

Hitachi Content Platform

運用ガイド

ガイドをよく読み、保管してください。

この装置をご使用になる前に、このガイドに書いてある安全上の指示をよくお読みください。本文中の注意事項を必ずお守りください。

このガイドをいつでも参照できるように、手近なところに保管してください。

対象製品

Hitachi Content Platform

5.0.2-01 以降

輸出時の注意

本製品を輸出される場合には、外国為替及び外国貿易法の規制並びに米国輸出管理規則など外国の輸出関連法規をご確認の上、必要な手続きをお取りください。

なお、不明な場合は、弊社担当営業にお問い合わせください。

商標類

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

ActiveX は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。

Firefox は Mozilla Foundation の登録商標です。

Internet Explorer は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。

Microsoft は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。

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

VeriSign は、VeriSign, Inc.の米国およびその他の国での登録商標です。

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

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

イーサネットは、富士ゼロックス株式会社の登録商標です。

その他記載の会社名、および商品名は各社の商標、または登録商標です。

装置の保証について

装置の動作について無償で保証する期間は、お買い求めになった日から 3 年です。

二重化されている部位の一点故障の場合でもそれが重大事故につながる恐れがある場合、装置は停止することがあります。

規制・対策などについて

次の項目については、「はじめに」の「関連マニュアル」に記載しているハードウェアのマニュアルをご参照ください。

- ・高調波電流規制について
- ・電波障害防止について
- ・システム装置の廃棄について
- ・設置場所の環境条件について

バックアップについて

HCP, HVFP, HVFP のクライアント、ストレージ自身のハードウェアまたはソフトウェアの不慮の事故によって、お客様の大切なデータが失われても弊社では保証できません。

そのような場合にデータの回復ができるよう、お客様自身で全データをバックアップしておいてください。データの被害を最小限に抑えることとなります。

ご注意

・HCP および HVFP を使用するために必ずこのガイドを読み、操作手順と指示事項をよく理解してから操作してください。特に「安全に関する共通的な注意事項」および「装置をご使用になる際の注意」の説明については内容を十分に理解して、このガイドの指示に従ってください。

・このガイドの内容については将来予告なしに変更することがあります。

・本装置がお客様によって不適当に使用されたり、このガイドの内容に従わないで取り扱われたり、修理・変更されたことなどに起因して生じた損害などにつきましては、責任を負いかねますのでご了承ください。

・このガイドの著作権は株式会社日立製作所にあります。このガイドのすべて、または一部分を書面による了解無しに転載、または複製することはできません。

安全に取り扱うために

安全に関する注意事項は、次に示す見出しによって表示されます。これは安全注意シンボルと「危険」、「警告」、および「注意」という見出し語を組み合わせたものです。



これは安全注意シンボルです。人への危害を引き起こす潜在的な危険に注意を喚起するために用いられます。起こりうる傷害、または死を回避するためにこのシンボルのあとに続く安全に関するメッセージに従ってください。



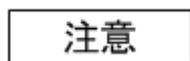
これは死亡、または重大な傷害を引き起こす可能性が高い、差し迫った危険の存在を示すのに用いられます。



これは死亡、または重大な傷害を引き起こすかもしれない潜在的な危険の存在を示すのに用いられます。



これは軽度の傷害、あるいは中程度の傷害を引き起こすおそれのある潜在的な危険の存在を示すのに用いられます。



これは装置の重大な損傷、または周囲の財物の損害をひき起こすおそれのある潜在的な危険の存在を示すのに用いられます。



これは、人身の安全や装置の損害に関係しない補足説明であることを示すのに用いられます。

安全に関する共通的な注意事項

装置をご使用になる際、お客様がケガなどをされないために、次のことを守ってください。内容をよく読んで、十分理解してください。

- ・操作は、このガイドに記載してある指示、手順に従ってください。
- ・装置に貼られているラベルに記載してある注意事項を必ず守ってください。
- ・このガイドに記載してある注意事項を必ず守ってください。
- ・このガイドに記載してある注意事項は、十分に検討されたものですが、予測を超えた事態が起こることが考えられます。操作の際は、このガイドに記載してある指示に従うだけでなく、お客様自身でもケガなどしないよう十分に注意してください。
- ・お客様が修理や改造、分解を行わないでください。通電部に触れて感電する、高温になる部品に触れてやけどをするなどの原因になります。また、装置を故障させる原因になります。
- ・この装置は、危険なレーザー光を出さない「クラス1のレーザーシステム」です。このガイドに従って操作してください。このガイドに書かれた以外の操作はしないでください。思わぬ故障や事故を起こす原因になります。

装置をご使用になる際の注意

- ・本製品には、同梱された電源コードセットを使用してください。また、同梱された電源コードセットはほかの製品には使用しないでください。故障や事故を起こす原因になります。
- ・異臭、異常な発熱、発煙などに気づかれたときは、装置への給電を遮断して保守員に連絡してください。そのまま放置すると、感電や火災の原因になります。
- ・落下させたり、ぶつけたりして装置に衝撃を与えないでください。感電や火災の原因になります。
- ・装置の上に乗って踏み台にするなど、目的以外の用途に使用しないでください。装置が倒れるなどして、ケガの原因になります。
- ・装置に重いものを載せないでください。落下によるケガの原因になります。また、装置が正常に動作しないことがあります。
- ・水の入った容器や虫ピン、クリップなどの小さな金属物を装置上に置かないでください。内部に入った場合、そのまま使用すると感電や発煙、発火の原因になります。

- ・テレビやラジオを近づけないでください。テレビやラジオなどを隣接して設置した場合、お互いに悪影響を及ぼすことがあります。テレビやラジオに雑音が入った場合は、装置とできるだけ離す、テレビやラジオのアンテナの向きを変えるなどの対処をしてください。
- ・ケーブルは、足などを引っかけないように配線してください。ケーブルに足を引っかけて転倒するなど、ケガの原因になります。
- ・ケーブルの上に重いものを載せないでください。また、熱を発生する器具などの近くに置かないでください。ケーブルの被膜が破れて、感電や火災の原因になります。
- ・湿気やほこりの多い場所では使用しないでください。電気絶縁の低下によって感電や火災の原因になります。
- ・硫化水素の発生するところや、塩分の多いところに置かないでください。温泉地など、硫化水素の発生するところや、海岸などの塩分の多いところでお使いになると本装置の寿命が短くなるおそれがあります。
- ・電源プラグに、ほこりが付いていないことを確認して、根元までしっかりと差し込んでください。プラグにほこりが付いていると火災の原因になるので、取り除いてください。
- ・装置前面の通気口から空気を取り込んで、背面の通気口から排気することで、装置内部の温度上昇を防いでいます。通気口の前に物を置いたり、立てかけたりしてふさいでしまうと、装置内部の温度が上昇し、感電や火災の原因になります。また、通気口にほこりなどが詰まっている場合は、取り除いてください。
- ・通気口から装置内にクリップなどの金属類や、紙などの燃えやすいものを入れないでください。感電や火災の原因になります。
- ・管理 LAN スイッチの ACC LED 点灯中は電源を切断しないでください。管理 LAN スイッチ正面にある ACC LED 点灯中はメモ리카ードにアクセス中です。アクセス中は、電源を切断しないでください。メモ리카ードを破損するおそれがあります。
- ・装置に故障が発生したときには、お客様がケガなどをされないために、このガイドに従って対処してください。このガイドに記載のない異常が発生した場合は、保守員に連絡してください。

感電事故を防ぐための注意

- ・装置の設置場所に感電事故の要因となり得るもの、例えば不完全な接地線や濡れた床などがいないか確認してください。
- ・非常時のために、非常用の電源切断スイッチの場所と操作方法を確認しておいてください。
- ・特別の指示がないかぎり、作業を始める前に装置への供給電源をすべて遮断してください。装置の電源スイッチを切断するだけでなく、分電盤のスイッチを切断するか、電源コードを抜いてください。分電盤のスイッチを切断した場合は、そこに「このスイッチを入れないこと」という貼り紙をしてください。

電源にロックアウト装置がある場合は電源切断後、鍵を掛けキーを持ってください。作業を引き継いだ場合などは、推測で電源断になっていると判断しないでください。スイッチの状態などで確認し、状況によっては計器でチェックしてください。

通知：ロックアウト装置(lockout device)は、作業等に際し、分電盤などのスイッチ(energy isolating device)を切断したあと、別の人が誤って電源を入れないように分電盤等を施錠等する装置であり、米国 OSHA(Occupational Safety & Health Administration U.S. Department of Labor) Regulations の 29 CFR 1910.147 “The control of hazardous energy(lockout/tagout)” で、次のように記載されています。

Lockout device. A device that utilizes a positive means such as a lock, either key or combination type, to hold an energy isolating device in a safe position and prevent the energizing of a machine or equipment. Included are blank flanges and bolted slip blinds.

Energy isolating device. A mechanical device that physically prevents the transmission or release of energy, including but not limited to the following: A manually operated electrical circuit breaker; a disconnect switch, a manually operated switch by which the conductors of a circuit can be disconnected from all ungrounded supply conductors, and, in addition, no pole can be operated independently; a line valve; a block; and any similar device used to block or isolate energy. Push buttons, selector switches and other control circuit type devices are not energy isolating devices.

- ・装置への給電を遮断しても、装置内には一定時間電気が残っている部分があります。感電を防ぐために、このガイドで指示している以外の個所には触れないでください。
- ・接地端子付きの装置を取り扱う場合は、接地線が接続されていることを確認してください。
- ・活電部分の近くで作業する場合は電源をいつでも遮断できるよう、別の人がそばで待機するようにしてください。

回転部や、可動部への巻き込みを防ぐための注意

- ・回転部や可動部のそばに寄る場合は巻き込まれるのを防ぐため、ネクタイやスカーフはたれ下がったままにしないでください。また、シャツの裾ははみ出さないようにきちんと留めてください。
- ・長い髪は結んでください。
- ・特別の指示がないかぎり、回転部や可動部のカバーを取り外した状態で通電しないでください。

非常時の処置

感電事故の発生

- ・あわてないこと。感電した人に触れて第2の被害者にならないようにしてください。
- ・まず被害者への電流源を遮断してください。非常用の電源切断スイッチ、またはそれがない場合は、常用の電源スイッチを遮断してください。これができない場合は、乾いた木の棒など非導電性のものを使って、被害者を電流源から引き離してください。
- ・救急車を呼んでください。
- ・被害者が意識不明の場合は、人工呼吸をしてください。このような場合に備えて、人工呼吸のやり方を前もって練習しておいてください。被害者の心臓が停止している場合は心臓マッサージを行う必要がありますが、この処置は訓練を受け、資格のある人以外に行ってはけません。

火災発生の場合

- ・まず、装置への電源を遮断してください。非常用の電源スイッチ、またはそれがない場合は常用の電源スイッチを切断してください。
- ・電源を遮断しても火災が収まらない場合は、状況に応じ、消火作業や消防署への電話などをしてください。

ガイド内の警告表示

このガイドの中に書かれている警告と、その記載個所を次に示します。



と表示されているもの：

この見出しを用いる警告文はありません。



と表示されているもの：

この見出しを用いる警告文はありません。



と表示されているもの：

- ・「B.2.1 装置の外観図」

発行

2012年10月（第3版）K6603796

著作権

(C) 2012, Hitachi, Ltd. All rights reserved.

(C) 2012, Hitachi Data Systems Corporation. All rights reserved.

目次

はじめに.....	15
対象読者.....	16
マニュアルの構成.....	16
マニュアル体系.....	16
関連マニュアル.....	17
このマニュアルでの表記.....	17
このマニュアルで使用する記号.....	17
このマニュアルで使用する構文要素.....	18
KB（キロバイト）などの単位表記について.....	18
カスタマーサービスとサポート.....	18
リモート保守.....	18
1. クライアントの環境を設定する.....	19
1.1 クライアントのマシン要件.....	20
1.2 Internet Explorer の設定.....	21
1.2.1 Internet Explorer を使用する場合の注意事項.....	21
1.2.2 フォントの設定.....	21
1.2.3 キャッシュの設定.....	22
1.2.4 信頼済みサイトゾーンへの URL の登録.....	22
1.2.5 ポップアップブロックの解除.....	23
1.2.6 ダウンロード防止機能の解除.....	23
1.2.7 セキュリティの設定.....	24
1.2.8 アニメーションの再生の設定.....	24
2. システムを構築する.....	25
2.1 HCP システムレベル管理者のユーザアカウントを作成する.....	26
2.1.1 システム管理コンソールの URL.....	26
2.1.2 デフォルトユーザでログインし、パスワードを変更する.....	26
2.1.3 HCP システムレベル管理者のユーザアカウントを作成する.....	27
2.1.4 HCP システムレベル管理者のユーザアカウントを変更する.....	27
2.1.5 システム管理コンソールへのアクセスについて設定する.....	28
2.1.6 HCP 管理 API から HCP システムへのアクセスについて設定する.....	29
2.1.7 デフォルトユーザでログアウトする.....	29
2.2 SSL を設定する.....	29
2.2.1 SSL サーバ証明書情報.....	29
2.2.2 新規証明書の生成とインストール.....	29
2.2.3 作成した証明書のインストール.....	30
2.2.4 CSR の作成と戻された証明書のインストール.....	30
(1) 証明書署名の作成.....	31

(2) HCP が生成した CSR に対して戻された証明書のインストール.....	31
2.2.5 SSL サーバ証明書のプロバイダ.....	32
2.3 SNMP を設定する.....	32
2.3.1 サポートされている標準 MIB ファイル.....	33
2.3.2 MIB の一覧表示.....	33
2.3.3 SNMP の設定.....	34
2.3.4 SNMP 接続のテスト.....	35
2.4 DNS を設定する.....	35
2.4.1 HCP サブドメインに設定するゾーンの種類.....	36
2.4.2 DNS の設定.....	36
(1) HCP サブドメインをスタブゾーンで設定する場合の DNS のセットアップ.....	37
(2) HCP サブドメインをフォワードゾーンで設定する場合の DNS のセットアップ.....	41
(3) Unix での HCP フォワードゾーンの設定.....	45
2.4.3 設定の検証.....	45
2.5 syslog ログ記録を設定する.....	46
2.5.1 syslog サーバに送信されるログメッセージ.....	46
2.5.2 syslog ログ記録の有効化.....	47
2.5.3 syslog 接続のテスト.....	48
2.6 システム管理コンソールでチャージバックレポートを作成する.....	48
2.6.1 チャージバックレポートについて.....	48
2.6.2 チャージバックレポートの作成.....	49
2.6.3 チャージバックレポートの内容.....	50
2.7 システム管理コンソールの警告を確認する.....	52
2.8 ゼロコピーフェイルオーバーを使用する.....	59
2.8.1 ゼロコピーフェイルオーバーとは.....	59
2.8.2 ストレージの設定.....	61
3. テナントおよびネームスペースを管理する.....	65
3.1 テナントを管理する.....	66
3.1.1 テナントを作成する.....	66
3.1.2 テナントレベル管理者のユーザアカウントでログインし、パスワードを変更する.....	67
3.1.3 テナントレベル管理者の情報を設定する.....	67
3.1.4 テナント管理コンソールへのアクセスについて設定する.....	68
3.1.5 HCP 管理 API からテナントへのアクセスについて設定する.....	68
3.1.6 テナントを変更する.....	69
3.1.7 テナントセキュリティ管理者のパスワードをリセットする.....	69
3.2 ネームスペースを管理する.....	70
3.2.1 ネームスペースを作成する.....	70
3.2.2 システム設定情報ファイルの保存先のネームスペースを作成する.....	71
3.2.3 カスタムメタデータの設定を変更する.....	72
3.2.4 HTTP プロトコルを使ったネームスペースへのアクセスについて設定する.....	72
3.2.5 ネームスペースの Quota を変更する.....	73
3.2.6 修復不可能なオブジェクトを削除する.....	73
3.3 テナントのユーザアカウントを設定する.....	74
3.3.1 アップグレード時の注意事項.....	75
(1) テナントのユーザアカウントのマージ.....	75
3.3.2 テナントのユーザアカウントにデータアクセス権限を設定する.....	77
3.3.3 テナントのユーザアカウントを変更する.....	78
3.4 テナント管理コンソールでチャージバックレポートを作成する.....	78
3.4.1 チャージバックレポートについて.....	79
3.4.2 チャージバックレポートの作成.....	79
3.4.3 チャージバック統計値の収集.....	80
3.4.4 チャージバックレポートの内容.....	80
3.5 テナント管理コンソールの警告を確認する.....	82

4. レプリケーション機能を使って運用する.....	85
4.1 システム構成.....	86
4.1.1 レプリケーショントポロジ.....	86
(1) 多対1のレプリケーション.....	87
(2) 双方向レプリケーション.....	87
4.2 レプリケーション機能を使用して運用を開始するまでの流れ.....	87
4.3 レプリケーション機能を使用する場合の事前検討.....	89
4.4 SSL サーバ証明書の公開鍵のインストール.....	93
4.4.1 公開鍵のダウンロード.....	94
4.4.2 公開鍵のアップロード.....	94
4.5 レプリケーション機能を使用する場合のテナントの作成.....	95
4.6 レプリケーション機能を使用する場合のネームスペースの作成.....	95
4.7 レプリケーションリンクを作成する.....	95
4.7.1 レプリケーションリンクを作成するときの考慮点.....	95
4.7.2 レプリケーションリンクの作成.....	96
4.8 レプリケーションリンクの受け入れ要求を承認する.....	97
4.9 レプリケーションリンクの設定を変更する.....	97
4.9.1 リンク設定の変更時の留意事項.....	98
4.9.2 レプリケーションリンクの設定の変更.....	98
4.9.3 レプリケーションリンクのスケジュールの設定.....	99
4.10 レプリケーションを一時停止する.....	100
4.11 レプリカで無効化されたユーザアカウントを再有効化する.....	100
4.12 バックログの確認.....	101
4.12.1 テナントのレプリケーション情報.....	101
4.12.2 テナントのレプリケーションの詳細情報.....	102
4.13 フェイルオーバーとリカバリの管理.....	102
4.13.1 リンクのリストア.....	103
4.13.2 リカバリ.....	103
4.13.3 リカバリ処理中の重複の解決.....	104
4.13.4 フェイルオーバーとリカバリのワークフロー.....	105
(1) プライマリシステム障害のワークフロー.....	105
(2) レプリカ障害のワークフロー.....	106
4.13.5 レプリカへのフェイルオーバー.....	107
4.13.6 障害からのリカバリ.....	107
(1) プライマリシステム障害後のデータリカバリ.....	107
(2) レプリカ障害後のレプリケーション再開.....	108
 付録 A HCP システムの起動と停止.....	 109
A.1 HCP システムを起動する.....	110
A.1.1 ハードウェアの電源を入れる.....	110
A.1.2 ハードウェアの動作状態を確認する.....	110
A.2 HCP システムを停止する.....	112
 付録 B HCP システムで使用するハードウェア.....	 115
B.1 ノード.....	116
B.2 バックエンドスイッチ.....	116
B.2.1 装置の外観図.....	116
(1) 装置の前面.....	117
(2) 装置の正面パネル.....	117
(3) 装置の後面.....	119
B.2.2 バックエンドスイッチの電源の入れ方および切り方.....	119
B.2.3 SNMP サーバおよび NTP サーバとの接続に使用するポート.....	120

B.3 ルーター.....	121
付録 C HCP システムで使用するサービス.....	123
C.1 サービスのデフォルトスケジュール.....	124
C.2 サービスのスケジュール.....	124
C.2.1 サービスに関する情報の表示.....	125
C.2.2 スケジュールを作成する前に.....	125
C.2.3 スケジュールの作成.....	125
C.2.4 スケジュールの変更.....	126
(1) 実行期間の追加.....	126
(2) 実行期間の変更.....	127
(3) 実行期間の削除.....	127
C.2.5 スケジュールのアクティブ設定.....	127
C.2.6 スケジュールの削除.....	127
C.3 保護サービスの実行契機.....	128
付録 D HCP システムログメッセージ.....	129
D.1 システムログメッセージ一覧.....	130
D.2 HCP システムログ.....	148
D.3 HCP 内部ログ.....	148
付録 E テナントログメッセージ.....	151
E.1 テナントログメッセージ一覧.....	152
付録 F 略語一覧.....	159
F.1 このマニュアルで使用している略語.....	160



目次

図 4-1 レプリケーション機能を使用する場合のシステム構成.....	86
図 4-2 運用を開始するまでの流れ.....	88
図 B-1 ノードで使用するポートの配置.....	116
図 B-2 バックエンドスイッチ（装置前面）.....	117
図 B-3 バックエンドスイッチ（装置正面パネル）.....	117
図 B-4 バックエンドスイッチ（ポート番号）.....	119
図 B-5 バックエンドスイッチ（装置後面）.....	119
図 B-6 バックエンドスイッチ（背面の電源スイッチ）.....	120
図 B-7 バックエンドスイッチ（SNMP サーバおよび NTP サーバの LAN 接続ポート）.....	120

表目次

表 1-1 クライアントのマシン要件.....	20
表 1-2 Internet Explorer のフォントの設定.....	21
表 1-3 Internet Explorer のセキュリティの設定.....	24
表 2-1 HCP での使用に適している SSL プロダクト.....	32
表 2-2 HCP ノードに対する完全修飾名とフロントエンドの IP アドレス.....	37
表 2-3 チャージバックレポートの内容.....	50
表 2-4 [Overview] ページの警告.....	52
表 2-5 [Hardware] ページの警告.....	56
表 2-6 [Storage Node] ページの警告.....	57
表 2-7 [Tenants] ページの警告.....	58
表 3-1 アップグレード時のテナントのユーザアカウントとデータアクセスアカウントの扱い.....	75
表 3-2 チャージバックレポートの内容.....	80
表 3-3 テナントの [Overview] ページの警告.....	82
表 3-4 [Namespaces] ページの警告.....	82
表 3-5 ネームスペースの [Overview] パネルの警告.....	83
表 4-1 必要な作業の関連ページ.....	88
表 4-2 事前確認が必要な情報.....	89
表 4-3 設定時にユーザの指定が必要な情報.....	90
表 4-4 レプリケーションステータスを示すアイコン.....	102
表 4-5 レプリケーションペアのプライマリシステムで障害が起こった場合の手順と発生内容.....	105
表 4-6 レプリケーションペアのレプリカで障害が起こった場合の手順と発生内容.....	106
表 B-1 バックエンドスイッチ（正面パネルの LED）.....	117
表 B-2 バックエンドスイッチ（正面パネルのスイッチ）.....	118
表 B-3 バックエンドスイッチ（正面パネルのコネクタ）.....	118
表 B-4 管理コンソールと HCP の間のファイアウォールで例外登録が必要なポート番号.....	121
表 C-1 HCP システムで使用するサービス.....	124
表 C-2 サービスのデフォルト実行スケジュール.....	124
表 D-1 システムログメッセージ.....	130
表 E-1 テナントログメッセージ.....	152



はじめに

このマニュアルは、Hitachi Content Platform (HCP) を運用するために必要な手順について説明しています。

- 対象読者
- マニュアルの構成
- マニュアル体系
- 関連マニュアル
- このマニュアルでの表記
- このマニュアルで使用する記号
- このマニュアルで使用する構文要素
- KB (キロバイト) などの単位表記について
- カスタマーサービスとサポート
- リモート保守

対象読者

このマニュアルは、次のユーザにお読みいただくことを前提としています。

- HCP システムレベル管理者
HCP システム全体に影響するパラメータの管理を行います。
- テナントレベル管理者
HCP システム内にある HCP テナントごとに存在し、その HCP テナントに関する設定の管理を行います。

マニュアルの構成

このマニュアルは、次に示す章と付録から構成されています。

章	内容
1. クライアントの環境を設定する	HCP システムを操作するクライアントの環境設定について説明しています。
2. システムを構築する	HCP システムレベル管理者の権限でシステム管理コンソールを使用して、HCP のシステムを構築する手順について説明しています。
3. テナントおよびネームスペースを作成する	テナントおよびネームスペースを作成する手順のほか、ネームスペースを使用するために必要な設定について説明しています。
4. レプリケーション機能を使って運用する	レプリケーション機能の概要やシステム構成、必要な設定など、HVFP 連携時のレプリケーション機能を使った HCP の運用について説明しています。
A. HCP システムの起動と停止	HCP システムの起動および停止の手順を説明しています。
B. HCP システムで使用するハードウェア	HCP で使用するノード、バックエンドスイッチ、およびルーターについて説明しています。
C. HCP システムで使用するサービス	HCP システムで使用するサービスについて説明しています。
D. HCP システムログメッセージ	システムログに HCP が書き込むメッセージや内部ログについて説明しています。
E. テナントログメッセージ	テナントログに HCP が書き込むメッセージについて説明しています。
略語一覧	このマニュアルで使用している略語を示しています。

マニュアル体系

HCP のマニュアル体系を次に示します。

マニュアル名	内容
Hitachi Content Platform HVFP 連携セットアップガイド	HCP と HVFP を連携して運用を開始するための設定手順および障害発生時の対応について説明しています。HCP と HVFP を連携するために、最初にお読みいただくマニュアルです。
Hitachi Content Platform Hitachi Adapter for Symantec Enterprise Vault ユーザーズガイド	Hitachi Adapter for Symantec Enterprise Vault (HASEV) を使用して、Symantec Enterprise Vault (Enterprise Vault) と HCP を連携した運用を開始するための設定手順について説明しています。HCP と Enterprise Vault を連携するために、最初にお読みいただくマニュアルです。
Hitachi Content Platform 運用ガイド (このマニュアル)	HCP を運用するために必要な手順やメッセージなどについて説明しています。

関連マニュアル

このマニュアルの関連マニュアルを次に示します。必要に応じてお読みください。

HVFP のマニュアル

- Hitachi Virtual File Platform システム構成ガイド
- Hitachi Virtual File Platform セットアップガイド
- Hitachi Virtual File Platform 仮想サーバ環境セットアップガイド
- Hitachi Virtual File Platform ユーザーズガイド
- Hitachi Virtual File Platform トラブルシューティングガイド
- Hitachi Virtual File Platform シングルノード構成セットアップガイド
- Hitachi Virtual File Platform シングルノード構成ユーザーズガイド
- Hitachi Virtual File Platform シングルノード構成トラブルシューティングガイド
- Hitachi Virtual File Platform コマンドリファレンス
- Hitachi Virtual File Platform API リファレンス
- Hitachi Virtual File Platform メッセージリファレンス
- Hitachi Virtual File Platform ファイルアクセス (CIFS/NFS) ユーザーズガイド

ハードウェアマニュアル

- 日立アドバンストサーバユーザーズガイド
HA8000/RS210-h HM/JM/KM (2012年4月～モデル)
HA8000/RS220 AK/BK/FK/HK/JK/KK/LK (2010年4月～モデル)
HA8000-es/RS220 CK/GK/MK/NK (2010年4月～モデル)
- Hitachi Adaptable Modular Storage 2010 ディスクアレイ ユーザーズガイド
- HT-4990-SW320H/SW360H 形 ファイバーチャネルスイッチ ユーザーズガイド/保守要項

このマニュアルでの表記

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

このマニュアルでの表記	製品名称または意味
Device Manager	Hitachi Device Manager Software
HCP	Hitachi Content Platform
HVFP	Hitachi Virtual File Platform
Internet Explorer	Windows(R) Internet Explorer(R)

このマニュアルで使用する記号

このマニュアルでは、次に示す記号を使用しています。

記号	意味
[]	ボタン、キーボードのキーなどを示します。 (例)

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

このマニュアルで使用する構文要素

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

種類	定義
英字	A~Z a~z
数字	0~9
英数字	A~Z a~z 0~9
ASCII 印字可能文字	A~Z a~z 0~9 ! " # \$ % & ' () * + , - . / : ; < = > ? @ [¥] ^ _ ` { } ~

注 すべての半角で指定してください。

KB（キロバイト）などの単位表記について

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

カスタマーサービスとサポート

弊社では、購入後のサポートサービスを提供しています。サポートサービスに関する詳細は、お問い合わせ先まで連絡してください。

リモート保守

HCP のソフトウェアに問題が発生した場合、リモート保守で問題を解決できます。リモート保守では、開発者がインターネット経由でお客様の HCP に接続して、調査および回復作業を実施します。リモート保守の詳細については「Hitachi Content Platform リモート保守適用のお願い」を参照してください。

クライアントの環境を設定する

ここでは、HCP システムを操作するクライアントの環境設定について説明します。

- 1.1 クライアントのマシン要件
- 1.2 Internet Explorer の設定

1.1 クライアントのマシン要件

クライアントに使用するマシンの要件を次に示します。なお、HCP と HVFP を一つのクライアントで操作する場合、HVFP のコンソールとしてのマシン要件も満たしている必要があります。HVFP のコンソールとしてのマシン要件については、HVFP のドキュメントを参照してください。

表 1-1 クライアントのマシン要件

項目	要件
OS	<ul style="list-style-type: none">• Microsoft(R) Windows(R) 7 Enterprise (SP なし, または SP1)• Microsoft(R) Windows(R) 7 Enterprise x64 Edition (SP なし, または SP1)• Microsoft(R) Windows(R) 7 Professional (SP なし, または SP1)• Microsoft(R) Windows(R) 7 Professional x64 Edition (SP なし, または SP1)• Microsoft(R) Windows(R) 7 Ultimate (SP なし, または SP1)• Microsoft(R) Windows(R) 7 Ultimate x64 Edition (SP なし, または SP1)• Microsoft(R) Windows Server(R) 2008 R2, Enterprise Edition[※] (SP なし, または SP2)• Microsoft(R) Windows Server(R) 2008 R2, Enterprise x64 Edition[※] (SP なし, または SP2)• Microsoft(R) Windows Server(R) 2008 R2, Standard Edition[※] (SP なし, または SP2)• Microsoft(R) Windows Server(R) 2008 R2, Standard x64 Edition[※] (SP なし, または SP2)
メモリ	<ul style="list-style-type: none">• 必須: 1GB 以上• 推奨: 2GB 以上 搭載 OS が要求するメモリ容量に準じます。
CPU	クライアントのマシンにインストールする OS の推奨 CPU
モニタの解像度	1,024×768 ピクセル以上
モニタの表示色	16,777,216 色 (True color, 32 ビット) 以上
Web ブラウザ	32 ビット版の次の Web ブラウザを使用できます。 <ul style="list-style-type: none">• Internet Explorer 8.0 (SP なし)• Internet Explorer 9.0 (SP なし)• Firefox 10.0• Firefox 11.0

注※

kb938397 がインストールされている必要があります。



注意 Windows の定期更新プログラムを適用すると、1,024 ビット未満の鍵長での通信ができなくなります。HCP で提供しているデフォルトの SSL 証明書 (512 ビットの鍵長) を使用している場合は、テナント管理コンソールやシステム管理コンソールへのアクセスを継続するため、クライアント側で更新プログラムを適用しないようにしてください。Windows の定期更新プログラムを適用したことでテナント管理コンソールやシステム管理コンソールにアクセスできなくなった場合は次のとおり対処してください。

- クライアントで更新プログラムをアンインストールする
- certutil コマンドで設定を変更する
- HCP で提供しているデフォルトの SSL 証明書ではなく、1,024 ビット以上の SSL 証明書を使用する
- Firefox 10.0 または 11.0 を使用する

Windows の定期更新プログラムや certutil コマンドについては、Windows のドキュメントを参照してください。

1.2 Internet Explorer の設定

ここでは、Internet Explorer の設定について説明します。Web ブラウザの設定を変更する場合は、すべてのブラウザを閉じてから実施してください。なお、示した設定手順は Internet Explorer 8.0 の場合です。使用している Internet Explorer のバージョンが異なっている場合の手順は、Internet Explorer のヘルプを参照してください。

1.2.1 Internet Explorer を使用する場合の注意事項

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

- タブブラウジング機能は使用できません。
次の手順に従って、タブブラウジングを無効にして使用してください。
 - a. Internet Explorer の [ツール] - [インターネット オプション] を選択します。
 - b. [全般] タブ内の [タブ] の [設定] ボタンをクリックします。
 - c. [タブブラウズを有効にする] チェックボックスのチェックを外します。
 - d. [OK] ボタンをクリックします。
- システム管理コンソールおよびテナント管理コンソールの一部のダイアログに証明書エラーと表示されることがあります。
HCP では、ノード、システム管理コンソールおよびテナント管理コンソールの間で https 通信を行うため、証明書エラーと表示されても問題ありません。
- メニューバーの表示有無の設定を変更すると、正しく動作しないことがあります。
- フォントサイズを拡大または縮小すると、GUI 表示が乱れたり、スクロールバーが表示されなくなったりすることがあります。

1.2.2 フォントの設定

表で示したフォントと異なるサイズのフォントを設定している場合、GUI 表示が乱れるおそれがあります。

表 1-2 Internet Explorer のフォントの設定

項目		設定
フォント	[言語セット]	「日本語」
	[Web ページフォント]	「MS P ゴシック」
	[テキスト形式フォント]	「MS ゴシック」
文字サイズ		「中」

フォントと文字サイズの設定方法を次に示します。

フォントの設定

- a. Internet Explorer の [ツール] - [インターネット オプション] を選択します。
- b. [全般] タブを選択します。
- c. [フォント] ボタンをクリックします。
- d. 必要な情報を指定して、[OK] ボタンをクリックします。
- e. [OK] ボタンをクリックして画面を閉じます。

文字サイズの設定

Internet Explorer の [表示] - [文字のサイズ] から選択します。

1.2.3 キャッシュの設定

キャッシュの設定が異なると、システム管理コンソールおよびテナント管理コンソールや、ノード上で動作するプログラムをバージョンアップした場合に、古いバージョンの GUI が表示されたり、GUI がフリーズしたりするおそれがあります。

キャッシュの設定方法を次に示します。

1. Internet Explorer の [ツール] - [インターネット オプション] を選択します。
2. [全般] タブ内の [閲覧の履歴] の [設定] ボタンをクリックします。
3. [Web サイトを表示するたびに確認する] ラジオボタンを選択して、[OK] ボタンをクリックします。
4. [OK] ボタンをクリックして画面を閉じます。

1.2.4 信頼済みサイトゾーンへの URL の登録

Internet Explorer セキュリティ強化の構成機能が有効になっていると、システム管理コンソールおよびテナント管理コンソールの GUI 操作が制限されることがあります。

この場合は、システム管理コンソールおよびテナント管理コンソールの URL を、Internet Explorer でセキュリティゾーンの信頼済みサイトゾーンに登録してください。

信頼済みサイトゾーンに登録する方法を次に示します。

1. Internet Explorer の [ツール] - [インターネット オプション] を選択します。
2. [セキュリティ] タブ内の [信頼済みサイト] を選択した状態で、[サイト] ボタンをクリックします。
3. [このゾーンのサイトにはすべてサーバの確認 (https:) を必要とする] チェックボックスのチェックを外します。
4. [この Web サイトをゾーンに追加する] テキストボックスに、システム管理コンソールおよびテナント管理コンソールの URL を指定して、[追加] ボタンをクリックします。

URL の指定形式を次に示します。

- システム管理コンソールの場合
https://admin.< HCP システムの DNS 名 >:8000
- テナント管理コンソールの場合
https://<テナント名>.< HCP システムのドメイン名 >:8000
<テナント名>は、すべて小文字で入力してください。

また、HCP および HVFP を一つのクライアントで操作する場合、HVFP の管理サーバおよび HVFP で管理しているすべての Physical Node の URL についても指定します。

URL の指定形式を次に示します。

- HVFP の管理サーバの場合
http://< HVFP の管理サーバの IP アドレスまたはホスト名 >
 - HVFP で管理している Physical Node の場合
https://< HVFP で管理している Physical Node の管理ポートの固有 IP アドレス >
https://< HVFP で管理している Physical Node の管理ポートの仮想 IP アドレス >
5. [閉じる] ボタンをクリックします。
 6. [OK] ボタンをクリックして画面を閉じます。

1.2.5 ポップアップブロックの解除

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

ポップアップブロックを解除する方法を次に示します。

1. Internet Explorer の [ツール] - [ポップアップブロック] - [ポップアップブロックの設定] を選択します。
2. [許可する Web サイトのアドレス] テキストボックスに、システム管理コンソールおよびテナント管理コンソールの URL を指定して、[追加] ボタンをクリックします。

URL の指定形式を次に示します。

- システム管理コンソールの場合
`https://admin.< HCP システムの DNS 名 >:8000`
- テナント管理コンソールの場合
`https://<テナント名>.< HCP システムのドメイン名 >:8000`
<テナント名>は、すべて小文字で入力してください。

また、HCP および HVFP を一つのクライアントで操作する場合、HVFP の管理サーバおよび HVFP で管理しているすべての Physical Node の URL についても指定します。

URL の指定形式を次に示します。

- HVFP の管理サーバの場合
`http://< HVFP の管理サーバの IP アドレスまたはホスト名 >`
- HVFP で管理している Physical Node の場合
`https://< HVFP で管理している Physical Node の管理ポートの固有 IP アドレス >`
`https://< HVFP で管理している Physical Node の管理ポートの仮想 IP アドレス >`

3. [閉じる] ボタンをクリックして画面を閉じます。

1.2.6 ダウンロード防止機能の解除

ダウンロード防止機能が有効になっていると、GUI を使用して MIB について定義されたファイルや HCP の内部ログなどをダウンロードできません。

ダウンロード防止機能の解除方法を次に示します。

1. Internet Explorer の [ツール] - [インターネット オプション] を選択します。
2. [セキュリティ] タブ内の [信頼済みサイト] を選択した状態で、[レベルのカスタマイズ] ボタンをクリックします。
3. [ダウンロード] の [ファイルのダウンロード時に自動的にダイアログを表示] で [有効にする] ラジオボタンを選択して、[OK] ボタンをクリックします。
4. [OK] ボタンをクリックして画面を閉じます。

ダウンロード元となる、システム管理コンソールおよびテナント管理コンソールを信頼済みサイトとして登録しておく必要があります。

登録方法については、「[1.2.4 信頼済みサイトゾーンへの URL の登録](#)」を参照してください。

1.2.7 セキュリティの設定

Internet Explorer のセキュリティの設定方法を次に示します。

1. Internet Explorer の [ツール] - [インターネット オプション] を選択します。
2. [セキュリティ] タブ内の [信頼済みサイト] を選択した状態で、[レベルのカスタマイズ] ボタンをクリックします。
3. 次のとおり設定されていることを確認してから、[OK] ボタンをクリックして画面を閉じます。

表 1-3 Internet Explorer のセキュリティの設定

項目	設定値
[ActiveX コントロールとプラグインの実行]	[有効にする]
[スクリプトを実行しても安全だとマークされている ActiveX コントロールのスクリプト実行]	[有効にする]
[アクティブスクリプト]	[有効にする]
[IFRAME のプログラムとファイルの起動]	次のどちらかになっていることを確認します。 <ul style="list-style-type: none">• [ダイアログを表示する]• [有効にする]
[暗号化されていないフォームデータの送信]	次のどちらかになっていることを確認します。 <ul style="list-style-type: none">• [ダイアログを表示する]• [有効にする]

1.2.8 アニメーションの再生の設定

プログレスバーなどのアニメーションを正しく再生するために設定が必要です。

アニメーションの再生の設定方法を次に示します。

1. Internet Explorer の [ツール] - [インターネット オプション] を選択します。
2. [詳細設定] タブを選択します。
3. [マルチメディア] の [Web ページのアニメーションを再生する] チェックボックスをチェックします。
4. [OK] ボタンをクリックして画面を閉じます。

システムを構築する

ここでは、HCP システムレベル管理者の権限でシステム管理コンソールを使用して、HCP のシステムを構築する手順について説明します。

- 2.1 HCP システムレベル管理者のユーザアカウントを作成する
- 2.2 SSL を設定する
- 2.3 SNMP を設定する
- 2.4 DNS を設定する
- 2.5 syslog ログ記録を設定する
- 2.6 システム管理コンソールでチャージバックレポートを作成する
- 2.7 システム管理コンソールの警告を確認する
- 2.8 ゼロコピーフェイルオーバを使用する

2.1 HCP システムレベル管理者のユーザアカウントを作成する

ここで説明する手順は、システム管理コンソールに初めてログインする場合を前提とします。HCP システムレベル管理者のユーザアカウントを作成する作業を次に示します。記載された順に作業を実施してください。

- デフォルトユーザでログインし、パスワードを変更する
- HCP システムレベル管理者のユーザアカウントを作成する
- システム管理コンソールへのアクセスについて設定する
- HCP 管理 API から HCP システムへのアクセスについて設定する
- デフォルトユーザでログアウトする

また、HCP の運用を開始したあとに発生したトラブルへの対応として、HCP システムレベル管理者のユーザアカウントを変更する作業が必要となることがあります。

それぞれの詳細な手順を次に説明します。

2.1.1 システム管理コンソールの URL

システム管理コンソールの URL は次の形式で指定します。

```
https://admin.< HCP システム名 >.< 企業ドメイン名 >:8000
```

HCP のシステム名は、企業ドメイン名と結合され、HCP システムの完全修飾された DNS 名となります。

例えば、HCP システムの完全修飾された DNS 名が「hcp-ma.example.com」の場合は、システム管理コンソールにアクセスするために次の URL を指定します。

```
https://admin.hcp-ma.example.com:8000
```

通常はこの形式の URL を指定してシステム管理コンソールにアクセスしますが、ユーザが特定のノード上でシステム管理コンソールにアクセスする必要がある場合は、ノードの IP アドレスを指定します。

例えば、IP アドレスが 192.168.210.16 のノード上のシステム管理コンソールにアクセスする場合は次の形式で URL を指定します。

```
https://192.168.210.16:8000
```

どちらの形式で URL を指定しても、システム管理コンソールでは HCP システム全体を管理できません。

2.1.2 デフォルトユーザでログインし、パスワードを変更する

初回のログインには、デフォルトユーザのアカウントを使用します。デフォルトユーザでの初回ログイン時には、パスワードの変更を求められるため、その変更手順についても説明します。

1. システム管理コンソールで、次のデフォルトユーザ名とパスワードを指定してログインします。
 - ユーザ名：security
 - パスワード：Chang3Me!パスワードの変更画面が表示されます。
2. 表示された画面で、パスワードの情報を指定します。
次の情報を指定してください。

- [Existing password] フィールドに、現在のデフォルトユーザのパスワードである「Chang3Me!」を指定してください。
 - [New password] フィールドに、新しいデフォルトユーザのパスワードを指定してください。
 - [Confirm new password] フィールドに、新しいデフォルトユーザのパスワードをもう一度指定してください。
3. [Update Password] ボタンをクリックします。
デフォルトユーザのパスワードが変更されます。

2.1.3 HCP システムレベル管理者のユーザアカウントを作成する

HCP システムレベル管理者のユーザアカウントを作成する手順を説明します。

1. システム管理コンソールで、[Security] にマウスカーソルを置くと表示されるメニューから、[Users] を選択します。
[Users] ページが表示されます。
2. [Users] ページで、[Create User Account] をクリックします。
[Create User Account] パネルが表示されます。
3. [Create User Account] パネルで、次の内容を設定します。次の内容以外はデフォルトのままとしてください。
 - [Username] フィールドで、ユーザ名を指定してください。
 - [Full Name] フィールドで、HCP システムレベル管理者の氏名を指定してください。
 - [Authentication] オプションが、[Local] となっていることを確認してください。
 - [Password] フィールドに、ユーザアカウントのパスワードを指定してください。
 - [Confirm Password] フィールドに、ユーザアカウントのパスワードをもう一度指定してください。
 - [Roles] セクションで、次のロールのチェックボックスを選択してください。
[Monitor], [Administrator] , [Security], [Compliance]
 - [Enable account] オプションのチェックボックスが選択されていることを確認してください。
4. [Create User Account] ボタンをクリックします。
指定した情報でユーザアカウントが作成されます。

2.1.4 HCP システムレベル管理者のユーザアカウントを変更する

ユーザアカウントの情報を変更できます。このとき、ユーザアカウントを有効または無効に設定することもできます。ログインしているユーザのアカウントを無効にした直後から、ユーザはすべての操作を実行できなくなります。

メモ：

自分のアカウントを無効にできます。ただし、一度無効にすると、自分では再度有効にできません。

HCP システムレベル管理者のユーザアカウントを変更するには次の手順に従ってください。

1. [Users] ページのユーザアカウントの一覧内で、変更したいアカウントの編集コントロール () をクリックしてください。
2. [Edit User Account] パネルで、必要な変更をしてください。

このパネルのフィールドとオプションは [Create User Account] パネルと同じです。[Create User Account] パネルについての詳細は、「[2.1.3 HCP システムレベル管理者のユーザアカウントを作成する](#)」を参照してください。

変更できる項目は、次のとおりです。

- ユーザ名
- パスワード
- ロール
- ユーザの説明
- 次回ログイン時にパスワードを変更するかしないかの設定

メモ：

[Edit User Account] パネルでユーザのパスワードを入力する際、現在のパスワードを再使用できます。ただし、[Change Password] ページで、自分のパスワードを入力する際には再使用できません。

3. [Update User Account] ボタンをクリックしてください。

2.1.5 システム管理コンソールへのアクセスについて設定する

ここでは、システム管理コンソールへのアクセスについて説明します。システム管理コンソールの [Console Security] ページで、次の内容を設定します。

- システム管理コンソールへアクセスできる IP アドレス
システム管理コンソールでは、指定した IP アドレスのアクセスを許可、または拒否できます。
- ユーザアカウントの有効期間
設定した日数を過ぎると、ユーザアカウントは自動的に無効になります。
保守用のユーザアカウントが無効になるのを防ぐため、0 日（無期限）とする必要があります。
- ユーザアカウントを無効にするログイン失敗回数
設定した回数を連続してログインに失敗すると、ユーザアカウントは自動的に無効になります。
ログイン失敗回数の初期設定値は 5 です。0 を指定すると、ログインに何度失敗してもユーザアカウントは無効になりません。ローカル認証された、Security ロールを持つユーザアカウントが一つだけの場合は、ログイン失敗によってユーザアカウントが無効になっても 1 時間後に再度有効になります。

システム管理コンソールへのアクセスについて設定する手順を説明します。

1. システム管理コンソールで、[Security] にマウスカーソルを置くと表示されるメニューから、[Console Security] を選択します。
[Console Security] ページが表示されます。
2. 次の内容を設定および確認します。
 - [Allow] タブで、システム管理コンソールへのアクセスを許可する IP アドレスを指定し、[Add] ボタンをクリックしてください。
 - [Deny] タブで、システム管理コンソールへのアクセスを拒否する IP アドレスを指定し、[Add] ボタンをクリックしてください。
 - [Disable user account if inactive more than] に指定されている値が、0 となっていることを確認してください。
 - [Disable user account after] に指定されている値を確認します。
ログインに何度失敗してもユーザアカウントが無効にならないようにする場合は、「0」に変更します。

2.1.6 HCP 管理 API から HCP システムへのアクセスについて設定する

HCP 管理 API から HCP システムへアクセスできるように設定します。

HCP 管理 API から HCP システムへのアクセスを有効にする手順を説明します。

1. システム管理コンソールで、[Security] にマウスカーソルを置くと表示されるメニューから、[MAPI] を選択します。
[MAPI] ページが表示されます。
2. [Management API Setting] セクションで、[Enable the management API] オプションを選択します。
3. [Update Setting] ボタンをクリックします。
HCP 管理 API から HCP システムへのアクセスが有効になります。

2.1.7 デフォルトユーザでログアウトする

セキュリティのため、このあとの「2.2 SSL を設定する」以降の操作では、デフォルトユーザのユーザアカウントは使用しないで、作成した HCP システムレベル管理者のユーザアカウントを使用してください。システム管理コンソールからログアウトする手順を説明します。

1. システム管理コンソールで、右上にある [Log Out] リンクをクリックして、ログアウトします。
ログアウト後に操作を終了する場合は、セキュリティを保持するため、ブラウザのキャッシュを削除してから、すべてのブラウザウィンドウを閉じてください。

2.2 SSL を設定する

2.2.1 SSL サーバ証明書情報

2.2.2 新規証明書の生成とインストール

2.2.3 作成した証明書のインストール

2.2.4 CSR の作成と戻された証明書のインストール

(1) 証明書署名の作成

(2) HCP が生成した CSR に対して戻された証明書のインストール

2.2.5 SSL サーバ証明書のプロバイダ

2.3 SNMP を設定する

SNMP を使用すると、システムログメッセージを指定した SNMP マネージャに送信できます。SNMP の使用は任意ですが、使用して運用することを推奨します。

2.3.1 サポートされている標準 MIB ファイル

HCP がサポートする標準 MIB は、ルートディレクトリが **mib-2** のサブツリー内と、ルートディレクトリが **ucdavis** のサブツリー内にあります。HCP が表示するフィールドは、次の MIB 内にあります (() 内のグループを除きます)。

- **mib-2** 以下のフィールド
 - DISMAN-EVENT-MIB
 - HOST-RESOURCES-MIB
 - IF-MIB
 - IP-FORWARD-MIB
 - IP-MIB (ipAddrTable, ipRouteTable, および ipNetToMediaEntry のグループを除く)
 - IPV6-MIB
 - MTA-MIB
 - NOTIFICATION-LOG-MIB
 - RFC1213-MIB (atTable のグループを除く)
 - SNMPv2-MIB
 - TCP-MIB (tcpConnTable のグループを除く)
 - UDP-MIB (udpTable のグループを除く)
- **ucdavis** 以下のフィールド
 - LM-SENSORS-MIB
 - UCD-DISKIO-MIB
 - UCD-DLMOD-MIB
 - UCD-SNMP-MIB

これらすべての MIB のファイルは、RFC1213-MIB を除き、<http://www.net-snmp.org/docs/mibs> からダウンロードできます。RFC1213-MIB は、<http://www.assure24.com/product/420-snmp-mibs-download.htm> からダウンロードできます。

2.3.2 MIB の一覧表示

HCP が **mib-2** と **ucdavis** 以下に正確にどのフィールドを表示するかを調べるには、MIB の一覧表示を行います。MIB の一覧表示とは、HCP が表示するフィールドを SNMP マネージャで表示することです。

MIB を一覧表示する方法は、使用する SNMP ツールにより異なります。次の手順では、インターネットで公開されている **net-snmp** パッケージのコマンドラインツールを使用します。このパッケージは、<http://www.net-snmp.org> からダウンロードできます。

net-snmp を使用して MIB の一覧表示を行うには、次の形式で **snmpwalk** コマンドを使用します。

```
snmpwalk -v snmp-version -c snmp-community-name node-ip-address-or-hostname mib-root
```

node-ip-address-or-hostname の部分は、HCP システムのストレージノードの IP アドレスまたはホスト名です。指定するノードは正常に実行中である必要があります。

次の **snmpwalk** コマンドの例では、IP アドレスが **192.168.210.16** のノードに対して、**mib-2** 以下のサブツリーのフィールドについて表示します。

```
snmpwalk -v 2c -c public 192.168.210.16 mib-2
```

2.3.3 SNMP の設定

SNMP を設定する手順を説明します。

1. システム管理コンソールで、[Monitoring] にマウスカーソルを置くと表示されるメニューから、[SNMP] を選択します。
[SNMP] ページが表示されます。
2. [SNMP] ページの [SNMP Settings] で、次の内容を設定します。
 - HCP システムですべての SNMP の使用を有効にする場合は、[Enable SNMP at snmp.<HCP のシステム名>.<HCP のドメイン名>] オプションのチェックボックスを選択してください。
 - SNMP を経由して HCP システムの設定を変更する場合は、[Allow writes/updates of HCP settings through SNMP] オプションのチェックボックスを選択してください。
 - [SNMP Version] は、[Use version 1 or 2c] オプションを選択してください。
 - [Community] フィールドにコミュニティ名を指定してください。
 - コンプライアンスイベントに関するログメッセージについても SNMP マネージャへ送信する場合は、[Send compliance events] オプションのチェックボックスを選択してください。
 - セキュリティイベントに関するログメッセージについても SNMP マネージャへ送信する場合は、[Send security events] オプションのチェックボックスを選択してください。
 - [Send log messages at this level or higher] フィールドでは、SNMP マネージャに送信されるログメッセージの重要度を選択できます。運用に合わせて、次のどれかを選択してください。
 - [OFF] : ログメッセージが送信されません。
 - [ERROR] : 重要度が Error のメッセージだけが送信されます。
 - [WARNING] : 重要度が Warning または Error のメッセージが送信されます。
 - [NOTICE] : 重要度が Notice, Warning, または Error のメッセージが送信されます。
3. [Update Settings] ボタンをクリックします。
設定した内容が反映されます。
4. [SNMP] ページの右側に表示される [Allow] タブと [Deny] タブで、SNMP を経由して HCP へアクセスする IP アドレスについて設定します。
 - [Allow] タブで、アクセスを許可する IP アドレスについて指定し、[Add] ボタンをクリックします。
 - [Deny] タブで、アクセスを拒否する IP アドレスについて指定し、[Add] ボタンをクリックします。
5. [SNMP] ページの右側に表示される [Trap Addresses] フィールドに、SNMP マネージャの IP アドレスを設定してください。
[Trap Addresses] フィールドに IP アドレスを指定し、[Add] ボタンをクリックすると設定できます。

SNMP マネージャへの接続のテスト

[SNMP] ページの [Test] ボタンをクリックすると、HCP から SNMP マネージャにテスト用のメッセージが送信され、SNMP マネージャへの接続をテストできます。テストの方法については、「[2.3.4 SNMP 接続のテスト](#)」を参照してください。

HCP-MIB.txt ファイルのダウンロードと取り込み

[SNMP] ページの [HCP-MIB.txt] リンクをクリックすると、HCP の MIB について定義されたファイルがダウンロードできます。必要に応じて SNMP マネージャに取り込んで使用してください。

テナントログメッセージの SNMP マネージャへの送信

SNMP マネージャには、テナントログメッセージを送信することもできます。送信する場合は、「3.2 ネームスペースを管理する」の手順を実行後、次のように設定してください。

- a. テナント管理コンソールで、[Monitoring] にマウスカーソルを置くと表示されるメニューから、[SNMP] を選択します。
[SNMP] ページが表示されます。
- b. [SNMP] ページで、[Enable SNMP logging] オプションのチェックボックスを選択します。
- c. [Update Settings] ボタンをクリックします。
設定した内容が反映されます。

2.3.4 SNMP 接続のテスト

[SNMP] ページに表示される IP アドレスを持つ SNMP マネージャへは、接続をテストできます。接続をテストすると、HCP はターゲットの IP アドレスにメッセージを送信します。接続が正常であることを確認するには、所有する SNMP ツールを利用してメッセージが到着したことを確認してください。

HCP が SNMP マネージャに送信するメッセージの重要度は [Notice] です。したがって、メッセージが正常に送信されるためには、送信するメッセージの重要度を [Notice] に設定してください。

指定された SNMP マネージャへの接続をテストするには、次の操作をしてください。

1. [SNMP] ページで、[Test] ボタンをクリックしてください。HCP は次のメッセージを SNMP マネージャに送信します。
2. 確実にメッセージが到着しているかどうか、各 SNMP マネージャを確認してください。

SNMP マネージャがメッセージを受信していない場合

- 指定したターゲット IP アドレスが正しいことを確認してください。
- ターゲット IP アドレスを正常に ping できることを確認してください。

問題の原因を特定できない場合、お問い合わせ先まで連絡してください。

2.4 DNS を設定する

ドメインネームシステム (DNS) は、クライアントのアクセスのためにドメイン名 (例えば、example.com) を IP アドレスに変換、または解決 (resolve) するネットワークサービスです。DNS サービスは、クライアントの要求を解決する 1 台以上のネームサーバと呼ばれるサーバにより提供されます。インターネットとローカル TCP/IP ネットワークの両方とも DNS を使用します。

HCP システムは、企業のドメインのサブドメインとして存在します。HCP のすべてのノードは、この一つのサブドメインに属しているため、クライアントアプリケーションからは一つの実体として見えます。HCP DNS マネージャは、すべてのストレージノード上で実行され、クライアントの要求をシステム内のノードに分散して処理します。

HCP ヘシステム名でアクセスできるようにするには、DNS で HCP サブドメインを設定する必要があります。この章では、Windows と Unix の両方での設定方法と、DNS の HCP 定義を検証する方法を説明します。

2.4.1 HCP サブドメインに設定するゾーンの種類

DNS により解決されるドメイン名はゾーンと呼ばれる部門に分けて管理され、各ゾーンには関連するホスト名と IP アドレスがセットで定義されています。例えば、企業のドメインは企業のゾーンで管理されています。

HCP は企業のドメインのサブドメインです。複数の IP アドレスは企業ゾーン内の 1 ゾーンを構成します。HCP サブドメインは、スタブゾーンで設定する方法と、フォワードゾーンで設定する方法があります。

HCP サブドメインをスタブゾーンで設定

スタブゾーンを使用すると、名前解決を効率化したり、ゾーンのレプリケーションを最小化したりして、ネットワーク上の DNS トラフィック量を削減できます。

スタブゾーンの定義には、サブドメインのマスタネームサーバの IP アドレス一覧が書かれています。そのサーバの個々のレコードは書かれていません。それらのレコードはマスタネームサーバ自身に保存されています。企業の DNS サーバは、スタブゾーンのマスタネームサーバ一覧から個々のネームサーバレコードを取得します。

HCP は、システムのすべてのストレージノードに関するネームサーバレコードを自動的に作成します。各ストレージノードは、それらのレコードのコピーを保存します。これによって、各ストレージノードはマスタネームサーバとなる資格が得られます。HCP によって、名前でシステムを識別するクライアント要求を受け取るには、それらのノードの一部または全部を、HCP スタブゾーンのマスタネームサーバとして登録する必要があります。ノードは、スタブゾーン定義の一覧に加えることによって登録できます。

HCP サブドメインをフォワードゾーンで設定

HCP サブドメインをフォワードゾーンで設定する場合、フォワードゾーンがゾーンの下位部門で、サブドメインに相当します。ゾーンのネームサーバはフォワードゾーンのネームサーバに名前解決の権限を委任することができます。Windows では、フォワードゾーンのネームサーバのグループを委任 (delegation) と呼びます。

HCP がクライアントの要求を受け入れられるようにするには、ネームサーバとして機能させる HCP ノードをすべてこのフォワードゾーンのネームサーバとして登録する必要があります。この登録は HCP 導入手順の一部です。

すべての HCP ストレージノードは、ノードがマスタネームサーバとして登録されているかどうかに関係なく、HCP DNS マネージャのネームサーバとして動作します。ただし、HCP にアクセス可能であるためには、登録されたノードが動作している必要があります。したがって、すべてのノードで同時に障害が起きることのないように、十分な数のノードを登録する必要があります。



参考 HCP が少数のストレージノードしか持っていない場合は、それらをすべてマスタネームサーバとして登録することをお勧めします。登録するノードの数が多いほど、DNS のクエリがより分散されます。

2.4.2 DNS の設定

DNS のセットアップでは、HCP システムの名前を指定します (例: hcp-ma)。この名前は、企業ドメイン名と結合され、HCP システムの完全修飾された DNS 名となります (例: hcp-ma.example.com)。この完全修飾名に使用できるのは、英小文字、数字、およびハイフン (-) です。また、三つ以上のピリオド (.) 区切りのセグメントで構成されている必要があります。

DNS のセットアップではまた、各ノードにフロントエンド IP アドレスを割り当てます。HCP サブドメインをフォワードゾーンで設定する場合は、ノードの名前も割り当てる必要があります。ノー

ド名はプリフィックスとノード番号で構成します。ノード番号には、ノードのバックエンド IP アドレスの最終オクテットを指定します。

ホスト名のプリフィックスは、1~12 文字で構成します。プリフィックスに使用できるのは、英小文字、数字、ハイフン (-) です。HCP の各ノードにデフォルトで割り当てられるプリフィックスは「hcp-node-」です。

HCP サブドメインをスタブゾーンで設定する場合、およびフォワードゾーンで設定する場合の DNS のセットアップ方法について説明します。

なお、この手順説明では、HCP がシステムの完全修飾ドメイン名が「hcp-ma.example.com」に設定されているほか、HCP ノードに対する完全修飾名とフロントエンドの IP アドレスが次のとおり設定されていることを前提としています。

表 2-2 HCP ノードに対する完全修飾名とフロントエンドの IP アドレス

ノード	完全修飾名	フロントエンドの IP アドレス
100	hcp-node-100.hcp-ma.example.com	192.168.5.10
99	hcp-node-099.hcp-ma.example.com	192.168.5.11
98	hcp-node-098.hcp-ma.example.com	192.168.5.12
97	hcp-node-097.hcp-ma.example.com	192.168.5.13

(1) HCP サブドメインをスタブゾーンで設定する場合の DNS のセットアップ

HCP サブドメインをスタブゾーンで設定する場合の DNS のセットアップ方法について説明します。

Windows での HCP スタブゾーンの設定

Windows では、GUI またはコマンド行を使ってスタブゾーンを設定することができます。ここでは、Windows Server 2008 R2 での GUI 設定手順を示します。Windows Server 2003 での手順も基本的には同じです。

ここでは、次の操作をしてください。

1. DNS マネージャを開いてください。

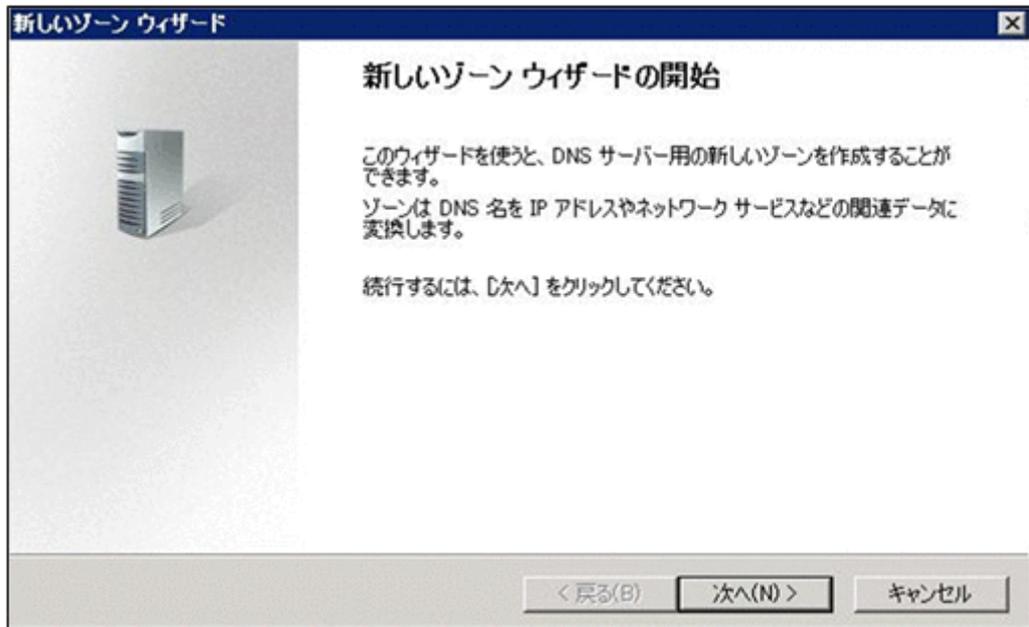
Windows のコントロールパネルで、[管理ツール] をダブルクリックしてください。

[管理ツール] ウィンドウで [DNS] をダブルクリックしてください。DNS マネージャウィンドウは、企業ドメインのゾーン階層を示します。

2. DNS マネージャウィンドウで、企業の DNS サーバの下にある [前方参照ゾーン] を右クリックして [新しいゾーン] を選択し、[新しいゾーン ウィザード] を起動してください。



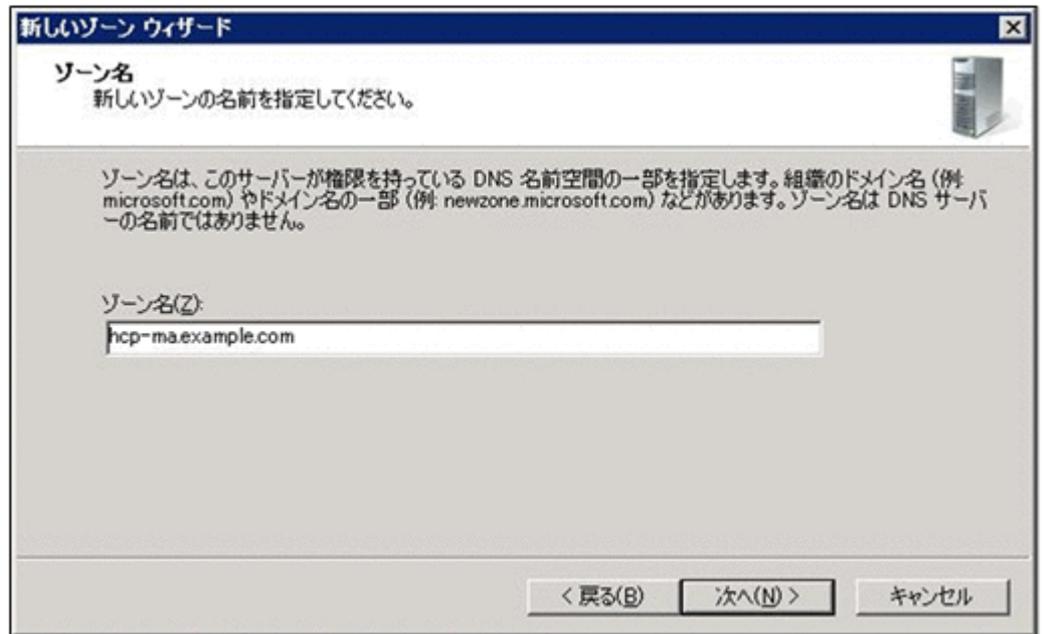
3. [新しいゾーン ウィザード] で、[次へ] ボタンをクリックしてください。



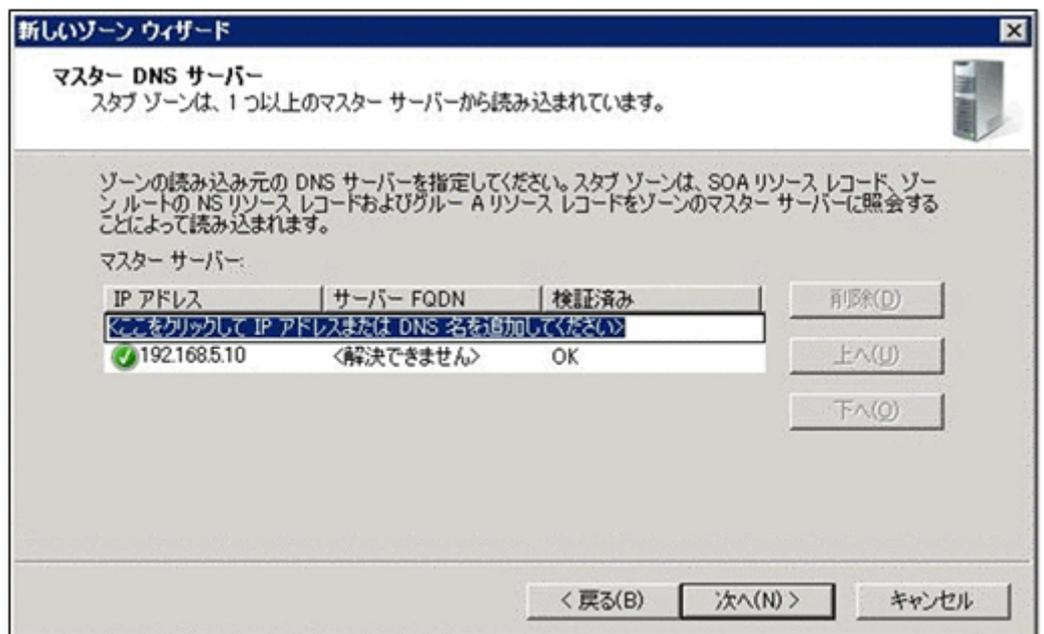
4. [ゾーンの種類] ページで, [スタブゾーン] オプションを選択してから, 次のどちらかを実行してください。
 - Windows の Active Directory Integration 機能を使わずにスタブゾーンを設定するには, [次へ] ボタンをクリックしてください。



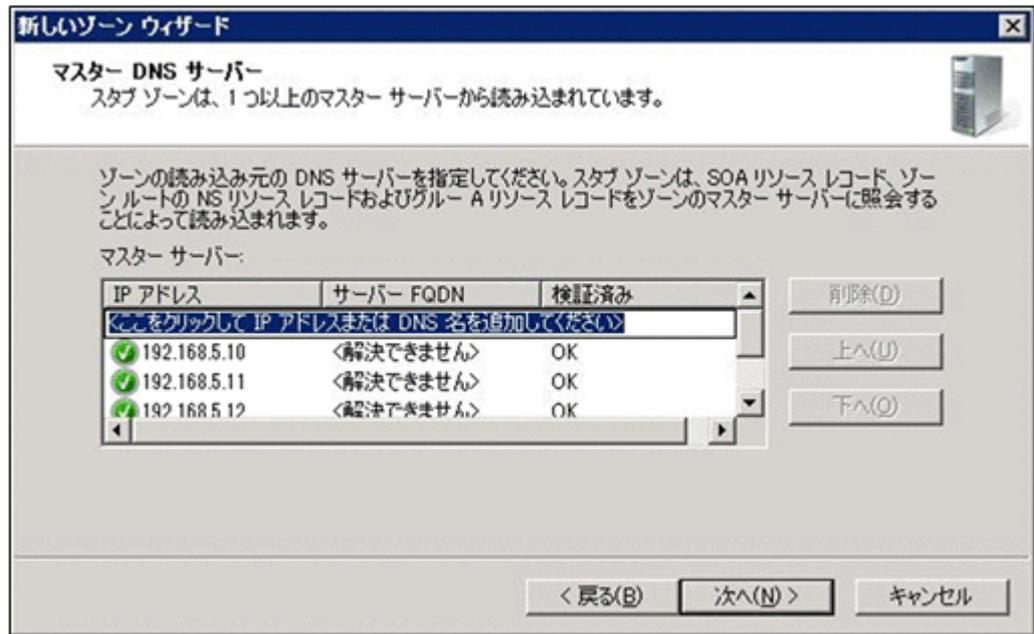
- Windows の Active Directory Integration 機能を使ってスタブゾーンを設定するには, 次の操作をしてください。
 1. [Active Directory にゾーンを格納する] オプションを選択してから, [次へ] ボタンをクリックしてください。
 2. [Active Directory ゾーン レプリケーション スコープ] ページで, ネットワークを通して DNS データをレプリケーションする方法のオプションを選択し, [次へ] ボタンをクリックしてください。
5. [ゾーン名] ページの [ゾーン名] フィールドで, HCP システムの完全修飾ドメイン名を入力してから, [次へ] ボタンをクリックしてください。



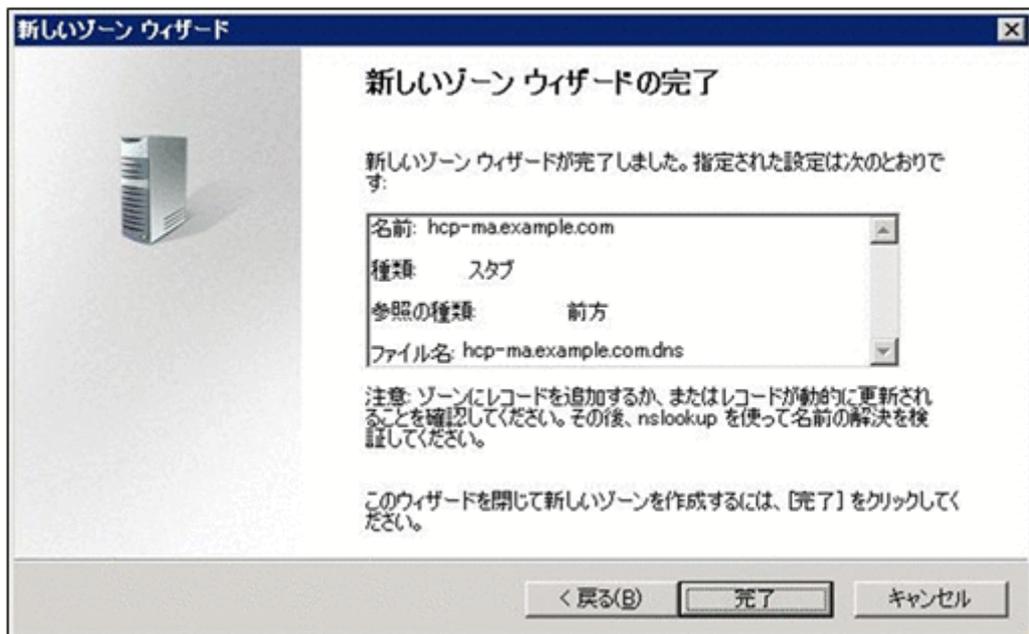
6. [マスタ DNS サーバー] ページで、マスタネームサーバとして登録したい HCP ストレージノードごとに、次の操作をしてください。
 - a. <ここをクリックして IP アドレスまたは DNS 名を追加してください>フィールドに、ノードのフロントエンドの IP アドレスを入力してください。
サーバー FQDN フィールドに<解決できません>と表示された場合も、問題ありません。



- b. すべてのノードのフロントエンドの IP アドレスを入力し、入力完了したら [次へ] ボタンをクリックしてください。



7. [完了] ボタンをクリックしてください。



8. HCP スタブゾーンが DNS マネージャウィンドウのゾーン階層に現れます。

次の画面が表示された場合は、[操作] メニューの [最新の情報に更新] をクリックすると設定した情報が表示されます。



Unix での HCP スタブゾーンの設定

Unix の BIND では、ゾーンが統合 DNS サーバの /etc/named.conf ファイルに定義されます。ユーザは、スタブゾーンの定義で次の項目を指定します。

四つの登録済みマスタネームサーバのある、hcp-ma.example.com という名前の HCP システムのスタブゾーンを定義するゾーン文のサンプルを示します。

- ユーザがスタブゾーンを定義しているサブドメインの完全修飾ドメイン名
- ゾーンタイプ
- DNS クエリの結果をより早く検索するためのキャッシュに使用するファイルの名称
- スタブゾーンのマスタネームサーバの IP アドレスのリスト (HCP システムでは、フロントエンドの IP アドレスを使用します)

```
zone "hcp-ma.example.com IN {  
    type stub;  
    file /var/named/stub/hcp-ma.example.com";  
    masters {192.168.210.15;192.168.210.16;192.168.210.17;192.168.210.18;};  
}
```

(2) HCP サブドメインをフォワードゾーンで設定する場合の DNS のセットアップ

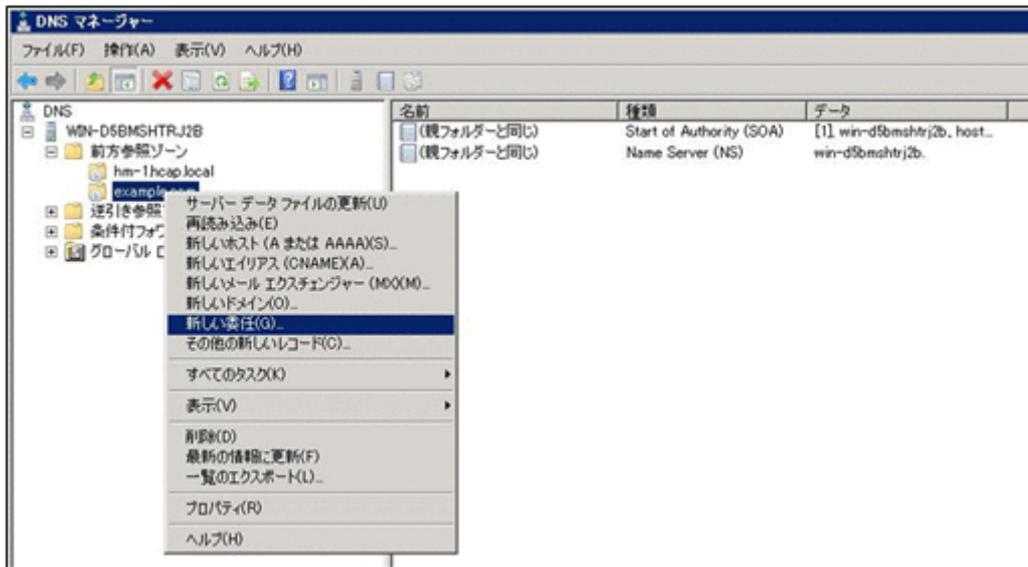
HCP サブドメインをフォワードゾーンで設定する場合の DNS のセットアップ方法について説明します。

Windows での委任の設定

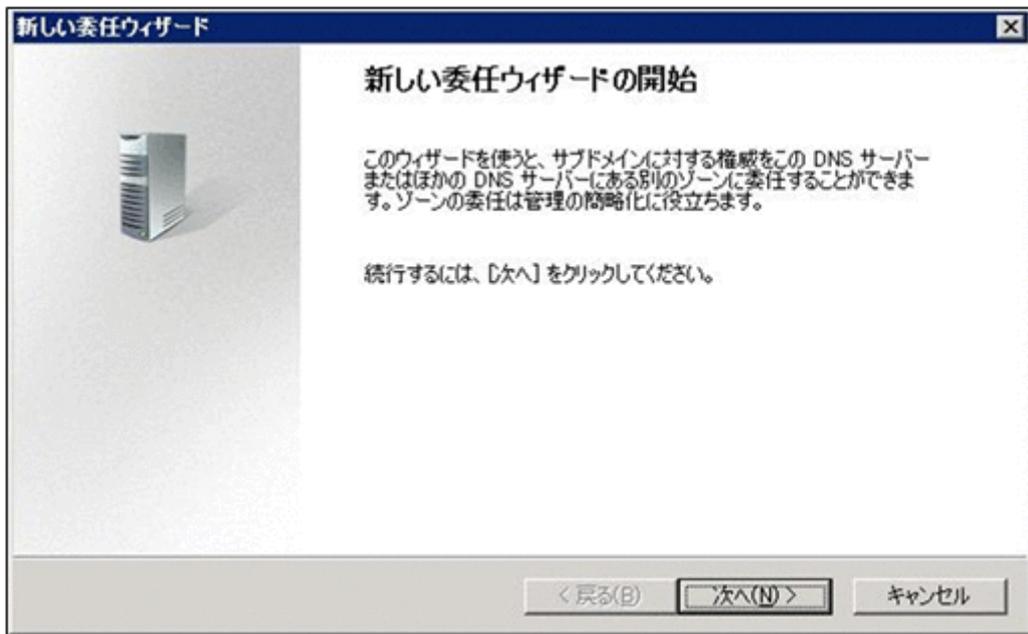
Windows で HCP の委任を設定するために、DNS 管理コンソールを使用します。このセクションでは、Windows Server 2008 R2 での GUI 設定手順を示します。Windows Server 2003 での手順も基本的には同じです。

ここでは、次の操作をしてください。

1. Windows のコントロールパネルで、[管理ツール] をダブルクリックしてください。[管理ツール] ウィンドウが開きます。
2. [管理ツール] ウィンドウで [DNS] をダブルクリックすると、DNS 管理コンソールが開きます。
DNS 管理コンソールは、企業ドメインのゾーン階層を示します。
3. ゾーン階層の [前方参照ゾーン] を開き、HCP 委任を作成したいゾーンの下で、ドロップダウンメニューを開いてください。
4. ドロップダウンメニューで、[新しい委任] を選択してください。



5. [新しい委任ウィザード] で, [次へ] ボタンをクリックしてください。



6. [委任されたドメイン] のフィールドで, HCP のシステム名を入力してください。その際, ドメイン名を含まないでください。例えば, システム名が hcp-ma であり, ドメイン名が example.com である場合, hcp-ma だけを入力してください。ウィザードは, 自動的に [完全修飾ドメイン名] フィールドに書き込まれます。

新しい委任ウィザード

委任されたドメイン名
提供する DNS ドメイン用の権威は別のゾーンに委任されます。

委任する DNS ドメインの名前を指定してください。

委任されたドメイン(D):
hcp-ma

完全修飾ドメイン名 (FQDN):
hcp-ma.example.com

< 戻る(B) 次へ(N) > キャンセル

7. [次へ] ボタンをクリックしてください。
8. 各 HCP ノードをネームサーバとして選択する場合は、[新しい委任ウィザード] で、[追加] ボタンをクリックしてください。

新しい委任ウィザード

ネーム サーバー
委任されたゾーンのホストになるネーム サーバーを 1 つ以上追加してください。

委任されたゾーンをホストする DNS サーバーの名前と IP アドレスを指定してください。

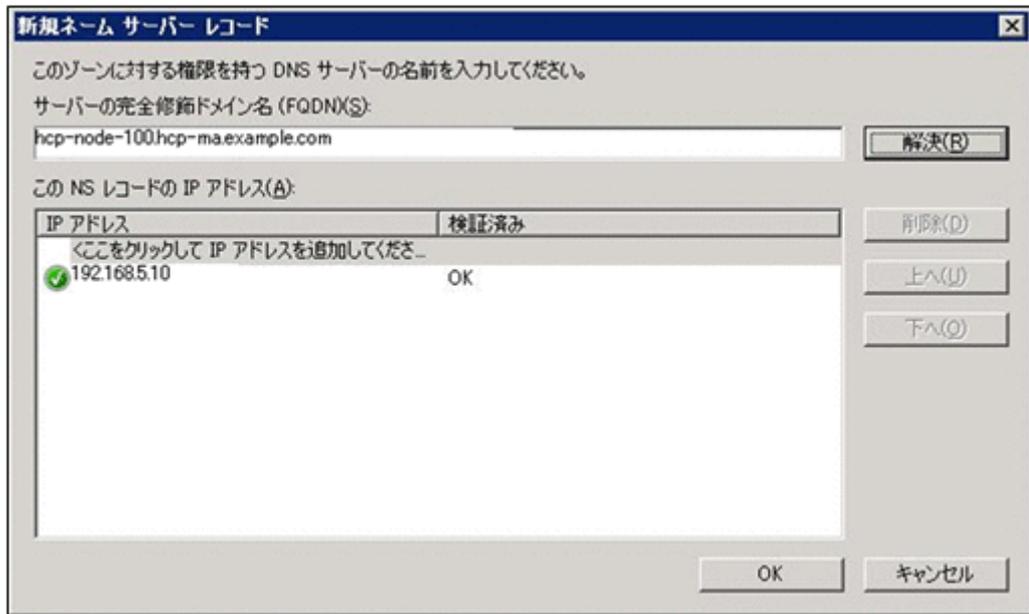
ネーム サーバー(S):

サーバーの完全修飾ドメイン名 (FQDN)	IP アドレス

追加(A) 編集(E) 削除(R)

< 戻る(B) 次へ(N) > キャンセル

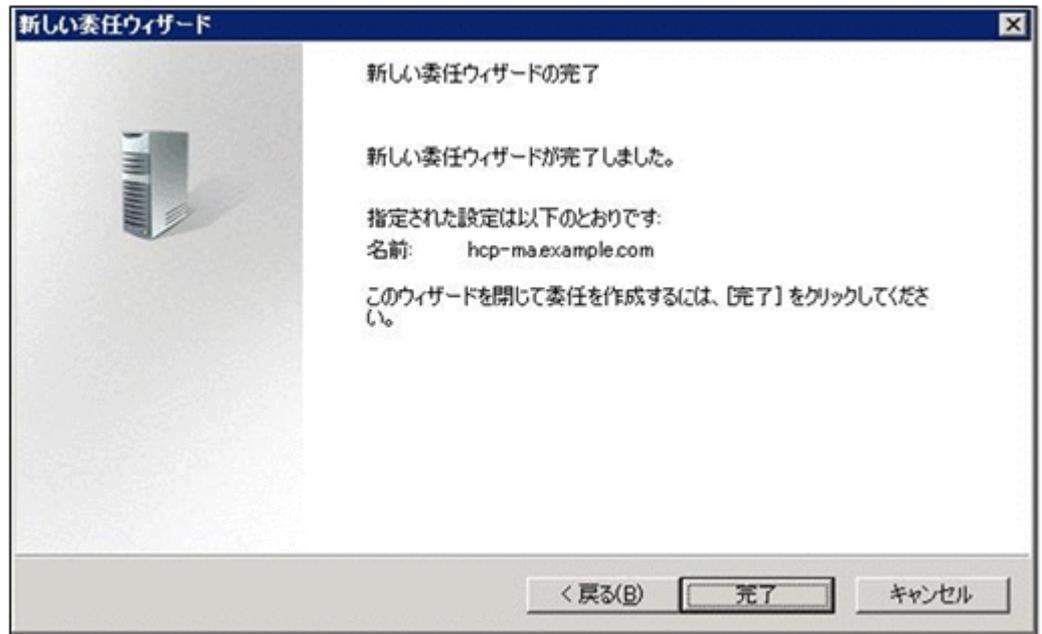
9. [新規ネームサーバーレコード] の [サーバの完全修飾ドメイン名] フィールドに HCP ノードの完全修飾名を入力し、<ここをクリックして IP アドレスを追加してください>フィールドに、ノードのフロントエンドの IP アドレスを入力してください。



10. [OK] ボタンをクリックすると、[新しい委任ウィザード] の [ネームサーバー] リストに追加され、HCP ノードをネームサーバとして選択できます。
11. 手順 8 から手順 10 を繰り返して、ネームサーバを追加します。



12. ネームサーバを追加したら、[次へ] ボタンをクリックしてください。
13. [完了] ボタンをクリックしてください。



HCP 委任が DNS 管理コンソールのゾーン階層に現れます。

(3) Unix での HCP フォワードゾーンの設定

Unix の BIND では設定がゾーンファイルと呼ばれるファイルに保管されます。ゾーンファイルはドメイン名からそのドメインネームサーバの IP アドレスへのマッピングを含んでいます。ファイル中の各マッピングの行はネームサーバ (NS) レコードと呼ばれます。

サブドメインの NS レコードを含んでいるゾーンファイルは、フォワードゾーンファイルと呼ばれます。HCP のフォワードゾーンファイルは NS レコードとネームサーバとして記録したいノードの A レコードを含んでいなくてはなりません。

次の例は、ドメイン名 example.com と hcp-ma という名前の HCP システムを持っている企業の、フォワードゾーンファイルの NS レコードと A レコードです。四つの NS レコードが HCP の完全修飾名を各 hcp ノードの名前にマップします。四つの A レコードがノード名の一つをそのノードのフロントエンド IP アドレスにマップします。

```
hcp-ma.example.com. IN NS hcp-node-001
hcp-ma.example.com. IN NS hcp-node-002
hcp-ma.example.com. IN NS hcp-node-003
hcp-ma.example.com. IN NS hcp-node-004
hcp-node-001 IN A 192.168.140.11
hcp-node-001 IN A 192.168.140.12
hcp-node-001 IN A 192.168.140.13
hcp-node-001 IN A 192.168.140.14
```

2.4.3 設定の検証

ユーザは HCP のゾーンが Windows のコマンドプロンプト画面または Unix のシェルから適切に動作することを検証できます。どちらの場合でも使用できる環境に応じて、ユーザは dig または nslookup コマンドを使用します。コマンドの構文を次に示します。

```
dig|nslookup (admin|nfs|cifs|www) .hcp-name.domain-name
```

このコマンドの対象者は、すべての HCP ストレージノードの IP アドレスリストに記載されているべきです。

10 ノードのうち 6 ノードがゾーンのマスタネームサーバとして登録されている例を、次に示します。

```
# nslookup www.hcp-ma.example.com
Server: adc1850.example.com
Address: 192.168.80.45
Name: www.hcp-ma.example.com
Addresses: 192.168.210.11, 192.168.210.12, 192.168.210.13, 192.168.210.14,
192.168.210.15, 192.168.210.16, 192.168.210.17, 192.168.210.18, 192.168.210.19,
192.168.210.20
```

ユーザが期待したノードリストを確認できない場合、ゾーンは正しく定義されていないことになります。

2.5 syslog ログ記録を設定する

HCP は、システムログメッセージを一つ以上の **syslog** サーバに送信できます。これを行う場合、ユーザの **syslog** 環境内のツールを使って、メッセージのソート、特定のイベントへのクエリ、またはモバイル装置へのエラーメッセージの転送などの機能を実行できます。テナントレベル管理者は、**syslog** サーバに送信されるシステムログメッセージにテナントログメッセージを含めることを選択できます。

2.5.1 syslog サーバに送信されるログメッセージ

イベントに関するシステムログメッセージごとに、HCP は次の情報を指定の **syslog** サーバに送信します。

- システムログエントリには、固有の ID。
- メッセージセグメント番号。1,024 文字を超えるメッセージは、二つ以上のメッセージに分割され、そのすべてが同一のログエントリ ID を持ちます。これらのメッセージセグメントには、最初のセグメントが 0 (ゼロ) から始まる連続した番号が割り当てられます。

HCP は、一つのログメッセージにつき最大 100 セグメント、合計 102,400 文字を送信します。これを超えるテキストは送信できません。

- イベント ID
- イベントが発生したシステム時間
- イベントの重要度
- イベントが発生したノードの IP アドレスと ID
- イベントが関係するボリューム ID (特定の論理ボリュームに關係する場合)
- イベントを発生させたユーザ名とユーザ ID
- メッセージの全文

送信するログメッセージの重要度レベルは選択できます。また、セキュリティイベント (無効なユーザ名によるシステム管理コンソールへのログイン) とコンプライアンスイベントに関するメッセージを送信するかしないかも選択できます。コンプライアンスイベントはネームスペースレベルで発生するため、そのメッセージが **syslog** サーバに送信されるのは、テナントレベルで **syslog** ログ記録が有効になっている場合だけです。

メモ :

システムログメッセージは、**syslog** サーバへ送信できない場合があります。これは、**syslog** プロトコルがデータ送信に UDP を使用するためです。

2.5.2 syslog ログ記録の有効化

HCP で syslog によりログメッセージを送信するには、一つ以上の syslog サーバの IP アドレスを指定してください。複数のサーバを指定すると、HCP はログメッセージをこれらのすべてのサーバに送信します。

システム管理コンソールの [Syslog] ページで、syslog 経由のログ記録を設定します。また、このページを使って、指定する syslog サーバへの接続をテストします。

[Syslog] ページを表示するには、次の手順に従ってください。

1. システム管理コンソールのトップレベルメニュー内の [Monitoring] の上にマウスカーソルを置き、セカンダリメニューを表示してください。
2. セカンダリメニュー内の [Syslog] をクリックしてください。

ロール :

[Syslog] ページを表示するユーザは、ユーザアカウントに Monitor ロール、Administrator ロール、または Security ロールが付与されている必要があります。また、syslog ログ記録を設定し、syslog サーバへの接続をテストするユーザは、ユーザアカウントに Administrator ロールまたは Security ロールが付与されている必要があります。

ログメッセージを syslog サーバへ送信するように HCP を設定するには、[Syslog] ページで次の操作をしてください。

- syslog 設定を指定してください。
 - syslog 設定を指定してください。
 - コンプライアンスイベントに関するログメッセージを含めるには、[Send compliance events] オプションを選択してください。
 - セキュリティイベントに関するログメッセージを含めるには、[Send security events] オプションを選択してください。
 - [Send log messages at this level or higher] フィールドで、指定された syslog サーバに送信するメッセージの重要度を選択してください。
 - [OFF] を選択すると、HCP はログメッセージを送きません。
 - [NOTICE] を選択すると、重要度が Notice, Warning, または Error のメッセージを送信します。
 - [WARNING] を選択すると、重要度が Warning または Error のメッセージだけを送信します。
 - [ERROR] を選択すると、重要度が Error のメッセージだけを送信します。

その後、[Update Settings] ボタンをクリックしてください。

補足 :

変更内容を登録する前に、「2.5.3 syslog 接続のテスト」に記述されているように、指定された syslog サーバへの接続をテストできます。

- 一つ以上の syslog サーバの IP アドレスを指定してください。それぞれの IP アドレスについて、次の操作をしてください。
 1. [Syslog Server IP Addresses] フィールドに、IP アドレスを入力してください。必要な場合、IP アドレスの後にコロンとポート番号を入れてください。ポート番号を省略すると、HCP はポート番号 514 を使用します。

このリスト内の各エントリは、必ず IP アドレス一つにしてください。IP アドレスレンジやコマで区切ったリストは、ここでは無効です。
 2. [Add] ボタンをクリックしてください。

IP アドレスがフィールドの下側のリストに移動します。

リストから IP アドレスを削除するには、対象の IP アドレスの削除コントロール () をクリックしてください。リストからすべての IP アドレスを削除するには、[Delete All] ボタンをクリックしてください。

2.5.3 syslog 接続のテスト

[Syslog] ページに表示される IP アドレスを持つ syslog サーバへは、接続をテストできます。接続をテストすると、HCP はターゲットの IP アドレスにメッセージを送信します。接続が正常であることを確認するには、所有する syslog ツールを利用してメッセージが到着したことを確認してください。

HCP が syslog サーバに送信するメッセージの重要度は [Notice] です。したがって、メッセージが正常に送信されるためには、送信するメッセージの重要度を [Notice] に設定してください。

指定された syslog サーバへの接続をテストするには、次の操作をしてください。

1. [Syslog] ページで、[Test] ボタンをクリックしてください。HCP は次のメッセージを syslog サーバに送信します。

```
User username sent system log test message. (ユーザ<ユーザ名>がシステムログテストメッセージを送信しました。)
```

2. 確実にメッセージが到着しているかどうか、各 syslog サーバを確認してください。

syslog サーバがメッセージを受信していない場合は、次のことを確認してください。

- 指定したターゲット IP アドレスが正しいか
- ターゲット IP アドレスを正常に ping できるか

問題の原因を特定できない場合、お問い合わせ先まで連絡してください。

2.6 システム管理コンソールでチャージバックレポートを作成する

HCP システム管理コンソールでチャージバックレポートを作成できます。チャージバックレポートには、テナントとそのネームスペースに関する現在および過去の統計値が、時間単位で記載されます。

チャージバックレポートはシステムを分析するための優れた情報源であるため、ストレージと帯域幅の割り当てを利用パターンに基づいて調整できます。このレポートは、テナントまたはネームスペースの単位で容量と帯域幅の利用状況に応じた費用の決定に必要な、請求アプリケーションの入力としても使用できます。

チャージバックレポートは HCP のテナントとネームスペースだけを対象としています。デフォルトテナントとデフォルトネームスペースは対象外です。

2.6.1 チャージバックレポートについて

チャージバックレポートには、システムで定義された HCP テナントごとに集計したネームスペースの統計値が記載されています。例えば、あるレポートの作成期間中のあるテナントの読み取り総数は、そのテナントが所有するすべてのネームスペースで、その期間中に発生した読み取りが成功した総数です。

チャージバックレポートには、HCP システム全体で集計した HCP テナント統計値も記載されています。例えば、あるレポートの作成期間中のシステムの読み取り総数は、システムの各 HCP テナントが所有するネームスペースの、その期間中に発生した読み取りが成功した総数です。チャージバックレポートのシステム統計値には、デフォルトテナントまたはデフォルトネームスペースは考慮されていません。

HCP テナントがシステムレベルのユーザ管理権限で自分自身にアクセスする権限を与えた場合、チャージバックレポートに、そのテナントが所有する個々のネームスペースごとの統計値が記載されます。

チャージバックレポートをシステム管理コンソールで作成した場合、CSV 形式となります。レポートの各行には、あるレポートの作成期間中の、一つのネームスペース、一つのテナント、または HCP システム全体の値が記載されます。

チャージバックレポートの行は、テナント名のアルファベット順に表示されます。レポートにあるテナントが所有するネームスペースがある場合、テナントの行の下にネームスペースがアルファベット順で表示されます。HCP システムの行はレポートの最後です。テナント、ネームスペース、またはシステムの行が複数の場合、発生した順に表示されます。

チャージバックデータの収集方法については、「[2.6.2 チャージバックレポートの作成](#)」を参照してください。チャージバックレポートの内容については、「[2.6.3 チャージバックレポートの内容](#)」を参照してください。

ロール :

チャージバックレポートを作成する場合、ユーザアカウントに **Monitor** ロールまたは **Administrator** ロールが必要です。

2.6.2 チャージバックレポートの作成

システム管理コンソールの [Chargeback] ページでチャージバックレポートを作成します。このページから、1 時間または 1 日単位のレポートを次のとおり作成できます。

- 1 時間単位のレポートには、直近の 1 時間の統計値と、現在時刻まで累積された統計値が掲載されます。例えば、2:30:15 p.m. にレポートを要求した場合、1:00:00 p.m. から 1:59:59 p.m. の期間の 1 組の統計値が掲載され、また 2:00:00 p.m. から 2:30:15 p.m. の期間で別の 1 組の統計値が掲載されます。
- 1 日単位のレポートには、直近の 1 日の統計値と、現在日まで累積された統計値が掲載されます。例えば、10 月 7 日の 2:30:15 p.m. にレポートを要求した場合、10 月 6 日の 00:00:00 から 23:59:59 の期間の 24 組の統計値が掲載され、また 10 月 7 日の 00:00:00 から 2:30:15 p.m. の期間の 15 組の統計値が掲載されます。

補足 :

HCP 管理 API を使用すると、さらに長い期間を対象とするチャージレポートを XML, JSON, または CSV 形式で作成できます。これにより、一定間隔でチャージバックレポートを作成して、そのレポートを請求システムに渡すアプリケーションを作成できます。

チャージバックレポートを作成するには

1. システム管理コンソールの最上位メニューで、[Monitoring] 上にマウスを置いてセカンダリメニューを表示します。
2. セカンダリメニューで、[Chargeback] をクリックしてください。
3. [Chargeback] ページで、[Hourly Chargeback Report] , [Daily Chargeback Report] または [Monthly Chargeback Report] をクリックして (規定どおり)、レポートをダウンロードするブラウザ固有オプションを選択します。

デフォルトでは、ダウンロードされたレポートファイルの名前は Hourly-Chargeback-Report.csv、Daily-Chargeback-Report.csv または Monthly-Chargeback-Report.csv のどれかです（該当する場合）。

2.6.3 チャージバックレポートの内容

チャージバックレポートの1行目には、次に続く行の値に対する識別子が書かれています。次の表で、それぞれの値について説明します。また、ある時点 (P) の値であるか、動的 (D) な値であるかを示します。

表 2-3 チャージバックレポートの内容

識別子	タイプ	値
systemName	—	次のどれかです。 <ul style="list-style-type: none"> その行の統計値セットが適用されるネームスペースを所有するテナントを含む HCP システムの DNS 名 その行の集計した統計値セットが適用されるテナントを含む HCP システムの DNS 名 その行の集計した統計値セットが適用される HCP システムの DNS 名
tenantName	N/A	次のどちらかです。 <ul style="list-style-type: none"> その行の統計値セットが適用されるネームスペースを所有するテナントの名前 その行の統計値セットが適用されるテナントの名前 システム全体の統計値が書かれた行には、このフィールドの値はありません。
namespaceName	N/A	その行の統計値セットが適用されるネームスペースの名前です。 テナントまたはシステム全体の統計値が書かれた行には、このフィールドの値はありません。
startTime	N/A	その行の統計値セットに対するレポート作成期間の開始時間。次の形式で書かれています。 yyyy-MM-dd hh:mm:ss hh には 24 時間形式の時間が出力されます。
endTime	N/A	その行の統計値セットに対するレポート作成期間の終了時間。startTime 値に使用された形式と同じ形式で書かれています。
objectCount	P	指定したテナントが所有するすべてのネームスペース、または HCP システムのすべての HCP ネームスペースの内の、指定したネームスペースのオブジェクト数です。
ingestedVolume	P	指定したネームスペース、指定したテナントが所有するすべてのネームスペース、または HCP システムのすべての HCP ネームスペースに追加される前の、格納済みデータとカスタムメタデータの合計サイズ（バイト単位）です。
storageCapacityUsed	P	指定したテナントが所有するすべてのネームスペース、または HCP システムのすべての HCP ネームスペースの内の、指定したネーム

識別子	タイプ	値
		スペースに保存されたデータが占める総バイト数です。これには、オブジェクトデータ、メタデータ、および適切な DPL を満たすために必要な冗長データが含まれます。
bytesIn	D	レポート作成期間中に、指定した名前空間、指定したテナントが所有するすべての名前空間、または HCP システムのすべての HCP 名前空間への書き込みが成功した総バイト数です。
bytesOut	D	レポート作成期間中に、指定した名前空間、指定したテナントが所有するすべての名前空間、または HCP システムのすべての HCP 名前空間から読み取りが成功した総バイト数です。
reads	D	レポート作成期間中に、指定した名前空間、特定したテナントが所有するすべての名前空間、または HCP システムのすべての HCP 名前空間で実行された読み取り操作が成功した総バイト数です。
writes	D	レポート作成期間中に、指定した名前空間、指定したテナントが所有するすべての名前空間、または HCP システムのすべての HCP 名前空間で実行された書き込み操作が成功した総バイト数です。
deletes	D	レポート作成期間中に、指定した名前空間、指定したテナントが所有するすべての名前空間、または HCP システムのすべての HCP 名前空間で実行された削除およびページ操作が成功した総バイト数です。
deleted	N/A	次のどれかです。 TRUE 名前空間またはテナントが、セットの統計値が収集された後に削除されました。 FALSE 現在名前空間またはテナントが存在します。 INCLUDED テナントまたは HCP システムの場合、そのセットの統計値には、後で削除された一つ以上の名前空間の値が含まれます。
valid	N/A	その行の統計値セットの状態です。値は次の可能性があります。 TRUE HCP はそのセットのすべての統計値を正常に収集しました。 FALSE そのセットの統計値は、レポート作成期間中に発生したすべてのアクティビティを反映しているわけではありません。例えば、一つ以上のノードがこの期間中に利用できない、ネットワークに障害が発

識別子	タイプ	値
		生じた、ほかのハードウェアに障害が発生した、などの原因が考えられます。

2.7 システム管理コンソールの警告を確認する

システム管理コンソールは、システム状態を表示するために、[Overview] ページ、[Hardware] ページ、[Storage Node] ページ、および [Tenants] ページでグラフィックとメッセージを使用します。これらのグラフィックは警告と呼ばれ、システムの特定の要素を表します。警告は、要素に問題ない、または問題が存在する、のどちらかを示すことができます。

警告は [Storage/Search Node] ページにテキストで表示されます。警告が表示されるすべてのページでは、警告の上にマウスを合わせると、テキストが表示されます。

ここでは、コンソールの各ページに表示される警告と、警告に伴って表示されるメッセージの一覧を示します。また、警告が表示された場合の対応方法も説明します。

表 2-4 [Overview] ページの警告

警告グラフィック	メッセージ	説明
	Hardware functioning properly	HCP ハードウェアのすべてが正常に機能しています。
	System is starting	HCP は起動中です。
	High load or swap	一つ以上のノードで過負荷またはページ切り替えが頻発しています。お問い合わせ先まで連絡してください。
	Unavailable nodes	一つ以上のノードが利用できません。ノードの状態がいつのまにか [available] から [Unavailable] に変わったり、ノードが自動的に起動しなかったりする場合、認定を受けた HCP サービスプロバイダに連絡してください。ノードは手動で再起動しないでください。問題の診断に必要な情報が失われる原因となる場合があります。
	Processor failure	IPMI センサが、動作していないプロセッサを含む一つ以上のノードを検出しています。お問い合わせ先まで連絡してください。
	Power supply failure	一つ以上のノードで、電源が一つしか動作していません。お問い合わせ先まで連絡してください。
	Abnormal temperature	IPMI センサが、温度値が推奨範囲外の一つ以上のノードを検出しています。詳細については、対象の [Storage/Search Node] ページを参照してください。
	Broken fan	IPMI センサが、ファン速度が推奨範囲外の一つ以上を検出し

警告グラフィック	メッセージ	説明
		ています。詳細については、対象の [Storage Node] ページを参照してください。
	Abnormal voltage	IPMI センサが、電圧値が推奨範囲外のノードを一つ以上検出しています。詳細については、対象の [Storage Node] ページを参照してください。
	Back-end switch error	一つ以上のバックエンド・スイッチは、正常に稼動していません。お問い合わせ先まで連絡してください。
	Network error	一つ以上のネットワーク接続が動作していません。システム内のすべてのネットワーク接続を確認してください。正常に機能しているようであれば、お問い合わせ先まで連絡してください。
	Storage device reporting errors	一つ以上の物理ドライブで障害が発生しています。お問い合わせ先まで連絡してください。
	Maximum namespaces exceeded	テナントのネームスペースの数は、上限を超えています。ネームスペースを削除してください。
	Maximum namespaces reached	HCP システムで定められたネームスペースの上限数に達しています。
	Storage usage is <i>percent-used</i>	ストレージノードが管理するストレージの使用率が 85 パーセント未満です。
	Storage usage is <i>percent-used</i>	ストレージノードが管理するストレージの使用率が 85 パーセント以上です。HCP システムへのストレージ容量の追加を検討してください。
	Storage usage is <i>percent-used</i>	ストレージノードが管理するストレージの使用率が 95 パーセント以上です。HCP はこれ以上新規のオブジェクトや、新規または置き換え用カスタムメタデータを保存しません。ただし、メタデータの変更は許可し続けます。
	Data access failover	ゼロコピーフェイルオーバーが有効になっている SAIN システムの場合、ほかのノードが正常に管理されているストレージの管理下にノードが引き継がれました。認定を受けた HCP サービスプロバイダに連絡してください。
	Multipath degraded to one	multipathing で設定された SAIN システムの場合、ノードと外部ストレージの間の物理接続が故障しました。認定を受けた HCP サービスプロバイダまで連絡してください。

警告グラフィック	メッセージ	説明
	All <i>operation-types</i> operations are disabled	示された種類の操作は現在許可されていません。この警告は、システム全体アクセス権限マスク内でアクセス権限のどれかが無効になると表示されます。
	An unrecoverable error has occurred.	HCP 自身で修復できない障害が発生しています。お問い合わせ先まで連絡してください。
	All objects are intact	HCP ポリシーではオブジェクトに問題はありませんでした。
	All metadata is intact	オブジェクトメタデータの問題はありませんでした。
	Metadata balancing.	メタデータをより分散化するため、HCP はオブジェクトのメタデータをノード間で移動中です。
	Below metadata protection level.Repairing...	一つ以上のオブジェクトが DPL により必要とされるコピーの数を保持していません。保護ポリシーは問題修復処理中です。
	Content verification repair disabled	コンテンツ検証サービスは現在、破損データを持つオブジェクトのチェックまたは修復をしていません。この警告が表示されるのは、[Content Verification] ページで [Do not check and repair objects] オプションが選択されている場合です。
	Replication link pending	システムは、レプリケーションリンクの要求をもう一つのシステムに送って、レスポンスを待っているか、またはシステムがレプリケーションリンクのリクエストを受け取って、まだ返答していないかのどちらかです。
	Replication link failure	アウトバウンドのレプリケーションリンクが、期待どおりに機能していません。プライマリシステムとレプリカ間のネットワーク接続を確認してください。接続が正常に機能しているようであれば、お問い合わせ先まで連絡してください。
	Replication link stalled	レプリケーションリンクが予想外に停止しました。プライマリシステムとレプリカ間でネットワークコネクションを確認してください。コネクションに問題がない場合、お問い合わせ先まで連絡してください。
	Replica storage almost full	レプリカストレージスペースの 90%以上が使用されています。レプリカにストレージ容量を追加することを検討してください。

警告グラフィック	メッセージ	説明
		この警告が表示されるのは、プライマリシステムのシステム管理コンソールだけです。
	Replica storage full (link suspended)	レプリカストレージスペースは94%使用されています。レプリカは、プライマリシステムからのレプリケーションデータ転送をこれ以上処理できません。HCPは自動的にレプリケーションリンク上の動作を一時停止しました。レプリカにストレージ容量を追加してください。その後、レプリケーションリンク上の動作を再開してください。 この警告が表示されるのは、プライマリシステムのシステム管理コンソールだけです。
	System auto-paused tenant(s) from replication	HCPは、一つ以上のHCPテナントのレプリケーションを自動的に一時停止しました。テナントごとに、レプリケーションが一時停止される原因となった状態を修正してください。次にテナントのレプリケーションを再開してください。
	Front-end connection error	一つ以上のノードに対するフロントエンド接続がすべて使用できません。このシステムが現在のレプリケーション元である場合、幾つかのオブジェクトがレプリケーションされません。このシステムがレプリケーション先である場合、レプリケーション性能が低下します。
	SSL server certificate expires soon	SSL証明書が90日以内に期限切れになります。「2.2.4」を参照して新しいSSLサーバ証明書をインストールしてください。
	SSL server certificate expires soon	SSL証明書が30日以内に期限切れになります。「2.2.4」を参照して新しいSSLサーバ証明書をインストールしてください。
	Replication certificates expire soon	一つ以上の信頼されたレプリカサーバ証明書は、90日以内に期限切れになります。「2.2.4」を参照してサーバ証明書を更新してください
	Replication certificates expire soon	一つ以上の信頼されたレプリカサーバ証明書は、30日以内に期限切れになります。「2.2.4」を参照してサーバ証明書を更新してください
	Expired replication certificates	一つ以上のレプリケーションサーバ証明書期限切れが発生したため、レプリケーションシステムは停止

警告グラフィック	メッセージ	説明
		しました。「2.2.4」を参照を参照してサーバ証明書を更新してください

表 2-5 [Hardware] ページの警告

警告グラフィック	メッセージ	説明
	Storage failure	ノードが管理する一つ以上の物理ストレージデバイスが正常に機能していません。お問い合わせ先まで連絡してください。
	Multipath degraded	multipathing 用に設定された SAN 接続ストレージ専用のメッセージ。ノードと外部ストレージの間の物理接続が故障しました。お問い合わせ先まで連絡してください。
	NIC failure	一つ以上の NIC が正常に機能していません。お問い合わせ先まで連絡してください。
	Temperature out of normal range	IPMI センサは、温度値が高いまたは低い（ただし危機的ではない）構成要素を一つ以上検出しています。[Storage Node] ページで温度値を監視してください。正常値に戻らない場合、お問い合わせ先まで連絡してください。
	Temperature critical	IPMI センサは、温度値が危機的に高いまたは低い構成要素を一つ以上検出しています。ノードをシャットダウンし、お問い合わせ先まで連絡してください。
	Power supply error	ノードで正常に動作している電源が一つだけです。お問い合わせ先まで連絡してください。
	Fan speed out or normal range	IPMI センサは、推奨範囲より速いまたは遅いファンを一つ以上検出していますが、危機的ではありません。[Storage Node] ページでファン速度を監視してください。正常値に戻らない場合、お問い合わせ先まで連絡してください。
	Fan speed critical	IPMI センサは、速度が危機的に速いまたは遅いファンを一つ以上検出しています。ノードをシャットダウンし、お問い合わせ先まで連絡してください。
	Voltage out of normal range	IPMI センサは、電圧値が高いまたは低い（ただし危機的ではない）構成要素を一つ以上検出しています。[Storage Node] ページで電圧値を監視してください。正常値に戻らない場合、お問い合わせ先まで連絡してください。

警告グラフィック	メッセージ	説明
	Voltage critical	IPMI センサは、電圧値が危機的に高いまたは低い構成要素を一つ以上検出しています。ノードをシャットダウンし、お問い合わせ先まで連絡してください。
	File system failure	一つ以上のファイルシステムに利用可能な空き容量または inode がありません。お問い合わせ先まで連絡してください。
	Node problem	ノードの負荷が高いか、ノードで高い確率でページスワッピングが行われています。お問い合わせ先まで連絡してください。
	Node has been removed	ノードが HCP システムから完全に削除されました。後で HCP システムに追加するノードに、このノードのバックエンド IP アドレスを再利用できません。

表 2-6 [Storage Node] ページの警告

警告グラフィック	メッセージ	説明
	Logical volume usage	警告を展開すると、ノードが管理する論理ボリュームのステータス、容量、および使用領域が表示されます。
	Core hardware is functioning normally	ノードの負荷とページスワッピング率は許容範囲内です。
	Core hardware may need attention	ノードに高い負荷がかかっているか、ノードのページスワッピング率が高くなっています。認定を受けた HCP サービスプロバイダまで連絡してください。
	Node is not available	ノードが使用できない理由は、次のどれかです。 <ul style="list-style-type: none"> ノードは起動しましたが、まだ HCP 機能を実行できません。 ノードは停止中のため、HCP 機能を実行できません。 ノードは実行中でないか、または HCP システムの残りとの通信ができません。
	Node has been removed	ノードが HCP システムから完全に削除されました。後で HCP システムに追加するノードに、このノードのバックエンド IP アドレスを再利用できません。
	Multipath degraded	multipathing で設定された SAN 接続ストレージの場合だけ、ノードと外部ストレージの間の物理接続に障害が発生しました。認定を受けた HCP サービスプロバイダまで連絡してください。

警告グラフィック	メッセージ	説明
	<i>file-system-count</i> file systems on <i>storage-device-count</i> devices	ノードは一つ以上のファイルシステムを持ち、それらのファイルシステムは一つ以上の物理ストレージデバイスにマッピングされていません。
	<i>bad-storage-device-count</i> of <i>storage-device-count</i> storage devices are not functioning correctly	ノードが管理する一つ以上の物理ストレージデバイスは正常に機能していません。お問い合わせ先まで連絡してください。
	All IPMI sensors report normal operation	IPMI が監視する構成要素はすべて正常に機能しています。
	<i>sensor-count</i> IPMI sensors are indicating problems	示された数の IPMI センサが、ノード内に一つ以上の問題を検出しています。詳細については、IPMI 詳細を確認してください。
	No IPMI status is available	ノードは IPMI センサを含みません。
	All network interfaces are functioning properly	ノード内のすべての NIC は正常に機能しています。
	<i>bad-interface-count</i> of <i>interface-count</i> network interfaces are not functioning properly	ノード内の一つ以上の NIC が正常に機能していません。お問い合わせ先まで連絡してください。
	All <i>file-system-count</i> file systems have sufficient space and inodes	ノード上のすべてのファイルシステムは、追加オブジェクトを保存するために利用可能なスペースと <i>inode</i> を持ちます。
	<i>bad-file-system-count</i> of <i>file-system-count</i> file systems are running out of space or inodes	一つ以上のファイルシステムのスペースまたは <i>inode</i> がこれ以上利用できません。お問い合わせ先まで連絡してください。

表 2-7 [Tenants] ページの警告

警告グラフィック	メッセージ	説明
	Soft quota exceeded	HCP テナント専用のメッセージ。HCP テナントが所有するすべての HCP ネームスペースで使用中の容量が、HCP テナントに対して設定されたソフト Quota を超過しています。テナントレベル管理者に連絡し、HCP テナントのハード Quota を増加してもらってください。
	Tenant with DPL 1 namespaces that are not replicating	HCP テナントの場合、そのテナントは、DPL が 1 がかつレプリケーションされていない一つ以上のネームスペースを所有しています。保存したデータが確実に保護されるように、DPL が 1 のすべての HCP ネームスペースをレプリケーションしてください。

警告グラフィック	メッセージ	説明
	Tenant may have directories that are not being replicated	デフォルトテナントの場合、そのデフォルト名前スペースは、DPLが1でかつデフォルト名前スペース内のディレクトリの一つ以上がレプリケーション中です。デフォルト名前スペースのDPLが1の場合、そのデフォルト名前スペース内のすべてのディレクトリは、保存データを保護するためにレプリケーションしてください。
	Receiving replication - read only	HCP テナント専用のメッセージ。テナントはレプリケーションリンクの受信側にあるため、テナントは読み取り専用です。
	Tenant has <i>broken-object-count</i> irreparable objects	テナントが所有する一つ以上の名前スペースに修復不可能なオブジェクトが含まれています。お問い合わせ先まで連絡してください。
	Tenant <i>tenant-name</i> has <i>irreparable-object-count</i> irreparable objects	テナントが持つ一つ以上の名前スペースに示された数の回復できないオブジェクトがあります。お問い合わせ先にご連絡ください。
	Tenant <i>tenant-name</i> has <i>irreparable-object-count</i> irreparable objects and <i>unavailable-object-count</i> unavailable objects	テナントが持つ一つ以上の名前スペースに示された数の回復できないオブジェクト、利用できないオブジェクトがあります。お問い合わせ先にご連絡ください。
	Namespace quota exceeded	テナントの名前スペースの数は、 Quota で設定した上限を超えています。
	Namespace quota reached	テナントの名前スペースの数は、 Quota で設定した上限に達しています。

2.8 ゼロコピーフェイルオーバーを使用する

HCP システムでのゼロコピーフェイルオーバーは、故障したノードが管理していたストレージを、別のノードが自動的に引き継ぐ処理です。ゼロコピーフェイルオーバーを使うには、ストレージを正しく構成し、HCP システム設定でゼロコピーフェイルオーバーを有効にしてください。



参考 ゼロコピーフェイルオーバーが適用されるのは、ストレージノードだけです。

ここでは、ゼロコピーフェイルオーバーをサポートするのに必要なストレージセットアップを説明し、さらにゼロコピーフェイルオーバーがどのように動作するのかを説明します。

2.8.1 ゼロコピーフェイルオーバーとは

正常な状況では、クロスマッピングされたペアの各ノードは、自身へプライマリマッピングを持つ論理ボリュームを管理します。ただし、ゼロコピーフェイルオーバーが有効になっている場合に片方

のノードが使用できなくなると、もう一方のノード（ピア）がボリューム管理を引き継ぎます。一方のノードがもう一方のノードからストレージ管理を引き継ぐことをフェイルオーバーと呼びます。

使用できなくなったノードが HCP システムに復帰すると、そのノードは自身の論理ボリューム管理を再開します。これをフェイルバックと呼びます。

フェイルオーバー時にシステム管理コンソールに表示される情報

フェイルオーバーが発生すると、利用不可能になったノードに関連づけられている論理ボリュームは最初、システム管理コンソールの [Hardware] ページで初期化状態 (🔴) を示すグラフィックとして表示されます。ピアが論理ボリュームを引き継ぐと、このグラフィックはピアの表示行へ移動し、利用可能を示すグラフィックに変わります (🟢)。

フェイルオーバー中の論理ボリュームがある間は、[Overview] ページに次に示す警告が表示されます。



Data access failover

[Overview] ページに表示される警告 (Alerts) の詳細については、「[2.7 システム管理コンソールの警告を確認する](#)」を参照してください。

フェイルオーバー時にデータアクセスが不可能となる時間

論理ボリュームがフェイルオーバー中は、その論理ボリュームに保存されているデータは一時的に使用できない状態になります。ボリュームを管理していたノードがシステム管理コンソールからのシャットダウンにより使用できなくなった場合は、最長で 5 分の間データにアクセスできなくなります。

その他の理由でノードが使用できなくなった場合（例えば、ノードとストレージレイの間の物理パスがすべて切断されたり、ノード自体に障害が発生した場合）は、きわめて長い時間、データにアクセスできない状態が続きます。データアクセスが不可能になる時間は、次の要因の影響を受けます。

- 論理ボリュームの数
- 論理ボリュームの合計サイズ
- 論理ボリュームに保存されているオブジェクトの数
- ノードが使用できなくなったときに生じていたデータストレージアクティビティの量

ノード再起動時にデータアクセスが不可能となる時間

システム管理コンソールからノードの再起動を実行すると、そのノードに管理されているストレージは、再起動処理のうちのシャットダウン段階で、ピア（ペアのもう一方のノード）にフェイルオーバーします。このフェイルオーバー処理は、再起動中のノードがシャットダウン処理を完了させる前に終了します。フェイルオーバーによりデータにアクセスできなくなる時間は最長で 5 分です。

ノードが回復したときは、フェイルバック処理のために、再起動に要する時間は 15~30 秒長くなります。フェイルバックによりデータにアクセスできなくなる時間は最長で 5 分です。

データ保護メカニズム

ゼロコピーフェイルオーバーでは、ピアグループ内の二つのノードが互いのストレージを誤って上書きするのを防止するため、データ保護メカニズムが使用されます。データ保護メカニズムを使用するには、すべてのストレージパスがアクセス可能になっている必要があります。データ保護メカニズムは、ペア内のノードがストレージボリュームをマウントまたはアンマウントするときに使用されます。データ保護メカニズムが使用されるのは次のようなときです。

- ノードの起動時
- ノードの停止時
- ノードがピアからストレージ管理を引き継ぐとき（フェイルオーバー）
- ノードが管理中のストレージの制御を解放するとき（フェイルバック）

これらの状態でないときは、データ保護メカニズムへのアクセスを確実にするため、ノードとストレージレイの間の二つのパスが利用可能になっている必要があります。どちらかのパスが利用できない場合、ノードは利用不可能状態になることで、データの安全を保証します。

パスが利用不可能になった場合、影響を受けているノードを開始または停止する前に原因を突き止め、修復してください。

フェイルオーバーと物理パスの利用不可

ノードとストレージレイ間の物理パスが利用できなくなった場合、正常に処理を継続します。そのノードに対する二つ目のパスが利用できなくなった場合に最初のパスがまだ利用できないときは、そのノードは利用できなくなり、フェイルオーバーが発生します。

そのノードを利用できるようにして論理ボリュームのフェイルバックを行うためには、そのノードを再起動する前に両方のパスを修復する必要があります。どちらかのパスが利用できない場合でもそのノードは利用できません。

ストレージのフェイルオーバーを管理するノードにパスの利用不可があり、そのピアが利用できない場合、正常に処理は継続します。しかし、そのピアがサービスを開始し、ストレージが元に戻った場合、パスの利用不可があるノードは利用できなくなり、次に示すように別方向にフェイルオーバーが発生します。

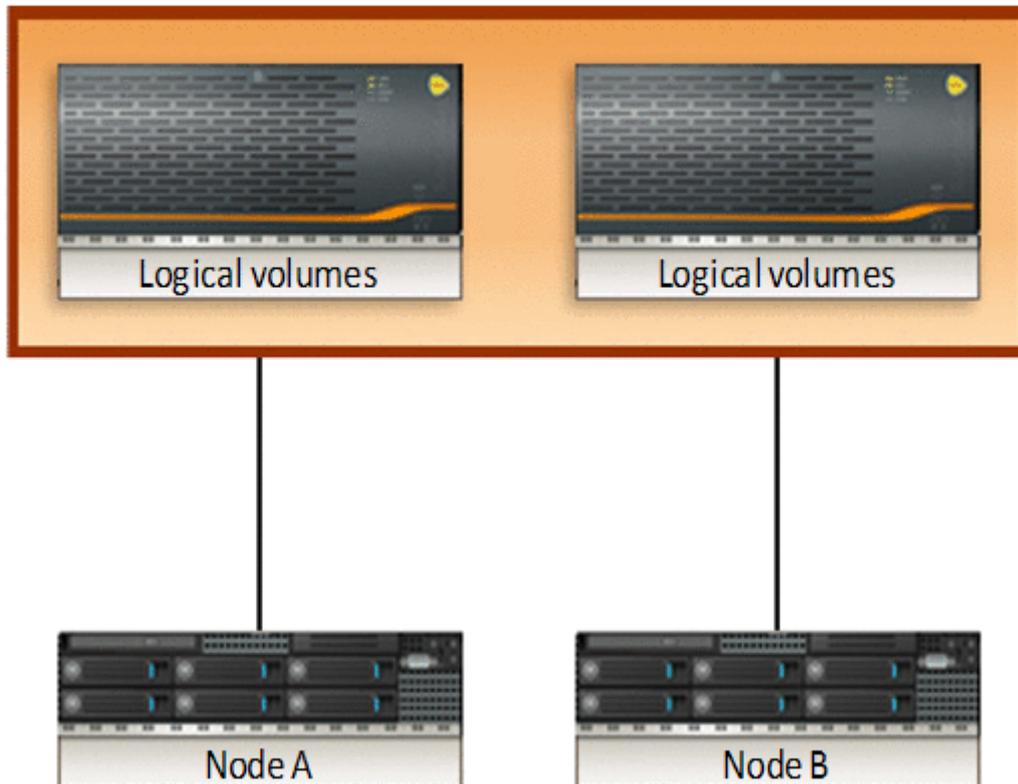
1. ノード A に障害が発生します。
2. ノード A のストレージからノード B にフェイルオーバーを実施します。
3. ノード B の一つのパスの利用ができません。
4. ノード A がサービスを開始します。
5. ノード A のストレージからノード B にフェイルバックを実施します。
6. ノード B が利用できなくなります。
7. ノード B のストレージがノード A にフェイルオーバーを実施します。

2.8.2 ストレージの設定

HCP システムでは、それぞれのノードは物理接続と論理接続の両方でストレージに接続されています。物理接続は、ファイバーチャネルのケーブルで確立されたパスを使用します。論理接続は、ストレージレイの各論理ボリュームと各ノードとのマッピングを使用します。

物理パス

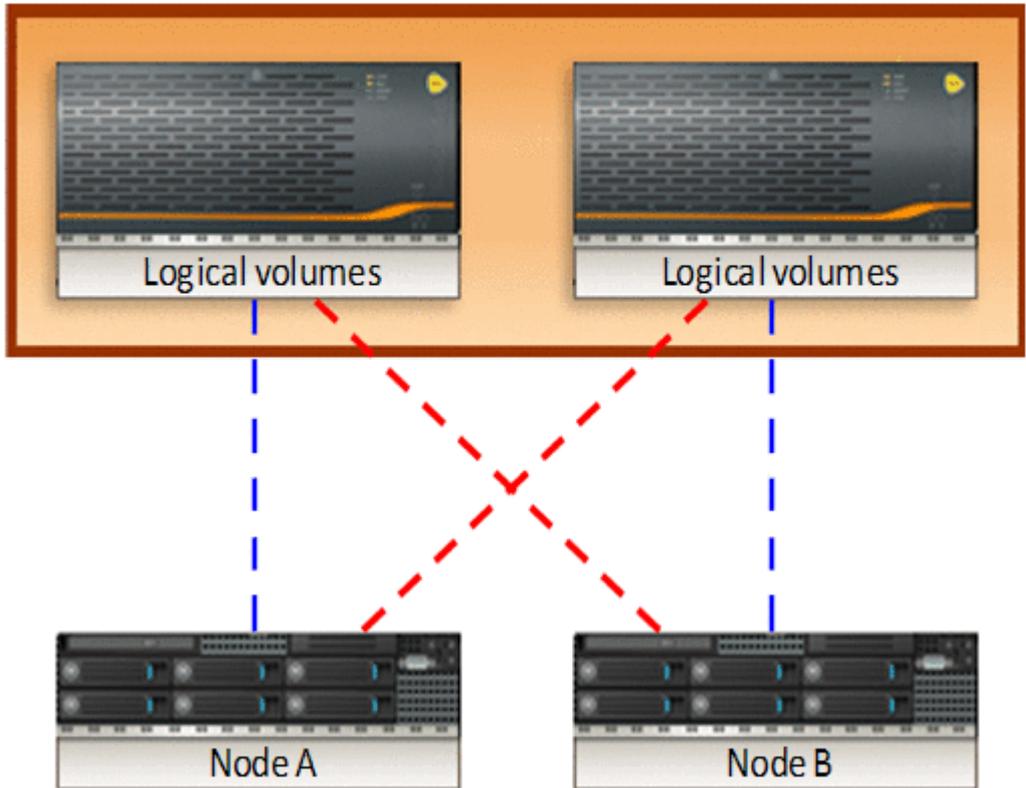
HCP システムでは、各ノードはストレージレイへの物理パスを二つ持ちます。これを **multipathing** と呼びます。次の図の下部に A と B の二つのノードを示します。それぞれのノードは上部のストレージレイへマルチパス接続されています。



マッピング

ゼロコピーフェイルオーバをサポートするには、ストレージレイ内の論理ボリュームとノードがクロスマッピングされている必要があります。クロスマッピングでは、一つのノード (A) にマッピングされる各論理ボリュームが、ピアノードと呼ばれる同じペア内のもう一方のノード (B) にもマッピングされる必要があります。ノード A へのマッピングは論理ボリュームに対するプライマリマッピングで、ノード B へのマッピングはスタンバイマッピングです。同様に、ノード B へのプライマリマッピングを持つ各論理ボリュームは、ノード A へのスタンバイマッピングも持つ必要があります。

次の図に、ストレージレイ内の 2 組の論理ボリュームが A と B の二つのノードにマッピングされている例を示します。各ノードのプライマリマッピングを青色で示します。セカンダリマッピングを赤色で示します。



テナントおよびネームスペースを管理する

ここでは、テナントおよびネームスペースを管理するために必要な作業について説明します。

- 3.1 テナントを管理する
- 3.2 ネームスペースを管理する
- 3.3 テナントのユーザアカウントを設定する
- 3.4 テナント管理コンソールでチャージバックレポートを作成する
- 3.5 テナント管理コンソールの警告を確認する

3.1 テナントを管理する

テナントを作成するに当たり必要となる作業を次に示します。記載された順に作業を実施してください。

なお、デフォルトテナントおよびデフォルトネームスペースは使用しないでください。

- テナントを作成する
- テナントレベル管理者のユーザアカウントでログインし、パスワードを変更する
- テナントレベル管理者の情報を設定する
- テナント管理コンソールへのアクセスについて設定する
- HCP システムレベル管理者にテナント管理コンソールへのアクセス権限を設定する
- HCP 管理 API からテナントへのアクセスについて設定する

また、HCP の運用を開始したあとに発生したトラブルへの対応としてテナントに対して次の作業が必要となることがあります。

- テナントを変更する
- テナントセキュリティ管理者のパスワードをリセットする

それぞれの詳細な手順を次に説明します。

3.1.1 テナントを作成する

テナントを作成する手順を説明します。

1. システム管理コンソールのメニューから、[Tenants] を選択します。
[Tenants] ページが表示されます。
2. [Tenants] ページで、[Create Tenant] をクリックします。
[Create Tenant] パネルが表示されます。
3. [Create Tenant] パネルで、次の内容を設定します。次の内容以外はデフォルトのままとしてください。
 - [Tenant Name] に、テナント名を指定してください。
 - [Username] フィールドに、テナントレベル管理者のユーザアカウントのユーザ名を指定してください。
 - [Password] フィールドに、テナントレベル管理者のユーザアカウントのパスワードを指定してください。
 - [Confirm Password] フィールドに、テナントレベル管理者のユーザアカウントのパスワードを、もう一度指定してください。
 - [Hard Quota] フィールドに、テナントが利用するストレージの容量を指定してください。
 - [Namespace Quota] フィールドに、テナントに作成できるネームスペース数の上限値を指定してください。HVFP と連携している場合は、ファイルシステムに対応するネームスペース数に 1 を足した数以上の値を指定する必要があります。
 - [Retention Mode Selection] オプションのチェックボックスを選択して、ネームスペースの作成時に保管モードを選択できるようにしてください。
 - [Versioning] オプションのチェックボックスを選択して、バージョン管理を有効にしてください。
 - [Search] オプションのチェックボックスのチェックを外して、検索機能を無効にしてください。

- [Service Plan Selection] オプションのチェックボックスのチェックを外して、サービスプランを無効にしてください。
 - レプリケーション機能を使用している場合は [Replication] をチェックします。
また、[Soft Quota] フィールドの値が、85%となっていることを確認してください。
4. [Create Tenant] ボタンをクリックします。
テナントが作成されます。

3.1.2 テナントレベル管理者のユーザアカウントでログインし、パスワードを変更する

テナント作成後、初めてテナント管理コンソールにログインする場合、テナント作成時に指定したテナントレベル管理者のユーザアカウントを使用します。初回のログイン時には、パスワードの変更を求められるため、その変更手順についても説明します。

1. 「3.1 テナントを管理する」で作成した、テナントレベル管理者のユーザアカウントで、テナント管理コンソールにログインします。
パスワードの変更画面が表示されます。
2. 表示された画面で、パスワードの情報を指定します。
次の情報を指定してください。
 - [Existing password] フィールドに、現在のテナントレベル管理者のパスワードを指定してください。
 - [New password] フィールドに、テナントレベル管理者の新しいパスワードを指定してください。
 - [Confirm new password] フィールドに、テナントレベル管理者の新しいパスワードをもう一度指定してください。
3. [Update Password] ボタンをクリックします。
テナントレベル管理者のパスワードが変更され、テナント管理コンソールが表示されます。

3.1.3 テナントレベル管理者の情報を設定する

テナントレベル管理者の情報設定について説明します。テナント管理コンソールの [Users] ページで、次の内容を設定します。

- 氏名の追加
テナントレベル管理者の氏名を設定します。
 - ログイン時の認証方法の確認
ログイン時の認証はローカル認証だけをサポートしているため、正しく設定されているか確認します。
 - ロールの変更
ネームスペースを作成するためには、テナントレベル管理者に特定のロールを与える必要があります。
1. テナント管理コンソールで、[Security] にマウスカーソルを置くと表示されるメニューから、[Users] を選択します。
[Users] ページが表示されます。
 2. [Users] ページで、テナントレベル管理者の左横にある、編集コントロール (✎) をクリックします。

[Edit User Account] ウィンドウが表示されます。

3. [Edit User Account] ウィンドウで、次の内容を設定します。次の内容以外はデフォルトのままとしてください。
 - [Full Name] フィールドに、テナントレベル管理者の氏名を指定してください。
 - [Roles] セクションで、次のロールのチェックボックスを選択してください。
[Monitor], [Administrator], [Security], [Compliance]
4. [Update User Account] ボタンをクリックします。
設定した内容が反映されます。
5. [Close] ボタンをクリックします。
[Edit User Account] ウィンドウが閉じます。

3.1.4 テナント管理コンソールへのアクセスについて設定する

テナント管理コンソールへのアクセスについて説明します。テナント管理コンソールの [Console Security] ページで、次の内容を設定します。

- テナント管理コンソールへアクセスできる IP アドレス
テナント管理コンソールでは、指定した IP アドレスのアクセスを許可、または拒否できます。
- ユーザアカウントの有効期間
設定した日数を過ぎると、ユーザアカウントは自動的に無効になります。
保守用のユーザアカウントが無効になるのを防ぐため、0 日（無期限）とする必要があります。
- ユーザアカウントを無効にするログイン失敗回数
設定した回数を連続してログインに失敗すると、ユーザアカウントは自動的に無効になります。
ログイン失敗回数の初期設定値は 5 です。0 を指定すると、ログインに何度失敗してもユーザアカウントは無効になりません。ローカル認証された、Security ロールを持つユーザアカウントが一つだけの場合は、ログイン失敗によってユーザアカウントが無効になっても 1 時間後に再度有効になります。

テナント管理コンソールへのアクセスについて設定する手順を説明します。

1. テナント管理コンソールで、[Security] にマウスカーソルを置くと表示されるメニューから、[Console Security] を選択します。
[Console Security] ページが表示されます。
2. 次の内容を設定および確認します。
 - [Allow] タブで、テナント管理コンソールへのアクセスを許可する IP アドレスを指定し、[Add] ボタンをクリックします。
 - [Deny] タブで、テナント管理コンソールへのアクセスを拒否する IP アドレスを指定し、[Add] ボタンをクリックします。
 - [Disable user account if inactive more than] に指定されている値が、「0」となっていることを確認します。
 - [Disable user account after] に指定されている値を確認します。
ログインに何度失敗してもユーザアカウントが無効にならないようにする場合は、「0」に変更します。

3.1.5 HCP 管理 API からテナントへのアクセスについて設定する

HCP 管理 API からテナントへアクセスできるように設定します。

HCP 管理 API からテナントへのアクセスを有効にする手順を説明します。

1. テナント管理コンソールで、[Security] にマウスカーソルを置くと表示されるメニューから、[MAPI] を選択します。
[MAPI] ページが表示されます。
2. [Management API Setting] セクションで、[Enable the management API] オプションを選択します。
3. [Update Setting] ボタンをクリックします。
HCP 管理 API からテナントへのアクセスが有効になります。

3.1.6 テナントを変更する

テナントを作成した後、プロパティの一部を変更できます。プロパティの変更はテナントの [Settings] パネルで行います。

ロール :

[Settings] パネルを表示するユーザは、ユーザアカウントに Monitor ロールまたは Administrator ロールが付与されている必要があります。テナントを変更するユーザは、ユーザアカウントに Administrator ロールが付与されている必要があります。

既存テナントを変更するには、次の手順に従ってください。

1. システム管理コンソールのトップレベルメニュー内の、[Tenants] をクリックしてください。
2. テナントの一覧でテナント名をクリックしてください。
3. テナント名の下タブの中の、[Settings] をクリックしてください。
4. [Settings] パネルで、テナントのプロパティを変更してください。このパネル内のフィールドでは次のプロパティを変更できます。
 - [Tenant Name] : テナント名
 - [Description] : テナントの説明
 - [Soft Quota] : HCP テナントの空き容量が少なくなったときに報告するパーセンテージ
 - [Namespace Quota] : HCP がテナントのために予約したネームスペース数
 - [Contact Information] : テナントレベル管理者への連絡先情報
 - [Create and Assign Tags] : 論理グループとフィルタリングのためのタグ付け
5. [Update Settings] ボタンをクリックしてください。

3.1.7 テナントセキュリティ管理者のパスワードをリセットする

HCP テナントの管理ユーザアカウントは、システムレベルユーザアカウントと同様に動作します。一つ以上のアカウントに Security ロールが付与されている必要があります、Security ロールを持つアカウントの一つ以上がローカルで認証されている必要があります。

HCP テナントの Security ロールを持つすべての管理ユーザが同時にパスワードを忘れると、HCP テナントのユーザアカウントを管理できなくなります。

この状態を修復するには、システム管理コンソールを使って、すべての HCP テナントの、Security ロールを持つ、ローカルで認証されたユーザアカウントのパスワードをリセットします。この操作を行う場合、影響を受けるすべてのアカウントに対して、一つのパスワードを指定します。

ロール :

HCP テナントの、Security ロールを持つ、ローカルで認証されたユーザアカウントのパスワードをリセットする管理ユーザは、管理ユーザアカウントに Administrator ロールが付与されている必要があります。

HCP テナントの、Security ロールを持つ、ローカルで認証されたすべての管理ユーザのパスワードをリセットするには、次の手順に従ってください。

1. システム管理コンソールのトップレベルメニュー内の、[Tenants] をクリックしてください。
2. テナントの一覧でテナント名をクリックしてください。
3. テナント名の下タブの中の、[Settings] をクリックしてください。
4. [Settings] パネルで、[Reset Security] ボタンをクリックしてください。
5. [Reset Password] ウィンドウで、次の操作をしてください。
 - [New Password] フィールドに、新しいパスワードを入力してください。パスワードは英数字の大文字・小文字を区別します。パスワードには、UTF-8 文字のうち半角の英字、数字、記号だけが使用できます。パスワードに使用できる文字は、英字、数字、記号の 3 種類に分けられます。パスワードには、3 種類の文字のうち、2 種類以上の文字を使用してください。日本語入力はサポートしていません。
パスワードの文字数は 64 文字以内で指定し、テナント設定が要求する最小文字数に適合するようにしてください。
 - [Confirm Password] フィールドに、新しいパスワードをもう一度入力してください。
6. [Change Password] ボタンをクリックしてください。

3.2 ネームスペースを管理する

HVFP でのファイルシステム作成時に、対応するネームスペースが作成されている場合は、この作業は不要です。ファイルシステム作成時に作成されたネームスペースの名称は「<ファイルシステム名>-<システムが自動で付与する HVFP ごとの ID >」となります。

ネームスペースを作成するに当たり必要となる作業を次に示します。記載された順に作業を実施してください。

なお、ここで説明する手順は、初めてネームスペースを作成する場合を前提とします。

- ネームスペースを作成する
- システム設定情報ファイルの保存先のネームスペースを作成する
- カスタムメタデータの設定を変更する
- HTTP プロトコルを使ったネームスペースへのアクセスについて設定する

また、HCP の運用を開始したあとに発生したトラブルへの対応としてネームスペースに対して次の作業が必要となることがあります。

- ネームスペースの Quota を変更する
- 修復不可能なオブジェクトを削除する

それぞれの詳細な手順を次に説明します。

3.2.1 ネームスペースを作成する

ネームスペースを作成する手順を説明します。

1. テナント管理コンソールで、[Namespaces] を選択します。

- [Namespaces] ページが表示されます。
- [Namespaces] ページで, [Create Namespace] をクリックします。
[Create Namespaces] パネルが表示されます。
 - [Create Namespaces] パネルで, 次の内容を設定します。次の内容以外はデフォルトのままとしてください。
 - [Namespace Name] フィールドに, ネームスペース名を指定してください。
 - [DPL] フィールドで, [1] または [2] を選択してください。
 - [Hard Quota] フィールドに, ネームスペースに割り当てるストレージの容量を指定してください。
 - [Retention Mode] の下にある [Enterprise] を選択して, ネームスペースの保管モードをエンタープライズモードに設定してください。
 - [Versioning] の下にある [On] を選択して, バージョン管理を有効にしてください。
また, [On] を選択すると表示される [Prune versions older than] フィールドで, [Primary System], [Replica System (if replicating)] とともに運用に応じた保管日数を指定して, プルーニングまでの保管日数を設定してください。プルーニングとは, 保管日数を過ぎたオブジェクトの古いバージョンを自動的に削除することです。
HCP にマイグレートした過去のバージョンのデータを HVFP のクライアントに公開する場合は, HVFP でのバージョンの保持期間より 1 日長く期間を設定してください。過去のバージョンのデータを公開しない場合は, 「2 日」を設定してください。
また, 次の内容を確認してください。
 - [Hash Algorithm] フィールドで, [SHA-256] が選択されていること
 - [Soft Quota] フィールドの値が, 85%となっていること
 - [Create Namespace] ボタンをクリックします。
ネームスペースが作成されます。

運用開始後のネームスペース追加時の注意事項

運用開始後に追加したネームスペースへ, 作成済みのユーザアカウントを使ってアクセスする場合は, ネームスペースへのアクセス権限を与える必要があります。「[3.3.3 テナントのユーザアカウントを変更する](#)」を参照して, ユーザアカウントに, [Read], [Write], [Delete] および [Purge] のアクセス権限を与えてください。

3.2.2 システム設定情報ファイルの保存先のネームスペースを作成する

システム設定情報ファイルの保存先のネームスペースを作成する手順を説明します。

- テナント管理コンソールで, [Namespaces] を選択します。
[Namespaces] ページが表示されます。
- [Namespaces] ページで, [Create Namespace] をクリックします。
[Create Namespaces] パネルが表示されます。
- [Create Namespaces] パネルで, 次の内容を設定します。次の内容以外はデフォルトのままとしてください。
 - [Namespace Name] フィールドで, 「system-backup-data」を指定してください。
 - [DPL] フィールドで, [1] または [2] を選択してください。
 - [Hash Algorithm] フィールドで, [SHA-256] が選択されていることを確認してください。
 - [Hard Quota] フィールドで, 「<テナントを使用しているシステムの合計数>×1GB」を指定してください。

<テナントを使用しているシステムの合計数>は、シングルノード構成またはクラスタ構成の HVFP のシステム数、および Virtual Server 数の合計です。

- [Soft Quota] フィールドの値が、「85%」となっていることを確認してください。
- [Retention Mode] の下にある [Enterprise] を選択して、ネームスペースの保管モードをエンタープライズモードに設定してください。
- [Versioning] の下にある [On] を選択して、バージョン管理を有効にしてください。
また、[On] を選択すると表示される [Prune versions older than] フィールドで、[Primary System]、[Replica System (if replicating)] とともに「2」を指定してください。

4. [Create Namespace] ボタンをクリックします。

ネームスペースが作成されます。

3.2.3 カスタムメタデータの設定を変更する

保持期間中のオブジェクトに対して、カスタムメタデータの追加、削除および置き換えができるように設定を変更する手順を説明します。なお、HVFP と連携している場合、この設定はファイルシステムに対応するネームスペースにだけ必要で、システム設定情報ファイルの保存先のネームスペースには不要です。

1. テナント管理コンソールで、[Namespaces] を選択します。
[Namespaces] ページが表示されます。
2. ネームスペースの一覧から、作成したネームスペース名をクリックします。
3. ネームスペース名の下タブにある [Policies] をクリックします。
[Policies] パネルが表示されます。
4. [Policies] パネルの左側の [Retention] をクリックします。
5. [Retention] パネルの [Custom Metadata] セクションで、[Add, delete, and replace] オプションを選択します。
6. [Update Setting] ボタンをクリックします。
設定した内容が反映されます。

3.2.4 HTTP プロトコルを使ったネームスペースへのアクセスについて設定する

ここでは、HTTP プロトコルを使った、ネームスペースへのアクセスの設定について説明します。テナント管理コンソールの [Protocols] パネルで、次の内容を設定します。

- SSL セキュリティ (HTTPS) の使用
ネームスペースへのアクセスに、SSL セキュリティを使用するかどうかを設定できます。
- HTTP プロトコルを使ってアクセスできる IP アドレスの設定
HTTP プロトコルを使ってネームスペースにアクセスできるかどうかを、IP アドレスごとに設定できます。

HTTP プロトコルを使った、ネームスペースへのアクセスについて設定する手順を説明します。

1. テナント管理コンソールで、[Namespaces] を選択します。
[Namespaces] ページが表示されます。
2. ネームスペースの一覧から、作成したネームスペース名をクリックします。
3. ネームスペース名の下タブにある [Protocols] をクリックします。
[Protocols] パネルが表示されます。

4. [Protocols] パネルで、次の内容を設定します。
 - SSL セキュリティを使用しない場合は [Enable HTTP] オプション、SSL セキュリティを使用する場合は [Enable HTTPS] オプションを選択してください。
 - [Allow] タブで、アクセスを許可する IP アドレスについて指定し、[Add] ボタンをクリックします。
 - [Deny] タブで、アクセスを拒否する IP アドレスについて指定し、[Add] ボタンをクリックします。
 - [Allow request when same IP is used in both lists] オプションでは、[Allow] タブおよび [Deny] タブで指定されていない、または両方に表示されている IP アドレスの扱いについて設定できます。
5. [Update Settings] ボタンをクリックします。
設定した内容が反映されます。

3.2.5 ネームスペースの Quota を変更する

HCP ネームスペースのハード Quota とソフト Quota はいつでも変更できます。

ロール :

HCP ネームスペースの Quota を変更するには、ユーザアカウントに Administrator ロールが付与されている必要があります。

HCP ネームスペースのハード Quota かソフト Quota、または両方を変更するには、次の手順に従ってください。

1. テナント管理コンソールのトップレベルメニューで、[Namespaces] をクリックしてください。
2. HCP ネームスペースのリストに Quota を変更したい HCP ネームスペースの Quota 変更コントロール () をクリックしてください。
3. [Modify Namespace Quota] ウィンドウで、次のどちらか、または両方を実行してください。
 - [Hard Quota] フィールドで、HCP ネームスペースに割り当てるストレージの GB 数または TB 数を入力し、測定単位を示す [GB] か [TB] を選択してください。測定単位に [GB] を選択した場合の最小値は 1 で、[TB] を選択した場合の最小値は 0.01 です。
 - [Soft Quota] フィールドに HCP ネームスペースの新しいソフト Quota を入力してください。有効な値は 10~95 の整数です。
4. [Update Quota] ボタンをクリックしてください。

3.2.6 修復不可能なオブジェクトを削除する

HCP システムは、検出した修復不可能なオブジェクトの記録をします。テナント管理コンソールで指定した HCP ネームスペースについて、修復不可能なオブジェクトを一覧表示できます。リストを表示するには、次の手順に従ってください。

1. テナント管理コンソールのトップレベルメニューで、[Namespaces] をクリックしてください。
2. HCP ネームスペースのリストで、対象の HCP ネームスペース名をクリックしてください。
3. HCP ネームスペース名の下タブにある [Monitoring] をクリックしてください。
4. [Monitoring] パネルの左側の [Irreparable Objects] をクリックしてください。

ロール :

[Irreparable Objects] パネルを表示するには、ユーザアカウントに、**Monitor** ロールまたは **Administrator** ロールが必要です。修復不可能になったオブジェクトに確認済みであることを示す目印を付けるには、ユーザアカウントに **Administrator** ロールが必要です。

リストのオブジェクトについて、[Irreparable Objects] パネルはオブジェクトへの絶対パス (rest から後ろの部分) と、オブジェクトが修復できないことを HCP が検出した日時を表示します。HCP ネームスペースのバージョン管理機能を有効にした場合、オブジェクトのバージョン ID もリストに表示されます。

一覧表示されたオブジェクトを HCP が修復すると、修復されたオブジェクトはリストから削除されます。

[Irreparable Objects] パネルで修復不可能なオブジェクトに確認済みであることを示す目印を付けられます。オブジェクトの行に目印となるチェックマークを付けます。このオプションを使うことで、修復不能になったことを確認したオブジェクトと最近修復不可能になったオブジェクトを区別できます。

保管期間を過ぎてから、削除操作 (オブジェクトが保管期間内の場合は特権削除を使って) を使って修復不可能なオブジェクトを HCP ネームスペースから削除できます。オブジェクトを削除すると、HCP は修復不可能なオブジェクトをリストから削除します。

HCP ネームスペースに修復不可能なオブジェクトが存在しない場合、[Irreparable Objects] パネルのリストは表示されません。

メモ :

修復不可能になったオブジェクトにチェックマークを付けても、HCP ネームスペースからオブジェクトは削除されません。

[Irreparable Objects] パネルの初期表示には、検出したオブジェクトが新しいものから順に 10 個ずつ表示されます。

- 表示するオブジェクト数を変更するには、[Items] フィールドでオブジェクト数を選択してください。
- 前後のページを表示するには、次 () または戻る () のコントロールをクリックしてください。

修復不可能なオブジェクトのリストでオブジェクトを承認する場合、次の操作をしてください。

- [Irreparable Objects] パネルで、承認したいオブジェクトをそれぞれに選択するか、[select all] リンクをクリックして、現在のページで未承認のオブジェクトをすべて選択してください。すべての選択を解除するには、[deselect all] リンクをクリックしてください。
- [Acknowledge Selected] ボタンをクリックしてください。

補足 :

選択されているかどうかに関係なく、1 回の操作ですべてのオブジェクトにチェックマークを付けるには、[Acknowledge All] ボタンをクリックしてください。

3.3 テナントのユーザアカウントを設定する

作成したネームスペースのデータにアクセスするためのユーザアカウントを作成する手順や作成したアカウントの設定を変更する手順を説明します。

3.3.1 アップグレード時の注意事項

HCP システムのバージョンを 4.x から 5.0 以降にアップグレードする場合の注意事項を次に示します。

- バージョン 5.0 ではデータアクセスアカウントが適用されません。
- バージョン 5.0 へアップグレードした場合、データアクセスアカウントはロールのないテナントユーザに割り当てられます。

アップグレードしたときのテナントのユーザアカウントとデータアクセスアカウントの扱いについて次の表に示します。

表 3-1 アップグレード時のテナントのユーザアカウントとデータアクセスアカウントの扱い

ケース	アップグレード前				アップグレード後			ネームスペースにアクセスするために必要な操作
	テナントのユーザアカウント		データアクセスアカウント		テナントのユーザアカウント			
	ユーザ名	ロール	ユーザ名	アクセスを許可されたネームスペース	ユーザ名	ロール	アクセスを許可されたネームスペース	
テナントのユーザアカウントとデータアクセスアカウントが異なるユーザ名の場合	Tntuser	あり	—	—	Tntuser	あり	なし	データアクセスアカウントにロールの付与が必要です。3.3.3 を参照してください。
	—	—	Dauser	あり	Dauser	なし	あり	
テナントのユーザアカウントとデータアクセスアカウントが同じユーザ名の場合	Tntuser	あり	—	—	Tntuser	あり	なし	ユーザ名が重複するため、ユーザアカウントのマージが必要です。(1) を参照してください。
	—	—	Tntuser	あり	Tntuser	なし	あり	
複数のデータアクセスアカウントが同一のネームスペースに割り当てられている場合	Tntuser	あり	—	—	Tntuser	あり	なし	データアクセスアカウントにロールの付与およびネームスペースの割り当てが必要です。3.3.3 を参照してください。
	—	—	Dauser1	あり (同一ネームスペース)	Dauser1	なし	なし	
	—	—	Dauser2		Dauser2	なし	なし	

(1) テナントのユーザアカウントのマージ

HCP システムのバージョンを 4.x から 5.0 以降にアップグレードした場合、テナントのユーザアカウントのユーザ名が重複することがあります。バージョン 5.0 以降へアップグレードしたときは、システム管理コンソールの [Overview] ページの [Major Event] セクションで Username conflict イベントが発生していないか確認してください。

Username conflict イベントが発生していた場合は、ユーザアカウントをマージする必要があります。

ユーザアカウントをマージする手順を次に示します。

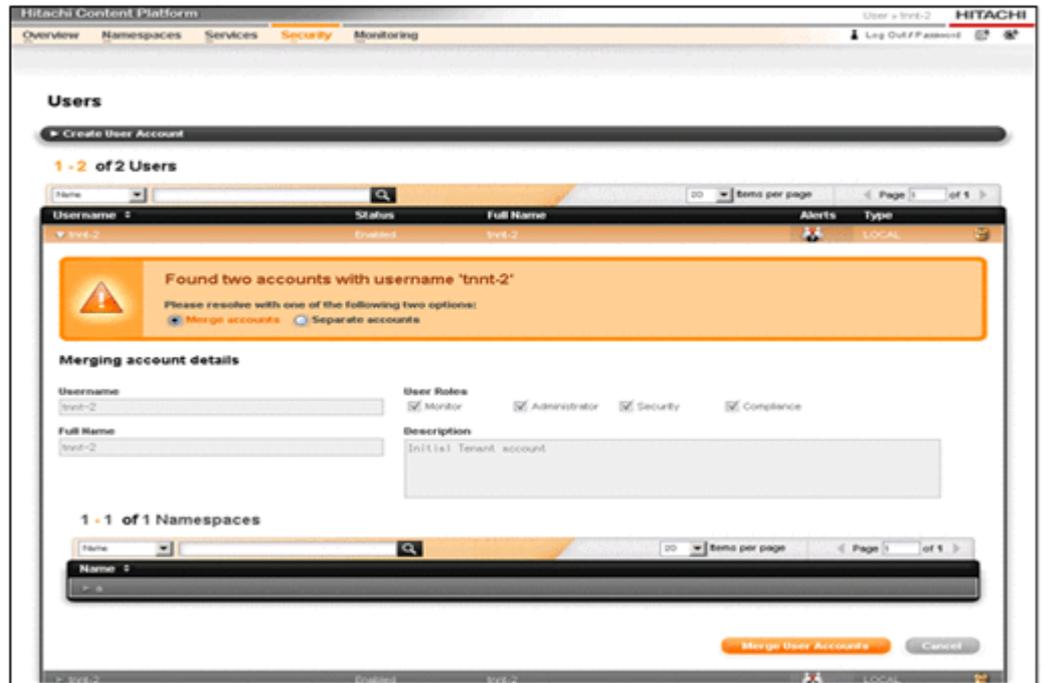
1. システム管理コンソールの [Overview] ページの [Major Event] セクションで Username conflict イベントの行をクリックし、ユーザ名が重複しているテナント名を確認してください。

User	Severity	Date	Event
[internal]	Notice	2/25/2012 5:40午後	Upgrade completed successfully
[internal]	Warning	2/25/2012 5:40午後	Username conflict
[internal]	Warning	2/25/2012 5:40午後	Username conflict
User ID: 1			
Event ID:	3036	Tenant trnt-2 has multiple user accounts with the same username.	
Node:	100		
[internal]	Warning	2/25/2012 5:40午後	Username conflict
[internal]	Error	2/25/2012 1:42午前	Power supply alarm
[internal]	Error	2/25/2012 1:42午前	Power supply alarm
[internal]	Error	2/25/2012 1:42午前	Power supply alarm
[internal]	Error	2/25/2012 1:42午前	Power supply alarm
[internal]	Error	2/25/2012 1:42午前	Power supply alarm
[internal]	Error	2/25/2012 1:42午前	Power supply alarm

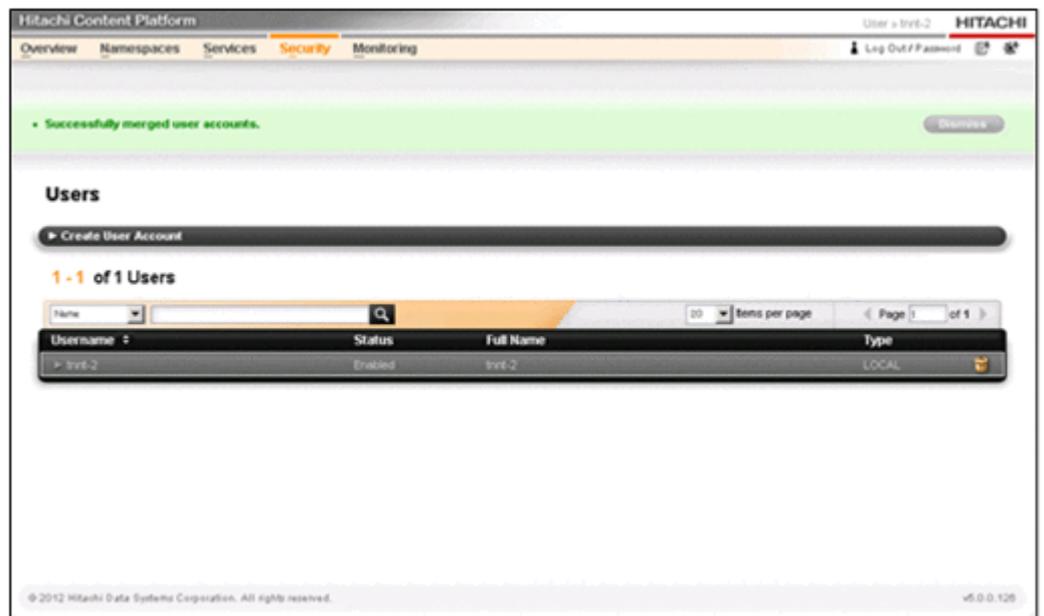
2. ユーザ名が重複しているテナント管理コンソールにログインしてください。
3. トップレベルメニューで [Security] の上にマウスカーソルを置いてセカンダリメニューを表示し、[Users] を選択してください。[Users] ページでは、重複しているユーザの Alerts に重複を示す警告アイコンが表示されています。

Username	Status	Full Name	Alerts	Type
trnt-2	Enabled	trnt-2		LOCAL
trnt-2	Enabled	trnt-2		LOCAL

4. 重複しているユーザアカウントのユーザ名をクリックしてください。
5. [Merge account] をチェックして、[Merge Users account] をクリックしてください。



6. 重複していたユーザがマージされます。



7. マージされたユーザ名をクリックし、ロールとネームスペースの割り当てがアップグレード前と同等になっているか確認してください。

3.3.2 テナントのユーザアカウントにデータアクセス権限を設定する

HVFP でのファイルシステム作成時に対応するネームスペースが作成されている場合は、データアクセス権限がユーザアカウントに設定されるため、この作業は不要です。

HVFP からのアクセス用に、テナント内のすべてのネームスペースにアクセスする権限をユーザアカウントに設定してください。

ユーザアカウントにデータアクセス権限を設定する手順を次に示します。

1. テナント管理コンソールで、[Security] タブを選択してから [Users] をクリックします。

- [Users] ページが表示されます。
2. アクセス権限を設定するユーザを一覧から選択してクリックします。
 3. [Assign Namespace Permissions] をクリックします。
[Find and Select Namespaces] が表示されます。
 4. ネームスペース名の右端の+をクリックして、このユーザでアクセスするネームスペースを選択します。
選択されたネームスペースの背景は緑色になります。
 5. [Assign Data Access Permissions for Selected Namespaces] で必要なアクセス権限のチェックボックスを選択します。
HVFP の場合は、[Browse], [Read], [Write], [Delete] および [Purge] を選択してください。
レプリケーションリンクのプライマリシステムのバージョンが 5.0 以降で、かつレプリカのバージョンが 4.x の場合は [Change Owner] を選択しないでください。
 6. [Assign Namespaces] をクリックします。

3.3.3 テナントのユーザアカウントを変更する

ユーザアカウントに関する任意の情報を変更できます。作業中にユーザアカウントを変更すると変更前の設定で動作を完了します。それ以降の HCP ネームスペースアクセスのリクエストには、新しいアカウントの情報が適用されます。

ユーザアカウントを変更する手順を次に示します。

1. テナント管理コンソールで、[Security] タブを選択してから [Users] をクリックします。
[Users] ページが表示されます。
2. アクセス権限を設定するユーザを一覧から選択してクリックします。
3. [Assign Namespace Permissions] をクリックします。
[Find and Select Namespaces] が表示されます。
4. ネームスペース名の右端の+をクリックして、このユーザでアクセスするネームスペースを選択します。
選択されたネームスペースの背景は緑色になります。
5. [Assign Data Access Permissions for Selected Namespaces] で必要なアクセス権限のチェックボックスを選択し直します。
HVFP の場合は、[Browse], [Read], [Write], [Delete] および [Purge] を選択してください。
レプリケーションリンクのプライマリシステムのバージョンが 5.0 以降で、かつレプリカのバージョンが 4.x の場合は [Change Owner] を選択しないでください。
6. [Assign Namespaces] をクリックします。

3.4 テナント管理コンソールでチャージバックレポートを作成する

テナント管理コンソールでチャージバックレポートを作成できます。チャージバックレポートには、テナントとそのネームスペースに関する現在および過去の統計値が、時間単位で記載されます。

チャージバックレポートはシステムを分析するための優れた情報源であり、ストレージと帯域幅の割り当てを利用パターンに基づいて調整できます。このレポートは、容量と帯域幅の利用状況に応じて費用を決定する請求システムへの入力情報としても役立ちます。

3.4.1 チャージバックレポートについて

チャージバックレポートには、テナントが所有するネームスペースごとに統計値が記載されています。テナントで合計した、ネームスペースの統計値も記載されます。例えば、あるレポート作成期間中のテナントの読み取り総数は、各ネームスペースでその期間中に発生した読み取りが成功した総数です。

チャージバックレポートをテナント管理コンソールで作成した場合、CSV形式となります。レポートの各行には、あるレポート作成期間中の、一つのネームスペースまたは一つのテナントの値が記載されます。

チャージバックレポートの行は、ネームスペース名のアルファベット順に表示されます。テナントの行はレポートの最後です。テナントまたはネームスペースの行が複数の場合、発生した順に表示されます。

チャージバック統計値の収集方法については、「[3.4.3 チャージバック統計値の収集](#)」を参照してください。チャージバックレポートの内容については、「[3.4.4 チャージバックレポートの内容](#)」を参照してください。

ロール：

チャージバックレポートを作成する場合、ユーザアカウントに **Monitor** ロールまたは **Administrator** ロールが必要です。

3.4.2 チャージバックレポートの作成

テナント管理コンソールの [Chargeback] ページでチャージバックレポートを作成します。このページから、1時間または1日単位のレポートを次のとおり作成できます。

- 1時間単位のレポートには、直近の1時間の統計値と、現在時刻まで累積された統計値が記載されます。例えば、2:30:15 p.m.にレポートを要求した場合、1:00:00 p.m.から1:59:59 p.m.の期間で1組の統計値が記載され、また2:00:00 p.m.から2:30:15 p.m.の期間で別の1組の統計値が記載されます。
- 1日単位のレポートには、直近の1日の統計値と、現在日の累積された統計値が記載されます。例えば、10月7日の2:30:15 p.m.にレポートを要求した場合、10月6日の00:00:00から23:59:59の期間で24組の統計値が記載され、また10月7日の00:00:00から2:30:15 p.m.の期間で15組の統計値が記載されます。

補足：

HCP 管理 API を使用すると、さらに長い期間を対象とするチャージレポートを XML, JSON, または CSV 形式で作成できます。これにより、一定間隔でチャージバックレポートを作成して、そのレポートを請求システムに渡すアプリケーションを作成できます。

チャージバックレポートを作成するには

1. テナント管理コンソールの最上位メニューで、[Monitoring] 上にマウスを置いてセカンダリメニューを表示します。
2. セカンダリメニューで、[Chargeback] をクリックします。
3. [Chargeback] ページで、[Hourly Chargeback Report] , [Daily Chargeback Report] または [Monthly Chargeback Report] をクリックして (規定どおり)、レポートをダウンロードするブラウザ固有オプションを選択します。

デフォルトでは、ダウンロードされたレポートファイルの名前は Hourly-Chargeback-Report.csv、Daily-Chargeback-Report.csv または Monthly-Chargeback-Report.csv のどれかです（該当する場合）。

3.4.3 チャージバック統計値の収集

チャージバックの統計値は、ある時点を反映するか、動的に取得されるかのどちらかです。ある時点の統計値はレポート作成期間の最後に取得された測定値です。例えば、ネームスペースの使用済みストレージ容量は1時間の最後に取られた値です。動的な統計値は、長時間累積された測定値（ネームスペースの読み取りまたは書き込みの数など）です。

HCP は、各時間の先頭から始まる1時間を単位に動的な統計値を累積します。このため、ある統計値が、11:00:00 から 11:59:59 に発生したネームスペースへの書き込みが成功した数を表す場合もあれば、12:00:00 から 12:59:59 に発生した同じネームスペースへの書き込みが成功した数を表す場合もあります。

3.4.4 チャージバックレポートの内容

チャージバックレポートの1行目には、次に続く行の値に対する識別子が書かれています。次の表で、それぞれの値について説明します。また、ある時点の値（P）であるか、動的な値（D）であるかを示します。

表 3-2 チャージバックレポートの内容

識別子	タイプ	値
systemName	N/A	次のどちらかです。 <ul style="list-style-type: none"> その行の統計値セットが適用されるネームスペースを所有するテナントを含む HCP システムの DNS 名 その行の集計した統計値セットが適用されるテナントを含む HCP システムの DNS 名
tenantName	N/A	次のどちらかです。 <ul style="list-style-type: none"> その行の統計値セットが適用されるネームスペースを所有するテナントの名前 その行の統計値セットが適用されるテナントの名前
namespaceName	N/A	その行の統計値セットが適用されるネームスペースの名前です。 テナントの統計値が書かれた行では、このフィールドの値はありません。
startTime	N/A	その行の統計値セットに対するレポート作成期間の開始時間。次の形式で書かれています。 yyyy-MM-dd hh:mm:ss hh には 24 時間形式の時間が出力されます。
endTime	N/A	その行の統計値セットに対するレポート作成期間の終了時間。startTime 値に使用された形式と同じ形式で書かれています。
objectCount	P	指定したネームスペースまたは指定したテナントが所有するすべてのネームスペースにあるオブジェクトの総数です。
ingestedVolume	P	指定したネームスペース、または指定したテナントが所有するすべてのネームスペースに追

識別子	タイプ	値
		加される前の、格納済みデータとカスタムメタデータの合計サイズ (バイト単位) です。
storageCapacityUsed	P	指定した名前空間または指定したテナントが所有するすべての名前空間に保存されたデータが占める総バイト数です。これには、オブジェクトデータ、メタデータ、および適切な DPL を満たすために必要な冗長データが含まれます。
bytesIn	D	レポート作成期間中に、指定した名前空間、または指定したテナントが所有するすべての名前空間に書き込みが成功した総バイトです。
bytesOut	D	レポート作成期間中に、指定した名前空間、または指定したテナントが所有するすべての名前空間から読み取りが成功した総バイトです。
reads	D	レポート作成期間中に、指定した名前空間、または指定したテナントが所有するすべての名前空間で実行が成功した読み取り操作の総数です。
writes	D	レポート作成期間中に、指定した名前空間、または指定したテナントが所有する名前空間で実行が成功した書き込み操作の総数です。
deletes	D	レポート作成期間中に、指定した名前空間、または指定したテナントが所有するすべての名前空間で実行が成功した削除およびページ操作の総数です。
deleted	N/A	次のどれかです。 TRUE セットの統計値が収集された後で名前空間が削除されました (名前空間の場合だけ)。 FALSE 現在名前空間またはテナントが存在します。 INCLUDED セットの統計値には、引き続いて削除された一つ以上の名前空間の値が含まれます (テナントの場合だけ)。
valid	N/A	その行の統計値セットの状態です。値は次の可能性があります。 TRUE HCP はそのセットのすべての統計値を正常に収集しました。 FALSE そのセットの統計値は、レポート作成期間中に発生したすべてのアクティビティを反映しているわけではありません。ネットワークに障害が発生した、他のハードウェアに障害が発生した、などの原因が考えられます。

3.5 テナント管理コンソールの警告を確認する

テナント管理コンソールはアイコンを使って、テナントと HCP ネームスペースの状態をテナントの [Overview] ページ, [Namespaces] ページ, および HCP ネームスペースの [Overview] パネルに表示します。これらのグラフィックは警告と呼ばれ、テナントの [Overview] ページとネームスペースの [Overview] パネルにテキストで表示されます。警告が表示されるすべてのページでは、警告の上にマウスを合わせると、テキストが表示されます。

ここでは、コンソールの各ページに表示される警告と、警告に伴って表示されるメッセージの一覧を示します。また、警告が表示された場合の対応方法も説明します。

表 3-3 テナントの [Overview] ページの警告

警告グラフィック	警告文	説明
	Soft quota exceeded	テナントが所有するすべてのネームスペースのストレージの使用量が、テナントで設定されたソフト Quota を超えています。ネームスペースからのオブジェクトの一部削除か、テナントのハード Quota の容量増加を検討してください。
	Tenant with DPL 1 namespaces that are not replicating	テナントは、DPL が [1] で、レプリケーションされていない一つ以上のネームスペースを所有しています。保存したデータが確実に保護されるように、DPL が [1] のすべての HCP ネームスペースをレプリケーションしてください。レプリケーションできない場合は、影響のあるネームスペースの DPL を増やしてください。
	Irreparable objects	表示されたネームスペースが、修復不可能なオブジェクトを含んでいます。HCP システムレベル管理者に連絡してください。どのオブジェクトが修復不可能なのかを確認するには、ネームスペースの [Irreparable Objects] パネルを開いてください。このパネルの詳細は、「3.2.6」を参照してください。

表 3-4 [Namespaces] ページの警告

警告グラフィック	警告文	説明
	Hard quota exceeded	ネームスペースのストレージ使用量が、ネームスペースに設定したハード Quota を超えています。既存オブジェクトの一部削除するか、ハード Quota を増加させるまで、クライアントはネームスペースにデータを追加できません。
	Soft quota exceeded	ネームスペースのストレージ使用量が、ネームスペースに設定したソフト Quota を超えています。ネームスペースからのオブジェクトの一部削除か、ハード Quota 増加を検討してください。

警告グラフィック	警告文	説明
	Irreparable objects found	ネームスペースに修復不可能なオブジェクトがあります。HCP システムレベル管理者に連絡してください。どのオブジェクトが修復不可能なのかを確認するには、ネームスペースの [Irreparable objects] パネルを開いてください。このパネルの詳細は、「3.2.6」を参照してください。

表 3-5 ネームスペースの [Overview] パネルの警告

警告グラフィック	警告文	説明
	Hard quota exceeded	ネームスペースのストレージ使用量が、ネームスペースに設定したハード Quota を超えています。既存オブジェクトを一部削除するか、ハード Quota を増加させるまで、クライアントはネームスペースにデータを追加できません。
	Soft quota exceeded	ネームスペースのストレージ使用量が、ネームスペースに設定したソフト Quota を超えています。ネームスペースからのオブジェクトの一部削除か、ハード Quota 増加を検討してください。
	Irreparable objects	ネームスペースに修復不可能なオブジェクトがあります。HCP システムレベル管理者に連絡してください。どのオブジェクトが修復不可能なのかを確認するには、ネームスペースの [Irreparable objects] パネルを開いてください。このパネルの詳細は、「3.2.6」を参照してください。

レプリケーション機能を使って運用する

レプリケーションとは、二つの HCP システム間でデータを同期させる機能です。レプリケーション機能を使用すると、一方のシステムが停止しても、もう一方のシステムに処理を引き継げるため、連携製品へのデータの提供を継続できます。

オブジェクトが最初に作成された HCP システムをプライマリシステム、コピーされたオブジェクトが保管されている HCP システムをレプリカと呼びます。

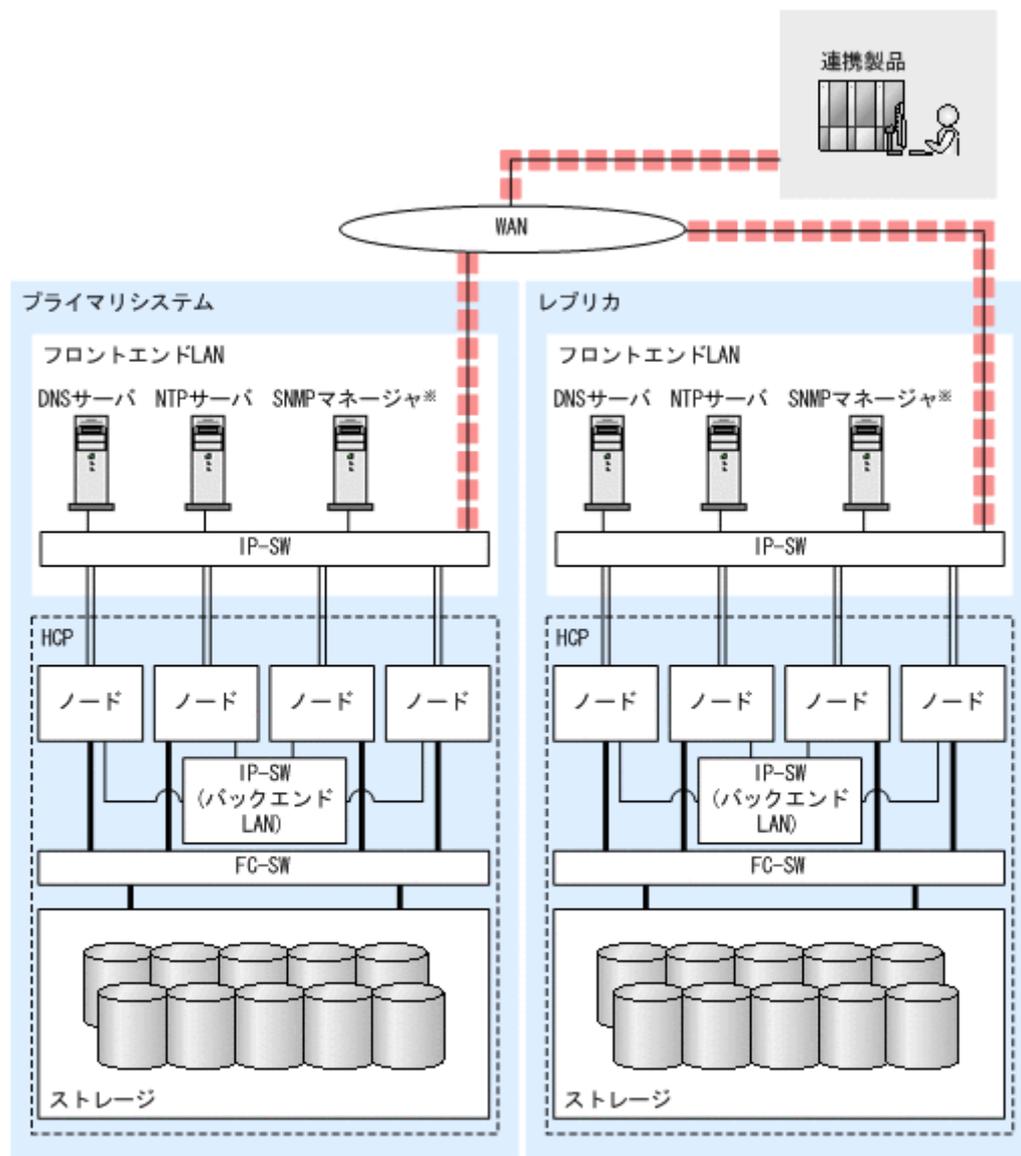
ここでは、レプリケーション機能を使って HCP を運用するときのシステム構成や設定の手順などについて説明します。

- 4.1 システム構成
- 4.2 レプリケーション機能を使用して運用を開始するまでの流れ
- 4.3 レプリケーション機能を使用する場合の事前検討
- 4.4 SSL サーバ証明書の公開鍵のインストール
- 4.5 レプリケーション機能を使用する場合のテナントの作成
- 4.6 レプリケーション機能を使用する場合のネームスペースの作成
- 4.7 レプリケーションリンクを作成する
- 4.8 レプリケーションリンクの受け入れ要求を承認する
- 4.9 レプリケーションリンクの設定を変更する
- 4.10 レプリケーションを一時停止する
- 4.11 レプリカで無効化されたユーザアカウントを再有効化する
- 4.12 バックログの確認
- 4.13 フェイルオーバーとリカバリの管理

4.1 システム構成

ネットワークを介してほかの製品と連携している場合に、レプリケーション機能をサポートします。システム構成について次の図に示します。

図 4-1 レプリケーション機能を使用する場合のシステム構成



(凡例)

■ ■ ■ : NAT, VPNまたはプロキシサーバによるリモートアクセス

注※ 設置は推奨です。

レプリケーションを使用すると、ネットワーク帯域に負荷が掛かるため、同じくフロントエンドLANを使用する連携製品との通信にも、影響を与えるおそれがあります。十分なネットワーク帯域を確保できるよう、フロントエンドLANは慎重に検討してから構築してください。

4.1.1 レプリケーショントポロジ

HCPシステムでは、次のレプリケーション形態を取ることができます。

- 二つのHCPシステム間で一方方向のレプリケーション形態

- ・ 二つの HCP システム間の両方向のレプリケーション形態（双方向レプリケーション）

(1) 多対1のレプリケーション

HCP システムでは、2 対 1 のレプリケーションをサポートしています。二つのプライマリシステムから、一つのレプリカにレプリケーションすることができます。ただし、双方向レプリケーションの場合は 1 対 1 だけです。

2 対 1 のレプリケーションの対象の HCP テナントの名称は、レプリカ上で一意にしてください。例えば、二つのプライマリシステムに **Tenant01** という名称のテナントがそれぞれあると、先にレプリケーションリンクを設定した **Tenant01** だけがレプリケーションされます。



重要 2 対 1 のレプリケーションでは、すべての HCP システムのバージョンが 5.0.1 以上である必要があります。

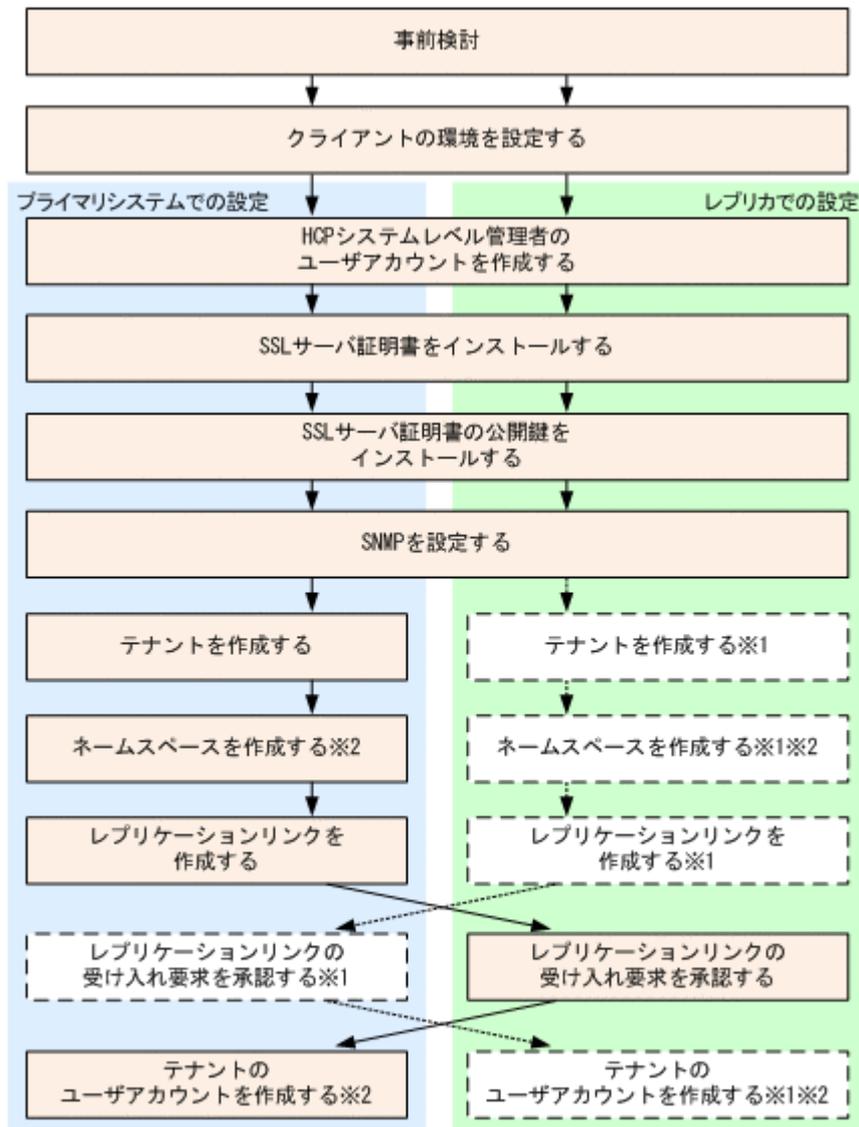
(2) 双方向レプリケーション

HCP システムの任意の 1 組に対して、さまざまな HCP テナントが双方向にレプリケーション設定されていると、それぞれのシステムはプライマリシステムとレプリカの両方の機能を果たすことができます。プライマリシステムおよびレプリカとして同時にサービスをするシステムは、リンクを二つ持っています。一つはアウトバウンドリンク、もう一つはインバウンドリンクです。このトポロジは双方向レプリケーションと呼ばれています。各リンクに対して、選択された HCP テナントとネームスペースは、プライマリシステムでは読み書き可能、レプリカでは読み取り専用です。

4.2 レプリケーション機能を使用して運用を開始するまでの流れ

運用を開始するまでの作業の流れを次に示します。

図 4-2 運用を開始するまでの流れ



注※1：双方向レプリケーション構成にする場合に実施する操作です。この構成にするとき、プライマリシステムは同時にレプリカに、レプリカは同時にプライマリシステムになります。

注※2：HVFPでファイルシステム作成時に、対応するネームスペースが作成されている場合は、この作業は不要です。

HVFP との連携を開始したあとにレプリケーション機能を使用する場合は、システム設定情報ファイルの保存先のネームスペース (system-backup-data) を含むすべてのネームスペースでレプリケーション機能を有効にする必要があります。

作業の詳細について説明している個所を次に示します。なお、作業の手順がレプリケーション機能を使用しない場合と同じときは、レプリケーション機能を使用しない場合の手順を参照先として示しています。

表 4-1 必要な作業の関連ページ

作業	参照先
事前検討	4.3
クライアントの環境を設定する	1.
HCP システムレベル管理者のユーザアカウントを作成する	2.1
SSL サーバ証明書をインストールする	2.2
SSL サーバ証明書の公開鍵をインストールする	4.4

作業	参照先
SNMP を設定する	2.3
テナントを作成する	4.5
ネームスペースを作成する※	4.6
レプリケーションリンクを作成する	4.7.2
レプリケーションリンクの受け入れ要求を承認する	4.8
テナントのユーザアカウントにデータアクセス権限を設定する※	3.3.2

注※

HVFP でのファイルシステム作成時に、対応するネームスペースが作成されている場合は不要な作業です。

4.3 レプリケーション機能を使用する場合の事前検討

設定前に、ユーザの指定が必要な情報を検討しておくことで、効率的に作業を進めることができます。事前に確認が必要な情報を次の表に示します。「表 4-2 事前確認が必要な情報」に確認結果を記録してください。

表 4-2 事前確認が必要な情報

確認対象	項目	入力値	入力値の条件	確認結果を必要とする作業
HCP	HCP システムの DNS 名		インストール時に設定された DNS 名を入力する。	1.2 2.2
HVFP※	HVFP の管理サーバの IP アドレスまたはホスト名		—	1.2
	HVFP で管理している Physical Node の管理ポートの固有 IP アドレス		—	1.2
	HVFP で管理している Physical Node の管理ポートの仮想 IP アドレス		—	1.2

(凡例) — : なし

注※ HVFP と連携している場合に確認が必要です。

また、設定前に、ユーザの指定が必要な情報を検討しておくことで、効率的に作業を進めることができます。「表 4-3 設定時にユーザの指定が必要な情報」に検討結果を記録してください。なお、設定時には、このマニュアルで説明されている項目以外は、デフォルト値のまま変更しないでください。

表 4-3 設定時にユーザの指定が必要な情報

項目		入力値	入力できる文字の種類	入力できる文字数	入力値の条件	確認結果を必要とする作業
デフォルトユーザのユーザアカウント	新しいパスワード		ASCII 印字可能文字	6~64 文字	<ul style="list-style-type: none"> 英字, 数字, 記号の 3 種類のうち, 2 種類以上の文字を組み合わせて指定する。 大文字と小文字は区別される。 	2.1.3
HCP システムレベル管理者のユーザアカウント	ユーザ名		ASCII 印字可能文字	1~64 文字	<ul style="list-style-type: none"> 大文字と小文字は区別されない。 先頭の文字に開き角括弧 ([) は使用できない。 	2.1.3
	氏名		ASCII 印字可能文字	1~64 文字	<ul style="list-style-type: none"> 大文字と小文字は区別されない。 	
	パスワード		ASCII 印字可能文字	6~64 文字	<ul style="list-style-type: none"> 英字, 数字, 記号の 3 種類のうち, 2 種類以上の文字を組み合わせて指定する。 大文字と小文字は区別される。 	
システム管理コンソールへのアクセス	アクセスを許可する IP アドレス		IPv4 に準ずる	IPv4 に準ずる	—	2.1.3
	アクセスを拒否する IP アドレス		IPv4 に準ずる	IPv4 に準ずる	—	
SNMP の設定 (任意)	コミュニティ名		ASCII 印字可能文字	1~32 文字	<ul style="list-style-type: none"> 大文字と小文字は区別される。 	2.3
	SNMP を経由したアクセスを許可する IP アドレス		IPv4 に準ずる	IPv4 に準ずる	—	
	SNMP を経由したアクセスを拒否する IP アドレス		IPv4 に準ずる	IPv4 に準ずる	—	
	SNMP マネージャの IP アドレス		IPv4 に準ずる	IPv4 に準ずる	—	
テナント	テナント名		英数字およびハイフン (-)	1~63 文字	<ul style="list-style-type: none"> 大文字と小文字は区別されない。 次の文字列は予約済みのため使用できない。 「admin」, 「default」, 「search」, 「www」 	1.2 3.1

項目	入力値	入力できる文字の種類	入力できる文字数	入力値の条件	確認結果を必要とする作業
				<ul style="list-style-type: none"> HCP システム内でユニークなテナント名とする。 ハイフン (-) で始まる, またはハイフン (-) で終わる名称は付けられない。 	
	ハード Quota	数字およびピリオド (.)	1GB～HCP システム全体の容量の上限	<ul style="list-style-type: none"> 単位で [GB] を選択した場合の最小値は 1, [TB] を選択した場合の最小値は 0.01。 	3.1
	ネームスペース Quota	半角数字	1～2000	<ul style="list-style-type: none"> HCP システムでユーザが作成できるネームスペース数の上限値は 2000 であるため, HCP システム全体で 2000 を超えないように指定する。 	
テナントレベル管理者のユーザアカウント	ユーザ名	ASCII 印字可能文字	1～64 文字	<ul style="list-style-type: none"> 大文字と小文字は区別されない。 先頭の文字に開き角括弧 ([]) は使用できない。 	3.1
	パスワード	ASCII 印字可能文字	6～64 文字	<ul style="list-style-type: none"> 英字, 数字, 記号の 3 種類のうち, 2 種類以上の文字を組み合わせて指定する。 大文字と小文字は区別される。 	
	新しいパスワード	ASCII 印字可能文字	6～64 文字	<ul style="list-style-type: none"> 英字, 数字, 記号の 3 種類のうち, 2 種類以上の文字を組み合わせて指定する。 大文字と小文字は区別される。 	
	氏名	ASCII 印字可能文字	1～64 文字	<ul style="list-style-type: none"> 大文字と小文字は区別されない。 	
テナント管理コンソールへのアクセス	アクセスを許可する IP アドレス	IPv4 に準ずる	IPv4 に準ずる	—	3.1
	アクセスを拒否する IP アドレス	IPv4 に準ずる	IPv4 に準ずる	—	
ネームスペース※	ネームスペース名	英数字およびハイフン (-)	1～63 文字	<ul style="list-style-type: none"> 大文字と小文字は区別されない。 	3.2

項目	入力値	入力できる文字の種類	入力できる文字数	入力値の条件	確認結果を必要とする作業	
				<ul style="list-style-type: none"> HCP システム内でユニークなネームスペース名とする。 ハイフン (-) で始まる, またはハイフン (-) で終わる名称は付けられない。 		
	ハード Quota	数字およびピリオド (.)	1GB~テナントのハード Quota の容量	<ul style="list-style-type: none"> 単位で [GB] を選択した場合の最小値は 1, [TB] を選択した場合の最小値は 0.01。 		
	古いバージョンのオブジェクトの保管日数	数字	0~36,500 日	—		
HTTP プロトコルを使ったネームスペースへのアクセス※	アクセスを許可する IP アドレス		IPv4 に準ずる	IPv4 に準ずる	—	3.2
	アクセスを拒否する IP アドレス		IPv4 に準ずる	IPv4 に準ずる	—	
テナントのユーザアカウント※	ユーザ名		ASCII 印字可能文字	1~64 文字	<ul style="list-style-type: none"> 大文字と小文字は区別されない。 先頭の文字に開き角括弧 ([]) は使用できない。 	3.3.2
	パスワード		ASCII 印字可能文字	6~64 文字	<ul style="list-style-type: none"> 英字, 数字, 記号の 3 種類のうち, 2 種類以上の文字を組み合わせて指定する。 大文字と小文字は区別される 	
レプリケーションリンク	レプリケーションリンク名		ASCII 印字可能文字	1~64 文字	<ul style="list-style-type: none"> 大文字と小文字は区別されない。 	4.7.2
	レプリカのホスト名 (FQDN)		ホスト名に使用できる文字	ホスト名に使用できる文字数	<ul style="list-style-type: none"> 連携する HVFP が 3.2.1-00 より前のバージョンの場合は, ホスト名は次の形式とする。 replication-〈プライマリシステムのドメイン名〉 	4.7.2
	レプリケーションの性能レベル		ドロップダウンリストで選択	—	次のどれかから選択する。 <ul style="list-style-type: none"> [Low] [Medium] [High] [Use Schedule] 	4.7.2

項目		入力値	入力できる文字の種類	入力できる文字数	入力値の条件	確認結果を必要とする作業
ネットワークアドレス変換 (NAT) 使用時の設定 (任意)	レプリカがプライマリシステムからデータを受け取るためのポート		数字	1~5 文字	—	4.7.2
	プライマリシステムの IP アドレス		IPv4 に準ずる	IPv4 に準ずる	—	4.7.2
	プライマリシステムがレプリカからのデータを受け取るためのポート		数字	1~5 文字	—	4.7.2

(凡例)

— : なし

注※

HVFP でのファイルシステム作成時に、対応するネームスペースが作成されている場合は、ユーザの指定が不要な項目です。

なお、次に示す項目は、HCP システムレベル管理者の権限で設定できません。設定を変更する必要がある場合は、お問い合わせ先まで連絡してください。

DNS 設定

- システム名 (DNS 名)

ネットワーク設定

- デフォルトゲートウェイ
- フロントエンド LAN の MTU 値
- 各ノードのフロントエンド LAN の IP アドレス
- 各ノードのバックエンド LAN の IP アドレス

時間設定

- タイムゾーン

4.4 SSL サーバ証明書の公開鍵のインストール

レプリケーション機能を使って運用する

93

4.4.1 公開鍵のダウンロード

4.4.2 公開鍵のアップロード

94

レプリケーション機能を使って運用する



4.5 レプリケーション機能を使用する場合のテナントの作成

レプリケーション機能を使用するには、テナントを複製できるように設定しておく必要があります。テナント作成時に、[Create Tenant] パネルの [Replication] オプションのチェックボックスを選択してください。テナントを作成する手順については、「3.1 テナントを管理する」を参照してください。

4.6 レプリケーション機能を使用する場合のネームスペースの作成

レプリケーション機能を使用するには、ネームスペースを複製できるように設定しておく必要があります。ネームスペース作成時に、[Create Namespaces] パネルの [Replication] フィールドで、[On] を選択してください。ネームスペースを作成する手順については、「3.2 ネームスペースを管理する」を参照してください。

HVFP でのファイルシステム作成時に、対応するネームスペースが作成されている場合はこの操作は不要です。なお、作成されるネームスペースの名称は「<ファイルシステム名>-<システムが自動で付与する HVFP ごとの ID >」となります。

4.7 レプリケーションリンクを作成する

レプリケーション機能を使用するために、プライマリシステムでレプリケーションリンクを作成します。レプリケーションリンクの作成について説明します。

4.7.1 レプリケーションリンクを作成するときの考慮点

レプリケーションリンクの作成には、次の点を考慮する必要があります。

- レプリケーションリンクを作成する前に、プライマリシステムに次の少なくとも一つが存在する必要があります。
 - レプリケーションする HCP テナント
 - カスケードレプリケーションに設定するインバウンドのレプリケーションリンク
- 同じ名前のテナントがレプリカにすでに存在している場合は、レプリケーションリンクに HCP テナントを設定できません。この問題に対処するには、プライマリシステムまたはレプリカのどちらかのテナント名を変更してください。
- 同じ名前のディレクトリがレプリカにすでに存在している場合は、レプリケーションリンクにデフォルトネームスペースのディレクトリを設定できません。
- レプリカで既存のテナントと同じ名前の HCP テナントがインバウンドリンクに設定されている場合は、レプリケーションリンクにインバウンドリンクを設定できません。
- システムレベルのユーザに HCP テナントへアクセスする権限がある場合だけ、HCP テナントに対してどのネームスペースをレプリケーションするかを選択できます。
- HCP テナントが所有するネームスペースのどれかに、レプリカがサポートする設定より高い明示的な DPL が設定されている場合、このネームスペースをレプリケーションリンクに設定でき

ません。テナントへの管理アクセス権限がないためにこれらのネームスペースを除外できない場合、レプリケーションリンクにテナントを設定できません。

- レプリケーションリンクのプライマリシステムのバージョンが 4.x で、かつレプリカのバージョンが 4.0 より前である場合、次の制限があります。
 - リンクに設定された各 HCP テナントが所有するすべてのネームスペースが、レプリケーション対象に自動的に選択される。
 - DPL 設定が **Dynamic** (動的) のネームスペースを所有する HCP テナントに、レプリケーションリンクを設定することができない。
 - リンクに設定された HCP ネームスペースの DPL を、レプリケーションを開始した後で変更することができない。
- レプリケーションリンクのプライマリシステムのバージョンが 5.0 以降で、かつレプリカのバージョンが 4.x の場合は、テナントのユーザアカウントに [Change Owner] のアクセス権限を付与しないでください。
- HCP テナントレベルのユーザがレプリケーションの詳細情報を参照しない場合は、レプリケーションリンクを作成する前に、この情報を表示するオプションが選択解除されていることを確認してください。

4.7.2 レプリケーションリンクの作成

レプリケーション機能を使用するために、プライマリシステムでレプリケーションリンクを作成し、レプリカ側にレプリケーションリンクを受け入れるよう要求します。レプリケーションリンクとは、HCP のサービスがレプリケーションを実行するために使用する、プライマリシステムとレプリカの情報のことです。

ここでは、プライマリシステムでレプリケーションリンクを作成する手順を説明します。なお、レプリケーションで複製したテナントに対して、レプリケーション対象から除外、またはレプリケーションリンクを削除すると、レプリケーションで再度複製できません。レプリケーションで複製したテナントに対してこれらの操作が必要な場合は、お問い合わせ先に連絡してください。

1. プライマリシステムのシステム管理コンソールで、[Services] にマウスカーソルを置くと表示されるメニューから、[Replication] を選択します。
[Replication] ページが表示されます。
2. [Replication] ページで、[Create Link] をクリックします。
[Create Link] パネルが表示されます。
3. [Create Link] パネルで、次の内容を設定します。次の内容以外はデフォルトのままとしてください。
 - [Link Name] フィールドに、リンク名を指定してください。
 - [Replica Addresses] フィールドに、レプリカのホスト名 (FQDN) を指定してください。
 - [Link Type] で、[Outbound] を選択してください。
 - [Compress data] オプションのチェックボックスが、選択されていないことを確認してください。
 - [Encrypt data] オプションのチェックボックスが、選択されていないことを確認してください。
 - [Performance Level] フィールドで、レプリケーションリンクの性能レベルを指定します。指定した性能レベルによって、各ノードで実行できるレプリケーションスレッドの数が次のとおりに制御されます。
 - [Low] : 1 スレッド

- [Medium] : 5 スレッド
 - [High] : 10 スレッド
 - [Use Schedule] : 性能レベルをスケジュール化して設定
- また, [Use Schedule] を指定した場合は, レプリケーションリンクにスケジュールを設定する必要があります。スケジュールを設定する手順については, 「[4.9.3 レプリケーションリンクのスケジュールの設定](#)」を参照してください。
- [Replication Priority] フィールドで, [Oldest Object First] が選択されていることを確認してください。
 - [Tenants] タブで, レプリケーションリンクの対象となるテナントを設定してください。
4. ネットワークアドレス変換 (NAT) を使用する場合, [Advanced Configuration] リンクをクリックして, 次の内容を設定します。
 - [Replica Port] フィールドに, レプリカがプライマリシステムからデータを受け取るためのポートを指定してください。
 - [Local Addresses] フィールドに, プライマリシステムの IP アドレスを指定してください。
 - [Local Port] フィールドに, プライマリシステムがレプリカからのデータを受け取るためのポートを指定してください。
 5. [Create Link] ボタンをクリックします。
レプリケーションリンクが作成され, レプリカにレプリケーションリンクの受け入れ要求が送信されます。

4.8 レプリケーションリンクの受け入れ要求を承認する

プライマリシステムから送信された, レプリケーションリンクの受け入れ要求をレプリカで承認すると, レプリケーションを開始できるようになります。レプリカで, レプリケーションリンクの受け入れ要求を承認する手順を説明します。

1. システム管理コンソールで, [Overview] を選択します。
[Overview] ページが表示されます。
2. [Overview] ページの [Alerts] セクションで, 保留中のリンク要求を示す警告の隣にあるリンクをクリックします。
3. レプリケーションリンクの一覧で, [Pending] のリンク要求をクリックします。
4. 開いたパネルの左側にある, [Configuration] をクリックします。
[Configuration] パネルが表示されます。
5. リンク設定を確認します。
6. [Accept Link] ボタンをクリックします。
プライマリシステムにリンクを受け入れた旨のメッセージが送信され, レプリケーションが開始されます。

4.9 レプリケーションリンクの設定を変更する

レプリケーションリンクの設定は, プライマリシステムまたはレプリカのどちらのシステム管理コンソールからでも, いつでも参照できます。ここでは, レプリケーションリンクの設定の変更について説明します。

4.9.1 リンク設定の変更時の留意事項

レプリケーションリンクの作成時の留意事項のほとんどは、リンク設定の変更時にも当てはまりません。リンクを設定する場合は、さらに次の留意事項があります。

- リンク方向（アウトバウンドまたはインバウンド）を除いて、リンクのプロパティはどれでも変更できます。
- どちらかのシステムの DNS 名または IP アドレスを変更する場合、新しい DNS 名または IP アドレスは同じシステムを特定する必要があります。これが当てはまらないのは、新しいシステムまたは再構成したシステムにリンクをリストアする前に、リンクを再設定している場合です。
- どちらかのシステムのポートを変更できるのは、新しいシステムまたは再作成したシステムにリンクを保存する前にそのリンクを再設定するときだけです。
- リンクがレプリカにフェイルオーバーされている間を除いて、HCP テナントをいつでもリンクから追加したり削除したりできます。

重要：

レプリケーションリンクからいったん削除したテナントまたはディレクトリを再追加するためには、リンクから削除したテナントまたはディレクトリをレプリカからも削除する必要があります。これは、現在そのディレクトリまたはテナントが、プライマリシステムとレプリカの両方に存在しているため、同じ名前でのレプリケーションができないからです。この場合、リンクを作成する場合とは異なり、プライマリシステムまたはレプリカのテナントの名前を変更しても解決しません。二つのテナントが同じ内部 ID を持っているためです。

- HCP ネームスペースのリンクへの追加はいつでもできます。HCP ネームスペースのリンクからの削除は、リンクがレプリカにフェイルオーバーされている間を除いて、いつでもできます。
- リンクに設定された HCP ネームスペースの DPL が、レプリカでサポートされていない明示的な DPL に変更された場合、ネームスペースを所有するテナントのレプリケーションは自動的に一時停止されます。この状況から回復するには、テナントの管理者に、レプリカがサポートする値（または Dynamic（動的））に DPL を変更してもらってください。次にテナントのレプリケーションを再開してください。
- リンク設定を更新している間、HCP システムは一時的にリンクの処理を中断します。

4.9.2 レプリケーションリンクの設定の変更

レプリケーションリンクの設定を変更する手順を次に示します。

1. システム管理コンソールのトップレベルメニューで、[Services] の上にマウスマウスカーソルを置いてセカンダリメニューを表示します。
2. セカンダリメニューで、[Replication] をクリックしてください。
[Replication] ページが表示されます。
3. [Replication] ページで、修正するリンクの名前をクリックしてください。
4. 開いたパネルの左側にある [Configuration] をクリックしてください。
[Configuration] パネルが表示されます。
5. [Configuration] パネルで、必要な変更を行ってください。
リンク名、相手のシステムの識別子、圧縮と暗号化のオプション、性能レベル、またはレプリケーションの優先順位を変更するには、[Link Settings] をクリックしてください。
6. [Update Link] ボタンをクリックしてください。

HCP テナント、デフォルトネームスペースのディレクトリ、またはインバウンドリンクを選択解除する場合、コンソールに確認メッセージが表示されます。

7. 確認メッセージが表示された画面で、チェックボックスをクリックしてアクションの結果を確認し、[Update Link] ボタンをクリックしてください。

HCP は現在行っているレプリケーション、または、データリカバリを停止し、リンク設定を変更します。変更が完了すると、リンクの処理が以前の状態に戻ります。

メモ：

- プライマリシステムでリンクを変更する場合、[Advanced Configuration] セクションのフィールドラベルは、順に [Replica Port], [Primary Addresses], [Primary Port] です。
- レプリカでリンクを変更する場合、[Source Addresses] フィールドラベルは [Primary Addresses] に置き換わり、[Advanced Configuration] セクションのフィールドラベルは、順に [Primary Port], [Replica Addresses], [Replica Port] です。
- デフォルトネームスペースに多くの最上位ディレクトリがある場合、[Default Namespace] タブをクリックすると、コンソールの表示に時間が掛かることがあります。同様に、多くの最上位ディレクトリがあるインバウンドリンクを展開すると、コンソールの表示に時間が掛かる場合があります。

4.9.3 レプリケーションリンクのスケジュールの設定

[Create Link] パネルの [Performance Level] フィールドで [Use Schedule] を指定した場合、性能レベルはスケジュールに従って、設定された時間になると自動的に変更されます。スケジュールは、[Replication] ページの [Schedule] パネルで1週間単位（日曜日から土曜日）で設定します。デフォルトでは、1週間全体の性能レベルが [Medium] です。

リンクのスケジュールを変更する手順を説明します。

1. HCP システム管理コンソールで、[Services] にマウスを置くと表示されるメニューから、[Replication] を選択します。
[Replication] ページが表示されます。
2. [Replication] ページで、リンク一覧のリンク名をクリックします。
レプリケーションリンクのパネルが表示されます。
3. パネルの左側で、[Schedule] をクリックします。
パネルにスケジュールの設定画面が表示されます。
4. 1週間全体に性能レベルを設定する場合、スケジュールの設定に必要な回数だけ次の手順を実行します。
 - a. [All] の上にマウスを置いて、性能レベルの一覧を表示します。
 - b. 設定する性能レベルをクリックします。
5. 曜日単位に性能レベルを設定する場合、スケジュールの設定に必要な回数だけ次の手順を実行します。
 - a. 曜日の名前の上にマウスを置いて、性能レベルの一覧を表示します。
 - b. 設定する性能レベルをクリックします。
6. 時間単位または指定した時間の範囲に性能レベルを設定する場合、スケジュールの設定に必要な回数だけ次の手順を実行します。
 - a. 性能レベルを設定する時間をクリックします。または、性能レベルを設定する時間の範囲を指定するために、時間をクリックして同じ日の別の時間までドラッグします。
[Set Performance Level] ウィンドウが開きます。

性能レベルを設定する時間の範囲を指定するときに、その日の最後の時間を含めるためには、時間の端まで正確にドラッグする必要があります。より簡単に設定するときは、以前の時間までドラッグして、[Set Performance Level] ウィンドウで最後の時間をリセットします。

- b. 必要に応じて、[Start time] と [End time] のフィールドで開始時間と終了時間を選択します。
 - c. [Level] フィールドで、設定する性能レベルを選択します。
 - d. [Submit] ボタンをクリックします。
7. [Update Schedule] ボタンをクリックします。

4.10 レプリケーションを一時停止する

ここでは、レプリケーションを一時停止する手順を説明します。この操作は、HCP をアップグレードする際に必要です。

1. プライマリシステムのシステム管理コンソールで、[Services] にマウスカーソルを置くと表示されるメニューから、[Replication] を選択します。
[Replication] ページが表示されます。
2. [Replication] ページで、処理を中断するリンク名をクリックします。
3. 開いたパネルの左側にある、[Management] をクリックします。
[Management] パネルが表示されます。
4. [Management] パネルで、[Suspend] ボタンをクリックします。
レプリケーションが一時停止します。
5. アップグレード後、レプリケーションを再開する場合は、同じ [Management] パネルで、[Resume] ボタンをクリックします。

注意：

レプリケーションリンクの状態表示を更新する場合、Web ブラウザのリフレッシュ機能を使用して更新しないでください。画面を更新する場合は、[Services] にマウスカーソルを置くと表示されるメニューから、[Replication] を再度選択してください。

4.11 レプリカで無効化されたユーザアカウントを再有効化する

HCP テナントの場合、テナントレベルのユーザアカウントはレプリケーションされるため、レプリカで使用できます。連続してログイン試行が失敗したことによって、アカウントがレプリカで無効になると、そのテナントは読み取り専用であるため、レプリカで再有効化できません。

ここでは、レプリカで無効化されたテナントレベルのユーザアカウントを再有効化する方法を説明します。

レプリカで無効化されているテナントレベルのユーザアカウントを再有効化するには、プライマリシステムの該当するテナントのテナント管理コンソールで、次の手順を実行してください。

1. 最上位メニューで、[Security] 上にマウスを置いてセカンダリメニューを表示してください。
2. セカンダリメニューで、[Users] をクリックしてください。
3. [Users] ページのユーザアカウント一覧で、変更するアカウントの編集コントロール (✎) をクリックしてください。

4. [Update User Account] ボタンをクリックしてください。
5. 更新されたアカウントがレプリケーションされるまで待ってください。アカウントがレプリケーションされると、レプリカで有効になります。

4.12 バックログの確認

アウトバウンドまたはインバウンドの任意のレプリケーションリンクに対して、リンクに設定されたテナントごとに、レプリケーションのステータスとバックログ時間を監視できます。バックログ時間は次の時間の差です。

- レプリケーションまたはリカバリがまだ行われていないオブジェクトと設定の変更に対する、最も前の変更時間（該当する場合）
- 現在の時間

テナントのステータスとバックログの情報を参照する手順を次に示します。

1. HCP システム管理コンソールの最上位メニューで、[Services] 上にマウスを置いてセカンダリメニューを表示してください。
2. セカンダリメニューで、[Replication] をクリックしてください。
[Replication] ページが表示されます。
3. [Replication] ページで、リンク一覧のリンクをクリックしてください。
4. 開いたパネルの左側で、[Tenants] をクリックしてください。
[Tenants] パネルが表示されます。
5. [Tenants] パネルのいちばん上に、[Overview] パネルの上部に表示される情報と同じ情報が表示されます。

リンクモードの場合、またはアウトバウンドリンクだけの場合は、[Objects pending] (HCP ネームスペースで保留中のオブジェクトの概数)、[Data pending] (HCP ネームスペースで保留中のデータの概算量)、および [Backlog time] (バックログ時間) が表示されます。

4.12.1 テナントのレプリケーション情報

[Tenants] パネルに、レプリケーションリンクに設定されたテナントの一覧が表示されます。デフォルトテナントのディレクトリがリンクに設定されている場合はデフォルトテナントを含みません。この一覧には、テナントごとに次の情報が表示されます。

- [Tenant Name] : テナント名
- テナントが所有するレプリケーション中のネームスペースに対する平均的なバックログ時間を示す進ちょくバーと、進ちょく時間（日単位の数値または時間単位（日より短い場合）の数値）。進ちょくバーの長さは 30 日を表し、右端が現在の時間です。
デフォルトテナントの場合、リンクに設定されたディレクトリの平均バックログ時間です。

補足：

- 幾つかのテナントにほかのテナントに比べてかなり大きなバックログがある場合、リンクのレプリケーション優先度を [Oldest Object First] に設定して、バックログを削減してください。
- 一つ以上のテナントでバックログ時間が常に増えている場合、レプリケーションの性能レベルを [High] に設定します。この設定を行っても、システムの処理能力をさらに高めたり（例えば、ノードの追加）、プライマリシステムとレプリカ間の帯域幅を増やしたりすることが必要となることがあります。

- ・ テナントがカスケードレプリケーションに含まれる場合は、が表示されます。
- ・ テナントの現在のレプリケーションステータスを示すアイコンの一覧を次の表に示します。

表 4-4 レプリケーションステータスを示すアイコン

アイコン	説明
	アイコンがアニメーション表示されている場合、テナントのレプリケーションまたはリカバリは正常に処理中です。アイコンが静止している場合、レプリケーションリンクのすべての処理が一時停止されました。
	テナントのレプリケーションは一時停止されました。
	テナントのレプリケーションは自動的に一時停止されました。このアイコンの上にマウスを置くと、テナントのレプリケーションが一時停止された理由がコンソールに表示されます。

4.12.2 テナントのレプリケーションの詳細情報

テナントのレプリケーションの詳細情報を参照するには、[Tenants] パネルの一覧にあるテナント名をクリックしてください。表示される情報は次のとおりです。

- ・ [Minimum backlog] : テナントが所有するネームスペースの中で最も短いバックログ時間。この時間は日単位または時間単位（日より短い場合）で表示されます。
デフォルトテナントの場合、レプリケーションリンクに設定されたディレクトリの中で最も短いバックログ時間です。
- ・ [Maximum backlog] : テナントが所有するネームスペースの中で最も長いバックログ時間。この時間は日単位または時間単位（日より短い場合）で表示されます。
デフォルトテナントの場合、レプリケーションリンクに設定されたディレクトリの中で最も長いバックログ時間です。
- ・ [Objects pending] : テナントが所有するネームスペースで現在レプリケーションを待っているオブジェクト数。この値はアウトバウンドリンクにある HCP テナントの場合だけ表示されます。
- ・ [Data pending] : テナントが所有するネームスペースで現在レプリケーションを待っているデータ量。この値はアウトバウンドリンクにある HCP テナントの場合だけ表示されます。

4.13 フェイルオーバーとリカバリの管理

レプリケーションペアのプライマリシステムが壊滅的に破損した場合、レプリケーションされたコンテンツをレプリカから読み取ることができるように、プライマリシステムのクライアントに指示できます。ただし、レプリカにレプリケーションされた HCP のテナントとネームスペースおよびデフォルトネームスペースディレクトリは読み取り専用のままです。そのため、クライアントはレプリケーションされたコンテンツを変更できません。

レプリカにレプリケーションされたエントリにクライアントが書き込みできるようにするには、手動でレプリケーションリンクをレプリカにフェイルオーバーする必要があります。リンクをフェイルオーバーすると、レプリケーションされたエントリはレプリカで読み書き可能になります。

プライマリシステムが修復または再構築された後に、リンクをリストアしてデータリカバリを起動する必要があります。データリカバリがほぼ終了したときに、最終リカバリ処理を明示的に起動する必要があります。

障害が発生したシステムがレプリカであった場合、該当するテナントとディレクトリはプライマリシステムでは読み書き可能のままであるため、フェイルオーバーする必要はありません。レプリカが修復または再構築された後に、リンクをリストアする必要があります。これを実行すると、レプリケーションは自動的に再開します。

ロール：レプリケーションリンクのフェイルオーバー、リンクのリストア、またはレプリケーションされたデータのリカバリを行うには、ユーザアカウントに Administrator ロールが必要です。

4.13.1 リンクのリストア

レプリケーションリンクをリストアさせる前に、プライマリシステムとレプリカの両方に SSL サーバ証明書をインストールして、公開鍵を交換してください。SSL 設定については、[4.4 SSL サーバ証明書の公開鍵のインストール](#)を参照してください。

システム障害の後にレプリケーションリンクをリストアする手順を次に示します。

1. 該当するプライマリシステムまたはレプリカのシステム管理コンソールのトップレベルメニューで、[Services] の上にマウスカーソルを置いてセカンダリメニューを表示します。
2. セカンダリメニューで、[Replication] をクリックしてください。
[Replication] ページが表示されます。
3. [Replication] ページで、リストアするリンクの名前をクリックしてください。
4. 必要に応じて、リンクの設定を更新します。この処理は、もう一方のシステムの DNS 名または IP アドレスが変更された場合にだけ実行してください。
リンク設定の更新の手順については、「[4.9.1 リンク設定の変更時の留意事項](#)」を参照してください。
5. パネルの左側にある [Advanced] をクリックしてください。
[Advanced] パネルが表示されます。
6. [Advanced] パネルで、[Restore Link] ボタンをクリックしてください。

メモ：

[Restore Link] ボタンが表示されない場合は、数分待ってください。次のことを HCP が確認するため、表示に時間が掛かります。

- もう一方のシステムが使用可能になっていること
- そのシステムに必要な SSL 証明書がインストールされていること
- 既存のリンク

ペンディングリンク要求がほかのシステムに発行されます。リンク作成のために最初に要求したのと同様にこれに応答してください。リンク要求に応答することについての詳細は、[4.8 レプリケーションリンクの受け入れ要求を承認する](#)を参照してください。

相手のシステムがリンクを受け入れた場合は、次のとおりです。

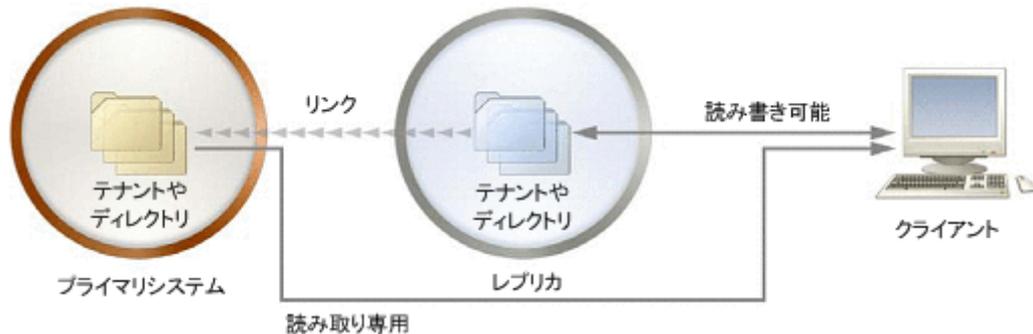
- ・ 該当システムがプライマリシステムの場合、リンクは [Suspended] (一時停止) 状態で再作成され、データリカバリを開始する必要があります。
- ・ 該当システムがレプリカである場合、リンクが受け入れられたときにレプリケーションが自動的に再開します。

4.13.2 リカバリ

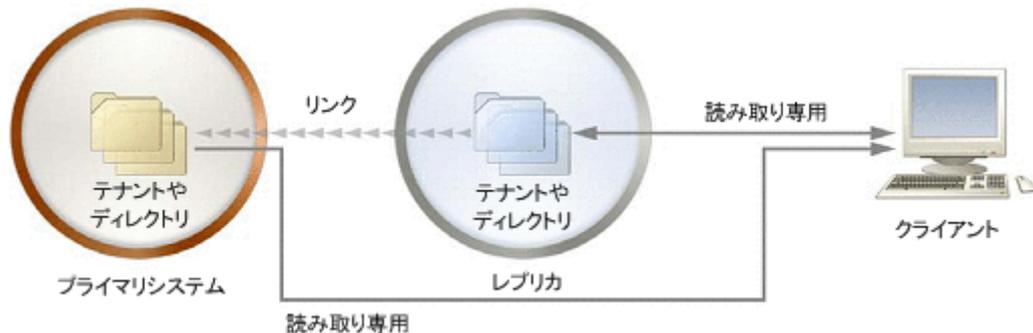
レプリケーションを行っている HCP システムに障害が発生した場合、システムを再インストールして構成を設定し直し、その後、障害が発生した HCP システムでリンクを再設定してください。

これによって、オブジェクト、HCP のテナントとネームスペースの設定情報、およびその他のデータをレプリカからリカバリするプロセスを開始できます。

リカバリ処理の前半では、クライアントから見て、プライマリシステムのテナントやディレクトリは読み取り専用であり、レプリカの対応するテナントやディレクトリは読み書き可能のままになります。リカバリ処理中、クライアントは書き込み処理をレプリカに実施します。



リカバリ処理の最終段階では、プライマリシステムとレプリカの両方のテナントやディレクトリは、短時間だけ読み取り専用になります。HCP システムレベル管理者は、読み取り専用の時間を考慮してリカバリを実施してください。



補足：リカバリ処理の最終段階では、プライマリシステムとレプリカの両方のテナントやディレクトリが読み取り専用となるため、この段階をクライアントがアクセスしない時間にリカバリ処理をスケジューリングしてください。

リカバリが完了すると、プライマリシステムのテナントやディレクトリは読み書き可能になり、レプリカのテナントやディレクトリは再び読み取り専用になり、レプリケーション処理が再開します。この時点で、HCP システムレベル管理者は再度クライアントの書き込み要求をプライマリシステムに送るよう設定し直す必要があります。

メモ：レプリケーションサービスは、レプリカに障害が発生した場合でも処理できます。

リカバリ処理の管理の手順については、「[4.13.6 障害からのリカバリ](#)」を参照してください。

4.13.3 リカバリ処理中の重複の解決

レプリケーションリンクが復元される前に、プライマリシステムのレプリケーションされたテナントやディレクトリに対する書き込みをクライアントに許可した場合、リカバリ処理中に重複が発生するおそれがあるため、推奨しません。同様に、プライマリシステムのテナント、ネームスペース、保管クラス、およびテナントのユーザアカウントに対して、HCP テナント管理者に設定変更を許可することも推奨しません。二つのオブジェクトが同じディレクトリパス、名前、バージョン ID (HCP テナントだけ) を持つ場合に、次のどちらかに該当すると重複が発生します。

- 異なる作成時刻を持つ場合。
- 異なるハッシュ値を持つ場合 (オブジェクトが一致しないことを意味する)。

既存のオブジェクトとレプリケーションされてくるオブジェクトが同じディレクトリパス、名前、ハッシュ値、作成時刻を持つ場合、それらは同じオブジェクトであると判断されます。このとき、レプリケーションサービスは既存オブジェクトのメタデータを、保存されるオブジェクトのメタデータに一致するように更新します。

レプリカからコピーして戻されたオブジェクトがプライマリシステムにすでに存在するオブジェクトと重複した場合、レプリケーションサービスは、インバウンドリンクオブジェクト（レプリカからプライマリシステムにコピーするオブジェクト）を `rest/.lost+found/replication/link-id/object-path` ディレクトリ（HCP ネームスペースの場合）または `fcfs_data/.lost+found/replication/link-id/object-path`（デフォルトネームスペースの場合）に保管します。`link-id` はレプリケーションリンクの内部識別子で、`object-path` は `fcfs_data` または `rest` の下のオブジェクトへのディレクトリパスです。

重複しているインバウンドリンクオブジェクトは、保管期間内でない場合にだけ削除できます。

設定の重複は、テナント、ネームスペース、保管クラス、またはテナントのユーザアカウントの設定がレプリカとプライマリで異なる場合に発生します。この場合、インバウンドの項目がプライマリシステムの項目より新しい構成変更情報を持っているときは、インバウンドオブジェクトがこのオブジェクトに置き換わります。それ以外の場合、インバウンドオブジェクトは無視されます。

メモ：レプリケーションサービスはリカバリ処理中の重複に対応できますが、レプリケーションリンクの復元前に、プライマリシステムで書き込みを許可しないでください。重複を見つけたら、お問い合わせ先まで連絡してください。

4.13.4 フェイルオーバーとリカバリのワークフロー

フェイルオーバーおよびリカバリを実施するシナリオには二つあります。一つはプライマリシステムで障害が発生した場合で、もう一つはレプリカで障害が発生した場合です。次のセクションでは、これらのシナリオの基本的なワークフローについて説明します。

(1) プライマリシステム障害のワークフロー

次の表は、レプリケーションペアのプライマリシステムで障害が起こった場合の手順と発生内容を示します。

表 4-5 レプリケーションペアのプライマリシステムで障害が起こった場合の手順と発生内容

番号	リカバリの手順	発生内容
プライマリシステムで障害発生		
1	レプリカで、フェイルオーバー処理を実行します。	レプリカの該当するテナントとディレクトリは読み書き可能となります。
2	クライアントにレプリカにだけ書き込みするように指示します。	--
プライマリシステムがオンラインに戻ります		
3	プライマリシステムが再構築された場合：プライマリシステムで、レプリカからレプリケーション SSL サーバ証明書をアップロードします。レプリカで、プライマリシステムからレプリケーション SSL サーバ証明書をアップロードします	--
4	レプリカで、必要に応じてリンク接続情報を更新します。	--
5	レプリカで、リンクをリストアする要求を送ります。	ペンディングリンク要求がプライマリシステムに表示されます。
6	プライマリシステムで、リストアされたリンクを受け取ります。	レプリケーションリンクが <code>Suspended</code> （待機）状態で再作成されます。

番号	リカバリの手順	発生内容
7	レプリカで、データリカバリを開始します。	レプリカの該当するテナントとディレクトリは、読み書き可能のままです。プライマリシステムの該当するテナントとディレクトリは読み取り専用になります。レプリカからプライマリシステムへのデータリカバリが開始します。
8	データリカバリのバックログ時間がゼロになるまで待機します。	--
9	プライマリシステムとレプリカの両方で、データリカバリを終了させます。	レプリカの該当するテナントとディレクトリは、読み取り専用になります。プライマリシステムの該当するテナントとディレクトリは、読み取り専用のままです。レプリカからプライマリシステムのデータリカバリが終了するまで続きます。
データリカバリが終了します		
10	特になし。	レプリカの該当するテナントとディレクトリは読み取り専用のままです。プライマリシステムの該当するテナントとディレクトリは読み書き可能になります。プライマリシステムからレプリカへのレプリケーションが再開します。
11	システムログに「Replication data recovery completed」というメッセージが表示されたら、クライアントにプライマリシステムだけに書き込みするように指示します。	--

(2) レプリカ障害のワークフロー

次の表は、レプリケーションペアのレプリカで障害が起こった場合の手順と発生内容を示します。

表 4-6 レプリケーションペアのレプリカで障害が起こった場合の手順と発生内容

番号	リカバリの手順	発生内容
レプリカで障害発生		
1	リンクのレプリケーションを停止します。	--
レプリカがオンラインに戻ります		
2	レプリカが再構築された場合：レプリカで、プライマリシステムからレプリケーション SSL サーバ証明書をアップロードします。プライマリシステムで、レプリカからレプリケーション SSL サーバ証明書をアップロードします。	--
3	プライマリシステムで、必要に応じてリンク設定情報を更新します。	--
4	プライマリシステムで、リンクをリストアする要求を送ります。	ペンディングリンク要求がレプリカに表示されます。
5	プライマリシステムで、リストアされたリンクを受け取ります。	レプリケーションリンクが Suspended (待機) 状態で再作成されます。
6	プライマリシステムで、最初からレプリケーションを再開します。	レプリケーションリンクが再作成された場合：プライマリシステムの該当するテナントとディレクトリは読み書き可能のままです。レプリカの該当するテナントとディレクトリは読み取り専用になります。 リンクが再開された場合：プライマリシステムからレプリカへのレプリケーションは最初から再開します。

4.13.5 レプリカへのフェイルオーバー

プライマリシステムで障害が発生した場合、レプリカのシステム管理コンソールから手動でフェイルオーバー処理を実行してください。フェイルオーバー処理により、レプリカの該当するテナントとディレクトリが読み書き可能になります。

重要：

- 書き込み先を、レプリカ側だけのレプリケーションされたネームスペースとディレクトリにするように、すべてのクライアントに指示する必要があります。データリカバリ処理が終了するまで、プライマリシステムのレプリケーションされたネームスペースとディレクトリには書き込みできません。
- 通常のレプリケーションに戻すためには、データリカバリ手順を最後まで実施する必要があります。リンクをリストアする必要がない場合でも、またレプリケーションされたエントリの設定またはコンテンツが変更されなかった場合でも、この手順を実施する必要があります。何も変更がなかった場合でも、このケースのデータリカバリ処理には5分以上掛かることがあります。

レプリケーションリンクでフェイルオーバー処理を実行するには、次の手順を実行してください。

- レプリカのシステム管理コンソールのトップレベルメニューで、[Services] の上にマウスカーソルを置いてセカンダリメニューを表示します。
- セカンダリメニューで、[Replication] をクリックしてください。
- [Replication] ページで、フェイルオーバーを開始するリンクの名前をクリックしてください。
- 開いたパネルの左側にある [Advanced] をクリックしてください。
- [Advanced] パネルで、[Fail Over] ボタンをクリックしてください。
- 確認メッセージが表示されたら、[Fail Over Link] ボタンをクリックしてください。

補足：フェイルオーバー処理の開始後に、コンテンツの検証と保護サービスがプライマリシステムから修復を行わないように、レプリケーションリンクを中断します。

4.13.6 障害からのリカバリ

障害が発生すると、HCP システムはすべての設定情報を失うことがあります。このようにシステムがレプリケーションを行った場合、そのシステムが復旧した後にリンク設定をリストアしてください。プライマリシステムに障害が発生した場合、ネームスペースのコンテンツとその他の該当情報をレプリカからリカバリする必要があります。レプリカに障害が発生した場合、レプリケーションは自動的に再開します。その場合、HCP はすべてのネームスペースまたは各ネームスペース内で最も古いメタデータの変更を持つオブジェクトから改めてレプリケーションを開始します。

メモ：障害が発生した HCP システムが再度有効になった場合に、そのシステムにリンク設定が残っているとき、リンクをリストアする必要はありません。

リンクをリストアした後に、確実にデータリカバリを開始するか、またはレプリケーションを再実行してください。リンクがリストアされたときは、どちらのプロセスも自動では開始されません。

リストアされたリンクの初期状態は [Suspended] (待機) です。データリカバリを開始したとき、またはレプリケーションを再開したときに、リンクの処理が自動的に再開します。

(1) プライマリシステム障害後のデータリカバリ

レプリカからプライマリシステムにデータとその他の該当情報をリストアするには、次の手順を実行してください。

- レプリカのシステム管理コンソールのトップレベルメニューで、[Services] の上にマウスカーソルを置いてセカンダリメニューを表示します。

2. セカンダリメニューで、[Replication] をクリックしてください。
3. [Replication] ページで、目的のリンクの名前をクリックしてください。
4. 開いたパネルの左側にある [Advanced] をクリックしてください。
5. [Advanced] パネルで、[Begin Recovery] ボタンをクリックしてください。

メモ: レプリケーションの新しいクライアント証明書のアップロード後に [Begin Recovery] ボタンがアクティブになるまで、10分以上かかることがあります。

レプリケーションサービスは、レプリカからプライマリシステムに該当する設定とオブジェクトのコピーを開始します。プライマリシステムからレプリカへのレプリケーションと同様に、すべてのネームスペース全体または各ネームスペース内で最も古いメタデータの変更を持つオブジェクトから、サービスが開始されます（リンク設定による）。
6. プライマリシステムかレプリカのどちらかのシステム管理コンソールの [Replication] ページに表示されるテナントバックログを定期的に確認することで、リカバリ処理を監視します。
7. リカバリ処理が、現在のレプリカのテナントとネームスペースの処理とほぼ同期が取れると、レプリカのシステム管理コンソールの [Advanced] パネルに戻ります。各テナントの最大バックログ時間がゼロに近づくと、同期は終了に近づきます。

メモ: クライアントがレプリカへの書き込みアクセスを続ける限り、同期化が 100%に達することはありません。同期化は、リカバリ処理を終えるために完了する必要はありません。
8. [Advanced] パネルで、[Complete Recovery] ボタンをクリックしてください。

補足: リポジトリのクライアント利用が少ないときに、データリカバリ処理の実行をスケジュールすることができます。

レプリカの該当するテナントとディレクトリは読み取り専用になります。レプリケーションサービスがリカバリ処理を終了するまで、テナントとディレクトリは読み取り専用のままです。これにかかる時間は、リカバリするデータがどれくらい残っているかによります。

リカバリ処理が終了すると、プライマリシステムのテナントとディレクトリは読み書き可能になり、その一方でレプリカのテナントやディレクトリは読み取り専用のままです。プライマリシステムのレプリケーションサービスはオブジェクトのレプリカへのコピーを再開します。
9. システムログに次のメッセージが表示されるまで待ちます。

Replication data recovery completed
10. プライマリシステムにレプリケーションされたテナントとディレクトリに、クライアントが書き込みを行うように変更します。

(2) レプリカ障害後のレプリケーション再開

レプリカへのレプリケーションリンクのリストア後にレプリケーションを再開するには、次の手順を実行してください。

1. プライマリシステムのシステム管理コンソールのトップレベルメニューで、[Services] の上にマウスカーソルを置いてセカンダリメニューを表示します。
2. セカンダリメニューで、[Replication] をクリックしてください。
3. [Replication] ページで、目的のリンクの名前をクリックしてください。
4. 開いたパネルの左側にある [Advanced] をクリックしてください。
5. [Advanced] パネルで、[Restart] ボタンをクリックしてください。
6. 確認メッセージが表示されたら、[Restart Replication] ボタンをクリックしてください。

レプリケーションサービスは、選択したテナントとディレクトリにあるすべてのオブジェクトとその他の該当情報を、プライマリシステムからレプリカにコピーします。

HCP システムの起動と停止

ここでは、HCP システムの起動および停止の手順を説明します。

- A.1 HCP システムを起動する
- A.2 HCP システムを停止する

A.1 HCP システムを起動する

ここでは、HCP システムを起動する手順を説明します。HCP システムの起動は、次のとおり行います。

- ハードウェアの電源を入れる。
- ハードウェアの動作状態を確認する。

それぞれの詳細な手順を次に説明します。

A.1.1 ハードウェアの電源を入れる

ここでは、ハードウェアの電源を入れる手順を説明します。なお、ノード以外のハードウェアの電源がすでに入っている場合、次の手順 8 から操作を開始してください。

1. ラック内にある、コンセントボックスのブレーカの電源を入れます。
電源の入れ方については、HCP に添付されているコンセントボックスのマニュアルを参照してください。
2. ファイバチャネルスイッチの電源を入れます。
電源の入れ方については、HCP に添付されているファイバチャネルスイッチのマニュアルを参照してください。
3. ファイバチャネルスイッチの LED を参照して、電源が入っていることを確認します。
確認する LED については、HCP に添付されているファイバチャネルスイッチのマニュアルを参照してください。
4. ストレージの電源を入れます。
電源の入れ方については、HCP に添付されているストレージのマニュアルを参照してください。
5. ストレージの LED を参照して、電源が入っていることを確認します。
確認する LED については、HCP に添付されているストレージのマニュアルを参照してください。
6. バックエンドスイッチの電源を入れます。
電源の入れ方については、「[B.2.2 バックエンドスイッチの電源の入れ方および切り方](#)」を参照してください。
7. バックエンドスイッチの LED を参照して、電源が入っていることを確認します。
確認する LED については、「[図 B-3 バックエンドスイッチ \(装置正面パネル\)](#)」および「[表 B-1 バックエンドスイッチ \(正面パネルの LED\)](#)」を参照してください。
8. ノードの電源を入れます。
電源の入れ方については、HCP に添付されているノードのマニュアルを参照してください。
9. ノードの LED を参照して、電源が入っていることを確認します。
確認する LED については、HCP に添付されているノードのマニュアルを参照してください。

A.1.2 ハードウェアの動作状態を確認する

ここでは、ハードウェアの動作状態を画面で確認する手順を説明します。

1. システム管理コンソールへログインします。
HCP システムに初めてログインする場合は、デフォルトユーザのアカウントを使用してください。デフォルトユーザでのログインについては、「[2.1.2 デフォルトユーザでログインし、パスワードを変更する](#)」を参照してください。
2. システム管理コンソールで、[Overview] を選択します。

- [Overview] ページが表示されます。
3. [Overview] ページの [Hardware Status] に、警告メッセージおよびエラーメッセージが表示されていないことを確認します。
警告メッセージおよびエラーメッセージの一覧については、「[2.7 システム管理コンソールの警告を確認する](#)」を参照してください。
警告メッセージは背景がオレンジ色、エラーメッセージは赤色で表示されます。警告メッセージまたはエラーメッセージが表示されている場合、お問い合わせ先まで連絡してください。
 4. システム管理コンソールで、[Monitoring] を選択します。
[Monitoring] ページが表示されます。
 5. [Monitoring] ページの [System Events] タブに表示されているイベントに、警告メッセージおよびエラーメッセージがないことを確認します。
警告メッセージおよびエラーメッセージの一覧については、「[2.7 システム管理コンソールの警告を確認する](#)」を参照してください。
システムログの警告メッセージは、[Severity] の文字色がオレンジ色、エラーメッセージは赤色で表示されます。
 6. システム管理コンソールで、[Overview] を選択します。
[Overview] ページが表示されます。
 7. [Overview] ページの [Hardware Status] に、次の表示があることを確認します。
 - Zero-copy failover enabled
 - Multipath enabled
 8. 暗号化を実行している場合、[Overview] ページの [System Status] に、次の表示があることを確認します。
 - Archive is encrypted using 128-bit AES
 9. システム管理コンソールで、[Hardware] を選択します。
[Hardware] ページが表示されます。
 10. 各ノードの論理ボリュームが正常であることを、[Hardware] ページの次の点で確認します。
 - すべてのノードの [Status] が、[Available] となっていること。
 - すべてのノードの [Logical Volumes] で、各論理ボリュームが緑色になっていること。
 11. すべてのノードと IP スイッチが正常に接続されていることを、ノードごとに次の手順を実行して確認します。
 - a. [Hardware] ページで、ノード ID をクリックします。
ノードの詳細情報が表示されます。
 - b. ノードの [Hardware Status] セクションに表示されている、ネットワークインタフェースカード (NIC) に関するメッセージをクリックします。
ネットワークインタフェースカード (NIC) の詳細情報が表示されます。
 - c. [Bonded Back-End Interface:bond1] で、[eth1] と [eth3] の [Active] が、[true] となっていることを確認します。
 12. すべてのノードとファイバチャネルスイッチが正常に接続されていることを、ノードごとに次の手順を実行して確認します。
 - a. [Hardware] ページで、ノード ID をクリックします。
ノードの詳細情報が表示されます。
 - b. ノードの [Hardware Status] セクションに表示されている、ストレージデバイスに関するメッセージをクリックします。

ストレージデバイスの詳細情報が表示されます。

- c. すべてのデバイスの [Status] が, [OK] となっていることを確認します。

A.2 HCP システムを停止する

ここでは, HCP システムを停止する手順を説明します。

なお, HCP システムを停止して HVFP のファイルシステムの運用を続ける場合は, HVFP 側で次の操作に対してエラーが発生するおそれがあるため, 注意してください。

- スタブファイルの読み込み処理
 - スタブファイルの更新処理
 - マイグレートされたファイルの削除
 - マイグレートされた WORM ファイルのリテンション期間の延長
 - 設定されたスケジュールでの, HCP へのシステム設定情報の保存
1. 連携製品からのアクセスを停止する。
メンテナンスなどによって連携製品を停止する場合は, HCP システムよりも先に連携製品を停止してください。
 2. システム管理コンソールにログインします。
 3. システム管理コンソールで, [Nodes] を選択します。
[Nodes] ページが表示されます。
 4. [Nodes] ページの下にある, [Shut Down System] ボタンをクリックします。
[Shut Down System] ウィンドウが表示されます。
 5. [Reason] フィールドに, ノードをシャットダウンする理由を入力してください。
[Reason] フィールドには, ASCII 表示可能文字を使って, 空白を含め 1,024 文字を入力できます。
 6. [Shut Down System] ボタンをクリックします。

注意:
システム管理コンソールの画面表示を更新する場合, Web ブラウザのリフレッシュ機能を使用して更新しないでください。画面を更新する場合は, システム管理コンソールの [Nodes] を再度選択してください。
 7. ブラウザウィンドウを閉じます。
システムの停止処理が完了すると, ノードの電源が切れます。
通常のシステムの停止はこれで完了です。停電対策やシステムの移設などの場合に限り, 次の手順以降も実行してください。
 8. バックエンドスイッチの電源を切ります。
電源の切り方については, 「B.2.2 バックエンドスイッチの電源の入れ方および切り方」を参照してください。
 9. バックエンドスイッチの LED を参照して, 電源が切れていることを確認します。
確認する LED については, 「図 B-3 バックエンドスイッチ (装置正面パネル)」および「表 B-1 バックエンドスイッチ (正面パネルの LED)」を参照してください。
 10. ストレージの電源を切ります。
電源の切り方については, HCP に添付されているストレージのマニュアルを参照してください。
 11. ストレージの LED を参照して, 電源が切れていることを確認します。

確認する LED については、HCP に添付されているストレージのマニュアルを参照してください。

12. ファイバチャネルスイッチの電源を切ります。
電源の切り方については、HCP に添付されているファイバチャネルスイッチのマニュアルを参照してください。
13. ファイバチャネルスイッチの LED を参照して、電源が切れていることを確認します。
確認する LED については、HCP に添付されているファイバチャネルスイッチのマニュアルを参照してください。

HCP システムで使用するハードウェア

HCP システムでは、ノード、ストレージ、IP スイッチなどのハードウェアを使用します。ここでは、ノード、バックエンドスイッチ、およびルーターについて説明します。ストレージなど、そのほかのハードウェアの詳細については、HCP に添付されているマニュアルを参照してください。

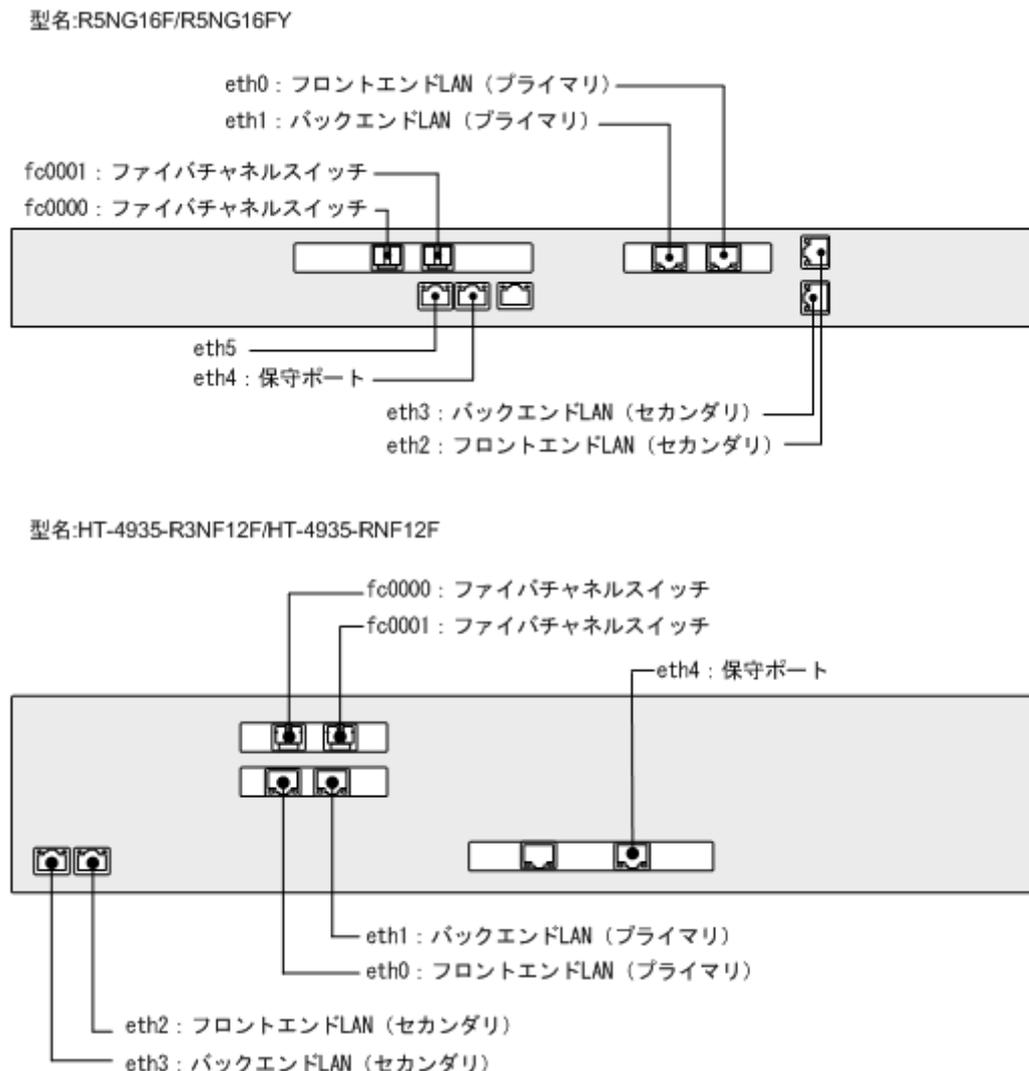
- B.1 ノード
- B.2 バックエンドスイッチ
- B.3 ルーター

B.1 ノード

ここでは、HCP システムで使用するノード上のポートの配置について説明します。

ポートの配置について次に示します。なお、ノードの機種によってポートの配置は異なります。

図 B-1 ノードで使用するポートの配置



B.2 バックエンドスイッチ

ここでは、バックエンドスイッチに関する次の情報を説明します。

- 装置の外観図
- 電源の入れ方および切り方
- SNMP サーバおよび NTP サーバとの接続に使用するポート

それぞれの詳細を次に説明します。

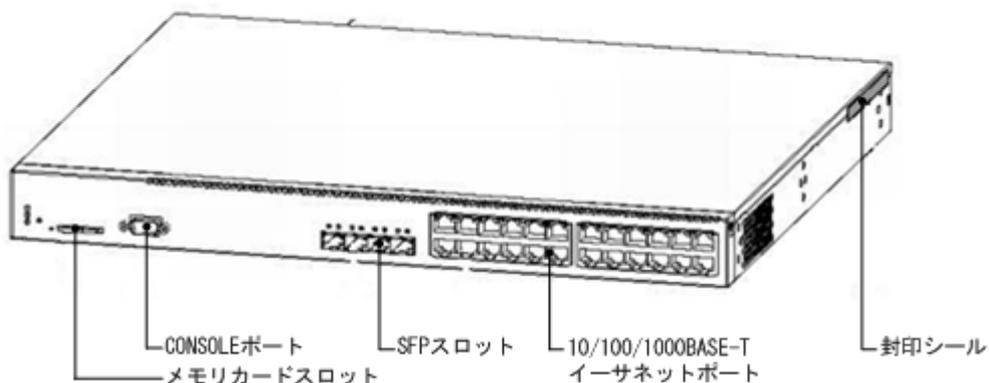
B.2.1 装置の外観図

装置の外観について次に示します。

(1) 装置の前面

装置の前面を次に示します。

図 B-2 バックエンドスイッチ（装置前面）



⚠ 注意

- 。 装置のカバーを外さないでください。感電の原因となります。

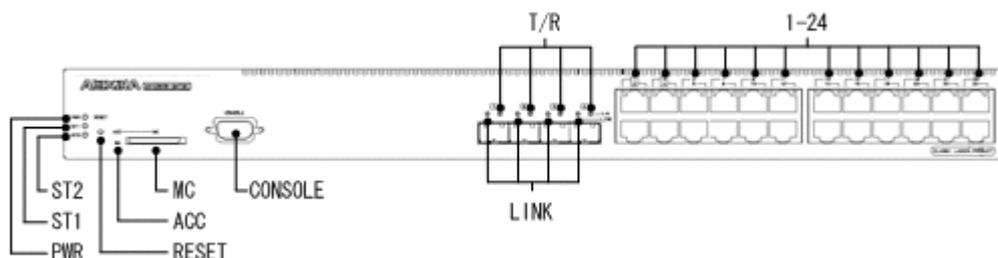
NOTE

封印シールをはがさないでください。封印シールをはがすと、「開封済み」の文字が浮かびます。「開封済み」の文字が浮かんだ機器は、保証の対象外となります。

(2) 装置の正面パネル

装置の正面パネルを次に示します。

図 B-3 バックエンドスイッチ（装置正面パネル）



各 LED、スイッチ、コネクタの詳細について次に示します。

表 B-1 バックエンドスイッチ（正面パネルの LED）

名称	LEDの種類	LEDの示す状態
PWR	緑	電源の状態を次のパターンで示します。 ・ 点灯：電源 ON ・ 消灯：電源 OFF, または電源異常
ST1	緑および赤	装置の状態を次のパターンで示します。 ・ 緑点灯：動作可能 ・ 緑点滅：準備中（起動中） ・ 赤点滅または点灯：装置の障害発生 ・ 消灯：電源 OFF, または電源異常

名称	LEDの種類	LEDの示す状態
ST2	緑	使用しません。
ACC	緑	メモ리카ードの状態を次のパターンで示します。 <ul style="list-style-type: none"> 点灯：メモ리카ードアクセス中 消灯：メモ리카ードアイドル中
LINK※	緑	SFP スロットのイーサネットポートの動作状態を示します。
T/R※	緑	
1-24	緑およびオレンジ	10/100/1000BASE-T イーサネットポートの動作状態を、次のパターンで示します。 <ul style="list-style-type: none"> 緑点灯：リンク確立 緑点滅：リンク確立およびフレーム送受信中 オレンジ点灯：回線障害検出 消灯：ST1 の LED が緑点灯の場合、リンク障害または閉塞

NOTE

注※

この個所はサポート対象外のため、使用しないでください。

表 B-2 バックエンドスイッチ（正面パネルのスイッチ）

名称	詳細
RESET※	装置のリセットスイッチです。

NOTE

注※

この個所はサポート対象外のため、使用しないでください。

表 B-3 バックエンドスイッチ（正面パネルのコネクタ）

名称	詳細
MC※	メモ리카ードのスロットです。
CONSOLE※	CONSOLE ポートです。

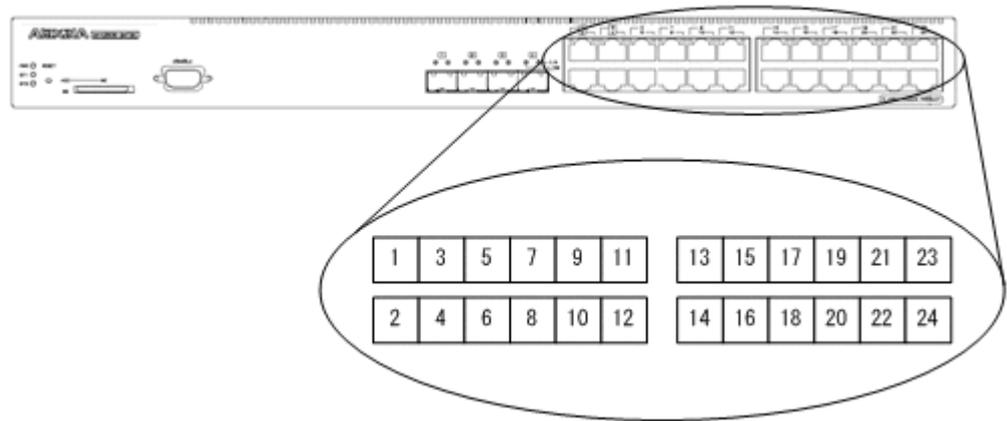
NOTE

注※

この個所は保守員が保守時に使用します。保守員以外の方は、メモ리카ードの抜き差しや CONSOLE ポートを使用しないでください。

なお、バックエンドスイッチのポート番号は次の図のとおりです。

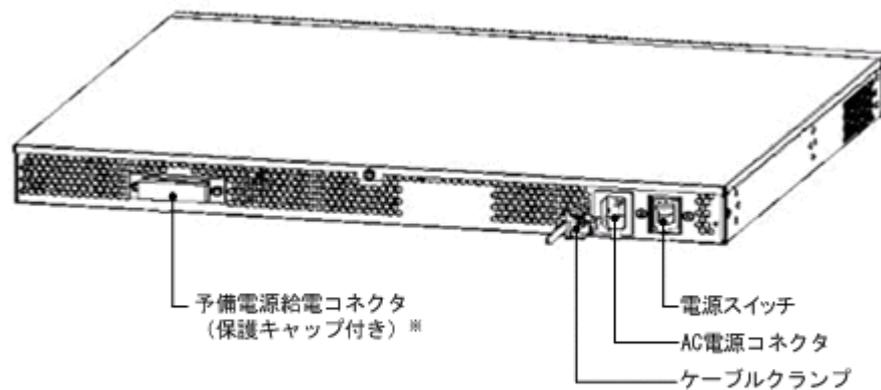
図 B-4 バックエンドスイッチ (ポート番号)



(3) 装置の後面

装置の後面を次に示します。

図 B-5 バックエンドスイッチ (装置後面)



NOTE

注※ この箇所はサポート対象外のため、使用しないでください。

B.2.2 バックエンドスイッチの電源の入れ方および切り方

ここでは、バックエンドスイッチでの電源の入れ方、および切り方について説明します。

電源の入れ方

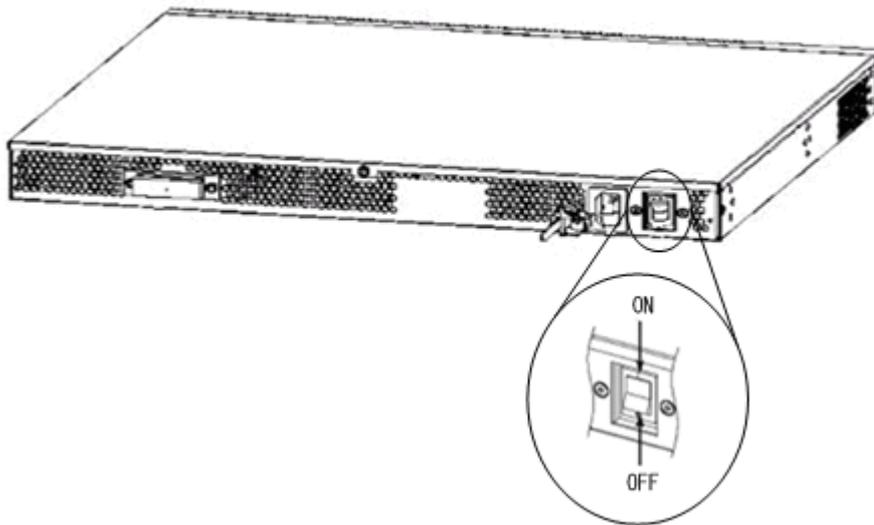
バックエンドスイッチの背面にある電源スイッチを ON にします。

電源の切り方

バックエンドスイッチの背面にある電源スイッチを OFF にします。

バックエンドスイッチの背面にある電源スイッチについて次に示します。

図 B-6 バックエンドスイッチ（背面の電源スイッチ）



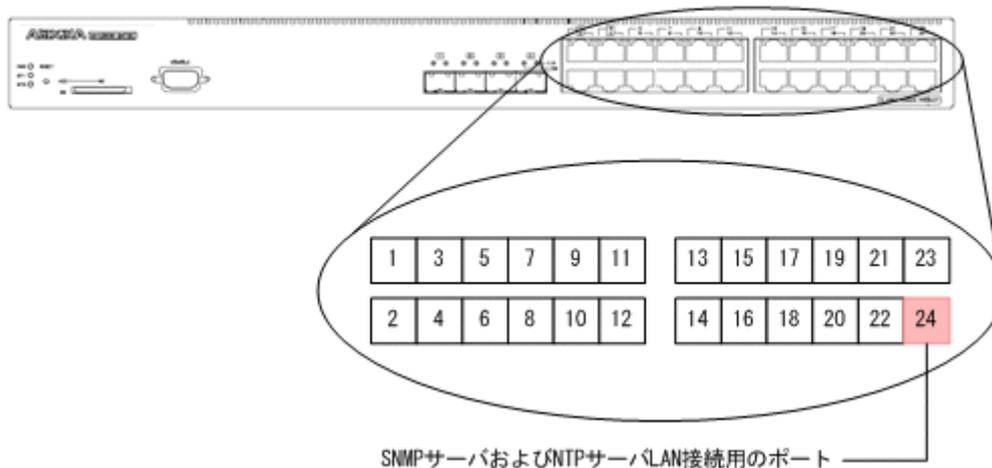
注意

- バックエンドスイッチの ACC の LED 点灯中は、電源を切らないでください。
バックエンドスイッチの正面パネルにある ACC の LED 点灯中は、メモ리카ードにアクセス中です。アクセス中に電源を切ると、メモ리카ードを破損するおそれがあります。
- ノードやストレージの電源を切ったあとに、バックエンドスイッチの電源を切ってください。

B.2.3 SNMP サーバおよび NTP サーバとの接続に使用するポート

バックエンドスイッチに対し、SNMP サーバから監視させる場合や NTP サーバと時刻を同期させる場合、SNMP サーバおよび NTP サーバと接続する LAN を、バックエンドスイッチの 24 番ポートに接続してください。24 番ポートの位置を次に示します。

図 B-7 バックエンドスイッチ（SNMP サーバおよび NTP サーバの LAN 接続ポート）



B.3 ルーター

ストレージを共有して HCP と HVFP を連携する場合、HVFP の管理 LAN とフロントエンド LAN の間にルーターを設置します。管理 LAN 上の管理コンソールがフロントエンド LAN 上の HCP と通信できるようにルーターを設定してください。設定するネットワークアドレスについて次に示します。

- 管理 LAN 側：管理コンソールのネットワークアドレス
- フロントエンド LAN 側：フロントエンド LAN のネットワークアドレス

ファイアウォールで例外登録するポート番号とプロトコル

使用するポートやプロトコルをファイアウォールで制限する場合、次のポート番号とプロトコルをファイアウォールの例外として登録してください。

表 B-4 管理コンソールと HCP の間のファイアウォールで例外登録が必要なポート番号

ポート番号	通信元	通信先
8000/tcp	管理コンソール	テナント管理コンソール
9090/tcp	管理コンソール	HCP 管理 API

HCP システムで使用するサービス

ここでは、HCP システムで使用するサービスについて説明します。

- C.1 サービスのデフォルトスケジュール
- C.2 サービスのスケジュール
- C.3 保護サービスの実行契機

C.1 サービスのデフォルトスケジュール

HCP システムで使用するサービスについて次の表に示します。

表 C-1 HCP システムで使用するサービス

サービス名	説明
Duplicate elimination	冗長データを削除するサービスです。
Garbage collection	削除対象のオブジェクトや、トランザクションログにある削除やページのレコードなど、リポジトリ内に残ったデータとメタデータを削除するサービスです。
Scavenging	リポジトリ内のオブジェクトが有効なメタデータを持っているかの確認、および修復をするサービスです。
Compression	オブジェクトのデータを圧縮するサービスです。
Disposition	期限が過ぎたオブジェクトを自動的に削除する HCP のサービスです。
Content Verification	オブジェクトのデータがハッシュ値と一致するかどうかを確認することで、オブジェクトの整合性を確保するサービスです。
Protection	ネームスペースごとに設定するデータ保護レベル (DPL) によってデータを冗長化して、データの欠落および破損を自動で修復をするサービスです。

これらのサービスに対して、デフォルトで実行されるスケジュールについて次の表に示します。

表 C-2 サービスのデフォルト実行スケジュール

時刻	土、日曜日に実行されるサービス		月～金曜日に実行されるサービス
0:00～10:00	Protection Scavenging		Garbage collection Disposition Duplicate elimination
10:00～13:00			Compression
13:00～18:00	Garbage collection	Compression	Content Verification
18:00～24:00	Disposition Duplicate elimination	Content Verification	

C.2 サービスのスケジュール

システム管理コンソールの [Schedule] ページでは、サービスのスケジュールとイベントログを管理できます。

[Schedule] ページを表示する手順を次に示します。

- プライマリシステムのシステム管理コンソールのトップレベルメニューで、[Services] の上にマウスカーソルを置いてセカンダリメニューを表示します。
- セカンダリメニューで、[Schedule] をクリックしてください。

ロール :

[Schedule] ページのスケジュールとイベントログを参照するには、Monitor ロールまたは Administrator ロールが付与されている必要があります。サービスのスケジュールを作成、変更、起動または削除するには、Administrator ロールが付与されている必要があります。

C.2.1 サービスに関する情報の表示

[Schedule] ページの上部には、各サービスを表すアイコンが表示されます。これらのアイコンにより、何のサービスがスケジュールされているかを確認することができます。表示されるアイコンは次のとおりです。

- ・ 圧縮サービス
 - ・ コンテンツ検証サービス
 - ・ ディスポジションサービス
 - ・ 重複排除サービス
 - ・ ガーベジコレクションサービス
 - ・ 保護サービス
 - ・ スカベンジングサービス
 - ・ ストレージ階層サービス
- スピンドウン記憶装置を持っている SAIN システムだけで表示されます。

スケジュール表の実行期間の上にマウスカーソルを移動すると、キャプションの上部にスケジュールの開始時刻および終了時間が表示されます。スケジュールされているサービスは、キャプションでハイライト表示されます。

C.2.2 スケジュールを作成する前に

サービスのスケジュールを作成する前に次のことを確認してください。

- ・ HCP Default Schedule は、修正および削除できません。
- ・ 最短の実行期間は 2 時間です。
- ・ 同じサービスを含まない場合、実行期間が重なっても設定できます。例えば、午前 1 時から始まる 5 時間の実行期間、午前 1 時から始まる 6 時間の実行期間、および午前 3 時から始まる 3 時間の実行期間を同じ日に対して設定できます。
- ・ 実行期間が二日にわたる設定はできません。
- ・ 実行期間内に設定するサービスの最大数は、実行期間（時間）を半分にして小数点以下を切捨てた数を推奨します。
- ・ 多くのサービスを同時に実行するスケジュールを設定すると、システムリソースの競合が多くなります。
- ・ スケジュールが実行されるたびにサービスが起動し、前回停止した部分から処理を続けます。
- ・ アクティブなスケジュールを修正すると、実行中のサービスが停止します。修正したときの時刻がサービスの実行期間内の場合、10 分以上実行期間が残っていればサービスが再開します。

また、優先的に実行されるサービスについて次に示します。

- ・ 保護サービスは、コンテンツ検証サービスと圧縮サービスよりも優先的に実行されます。保護サービスが開始すると、実行中のコンテンツ検証サービスや圧縮サービスは自動的に停止します。保護サービスが停止すると、自動的に停止していたサービスが再開し、その時間で実行されるようにスケジュールリングされます。

C.2.3 スケジュールの作成

サービスのスケジュールを作成する手順を次に示します。

1. 既存のスケジュールから新しいスケジュールを作成する場合、スケジュール表の左上のフィールドでスケジュールを選択します。
2. [Create New Schedule] ボタンをクリックします。
3. [Create New Schedule] ウィンドウで新しいスケジュール名を入力します。
スケジュール名は1~64文字で指定します。指定できる文字は英数字、ハイフン (-)、アンダーライン (_), ピリオド (.), コンマ (,) およびスペースです。入力した英大文字と英小文字は区別されません。なお、HCP Default Schedule, HCP Spindown は、スケジュール名として使用できません。既存のスケジュールから作成する場合は、[From current load schedule:] オプションを選択してください。既存のスケジュールから作成しない場合は、[From blank schedule] オプションを選択してください。
4. [Save] ボタンをクリックします。
スケジュール表に新しいスケジュールが表示されます。この時点のスケジュールはアクティブではありません。

C.2.4 スケジュールの変更

サービスのスケジュールを変更する手順を次に示します。

1. スケジュール表の左上のフィールドで、スケジュールを選択します。
2. スケジュールに実行期間を追加、修正または削除します。
3. [Update Schedule] ボタンをクリックします。

(1) 実行期間の追加

サービスのスケジュールに実行期間を追加する手順を次に示します。

1. スケジュール表の左上のフィールドで、実行期間を追加したいスケジュールを選択します。
2. スケジュール表で実行期間を設定します。
次のどれかの方法で設定してください。
 - 開始時間をクリックしてください。デフォルトで2時間の実行期間が設定されます。実行期間を保存する前に、開始時間および終了時間を変更できます。
 - 同じ日内の任意の時間をドラッグして範囲を選択してください。選択した範囲の時間が実行期間として設定されます。実行期間を保存する前に、開始時間および終了時間を変更できます。
 - 既存の実行期間をクリックしてください。
 - 曜日からクリックしてください。24時間の実行期間が設定されます。この実行期間を保存するとき、同じ日のほかのすべての実行期間が削除されます。
 - All をクリックしてください。1週間、毎日24時間の実行期間が設定されます。この実行期間を保存するとき、同じスケジュールのほかのすべての実行期間が削除されます。[Edit Time Period] ウィンドウがポップアップ表示されます。このウィンドウの上部には、実行期間と開始時間と終了時間が表示されています。[Edit Time Period] ウィンドウは、スケジュールされたサービスのパフォーマンスレベルを一覧表示します。[Edit Time Period] ウィンドウのサービスステータスの表示について次に示します。
 - [Service not scheduled] : 編集の実行期間にサービスがスケジュールされていません。パフォーマンスレベルは設定されていません。
 - [Service scheduled] : 編集の実行期間にサービスがスケジュールされています。パフォーマンスレベルは Low, Medium または High のどれかが表示されます。

- [Service already scheduled] : 編集中の実行期間と重なっているスケジュールが設定されています。パフォーマンスレベルは表示されません。
 - [Service preempted] : 編集中の実行期間にすでにスケジュールされているもう一つの優先度の高いサービスによって、サービスは割り込まれます。パフォーマンスレベルは表示されません。
3. 任意の実行期間を設定する場合（曜日または A11 以外を選択した場合）、From フィールドで開始時間を選択します。
 4. 任意の実行期間を設定する場合（曜日または A11 以外を選択した場合）、To フィールドで終了時間を選択します。
 5. 実行させるサービスのパフォーマンスレベルを、Level フィールドで Low, Medium または High から選択します。実行しないサービスは、Off を選択します。
 6. 次のどれかの操作をします。
 - スケジュール表をクリックまたはドラッグするか、曜日をクリックします。
 - A11 をクリックしてスケジュールを作成した場合は、[Update Schedule] ボタンをクリックします。
 - スケジュール表の既存の実行期間をクリックした場合は、[Create New Period] ボタンをクリックします。新しい実行期間が作成されます。

(2) 実行期間の変更

サービスのスケジュールの実行期間を変更する手順を次に示します。

1. スケジュール表の左上のフィールドで、実行期間を変更したいスケジュールを選択します。
2. スケジュール表で、変更したい実行期間をクリックします。
3. [Edit Time Period] ウィンドウで実行期間を変更します。
4. [Update Schedule] ボタンをクリックします。

(3) 実行期間の削除

サービスのスケジュールの実行期間を削除する手順を次に示します。

1. スケジュール表の左上のフィールドで、実行期間を削除したいスケジュールを選択します。
2. スケジュール表で、削除したい実行期間をクリックします。
3. [Edit Time Period] ウィンドウで [Delete Period] ボタンをクリックします。
4. すべてのサービスのパフォーマンスレベルを Off に設定します。
5. [Update Schedule] ボタンをクリックします。

C.2.5 スケジュールのアクティブ設定

サービスのスケジュールをアクティブに設定する手順を次に示します。

1. スケジュール表の左上のフィールドで、アクティブにしたいスケジュールを選択します。
2. [Activate Schedule] ボタンをクリックしてください。
[Activate Schedule] ボタンは、表示されたスケジュールがアクティブでない場合にのみ表示されます。

C.2.6 スケジュールの削除

サービスのスケジュールを削除する手順を次に示します。

1. スケジュール表の左上のフィールドで、削除したいスケジュールを選択します。
アクティブなスケジュールは削除できません。現在アクティブなスケジュールを削除したい場合は、削除したいスケジュールとは別のスケジュールを表示してください。
2. [Delete Schedule] ボタンをクリックしてください。
3. 応答確認メッセージで [Delete Schedule] ボタンをクリックします。
スケジュールが削除され、スケジュール表にはアクティブなスケジュールが表示されます。

C.3 保護サービスの実行契機

保護サービスは、指定したスケジュールに従って実行されるほか、次のとおり継続的にオブジェクトデータが利用できないおそれがある場合に実行されます。

- ノード停止後、90 分後に保護サービスを実行します。
- 論理ボリュームの故障を HCP システムが検知後、1 分後に保護サービスを実行します。
- HCP システムからノードが削除された後、10 分後に保護サービスを実行します。

これらの保護サービスの実行は、スケジュールによる実行よりも処理が優先されます。

HCP システムログメッセージ

HCP は、システムで発生するイベントに関するメッセージをシステムログに記録します。システムログに HCP が書き込むメッセージや内部ログについて説明します。

- [D.1 システムログメッセージ一覧](#)
- [D.2 HCP システムログ](#)
- [D.3 HCP 内部ログ](#)

D.1 システムログメッセージ一覧

表のメッセージごとの項目を次に示します。

- ・ イベント ID
- ・ メッセージが関係するイベントを識別するメッセージの概要
- ・ メッセージの説明
- ・ メッセージに対応してとる必要があるアクション（アクションが必要な場合）
- ・ メッセージの重要度

表 D-1 システムログメッセージ

ID	イベント	説明	アクション	重要度
1000	HCP started	HCP システムが起動しました。	アクションは必要ありません。	Notice
1001	HCP shutting down	HCP システムがシャットダウンしています。	どれかのノードの電源が自動的に切れない場合、数分待ち、手動で電源を切ってください。	Notice
1002	Node started	ノードが起動しました。	アクションは必要ありません。	Notice
1003	Node shut down	ノードがシャットダウンしました。	このイベントが予想外の場合や、ノードが自動的に再起動しない場合は、お問い合わせ先まで連絡してください。ノードは手動で再起動しないようにしてください。問題の解析に必要な情報がなくなる原因となる場合があります。	Notice
1004	Volume started	論理ボリュームがオンラインになりました。	アクションは必要ありません。	Notice
1005	Volume shut down	論理ボリュームがオフラインになりました。	お問い合わせ先まで連絡してください。	Notice
1006	Volume failure	論理ボリュームに障害が発生しました。	お問い合わせ先まで連絡してください。	Error
1007	Node removed	ノードが永続的に HCP システムから削除されました。	アクションは必要ありません。	Notice
1008	Time sync problem	ノードの内部クロックが残りの HCP システムのノードのクロックと同期していません。	問題が解決しない場合は、お問い合わせ先まで連絡してください。	Error
1009	Node added	新規ノードが HCP システムに追加されました。	アクションは必要ありません。	Notice
1010	Previously removed node re-added	システムから削除されたノードの電源が再び入りました。	ノードを再び削除してください。	Error

ID	イベント	説明	アクション	重要度
1012	Metadata DPL is 1	システムはメタデータ DPL1 で設定されました。	アクションは必要ありません。	Notice
1013	Failover	クロスマッピングされたノードに障害が発生しました。もう一方のノードが、これまで障害ノードが管理していた論理ボリュームの管理を引き継ぎました。	障害のノードが自動的に再起動しない場合は、お問い合わせ先まで連絡してください。ノードは手動で再起動しないようにしてください。問題の解析に必要な情報がなくなる原因となる場合があります。	Error
1014	HCP rebooting	HCP システムが再起動しています。	アクションは必要ありません。	Notice
1015	Failover	クロスマッピングされたノードに障害が発生しました。もう一方のノードが、これまで障害ノードが管理していた論理ボリュームの管理を引き継ぎました。	障害のノードが自動的に再起動しない場合は、お問い合わせ先まで連絡してください。ノードは手動で再起動しないようにしてください。問題の解析に必要な情報がなくなる原因となる場合があります。	Error
1016	Volume recovered	論理ボリュームの障害が修復しました。	アクションは必要ありません。	Notice
1017	Node down for an extended amount of time	ノードは長時間利用不可能でした。	お問い合わせ先まで連絡してください。	Error
1018	HCP is read-only	メタデータが使用できないため、HCP システムは読み取り専用になりました。設定の変更とネームスペースコンテンツに対する変更は許可されていません。サービスは一時停止されました。	お問い合わせ先まで連絡してください。	Error
1019	HCP is no longer read-only	これまで使用できなかったメタデータが使用可能になったため、すでに HCP システムはメタデータの使用不可による読み取り専用ではなくなりました。	アクションは必要ありません。	Notice
1020	Region-count setting is invalid	領域計算が、大きすぎる、小さすぎる、または数値でない値に変更されました。領域の実際の値は変更されませんでした。	お問い合わせ先まで連絡してください。	Error
1021	Region count is changing	領域計算が新しい値に設定されました。	アクションは必要ありません。	Notice

ID	イベント	説明	アクション	重要度
1022	Region count has changed	領域計算が新しい値への変更を終了しました。	アクションは必要ありません。	Notice
1023	Region count change has been canceled	領域計算の変更がキャンセルされました。	アクションは必要ありません。	Notice
1024	Support for DPL 1 changed	DPL 1 のサポートが有効化または無効化されました。	アクションは必要ありません。	Warning
1100	Storage capacity warning	HCP ストレージノードの空き容量が少なくなっています。	空き容量が 15%以下になる前に、ストレージ容量を HCP システムに追加することを検討してください。	Warning
1101	Storage capacity critical	HCP ストレージノードの空き容量が、新しいオブジェクトの追加をサポートするには不十分です。	ストレージ容量を追加するか、リポジトリからオブジェクトを削除して、ストレージの空き容量を増やしてください。	Error
1104	Internal SLAB process down	内部 SLAB プロセスが起動していません。このプロセスを再起動するために、ノードは自動的にリポートします。	アクションは必要ありません。問題が解決しない場合は、お問い合わせ先まで連絡してください。	Error
1105	IPMI status became unavailable	ハードウェアの状態により、IPMI 状態が Unavailable になりました。	アクションは必要ありません。	Warning
1106	Location metrics	スケジュールに従って、評価指標のログが取られました。	アクションは必要ありません。	Notice
1107	Adding logical volumes	新しい論理ボリュームが、ノードに追加されています。	アクションは必要ありません。	Notice
1108	Logical volumes added	新しい論理ボリュームがノードに追加されたため、このノードのストレージ容量が増加しました。	アクションは必要ありません。	Notice
1109	Logical volumes added	新しい論理ボリュームがノードに追加されました。このボリュームはゼロコピーフェイルオーバー用のスタンバイボリュームです。	アクションは必要ありません。	Notice
1110	Failed to add logical volumes	新しい論理ボリュームのノードへの追加は失敗しました。	お問い合わせ先まで連絡してください。	Error
1111	Front-end communication status became unavailable	ハードウェアの状態によって、フロントエンド LAN を使用できなくなりました。	アクションは必要ありません。	Warning

ID	イベント	説明	アクション	重要度
1112	Storage status became unavailable	ハードウェアの状態によって、ストレージが無効な状態になりました。	アクションは必要ありません。	Warning
1201	Log handler test message	ユーザが syslog サーバまたは SNMP マネージャにテストメッセージを送信しました。	アクションは必要ありません。	Notice
1202	About to change syslog settings	ユーザが syslog のロギングの設定を変更しました。	アクションは必要ありません。	Notice
1203	Syslog settings changed	ユーザが syslog のロギングの設定を変更しました。	アクションは必要ありません。	Notice
1204	About to change SNMP settings	ユーザが SNMP のロギングの設定を変更しました。	アクションは必要ありません。	Notice
1205	SNMP settings changed	ユーザが SNMP のロギングの設定を変更しました。	アクションは必要ありません。	Notice
1220	Successfully downloaded logs	HCP の内部ログのダウンロードが完了しました。	アクションは必要ありません。	Notice
1221	Started to download logs	ユーザが HCP の内部ログのダウンロードを要求しました。	アクションは必要ありません。	Notice
1222	Failed to download logs	HCP の内部ログの要求されたダウンロードが失敗しました。	再度ログのダウンロードを試みてください。ダウンロードできない場合は、お問い合わせ先まで連絡してください。	Warning
1223	Started to download logs for node	HCP がノードで内部ログのダウンロードを開始しました。	アクションは必要ありません。	Notice
1224	Successfully downloaded logs for node	HCP がノードで内部ログのダウンロードを終了しました。	アクションは必要ありません。	Notice
1225	Failed to download logs for node	HCP がノードからの内部ログのダウンロードに失敗し、次のノードに引き継がれています。	アクションは必要ありません。	Warning
1226	Logs marked	ユーザが HCP の内部ログにメッセージを書き込みました。	アクションは必要ありません。	Notice
1227	Log encryption key uploaded	ユーザが HCP の内部ログのダウンロード時に使用する暗号鍵をアップロードしました。	アクションは必要ありません。	Notice

ID	イベント	説明	アクション	重要度
1228	Log encryption key deleted	ユーザが HCP の内部ログのダウンロード時に使用した暗号鍵を削除しました。	アクションは必要ありません。	Notice
1229	Log download preparation started	ユーザが HCP 内部ログのダウンロードを要求しました。	アクションは必要ありません。	Notice
1230	Log download preparation complete	ログダウンロードの準備が完了し、HCP 内部ログはダウンロードできます。	アクションは必要ありません。	Notice
1231	Log download has started	HCP 内部ログは HTTP クライアントへのストリーミングを開始しました。	アクションは必要ありません。	Notice
1232	Log download has completed	HCP 内部ログのダウンロードが完了しました。	アクションは必要ありません。	Notice
1980	Service schedule activated	ユーザはサービスのスケジュールをアクティブにしました。	アクションは必要ありません。	Notice
1981	Service schedule activation failed	ユーザはサービスのスケジュールをアクティブにしようとしたが、失敗しました。	スケジュールが削除されていないか確認してください。スケジュールが削除されていない場合は、お問い合わせ先にご連絡ください。	Error
1982	Service schedule created	ユーザがサービスのスケジュールを作成しました。	アクションは必要ありません。	Notice
1983	Service schedule updated	ユーザがサービスのスケジュールを更新しました。	アクションは必要ありません。	Notice
1984	Service schedule deleted	ユーザがサービスのスケジュールを削除しました。	アクションは必要ありません。	Notice
2000	Protection service started	保護サービスが起動しました。	アクションは必要ありません。	Notice
2001	Protection service finished: run complete	保護サービスが完了しました。	アクションは必要ありません。	Notice
2003	Protection service stopped without finishing	保護サービスがすべてのオブジェクトを実証することなく中断されました。	アクションは必要ありません。	Warning
2004	Protection service changed protection sets	保護サービスが保護セットを変更しました。	アクションは必要ありません。	Notice
2007	Protection service beginning repairs	保護サービスが違反の修復を開始しました。	アクションは必要ありません。	Warning
2008	Protection service: irreparable object	保護サービスが修復できない違反を検出しました。	お問い合わせ先まで連絡してください。	Error

ID	イベント	説明	アクション	重要度
2010	Garbage collection service started	ガーベジコレクションサービスが起動しました。	アクションは必要ありません。	Notice
2011	Garbage collection service finished: run complete	ガーベジコレクションサービスが完了しました。	アクションは必要ありません。	Notice
2013	Garbage collection stopped without finishing	ガーベジコレクションサービスが実行を完了することなく停止しました。ガーベジコレクションサービスは後で自動的に再開します。	アクションは必要ありません。	Warning
2017	Garbage collection service beginning repairs	ガーベジコレクションサービスが違反の修復を開始しました。	アクションは必要ありません。	Notice
2020	Scavenging service started	スカビンジングサービスが起動しました。	アクションは必要ありません。	Notice
2021	Scavenging service finished: run complete	スカビンジングサービスが完了しました。	アクションは必要ありません。	Notice
2022	Scavenging service finished: run bypassed object(s)	スカビンジングサービスが完了しました。幾つかのオブジェクトは、この実行でスカビンジングされませんでした。これらは今後の実行でチェックされます。	アクションは必要ありません。	Notice
2023	Scavenging service stopped without finishing	スカビンジングサービスが実行を完了することなく停止しました。スカビンジングは後で自動的に再開します。	アクションは必要ありません。	Warning
2027	Scavenging service beginning repairs	スカビンジングサービスが修復を開始しました。	アクションは必要ありません。	Warning
2029	Scavenging service irreparable object	スカビンジングサービスはオブジェクトを修復できませんでした。修復は後でリトライされる可能性があります。	システム管理コンソールを使って、システムが正常かどうかを検証してください。問題が解決しない場合は、お問い合わせ先まで連絡してください。	Error
2030	Capacity balancing service started	容量バランスサービスが起動しました。	アクションは必要ありません。	Notice
2031	Capacity balancing service finished: run complete	容量バランスサービスが完了しました。	アクションは必要ありません。	Notice
2032	Capacity balancing service finished: run bypassed object(s)	幾つかのオブジェクトが、容量バランスサービスの実行中にバイパスされました。これらのオブジェクトはその	アクションは必要ありません。	Notice

ID	イベント	説明	アクション	重要度
		後の実行で処理され ます。		
2033	Capacity balancing service stopped without finishing	容量バランスサービス が実行を完了するこ となく停止しました。	アクションは必要あり ません。	Warning
2037	Capacity balancing service beginning repairs	容量バランスサービス が修復を開始しまし た。	アクションは必要あり ません。	Warning
2040	Content verification service started	コンテンツ検証サービ スが起動しました。	アクションは必要あり ません。	Notice
2041	Content verification service stopped: run complete	コンテンツ検証サービ スが完了しました。	アクションは必要あり ません。	Notice
2043	Content verification service stopped without finishing	コンテンツ検証サービ スが完了することなく 停止しました。しばら くするとサービスが再 開します。	アクションは必要あり ません。	Notice
2047	Content verification service beginning repairs	コンテンツ検証サービ スが修復を開始しまし た。	アクションは必要あり ません。	Warning
2048	Content verification service: irreparable object	コンテンツ検証サービ スが修復できない違反 を検出しました。	お問い合わせ先まで連 絡してください。	Error
2050	Duplicate elimination service started	重複排除サービスが起 動しました。	アクションは必要あり ません。	Notice
2051	Duplicate elimination service finished: run complete	重複排除サービスが完 了しました。	アクションは必要あり ません。	Notice
2052	Duplicate elimination service finished: run bypassed object(s)	重複排除サービスが完 了しました。幾つかの オブジェクトは、この 実行でチェックされま せんでした。これらは 今後の実行でチェック されます。	アクションは必要あり ません。	Notice
2053	Duplicate elimination service policy stopped without finishing	重複排除サービスが、 マージ段階中に実行を 完了することなく停止 しました。サービスは 後で再開します。	アクションは必要あり ません。	Warning
2057	Duplicate elimination service beginning repairs	重複排除サービスがオ ブジェクトのマージを 開始しました。	アクションは必要あり ません。	Notice
2080	Compression service started	圧縮サービスが起動し ました。	アクションは必要あり ません。	Notice
2081	Compression service finished:run complete	圧縮サービスが完了し ました。	アクションは必要あり ません。	Notice
2082	Compression service stopped without finishing	圧縮サービスが実行を 完了することなく停止 しました。サービスは 後で再開します。	アクションは必要あり ません。	Warning

ID	イベント	説明	アクション	重要度
2083	Service could not start	サービスの実行が要求されましたが、何らかの理由により開始できませんでした。	アクションは必要ありません。	Warning
2105	Replication link created	ユーザがレプリケーションリンクを作成しました。	アクションは必要ありません。	Notice
2106	Replication link suspended	レプリケーションリンクが中断しました。	アクションは必要ありません。	Notice
2107	Replication link resumed	中断したレプリケーションリンクが再開しました。	アクションは必要ありません。	Notice
2108	Replication link failure	レプリケーションリンクが動作していません。	リモートシステムへのネットワーク接続を確認してください。	Error
2109	Replication link deleted	レプリケーションリンクが削除されました。	このイベントが予想外の場合は、お問い合わせ先まで連絡してください。	Warning
2110	Replication link read-only	レプリケーションリンクに含まれるテナントとディレクトリは、このシステムでは現在読み取り専用です。	アクションは必要ありません。	Notice
2111	Replication link authorized	レプリケーションリンクに権限が付与されました。	アクションは必要ありません。	Notice
2112	Replication link updated	ユーザがレプリケーションリンクの設定を変更しました。	アクションは必要ありません。	Notice
2113	Replication link failed over	ユーザがレプリケーションリンクをフェイルオーバーしました。複製されたテナントとディレクトリは現在、レプリカでは読み書き可能、プライマリシステムでは読み取り専用です。	クライアントの要求をレプリカシステムにリダイレクトしてください。	Notice
2114	Replication link failed back	データリカバリが完了しました。複製されたテナントとディレクトリは、プライマリシステムでは読み書き可能、レプリカでは読み取り専用です。	アクションは必要ありません。	Notice
2115	Replication data recovery started	データリカバリがレプリケーションリンクで開始しました。複製されたテナントとディレクトリは、レプリカでは読み書き可能、プラ	システム管理コンソールでリカバリの進捗を監視してください。	Warning

ID	イベント	説明	アクション	重要度
		イマリシステムでは読み取り専用です。		
2116	Replication data recovery completed	データリカバリがレプリケーションリンクで完了しました。現在、レプリケーションされたディレクトリは、レプリカで読み書き可能、プライマリシステムで読み取り専用になっています。	クライアントの要求をプライマリシステムにリダイレクトしてください。	Warning
2117	Replication link missing on remote system	このシステムで設定されたレプリケーションリンクがリモートシステムにありません。リンクが中断しています。	レプリケーションリンクのリストアを実行してください。	Error
2118	Object replicated with collisions	レプリケーションされているオブジェクトが対象システムの既存のオブジェクトと競合します。オブジェクトは対象システムの.lost+foundディレクトリに保存されています。	アクションは必要ありません。	Warning
2119	Object did not replicate	オブジェクトがレプリケーションされませんでした。	お問い合わせ先まで連絡してください。	Error
2120	Object did not replicate; will retry later	オブジェクトがレプリケーションされませんでした。オブジェクトのレプリケーションは後で再試行されます。	このオブジェクトが最終的にレプリケーションされるかどうか、レプリカを監視してください。オブジェクトが1週間以内にレプリケーションされない場合は、お問い合わせ先まで連絡してください。	Warning
2121	Duplicate elimination service sort started	重複排除サービスが実行のソート段階を開始しました。	アクションは必要ありません。	Notice
2122	Duplicate elimination service sort finished	重複排除サービスが実行のソート段階を正常に終了しました。	アクションは必要ありません。	Notice
2123	Duplicate elimination service sort stopped without finishing	重複排除サービスが、実行を完了しないでソート段階で停止しました。サービスは後で再開します。	アクションは必要ありません。	Warning
2126	Replica capacity limit reached	レプリカの容量が不十分なため、HCPはレプリケーションリンクを一時停止しました。	レプリカにストレージ容量を追加し、レプリケーションリンクを再開してください。	Warning

ID	イベント	説明	アクション	重要度
2140	Replication SSL certificate downloaded	ユーザがレプリケーションのために SSL サーバ証明書をダウンロードしました。	アクションは必要ありません。	Notice
2141	New replication SSL certificate uploaded	ユーザが新しいレプリケーションクライアント証明書をアップロードしました。	アクションは必要ありません。	Notice
2142	Replication SSL certificate deleted	ユーザがレプリケーションクライアント証明書を削除しました。	アクションは必要ありません。	Notice
2144	Replication link rejected	レプリケーションリンクが拒絶されました。	このイベントが予想外の場合は、お問い合わせ先まで連絡してください。	Warning
2145	Replication link final data recovery pass started	レプリケーションリンクで最終データリカバリ処理が開始しました。複製されたテナントとディレクトリは現在、プライマリシステムとレプリカの両方で読み取り専用です。	アクションは必要ありません。	Warning
2146	Replication link suspended automatically	問題が発生したため、レプリケーションリンクは一時停止になりました。	プライマリシステム、レプリカ、およびネットワークが正常であることを確認してください。その後、リンクを再開してください。	Error
2147	Replication adversely affected due to failed network connections	フロントエンドネットワーク接続が使用できません。	ハードウェアが正常に機能していることを確認してください。問題がある場合は、お問い合わせ先まで連絡してください。	Error
2148	Replication automatically paused for a tenant due to error	HCP 単独では回復できない問題により、テナントのレプリケーションは自動的に一時停止されました。	プライマリシステム、レプリカ、およびネットワークが正常であること、またテナントの不一致がなかったことを確認してください。次に、一時停止されたテナントのレプリケーションを再開してください。	Error
2149	Replication paused for a tenant	ユーザはテナントのレプリケーションを一時停止しました。	アクションは必要ありません。	Notice
2150	Replication resumed for a tenant	ユーザはテナントのレプリケーションを再開しました。	アクションは必要ありません。	Notice

ID	イベント	説明	アクション	重要度
2151	Replication link suspended according to schedule	レプリケーションリンクはスケジュールに従って保留されました。	アクションは必要ありません。	Notice
2152	Replication link performance level changed according to schedule	レプリケーションリンクの性能レベルが、スケジュールに従って変更されました。	アクションは必要ありません。	Notice
2153	Replication link schedule updated	レプリケーションリンクのスケジュールが更新されました。	アクションは必要ありません。	Notice
2300	User account created	ユーザがユーザアカウントを作成しました。	アクションは必要ありません。	Notice
2301	User account updated	ユーザがユーザアカウントを変更しました。	アクションは必要ありません。	Notice
2302	User account deleted	ユーザがユーザアカウントを削除しました。	アクションは必要ありません。	Notice
2303	User authenticated	システム管理コンソールへのユーザログインが認証されました。	アクションは必要ありません。	Notice
2304	Authentication attempt by unknown user	ユーザが不明なユーザ名でログインを試みました。	ユーザを有効なユーザ名とパスワードでログインさせてください。	Warning
2305	Account reenabled by timer	無効なセキュリティユーザアカウントが自動的に再び有効になりました。	アクションは必要ありません。	Notice
2306	Account is disabled	ユーザが無効なアカウントでログインを試みました。	ユーザがログインできるように、ユーザアカウントを再び有効にしてください。	Warning
2307	Account has been inactive for too long	ユーザがしばらく使用していなかったために無効になったアカウントでログインを試みました。	ユーザがログインできるように、ユーザアカウントを再び有効にしてください。	Warning
2308	Account does not include the required roles	ユーザが必要なロールを付与されていないアカウントでログインを試みました。	ユーザがログインできるように、必要なロールが付与されるようアカウントを変更してください。	Warning
2309	Password is invalid	ユーザが無効なパスワードでログインを試みました。	ユーザを有効なユーザ名とパスワードでログインさせてください。	Warning
2311	Password changed	ユーザがユーザアカウントのパスワードを変更しました。	アクションは必要ありません。	Notice
2312	Account enabled	ユーザアカウントが有効になっています。	アクションは必要ありません。	Notice
2313	Account disabled	ユーザアカウントが無効になっています。	アクションは必要ありません。	Notice

ID	イベント	説明	アクション	重要度
2314	Account disabled due to too many failed logins	上限を超えてログインに失敗したため、ユーザアカウントは自動的に無効になりました。	ユーザアカウントを再び有効にし、有効なユーザ名とパスワードでユーザにログインさせてください。	Warning
2315	Account will be reenabled	セキュリティユーザアカウントが待機後に再び自動的に有効になります。	アクションは必要ありません。	Notice
2316	All accounts reset	ユーザがユーザアカウントを初期設定に再設定しました。すべてのアカウントは削除され、初期アカウントが再作成されました。	アクションは必要ありません。	Warning
2400	New SSL server certificate uploaded	ユーザが SSL サーバ証明書をダウンロードしました。	アクションは必要ありません。	Notice
2401	New SSL server certificate signing request generated	ユーザが新しい証明書署名を要求しました。	アクションは必要ありません。	Notice
2402	New SSL server certificate generated	ユーザが新しい SSL サーバ証明書の作成を要求しました。	アクションは必要ありません。	Notice
2403	SSL server certificate expires soon	SSL サーバ証明書は間もなく期限切れになります。証明書の期限が切れると、このシステムへの HTTPS アクセスやレプリケーションができなくなります。	SSL サーバ証明書を更新してください。	Warning
2404	SSL server certificate expired	SSL サーバ証明書の期限が切れています。このシステムへの HTTP アクセスは許可されず、レプリケーションは停止します。	SSL サーバ証明書を更新してください。	Error
2405	Trusted replication server certificate expires soon	信頼されたレプリカサーバ証明書が、間もなく期限切れになります。期限が切れると、証明書を取得したシステムとのレプリケーションができなくなります。	リモートシステムで SSL サーバ証明書を更新した場合は、信頼されたレプリケーションサーバの証明書として、このシステムでも証明書を更新してください。	Error
2406	Trusted replication server certificate expired	信頼されたレプリカサーバ証明書は期限が切れています。証明書を取得したシステムとのレプリケーションが停止します。	リモートシステムで SSL サーバ証明書を更新した場合は、信頼されたレプリケーションサーバの証明書として、このシステムでも証明書を更新してください。	Error

ID	イベント	説明	アクション	重要度
2600	Node shutdown requested from System Management Console	ユーザがシステム管理コンソールからノードをシャットダウンしました。	アクションは必要ありません。	Notice
2601	HCP shutdown requested from System Management Console	ユーザがシステム管理コンソールから HCP をシャットダウンしました。	アクションは必要ありません。	Notice
2602	Service started	ユーザがシステム管理コンソールからサービスを開始しました。	アクションは必要ありません。	Notice
2603	Service stopped	ユーザがシステム管理コンソールからサービスを停止しました。	アクションは必要ありません。	Notice
2604	Service enabled	ユーザがシステム管理コンソールからサービスを有効にしました。	アクションは必要ありません。	Notice
2605	Service disabled	ユーザがシステム管理コンソールからサービスを無効にしました。	アクションは必要ありません。	Notice
2606	Configuration changed	ユーザが HCP コンポーネントの設定値を変更しました。	アクションは必要ありません。	Notice
2607	Version upgraded	ユーザが内部メッセージバージョンを更新し、ソフトウェアアップグレードを完了させました。	アクションは必要ありません。	Notice
2609	Irreparable object acknowledged	ユーザが修復不可能なオブジェクトを承認しました。	アクションは必要ありません。	Warning
2610	All irreparable objects acknowledged	ユーザがすべての修復不可能なオブジェクトを承認しました。	アクションは必要ありません。	Warning
2611	Eject CD requested from System Management Console	ユーザがノードから CD トレイのイジェクトを要求しました。	アクションは必要ありません。	Notice
2614	Unauthorized action	ユーザがユーザアカウントに権限を付与されていない操作を要求しました。	ユーザがこの操作を行うことが許可されている場合は、ユーザアカウントに必要なロールを追加してください。	Warning
2615	Configuration changed	ユーザが HCP コンポーネントの設定値を変更しました。	アクションは必要ありません。	Notice
2616	Upgrade started	ユーザが HCP ソフトウェアのアップグレードを開始しました。	アクションは必要ありません。	Notice
2617	Node restart requested from System Management Console	ユーザがシステム管理コンソールからノードを再起動しました。	アクションは必要ありません。	Notice

ID	イベント	説明	アクション	重要度
2618	HCP restart requested from System Management Console	ユーザがシステム管理コンソールから HCP を再起動しました。	アクションは必要ありません。	Notice
2619	Restart or shutdown command could not be executed	ノードの再起動またはシャットダウンは実行できませんでした。 ノードはすでに停止している可能性があります。	アクションは必要ありません。	Notice
2620	Upgrade completed successfully	HCP ソフトウェアのアップグレードは正常に完了しました。	アクションは必要ありません。	Notice
2800	Network interface down	ネットワークインタフェースがダウンしました。	ハードウェアが正常に機能していることをチェックしてください。問題がある場合は、お問い合わせ先まで連絡してください。	Error
2801	Network interface up	ネットワークインタフェースが回復しました。	アクションは必要ありません。	Notice
2802	Temperature sensor alarm	温度センサが推奨範囲を外れた温度を示しています。	ハードウェアが正常に機能していることをチェックしてください。問題がある場合は、お問い合わせ先まで連絡してください。	Error
2803	Temperature sensor alarm removed	温度センサが許容動作温度に戻ったことを示しています。	アクションは必要ありません。	Notice
2804	Fan sensor alarm	ファンセンサが推奨範囲を外れたファン回転速度を示しています。	ハードウェアが正常に機能していることをチェックしてください。問題がある場合は、お問い合わせ先まで連絡してください。	Error
2805	Fan sensor alarm removed	ファンセンサが許容ファン回転速度に戻ったことを示しています。	アクションは必要ありません。	Notice
2806	Voltage sensor alarm	電圧センサが推奨範囲を外れた電圧を示しています。	ハードウェアが正常に機能していることをチェックしてください。問題がある場合は、お問い合わせ先まで連絡してください。	Error
2807	Voltage sensor alarm removed	電圧センサが許容動作電圧に戻ったことを示しています。	アクションは必要ありません。	Notice
2808	File system alarm	ファイルシステムが容量警告しきい値に到達しました。	空き容量が 15% 以下になる前に、ストレージ	Error

ID	イベント	説明	アクション	重要度
			ジ容量を HCP システムに追加することを検討してください。	
2809	File system alarm removed	ファイルシステムが容量警告しきい値を下回りました。	アクションは必要ありません。	Notice
2810	Disk device alarm	ディスクデバイスが完全な機能状態ではないことを示しています。	ハードウェアが正常に機能していることをチェックしてください。問題がある場合は、お問い合わせ先まで連絡してください。	Error
2811	Disk device alarm removed	ディスクデバイスが完全な機能状態に戻ったことを示しています。	アクションは必要ありません。	Notice
2812	Power supply alarm	電源に問題があることを示しています。	ハードウェアが正常に機能していることをチェックしてください。問題がある場合は、お問い合わせ先まで連絡してください。	Error
2813	Power supply alarm removed	電源が完全な機能状態に戻ったことを示しています。	アクションは必要ありません。	Notice
2814	Processor alarm	プロセッサに問題があることを示しています。	ハードウェアが正常に機能していることをチェックしてください。問題がある場合は、お問い合わせ先まで連絡してください。	Error
2815	Processor alarm removed	プロセッサが完全な機能状態に戻ったことを示しています。	アクションは必要ありません。	Notice
2816	Multipath degraded	ストレージへの冗長ファイバーチャネル接続が正常に機能していません。	ストレージへの接続をチェックしてください。問題がある場合は、お問い合わせ先まで連絡してください。	Error
2817	Multipath restored	下位ストレージへの冗長アクセスが回復しました。	アクションは必要ありません。	Notice
2820	IP configuration information changed	ユーザがシステム管理コンソールを使用してネットワーク設定を変更しました。	アクションは必要ありません。	Notice
2830	Time is unsynchronized	時刻同期を行おうとしましたが、外部タイムサーバと内部タイムサーバのどちらにもアクセスできませんでした。	ネットワークと時間の設定が正しいか確認してください。	Warning
2831	Using internal time server	時刻同期を行おうとしましたが、外部タイム	内部タイムサーバを使用するようシステムが	Notice

ID	イベント	説明	アクション	重要度
		サーバにアクセスできませんでした。	設定されている場合、アクションは必要ありません。それ以外の場合は、ネットワークと時間の設定が正しいか確認してください。	
2832	Using external time server	時刻同期のための外部タイムサーバへのアクセスが成功しました。	アクションは必要ありません。	Notice
2833	Lost connection to external time server	外部タイムサーバと同期を取るための接続ができませんでした。	ネットワーク設定と時間設定が正しいことをチェックしてください。	Notice
2834	System time changed due to resynchronization with external time server	HCP が起動したとき、システム時間のずれが 1000 秒を超えていたため、外部タイムサーバと再度同期を取りました。この時間の変更が、オブジェクトの保管に影響を与える場合があります。	ネットワークと時間の設定が正しいことを確認してください。	Warning
2843	Front-end Ethernet communication error	ネットワークスイッチを使用できないおそれがあります。	ハードウェアの稼働状態を確認してください。問題がある場合は、お問合せ先にご連絡ください。	Error
2844	Front-end Ethernet communication restored	フロントエンド LAN に接続するイーサネットインターフェースが正常な状態に戻りました。	アクションは必要ありません。	Notice
3000	System updated	HCP システムプロパティが更新されました。	アクションは必要ありません。	Notice
3001	Tenant created	ユーザがテナントを作成しました。	アクションは必要ありません。	Notice
3002	Tenant updated	ユーザがテナントを更新しました。	アクションは必要ありません。	Notice
3003	Tenant deleted	ユーザがテナントを削除しました。	アクションは必要ありません。	Notice
3026	Tenant over soft quota	テナントが所有するすべてのネームスペースで使用中の容量が、テナントに設定されたソフト Quota を超過しています。	テナントレベル管理者に連絡し、テナントのハード Quota を増加してもらってください。	Warning
3027	Tenant under soft quota	テナントが所有するすべてのネームスペースで使用中の容量が、テナントに設定されたソフト Quota 未満です。	アクションは必要ありません。	Warning

ID	イベント	説明	アクション	重要度
3029	Installed new HCP version	HCP ソフトウェアの新バージョンが正常にインストールされました。	アクションは必要ありません。	Notice
3030	Tenant at namespace quota	テナントが所有するネームスペース数が、ネームスペース Quota の制限に達しています。	アクションは必要ありません。	Notice
3031	Tenant over namespace quota	テナントが所有するネームスペース数が、ネームスペース Quota の制限を超過しています。	テナントのネームスペース Quota の設定を見直すか、テナント管理者の権限でネームスペースを削除してください。	Warning
3034	Namespace maximum reached	ネームスペース数が、HCP システムで許可されている上限に達しています。	アクションは必要ありません。	Warning
3035	Namespace maximum exceeded	ネームスペース数が、HCP システムで許可されている上限を超過しています。	テナント管理者の権限で、上限を下回るまでネームスペースを削除してください。	Warning
3036	Username conflict	テナントでユーザアカウントのユーザ名が重複しています。テナント内のユーザアカウントのユーザ名は一意にする必要があります。	テナント管理者の権限で、アカウントのユーザ名を変更するか、重複しているアカウントをマージしてください。	Warning
4103	Failure creating search index for a namespace	HCP がネームスペースのインデックスを作成できませんでした。	アクションは必要ありません。このエラーが再度発生する場合、お問い合わせ先まで連絡してください。	Warning
4105	Failure creating search index for a namespace	HCP はネームスペースにインデックスを作成できませんでした。後で再試行します。	アクションは必要ありません。この状態が続く場合は、お問い合わせ先まで連絡してください。	Warning
4106	Ingest-time override setting has been changed	保存期間の無効設定が変更されました。	アクションは必要ありません。	Warning
4107	Chassis communication error	HCP は SNMP 経由で指定されたシャーシに接続できませんでした。	指定されたシャーシへのネットワーク接続を確認してください。また、指定されたシャーシで、HCP の最小番号のストレージからの SNMP アクセスを許可する設定になっていることを確認してください。	Error

ID	イベント	説明	アクション	重要度
4108	Communication from unknown node	ほかの HCP システムのノードが、ネットワーク上で検出されました。	バックエンド LAN を確認してください。バックエンド LAN は、一つの HCP システムだけで構成されます。	Error
4204	Back-end switch communication failure	バックエンドスイッチと HCP が通信できません。	スイッチの稼働状態を確認してください。問題が解決しない場合は、お問合せ先にご連絡ください。	Error
4205	Back-end switch failure	バックエンドスイッチに問題が発生しました。	スイッチの稼働状態を確認してください。問題が解決しない場合は、お問合せ先にご連絡ください。	Error
4206	Back-end switch restored	バックエンドスイッチが稼働している状態に戻りました。	アクションは必要ありません。	Notice
4209	Time server changed	ユーザは HCP システムのタイムサーバを変更しました。	アクションは必要ありません。	Notice
4210	Current time changed	ユーザは HCP システムの現在時刻を変更しました。	アクションは必要ありません。	Notice
4211	Time zone changed	ユーザは HCP システムのタイムゾーンを変更しました。	アクションは必要ありません。	Notice
4212	Service plan created	ユーザはサービスプランを作成しました。	アクションは必要ありません。	Notice
4213	Service plan updated	ユーザはサービスプランを更新しました。	アクションは必要ありません。	Notice
4214	Service plan deleted	ユーザはサービスプランを削除しました。	アクションは必要ありません。	Notice
4215	Failover completed	クロスマッピングされたノードに障害が発生しました。もう一方のノードが、これまで障害ノードが管理していた論理ボリュームの管理を引き継ぎました。	アクションは必要ありません。	Warning
4216	Failback started	障害が発生したノードは、クロスマッピングされたもう一方のノードから論理ボリュームの管理を引き戻し、再び利用するためのプロセスを開始しました。	アクションは必要ありません。	Warning
4217	Failback completed	障害から復旧したノードは、クロスマッピングされたもう一方のノードにフェールオーバーしていた論理ボ	アクションは必要ありません。	Notice

ID	イベント	説明	アクション	重要度
		リユームの管理を引き戻しました。		
4218	Monitored component added	ユーザは監視するコンポーネントを追加しました。	アクションは必要ありません。	Notice
4219	Monitored component deleted	ユーザは監視するコンポーネントを削除しました。	アクションは必要ありません。	Notice

D.2 HCP システムログ

システム管理コンソールの [Overview] ページがシステム全体の状態を表示する一方で、HCP システムログを使ってより詳細なレベルでシステムの動作を監視できます。ログは次のようなシステムイベントを記録します。

- ノードとサービスの起動
- システム設定の変更
- 論理ボリュームの故障
- システム管理コンソールへのユーザログイン

イベントについて記録されるそれぞれのエントリをメッセージと呼びます。システムログは、HCP システムがインストールされて以降に書き込まれたすべてのメッセージを保存します。

システム管理コンソールにはログが複数の形式で表示されます。

- [System Events] ページの [All Events] パネルには、システムログ内の、ユーザのロールに応じて表示が許可されるすべてのメッセージが表示されます。
- [System Events] ページの [Security Events] パネルには、無効なユーザ名によるシステム管理コンソールへのログイン試行に関するメッセージだけが表示されます。Security ロールを持つユーザだけがこのパネルを表示できます。
- [Overview] ページの [Major Events] パネルには、主なイベント（ノードの追加や故障など）に関するメッセージだけが表示されます。
- [Storage Node] ページの [Node Events] パネルには、特定のノードに関連するイベントのメッセージだけが表示されます。

システムログに表示されるメッセージと、メッセージに対応してとる必要があるアクションについての詳細は、「[D.1 システムログメッセージ一覧](#)」を参照してください。

D.3 HCP 内部ログ

システム管理コンソールに表示されるシステムログに加え、HCP は内部ログを保存します。内部ログは、HCP システムのさまざまな構成要素の処理動作を記録します。システムに問題が発生すると、保守員は内部ログを使って問題を解析・解決します。

トラブルシューティングをサポートするため、内部ログをダウンロードし、HCP サポートセンターへ送信できます。取り扱いを容易にするため、HCP はログを一つのファイルにダウンロードします。

HCP は最大で 35 日の内部ログを保存します。この間はどのような期間のログもダウンロードできます。これを行うときは、必ずシステムに問題が発生したすべての日を含むようにします。

ログをダウンロードするとき、サポートセンターにメッセージを送信できます。このメッセージには、問題の説明、自身の連絡先、対象のケース番号（割り当てられている場合）、保守員が問題を解決する支援となりうるその他の情報が含まれるようにします。

HCP はダウンロードされたログファイルを暗号化します。保守員だけがログを解読するのに必要な鍵を持ちます。

重要：

内部ログをダウンロードすると、HCP システムに負荷が掛かります。HVFP 連携のマイグレーションや EV 連携のアーカイブ実行時間帯を避けてダウンロードしてください。

内部ログのダウンロードは次の 2 段階に分けて行われる処理です。

1. ログをダウンロード用に準備してください。
2. ログを含むファイルをダウンロード・保存してください。

HCP 内部ログを準備し、ダウンロードするには、次の手順に従ってください。

1. システム管理コンソールのトップレベルメニュー内の、[Monitoring] の上にマウスカーソルを置き、セカンダリメニューを表示してください。
2. セカンダリメニュー内の [Internal Logs] をクリックしてください。

ルール：

HCP 内部ログをダウンロードするユーザは、ユーザアカウントに Administrator ロールが付与されている必要があります。

3. [Internal Logs] ページで、[Download Internal Logs] をクリックしてください。
4. [Download Internal Logs] パネルで、次の操作を行なってください。
 - [Start date] フィールドに、必要とするログの期間の開始日を入力してください。日付フォーマットとして、mm/dd/yyyy を使用してください。
 - [End date] フィールドに、必要とするログの期間の終了日を入力してください。日付フォーマットとして、mm/dd/yyyy を使用してください。
 - 必要な場合、[Insert this message into the internal logs] フィールドに、ログをダウンロードする前にログに書き込みたいメッセージとダウンロードされるログに付随するマニフェストに含めたいメッセージを入力してください。この文は、任意の UTF-8 文字を使用して、空白を含めて 1,024 文字以内で作成できます。
5. [Prepare Internal Logs] ボタンをクリックしてください。

HCP はダウンロードできるようにログを準備します。準備中、HCP は [Download Internal Logs] パネルに進行状況を報告します。この処理中は、[Internal Logs] ページを表示したままにする必要はありません。

HCP がログの準備を終えると、[Prepare Internal Logs] ボタンが [Download Internal Logs] に変わります。

メモ：

以前にログを準備したがダウンロードしなかった場合、再度内部ログを準備するには、[Cancel] ボタンをクリックして、[Prepare Internal Logs] ボタンを再度有効にしてください。

6. [Download Internal Logs] ボタンをクリックしてください。
7. システムからファイルの保存を促された場合、ファイルを保存する場所を選択してください。

HCP はログをダウンロードします。ダウンロード中、HCP は [Download Internal Logs] パネルに進行状況を報告します。この処理中は、[Internal Logs] ページを表示したままにする必要はありません。

メモ：

ファイルの保存を促すプロンプトが表示される前に、一定の時間内でアクションがなくシステム管理コンソールのセッションがタイムアウトになった場合、ダウンロードは失敗します。この場合、タイムアウトの時間を増やし、ダウンロードを再度試みてください。



テナントログメッセージ

テナントログには、テナントレベルとネームスペースレベルで発生したイベントに関するメッセージが記録されます。テナントログに HCP が書き込むメッセージについて説明します。

□ E.1 テナントログメッセージ一覧

E.1 テナントログメッセージ一覧

メッセージをイベント ID 順に次の表に示します。表のメッセージごとの項目を次に示します。

- イベント ID
- メッセージが関係するイベントを識別するメッセージの概要
- メッセージの説明
- メッセージに対応してとる必要があるアクション（アクションが必要な場合）
- メッセージの重要度

表 E-1 テナントログメッセージ

ID	イベント	説明	アクション	重要度
2006	HCP found an irreparable object	保護サービスが修復できない違反を検出しました。	HCP のお問い合わせ先まで連絡してください。	Error
2028	HCP found an irreparable object	HCP はオブジェクトを修復できませんでした。修復は後で再試行される場合があります。	HCP のお問い合わせ先まで連絡してください。	Error
2046	HCP found an irreparable object	コンテンツ検証サービスが修復できない違反を検出しました。	HCP のお問い合わせ先まで連絡してください。	Error
2070	Object has been shredded	オブジェクトがシュレディングされました。	アクションは必要ありません。	Notice
2154	Additional namespaces included in tenant replication	表示されたネームスペースが選択され、テナントのレプリケーションに追加されました。	アクションは必要ありません。	Notice
2155	One or more namespaces removed from tenant replication	表示されたネームスペースがテナントのレプリケーションから削除されました。	アクションは必要ありません。	Notice
2156	Replication automatically paused for this tenant	テナントのレプリケーションが、表示された理由で自動的に一時停止されました。	一つ以上のネームスペース名の不一致が原因である場合、表示された各ネームスペースの名前を変更してください。レプリカが一つ以上のネームスペースの DPL をサポートしていないことが原因である場合は、表示された各ネームスペースの DPL を下げてください。またどちらの場合でも、そのネームスペースのレプリケーションを選択解除できません。必要な変更を行った後は、問題が解決されたことを HCP	Error

ID	イベント	説明	アクション	重要度
			システム管理者に連絡してください。	
2157	Namespace replication collision detected	ネームスペースのレプリケーションの不一致が検出されたため、テナント管理者の介入が必要となる可能性があります。	一つ以上のネームスペース名の不一致が原因である場合、表示された各ネームスペースの名前を変更してください。レプリカが一つ以上のネームスペースのDPLをサポートしていないことが原因である場合は、表示された各ネームスペースのDPLを下げてください。またどちらの場合でも、そのネームスペースのレプリケーションを選択解除できます。必要な変更を行った後は、問題が解決されたことをHCPシステム管理者に連絡してください。	Notice
2160	User account replicated with collisions	バージョン 4.x で同じユーザ ID を持つ二つのユーザアカウントのどちらか、または両方がシステム上で変更されたため、不整合となっているプロパティがあります。バージョン 4.x からのレプリケーションの際に、プロパティの値がアカウントのロールから削除されました。	ユーザアカウントが正しく設定されていることを確認してください。	Warning
2900	Privileged delete requested	ユーザが特権削除操作を要求しました。	アクションは必要ありません。	Notice
2901	Privileged delete succeeded	特権削除操作が成功しました。	アクションは必要ありません。	Notice
2902	Privileged delete failed	特権削除操作が失敗しました。	アクションは必要ありません。	Notice
2906	Retention mode set	ネームスペース保管モードが変更されています。	アクションは必要ありません。	Notice
2907	Privileged purge requested	ユーザが特権パージ操作を要求しました。	アクションは必要ありません。	Notice
2908	Privileged purge succeeded	特権パージ操作が成功しました。	アクションは必要ありません。	Notice
2909	Privileged purge failed	特権パージ操作が失敗しました。	アクションは必要ありません。	Notice
3004	Namespace created	ユーザがネームスペースを作成しました。	アクションは必要ありません。	Notice

ID	イベント	説明	アクション	重要度
3005	Namespace updated	ユーザがネームスペースを更新しました。	アクションは必要ありません。	Notice
3006	Namespace deleted	ユーザがネームスペースを削除しました。	アクションは必要ありません。	Notice
3011	User account created	ユーザがユーザアカウントを作成しました。	アクションは必要ありません。	Notice
3012	User account updated	ユーザがユーザアカウントを更新しました。	アクションは必要ありません。	Notice
3013	User account deleted	ユーザがユーザアカウントを削除しました。	アクションは必要ありません。	Notice
3014	User account is disabled	無効なユーザアカウントでユーザがログインを試みました。	ユーザがログインできるように、ユーザアカウントを再び有効にしてください。	Warning
3015	User account disabled	ユーザアカウントが無効になりました。	アクションは必要ありません。	Notice
3016	User account enabled	ユーザアカウントが有効になりました。	アクションは必要ありません。	Notice
3017	User account password changed	ユーザがユーザアカウントのパスワードを変更しました。	アクションは必要ありません。	Notice
3018	User account failed login	ユーザが、ユーザアカウントに一致しないユーザ名とパスワードでログインを試みました。	ユーザに、ユーザアカウントに対して有効なユーザ名とパスワードでログインさせてください。	Warning
3020	Namespace over hard quota	ネームスペースのストレージ使用量が、設定ハード Quota を超えています。	ネームスペースからのオブジェクトの一部削除か、ハード Quota の容量増加をしてください。	Warning
3021	Namespace under hard quota	ネームスペースのストレージ使用量が、設定ハード Quota 未満です。	アクションは必要ありません。	Warning
3022	Namespace over soft quota	ネームスペースのストレージ使用量が、設定されたソフト Quota を超えています。	ネームスペースからのオブジェクトの一部削除か、ハード Quota の容量増加を検討してください。	Warning
3023	Namespace under soft quota	ネームスペースのストレージ使用量が、設定ソフト Quota 未満です。	アクションは必要ありません。	Warning
3024	Tenant over soft quota	テナントが所有するすべてのネームスペースのストレージ使用量が、テナントに設定したソフト Quota を超えています。	ネームスペースからのオブジェクトの一部削除か、テナントのハード Quota の容量増加を検討してください。	Warning
3025	Tenant under soft quota	テナントが所有するすべてのネームスペース	アクションは必要ありません。	Warning

ID	イベント	説明	アクション	重要度
		のストレージ使用量が、テナントに設定したソフト Quota 未満です。		
3028	Failed user account login attempt	ユーザアカウントが認証できないため、テナントへログインできませんでした。	アクションは必要ありません。	Warning
3032	Tenant at namespace quota	テナントが所有するネームスペース数が、ネームスペース Quota の制限に達しています。	アクションは必要ありません。	Notice
3033	Tenant over namespace quota	テナントが所有するネームスペース数が、ネームスペース Quota の制限を超過しています。	ネームスペースを削除するか、HCP システム管理者の権限でネームスペース Quota の設定を見直してください。	Warning
3037	Username conflict	ユーザアカウントのユーザ名が重複しています。ユーザアカウントのユーザ名は一意にする必要があります。	アカウントのユーザ名を変更するか、重複しているアカウントをマージしてください。	Warning
3508	HCP found an irreparable object	HCP は、修復できなかった破損オブジェクトを検出しました。	HCP システムレベル管理者に連絡してください。	Error
4000	HCP search facility indexing failure	HCP が、インデックス付けできないオブジェクトを検出しました。	HCP システムレベル管理者に連絡してください。	Error
4002	User account created	ユーザがユーザアカウントを作成しました。	アクションは必要ありません。	Notice
4003	User account updated	ユーザがユーザアカウントを変更しました。	アクションは必要ありません。	Notice
4004	User account deleted	ユーザがユーザアカウントを削除しました。	アクションは必要ありません。	Notice
4005	User authenticated	テナント管理コンソールへのユーザログインが認証されました。	アクションは必要ありません。	Notice
4006	Authentication attempt by unknown user	ユーザが不明なユーザ名でログインを試みました。	ユーザを有効なユーザ名とパスワードでログインさせてください。	Warning
4007	Account reenabled by timer	権限のないセキュリティユーザアカウントが自動的に再び有効になりました。	アクションは必要ありません。	Notice
4008	Account is disabled	ユーザが権限のないアカウントでログインを試みました。	ユーザがログインできるように、ユーザアカウントを再び有効にしてください。	Warning
4009	Account has been inactive for too long	ユーザが、しばらく使用されていない	ユーザがログインできるように、ユーザアカ	Warning

ID	イベント	説明	アクション	重要度
		めに無効になったアカウントでログインを試みました。	アカウントを再び有効にしてください。	
4010	Account does not include the required roles	ユーザが必要なロールを含まないアカウントでログインを試みました。	ユーザがログインできるように、アカウントを変更して必要なロールを含むようにしてください。	Warning
4011	Password is invalid	ユーザが権限のないパスワードでログインを試みました。	ユーザを有効なユーザ名とパスワードでログインさせてください。	Warning
4013	Password changed	ユーザがユーザアカウントのパスワードを変更しました。	アクションは必要ありません。	Notice
4014	Account enabled	ユーザアカウントは有効になりました。	アクションは必要ありません。	Notice
4015	Account disabled	ユーザアカウントが無効になっています。	アクションは必要ありません。	Notice
4016	Account disabled due to too many failed logins	上限を超えてログインに失敗したため、ユーザアカウントは自動的に無効になりました。	ユーザアカウントを再び有効にし、有効なユーザ名とパスワードでユーザにログインさせてください。	Warning
4017	Account will be reenabled	セキュリティユーザアカウントが待機後に再び自動的に有効になりました。	アクションは必要ありません。	Notice
4019	Configuration changed	ユーザが HCP コンポーネントの設定値を変更しました。	アクションは必要ありません。	Notice
4020	Configuration changed	ユーザが HCP コンポーネントの設定値を変更しました。	アクションは必要ありません。	Notice
4021	Irreparable object acknowledged	ユーザが修復不可能なオブジェクトを承認しました。	アクションは必要ありません。	Warning
4022	All irreparable objects acknowledged	ユーザがすべての修復不可能なオブジェクトを承認しました。	アクションは必要ありません。	Warning
4023	Unauthorized action	ユーザがユーザアカウントで許可されていない操作を要求しました。	ユーザにこの操作を許可する場合は、ユーザアカウントに必要なロールを付与してください。	Warning
4024	User account created	ユーザがユーザアカウントを作成しました。	アクションは必要ありません。	Notice
4025	User account updated	ユーザがユーザアカウントを更新しました。	アクションは必要ありません。	Notice
4026	User account deleted	ユーザがユーザアカウントを削除しました。	アクションは必要ありません。	Notice

ID	イベント	説明	アクション	重要度
4027	User account is disabled	無効なユーザアカウントでユーザがログインを試みました。	ユーザがログインできるように、ユーザアカウントを再び有効にしてください。	Warning
4028	User account disabled due to too many failed logins	上限を超えてログインに失敗したため、ユーザアカウントは自動的に無効になりました。	ユーザがログインできるように、ユーザアカウントを再び有効にしてください。	Warning
4029	User account disabled	ユーザアカウントが無効になっています。	アクションは必要ありません。	Notice
4031	User account password changed	ユーザがユーザアカウントのパスワードを変更しました。	アクションは必要ありません。	Notice
4100	Object replicated with collisions	レプリケーションされているオブジェクトが対象システムの既存のオブジェクトと競合します。オブジェクトは、対象システムの .lost+found ディレクトリに保存されています。	アクションは必要ありません。	Warning
4101	Object did not replicate	オブジェクトがレプリケーションされませんでした。	HCP システムレベル管理者に連絡してください。	Error
4102	Object did not replicate; will retry later	オブジェクトがレプリケーションされませんでした。オブジェクトのレプリケーションは後で再試行されます。	このオブジェクトが最終的にレプリケーションされるかどうか、レプリカを監視してください。オブジェクトが1週間以内にレプリケーションされない場合は、HCP システムレベル管理者に連絡してください。	Warning
4220	Namespace tags updated	ユーザがネームスペースのタグを更新しました。	アクションは必要ありません。	Notice



略語一覧

ここでは、このマニュアルで使用している略語を示します。

- F.1 このマニュアルで使用している略語

F.1 このマニュアルで使用している略語

このマニュアルでは、次に示す略語を使用しています。

AC	Alternating Current
ASCII	American Standard Code for Information Interchange
BIND	Berkeley Internet Name Domain
CA	certificate authority
CPU	central processing unit
CSR	certificate signing request
DNS	Domain Name System
DPL	Data Protection Level
FQDN	fully qualified domain name
GUI	graphical user interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ID	identifier
IP	Internet Protocol
IP-SW	IP switch
IPMI	Intelligent Platform Management Interface
JSON	JavaScript Object Notation
LAN	local area network
LED	light-emitting diode
LU	logical unit
MIB	management information base
MTU	maximum transmission unit
NAT	network address translation
NDMP	Network Data Management Protocol
NIC	network interface card
NTP	Network Time Protocol
OS	operating system
PC	personal computer
RAID	Redundant Array of Independent Disks
SAIN	SAN-attached array of independent nodes
SAN	storage area network
SFP	Small Form Factor Pluggable
SNMP	Simple Network Management Protocol
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
URL	Uniform Resource Locator
UTF	UCS Transformation Format
VPN	Virtual Private Network
WAN	wide area network
WORM	Write Once, Read Many

XML	Extensible Markup Language
-----	----------------------------

