレクトリ1」があり、その下にある「ディレクトリ2」をバックアップ先とし、ファイルシステムに対して「¥¥xxx.xxx.xxx¥¥{ファイルシステム}¥{ディレクトリ1}¥{ディレクトリ2}¥」とアクセスする場合、「ファイルシステム」名・「ディレクトリ1」名・「ディレクトリ2」名は合わせて 11 文字以内になるように設定する必要があります。

1-2 マーカーフィルタリング

Arcserveでは、マーカーと呼ばれる管理情報をバックアップ対象ファイル毎に付加します。付加されたマーカーはバックアップ毎にユニークになる場合があるため、バックアップデータの重複排除率を低下させる要因になることがあります。ファイルシステムのマーカーフィルタリングオプションは、このマーカーのフィルタリングを行ない、データ保存時の重複排除機能を最適化するオプションです(*1)(*2)。

バックアップ対象ファイル毎に付加されるマーカーは、バックアップ対象ファイルのサイズが小さいと重複排除を阻害する要因となりますが、ファイルサイズが大きい場合は重複排除機能に及ぼす影響は小さくなります。

目安としてバックアップ対象ファイルの平均ファイルサイズが1MB以下の場合、マーカーフィルタリング機能を使用することを推奨します。

マーカーフィルタリングオプションの設定は、ファイルシステムの作成時にiStorage HSのGUI/CLIから行えます。GUIから設定する場合は、ファイルシステムの作成時に「マーカーフィルタリング」の「有効」のチェックボックスを選択し、マーカータイプとして"ARC1(Arcserve Backup)"を選択します。

ファイルシステム作成

後援計画ファイルシステム

① エントリを分けるには半角スペースを使用します。

アクセス権限 ☒ 読み書き ☐ 読み取り専用

ユーザアクセス 全てのユーザを匿名ユーザとしてアクセスさせる。(all_squash)

① 匿名ユーザ: UID=1000、GID=1000

その他のオプション ☒ 1024番以上のポートからのアクセスを拒否する。(secure)

高度なオプション

マーカーフィルタリング ☒ 有効 ARC1(Arcserve Backup)

フェイルオーバー -

WORM 無効 (WORMライセンスがない)

ACL ☐ 有効

ファイル情報 ☐ ファイル属性 ☐ タイムスタンプ ☐ アクセス日時

暗号化 ☐ 有効

暗号化キー

⚠ フェイルオーバーが使用可能な場合のみフェイルオーバー設定は有効になります。

OK キャンセル

詳細なファイルシステムの作成方法については「iStorage HSシリーズ ユーザーズガイド」を参照してください。また、CLIから設定する場合は「iStorage HSシリーズ コマンドリファレンス」を参照してください。

マーカーフィルタリングオプションを使用する場合の注意事項を以下に列挙します。各機能についての説明は「iStorage HSシリーズ ユーザーズガイド」を参照してください。

- ファイルシステムの作成後は、マーカーフィルタリングの設定を変更することはできません。
- レプリケーションセットのマスタとレプリカでは、同じマーカーフィルタリングとマーカータイプを持っている必要があります。
- マーカーフィルタリングが有効となっているファイルシステムがレプリケーションの対象となっている場合、初回のレプリケーションが終了するまで、レプリカのファイルシステムはエクスポートできません。

(*1) マーカータイプ“ARC1(Arcserve Backup)”は iStorage HSバージョン5.0.5から利用可能です。

(*2) rawバックアップでは、マーカーがほぼ挿入されないため本オプションの指定は不要です。

2. Arcserve Backupの設定

2-1 iStorage HSをリモートファイルシステムデバイスとして設定

iStorage HSのファイルシステムをArcserve Backupのバックアップデータの格納先となるリモートファイルシステムデバイスと指定してください。Arcserve Backupのディスクベースのストレージに対して有効なチューニング項目はiStorage HSに対しても有効です。

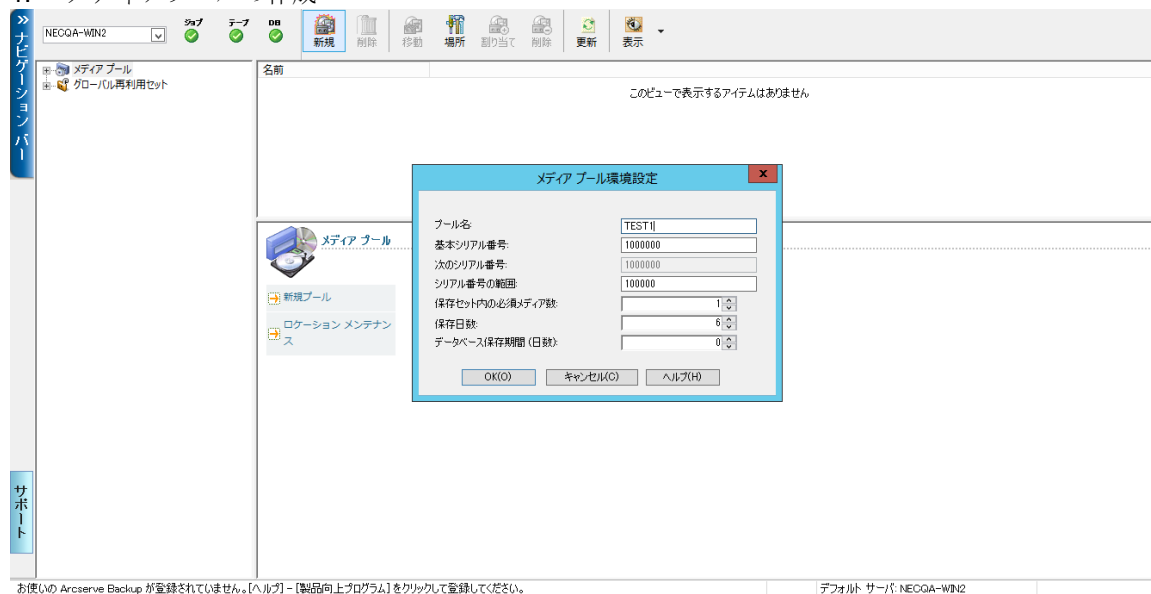
2-2 複数ジョブ実行設定

Arcserve Backupで複数のバックアップジョブを並列実行する場合、下記手順で行ってください。

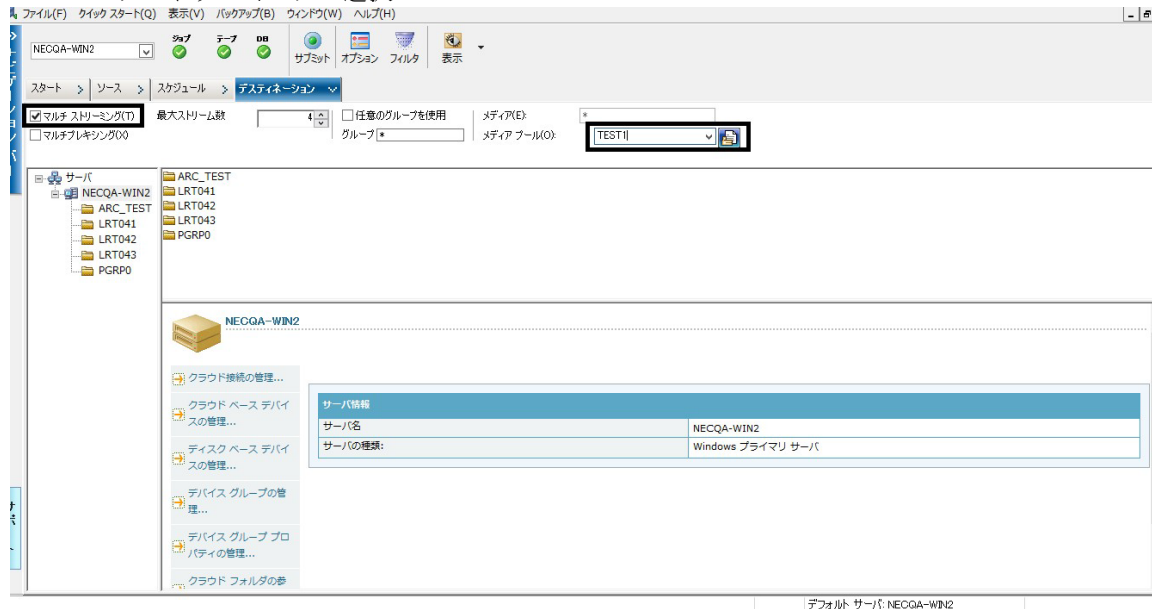
1. メディアプールを作成し、デスティネーションタブで作成したプールを選択
2. デスティネーションタブでマルチストリーミングのチェックボックスを選択

【詳細】

1. メディアプールの作成



2. マルチストリーミングの選択



2-3 Arcserve Backupの圧縮 / 暗号化機能

iStorage HSではバックアップ時に物理データ圧縮と重複排除を行っています。Arcserve Backup による圧縮処理はバックアップサーバ上で実行されるため、バックアップ性能に影響を与える可能性があります。このため、Arcserve Backupのポリシー設定時に圧縮機能を無効にしてください。

また、Arcserve Backup 設定時に暗号化機能を有効にした場合、iStorage HSでの重複排除率に影響を及ぼす可能性があります。Arcserve Backupのポリシー設定時に暗号化機能を無効にしてください。

2-4 Arcserve Backupの重複排除バックアップ機能

Arcserve Backupの重複排除機能を利用した場合、iStorage HSでの重複排除率が低下するため、Arcserve Backupでの重複排除機能を無効とすることを推奨します。

3. バックアップサーバの設定

iStorage HS に対してより高速なバックアップ/リストアを行うには、Arcserve Backup がインストールされているバックアップサーバの設定変更が必要になります。
バックアップサーバの設定については「付録C オペレーティングシステムの設定」を参照してください。

4. ネットワークの構成

iStorage HS に対してより高速なバックアップ/リストアを行うには、専用のネットワークの利用を推奨します。ネットワークを専用とすることで、バックアップ/リストア用の帯域幅が他の通信により減少することを防ぐことができます。
iStorage HS 利用時のネットワークの構成については「第2章 配備計画 Step 2. ネットワークの計画」を参照してください。

5. Arcserve Backup運用時の注意事項

5-1 小さなサイズのファイルのバックアップ

Arcserve Backupを用いてiStorage HSへのバックアップ処理を行う際、バックアップするデータに数十 KB未満の小さなファイルが多く含まれていると、iStorage HSの重複排除率は低くなります(*1)。これは、Arcserve Backupが各バックアップ対象ファイルのヘッダ部に管理情報を付加することに起因します。

iStorage HSではブロックレベルで重複データを検出し、重複しないユニークなデータのみを圧縮・格納することによって効率的なストレージ格納容量を実現します。(DataRedux®)

Arcserve Backupの管理情報はバックアップ対象ファイル毎に付加されます。そのため、iStorage HS がバックアップデータをブロックレベルに分割する際に、バックアップデータに数十KB未満の小さなファイルが含まれていると、分割されたバックアップデータの個々のブロックの多くに Arcserve Backup によって付加された管理情報が含まれることになります。この付加された管理情報には、バックアップ毎にユニークな情報が含まれます。そのため、管理情報が含まれたブロックは前回バックアップ時と比べて重複しないユニークなデータとみなされ、排除されずに iStorage HSへ格納されます。これによって iStorage HSの重複排除率は低くなります。

(*1) iStorage HS のマーカーフィルタリング機能を使用すれば、小ファイルのバックアップにおける重複排除率の低下を防ぐことができます。マーカーフィルタリング機能はiStorage HSバージョン5.0.5から利用可能です。詳しくは、「2-2 マーカーフィルタリング」を参照してください。

5-2 ANクラスタ機能の利用

iStorage HSでは、複数のHN/ANを組み合わせて高可用性クラスタを構成することができます (ANクラスタ機能)。ANクラスタに組まれているHN/ANの障害時には、他の正常に稼動しているHN/ANに対し、IPアドレスおよびファイルシステムを引き継ぎ、障害発生時に停止したサービスを、ANクラスタの他のHN/ANによって自動的に再開することが可能です。障害が発生したHN/ANのIPアドレスおよびファイルシステムを、他のHN/ANに引き継ぐ操作を「フェイルオーバー」、他のHN/ANに引き継がれたIPアドレスおよびファイルシステムを、復旧したHN/ANに戻す操作を「テイクバック」といいます。

Arcserve BackupにおいてANクラスタ機能を有効にする場合、バックアップ/リストア中にフェイルオーバーが発生した場合、実行されているバックアップ/リストアは失敗し、エラーとなります。フェイルオーバーの完了後、手動でバックアップ/リストアを再実行してください。失敗した時点からの再開ではなく、最初からやり直しとなります。

5-3 トラブルシューティングについて

バックアップソフトウェア固有の問題が発生した場合は、バックアップソフトウェアのログを収集しArcserve Backupのご購入元へ確認を行ってください。ログの収集手順はお使いのArcserve Backupのマニュアルを参照してください。

iStorage HSで問題が発生した場合は、イベントを確認し、「iStorage HSシリーズ メッセージハンドブック」を参照して適切な対処を行ってください。iStorage HSでは、メール通報、SNMPインタフェース、イベントビューアといった3つの方法を利用してイベントを受信できます。それぞれの設定方法については、「iStorage HSシリーズ ユーザーズガイド」を参照してください。

Backup Exec

1. iStorage HSの設定

iStorage HSをBackup Execとの組み合わせでお使いいただく場合、iStorage HSで必要となる特別な設定はありません。

2. Backup Execの設定

2-1 iStorage HSをディスクへのバックアップフォルダとして設定

iStorage HSのファイルシステムをBackup Execのバックアップデータの格納先ディスクへのバックアップフォルダとしてください。Backup Execのディスクベースのストレージに対して有効なチューニング項目はiStorage HSに対しても有効です。

3. バックアップサーバの設定

iStorage HSに対してより高速なバックアップ/リストアを行うには、Backup Execがインストールされているバックアップサーバの設定変更が必要になります。
バックアップサーバの設定については「付録C オペレーティングシステムの設定」を参照してください。

4. ネットワークの構成

iStorage HSに対してより高速なバックアップ/リストアを行うには、専用のネットワークの利用を推奨します。ネットワークを専用とすることで、バックアップ/リストア用の帯域幅が他の通信により減少することを防ぐことができます。

iStorage HS利用時のネットワークの構成については「第2章 配備計画 Step 2. ネットワークの計画」を参照してください。

5. Backup Exec運用時の注意事項

5-1 小さなサイズのファイルのバックアップ

Backup Execを用いてiStorage HSへのバックアップ処理を行う際、バックアップするデータに数十KB未満の小さなファイルが多く含まれていると、iStorage HSの重複排除率は低くなります。これは、Backup Execが各バックアップ対象ファイルのヘッダ部に管理情報を付加することに起因します。

iStorage HSではブロックレベルで重複データを検出し、重複しないユニークなデータのみを圧縮・格納することによって効率的なストレージ格納容量を実現します。(DataRedux®)

Backup Execの管理情報はバックアップ対象ファイル毎に付加されます。そのため、iStorage HSがバックアップデータをブロックレベルに分割する際に、バックアップデータに数十KB未満の小さなファイルが含まれていると、分割されたバックアップデータの個々のブロックの多くにBackup Execによって付加された管理情報が含まれることになります。この付加された管理情報には、バックアップ毎にユニークな情報が含まれます。そのため、管理情報が含まれたブロックは前回バックアップ時と比べて重複しないユニークなデータとみなされ、排除されずにiStorage HSへ格納されます。これによってiStorage HSの重複排除率は低くなります。

5-2 ANクラスタ機能を用いる際のリトライ設定

Backup Execを用いたiStorage HSへのバックアップ処理実行中、バックアップ先HN/ANに障害が発生した場合でも、iStorage HSのANクラスタ機能を利用してバックアップを再試行させるための設定について記述します。

以下の2パターンについて記述します。設定変更が必要な場合は環境に合わせて設定を行ってください。

- 1) スケジュールバックアップでバックアップ
- 2) コマンドベースでのバックアップ

設定変更が必要な場合は、フェイルオーバー/テイクバックに要する時間に合わせ、設定が必要になります。フェイルオーバー/テイクバックに要する時間については付録を参考にしてください。

スケジュールバックアップでバックアップ

HN/AN障害時にファイルシステムに接続不可能になった際、バックアップ処理は一時的に停止します。したがって、Backup Execのリトライ設定を変更することで、バックアップ処理を再試行させる必要があります。Backup Execでは、特定のエラーコードに対して再試行オプションを適用することが出来ます。この設定を行うことで、フェイルオーバー/テイクバックによりバックアップジョブが停止しても、バックアップ処理を継続させることが可能となります。

以下に設定手順を示します。

1. Backup Execのツールメニューから[Error-Handling Rules]を選択します。
2. [New]をクリックします。
3. 以下の設定を行います。

Name	: 任意の名前を入力
Error category	: Backup Deviceを選択
Enabled	: チェックボックスをオン
Error Code	: E00084C8 The backup storage device has failedを選択
Retry job	: チェックボックスをオン
Maximum retries	: 4を入力(*1)
Retry interval	: 20を入力(*1)
Reschedule job for its next scheduled service	: チェックボックスをオン

コマンドベースでのバックアップ

コマンドベースのバックアップ時も、スケジューラベースと同様にBackup Execのリトライ設定を変更可能です。Backup Execコマンドラインアプレットを使用して、コマンドプロンプトウィンドウにコマンドスイッチを入力することで、特定のエラーに対して再試行オプションを適用することが出来ます。

コマンドラインアプレットを使用するには、コマンドプロンプトウィンドウで、**bemcmd**とスイッチを組み合わせて入力します。要求したタスクがコマンドラインアプレットによって実行され、コマンドプロンプトに成功または失敗を示す値が返されます。

特定のエラーに対しての処理を行うには、**bemcmd -o311**を実行します。**bemcmd -o311**は、1)で設定された内容をルールIDとして指定することで、リトライ設定の変更が可能です。ルールIDは、スケジューラベースで1)の設定をした際に、その設定に対してルールIDが定義されます。

ルールIDを確認するには、**bemcmd -o310**を実行します。コマンドプロンプトに以下のコマンドを入力することでルールIDのリストが一覧で表示されます。

> bemcmd -o310

Backup Execのリトライ設定を変更するには、コマンドプロンプトに以下のコマンドを入力します。

> bemcmd -o311 -irule ID -mr:maximum retries -ri:retry interval

-o311	: エラー処理用スイッチ
rule ID	: ルール ID
maximum retries	: 最大再試行回数を指定(1-99)
retry interval	: ジョブを再試行する間隔を分単位で指定(1-1440)

- (*1) iStorage HS上に作成されているファイルシステム数や使用容量によってフェイルオーバーに要する時間が変化する為、必要に応じて設定値を変更する必要があります。

5-3 HN/AN間のファイルシステムのエクスポート先変更

Backup Execでバックアップ先として指定したファイルシステムを異なるHN/ANへ移動した場合、移動先のHN/ANに応じてファイルシステムのネットワークパスが変更されるため、バックアップフォルダのパスを変更する必要があります(*2)。

バックアップフォルダのパスの変更手順を以下に示します。

1. Backup Execのナビゲーションバーの「デバイス」をクリックします。
2. バックアップフォルダが存在しているコンピュータのアイコンを展開します。
3. 削除するバックアップフォルダを選択します。
4. タスクペインの「一般タスク」の下にある「削除」を選択します。
5. 「はい」をクリックします(*3)。
6. ナビゲーションバーの「デバイス」をクリックします。
7. タスクペインの「ディスクへのバックアップタスク」の下にある「新規フォルダ」をクリックします。
8. バックアップフォルダの設定を行います。
 名前 : 削除したバックアップフォルダ名を指定
 パス : 移動したファイルシステムのパスを指定
 (例:¥¥移動先HN/ANのIPアドレス¥¥ファイルシステム名)
 なお、上記以外の項目は、削除したバックアップフォルダと同様の設定にしてください。
9. [OK]をクリックします。

(*2) iStorage HS のANクラスタ機能により、ファイルシステムが異なるHN/ANへ移動(フェイルオーバー)した場合、バックアップ先のパスを変更する必要はありません。ANクラスタ機能について詳しくは、「iStorage HSシリーズ ユーザーズガイド」を参照してください。

(*3) 指定したバックアップフォルダは、Backup Execからは削除されますが、ファイルとフォルダファイルシステム上に残っているため、同じ名前でバックアップフォルダを作成する事によってバックアップ情報を引き継ぐことが出来ます。

6. トラブルシューティングについて

バックアップソフトウェア固有の問題が発生した場合は、バックアップソフトウェアのログを収集しBackup Execのご購入元へ確認を行ってください。ログの収集手順はお使いのBackup Execのマニュアルを参照してください。

iStorage HSで問題が発生した場合は、イベントを確認し、「iStorage HSシリーズ メッセージハンドブック」を参照して適切な対処を行ってください。iStorage HSでは、メール通報、SNMPインタフェース、イベントビューアといった3つの方法を利用してイベントを受信できます。それぞれの設定方法については、「iStorage HSシリーズ ユーザーズガイド」を参照してください。

Commvault

1. iStorage HSの設定

iStorage HS の重複排除機能を最適化するために、マーカーフィルタリング機能を有効にしてください。

また、Commvault を利用する際は、iStorage HSのファイルシステム容量に注意する必要があります。

1-1 マーカーフィルタリングオプション

Commvaultでは、マーカーと呼ばれる管理情報をバックアップ対象ファイル毎や一定間隔で付加します。付加されたマーカーはバックアップ毎にユニークになる場合があるため、バックアップデータの重複排除率を低下させる要因になることがあります。ファイルシステムのマーカーフィルタリングオプションは、このマーカーのフィルタリングを行ない、データ保存時の重複排除機能を最適化するオプションです。

マーカーフィルタリングオプションの設定は、ファイルシステムの作成時にiStorage HSのGUI/CLIから行えます。GUIから設定する場合は、ファイルシステムの作成時に「マーカーフィルタリング」の「有効」のチェックボックスを選択し、マーカータイプとして「CVS1(Commvault)」を選択します。

The screenshot shows the 'File System Creation' (ファイルシステム作成) window. Under the 'Advanced Options' (高度なオプション) section, the 'Marker Filtering' (マーカーフィルタリング) checkbox is checked and highlighted with a red rectangle. The dropdown menu next to it shows 'CVS1(Commvault)'. Other options include 'Failover' (フェイルオーバー) checked, 'WORM' set to 'None' (無効), 'Retention Period' (保留期間) with 'Default' (デフォルト) selected, 'ACL' unchecked, 'File Information' (ファイル情報) unchecked, and 'Encryption' (暗号化) unchecked. The 'OK' and 'Cancel' buttons are at the bottom right.

詳細なファイルシステムの作成方法については「iStorage HSシリーズ ユーザーズガイド」を参照してください。また、CLIから設定する場合は「iStorage HSシリーズ コマンドリファレンス」を参照してください。

マーカーフィルタリングオプションを使用する場合の注意事項を以下に列挙します。各機能についての説明は「iStorage HSシリーズ ユーザーズガイド」を参照してください。

- ファイルシステムの作成後は、マーカーフィルタリングの設定を変更することはできません。
- レプリケーションセットのマスタとレプリカでは、同じマーカーフィルタリングとマーカータイプを持っている必要があります。
- マーカーフィルタリングが有効となっているファイルシステムがレプリケーションの対象となっている場合、初回のレプリケーションが終了するまで、レプリカのファイルシステムはエクスポートできません。

1-2 ファイルシステム容量

Commvault 7.0/8.0/9.0は2PBより大きなファイルシステムを処理することができません。そのため、Commvault 7.0/8.0/9.0を利用する場合は、iStorage HSのファイルシステムサイズを2PB以下に設定してください。Commvault 10.0/11.0ではiStorage HSのファイルシステムサイズの既定値である 256PB をサポートしています。

Commvaultでは、Reserve Spaceとしてファイルシステム容量の一部を予約しており、利用者の使用可能容量はReserve Space分だけ少なくなります。このため、利用者の使用するファイルのサイズに加えてReserve Space(既定値は2GB)の余裕を持たせた容量見積もりを行う必要があります。

ファイルシステムの容量の変更は、ファイルシステム単位にiStorage HSの GUI/CLIから行えます。以下に GUIから iStorage HSのファイルシステムの容量を2PBにする手順を示します。CLIから設定する場合は、「iStorage HSシリーズ コマンドリファレンス」を参照してください。

1-2.1 新規のファイルシステムをCommvaultで使用する場合

ファイルシステムの作成時に、ファイルシステムの容量を2PBに設定してください。

ファイルシステム作成

ファイルシステムオプション

ファイルシステム名: fs1

ノード: AN 01 01

エクスポートタイプ: ☐ NFS ☒ CIFS

容量: ファイルシステムの容量: 2 PB

☐ ハードクォータを有効にする

☐ ソフトクォータを有効にする ソフトリミット: 90 %

パリティ数: 3 (オーバーヘッド: 25%)

説明:

エクスポートオプション

エクスポート名: fs1

コメント:

アクセス権限: ☒ 読み書き ☐ 読み取り専用

接続許可クライアント:

① エントリを分けるには半角スペースを使用します。

OK キャンセル

1-2.2 既存のファイルシステムをCommvaultで使用する場合

Step.1 当該ファイルシステムのアンエクスポート処理を行ってください。

ファイルシステム概要

フィルタ

ファイルシステム名:

状態: エクスポート, アンエクスポート, 不明, ア

格納済み容量: From GB To GB

ノード: AN0101, AN0102

表示

☐	ファイルシステム名	ノード	状態	タイプ	格納済み容量	権限	マーカータイプ	フェイルオーバー	WORM	クォータ状態	ACL	説明
☐	CIFS_FS	AN0101	エクスポート	CIFS	1.1KB	読み書き		対象		無効	無効	This filesystem
☐	NFS_FS	AN0101	エクスポート	NFS	1.1KB	読み書き		対象		無効	無効	This filesystem
☒	fs1	AN0101	エクスポート	NFS	1.1KB	読み書き		対象		無効	無効	

1ページ中 1 ページ目 10 3件中 1 - 3 を表示

① 上記の格納済み容量は2のべき乗に基づく単位で表示しています。(GB = 1024 × 1024 × 1024)

ファイルシステムの格納済み容量について、容量を参照してください。

作成 移動 削除 エクスポート アンエクスポート チェック 修復 クローン

Step.2 当該ファイルシステムの容量を2PBに変更してください。

当該ファイルシステムを選択すると表示される以下のポップアップから設定を変更します。

ファイルシステム変更(fs1)

⚠ フェイルオーバーが使用可能な場合のみフェイルオーバー設定は有効となります。

ファイルシステムオプション

ファイルシステム名	fs1
ノード	AN0101
状態	アンエクスポート
エクスポートタイプ	☐ NFS ☒ CIFS
容量	ファイルシステムの容量: 2 PB
	☐ ハードクォータを有効にする
	☐ ソフトクォータを有効にする ソフトリミット: %
格納済み容量	4.4KB
パリティ数	3
オーバーヘッド	25%
説明	
作成日時	2011/02/24 17:00:31

① 上記のファイルシステムの容量と格納済み容量は2のべき乗に基づく単位で表示しています。(GB = 1024 × 1024 × 1024)

OK キャンセル

1-3 iStorage HSでの容量超過の監視

iStorage HSとCommvaultを組み合わせで使用する場合、容量超過の監視はCommvaultの容量監視機能が行い、iStorage HSのハードクォータ機能は有効にしても機能しません。ファイルシステムの空き容量がReserve Space(既定値=2GB)以下となった時点で、Commvaultは以降の書き込み要求をWait状態とし、書き込みを抑制します(空き容量が回復した時点で書き込みが可能となります)。このためiStorage HSのハードクォータ機能を有効に設定しても、iStorage HSによる容量超過の通報は行われません。

なお、ソフトクォータ機能は有効に機能します。

Reserve Spaceについて詳細は、Commvaultの説明書を参照してください。

2. Commvault の設定

以下の設定は特に記載がない限り Commvault 7.0/8.0 のものであり、それ以外のバージョンでは変更される可能性がありますのでご注意ください。

2-1 iStorage HS を Magnetic Library として設定

iStorage HS のファイルシステムを Commvault の Magnetic Library として構成できます。iStorage HS を Magnetic Library として構成する場合は、以下のように設定します。

- UNC 形式を使用して、iStorage HS で以下のようにディレクトリ名を指定します。
¥¥<コンピュータ名>¥¥<共有ディレクトリ名>¥¥<オプションパス>
Windows のユーザ名を指定する場合は、適切なアクセス権限を与えてください。
- [Mount Path] タブで [Disks within this library support single instancing] チェックボックスを選択します。このオプションを選択することで、iStorage HS のデータ圧縮技術を最大限まで利用できます。

注：このチェックボックスを選択できるのは、ライブラリがまだ未使用状態の場合だけです。いったんライブラリを使用すると、チェックボックスはグレー表示となり選択できなくなります。

ライブラリ構成の詳細については、Commvault のマニュアルを参照してください。

2-2 同時バックアップジョブでのストレージポリシー設定

1 つの Magnetic Library に同時バックアップジョブを割り当てる場合は、複数のストリームを処理するストレージポリシーを設定します。ストレージポリシーの設定方法は、以下のとおりです。

[CommCell Browser] (左ペイン) -> [Storage Policies] -> <ストレージポリシー名> を右クリック -> [Properties] -> [Storage Policy Properties] ウィンドウ -> [Device Streams] -> 必要な数を設定。

2-3 ブロックサイズの拡大

Magnetic Library のブロックサイズを増やすと、Commvault が一回あたりに書き込めるサイズが増加します。

[CommCell Browser] (左ペイン) -> [Storage Policies] -> <ストレージポリシー名> -> [CommCell Browser] (右ペイン) -> データを右クリック -> [Copy Properties (Storage Policy: <ストレージポリシー名>)] -> [Data Paths] -> データをクリック -> [Properties] -> [Block Size (KB)] -> 指定された値を使用 -> ブロックサイズを指定。

ライブラリ性能のチューニングの詳細は、Commvault のマニュアルを参照してください。

2-4 Deduplication (Commvault 8.0/9.0/10.0/11.0)

Deduplication機能を利用するとiStorage HSの重複排除率が悪くなることが検証評価にて確認されています。Deduplication機能は利用しないことを推奨します。

3. ネットワークの構成

iStorage HSに対してより高速なバックアップ/リストアを行うには、専用のネットワークの利用を推奨します。ネットワークを専用とすることで、バックアップ/リストア用の帯域幅が他の通信により減少することを防ぐことができます。

iStorage HSご利用時のネットワークの構成については「第2章 配備計画 Step 2. ネットワークの計画」を参照してください。

4. Commvault運用時の注意事項

以下の設定は特に記載がない限りCommvault7.0/8.0のものであり、それ以外のバージョンでは変更される可能性がありますのでご注意ください。

4-1 HN/AN間でのファイルシステムのエクスポート先変更

Commvault Magnetic Libraryに関連付けられた iStorage HSのファイルシステムをHN/AN間で移動すると、Commvaultの動作に影響があります。リカバリプロセスの直前にMagnetic Libraryを別のHN/ANに移動すると、CommvaultはMagnetic Libraryが関連付けられているファイルシステムを識別できず、エラーが発生します。ただし、HN/ANが故障した場合は、HN/AN 間で Magnetic Libraryを移動する必要があります。

このような場合は、以下の手順でHN/AN間のMagnetic Library(ファイルシステム)を移動してください。

1. 既存のHN/ANでファイルシステムを無効にする

CommCell コンソールにログインし、以下の1-1または1-2のいずれかの操作を実行します。(これらの操作は内部で互いにインタフェース接続されているので、一方の操作の設定が他方に反映されます。)

1-1. [Storage Resources] > [Libraries]を選択してターゲットライブラリを右クリックします。[Properties]を選択して[General]タブに移動し、[Enable Library]チェックボックスの選択を外します。

1-2. [Storage Resources] > [MediaAgents] > [MediaServerName]を選択してターゲットライブラリを右クリックします。[Properties]を選択して[General]タブに移動し、[Enable Library]チェックボックスの選択を外します。

2. HN/AN間でファイルシステムを移動した後にCommvaultにファイルシステムを認識させる

CommCellコンソールにログインし、以下の操作を実行します。

2-1. メニューバーの[Tools] > [Control Panel] > [Library and Drive Configuration] > [Select Media Agents]を選択してターゲットの MediaAgent を選択します。次に[Data Paths] タブに移動して、ターゲットの[Magnetic Library]の左側にある「+」をクリックして、その下のパスを開きます。ターゲットのファイルシステムの[Properties]を選択し、[NetworkPath]内の[MountPath]のアドレスを変更します。[OK]をクリックして変更を反映します。

2-2. <既存のアクセラレータノードでファイルシステムを無効にする>でいったん選択を外した[Enable Library]チェックボックスを選択します。

3. Commvault がファイルシステムを認識していることを確認する方法

CommCellコンソールにログインしてMagnetic Libraryを作成した後、CommvaultがMagnetic Libraryを正しく認識していることを左ペインから以下の方法で確認します。以下の3-1または3-2のいずれかを実行することで必要な情報を得ることができます。

3-1. [Storage Resources] > [Libraries]を選択して、ターゲットライブラリを選択します。

3-2. [Storage Resources] > [MediaAgents] > [MediaServerName]を選択して、ターゲットライブラリを選択します。

どちらの方法でも右ペインに以下の情報が表示されます。

列のタイトル

MountPath	: 更新されたパスが正しく表示されることを確認します。
Status	: 更新されたパスがready状態になっていることを確認します。
Free Space(MB)	: 以前のパスを認識している場合は空き容量が同じであることを確認します。
Capacity(MB)	: 容量を確認します。

4-2 ANクラスタ

iStorage HSでは複数のHN/ANを使用して高可用クラスタ構成を組むことが可能です。ANクラスタの一部のHN/ANに障害が発生した場合、IPアドレスとファイルシステムは他のHN/ANに移動し、停止したサービスは移動先のHN/ANで自動的に再開します。障害が発生したHN/ANからIPアドレスとファイルシステムが移動することを“フェイルオーバー”、障害から復旧したHN/ANに戻ることを“テイクバック”と呼びます。

Commvaultを使用した環境でANクラスタが有効になっており、バックアップもしくはリストア中にフェイルオーバーが発生した場合、バックアップもしくはリストアがエラーになります。その場合はフェイルオーバー完了後にバックアップもしくはリストアを再実行してください。その際、失敗した箇所から再開するのではなく、最初から再実行してください。

5. トラブルシューティングについて

バックアップソフトウェア固有の問題が発生した場合は、バックアップソフトウェアのログを収集しCommvaultのご購入元へ確認を行ってください。ログの収集手順はお使いのCommvaultのマニュアルを参照してください。

iStorage HSで問題が発生した場合は、イベントを確認し、「iStorage HSシリーズ メッセージハンドブック」を参照して適切な対処を行ってください。iStorage HSでは、メール通報、SNMPインタフェース、イベントビューアといった3つの方法を利用してイベントを受信できます。それぞれの設定方法については、「iStorage HSシリーズ ユーザーズガイド」を参照してください。

Data Protector

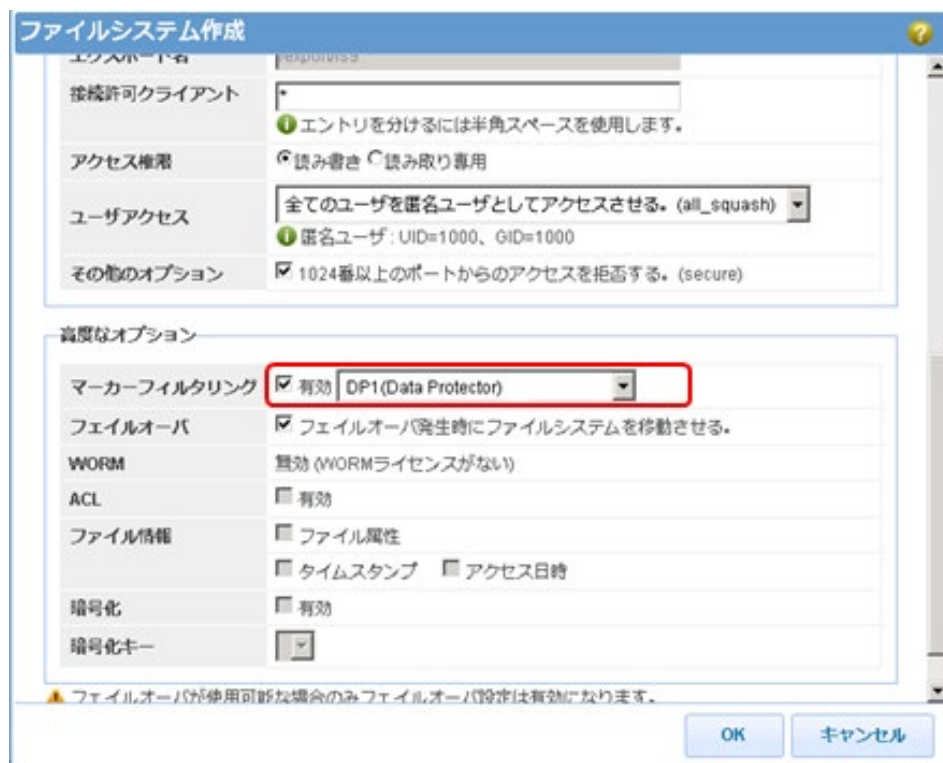
1. iStorage HSの設定

1-1 マーカーフィルタリングオプション

Data Protectorでは、データを固定サイズのブロック単位に分け、各ブロックを制御する管理情報(ここではマーカーと呼びます)をつけて、iStorage HSに書き込みます。マーカーはバックアップごとにユニークな情報となる場合があるため、Data Protectorがバックアップデータに多くのマーカーを挿入すると、重複排除率が低下する要因となることがあります。

マーカーフィルタリング機能を利用することにより、バックアップデータ中のマーカーを除外して効率的にデータ格納を行うことができ、重複排除率を向上することができます。

マーカーフィルタリングオプションの設定は、ファイルシステムの作成時にiStorage HSのGUI/CLIから行えます。GUIから設定する場合は、ファイルシステムの作成時に「マーカーフィルタリング」の「有効」のチェックボックスを選択し、マーカータイプとして「DP1(Data Protector)」を選択します。



詳細なファイルシステムの作成方法については「iStorage HSシリーズ ユーザーズガイド」を参照してください。また、CLIから設定する場合は「iStorage HSシリーズ コマンドリファレンス」を参照してください。

マーカーフィルタリングオプションを使用する場合の注意事項を以下に列挙します。各機能についての説明は「iStorage HSシリーズ ユーザーズガイド」を参照してください。

- レプリケーションセットのマスタとレプリカでは、同じマーカーフィルタリングとマーカータイプを持っている必要があります。
- マーカーフィルタリングが有効となっているファイルシステムがレプリケーションの対象となっている場合、初回のレプリケーションが終了するまで、レプリカのファイルシステムはエクスポートできません。

1-2 ファイルシステムの容量上限について

Data Protectorではファイルシステムの容量値として4TBまでしか扱うことができません。そのため、Data Protectorを利用する場合は、iStorage HSのファイルシステムを4TB以下に設定してください。

ファイルシステムの容量の変更は、ファイルシステム単位にiStorage HSGUI/CLIから行えます。以下に GUI から iStorage HS のファイルシステムの容量を 4TB にする手順を示します。CLI から設定する場合は、「iStorage HSシリーズ コマンドリファレンス」を参照してください。

1-2.1 新規のファイルシステムをData Protectorで使用する場合

ファイルシステムの作成時に、ファイルシステムの容量を4TBに設定してください。

The screenshot shows the 'File System Creation' (ファイルシステム作成) window. The 'File System Options' (ファイルシステムオプション) section is highlighted with a red box. The 'Capacity' (容量) field is set to '4 TB'. Other fields in this section include 'File System Name' (fs1), 'Node' (AN 01 01), 'Export Type' (NFS), 'Parity' (3), and 'Description' (説明). The 'Export Options' (エクスポートオプション) section is also visible, showing 'Export Name' (exportfs1), 'Access Control List' (*), 'Access Rights' (read/write), and 'User Access' (all_squash).

1-2.2 既存のファイルシステムをData Protectorで使用する場合

Step.1 当該ファイルシステムをアンエクスポートしてください。

ファイルシステム概要

フィルタ

ファイルシステム名: 状態: エクスポート, アンエクスポート, 不明, ア

格納済み容量: From GB To GB ノード: AN0101, AN0102

☐	ファイルシステム名	ノード	状態	タイプ	格納済み容量	権限	マーカータイプ	フェイルオー	WORM	クォータ状態	ACL	説明
☐	CIFS_FS	AN0101	エクスポート	CIFS	1.1KB	読み書き		対象		無効	無効	This filesystem
☐	NFS_FS	AN0101	エクスポート	NFS	1.1KB	読み書き		対象		無効	無効	This filesystem
☒	fs1	AN0101	エクスポート	NFS	1.1KB	読み書き		対象		無効	無効	

1 上記の格納済み容量は2のべき乗に基づく単位で表示しています。(GB = 1024 × 1024 × 1024)

ファイルシステムの格納済み容量について、容量を参照してください。

Step.2 当該ファイルシステムの容量を4TBに変更してください。

当該ファイルシステムを選択すると表示される以下のポップアップから設定を変更します。

ファイルシステム変更(fs1)

⚠ フェイルオーバーが使用可能な場合のみフェイルオーバー設定は有効になります。

ファイルシステムオプション

ファイルシステム名: fs1

ノード: AN0101

状態: アンエクスポート

エクスポートタイプ: ☒ NFS ☐ CIFS

容量: TB

☐ ハードクォータを有効にする

☐ ソフトクォータを有効にする ソフトリミット: %

格納済み容量: 4.4KB

パリティ数: 3

オーバーヘッド: 25%

説明:

作成日時: 2011/02/24 17:00:31

1 上記のファイルシステムの容量と格納済み容量は2のべき乗に基づく単位で表示しています。(GB = 1024 × 1024 × 1024)

1-3 iStorage HSでの容量超過の監視

iStorage HS と Data Protectorを組み合わせて使用する場合、容量超過の監視は Data Protector の容量監視機能が行うため、iStorage HS のハードクォータ機能を利用する必要はありません。Data Protectorが iStorage HSに作成したファイルシステムに対してバックアップを行い、書き込み容量がファイルシステム作成時に設定した容量の99%に達した時、Data Protectorにより書き込みが停止され、ダイアログメッセージが表示されます。このためiStorage HSのハードクォータ機能を有効に設定しても、iStorage HSによる容量超過の通報は行われません。ソフトクォータ機能は有効です。

2. Data Protectorの設定

2-1 Data Protector ライセンス

Data Protector を iStorage HSと組み合わせて使用するには、Advanced Backup to Diskオプションライセンスが必要です。

2-2 iStorage HS をファイルライブラリとして設定

iStorage HSのファイルシステムをData Protectorのデバイスタイプをファイルライブラリとしてください。Data Protectorのディスクベースのストレージに対して有効なチューニング項目は iStorage HS に対しても有効です。

3. バックアップサーバの設定

iStorage HSに対してより高速なバックアップ/リストアを行うには、Data Protectorがインストールされているバックアップサーバの設定変更が必要になります。バックアップサーバの設定については「付録C オペレーティングシステムの設定」を参照してください。

4. ネットワークの構成

iStorage HSに対してより高速なバックアップ/リストアを行うには、専用のネットワークの利用を推奨します。ネットワークを専用とすることで、バックアップ/リストア用の帯域幅が他の通信により減少することを防ぐことができます。

iStorage HSご利用時のネットワークの構成については「第2章 配備計画 Step 2. ネットワークの計画」を参照してください。

5. Data Protector運用時の注意事項

5-1 小さなサイズのファイルのバックアップ

Data Protectorを用いて iStorage HSへのバックアップ処理を行う際、バックアップするデータに数十KB未満の小さなファイルが多く含まれていると、iStorage HSの重複排除率は低くなります(*1)。これは、Data Protectorが各バックアップ対象ファイルのヘッダ部に管理情報を付加することに起因します。

iStorage HSではブロックレベルで重複データを検出し、重複しないユニークなデータのみを圧縮・格納することによって効率的なストレージ格納容量を実現します。(DataRedux®)

Data Protectorの管理情報はバックアップ対象ファイル毎に付加されます。そのため、iStorage HS がバックアップデータをブロックレベルに分割する際に、バックアップデータに数十KB未満の小さなファイルが含まれていると、分割されたバックアップデータの個々のブロックの多くに Data Protectorによって付加された管理情報が含まれることになります。この付加された管理情報には、バックアップ毎にユニークな情報が含まれます。そのため、管理情報が含まれたブロックは前回バックアップ時と比べて重複しないユニークなデータとみなされ、排除されずにiStorage HSへ格納されます。これによってiStorage HSの重複排除率は低くなります。

(*1) iStorage HSのマーカーフィルタリング機能を使用すれば、小ファイルのバックアップにおける重複排除率の低下を防ぐことができます。詳しくは、「2-1 マーカーフィルタリングオプション」を参照下さい。

6. トラブルシューティング

バックアップソフトウェア固有の問題が発生した場合は、バックアップソフトウェアのログを収集しData Protectorのご購入元へ確認を行ってください。ログの収集手順はお使いのData Protectorのマニュアルを参照してください。

iStorage HSで問題が発生した場合は、イベントを確認し、「iStorage HSシリーズ メッセージハンドブック」を参照して適切な対処を行ってください。iStorage HSでは、メール通報、SNMPインタフェース、イベントビューアといった3つの方法を利用してイベントを受信できます。それぞれの設定方法については、「iStorage HSシリーズ ユーザーズガイド」を参照してください。

Veritas NetBackup

1. iStorage HS の設定

iStorage HSの重複排除機能を最適化するために、マーカーフィルタリング機能が利用できます。

また、バックアップサーバとしてAIXを使用する場合は、iStorage HSのファイルシステムの容量を変更する必要があります。

上記にあてはまらない場合は、iStorage HSで必要となる特別な設定はありません。

1-1 マーカーフィルタリングオプション

NetBackupでは、マーカーと呼ばれる管理情報をバックアップ対象ファイル毎に付加します。付加されたマーカーはバックアップ毎にユニークになる場合があるため、バックアップデータの重複排除率を低下させる要因になることがあります。ファイルシステムのマーカーフィルタリングオプションは、このマーカーのフィルタリングを行ない、データ保存時の重複排除機能を最適化するオプションです(*1)。

バックアップ対象ファイル毎に付加されるマーカーは、バックアップ対象ファイルのサイズが小さいと重複排除を阻害する要因となりますが、ファイルサイズが大きい場合は重複排除機能に及ぼす影響は小さくなります。

目安としてバックアップ対象ファイルの平均ファイルサイズが1MB以下の場合、マーカーフィルタリング機能を使用することを推奨します。

マーカーフィルタリングオプションの設定は、ファイルシステムの作成時にiStorage HSのGUI/CLIから行えます。GUIから設定する場合は、ファイルシステムの作成時に「マーカーフィルタリング」の「有効」のチェックボックスを選択し、マーカータイプとして"NBU1(Veritas NetBackup)"を選択します。

ファイルシステム作成

接続許可クライアント: *

① エントリを分けるには半角スペースを使用します。

アクセス権限: ☒ 読み書き ☐ 読み取り専用

ユーザアクセス: 全てのユーザを匿名ユーザとしてアクセスさせる。(all_squash) ▼

① 匿名ユーザ: UID=1000、GID=1000

その他のオプション: ☒ 1024番以上のポートからのアクセスを拒否する。(secure)

高度なオプション

マーカーフイルタリング: ☒ 有効 NBU1(Veritas NetBackup) ▼

フェイルオーバー: ☒ フェイルオーバー発生時にファイルシステムを移動させる。

WORM: 無効 ▼

保護期間: デフォルト [] 年 ▼

☐ 最小値 [] 年 ▼

☐ 最大値 [] 年 ▼

ACL: ☐ 有効

ファイル情報: ☐ ファイル属性

☐ タイムスタンプ ☐ アクセス日時

暗号化: ☐ 有効

OK キャンセル

詳細なファイルシステムの作成方法については「iStorage HS シリーズ ユーザーズガイド」を参照してください。また、CLIから設定する場合は「iStorage HS シリーズ コマンドリファレンス」を参照してください。

マーカーフイルタリングオプションを使用する場合の注意事項を以下に列挙します。各機能についての説明は「iStorage HSシリーズ ユーザーズガイド」を参照してください。

- ファイルシステムの作成後は、マーカーフイルタリングの設定を変更することはできません。
- レプリケーションセットのマスタとレプリカでは、同じマーカーフイルタリングとマーカータイプを持っている必要があります。
- マーカーフイルタリングが有効となっているファイルシステムがレプリケーションの対象となっている場合、初回のレプリケーションが終了するまで、レプリカのファイルシステムはエクスポートできません。

(*1) rawバックアップでは、マーカークがほぼ挿入されないため本オプションの指定は不要です。

1-2 AIXバックアップサーバ使用時のiStorage HSファイルシステム容量

iStorage HSのファイルシステム初期容量は256PBですが、バックアップサーバとしてAIXを利用する場合、NetBackupではファイルシステムの容量値として128TBまでしか扱うことができません(*2)。バックアップサーバとしてAIXを利用する場合は、iStorage HSのファイルシステムサイズを128TB以下に設定してください。

ファイルシステムの容量の変更は、ファイルシステム単位にiStorage HSの GUI/CLIから行えます。以下にGUIからiStorage HSのファイルシステムの容量を128TBにする手順を示します。CLI から設定する場合は、「iStorage HSシリーズ コマンドリファレンス」を参照してください。

(*2) 本上限は、2009年8月時点で確認した上限であり、NetBackup 7では256PBを扱えることを確認しています。お使いのバージョンが対応済みかどうかは、NetBackupの購入元に確認してください。

1-2.1 新規のファイルシステムをNetBackupで使用する場合

ファイルシステムの作成時に、ファイルシステムの容量を128TB に設定してください。

ファイルシステム作成

ファイルシステムオプション

ファイルシステム名: fs1

ノード: AN 01 01

エクスポートタイプ: ☒ NFS ☐ CIFS

容量: ファイルシステムの容量: 128 TB

☐ ハードクォータを有効にする

☐ ソフトクォータを有効にする ソフトリミット: 90 %

パリティ数: 3 (オーバーヘッド: 25%)

説明:

エクスポートオプション

エクスポート名: /export/fs1

接続許可クライアント: *

アクセス権限: ☒ 読み書き ☐ 読み取り専用

ユーザアクセス: 全てのユーザを匿名ユーザとしてアクセスさせる。(all_squash)

匿名ユーザ: UID=1000, GID=1000

OK キャンセル

1-2.2 既存のファイルシステムを NetBackup で使用する場合

Step.1 当該ファイルシステムのアンエクスポート処理を行ってください。

ファイルシステム概要

フィルタ

ファイルシステム名: 状態: エクスポート, アンエクスポート, 不明, ア 表示

格納済み容量: From GB To GB ノード: AN0101, AN0102

ファイルシステム名	ノード	状態	タイプ	格納済み容量	権限	マーカータイプ	フェイルオー	WORM	クォータ状態	ACL	説明
☐ CIFS_FS	AN0101	エクスポート	CIFS	1.1KB	読み書き	対象			無効	無効	This filesystem
☐ NFS_FS	AN0101	エクスポート	NFS	1.1KB	読み書き	対象			無効	無効	This filesystem
☒ fs1	AN0101	エクスポート	NFS	1.1KB	読み書き	対象			無効	無効	

1ページ中 1 ページ目 10 3件中 1 - 3を表示

上記の格納済み容量は2のべき乗に基づく単位で表示しています。(GB = 1024 × 1024 × 1024)

ファイルシステムの格納済み容量について、容量を参照してください。

作成 移動 削除 エクスポート **アンエクスポート** チェック 修復 クローン

Step.2 当該ファイルシステムの容量を128TBに変更してください。

当該ファイルシステムを選択すると表示される以下のポップアップから設定を変更します。

ファイルシステム変更 (fs1)

⚠ フェイルオーバーが使用可能な場合のみフェイルオーバー設定は有効になります。

ファイルシステムオプション

ファイルシステム名	fs1
ノード	AN0101
状態	アンエクスポート
エクスポートタイプ	☒ NFS ☐ CIFS
容量	ファイルシステムの容量 128 TB
	☐ ハードクォータを有効にする
	☐ ソフトクォータを有効にする ソフトリミット: %
格納済み容量	4.4KB
パリティ数	3
オーバーヘッド	25%
説明	
作成日時	2011/02/24 17:00:31

ⓘ 上記のファイルシステムの容量と格納済み容量は2のべき乗に基づく単位で表示しています。(GB = 1024 × 1024 × 1024)

OK キャンセル

2. NetBackupの設定

2-1 iStorage HSをディスクストレージユニットとして設定

iStorage HSのファイルシステムをNetBackupのバックアップデータの格納先ディスクストレージユニットとしてください。NetBackupのディスクベースのストレージに対して有効なチューニング項目はiStorage HSに対しても有効です。

iStorage HSのファイルシステムは、BasicDisk、AdvancedDisk(*1)、またはOpenStorage(*2)のNetBackupディスクストレージユニットとして構成できます。

iStorage HSのファイルシステムをNearStoreまたはSharedDiskのNetBackupディスクストレージユニットとして構成することはできません。

iStorage HSは重複排除機能を搭載しています。そのため、iStorage HSのファイルシステムをPureDiskのNetBackupディスクストレージユニットとして構成することは推奨しません。

- (*1) AdvancedDiskのディスクストレージユニットは、NetBackup 6.5以降でサポートされています。この機能を使用する場合は、NetBackupマスタサーバでFlexible Disk Optionのライセンスキーを入力する必要があります。なお、Windows環境(CIFS)では、iStorage HSのファイルシステムを AdvancedDiskNetBackupディスクストレージユニットとして構成することはできません。AdvancedDiskの作成方法はNetBackupのマニュアルを参照してください。
- (*2) OpenStorage(OST)を利用される場合は「iStorage HSシリーズ OpenStorage(OST)ユーザーズガイド」を参照してください。

2-2 NetBackupのフラグメントサイズについて

NetBackupがストレージ上に生成するバックアップイメージファイルは、あらかじめ設定されたフラグメントサイズ毎に分割されて格納されます。バックアップする容量に合わせて大きな値を指定することで、バックアップイメージファイルが分割されないようにすることもできます。ただし、以下のような場合には、バックアップ性能やリストア性能が悪くなる傾向があるため、フラグメントのサイズを適宜調整する必要があります。

- RHELにおいてバックアップをする場合
RHELでは、バックアップイメージファイルのサイズが大きくなると、バックアップ性能が著しく悪くなる傾向があります。サイズが大きいほど性能への影響が大きくなります。弊社検証環境においては、フラグメントサイズに2GBより大きな値を設定すると、バックアップ性能が著しく悪くなる検証結果が得られています。
- 小数のファイルを個々にリカバリする場合
フラグメントサイズが大きいと、バックアップイメージファイルからの読み込みサイズが大きくなり、リカバリに必要な部分のデータを読み込むこととなり、結果としてリカバリ性能が悪くなります。上記に該当する場合には、フラグメントのサイズをデフォルトサイズよりも小さく調整することで、バックアップやリストア時間を短縮できる可能性があります。

フラグメントサイズは、ストレージユニットの[Reduce fragment size to]の項目により設定します(フラグメントのデフォルトサイズは、512GBです)。

なお、フラグメントサイズを極端に小さくすると、バックアップイメージファイルが大量に生成されることになり、たとえばファイル一覧の取得(lsなど)の所要時間が長くなるなどの影響も考えられるので留意してください。

フラグメントサイズに関する詳細については、Veritas 社から提供されている『*Veritas NetBackupBackup Planning and Performance Tuning Guide*』を参照してください。

2-3 NetBackupが使用する共有メモリについて

NetBackupのメディアサーバは共有バッファを利用しています。この共有メモリの容量を変更することによって、メディアサーバが利用する共有メモリの最適化がはかれ、性能の向上が見込めます。

メディアサーバ上でSIZE_DATA_BUFFERS_DISKとNUMBER_DATA_BUFFERS_DISKの2つのファイル内の値を変更してください。これらのファイルは以下に格納されています。

- UNIX系サーバの場合
 - /usr/openv/netbackup/db/config/SIZE_DATA_BUFFERS_DISK
 - /usr/openv/netbackup/db/config/NUMBER_DATA_BUFFERS_DISK
- Windowsの場合
 - *install_path*¥NetBackup¥db¥config¥SIZE_DATA_BUFFERS_DISK
 - *install_path*¥NetBackup¥db¥config¥NUMBER_DATA_BUFFERS_DISK

ファイルがない場合は、ファイルを作成してください。ファイルが存在する場合は、ファイル内の値が下記の設定であることを確認してください。ファイルと値は以下のとおりです。

- メモリが2GB以下の場合
 - SIZE_DATA_BUFFERS_DISK ⇒262144以上の値を設定してください。
 - NUMBER_DATA_BUFFERS_DISK ⇒16以上の値を設定してください。
- メモリが2GB以上の場合
 - SIZE_DATA_BUFFERS_DISK ⇒262144以上の値を設定してください。
 - NUMBER_DATA_BUFFERS_DISK ⇒32以上の値を設定してください。

2-4 NetBackupの圧縮/暗号化機能について

NetBackupのポリシーの設定において、圧縮機能を無効にしてください。iStorage HSではバックアップ時に重複排除と物理データ圧縮を行っています。データの物理圧縮はiStorage HS内で実行しているため、NetBackupで実行する必要はありません。また、NetBackupによる圧縮はバックアップサーバ上で実行されるため、性能に影響を与えることがあります。

NetBackupのポリシーの設定において、暗号化機能を無効にしてください。暗号化機能を無効にすることでiStorage HSでより効果的に重複排除を行うことができます。

2-5 NetBackupのタイムアウト設定について

NetBackup Administration Console から以下のようにタイムアウト値を設定してください。

- [Host properties] -> [Master Server] -> [Timeouts]
 - クライアントの接続タイムアウト : 600 秒
 - クライアントの読み込みタイムアウト : 600 秒
- [Host properties] -> [Media Server] -> [Timeouts]
 - クライアントの接続タイムアウト : 600 秒
 - クライアントの読み込みタイムアウト : 600 秒
- [Host properties] -> [Clients] -> [Timeouts]
 - クライアントの読み込みタイムアウト : 600 秒

2-6 NetBackupの多重処理について

バックアップを多重化することで、iStorage HSへのバックアップ性能が向上する可能性があります。バックアップ性能が向上するかどうかは、NetBackupやネットワークの構成によります。詳しくはVeritas社から提供されている『*NetBackup Backup Planning and Performance Tuning Guide*』を参照してください。

バックアップを多重化するには以下の設定を行ってください。

- 1つのポリシーから多重でバックアップを行う場合は、ポリシーに対して[*Allow multiple data streams*]の設定を行い、バックアップ対象リストを設定する際にNEW_STREAM指示句を使用してください。NEW_STREAM指示句が存在するバックアップ対象リストのそれぞれの箇所で、バックアップストリームが生成されます。
例えば、バックアップ対象リストが以下の場合、2つのバックアップストリームが生成されます。1つめのストリームでは D:¥Program Files と C:¥Winnt が、2つめのストリームではC:¥users と D:¥DataFiles がそれぞれバックアップされます。

```
NEW_STREAM
D:¥Program
FilesC:¥Winnt
NEW_STREAM
C:¥users
D:¥DataFiles
```

- 1つのディスクストレージユニットに対して、多重でバックアップを行う場合は、ディスクストレージユニットで[*Maximum concurrent jobs*]の設定を行ってください。[*Maximum concurrent jobs*]には、そのストレージユニットに対して同時に行うジョブの数を指定してください。
- バックアップの多重化は、ホストプロパティの[*Maximum jobs per clients*]や[*Maximum data streams*]、ポリシー属性の[*Limit jobs per policy*]の設定も影響します。詳しくはVeritas社から提供されているNetBackupの「管理者ガイド」を参照してください。

3. バックアップサーバの設定

iStorage HSに対してより高速なバックアップ/リストアを行うには、NetBackupがインストールされているメディアサーバの設定変更が必要になります。

メディアサーバの設定については「付録C オペレーティングシステムの設定」を参照してください。

4. ネットワークの構成

iStorage HSに対してより高速なバックアップ/リストアを行うには、専用のネットワークの利用を推奨します。ネットワークを専用とすることで、バックアップ/リストア用の帯域幅が他の通信により減少することを防ぐことができます。

iStorage HSご利用時のネットワークの構成については「第2章 配備計画 Step 2. ネットワークの計画」を参照してください。

5. NetBackup 運用時の注意事項

5-1 HN/AN間のファイルシステムのエクスポート先変更

NetBackupでバックアップ先として指定したファイルシステムを異なるHN/ANへ移動する場合、移動先のHN/ANに応じてファイルシステムのネットワークパスが変更されます(*1)。バックアップ済みのデータをリストアするためには、バックアップ済みのバックアップイメージをインポートする必要があります。NFS経由でバックアップを行っている場合は、バックアップイメージのインポートを行わなくても、NFSマウント先アドレスを変更することでリストアが可能になります。

それぞれの手順を以下に示します。CIFS経由でバックアップを行っている場合は5-1.1を、NFS経由でバックアップを行っている場合は5-1.1または5-1.2を行ってください。

(*1) iStorage HSのANクラスタ機能により、ファイルシステムが異なるHN/ANへ移動(フェイルオーバー)した場合、バックアップ先のパスは変更されません。ANクラスタ機能について詳しくは、「iStorage HSシリーズ ユーザーズガイド」を参照してください。

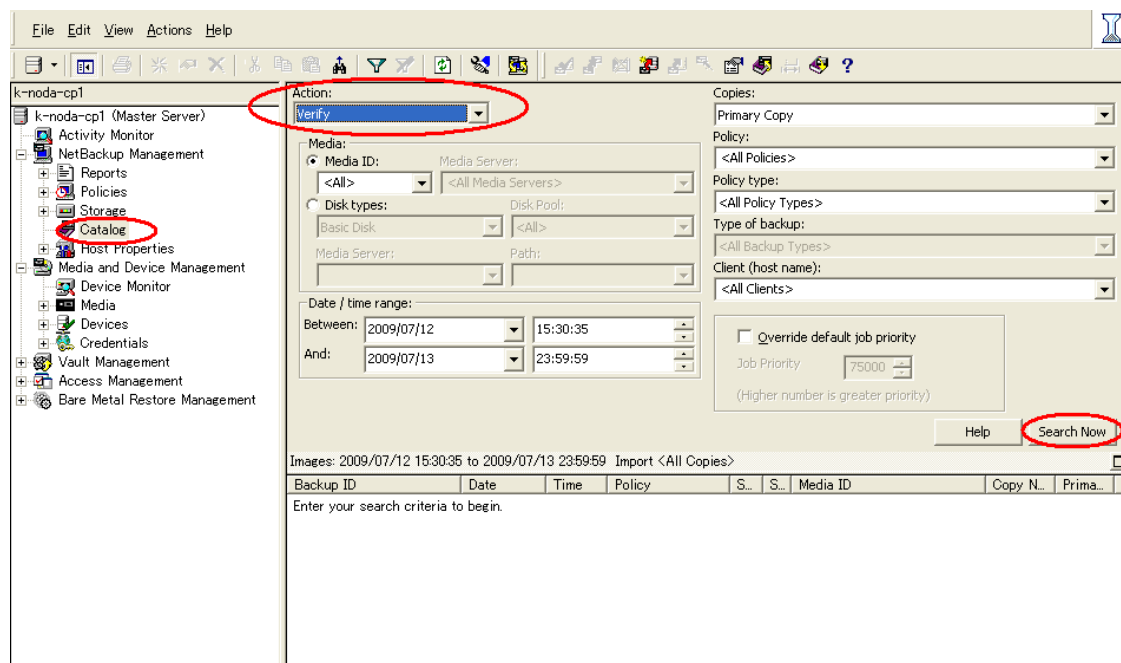
5-1.1 移動したファイルシステムのバックアップイメージをインポート

移動したファイルシステムのバックアップイメージをインポートし、ファイルシステムが移動する前にバックアップされていたデータのリストアを可能にします。また、ストレージユニットのパスを変更してバックアップを可能にします。

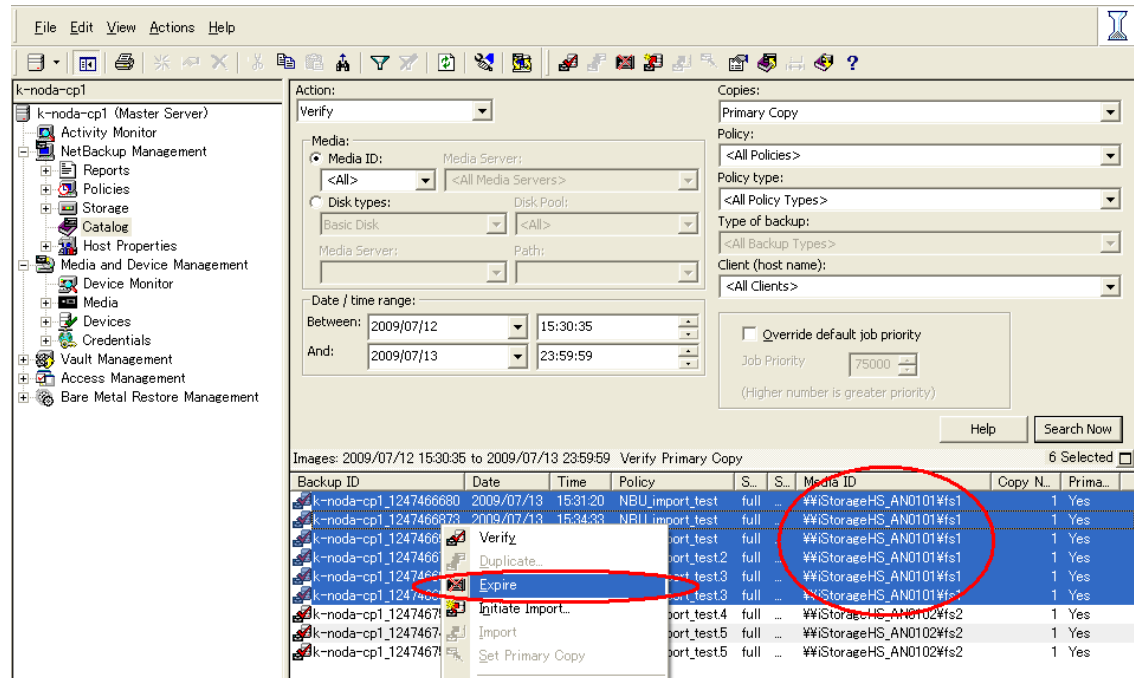
なお、この手順はWindows サーバ(CIFS)、Linux/UNIX 系サーバ(NFS)に対して有効です。

Windows サーバでの手順は以下の通りです。

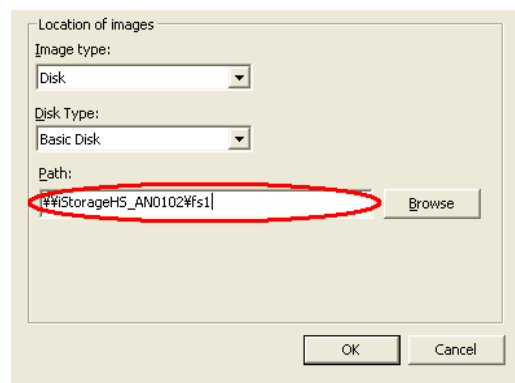
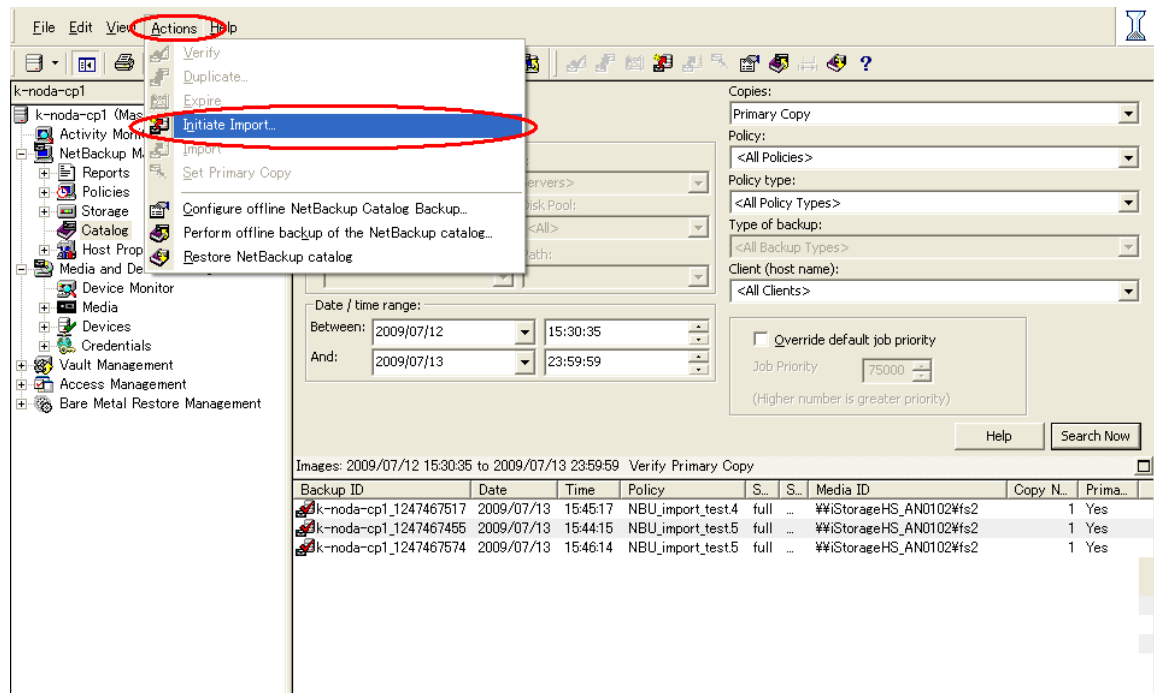
- 1) ファイルシステム fs1 を AN0101 から、AN0102 に移動します。
以降の手順では、この移動によって fs1 への UNC が”\\¥iStorageHS_AN0101¥fs1”から”\\¥iStorageHS_AN0102¥fs1”に変更されたとしています。
- 2) NetBackup 管理コンソールを開き、[Catalog] > [Action]と移動して[verify]を選択し、「SearchNow」をクリックします。



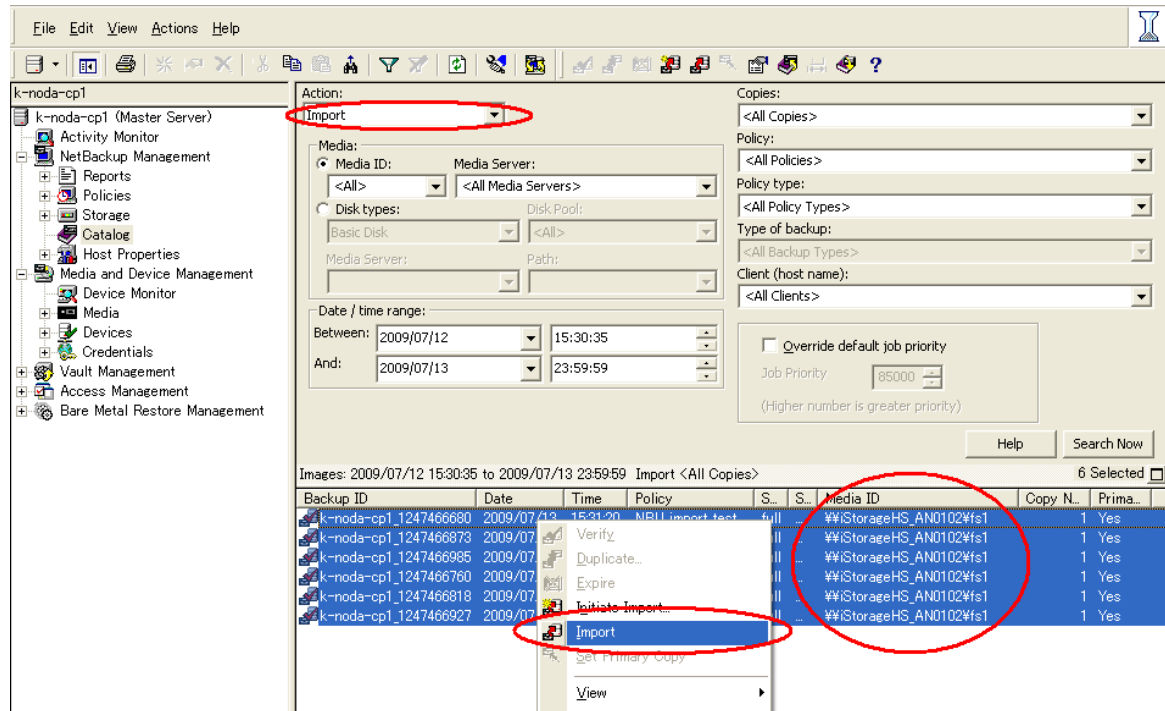
- 3) 「Search Now」をクリックすると、Backup_IDの一覧が表示されます。Media IDが「¥¥iStorageHS_AN0101¥fs1」となっているBackup_IDを右クリックして、[Expire]ボタンを選択し、移動前のANのバックアップ情報を消去します。



4) Actionsから[Initialize Import]を選択し、“¥¥iStorageHS_AN0102¥fs1”を指定します。



- 5) NetBackup管理コンソールを開き、[Catalog] > [Action]と移動して[import]を選択します。[Search Now]ボタンをクリックし、Media IDが“¥¥iStorageHS_AN0102¥fs1”となっているBackup_IDを右クリックして、[Import]ボタンを選択します。



- 6) リストアを実行できるようになります。
- 7) 同じポリシーで今後もバックアップを行う時は、そのポリシーが使用しているストレージユニットのディレクトリへの絶対パス名を“¥¥iStorageHS_AN0101¥fs1”から“¥¥iStorageHS_AN0102¥fs1”に変更してください。

5-1.2 NFSマウント先ディレクトリの変更

NFSのマウント先ディレクトリを変更することで、ファイルシステムが移動する前にバックアップされていたデータのリストアを可能にします。また、ファイルシステム移動後のバックアップを可能にします。

なお、この手順はLinux/UNIX系サーバ(NFS)に対して有効です。

- 1) NFSファイルシステムのアンマウントを行います。
- 2) iStorage HSのファイルシステムを移動させます。
- 3) NFSのマウント先アドレスを変更して再度マウントを行います。

5-2 小さなサイズのファイルのバックアップ

NetBackupを用いてiStorage HSへのバックアップ処理を行う際、バックアップするデータに数十KB未満の小さなファイルが多く含まれていると、iStorage HSの重複排除率は低くなります(*2)。これは、NetBackupが各バックアップ対象ファイルのヘッダ部に管理情報(マーカ)を付加することに起因します。iStorage HSではブロックレベルで重複データを検出し、重複しないユニークなデータのみを圧縮・格納することによって効率的なストレージ格納容量を実現します。(DataRedux®)

NetBackupの管理情報はバックアップ対象ファイル毎に付加されます。そのため、iStorage HS がバックアップデータをブロックレベルに分割する際に、バックアップデータに数十KB未満の小さなファイルが含まれていると、分割されたバックアップデータの個々のブロックの多くにNetBackupによって付加された管理情報が含まれることになります。この付加された管理情報にはバックアップ時刻等が含まれるため、バックアップ毎にユニークになります。そのため、管理情報が含まれたブロックは前回バックアップ時と比べて重複しないユニークなデータとみなされ、排除されずにiStorage HSへ格納されます。これによってiStorage HSの重複排除率は低くなります。

(*2) iStorage HS のマーカフィルタリング機能を使用すれば、小ファイルのバックアップにおける重複排除率の低下を防ぐことができます。詳しくは、「1-1 マーカフィルタリング」を参照下さい。

5-3 ANクラスタ機能を用いる際のリトライ設定

NetBackupを用いたiStorage HSへのバックアップ処理実行中、バックアップ先のHN/ANで障害が発生した場合でも、iStorage HSのANクラスタ機能を利用してバックアップを継続/再試行させるための設定について記述します。

以下の4パターンについて記述します。設定変更が必要な場合は環境に合わせて設定を行ってください。

- 1) バックアップ先ファイルシステムにNFSを使用している場合
 - 1-1) スケジュールバックアップでバックアップ
 - 1-2) スケジュールバックアップ以外でバックアップ
- 2) バックアップ先ファイルシステムにCIFSを使用している場合
 - 2-1) スケジュールバックアップでバックアップ
 - 2-2) スケジュールバックアップ以外でバックアップ

設定変更が必要な場合は、フェイルオーバー/テイクバックに要する時間に合わせ、設定が必要になります。フェイルオーバー/テイクバックに要する時間については付録を参考にしてください。

1-1) バックアップ先に NFSを指定し、スケジュールバックアップでバックアップ iStorage HSへのNFSマウント時にオプションとしてhardを指定して下さい。

バックアップ先のファイルシステムとして NFSを使用している場合、HN/AN障害時にファイルシステムに接続不可能になっても、iStorage HSはバックアップサーバに対しエラーを返しません。NetBackupのバックアップ処理は中断されることなく、バックアップ先ファイルシステムが接続可能となった時点で、それまで書き込んでいたバックアップイメージに対して継続して書き込みを行います。NetBackupの設定変更の必要はありません。

1-2) バックアップ先にNFSを指定し、スケジュールバックアップ以外でバックアップ

「1-1) バックアップ先にNFSを指定し、スケジュールバックアップでバックアップ」と同様の理由でNetBackupの設定変更の必要はありません。

2-1) バックアップ先に CIFS を指定し、スケジュールバックアップでバックアップ

バックアップ先のファイルシステムとしてCIFSを使用している場合、HN/AN障害時にファイルシステムに接続不可能になった際、バックアップ処理はエラーとなります。したがって、NetBackupのリトライ設定を変更することで、バックアップ処理を再試行させる必要があります。リトライ機能を利用することでフェイルオーバーした際にバックアップ処理を一時的に停止させ（“Waiting Retry”状態）再度バックアップを再試行させることができます。再試行されたバックアップは、新規バックアップイメージとして書き込みを行います。

以下に設定手順を示します。

Step.1 NetBackup の設定を行ってください。

NetBackup Administration Console → Host Properties

→ Master Server → Global Attributes

- Job retry delayを編集

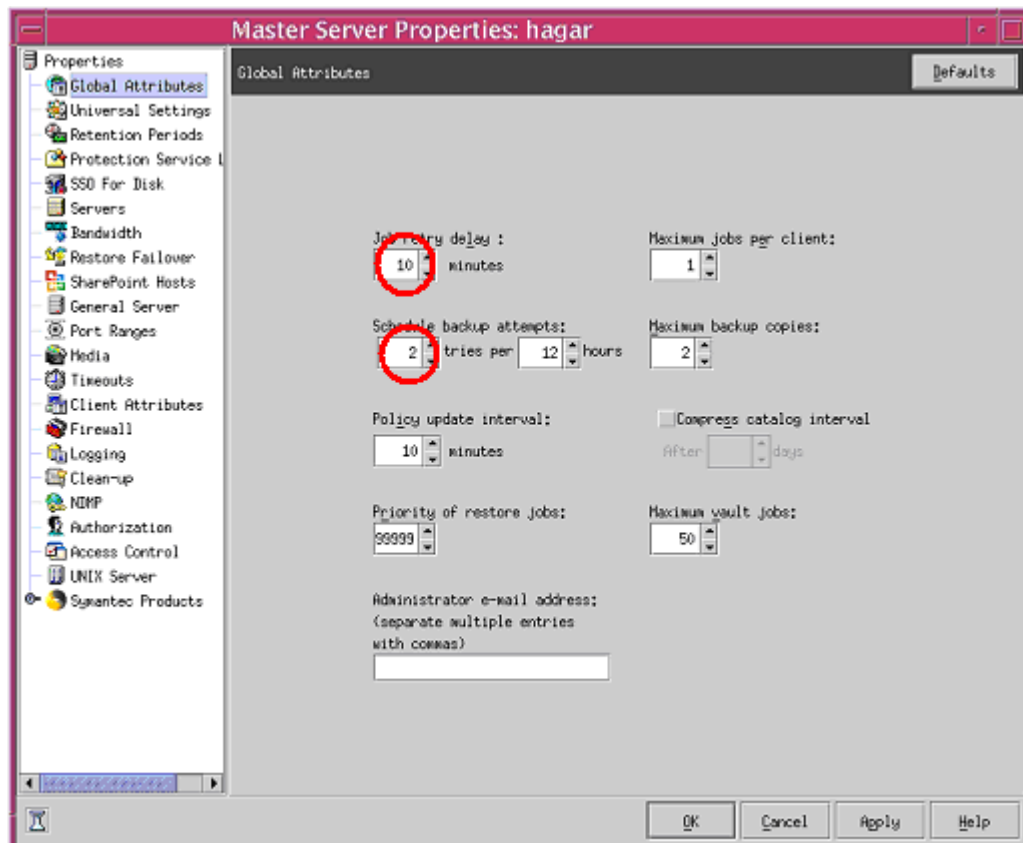
フェイルオーバー/テイクバックに要する時間よりも長い時間を設定してください。

下図では、例として10分間を設定しています。

- Schedule backup attempts を編集

万が一、「Job retry delay」で設定した時間内にフェイルオーバー/テイクバックが完了しない場合を考慮して試行回数には3以上の値を設定してください。

デフォルトは、12時間に2回です(*3) (*4)。



Step.2 NetBackupのサービスの再起動を行い、Step.1で変更した設定を有効にしてください。

2-2) バックアップ先にCIFSを指定し、スケジュールバックアップ以外でバックアップ

バックアップ先のファイルシステムとしてCIFSを使用している場合、HN/AN障害時にファイルシステムに接続不可能になった際、バックアップ処理はエラーとなります。スケジュールバックアップ以外でバックアップをする場合、NetBackupではタイムアウトや再試行といった機能は提供されていません。そのため、バックアップ処理をリトライするスクリプトを組む必要があります。

リトライ間隔に関しては、付録のフェイルオーバー/テイクバックの所要時間を参考にしてください。

- (*3) 初回バックアップでattemptは1です。Schedule backup attemptsにnを指定した場合、実際のリトライ回数はn-1回になります。
- (*4) Schedule backup attemptsで指定するのはPolicy毎の試行回数であり、Job毎の試行回数ではありません。

5-4 ActiveDirectory環境での注意事項

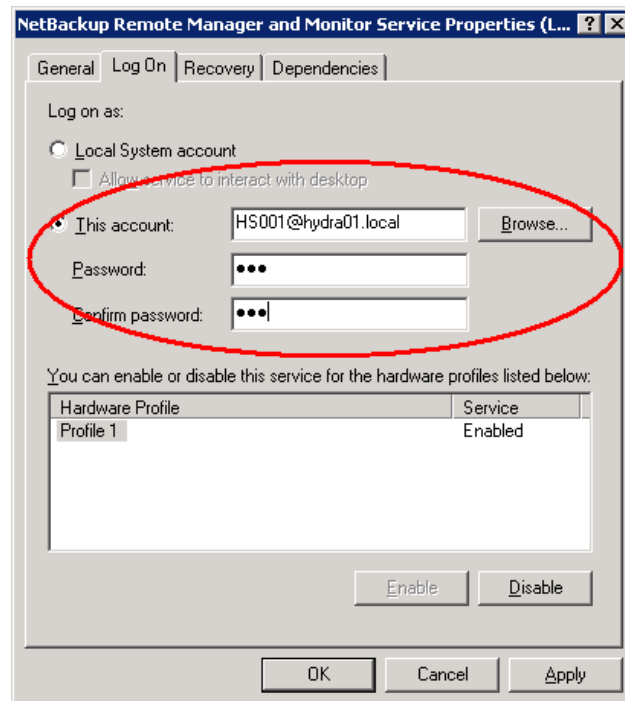
CIFSの認証方式としてActiveDirectoryが指定されている場合、NetBackupサービスの起動ユーザを、iStorage HSのファイルシステムへのアクセス権限を持ったユーザアカウントに変更する必要があります。

以下の手順で変更を行ってください。

- 1) コントロールパネル > 管理ツール > サービス > を開き、以下のサービスに対し ログオン・アカウントをLocal Systemから、使用するiStorage HSのファイルシステムへのアクセス権を持っている、Active Directoryドメインユーザに変更します。

- NetBackup Client Service
- NetBackup Remote Manager and Monitor Service
- NetBackup Service Layer
- NetBackup Legacy Network Service
- NetBackup Legacy Client Service

以下の例では、アクセス権を持ったユーザアカウントとしてHS001@hydra01.localを設定しています。



2) NetBackupのサービスの再起動を行ってください。

5-5 Windows環境でのファイルシステム容量表示

Windows 環境のNetBackup(*5)では、Storage Unit として容量が2PBよりも大きいファイルシステムを指定すると、ファイルシステム容量表示画面で不正な容量が表示されます。NetBackup管理コンソールの「Storage Unit」画面にて「Directory Properties」を確認したときに発生します。

なお、本現象は、表示上の問題であり、動作への影響がないことを確認しています。

(*5) 2010年4月時点では、NetBackup 6.5.4で本現象が発生することを確認しています。NetBackupの新しいバージョンでは修正されている可能性があります。対応状況については、NetBackupの購入元に確認してください。

6. トラブルシューティングについて

バックアップソフトウェア固有の問題が発生した場合は、バックアップソフトウェアのログを収集しNetBackupのご購入元へ確認を行ってください。ログの収集手順はお使いのNetBackupのマニュアルを参照してください。

iStorage HSで問題が発生した場合は、イベントを確認し、「iStorage HSシリーズ メッセージハンドブック」を参照して適切な対処を行ってください。iStorage HSでは、メール通報、SNMPインタフェース、イベントビューアといった3つの方法を利用してイベントを受信できます。それぞれの設定方法については、「iStorage HSシリーズ ユーザーズガイド」を参照してください。

NetVault Backup

1. iStorage HSの設定

NetVault Backupではデバイスタイプによっては、認識できるデバイス容量に上限が設けられています。iStorage HSのファイルシステム容量の既定値は256PBのため、既定値容量のままではNetVault Backupがデバイスとして認識できない場合があります。その場合には、ファイルシステムの容量変更が必要になります。容量変更が必要な場合に関しては、「2-1 iStorage HSをVTLとして設定」を参照してください。

上記にあてはまらない場合は、iStorage HSで必要となる特別な設定はありません。

1-1 iStorage HS ファイルシステム容量の変更

NetVault Backupの格納先デバイスタイプによっては、iStorage HSのファイルシステム容量の変更が必要な場合があります。詳しくは「2. NetVault Backupの設定」 - 「2-1 iStorage HSをVTLとして設定」 - 「2-1-1 iStorage HSのファイルシステムをVTLとして構成」を参照してください。ここではiStorage HSのファイルシステム容量の変更が必要な場合に行う手順を記載します。

ファイルシステムの容量の変更は、ファイルシステム単位にiStorage HSGUI/CLIから行えます。以下にGUIからiStorage HSのファイルシステムの容量を2PBにする手順を示します。

CLIから設定する場合は、「iStorage HSシリーズ コマンドリファレンス」を参照してください。

1-1-1 新規ファイルシステムの容量を変更する場合

ファイルシステムの作成時に、ファイルシステムの容量を2PBで設定してください。

ファイルシステム作成

ファイルシステムオプション

ファイルシステム名: fs

エクスポート先: HN / 01 / 01

エクスポートタイプ: ☒ NFS ☐ CIFS

容量: ファイルシステムの容量: 2 PB

☐ ハードクォータを有効にする

☐ ソフトクォータを有効にする ソフトリミット: 90 %

パリティ数: 3 (オーバーヘッド: 25%)

説明:

① 上記のファイルシステムの容量は2のべき乗に基づく単位で表示しています。(GB = 1024 × 1024 × 1024)

エクスポートオプション

エクスポート名: /exportfs

接続許可クライアント: *

① エントリを分けるには半角スペースを使用します。

アクセス権限: ☒ 読み書き ☐ 読み取り専用

OK キャンセル

既存ファイルシステムの容量を変更する場合

Step.1 当該ファイルシステムのアンエクスポート処理を行ってください。

ファイルシステム概要

フィルタ

ファイルシステム名: 状態: エクスポート, アンエクスポート, 不明, ア

格納済み容量: From GB To GB ノード: AN0101, AN0102

ファイルシステム名	ノード	状態	タイプ	格納済み容量	権限	マーカータイプ	フェイルオーバー	WORM	クォータ状態	ACL	説明
☐ CIFS_FS	AN0101	エクスポート-CIFS		1.1KB	読み書き	対象			無効	無効	This filesystem
☐ NFS_FS	AN0101	エクスポート-NFS		1.1KB	読み書き	対象			無効	無効	This filesystem
☒ fs1	AN0101	エクスポート-NFS		1.1KB	読み書き	対象			無効	無効	

1 - 3件中 1 - 3を表示

上記の格納済み容量は2のべき乗に基づく単位で表示しています。(GB = 1024 × 1024 × 1024)

ファイルシステムの格納済み容量について、容量を参照してください。

作成 移動 削除 エクスポート アンエクスポート チェック 修復 クローン

Step.2 当該ファイルシステムの容量を2PBに変更してください。

当該ファイルシステムを選択すると表示される以下のポップアップから設定を変更します。

ファイルシステム変更(fs1)

⚠ フェイルオーバーが使用可能な場合のみフェイルオーバー設定は有効になります。

ファイルシステムオプション

ファイルシステム名: fs1

エクスポート先: HN0101

状態: アンエクスポート

エクスポートタイプ: ☒ NFS ☐ CIFS

容量: ファイルシステムの容量:

☐ ハードクォータを有効にする

☐ ソフトクォータを有効にする ソフトリミット: %

格納済み容量: 4.4KB

パリティ数: 3

オーバーヘッド: 25%

説明:

作成日時: 2018/12/04 17:19:00

上記のファイルシステムの容量と格納済み容量は2のべき乗に基づく単位で表示しています。(GB = 1024 × 1024 × 1024)

OK キャンセル

2. NetVault Backupの設定

iStorage HSのファイルシステムは、NetVault Backup のVTL(Virtual Tape Library, 仮想テープ・ライブラリ)、仮想単体ドライブ、NVSD(NetVault SmartDisk)デバイス、として使用することができます(*1)。

NetVault Backupのディスクベースのストレージに対して有効なチューニング項目はiStorage HSに対しても有効です。

(*1) 各デバイスをサポートしているNetVault BackupのバージョンについてはNetVault Backupのご購入元へ確認を行ってください。

2-1 iStorage HSをVTLとして設定

iStorage HSのファイルシステムをNetVault BackupのVTLとして構成できます(*2)。

BackupサーバとしてWindowsをご利用の場合、VTL作成にそれほど時間はかかりませんが、BackupサーバとしてLinuxをご利用の場合は、NetVault Backupが全体のプリフォーマットを行うため、スロット数やメディアの容量によっては、VTL作成完了に時間を要します。

NetVault Backupの空き容量チェックが有効になっている場合や、iStorage HSのハードクォータ機能を使用している場合は、ファイルシステム容量を超えるメディアの作成がエラーになることがあります。その場合、スロット数やメディア容量をファイルシステム容量におさまるように設定してください。なお、メディアの最大サイズは800GB (819,200MB) です。

iStorage HSのファイルシステムをNetVault BackupのVTLとして構成する際の設定を以下に列挙します。

(*2) BackupサーバとしてWindowsをご利用の場合、iStorage HSのCIFSファイルシステムをNetVault BackupのVTLとして構成できるのは、NetVault Backupバージョン8.2以降になります。

2-1-1 iStorage HSのファイルシステムをVTLとして構成

iStorage HSのファイルシステム初期容量は256PBですが、バックアップ・デバイスとしてVTLを利用する場合、NetVault Backupではファイルシステムの容量値として2PBまでしか扱うことができません。ただし、使用されているNetVault Backupのバージョンが8.2以降の場合、VTLのディスク空き容量チェックを無効にすることで、本ファイルシステム容量の制限を回避できます。バックアップ・デバイスとしてVTLを利用する場合、iStorage HSのファイルシステムの容量を2PB以下に設定、もしくは、VTLのディスク空き容量チェックの無効化を行ってください。

ファイルシステム容量の変更手順に関して詳細は、「1-1 iStorage HSファイルシステム容量の変更」を参照してください。NetVault Backupのディスク空き容量チェックを無効にする手順を以下に示します。

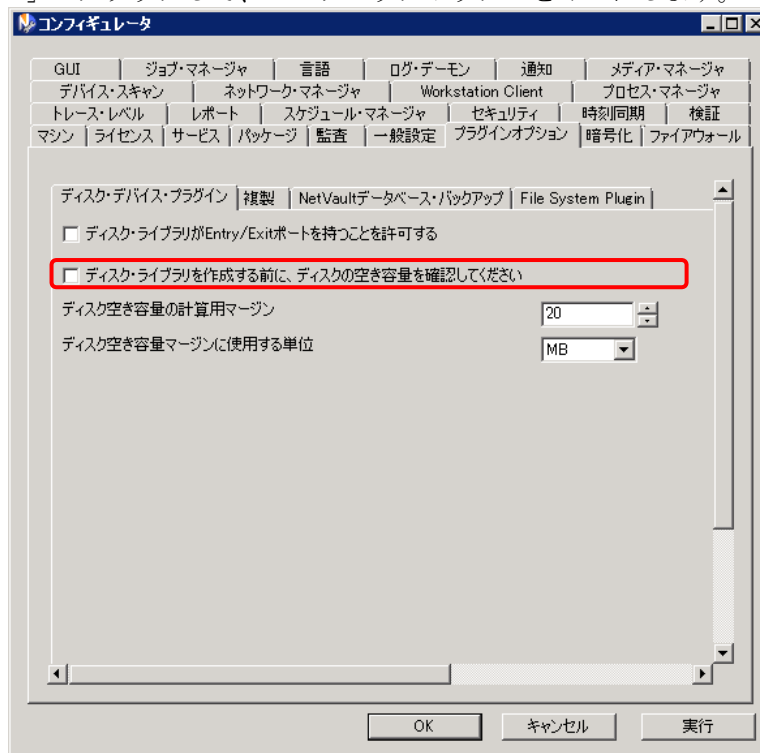
Step.1 NetVault Backupコンフィギュレータを起動します。

Step.2 [コンフィギュレータ] ウィンドウの [プラグイン・オプション] タブをクリックします。

Step.3 [ディスク・デバイス・プラグイン] サブタブをクリックします。

Step.4 以下のパラメータを設定します。

- [ディスク・ライブラリを作成する前に、ディスクの空き容量を確認してください] をクリックして、このチェックボックスをオフにします。



Step.5 [OK] をクリックして変更を適用し、コンフィギュレータを終了します。あるいは [実行] をクリックすると、コンフィギュレータを終了せずに新規の設定を適用させることができます。

2-1-2 メディア・ブロック・サイズについて

iStorage HSでは、VTLのメディア・ブロック・サイズを2048KBに設定することを推奨します。メディア・ブロック・サイズを2048KBに設定することで、バックアップ性能が向上する可能性があります。

メディア・ブロック・サイズはデフォルトでは32KBになっていますので、2048KBに増やしてください。また、メディア・ブロック・サイズを増やす場合は、共有メモリ設定も共に増やす必要があります。共有メモリの設定値は、少なくとも、メディア・ブロック・サイズの4倍の値に1KBを足した値になるようにしてください。

2-1-3 データ圧縮機能について

iStorage HSの重複排除を効果的に機能させるために、NetVault Backupのデータ圧縮機能は使用しないことを推奨します。

iStorage HSではバックアップ時に重複排除と物理データ圧縮を行っています。データの物理圧縮はiStorage HS内で実行しているため、NetVault Backupで実行する必要はありません。

2-2 iStorage HS を仮想単体ドライブとして設定

iStorage HSのファイルシステムをNetVault Backupの仮想単体ドライブとして構成できます。

iStorage HS のファイルシステムをNetVault Backupの仮想単体ドライブとして構成する際の設定を以下に列挙します。

2-2-1 メディア・ブロック・サイズについて

iStorage HSでは、仮想単体ドライブのメディア・ブロック・サイズを2048KBに設定することを推奨します。メディア・ブロック・サイズを2048KBに設定することで、バックアップ性能が向上する可能性があります。

メディア・ブロック・サイズはデフォルトでは32KBになっていますので、2048KBに増やしてください。また、メディア・ブロック・サイズを増やす場合は、共有メモリ設定も共に増やす必要があります。共有メモリの設定値は、少なくとも、メディア・ブロック・サイズの4倍の値に1KBを足した値になるようにしてください。

2-2-2 データ圧縮機能について

iStorage HSの重複排除を効果的に機能させるために、NetVault Backupのデータ圧縮機能は使用しないことを推奨します。

iStorage HSではバックアップ時に重複排除と物理データ圧縮を行っています。データの物理圧縮はiStorage HS内で実行しているため、NetVault Backupで実行する必要はありません。

2-3 iStorage HSをNVSDとして設定

iStorage HSのファイルシステムをNetVault BackupのNVSDとして構成できます。

iStorage HSのファイルシステムをNVSDとして構成する際の設定を列挙します。

NVSDの設定と管理は主に NVSDコマンドライン・インタフェース(CLI)を介して行われます。後述するNVSD CLIの例はWindows環境での例になります。NVSD CLIに関して詳細はNetVaultBackupのマニュアルを参照してください。

2-3-1 iStorage HSのファイルシステムをNVSDとして構成

NVSDはインストール時に、データを格納するステージング・パス・フォルダやストア・パス・フォルダを指定する必要があります。しかし、インストール時にステージング・パス・フォルダやストア・パス・フォルダのパスをUNC指定で設定することができません。

そのため、ステージング・パス・フォルダやストア・パス・フォルダとして iStorage HSのファイルシステムを指定する場合、インストール時には一旦別のフォルダを指定し、インストール後にiStorage HSのファイルシステムを指定する必要があります。インストール後に以下の手順で、iStorage HSのファイルシステムを指定してください。

Step.1 インストール時に設定したステージング・パス・フォルダやストア・パス・フォルダを無効にします。

```
> <install path>%foundation%bin%smartdisk.bat" config --update --volume <インストール時に指定したステージング・パス・フォルダ> --favour none --deny all
> <install path>%foundation%bin%smartdisk.bat" config --update --volume <インストール時に指定したストア・パス・フォルダ> --favour none --deny all
```

Step.2 iStorage HSのファイルシステムのパスをステージング・パス・フォルダとして指定します。

```
> <install path>%foundation%bin%smartdisk.bat" config --add --volume <iStorage HSのファイルシステムのパスをUNC指定> --pool <label> --favour Staging --favour "Disk Index" --favour "Chunk Index" --account <account> --password <password>
```

Step.3 Step.1,2で設定した内容が反映されているかNVSDの設定を確認します(*3)。

```
> <install path>%foundation%bin%smartdisk.bat" config --show
```

(*3) iStorage HSのファイルシステムは初期容量の256PBのままで、ステージング・パス・フォルダとして指定できますが、使用可能な空き容量を表すSpace.Availableとしては約92PBまでしか認識されません。

2-3-2 ブロック・サイズについて

iStorage HSでは、NVSDのブロック・サイズを2048KBに設定することを推奨します。メディア・ブロック・サイズを2048KBに設定することで、バックアップ性能が向上する可能性があります。

ブロック・サイズはデフォルトでは32KBになっていますので、2048KBに増やしてください。

2-3-3 NVSD 重複排除機能の無効化

NVSDの重複排除機能を無効にしてください。iStorage HSではバックアップ時に重複排除と物理データ圧縮を行っています。重複排除はiStorage HS内で実行しているため、NetVault Backupで実行する必要はありません。

2-4 NetVault Backupのバックアップの暗号化機能について

NetVault Backupのバックアップの暗号化機能を使用しないでください。暗号化機能を使用しないことでiStorage HSでより効果的に重複排除を行うことができます。

3. バックアップサーバの設定

iStorage HSに対してより高速なバックアップ/リストアを行うには、NetVault Backup がインストールされているサーバの設定変更が必要になります。
バックアップサーバの設定については「付録C オペレーティングシステムの設定」を参照してください。

4. ネットワークの構成

iStorage HSに対してより高速なバックアップ/リストアを行うには、専用のネットワークの利用を推奨します。ネットワークを専用とすることで、バックアップ/リストア用の帯域幅が他の通信により減少することを防ぐことができます。

iStorage HSご利用時のネットワークの構成については「第2章 配備計画 Step 2. ネットワークの計画」を参照してください。

5. NetVault Backup 運用時の注意事項

5-1 小さなサイズのファイルのバックアップ

NetVault Backupを用いて iStorage HSへのバックアップ処理を行う際、バックアップするデータに数十 KB 未満の小さなファイルが多く含まれていると、iStorage HSの重複排除率は低くなる可能性があります。これは、NetVault Backupが各バックアップ対象ファイルのヘッダ部に管理情報(マーカー)を付加することに起因します。

iStorage HSではブロックレベルで重複データを検出し、重複しないユニークなデータのみを圧縮・格納することによって効率的なストレージ格納容量を実現します。(DataRedux®)
NetVault Backupの管理情報はバックアップ対象ファイル毎に付加されます。そのため、iStorage HSがバックアップデータをブロックレベルに分割する際に、バックアップデータに数十KB未満の小さなファイルが含まれていると、分割されたバックアップデータの個々のブロックの多くにNetVault Backupによって付加された管理情報が含まれることになります。この付加された管理情報がバックアップ毎にユニークになることがあるため、管理情報が含まれたブロックは前回バックアップ時と比べて重複しないユニークなデータとみなされ、排除されずに iStorage HSへ格納されます。これによって iStorage HSの重複排除率は低くなる場合があります。

6. トラブルシューティングについて

バックアップソフトウェア固有の問題が発生した場合は、バックアップソフトウェアのログを収集しNetVault Backupのご購入元へ確認を行ってください。ログの収集手順はお使いのNetVault Backupのマニュアルを参照してください。

iStorage HSで問題が発生した場合は、イベントを確認し、「iStorage HSシリーズ メッセージハンドブック」を参照して適切な対処を行ってください。iStorage HSでは、メール通報、SNMPインタフェース、イベントビューアといった3つの方法を利用してイベントを受信できます。それぞれの設定方法については、「iStorage HSシリーズ ユーザーズガイド」を参照してください。

NetWorker

1. iStorage HS の設定

iStorage HSの重複排除機能を最適化するために、マーカーフィルタリング機能を有効にしてください。

また、ファイルシステムの容量を変更する場合は、設定する容量値に注意する必要があります。上記にあてはまらない場合は、iStorage HSで必要となる特別な設定はありません。

1-1 マーカーフィルタリングオプション

NetWorkerでは、マーカーと呼ばれる管理情報をバックアップ対象ファイル、バックアップデータブロック毎に付加します。付加されたマーカーはバックアップ毎にユニークになる場合があります。そのため、バックアップデータの重複排除率を低下させる要因になることがあります。ファイルシステムのマーカーフィルタリングオプションは、このマーカーのフィルタリングを行ない、データ保存時の重複排除機能を最適化するオプションです。

マーカーフィルタリングオプションの設定は、ファイルシステムの作成時にiStorage HSのGUI/CLIから行えます。GUIから設定する場合は、ファイルシステムの作成時に「マーカーフィルタリング」の「有効」のチェックボックスを選択し、マーカータイプとして”NW1(EMC NetWorker)”を選択します。

The screenshot shows the 'File System Creation' (ファイルシステム作成) window. The 'Export Options' (エクスポートオプション) section includes fields for 'Export Name' (fs1), 'Comment', 'Access Permissions' (Read/Write selected), 'Connect Allowed Clients', and 'Connect Denied Clients'. The 'Advanced Options' (高度なオプション) section shows 'Marker Filtering' (マーカーフィルタリング) checked and set to 'NW1(EMC NetWorker)'. Other options include 'Failover' (checked), 'WORM' (disabled), and 'ACL' (disabled). A warning message at the bottom states: 'フェイルオーバーが使用可能な場合のみフェイルオーバー設定は有効になります。' (Failover settings are only valid when failover is usable).

詳細なファイルシステムの作成方法については「iStorage HSシリーズ ユーザーズガイド」を参照してください。また、CLIから設定する場合は「iStorage HSシリーズ コマンドリファレンス」を参照してください。

マーカーフィルタリングオプションを使用する場合は、NetWorkerの設定も行う必要があります。設定方法に関しては、“2-2 iStorage HSをAdvanced File Type Device(AFTD)として設定”、“2-3 iStorage HSの重複排除機能を最適化するNetWorkerのブロックサイズ”を参照してください。

マーカーフィルタリングオプションを使用する場合の注意事項を以下に列挙します。各機能についての説明は「iStorage HSシリーズ ユーザーズガイド」を参照してください。

- ファイルシステムの作成後は、マーカーフィルタリングの設定を変更することはできません。
- レプリケーションセットのマスタとレプリカでは、同じマーカーフィルタリングとマーカータイプを持っている必要があります。
- マーカーフィルタリングが有効となっているファイルシステムがレプリケーションの対象となっている場合、初回のレプリケーションが終了するまで、レプリカのファイルシステムはエクスポートできません。

1-2 Advanced File Type Device(AFTD)使用時のファイルシステム容量

iStorage HSでは、重複排除率を最適化するために、NetWorkerのブロックサイズを変更する必要があります。そのため、NetWorker DiskBackupで設定するファイルタイプデバイスとしてブロックサイズが変更可能な Advanced File Type Device(AFTD)を推奨しています。

AFTDを使用している場合、書き込み先デバイスの空き容量が2GB未満になると、NetWorkerサーバは転送データをストレージデバイス上に同期させる内部処理を頻繁に実行するようになり、データ転送速度が著しく低下します。

iStorage HSのファイルシステム容量を変更する際には、この現象を避けるために、iStorage HSのファイルシステムサイズを必要容量 + 2GB以上で作成してください。

クォータ機能を使用し、ソフトクォータを有効にする際には、データ転送速度が低下する前に容量制限の通知を出すために、ソフトリミットをファイルシステムサイズ - 2GB以下になるように設定してください。

Advanced File Type Device(AFTD)については、“2-2 iStorage HS をAdvanced File Type Device(AFTD)として設定”を参照してください。

1-3 Advanced File Type Device(AFTD)使用時のNFSの設定(NetWorker8.0以降利用時)

NetWorker8.0で Advanced File Type Device(AFTD)を利用する場合、NFSの設定で iStorage HSに対し root ユーザでアクセスする設定を行う必要があります。

GUIから設定をする場合は、ファイルシステムの作成時、もしくは、ファイルシステム設定変更時に、「エクスポートオプション」項目の「ユーザアクセス」ドロップダウンリストから、以下のオプションを選択してください。

「root ユーザを root ユーザとしてアクセスさせる。(no_root_squash)」

ファイルシステム作成

① エントリを分けるには半角スペースを使用します。

アクセス権限 ☒ 読み書き ☐ 読み取り専用

ユーザアクセス **rootユーザをrootユーザとしてアクセスさせる。(no_root_squash)**

匿名ユーザ: UID=1000、GID=1000

その他のオプション ☒ 1024番以上のポートからのアクセスを拒否する。(secure)

高度なオプション

マーカーフィルタリング ☐ 有効 CVS1 (CommVault Simpana)

フェイルオーバー ☒ フェイルオーバー発生時にファイルシステムを移動させる。

WORM 無効 (WORMライセンスがない)

ACL ☐ 有効

ファイル情報 ☐ ファイル属性 ☐ タイムスタンプ ☐ アクセス日時

暗号化 ☐ 有効

暗号化キー

⚠ フェイルオーバーは使用可能な場合のみフェイルオーバー設定は有効になります。

OK キャンセル

CLIで設定をする場合は、nfs export実行時に以下のパラメータを指定してください。

nfs export name=<filesystem 名> **anonymous=no** ~

上記の設定を行わない場合、AFTDにラベル付けをするコマンド実行時(nsrmm -l)に、以下のエラーを出力してラベル付けに失敗します。

6211:nsrmm: The user 'root (uid=0)' does not own the contents of device '<filesystem 名>'.

2. NetWorkerの設定

2-1 NetWorkerライセンス

NetWorker を iStorage HSと組み合わせて使用するには、NetWorker DiskBackupオプションライセンスが必要です。

2-2 iStorage HSをAdvanced File Type Device(AFTD)として設定

iStorage HSでは、重複排除率を最適化するために、NetWorkerのブロックサイズを変更する必要があります(*1)。そのため、iStorage HSのファイルシステムをブロックサイズが変更可能なAdvanced File Type Device(AFTD)として構成してください。

NetWorkerのディスクベースのストレージに対して有効なチューニング項目はiStorage HSに対しても有効です。

設定手順については、NetWorkerのマニュアルを参照してください。

(*1) マーカーフィルタリングオプションを使用する場合でもブロックサイズの変更を行う必要があります。マーカーフィルタリングオプション使用時に設定するブロックサイズに関しては、“2-3 iStorage HSの重複排除機能を最適化するNetWorkerのブロックサイズ”を参照してください。

2-3 iStorage HSの重複排除機能を最適化するブロックサイズについて

iStorage HSはブロックレベルで重複データを検出し、重複していない一意のデータだけを圧縮して保存することによって、効率的なストレージを実現します(DataRedux®)。

NetWorker が短い間隔でバックアップデータに管理情報を挿入すると、iStorage HSが分割し作成したバックアップデータブロックの多くに管理情報が追加されます。

iStorage HSのデータ圧縮技術を最大限に利用できるように、AFTDのブロックサイズを、選択可能なサイズの中で最大サイズに設定することを推奨します。ブロックサイズの最大値はプラットフォームに依存します。

なお、マーカーフィルタリングオプションを使用する場合は、フィルタリング処理のオーバーヘッドを少なくするためブロックサイズとして1024KBを指定してください。

設定手順については、NetWorkerのマニュアルを参照してください。

2-4 AN クラスタ機能利用時のNetWorkerの設定

iStorage HSでは、HN/ANを組み合わせて高可用性クラスタを構成することができます(AN クラスタ機能)。クラスタに参加したHN/ANの障害時には、別のHN/ANに IPアドレスおよびファイルシステムを引き継ぎ、一時的に停止したサービスを自動的に回復します。障害が発生したHN/ANのサービスを他のHN/ANに引き継ぐ操作を「フェイルオーバー」、他のHN/ANに引き継がれたサービスを元の HN/ANに戻す操作を「テイクバック」といいます。

この AN クラスタ機能を用いれば、NetWorkerを用いたバックアップ中にバックアップ先 HN/ANに障害が発生した場合でも、他のANでサービスを引き継ぎ、バックアップ処理を継続/再試行することが可能になります。

フェイルオーバー/テイクバックが行われる際には、一時的にバックアップ先のファイルシステムに接続できなくなります。したがって、バックアップ方法によっては、フェイルオーバー/テイクバック中にバックアップ処理が異常終了しないように、NetWorkerの設定を変更する必要があります。

1-1) バックアップ先にNFSを指定し、スケジュールバックアップでバックアップ

iStorage HS へのnfsマウント時にオプションとしてhard 指定して下さい。

バックアップ先のファイルシステムとしてnfsを使用している場合、HN/AN障害時にファイルシステムに接続不可能になっても、iStorage HS はバックアップサーバに対しエラーを返しません。そのため、NetWorkerは「インアクティビティタイムアウト」に設定されている時間待ち合わせた後で、バックアップ処理を停止します。

バックアップ処理を継続させるためには、「インアクティビティタイムアウト」に、フェイルオーバー/テイクバックの所要時間よりも長い時間を設定してください。「インアクティビティタイムアウト」に設定されている時間内にフェイルオーバー/テイクバックが完了した場合、バックアップ先ファイルシステムが接続可能となった時点で、それまで書き込んでいたバックアップイメージに対して継続して書き込みを行います。

以下に設定手順を示します。

1. NetWorkerの「管理」ウィンドウで、「構成」をクリックします。
2. 展開された左側のペインで、「グループ」を選択します。
3. 編集するグループを選択します。
4. 「ファイル」メニューから「プロパティ」を選択します。
5. 「高度」タブをクリックします。
6. 「インアクティビティタイムアウト」の値を編集します。
フェイルオーバー/テイクバックの所要時間よりも長い時間を設定してください。
※フェイルオーバー/テイクバックの所要時間は付録を参照ください。
7. 「クライアントの再試行回数」属性の試行回数を編集します。
万が一、「インアクティビティタイムアウト」で設定した時間内にフェイルオーバー/テイクバックが完了しない場合を考慮して1以上の値を設定してください。
8. 「OK」をクリックします。
※NetWorkerのサービスの再起動は必要ありません。この設定は次回バックアップ実行時から反映されます。

1-2) バックアップ先にNFSを指定し、saveコマンドでバックアップ

iStorage HSへのnfsマウント時にオプションとしてhardを指定して下さい。

バックアップ先のファイルシステムとしてnfsを使用している場合、HN/AN障害時にファイルシステムに接続不可能になっても、iStorage HSはバックアップサーバに対しエラーを返しません。NetWorkerのバックアップ処理は中断されることなく、バックアップ先ファイルシステムが接続可能となった時点で、それまで書き込んでいたバックアップイメージに対して継続して書き込みを行います。NetWorkerの設定変更の必要はありません。

2-1) バックアップ先にCIFSを指定し、スケジュールバックアップでバックアップ

バックアップ先のファイルシステムとしてcifsを使用している場合、HN/AN障害時にファイルシステムに接続不可能になった際、バックアップ処理はエラーとなります。バックアップ処理がエラーとなった後、NetWorkerは「インアクティビティタイムアウト」に設定されている時間待ち合わせた後で、バックアップを再試行します。

バックアップ処理を再試行させるためには、以下の2点を行ってください。

- 「インアクティビティタイムアウト」に、フェイルオーバー/テイクバックの所要時間よりも長い時間を設定してください。
- 「クライアントの再試行回数」属性の試行回数を変更してください。

「インアクティビティタイムアウト」に設定されている時間内にフェイルオーバー/テイクバックが完了した場合でも、NetWorkerはインアクティビティタイムアウトに設定されている時間待ち合わせた後で、バックアップを再試行します。再試行されたバックアップは、新規バックアップイメージとして書き込みを行います。

以下に設定手順を示します。

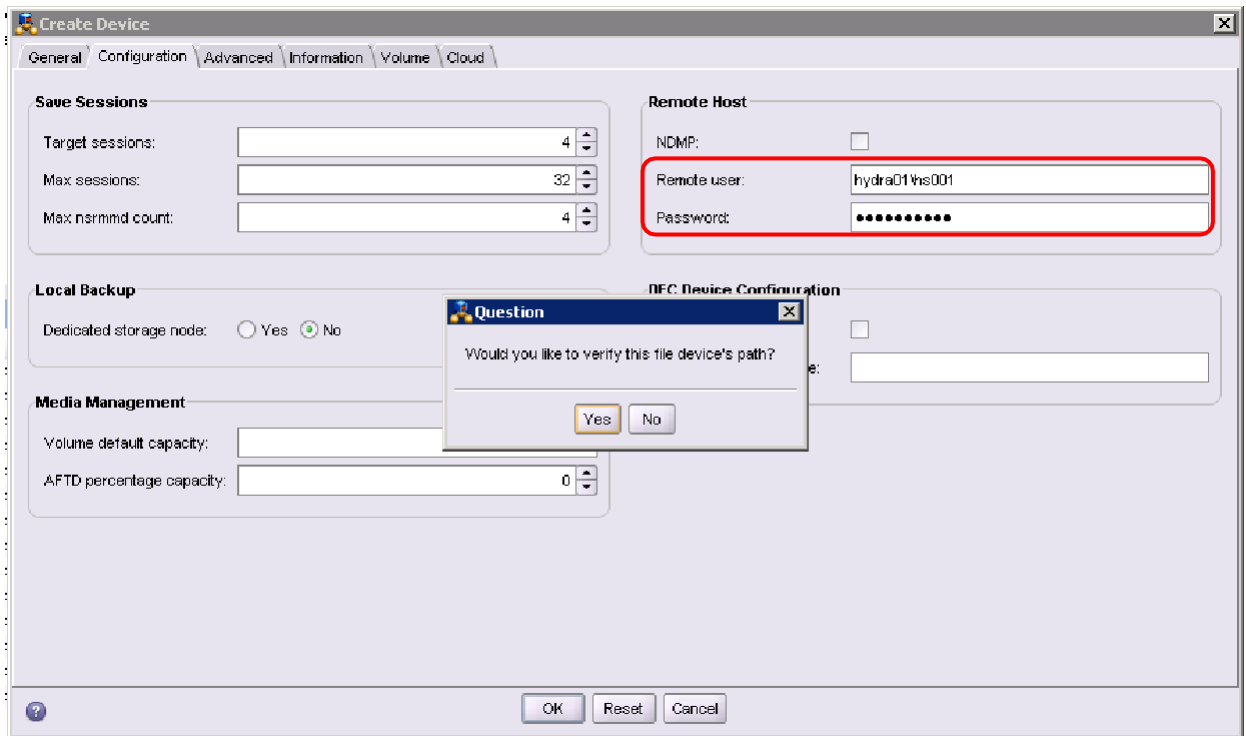
1. NetWorkerの「管理」ウィンドウで、「構成」をクリックします。
2. 展開された左側のペインで、「グループ」を選択します。
3. 編集するグループを選択します。
4. 「ファイル」メニューから「プロパティ」を選択します。
5. 「高度」タブをクリックします。
6. 「インアクティビティタイムアウト」の値を編集します。
フェイルオーバー/テイクバックの所要時間よりも長い時間を設定してください。
※フェイルオーバー/テイクバックの所要時間は付録を参照ください。
7. 「クライアントの再試行回数」属性の試行回数を編集します。
万が一、「インアクティビティタイムアウト」で設定した時間内にフェイルオーバー/テイクバックが完了しない場合を考慮して2以上の値を設定してください。
8. 「OK」をクリックします。
※NetWorkerのサービスの再起動は必要ありません。この設定は次回バックアップ実行時から反映されます。

2-2) バックアップ先にCIFSを指定し、saveコマンドでバックアップ

バックアップ先のファイルシステムとしてCIFSを使用している場合、HN/AN障害時にファイルシステムに接続不可能になった際、バックアップ処理はエラーとなります。コマンドを用いてバックアップをする場合、NetWorkerではタイムアウトや再試行といった機能は提供されていません。そのため、バックアップ処理をリトライするスクリプトを組む必要があります。リトライ間隔に関しては、付録のフェイルオーバー/テイクバックの所要時間を参考にしてください。

2-5 Active Directory 認証のための NetWorker 8.1 の設定

Active Directory認証でデバイスを作成する際、「設定」タブにてリモートユーザとパスワードを入力する必要があります。iStorage HS にActive Directory認証の設定がされている場合、NetWorker 8.1はユーザ名とパスワードを入力するまでデバイスの作成を許可しません。



3. バックアップサーバの設定

iStorage HSに対してより高速なバックアップ/リストアを行うには、NetWorkerがインストールされているバックアップサーバの設定変更が必要になります。

バックアップサーバの設定については「付録C オペレーティングシステムの設定」を参照してください。

4. ネットワークの構成

iStorage HSに対してより高速なバックアップ/リストアを行うには、専用のネットワークの利用を推奨します。ネットワークを専用とすることで、バックアップ/リストア用の帯域幅が他の通信により減少することを防ぐことができます。

iStorage HSご利用時のネットワークの構成については「第2章 配備計画 Step 2. ネットワークの計画」を参照してください。

5. NetWorker 運用時の注意事項

5-1 小さなファイルをバックアップするときの重複排除率

iStorage HSではブロックレベルで重複データを検出し、重複しないユニークなデータのみを圧縮・格納することによって効率的なストレージ格納容量を実現します。(DataRedux®) NetWorkerの管理情報はバックアップ対象ファイル毎に付加されます。そのため、iStorage HSがバックアップデータをブロックレベルに分割する際に、バックアップデータに数十KB未満の小さなファイルが含まれていれば、分割されたバックアップデータの個々のブロックの多くに NetWorkerによって付加された管理情報が含まれることになります。この付加された管理情報にはバックアップデータの先頭からのオフセット情報が含まれるため、バックアップデータに変更があると、前回のバックアップ時と比べてユニークになります。そのため、管理情報が含まれたブロックは前回バックアップ時と比べて重複しないユニークなデータとみなされ、排除されずにiStorage HSへ格納されます。これによってiStorage HSの重複排除率は低くなります(*1)。

5-2 サーバ・クライアント構成について

NetWorkerのサーバとクライアントが別のマシンで構成されている場合、サーバ・クライアント間に流れるバックアップデータは、64KBにブロッキングされます。このサイズは、“2-3 iStorage HSの重複排除機能を最適化するブロックサイズ”の方法でNetWorkerのブロックサイズを変更しても変わりません。その結果、サーバとクライアントが同じマシンで構成されている場合に比べて、iStorage HSの重複排除率は小さくなる場合があります(*1)。

(*1) iStorage HSのマーカーフィルタリング機能を使用すれば、重複排除率の低下を防ぐことができます。詳しくは、「1-1 マーカーフィルタリングオプション」を参照下さい。

6. トラブルシューティングについて

バックアップソフトウェア固有の問題が発生した場合は、バックアップソフトウェアのログを収集しNetWorkerのご購入元へ確認を行ってください。ログの収集手順はお使いのNetWorkerのマニュアルを参照してください。

iStorage HSで問題が発生した場合は、イベントを確認し、「iStorage HSシリーズ メッセージハンドブック」を参照して適切な対処を行ってください。iStorage HSでは、メール通報、SNMPインタフェース、イベントビューアといった3つの方法を利用してイベントを受信できます。それぞれの設定方法については、「iStorage HSシリーズ ユーザーズガイド」を参照してください。

Oracle Exadata Database Machine

1. iStorage HS の設定

1-1 マーカーフィルタリングオプション

iStorage HSバージョン 4.0以降をご利用の場合は、iStorage HSの重複排除機能を最適化するために、RMAN対応のマーカーフィルタリング機能が利用できます。RMANでは、バックアップファイルに対してデータベースのブロックサイズ単位にマーカーを付加します。バックアップ・セット方式(*1)でバックアップを実行している場合、ブロック内のデータに変化がなかったとしても、マーカーはバックアップ毎にユニークになることがあるため、バックアップデータの重複排除率を低下させる要因になることがあります。ファイルシステムのマーカーフィルタリングオプションは、このマーカーのフィルタリングを行い、データ保存時の重複排除機能を最適化するオプションです。Exadataのバックアップでは、マーカーフィルタリングオプションの利用を推奨します。

マーカーフィルタリングオプションの設定は、ファイルシステムの作成時にiStorage HSのGUI/CLIから行えます。GUIから設定する場合は、ファイルシステムの作成時に「マーカーフィルタリング」の「有効」チェックボックスを選択し、マーカータイプとして「RM1(Oracle Recovery Manager)」を選択してください。

The screenshot shows the 'File System Creation' (ファイルシステム作成) window. In the 'Advanced Options' (高度なオプション) section, the 'Marker Filtering' (マーカーフィルタリング) checkbox is checked, and the dropdown menu is set to 'RM1(Oracle Recovery Manager)'. Other options include 'File Overwrite' (フェイルオーバー) checked, 'WORM' set to 'None' (無効), 'ACL' unchecked, 'File Information' (ファイル情報) unchecked, 'Encryption' (暗号化) unchecked, and 'Encryption Key' (暗号化キー) set to 'Default' (デフォルト). The 'OK' and 'Cancel' buttons are at the bottom right.

詳細なファイルシステムの作成方法については「iStorage HSシリーズ ユーザーズガイド」を参照してください。また、CLIから設定する場合は「iStorage HSシリーズ コマンドリファレンス」を参照してください。

マーカーフィルタリングオプションを使用する場合の注意事項を以下に列挙します。各機能についての説明は「iStorage HSシリーズ ユーザーズガイド」を参照してください。

- ファイルシステムの作成後は、マーカーフィルタリングの設定を変更することはできません。
- レプリケーションセットのマスタとレプリカでは、同じマーカータイプを持っている必要があります。
- マーカーフィルタリングが有効となっているファイルシステムがレプリケーションの対象となっている場合、初回のレプリケーションが終了するまで、レプリカのファイルシステムはエクスポートできません。

- (*1) イメージ・コピー方式の場合は、マーカーフィルタリングオプションが無くても、iStorage HSの重複排除が効果的に働きます。ただし、イメージ・コピー方式ではバックアップファイルの分割ができないため、バックアップ多重度の調整が難しくなります。詳しくは「2-3 RMANバックアップファイル分割について」を参照ください。

1-2 ファイルシステムの非同期設定

iStorage HSバージョン4.0以降をご利用の場合は、NFSを利用したRMANバックアップによる転送時間を短縮するために、ファイルシステムの非同期設定が利用できます。iStorage HSのファイルシステムをExadataのデータベースサーバから NFS マウントしてRMANでアクセスする場合、ファイルシステムの非同期設定を行うことで転送性能を向上することができます。

ただし、本機能を使用すると、コマンドで明示的に同期を行う前にiStorage HS側のノードがダウンした場合に、バックアップデータが失われる可能性があります。ファイルシステムの非同期設定を行う場合は、本リスクに注意して運用を行ってください。なお、ユニバーサル高速I/Oを使用する場合は非同期設定によるリスクを負うことなく転送時間を短縮できます。

ファイルシステムの非同期設定はiStorage HSのCLIから行えます。ファイルシステムの作成/変更時に“**async=enable**”を追加してください。

例：ファイルシステムを新規作成する場合

```
# fs create node=HN0101 name=fs1 marker-type=RM1 async=enable
# nfs export name=fs1
```

例：既存のファイルシステムを変更する場合

```
# nfs unexport name=fs1
# fs modify name=fs1 async=enable
# nfs export name=fs1
```

既存のファイルシステムを変更する場合は、ファイルシステムを一旦アンエクスポートする必要があります。そのため、設定変更時は当該ファイルシステムに対するバックアップ/リストアを行わないでください。

CLIによる詳細なファイルシステムの作成方法については「iStorage HSシリーズ コマンドリファレンス」を参照してください。

非同期設定のファイルシステムに対して書き込み処理を行う場合、NFSクライアントは、iStorage HSのディスクにデータが反映される前に書き込み処理を終了します。そのため、バックアップジョブが完了したタイミングで必ず明示的に同期を行ってください。ファイルシステムの同期は、iStorage HSのCLIの"**fs sync**"コマンドを利用してください。RMANのバックアップ運用に組み込むには、RMANバックアップジョブの実行完了後に、RSHクライアントなどから iStorage HSに対してコマンドを送信します。

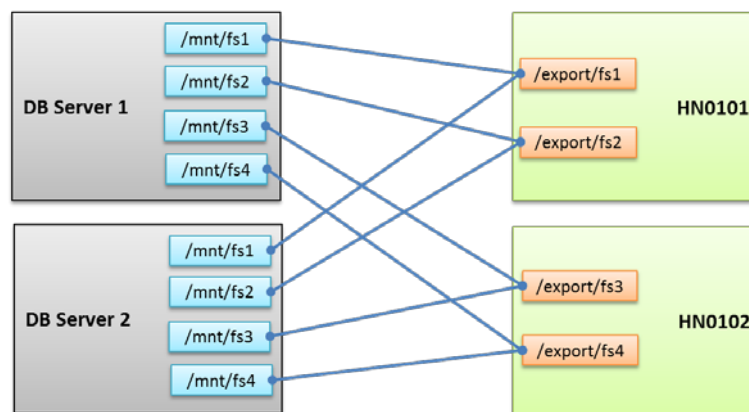
例：fs1に対してfs syncを実行する場合

```
# fs sync end name=fs1
```

2. Exadataの設定

2-1 iStorage HSのファイルシステムをマウントする

ExadataからiStorage HSにRMANのバックアップを実行するには、ExadataのデータベースサーバからiStorage HSのファイルシステムをマウントする必要があります。マウントポイントは多重実行による性能向上を目的として複数用意することを推奨します。また、RMANを実行する各データベースサーバが、同じマウントポイント名で各ファイルシステムをマウントするようにしてください。下記に、Exadataのデータベースサーバ2台からハイブリッドノード2台に対してマウントをする際の構成例を示します。



NFSのデータ転送サイズの推奨値は読み込み131072バイト、書き込み32768バイトです。また、ExadataはRAC構成のため、マウント時に"actimeo=0"のオプションが必要です。指定されていない場合、RMANのバックアップに失敗する可能性があります。以下にマウントオプションの例を示します。

```
# mount -t nfs -o
  rw,bg,hard,intr,nfsvers=3,tcp,actimeo=0,rsz=131072,wsz=32768
  <iStorage HS の IP アドレス>:/export/fs1 /mnt/fs1
```

2-2 RMANの実行多重度について

バックアップとリストアは多重実行することで、iStorage HSへの転送性能が向上する可能性があります。アクセラレータ機能を持つノードが1台の場合はバックアップとリストアはそれぞれ4多重を推奨します。同2台以上の場合はバックアップとリストアはそれぞれ8多重を推奨します。

RMANのストリーム多重度の設定は、手動構成と自動構成の2つの方法があります。両方が設定されている場合は手動構成が優先されます。手動構成では、RMANの実行文において、多重度分のチャンネルをその都度作成します。それぞれのチャンネルの作成時に、ネットワークセグメントやファイルシステムが異なるマウントポイントを指定することで、転送経路を分散させることができます。自動構成の場合は、単一のマウントポイントに対して複数のチャンネルを作るので、転送経路の分散ができません。多くの場合、転送経路の分散はバックアップとリストアの転送性能向上に有効です。そのため、本書では手動構成による設定方法を推奨します。

バックアップの場合の手動構成設定例を示します。下記例のように、チャンネルを作成する際に **format** 句を利用して、バックアップファイルの出力先を明示的に指定します。

```
RMAN> RUN{
  2> allocate channel c1 device type disk format '/mnt/fs1/file_%U';
  3> allocate channel c2 device type disk format '/mnt/fs1/file_%U';
  4> allocate channel c3 device type disk format '/mnt/fs2/file_%U';
  5> allocate channel c4 device type disk format '/mnt/fs2/file_%U';
  6> allocate channel c5 device type disk format '/mnt/fs3/file_%U';
  7> allocate channel c6 device type disk format '/mnt/fs3/file_%U';
  8> allocate channel c7 device type disk format '/mnt/fs4/file_%U';
  9> allocate channel c8 device type disk format '/mnt/fs4/file_%U';
 10> backup section size 25G database;
 11> release channel c1;
 12> release channel c2;
 13> release channel c3;
 14> release channel c4;
 15> release channel c5;
 16> release channel c6;
 17> release channel c7;
 18> release channel c8;
 19> }
```

リストアの場合の手動構成設定例を示します。リストアの場合、各バックアップファイルがどのパスに保存されているかは **RMAN** のカタログ情報から自動把握できるので、**format** 句で明示的に示す必要はありません。

```
RMAN> RUN{
  2> allocate channel c1 device type disk;
  3> allocate channel c2 device type disk;
  4> allocate channel c3 device type disk;
  5> allocate channel c4 device type disk;
  6> allocate channel c5 device type disk;
  7> allocate channel c6 device type disk;
  8> allocate channel c7 device type disk;
  9> allocate channel c8 device type disk;
 10> restore database;
 11> recover database;
 12> release channel c1;
 13> release channel c2;
 14> release channel c3;
 15> release channel c4;
 16> release channel c5;
 17> release channel c6;
 18> release channel c7;
 19> release channel c8;
 20> }
```

また、多重実行を効果的に動作させるために、「**2-3 RMAN** バックアップファイル分割について」もあわせてご確認ください。

RMAN の多重度について、詳細は **Oracle** 社発行のドキュメントを参照してください。

2-3 RMANバックアップファイルの分割について

バックアップ・セット方式によるRMANバックアップでは、バックアップ文中で“section size”のパラメータを用いてバックアップファイルを任意のサイズに分割することができます。

バックアップを多重実行する場合、多重度数分のチャンネルを使用し転送経路を分散することが転送性能の向上に有効なため、バックアップ・セット方式では、バックアップファイルを分割し、各チャンネルに割り振る運用を推奨します。

なお、イメージ・コピー方式では、データファイルをそのままの形でコピーするという特性上、バックアップファイルを分割することはできません。データファイル数が必要な多重度を満たさない場合は、バックアップファイルを分割できるバックアップ・セット方式を利用することを推奨します。

以下に“section size”の設定例を示します。

```
> backup section size 25G database;
```

バックアップの多重実行については、「2-2 RMANの実行多重度について」もあわせてご確認ください。

2-4 10GbEネットワークを利用する場合のバッファチューニング

10GbEネットワークを利用する場合、広帯域を効率的に利用するために、I/Oバッファのチューニングが有効です。Oracle Databaseでは以下の初期化パラメータを推奨します。

```
_backup_disk_bufcnt=64  
_backup_file_bufcnt=64  
_backup_disk_bufsz=1048576  
_backup_file_bufsz=1048576
```

以下に、SQLPlusでの設定例を示します。

```
SQL> alter system set "_backup_disk_bufcnt"=64 scope=memory;  
SQL> alter system set "_backup_file_bufcnt"=64 scope=memory;  
SQL> alter system set "_backup_disk_bufsz"=1048576 scope=memory;  
SQL> alter system set "_backup_file_bufsz"=1048576 scope=memory;
```

パラメータの詳細についてはOracle社発行のドキュメントを参照してください。

3. ネットワークの構成

3-1 バックアップ専用ネットワーク

iStorage HSに対してより高速なバックアップ/リストアを行うには、専用のネットワークの利用を推奨します。ネットワークを専用とすることで、バックアップ/リストア用の帯域幅が他の通信により減少することを防ぐことができます。

3-2 10GbE ネットワーク

大容量のデータベースを短時間で効率的にバックアップする必要がある場合、標準の1GbE ネットワークよりも広帯域な10GbEネットワークの利用を検討してください。

3-3 ネットワークのセグメント

複数のチャネルを使用する場合、単一のネットワークセグメントに流すよりも、複数のネットワークセグメントに流した方がNFSの応答速度が速くなるため、バックアップ・リストアの転送速度が向上します。そのため、複数のネットワークセグメントを利用することを強く推奨します。タグVLANを利用すると、1つの物理インタフェースに複数のセグメントのIPアドレスを持たせることができます。

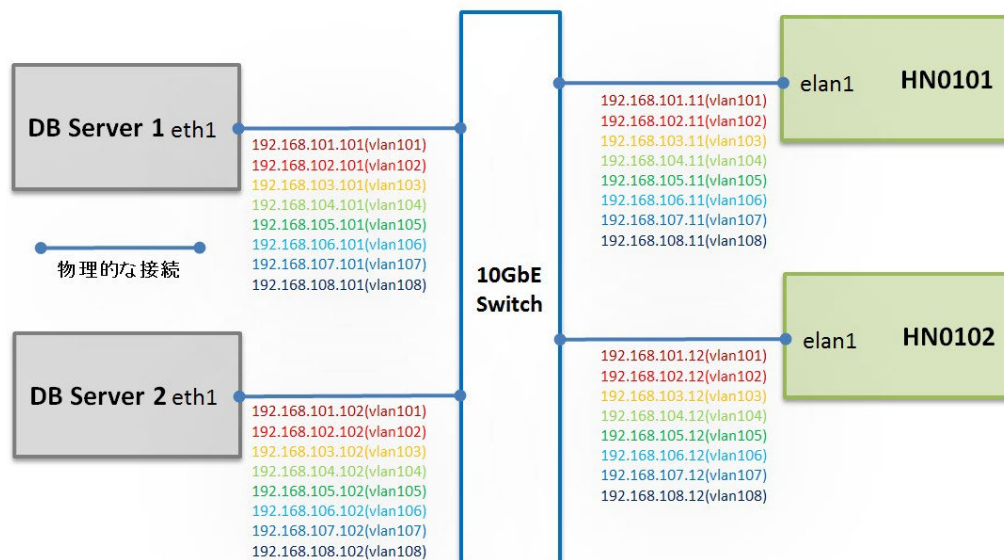
タグ VLANの設定は iStorage HSのCLI から行えます。

例：HN0101のelan1にvlan id 101のIPアドレスを設定する場合

```
# vlan set node=HN0101 id=101 port=elan1 address=192.168.101.11 mask=255.255.255.0
```

CLIによるタグVLANの設定方法の詳細については「iStorage HSシリーズ コマンドリファレンス」を参照してください。

以下に8つのネットワークセグメントを利用する場合のネットワーク構成例を示します。



4. Exadata 運用時の注意事項

4-1 RMANバックアップのバイナリ圧縮の非推奨

RMANでは、BACKUPコマンドで"AS COMPRESSED BACKUP"を指定するとバックアップ・セットのバイナリ圧縮を実施できますが、この機能の利用は推奨しません。iStorage HSではバックアップ時に重複排除とバイナリ圧縮を行っています。データのバイナリ圧縮は iStorage HS内で実行しているため、ストレージ容量の削減を目的とする場合はRMANで実行する必要はありません。RMANによるバイナリ圧縮は iStorage HSの重複排除の効率を下げる可能性があります。

4-2 HN/AN間のファイルシステムのエクスポート先変更

RMANで保存先としたファイルシステムを異なるHNあるいはANへ移動した場合、移動先のノードに応じてファイルシステムのネットワークパスが変更されるため、データベースサーバのNFSマウントパスを変更する必要があります。

iStorage HSのANクラスタ機能により、ファイルシステムが異なるHN/ANへ移動(フェイルオーバー)した場合、バックアップ先のパスは変更されません。AN クラスタ機能について詳しくは、「iStorage HS シリーズ ユーザーズガイド」を参照してください。

4-3 NFSのアクセス許可ポート設定(Oracle Direct NFS利用時のみ)

Oracle Direct NFSを利用する場合、iStorage HSNFSファイルシステムを1024番以上のポートからアクセスできるように設定する必要があります。アクセス許可ポートの設定は iStorage HS のGUI/CLIから行えます。GUIから設定する場合は、ファイルシステムの作成/変更時に「その他の オプション」の「1024番以上のポートからのアクセスを拒否する。(secure)」のチェックボックスを外してください。

5. トラブルシューティングについて

Exadata固有の問題が発生した場合は、Exadataのログを収集し、ご購入元へ確認を行ってください。ログの収集手順はOracle社発行のマニュアルを参照してください。

iStorage HSで問題が発生した場合は、イベントを確認し、「iStorage HSシリーズ メッセージハンドブック」を参照して適切な対処を行ってください。iStorage HSでは、メール通報、SNMPトラップ、イベントビューアといった3つの方法を利用してイベントを受信できます。それぞれの設定方法については、「iStorage HSシリーズ ユーザーズガイド」を参照してください。

Spectrum Protect

1. iStorage HSの設定

1-1 ファイルシステムの設定

iStorage HSのファイルシステム容量のデフォルトサイズは256PBですが、使用するSpectrum Protectのバージョンによっては、表示コマンドの結果などが不正になる場合があります。

例：Tivoli Storage Manager 5.5(on AIX5.3)では、ファイルシステム容量を32Tバイト以上に設定すると、バックアップ実行後にQuery STGPOOLコマンドで、STGPOOLが表示されません。バックアップ自体は成功します。

これを回避するには、iStorage HSでファイルシステムを作成する際に、以下の画面を参照してサイズを小さく設定してください。

なお、Spectrum Protectで利用可能なファイルシステム容量については、Spectrum Protectの購入元にご確認ください。

The screenshot shows the 'File System Creation' dialog box. The 'File System Options' section includes fields for 'File System Name' (fs1), 'Node' (AN 01 01), 'Export Type' (NFS), and 'Capacity' (256 PB). The 'Capacity' field is highlighted with a red box. Below this, there are checkboxes for 'Hard Quota' and 'Soft Quota', and a 'Soft Limit' field set to 90%. The 'Parity Count' is set to 3. The 'Export Options' section includes fields for 'Export Name' (/export/fs1), 'Access Type' (Read/Write), and 'User Access' (All users as anonymous user (all_squash)).

図 2: ファイルシステム容量変更方法

1-2 マーカーフィルタリングの設定

iStorage HSの重複排除機能を最適化するために、マーカーフィルタリング機能を有効にしてください。Spectrum Protectでのデータ保存時の重複排除機能を最適化するオプションとして、マーカーフィルタリングオプション(マーカータイプTSM1)を用意しており、ファイルシステム毎に適用します。

iStorage HSでマーカーフィルタリングオプションを使用する場合は、ファイルシステムの作成時にマーカーフィルタリングオプションを有効に設定し、マーカータイプは「TSM1(IBM Spectrum Protector)」を選択します。

The screenshot shows the 'File System Creation' dialog box. The 'Advanced Options' section is expanded. The 'Marker Filtering' option is checked and set to 'TSM1(IBM Spectrum Protect)'. Other options include 'Failover' (set to '-'), 'WORM' (set to 'Invalid (WORM license not found)'), 'ACL' (unchecked), 'File Information' (unchecked), 'Encryption' (unchecked), and 'Encryption Key' (set to '-'). A warning message at the bottom states: 'Failover is only available when Failover setting is enabled.' The 'OK' and 'Cancel' buttons are at the bottom right.

図 3: マーカーフィルタリング設定方法

マーカーフィルタリングオプションを使用する場合の注意事項を以下に列挙します。各機能についての説明は「iStorage HSシリーズ ユーザーズガイド」を参照してください。

- ファイルシステムの作成後は、マーカーフィルタリングの設定を変更することはできません。
- レプリケーションセットのマスタとレプリカでは、同じマーカーフィルタリングとマーカータイプを持っている必要があります。
- マーカーフィルタリングが有効となっているファイルシステムがレプリケーションの対象となっている場合、初回のレプリケーションが終了するまで、レプリカのファイルシステムはエクスポートできません。

- Spectrum Protectのバックアップサーバ(Spectrum Protect Serverをインストールしたサーバ) には4GB以上のメモリを搭載してください。メモリ量が少ない場合、バックアップの性能低下や重複排除率の低下を引き起こす可能性があります。

2. Spectrum Protect の設定

2-1 iStorage HS をストレージとして設定

iStorage HSのファイルシステムをSpectrum Protectのバックアップデータの格納先ストレージとしてください。Spectrum Protectのディスクベースのストレージに対して有効なチューニング項目はiStorage HSに対しても有効です。

2-2 デバイスファイルについての設定方法

iStorage HSのファイルシステムをバックアップ先に指定する場合は、**devclass**と**stgpool**を作成する必要があります。**devtype**が**file**の**devclass**に**stgpool**を作成し、**dataformat**として**nonblock**を指定します。

1) devtypeがfileのdevclassを作成する方法

マウントポイントを/hydra/001として作成する例を以下に記します。

1-1) iStorage HSのファイルシステムを作成してマウントします。

1-2) Spectrum Protectサーバのdsmadmcで管理コマンドモードを開始します。

1-3) defineコマンドでdevclassを001として作成します。使用するファイルシステムの容量をmaxcapacityパラメータに指定します。

RHELをご利用される場合は「2-3 RHELのmaxcapacityパラメータとバックアップ性能」も参照してください。

```
>define devclass 001 devtype=file directory=/hydra/001 maxcapacity=64g
```

2) stgpoolを作成する方法

作成したdevclassを基にstgpool を00001として作成する例を以下に記します。

2-1) Spectrum Protectサーバのdsmadmcで管理コマンドモードを開始します。

2-2) defineコマンドでstgpoolを00001として作成します。

```
>define stgpool 00001 001 dataformat=nonblock maxscratch=99999
```

2-3 RHELのmaxcapacityパラメータとバックアップ性能

Spectrum ProtectがiStorage HSシリーズに生成するバックアップイメージファイルは、Spectrum Protectサーバの装置クラスを定義するときに指定するmaxcapacityパラメータの値ごとに分割されて格納されます。バックアップする容量に合わせてmaxcapacityの値を大きくすることでバックアップイメージファイルを分割しないようにすることもできます。ただし、RHELにおいては、バックアップイメージファイルのサイズが大きくなると、バックアップ性能が著しく悪くなるという傾向があります。このため、RHELでSpectrum Protectをご利用される場合、maxcapacityパラメータの値を大きくせず、既定値の2GBのままご利用されることを推奨します。

2-4 Spectrum Protectの圧縮/暗号化機能について

Spectrum Protectの設定において、圧縮機能を無効にしてください。iStorage HSではバックアップ時に重複排除と物理データ圧縮を行っています。データの物理圧縮はiStorage HS内で実行しているため、Spectrum Protectで実行する必要はありません。また、Spectrum Protectによる圧縮はバックアップサーバ上で実行されるため、性能に影響を与えることがあります。

Spectrum Protectの設定において、暗号化機能を無効にしてください。暗号化機能を無効にすることでiStorage HSでより効果的に重複排除を行うことができます。

2-5 サーバオプション、クライアントオプションの設定

バックアップの性能を向上するため、以下のサーバオプション、クライアントオプションを設定してください。

Set TXNGroupmax to 65000
Set DIRECTIO to NO
Set Diskbuffsize to 256 or more
Set Txnbytelimit to 2G

Spectrum Protectサーバオプションはコンソールもしくはdsmserv.optファイルで設定可能です。

Set TXNGroupmax to 65000
Set DIRECTIO to NO

Spectrum Protectクライアントオプションは、Windowsではdsm.opt、他のOSではdsm.sysファイルで設定可能です。

Set Diskbuffsize to 256 or more
Set Txnbytelimit to 2G

設定を有効化するためにSpectrum Protectのサーバを再起動してください。

また、上記以外にもResource utilizationオプションの設定を変更し並列セッション数を調整することでも性能の向上が見込めます。
詳しくは IBM 社から提供されているSpectrum Protectのマニュアルを参照してください。

3. バックアップサーバの設定

iStorage HS に対してより高速なバックアップ/リストアを行うには、Spectrum Protectがインストールされているバックアップサーバの設定変更が必要になります。
バックアップサーバの設定については「付録C オペレーティングシステムの設定」を参照してください。

4. ネットワークの構成

iStorage HSに対してより高速なバックアップ/リストアを行うには、専用のネットワークの利用を推奨します。ネットワークを専用とすることで、バックアップ/リストア用の帯域幅が他の通信により減少することを防ぐことができます。

iStorage HSご利用時のネットワークの構成については「第2章 配備計画 Step 2. ネットワークの計画」を参照してください。

5. Spectrum Protect 運用時の注意事項

5-1 小さなサイズのファイルのバックアップ

Spectrum Protectを用いてiStorage HSへのバックアップ処理を行う際、バックアップするデータに数十 KB未満の小さなファイルが多く含まれていると、iStorage HSの重複排除率は低くなります。これは、Spectrum Protect が各バックアップ対象ファイルのヘッダ部に管理情報(マーカー)を付加することに起因します。

iStorage HSではブロックレベルで重複データを検出し、重複しないユニークなデータのみを圧縮・格納することによって効率的なストレージ格納容量を実現します。(DataRedux®) Spectrum Protect の管理情報はバックアップ対象ファイルごとに付加されます。そのため、iStorage HSがバックアップデータをブロックレベルに分割する際に、バックアップデータに数十KB 未満の小さなファイルが含まれていると、分割されたバックアップデータの個々のブロックの多くにSpectrum Protectによって付加された管理情報が含まれることになります。この付加された管理情報にはバックアップ時刻等が含まれるため、バックアップごとにユニークになります。そのため、管理情報が含まれたブロックは前回バックアップ時と比べて重複しないユニークなデータとみなされ、排除されずに iStorage HSへ格納されます。これによって iStorage HSの重複排除率は低くなります。

この現象は、マーカーフィルタリングオプションを使用しても回避することはできませんので、特に小さなファイルを大量にバックアップする際は注意してください。

5-2 ファイルサイズが性能に与える影響

Spectrum Protectを用いて iStorage HSへのバックアップ処理を行う際、バックアップするファイルサイズが小さいほど性能が低くなる傾向があります。

バックアップするデータのファイルサイズによって性能に差がでるため、バックアップ時間の見積もり等を行う際は注意してください。

5-3 Tivoli Storage Manager 5.3におけるdevclassの利用容量

devclassの利用容量を、引数“MAXCAPACITY”で定義する場合に制限があります。
Tivoli Storage Manager 5.3ではdevtypeがfileのdevclassを作成する場合に以下の容量が最大値となります。

- AIX and Linux 64GB
- HPUX 128GB
- Solaris 1TB
- RHEL 2GB

この制限はTivoli Storage Manager 5.3の仕様です。詳細については、Tivoli Storage Manager購入元にご確認ください。

なお、devclassはファイルシステム内に複数作成できるため、iStorage HSのファイルシステム容量を上記数値に制限する必要はありません。

5-4 HN/AN間のファイルシステムのエクスポート先変更

Spectrum Protectでバックアップ先として指定したファイルシステムを異なるHN/ANへ移動する場合、移動先のHN/ANに応じてファイルシステムのネットワークパスが変更されます(*1)。

NFS経由でバックアップを行っている場合、バックアップ済みのデータをリストアするためにはNFSマウント先アドレスを変更することでリストアが可能になります。設定方法を以下に示します。

(*1) iStorage HSのANクラスタ機能により、ファイルシステムが異なるHN/ANへ移動(フェイルオーバー)した場合、バックアップ先のパスは変更されません。AN クラスタ機能について詳しくは、「iStorage HSシリーズ ユーザーズガイド」を参照してください。

設定方法

NFSのマウント先ディレクトリを変更することで、ファイルシステムが移動する前にバックアップされていたデータのリストアを可能にします。また、ファイルシステム移動後のバックアップを可能にします。

なお、この手順はLinux/UNIX系サーバ(NFS)に対して有効です。

- 1) NFSファイルシステムのアンマウントを行います。
- 2) iStorage HSのファイルシステムを移動させます。
- 3) NFSのマウント先アドレスを変更して再度NFSマウントを行います。

5-5 ANクラスタ

デフォルト設定でSpectrum Protectを使用する際、バックアップ・リストアでフェイルオーバーが発生した場合は、バックアップ・リストアも自動的にプロセスを続行します。

AN クラスタ機能について詳しくは、「iStorage HSシリーズ ユーザーズガイド」を参照してください。

6. トラブルシューティングについて

バックアップソフトウェア固有の問題が発生した場合は、バックアップソフトウェアのログを収集しSpectrum Protectのご購入元へ確認を行ってください。ログの収集手順はお使いのSpectrumProtectのマニュアルを参照してください。

iStorage HSで問題が発生した場合は、イベントを確認し、「iStorage HSシリーズ メッセージハンドブック」を参照して適切な対処を行ってください。iStorage HSでは、メール通報、SNMPインタフェース、イベントビューアといった3つの方法を利用してイベントを受信できます。それぞれの設定方法については、「iStorage HSシリーズ ユーザーズガイド」を参照してください。

Veritas System Recovery

1. iStorage HSの設定

iStorage HSをVeritas System Recoveryとの組み合わせでお使いいただく場合、iStorage HSで必要となる特別な設定はありません。

2. Veritas System Recoveryの設定

iStorage HSのファイルシステムをVeritas System Recoveryのバックアップデータの格納先ディスクへのバックアップフォルダとしてください。Veritas System Recoveryのディスクベースのストレージに対して有効なチューニング項目はiStorage HSに対しても有効です。

2-1 重複排除オプション

iStorage HSによる重複排除機能をより効果的にご利用いただくため、Veritas System Recoveryによる重複排除機能を使用しないことを推奨します。
iStorage HSにて重複排除や圧縮を行うため、Veritas System Recoveryによる重複排除は不要です。

2-2 Veritas System Recovery暗号化機能

iStorage HSによる重複排除をより効果的に利用いただくため、Veritas System Recoveryの暗号化機能は使用しないでください。

3. バックアップサーバの設定

iStorage HSに対してより高速なバックアップ/リストアを行うには、Veritas System Recoveryがインストールされているバックアップサーバの設定変更が必要になります。
バックアップサーバの設定については「付録C オペレーティングシステムの設定」を参照してください。

4. ネットワークの構成

iStorage HSに対してより高速なバックアップ/リストアを行うには、専用のネットワークの利用を推奨します。ネットワークを専用とすることで、バックアップ/リストア用の帯域幅が他の通信により減少することを防ぐことができます。
iStorage HSご利用時のネットワークの構成については「第2章 配備計画 Step 2. ネットワークの計画」を参照してください。

5. Veritas System Recovery運用時の注意事項

5-1 小さなサイズのファイルのバックアップ

バックアップ対象のファイルが小さい場合、多くのバックアップイメージが生成される“ファイルとフォルダのバックアップ”は“ドライブベースのバックアップ”に比べて、性能が低下します。小さなサイズのファイルが多い場合は、“ドライブベースのバックアップ”を行ってください。

5-2 HN/AN 間のファイルシステムのエクスポート先の変更

Veritas System Recoveryでバックアップ先として指定したファイルシステムのエクスポート先を異なるHN/ANに変更する場合、変更先のHN/ANに応じてファイルシステム(リカバリポイント)のネットワークパスが変更されます(*1)。

そのためiStorage HSへのバックアップはリカバリポイントの選択が可能な“ドライブベースのバックアップ”を推奨します。

(*1) iStorage HSのAN クラスタ機能により、ファイルシステムが異なるANへ移動(フェイルオーバー)した場合、バックアップ先のパスは変更されません。ANクラスタ機能について詳しくは、「iStorage HSシリーズ ユーザーズガイド」を参照してください。

6. トラブルシューティングについて

バックアップソフトウェア固有の問題が発生した場合は、バックアップソフトウェアのログを収集しVeritas System Recoveryのご購入元へ確認を行ってください。ログの収集手順はお使いのVeritas System Recoveryのマニュアルを参照してください。

iStorage HSで問題が発生した場合は、イベントを確認し、「iStorage HSシリーズ メッセージハンドブック」を参照して適切な対処を行ってください。iStorage HSでは、メール通報、SNMPインタフェース、イベントビューアといった3つの方法を利用してイベントを受信できます。それぞれの設定方法については、「iStorage HSシリーズ ユーザーズガイド」を参照してください。

iStorage HS3/HS8 シリーズ
iStorage HS Virtual Appliance
構成設計の手引

I H 2 4 0 4 - 1 - B
2 0 2 6 年 9 月 初 版

日 本 電 気 株 式 会 社
東京都港区芝五丁目 7 番 1 号
TEL(03)3454-1111 (大代表)

©NEC Corporation 2026

日本電気株式会社の許可なく複製・改変などを行うことはできません。
本書の内容に関しては将来予告なしに変更することがあります。