

CLUSTERPRO® X 4.1 *for Solaris*

スタートアップガイド

2019.05.17

第2版

CLUSTERPRO

改版履歴

版数	改版日付	内 容
1	2019/04/10	新規作成
2	2019/05/17	内部バージョン 4.1.1-1 に対応

免責事項

本書の内容は、予告なしに変更されることがあります。

日本電気株式会社は、本書の技術的もしくは編集上の間違い、欠落について、一切責任をおいせん。

また、お客様が期待される効果を得るために、本書に従った導入、使用および使用効果につきましては、お客様の責任とさせていただきます。

本書に記載されている内容の著作権は、日本電気株式会社に帰属します。本書の内容の一部または全部を日本電気株式会社の許諾なしに複製、改変、および翻訳することは禁止されています。

商標情報

CLUSTERPRO® は、日本電気株式会社の登録商標です。

Oracle、Oracle Database、Solaris、MySQL、Tuxedo、WebLogic Server、Container、Java およびすべての Java 関連の商標は、Oracle Corporationおよびその子会社、関連会社の米国およびその他の国における商標または登録商標です。

Microsoft、Windows、Windows Server、Internet Explorer、Azure、Hyper-V は、米国 Microsoft Corporation の米国およびその他の国における登録商標です。

Firefoxは、Mozilla Foundation の商標または登録商標です。

Google Chrome は、Google, Inc.の商標または登録商標です。

PostgreSQL は、PostgreSQL Global Development Group の登録商標です。

本書に記載されたその他の製品名および標語は、各社の商標または登録商標です。

目次

はじめに	ix
対象読者と目的	ix
本書の構成	ix
CLUSTERPRO マニュアル体系	x
本書の表記規則	xi
最新情報の入手先	xii
第 1 章 クラスタシステムとは?	13
クラスタシステムの概要	14
HA (High Availability) クラスタ	15
共有ディスク型	15
データミラー型	17
障害検出のメカニズム	19
共有ディスク型の諸問題	20
ネットワークパーティション症状(Split-brain-syndrome)	20
クラスタリソースの引き継ぎ	21
データの引き継ぎ	21
アプリケーションの引き継ぎ	22
フェイルオーバー総括	22
Single Point of Failureの排除	23
共有ディスク	23
共有ディスクへのアクセスパス	24
LAN	25
可用性を支える運用	26
運用前評価	26
障害の監視	26
第 2 章 CLUSTERPRO の使用方法	27
CLUSTERPRO とは?	28
CLUSTERPRO の製品構成	29
CLUSTERPRO のソフトウェア構成	30
CLUSTERPRO の障害監視のしくみ	30
サーバ監視とは	31
業務監視とは	32
内部監視とは	32
監視できる障害と監視できない障害	32
サーバ監視で検出できる障害とできない障害	32
業務監視で検出できる障害とできない障害	33
ネットワークパーティション解決	34
フェイルオーバーのしくみ	35
フェイルオーバーリソース	36
フェイルオーバー型クラスタのシステム構成	37
共有ディスク型のハードウェア構成	40
クラスタオブジェクトとは?	41
リソースとは?	42
ハートビートリソース	42
ネットワークパーティション解決リソース	42
グループリソース	42
モニタリソース	43
CLUSTERPRO を始めよう!	45

最新情報の確認	45
クラスタシステムの設計	45
クラスタシステムの構築	45
クラスタシステムの運用開始後の障害対応	45
第 3 章 CLUSTERPRO の動作環境	47
ハードウェア	48
スペック	48
ソフトウェア	49
CLUSTERPRO Serverの動作環境	49
動作可能なバージョン	49
監視オプションの動作確認済アプリケーション情報	50
必要メモリ容量とディスクサイズ	51
Cluster WebUI の動作環境	52
動作確認済OS、ブラウザ	52
必要メモリ容量/ディスク容量	52
第 4 章 最新バージョン情報	53
CLUSTERPRO とマニュアルの対応一覧	54
機能強化	55
修正情報	57
第 5 章 注意制限事項	59
システム構成検討時	60
機能一覧と必要なライセンス	60
共有ディスクの要件について	60
IPv6 環境について	60
ネットワーク構成について	61
モニタリソース回復動作の「最終動作前にスクリプトを実行する」について	61
NIC Link Up/Down モニタリソース	62
メール通報について	62
ネットワーク警告灯の要件について	62
OS インストール前、OS インストール時	63
/opt/nec/clusterpro のファイルシステムについて	63
依存するライブラリ	63
OS インストール後、CLUSTERPRO インストール前	64
通信ポート番号	64
通信ポート番号の自動割り当て範囲の変更	65
ポート数不足を回避する設定について	66
時刻同期の設定	66
共有ディスクについて	66
OS 起動時間の調整	66
ネットワークの確認	66
ipmiutil, OpenIPMI について	67
nsupdate, nslookup について	67
Samba モニタリソースについて	67
CLUSTERPRO の情報作成時	69
CLUSTERPRO インストールパス配下のディレクトリ、ファイルについて	69
環境変数	69
強制停止機能、筐体 ID ランプ連携	69
サーバのリセット、パニック、パワーオフ	69
グループリソースの非活性異常時の最終アクション	70
遅延警告割合	70
ディスクモニタリソースの監視方法TURについて	70
LAN ハートビートの設定について	71
COM ハートビートの設定について	71

スクリプトのコメントなどで取り扱える 2 バイト系文字コードについて	71
仮想マシングループのフェイルオーバー排他属性の設定について	71
CLUSTERPRO 運用後	72
回復動作中の操作制限	72
コマンド編に記載されていない実行形式ファイルやスクリプトファイルについて	72
EXEC リソースで使用するスクリプトファイルについて	72
活性時監視設定のモニタリソースについて	72
Cluster WebUI について	73
サービス起動時間について	74
ログ収集について	74
フローティング IP、仮想 IP リソースについて	74
CLUSTERPRO の構成変更時	75
グループ共通プロパティの排他ルールについて	75
グループリソースの追加、削除について	75
外部連携モニタリソースのクラスタ統計情報の設定について	75
CLUSTERPRO バージョンアップ時	76
機能変更一覧	76
削除機能一覧	76
パラメータ削除一覧	76
既定値変更一覧	77
パラメータ移動一覧	80
第 6 章 アップグレード手順.....	81
CLUSTERPRO X のアップグレード手順.....	82
X 3.0/3.1/3.2/3.3 から X 4.0/4.1 へのアップグレード.....	82
付録 A 用語集	83
付録 B 索引.....	87

はじめに

対象読者と目的

『CLUSTERPRO® X スタートアップガイド』は、CLUSTERPRO をはじめてご使用になるユーザの皆様を対象に、CLUSTERPRO の製品概要、クラスタシステム導入のロードマップ、他マニュアルの使用方法についてのガイドラインを記載します。また、最新の動作環境情報や制限事項などについても紹介します。

本書の構成

第 1 章	クラスタシステムとは？ クラスタシステムおよびCLUSTERPRO の概要について説明します。
第 2 章	CLUSTERPRO の使用方法 クラスタシステムの使用方法および関連情報について説明します。
第 3 章	CLUSTERPRO の動作環境 導入前に確認が必要な最新情報について説明します。
第 4 章	最新バージョン情報 CLUSTERPRO の最新バージョンについての情報を示します。
第 5 章	注意制限事項 既知の問題と制限事項について説明します。
第 6 章	アップグレード手順 既存バージョンから最新版へのアップデート情報について説明します。
付録 A	用語集
付録 B	索引

CLUSTERPRO マニュアル体系

CLUSTERPRO のマニュアルは、以下の 6 つに分類されます。各ガイドのタイトルと役割を以下に示します。

『CLUSTERPRO X スタートアップガイド』(Getting Started Guide)

すべてのユーザを対象読者とし、製品概要、動作環境、アップデート情報、既知の問題などについて記載します。

『CLUSTERPRO X インストール&設定ガイド』(Install and Configuration Guide)

CLUSTERPRO を使用したクラスタシステムの導入を行うシステムエンジニアと、クラスタシステム導入後の保守・運用を行うシステム管理者を対象読者とし、CLUSTERPRO を使用したクラスタシステム導入から運用開始前までに必須の事項について説明します。実際にクラスタシステムを導入する際の順番に則して、CLUSTERPRO を使用したクラスタシステムの設計方法、CLUSTERPRO のインストールと設定手順、設定後の確認、運用開始前の評価方法について説明します。

『CLUSTERPRO X リファレンスガイド』(Reference Guide)

管理者、および CLUSTERPRO を使用したクラスタシステムの導入を行うシステムエンジニアを対象とし、CLUSTERPRO の運用手順、各モジュールの機能説明およびトラブルシューティング情報等を記載します。『インストール&設定ガイド』を補完する役割を持ちます。

『CLUSTERPRO X メンテナンスガイド』(Maintenance Guide)

管理者、および CLUSTERPRO を使用したクラスタシステム導入後の保守・運用を行うシステム管理者を対象読者とし、CLUSTERPRO のメンテナンス関連情報を記載します。

『CLUSTERPRO X ハードウェア連携ガイド』(Hardware Feature Guide)

管理者、および CLUSTERPRO を使用したクラスタシステムの導入を行うシステムエンジニアを対象読者とし、特定ハードウェアと連携する機能について記載します。『インストール&設定ガイド』を補完する役割を持ちます。

『CLUSTERPRO X 互換機能ガイド』(Legacy Feature Guide)

管理者、および CLUSTERPRO を使用したクラスタシステムの導入を行うシステムエンジニアを対象読者とし、CLUSTERPRO X 4.0 WebManager および Builder に関する情報について記載します。

本書の表記規則

本書では、注意すべき事項、重要な事項および関連情報を以下のように表記します。

注：は、重要ではあるがデータ損失やシステムおよび機器の損傷には関連しない情報を表します。

重要：は、データ損失やシステムおよび機器の損傷を回避するために必要な情報を表します。

関連情報：は、参照先の情報の場所を表します。

また、本書では以下の表記法を使用します。

表記	使用方法	例
[] 角かっこ	コマンド名の前後 画面に表示される語 (ダイアログ ボックス、メニューなど) の前後	[スタート] をクリックします。 [プロパティ] ダイアログボックス
コマンドライン中の [] 角かっこ	かっこ内の値の指定が省略可能であることを示します。	<code>clpstat -s[-h host_name]</code>
#	Solaris ユーザが、root でログインしていることを示すプロンプト	<code># clpcl -s -a</code>
モノスペースフォント (courier)	パス名、コマンドライン、システムからの出力 (メッセージ、プロンプトなど)、ディレクトリ、ファイル名、関数、パラメータ	<code>/Solaris/4.1/jpn/server/</code>
モノスペースフォント太字 (courier)	ユーザが実際にコマンドラインから入力する値を示します。	以下を入力します。 <code># clpcl -s -a</code>
モノスペースフォント斜体 (courier)	ユーザが有効な値に置き換えて入力する項目	<code>pkgadd -d NECclusterpro-<バージョン番号>-<リリース番号>-x86_64.pkg</code>

最新情報の入手先

最新の製品情報については、以下のWebサイトを参照してください。

<https://jpn.nec.com/clusterpro/>

第 1 章 クラスタシステムとは？

本章では、クラスタシステムの概要について説明します。

本章で説明する項目は以下のとおりです。

• クラスタシステムの概要.....	14
• HA (High Availability) クラスタ.....	15
• 障害検出のメカニズム	19
• クラスタリソースの引き継ぎ	21
• Single Point of Failureの排除	23
• 可用性を支える運用.....	26

クラスタシステムの概要

現在のコンピュータ社会では、サービスを停止させることなく提供し続けることが成功への重要なカギとなります。例えば、1 台のマシンが故障や過負荷によりダウンしただけで、顧客へのサービスが全面的にストップしてしまうことがあります。そうすると、莫大な損害を引き起こすだけでなく、顧客からの信用を失いかねません。

このような事態に備えるのがクラスタシステムです。クラスタシステムを導入することにより、万一のときのシステム稼働停止時間(ダウンタイム)を最小限に食い止めたり、負荷を分散させたりすることでシステムダウンを回避することが可能になります。

クラスタとは、「群れ」「房」を意味し、その名の通り、クラスタシステムとは「複数のコンピュータを一群(または複数群)にまとめて、信頼性や処理性能の向上を狙うシステム」です。クラスタシステムには様々な種類があり、以下の 3 つに分類できます。この中で、CLUSTERPRO はハイアベイラビリティクラスタに分類されます。

◆ HA (ハイ アベイラビリティ) クラスタ

通常時は一方が現用系として業務を提供し、現用系障害発生時に待機系に業務を引き継ぐような形態のクラスタです。高可用性を目的としたクラスタで、データの引継ぎも可能です。共有ディスク型、データミラー型、遠隔クラスタがあります。

◆ 負荷分散クラスタ

クライアントからの要求を適切な負荷分散ルールに従って負荷分散ホストに要求を割り当てるクラスタです。高スケーラビリティを目的としたクラスタで、一般的にデータの引継ぎはできません。ロードバランスクラスタ、並列データベースクラスタがあります。

◆ HPC(High Performance Computing)クラスタ

全てのノードの CPU を利用し、単一の業務を実行するためのクラスタです。高性能化を目的としており、あまり汎用性はありません。

なお、HPC の 1 つであり、より広域な範囲のノードや計算機クラスタまでを束ねた、グリッドコンピューティングという技術も近年話題に上ることが多くなっています。

HA (High Availability) クラスタ

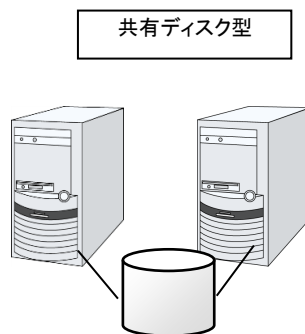
一般的にシステムの可用性を向上させるには、そのシステムを構成する部品を冗長化し、Single Point of Failure をなくすことが重要であると考えられます。Single Point of Failure とは、コンピュータの構成要素（ハードウェアの部品）が 1 つしかないために、その箇所で障害が起きると業務が止まってしまう弱点のことを指します。HA クラスタとは、サーバを複数台使用して冗長化することにより、システムの停止時間を最小限に抑え、業務の可用性 (availability) を向上させるクラスタシステムをいいます。

システムの停止が許されない基幹業務システムはもちろん、ダウンタイムがビジネスに大きな影響を与えてしまうそのほかのシステムにおいても、HA クラスタの導入が求められています。

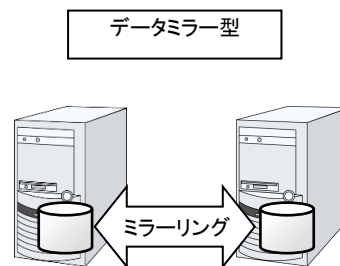
HA クラスタは、共有ディスク型とデータミラー型に分けることができます。以下にそれぞれのタイプについて説明します。

共有ディスク型

クラスタシステムでは、サーバ間でデータを引き継がなければなりません。このデータを共有ディスク上に置き、ディスクを複数のサーバで利用する形態を共有ディスク型といいます。



- 共有ディスクが必要になるため高価
- 大規模データを扱うシステム向き



- 共有ディスクが不要なので安価
- ミラーリングのためデータ量が多くないシステム向き

図 1-1 HA クラスタ構成図

業務アプリケーションを動かしているサーバ(現用系サーバ)で障害が発生した場合、クラスタシステムが障害を検出し、待機系サーバで業務アプリケーションを自動起動させ、業務を引き継がせます。これをフェイルオーバーといいます。クラスタシステムによって引き継がれる業務は、ディスク、IP アドレス、アプリケーションなどのリソースと呼ばれるもので構成されています。

クラスタ化されていないシステムでは、アプリケーションをほかのサーバで再起動させると、クライアントは異なる IP アドレスに再接続しなければなりません。しかし、多くのクラスタシステムでは、業務単位に仮想 IP アドレスを割り当てています。このため、クライアントは業務を行っているサーバが現用系か待機系かを意識する必要はなく、まるで同じサーバに接続しているように業務を継続できます。

データを引き継ぐためには、ファイルシステムの整合性をチェックしなければなりません。通常は、ファイルシステムの整合性をチェックするためにチェックコマンド（例えば、Solaris の場合は fsck）を実行しますが、ファイルシステムが大きくなるほどチェックにかかる時間が長くなり、その間業務が止まってしまいます。この問題を解決するために、ジャーナリングファイルシステムなどでフェイルオーバー時間を短縮します。

業務アプリケーションは、引き継いだデータの論理チェックをする必要があります。例えば、データベースならばロールバックやロールフォワードの処理が必要になります。これらによって、クライアントは未コミットの SQL 文を再実行するだけで、業務を継続することができます。

障害からの復帰は、障害が検出されたサーバを物理的に切り離して修理後、クラスタシステムに接続すれば待機系として復帰できます。業務の継続性を重視する実際の運用の場合は、ここまでの復帰で十分な状態です。

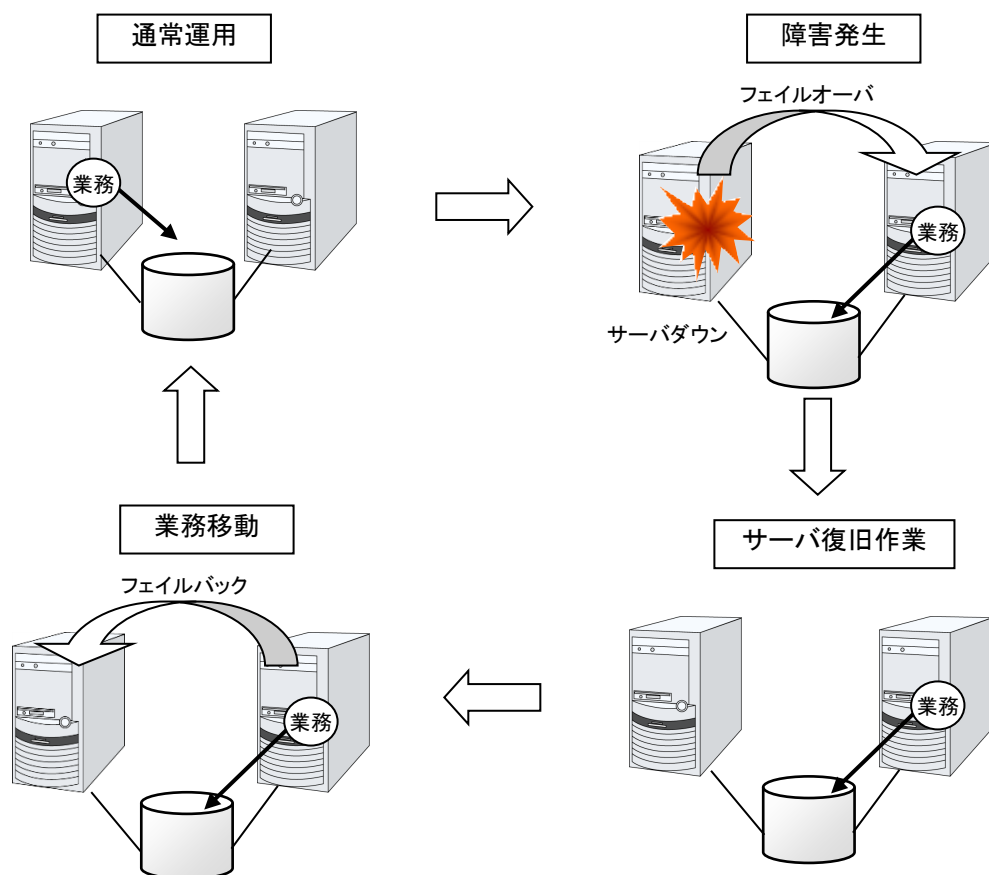


図 1-2 障害発生から復旧までの流れ

フェイルオーバー先のサーバのスペックが十分でなかったり、双方向スタンバイで過負荷になるなどの理由で元のサーバで業務を行うのが望ましい場合には、元のサーバで業務を再開するためにフェイルバックを行います。

図 1-3 のように、業務が 1 つであり、待機系では業務が動作しないスタンバイ形態を片方向スタンバイといいます。業務が 2 つ以上で、それぞれのサーバが現用系かつ待機系である形態を双方向スタンバイといいます。

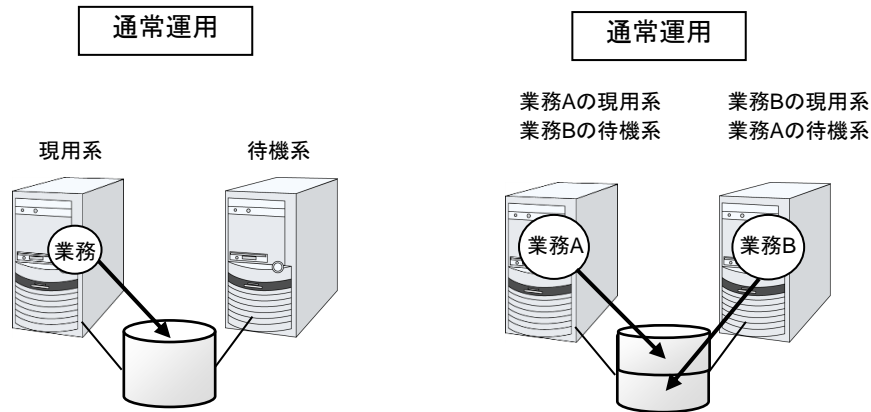


図 1-3 HA クラスタの運用形態

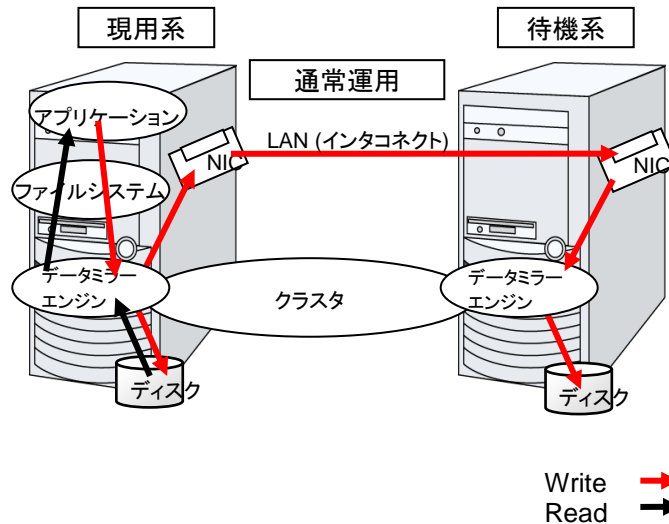
データミラー型

前述の共有ディスク型は大規模なシステムに適していますが、共有ディスクはおおむね高価なためシステム構築のコストが膨らんでしまいます。そこで共有ディスクを使用せず、各サーバのディスクをサーバ間でミラーリングすることにより、同じ機能をより低価格で実現したクラスタシステムをデータミラー型といいます。

しかし、サーバ間でデータをミラーリングする必要があるため、大量のデータを必要とする大規模システムには向きません。

アプリケーションからの Write 要求が発生すると、データミラーエンジンはローカルディスクにデータを書き込むと同時に、インタコネクトを通して待機系サーバにも Write 要求を振り分けます。インタコネクトとは、サーバ間をつなぐネットワークのことで、クラスタシステムではサーバの死活監視のために必要になります。データミラータイプでは死活監視に加えてデータの転送に使用することがあります。待機系のデータミラーエンジンは、受け取ったデータを待機系のローカルディスクに書き込むことで、現用系と待機系間のデータを同期します。

アプリケーションからの Read 要求に対しては、単に現用系のディスクから読み出すだけです。



注: CLUSTERPRO X 4.1 for Solaris ではデータミラー型のクラスタを構築することはできません。

図 1-4 データミラーの仕組み

データミラーの応用例として、スナップショットバックアップの利用があります。データミラータイプのクラスタシステムは 2 カ所に共有のデータを持っているため、待機系のサーバをクラスタから切り離すだけで、バックアップ時間をかけることなくスナップショットバックアップとしてディスクを保存する運用が可能です。

フェイルオーバーの仕組みと問題点

ここまで、一口にクラスタシステムといってもフェイルオーバークラスタ、負荷分散クラスタ、HPC(High Performance Computing)クラスタなど、さまざまなクラスタシステムがあることを説明しました。そして、フェイルオーバークラスタは HA(High Availability)クラスタと呼ばれ、サーバそのものを多重化することで、障害発生時に実行していた業務をほかのサーバで引き継ぐことにより、業務の可用性(Availability)を向上することを目的としたクラスタシステムであることを見てきました。次に、クラスタの実装と問題点について説明します。

障害検出のメカニズム

クラスタソフトウェアは、業務継続に問題をきたす障害を検出すると業務の引き継ぎ(フェイルオーバー)を実行します。フェイルオーバー処理の具体的な内容に入る前に、簡単にクラスタソフトウェアがどのように障害を検出するか見ておきましょう。

ハートビートとサーバの障害検出

クラスタシステムにおいて、検出すべき最も基本的な障害はクラスタを構成するサーバ全てが停止してしまうものです。サーバの障害には、電源異常やメモリエラーなどのハードウェア障害や OS のパニックなどが含まれます。このような障害を検出するために、サーバの死活監視としてハートビートが使用されます。

ハートビートは、ping の応答を確認するような死活監視だけでもよいのですが、クラスタソフトウェアによっては、自サーバの状態情報などを相乗りさせて送るものもあります。クラスタソフトウェアはハートビートの送受信を行い、ハートビートの応答がない場合はそのサーバの障害とみなしてフェイルオーバー処理を開始します。ただし、サーバの高負荷などによりハートビートの送受信が遅延することも考慮し、サーバ障害と判断するまである程度の猶予時間が必要です。このため、実際に障害が発生した時間とクラスタソフトウェアが障害を検知する時間とにはタイムラグが生じます。

リソースの障害検出

業務の停止要因はクラスタを構成するサーバ全ての停止だけではありません。例えば、業務アプリケーションが使用するディスク装置や NIC の障害、もしくは業務アプリケーションそのものの障害などによっても業務は停止してしまいます。可用性を向上するためには、このようなリソースの障害も検出してフェイルオーバーを実行しなければなりません。

リソース異常を検出する手法として、監視対象リソースが物理的なデバイスの場合は、実際にアクセスしてみるという方法が取られます。アプリケーションの監視では、アプリケーションプロセスそのものの死活監視のほか、業務に影響のない範囲でサービスポートを試してみるような手段も考えられます。

共有ディスク型の諸問題

共有ディスク型のフェイルオーバークラスタでは、複数のサーバでディスク装置を物理的に共有します。一般的に、ファイルシステムはサーバ内にデータのキャッシュを保持することで、ディスク装置の物理的な I/O 性能の限界を超えるファイル I/O 性能を引き出しています。

あるファイルシステムを複数のサーバから同時にマウントしてアクセスするとどうなるでしょうか？

通常のファイルシステムは、自分以外のサーバがディスク上のデータを更新するとは考えていないので、キャッシュとディスク上のデータとに矛盾を抱えることとなり、最終的にはデータを破壊します。フェイルオーバークラスタシステムでは、次のネットワークパーティション症状などによる複数サーバからのファイルシステムの同時マウントを防ぐために、ディスク装置の排他制御を行っています。

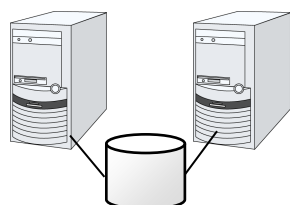


図 1-5 共有ディスクタイプのクラスタ構成

ネットワークパーティション症状(Split-brain-syndrome)

サーバ間をつなぐすべてのインタコネクトが切断されると、ハートビートによる死活監視で互いに相手サーバのダウンを検出し、フェイルオーバー処理を実行してしまいます。結果として、複数のサーバでファイルシステムを同時にマウントしてしまい、データ破壊を引き起こします。フェイルオーバークラスタシステムでは異常が発生したときに適切に動作しなければならないことが理解できると思います。

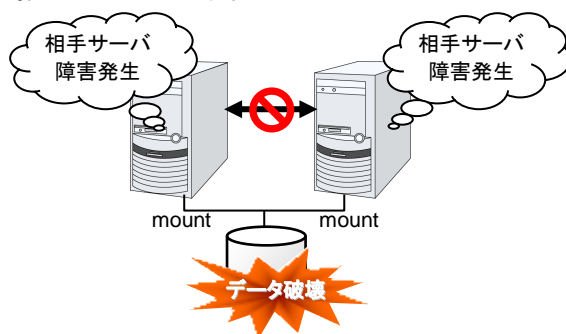


図 1-6 ネットワークパーティション症状

このような問題を「ネットワークパーティション症状」または「スプリットブレインシンドローム (Split-brain-syndrome)」と呼びます。フェイルオーバークラスタでは、すべてのインタコネクトが切断されたときに、確実に共有ディスク装置の排他制御を実現するためのさまざまな対応策が考えられています。

クラスタリソースの引き継ぎ

クラスタが管理するリソースにはディスク、IP アドレス、アプリケーションなどがあります。これらのクラスタリソースを引き継ぐための、フェイルオーバークラスタシステムの機能について説明します。

データの引き継ぎ

クラスタシステムでは、サーバ間で引き継ぐデータは共有ディスク装置上のパーティションに格納します。すなわち、データを引き継ぐとは、アプリケーションが使用するファイルが格納されているファイルシステムを健全なサーバ上でマウントしなおすことにほかなりません。共有ディスク装置は引き継ぐ先のサーバと物理的に接続されているので、クラスタソフトウェアが行うべきことはファイルシステムのマウントだけです。

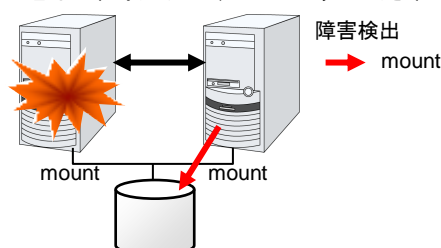


図 1-7 データの引き継ぎ

単純な話のようですが、クラスタシステムを設計・構築するうえで注意しなければならない点があります。

1 つは、ファイルシステムの復旧時間の問題です。引き継ごうとしているファイルシステムは、障害が発生する直前までほかのサーバで使用され、もしかしたらまさに更新中であつたかもしれません。このため、引き継ぐファイルシステムは通常ダーティであり、ファイルシステムの整合性チェックが必要な状態となっています。ファイルシステムのサイズが大きくなると、整合性チェックに必要な時間は莫大になり、場合によっては数時間もの時間がかかってしまいます。それがそのままフェイルオーバー時間(業務の引き継ぎ時間)に追加されてしまい、システムの可用性を低下させる要因になります。

もう 1 つは、書き込み保証の問題です。アプリケーションが大切なデータをファイルに書き込んだ場合、同期書き込みなどを利用してディスクへの書き込みを保証しようとします。ここでアプリケーションが書き込んだと思い込んだデータは、フェイルオーバー後にも引き継がれていることが期待されます。例えばメールサーバは、受信したメールをスプールに確実に書き込んだ時点で、クライアントまたはほかのメールサーバに受信完了を応答します。これによってサーバ障害発生後も、スプールされているメールをサーバの再起動後に再配信することができます。クラスタシステムでも同様に、一方のサーバがスプールへ書き込んだメールはフェイルオーバー後にもう一方のサーバが読み込めることを保証しなければなりません。

アプリケーションの引き継ぎ

クラスタソフトウェアが業務引き継ぎの最後に行う仕事は、アプリケーションの引き継ぎです。フォールトトレラントコンピュータ(FTC)とは異なり、一般的なフェイルオーバークラスタでは、アプリケーション実行中のメモリ内容を含むプロセス状態などを引き継ぎません。すなわち、障害が発生していたサーバで実行していたアプリケーションを健全なサーバで再実行することでアプリケーションの引き継ぎを行います。

例えば、データベース管理システム(DBMS)のインスタンスを引き継ぐ場合、インスタンスの起動時に自動的にデータベースの復旧(ロールフォワード/ロールバックなど)が行われます。このデータベース復旧に必要な時間は、DBMS のチェックポイントインターバルの設定などによってある程度の制御ができますが、一般的には数分程度必要となるようです。

多くのアプリケーションは再実行するだけで業務を再開できますが、障害発生後の業務復旧手順が必要なアプリケーションもあります。このようなアプリケーションのためにクラスタソフトウェアは業務復旧手順を記述できるよう、アプリケーションの起動の代わりにスクリプトを起動できるようにになっています。スクリプト内には、スクリプトの実行要因や実行サーバなどの情報をもとに、必要に応じて更新途中であったファイルのクリーンアップなどの復旧手順を記述します。

フェイルオーバー総括

ここまでの内容から、次のようなクラスタソフトの動作が分かります。

- ◆ 障害検出(ハートビート/リソース監視)
- ◆ ネットワークパーティション状態の解決(NP解決)
- ◆ クラスタ資源切り替え
- データの引き継ぎ
- IP アドレスの引き継ぎ
- アプリケーションの引き継ぎ

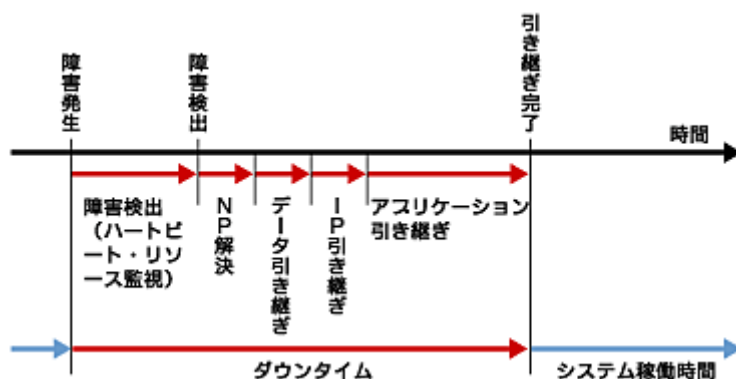


図 1-8 フェイルオーバータイムチャート

クラスタソフトウェアは、フェイルオーバー実現のため、これらの様々な処置を 1 つ 1 つ確実に、短時間で実行することで、高可用性(High Availability)を実現しているのです。

Single Point of Failure の排除

高可用性システムを構築するうえで、求められるもしくは目標とする可用性のレベルを把握することは重要です。これはすなわち、システムの稼働を阻害し得るさまざまな障害に対して、冗長構成をとることで稼働を継続したり、短い時間で稼働状態に復旧したりするなどの施策を費用対効果の面で検討し、システムを設計するということです。

Single Point of Failure(SPOF)とは、システム停止につながる部位を指す言葉であると前述しました。クラスタシステムではサーバの多重化を実現し、システムの SPOF を排除することができますが、共有ディスクなど、サーバ間で共有する部分については SPOF となり得ます。この共有部分を多重化もしくは排除するようシステム設計することが、高可用性システム構築の重要なポイントとなります。

クラスタシステムは可用性を向上させますが、フェイルオーバーには数分程度のシステム切り替え時間が必要となります。従って、フェイルオーバー時間は可用性の低下要因の 1 つともいえます。このため、高可用性システムでは、まず単体サーバの可用性を高める ECC メモリや冗長電源などの技術が本来重要なのですが、ここでは単体サーバの可用性向上技術には触れず、クラスタシステムにおいて SPOF となりがちな下記の 3 つについて掘り下げて、どのような対策があるか見ていきたいと思います。

- ◆ 共有ディスク
- ◆ 共有ディスクへのアクセスパス
- ◆ LAN

共有ディスク

通常、共有ディスクはディスクアレイにより RAID を組むので、ディスクのベアドライブは SPOF となりません。しかし、RAID コントローラを内蔵するため、コントローラが問題となります。多くのクラスタシステムで採用されている共有ディスクではコントローラの二重化が可能になっています。

二重化された RAID コントローラの利点を生かすためには、通常は共有ディスクへのアクセスパスの二重化を行う必要があります。ただし、二重化された複数のコントローラから同時に同一の論理ディスクユニット(LUN)へアクセスできるような共有ディスクの場合、それぞれのコントローラにサーバを 1 台ずつ接続すればコントローラ異常発生時にノード間フェイルオーバーを発生させることで高可用性を実現できます。

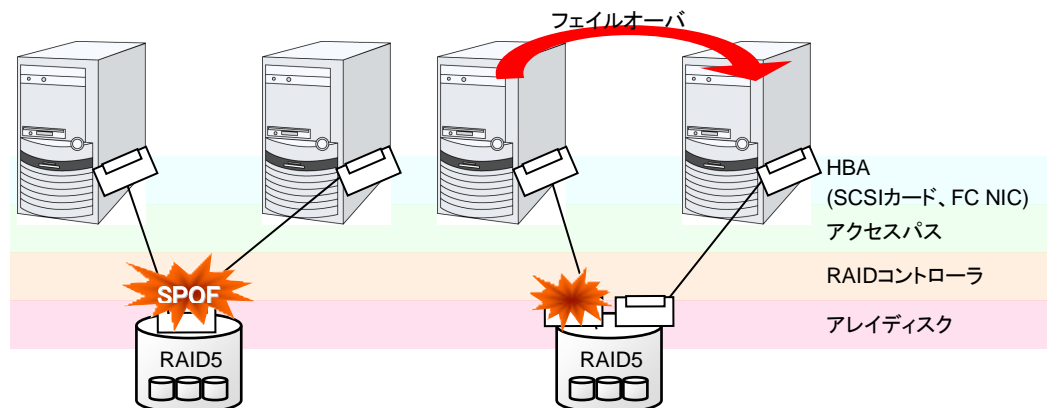


図 1-9 共有ディスクの RAID コントローラとアクセスパスが SPOF となっている例(左)と RAID コントローラとアクセスパスを分割した例

一方、共有ディスクを使用しないデータミラー型のフェイルオーバークラスタでは、すべてのデータをほかのサーバのディスクにミラーリングするため、SPOF が存在しない理想的なシステム構成を実現できます。ただし、欠点とはいええないまでも、次のような点について考慮する必要があります。

- ◆ ネットワークを介してデータをミラーリングすることによるディスクI/O性能(特にwrite性能)
- ◆ サーバ障害後の復旧における、ミラー再同期中のシステム性能(ミラーコピーはバックグラウンドで実行される)
- ◆ ミラー再同期時間(ミラー再同期が完了するまでクラスタに組み込めない)

すなわち、データの参照が多く、データ容量が多くないシステムにおいては、データミラー型のフェイルオーバークラスタを採用するというのも可用性を向上させるポイントといえます。

共有ディスクへのアクセスパス

共有ディスク型クラスタの一般的な構成では、共有ディスクへのアクセスパスはクラスタを構成する各サーバで共有されます。SCSI を例に取れば、1 本の SCSI バス上に 2 台のサーバと共有ディスクを接続するということです。このため、共有ディスクへのアクセスパスの異常はシステム全体の停止要因となり得ます。

対策としては、共有ディスクへのアクセスパスを複数用意することで冗長構成とし、アプリケーションには共有ディスクへのアクセスパスが 1 本であるかのように見せることが考えられます。これを実現するデバイスドライバをパスフェイルオーバードライバなどと呼びます。このパスフェイルオーバードライバを利用し、共有ディスクへのアクセスパスを多重化することが可用性を向上させるポイントになります。

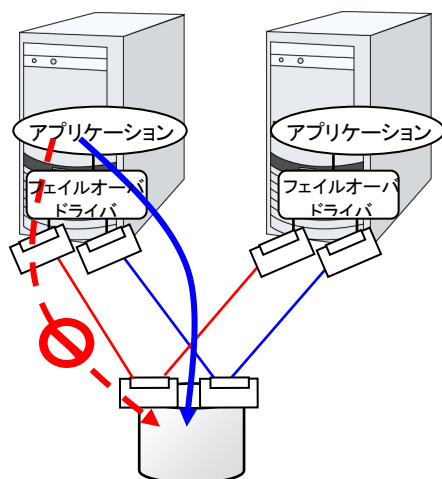


図 1-10 パスフェイルオーバードライバ

LAN

クラスタシステムに限らず、ネットワーク上で何らかのサービスを実行するシステムでは、LAN の障害はシステムの稼働を阻害する大きな要因です。クラスタシステムでは適切な設定を行えば NIC 障害時にノード間でフェイルオーバーを発生させて可用性を高めることは可能ですが、クラスタシステムの外側のネットワーク機器が故障した場合はやはりシステムの稼働を阻害します。

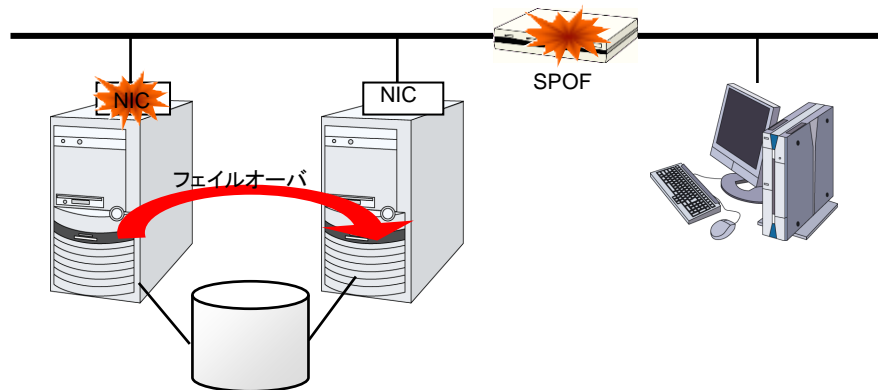


図 1-11 ルータが SPOF となる例

このようなケースでは、LAN を冗長化することでシステムの可用性を高めます。クラスタシステムにおいても、LAN の可用性向上には単体サーバでの技術がそのまま利用可能です。例えば、予備のネットワーク機器の電源を入れずに準備しておき、故障した場合に手動で入れ替えるといった原始的な手法や、高機能のネットワーク機器を冗長配置してネットワーク経路を多重化することで自動的に経路を切り替える方法が考えられます。また、インテル社の ANS ドライバのように NIC の冗長構成をサポートするドライバを利用するということも考えられます。

ロードバランス装置 (Load Balance Appliance) やファイアウォールサーバ (Firewall Appliance) も SPOF となりやすいネットワーク機器です。これらもまた、標準もしくはオプションソフトウェアを利用することで、フェイルオーバー構成を組めるようになっているのが普通です。同時にこれらの機器は、システム全体の非常に重要な位置に存在するケースが多いため、冗長構成をとることはほぼ必須と考えるべきです。

可用性を支える運用

運用前評価

システムトラブルの発生要因の多くは、設定ミスや運用保守に起因するものであるともいわれています。このことから考えても、高可用性システムを実現するうえで運用前の評価と障害復旧マニュアルの整備はシステムの安定稼働にとって重要です。評価の観点としては、実運用に合わせて、次のようなことを実践することが可用性向上のポイントとなります。

- ◆ 障害発生箇所を洗い出し、対策を検討し、擬似障害評価を行い実証する
- ◆ クラスタのライフサイクルを想定した評価を行い、縮退運転時のパフォーマンスなどの検証を行う
- ◆ これらの評価をもとに、システム運用、障害復旧マニュアルを整備する

クラスタシステムの設計をシンプルにすることは、上記のような検証やマニュアルが単純化でき、システムの可用性向上のポイントとなることが分かります。

障害の監視

上記のような努力にもかかわらず障害は発生するものです。ハードウェアには経年劣化があり、ソフトウェアにはメモリリークなどの理由や設計当初のキャパシティプランニングを超えた運用をしてしまうことによる障害など、長期間運用を続ければ必ず障害が発生してしまいます。このため、ハードウェア、ソフトウェアの可用性向上と同時に、さらに重要となるのは障害を監視して障害発生時に適切に対処することです。万が一サーバに障害が発生した場合を例にとると、クラスタシステムを組むことで数分の切り替え時間でシステムの稼働を継続できますが、そのまま放置しておけばシステムは冗長性を失い次の障害発生時にはクラスタシステムは何の意味もなさなくなってしまいます。

このため、障害が発生した場合、すぐさまシステム管理者は次の障害発生に備え、新たに発生したSPOFを取り除くなどの対処をしなければなりません。このようなシステム管理業務をサポートするうえで、リモートメンテナンスや障害の通報といった機能が重要になります。Solarisでは、リモートメンテナンスの面ではいうまでもなく非常に優れていますし、障害を通報する仕組みも整いつつあります。

以上、クラスタシステムを利用して高可用性を実現するうえで必要とされる周辺技術やそのほかのポイントについて説明しました。簡単にまとめると次のような点に注意しましょうということになるかと思います。

- ◆ Single Point of Failureを排除または把握する
- ◆ 障害に強いシンプルな設計を行い、運用前評価に基づき運用・障害復旧手順のマニュアルを整備する
- ◆ 発生した障害を早期に検出し適切に対処する

第 2 章 CLUSTERPRO の使用方法

本章では、CLUSTERPRO を構成するコンポーネントの説明と、クラスタシステムの設計から運用手順までの流れについて説明します。

本章で説明する項目は以下のとおりです。

• CLUSTERPRO とは?.....	28
• CLUSTERPRO の製品構成.....	29
• CLUSTERPRO のソフトウェア構成	30
• ネットワークパーティション解決	34
• フェイルオーバーのしくみ.....	35
• リソースとは?	42
• CLUSTERPRO を始めよう!.....	45

CLUSTERPRO とは？

クラスタについて理解したところで、CLUSTERPRO の紹介を始めましょう。CLUSTERPRO とは、冗長化（クラスタ化）したシステム構成により、現用系のサーバでの障害が発生した場合に、自動的に待機系のサーバで業務を引き継がせることで、飛躍的にシステムの可用性と拡張性を高めることを可能にするソフトウェアです。

CLUSTERPRO の製品構成

CLUSTERPRO は大きく分けると 2 つのモジュールから構成されています。

- ◆ CLUSTERPRO Server

CLUSTERPRO の本体で、サーバの高可用性機能の全てが包含されています。また、Cluster WebUI のサーバ側機能も含まれます。

- ◆ Cluster WebUI

CLUSTERPRO の構成情報の作成や運用管理を行うための管理ツールです。ユーザーインターフェイスとして Web ブラウザを利用します。実体は CLUSTERPRO Server に組み込まれていますが、操作は管理端末上の Web ブラウザで行うため、CLUSTERPRO Server 本体とは区別されています。

CLUSTERPRO のソフトウェア構成

CLUSTERPRO のソフトウェア構成は次の図のようになります。Solaris サーバ上には「CLUSTERPRO Server(CLUSTERPRO 本体)」をインストールします。Cluster WebUI の本体機能は CLUSTERPRO Server に含まれるため、別途インストールする必要がありません。Cluster WebUI は管理 PC 上の Web ブラウザから利用するほか、クラスタを構成する各サーバ上の Web ブラウザでも利用できます。

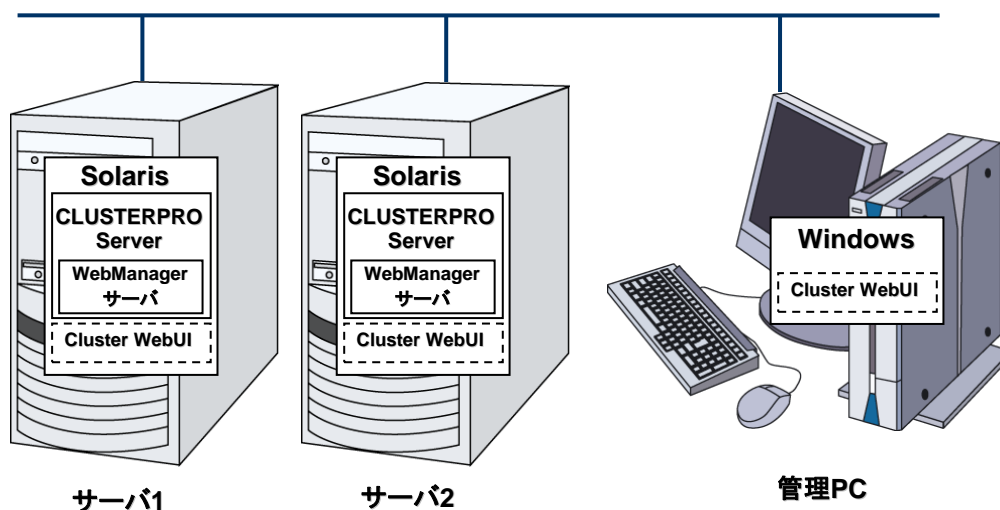


図 2-1 CLUSTERPRO のソフトウェア構成

CLUSTERPRO の障害監視のしくみ

CLUSTERPRO では、サーバ監視、業務監視、内部監視の 3 つの監視を行うことで、迅速かつ確実な障害検出を実現しています。以下にその監視の詳細を示します。

サーバ監視とは

サーバ監視とはフェイルオーバ型クラスタシステムの最も基本的な監視機能で、クラスタを構成するサーバが停止していないかを監視する機能です。

CLUSTERPRO はサーバ監視のために、定期的にサーバ同士で生存確認を行います。この生存確認をハートビートと呼びます。ハートビートは以下の通信パスを使用して行います。

◆ プライマリインタコネクト

フェイルオーバ型クラスタ専用の通信パスで、一般の Ethernet NIC を使用します。ハートビートを行うと同時にサーバ間の情報交換に使用します。

◆ セカンダリインタコネクト

クライアントとの通信に使用している通信パスを予備のインタコネクトとして使用します。TCP/IP が使用できる NIC であればどのようなものでも構いません。ハートビートを行うと同時にサーバ間の情報交換に使用します。

◆ 共有ディスク

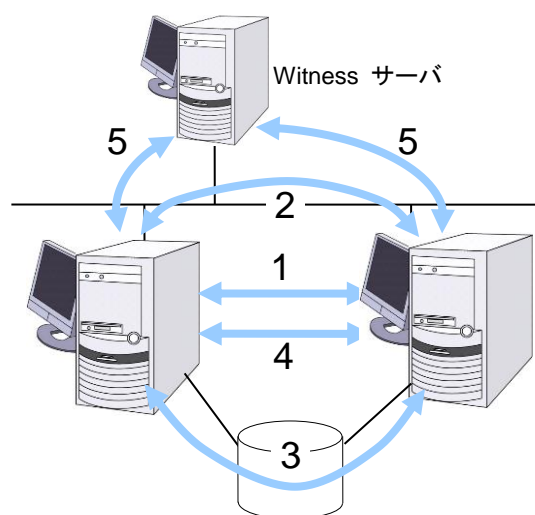
フェイルオーバ型クラスタを構成する全てのサーバに接続されたディスク上に、CLUSTERPRO 専用のパーティション(CLUSTER パーティション)を作成し、CLUSTER パーティション上でハートビートを行います。

◆ COM ポート

フェイルオーバ型クラスタを構成するサーバ間を、COM ポートを介してハートビート通信を行い、他サーバの生存を確認します。

◆ Witness

フェイルオーバ型クラスタを構成する各サーバと Witness サーバサービスが動作している外部サーバ (Witness サーバ) 間で通信を行い、Witness サーバが保持する他サーバとの通信情報から生存を確認します。



- | | |
|---|--------------|
| 1 | プライマリインタコネクト |
| 2 | セカンダリインタコネクト |
| 3 | 共有ディスク |
| 4 | COMポート |
| 5 | Witness |

図 2-2 サーバ監視

これらの通信経路を使用することでサーバ間の通信の信頼性は飛躍的に向上し、ネットワークパーティション状態の発生を防ぎます。

注： ネットワークパーティション状態について：クラスタサーバ間の全ての通信路に障害が発生しネットワーク的に分断されてしまう状態のことです。ネットワークパーティション状態に対応できていないクラスタシステムでは、通信路の障害とサーバの障害を区別できず、同一資源を複数のサーバからアクセスしデータ破壊を引き起こす場合があります。

業務監視とは

業務監視とは、業務アプリケーションそのものや業務が実行できない状態に陥る障害要因を監視する機能です。

◆ アプリケーションの死活監視

アプリケーションを起動用のリソース (EXEC リソースと呼びます) により起動を行い、監視用のリソース (PID モニタリソースと呼びます) により定期的にプロセスの生存を確認することで実現します。業務停止要因が業務アプリケーションの異常終了である場合に有効です。

注:

- CLUSTERPRO が直接起動したアプリケーションが監視対象の常駐プロセスを起動し終了してしまうようなアプリケーションでは、常駐プロセスの異常を検出することはできません。
 - アプリケーションの内部状態の異常 (アプリケーションのストールや結果異常) を検出することはできません。
-

◆ リソースの監視

CLUSTERPRO のモニタリソースによりクラスタリソース(ディスクパーティション、IP アドレスなど)やパブリック LAN の状態を監視することで実現します。業務停止要因が業務に必要なリソースの異常である場合に有効です。

内部監視とは

内部監視とは、CLUSTERPRO 内部のモジュール間相互監視です。CLUSTERPRO の各監視機能が正常に動作していることを監視します。

次のような監視を CLUSTERPRO 内部で行っています。

◆ CLUSTERPROプロセスの死活監視

監視できる障害と監視できない障害

CLUSTERPRO には、監視できる障害とできない障害があります。クラスタシステム構築時、運用時に、どのような監視が検出可能なのか、または検出できないのかを把握しておくことが重要です。

サーバ監視で検出できる障害とできない障害

監視条件: 障害サーバからのハートビートが途絶

◆ 監視できる障害の例

- ハードウェア障害(OS が継続動作できないもの)
- panic

◆ 監視できない障害の例

- OS の部分的な機能障害(マウス/キーボードのみが動作しない等)

業務監視で検出できる障害とできない障害

監視条件: 障害アプリケーションの消滅、継続的なリソース異常、あるネットワーク装置への通信路切断

◆ 監視できる障害の例

- アプリケーションの異常終了
- 共有ディスクへのアクセス障害(HBA¹の故障など)
- パブリック LAN NIC の故障

◆ 監視できない障害の例

- アプリケーションのストール/結果異常

アプリケーションのストール/結果異常を CLUSTERPRO で直接監視することはできませんが、アプリケーションを監視し異常検出時に自分自身を終了するプログラムを作成し、そのプログラムを EXEC リソースで起動、PID モニタリソースで監視することで、フェイルオーバを発生させることは可能です。

¹ Host Bus Adapterの略で、共有ディスク側ではなく、サーバ本体側のアダプタのことです。

ネットワークパーティション解決

CLUSTERPRO は、あるサーバからのハートビート途絶を検出すると、その原因が本当にサーバ障害なのか、あるいはネットワークパーティション状態によるものなのかの判別を行います。サーバ障害と判断した場合は、フェイルオーバ(健全なサーバ上で各種リソースを活性化し業務アプリケーションを起動)を実行しますが、ネットワークパーティション状態と判断した場合には、業務継続よりもデータ保護を優先させるため、緊急シャットダウンなどの処理を実施します。

ネットワークパーティション解決方式には下記の方法があります。

- ◆ ping 方式
- ◆ http 方式

関連情報: ネットワークパーティション解決方法の設定についての詳細は、『リファレンスガイド』の「第 5 章 ネットワークパーティション解決リソースの詳細」を参照してください。

フェイルオーバーのしくみ

CLUSTERPRO は障害を検出すると、フェイルオーバー開始前に検出した障害がサーバの障害かネットワークパーティション状態かを判別します。この後、健全なサーバ上で各種リソースを活性化し業務アプリケーションを起動することでフェイルオーバーを実行します。

このとき、同時に移動するリソースの集まりをフェイルオーバーグループと呼びます。フェイルオーバーグループは利用者から見た場合、仮想的なコンピュータとみなすことができます。

注: クラスタシステムでは、アプリケーションを健全なノードで起動しなおすことでフェイルオーバーを実行します。このため、アプリケーションのメモリ上に格納されている実行状態をフェイルオーバーすることはできません。

障害発生からフェイルオーバー完了までの時間は数分間必要です。以下にタイムチャートを示します。

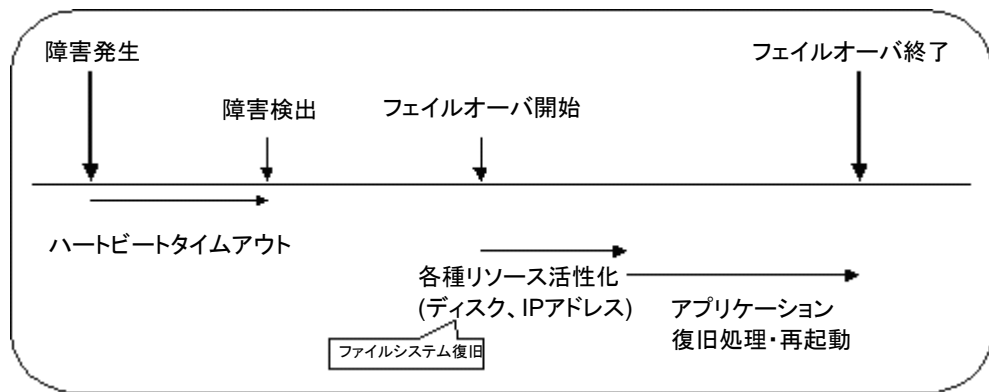


図 2-3 フェイルオーバーのタイムチャート

◆ ハートビートタイムアウト

- ・ 業務を実行しているサーバの障害発生後、待機系がその障害を検出するまでの時間です。
- ・ 業務の負荷に応じてクラスタプロパティの設定値を調整します。
(出荷時設定では 90 秒に設定されています。)

◆ 各種リソース活性化

- ・ 業務で必要なリソースを活性化するための時間です。
- ・ 一般的な設定では数秒で活性化しますが、フェイルオーバーグループに登録されているリソースの種類や数によって必要時間は変化します。
(詳しくは、『インストール&設定ガイド』を参照してください。)

◆ 開始スクリプト実行時間

- ・ データベースのロールバック/ロールフォワードなどのデータ復旧時間と業務で使用するアプリケーションの起動時間です。
- ・ ロールバック/ロールフォワード時間などはチェックポイントインターバルの調整である程度予測可能です。詳しくは、各ソフトウェア製品のドキュメントを参照してください。

フェイルオーバーリソース

CLUSTERPRO がフェイルオーバー対象とできる主なリソースは以下のとおりです。

- ◆ 切替パーティション (ディスクリソースなど)
 - 業務アプリケーションが引き継ぐべきデータを格納するためのディスクパーティションです。
- ◆ フローティングIPアドレス (フローティングIPリソース)
 - フローティング IP アドレスを使用して業務へ接続することで、フェイルオーバーによる業務の実行位置(サーバ)の変化をクライアントは気にする必要がなくなります。
 - パブリック LAN アダプタへの IP アドレス動的割り当てと ARP パケットの送信により実現しています。ほとんどのネットワーク機器からフローティング IP アドレスによる接続が可能です
- ◆ スクリプト (EXEC リソース)
 - CLUSTERPRO では、業務アプリケーションをスクリプトから起動します。
 - 共有ディスクにて引き継がれたファイルはファイルシステムとして正常であっても、データとして不完全な状態にある場合があります。スクリプトにはアプリケーションの起動のほか、フェイルオーバー時の業務固有の復旧処理も記述します。

注: クラスタシステムでは、アプリケーションを健全なノードで起動しなおすことでフェイルオーバーを実行します。このため、アプリケーションのメモリ上に格納されている実行状態をフェイルオーバーすることはできません。

フェイルオーバー型クラスタのシステム構成

フェイルオーバー型クラスタは、ディスクアレイ装置をクラスタサーバ間で共有します。サーバ障害時には待機系サーバが共有ディスク上のデータを使用し業務を引き継ぎます。

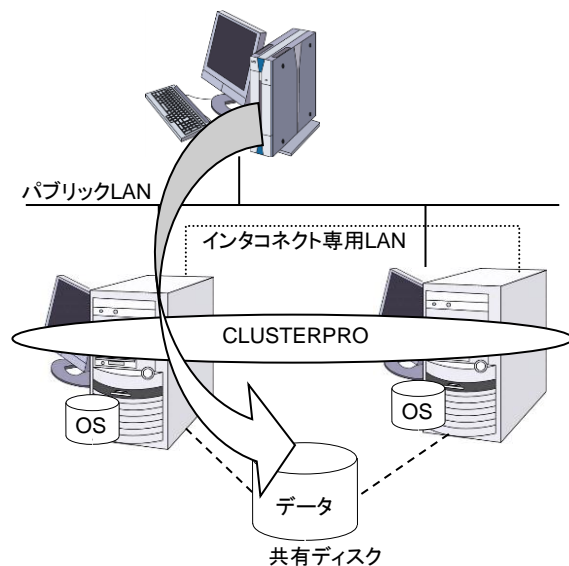


図 2-4 システム構成

フェイルオーバー型クラスタでは、運用形態により、次のように分類できます。

片方向スタンバイクラスタ

一方のサーバを現用系として業務を稼働させ、他方のサーバを待機系として業務を稼働させない運用形態です。最もシンプルな運用形態でフェイルオーバー後の性能劣化のない可用性の高いシステムを構築できます。

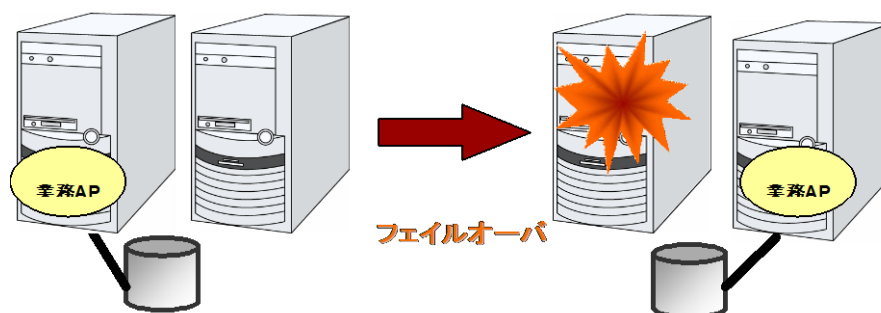
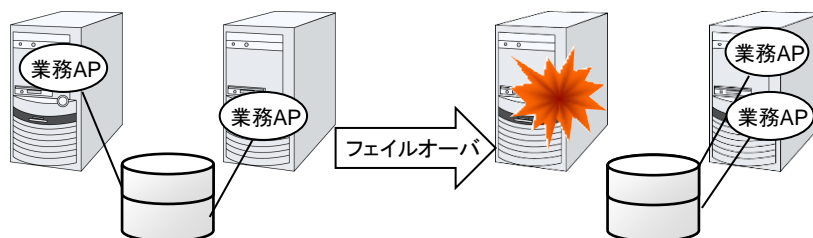


図 2-5 片方向スタンバイクラスタ

同一アプリケーション双方向スタンバイクラスタ

複数のサーバである業務アプリケーションを稼働させ相互に待機する運用形態です。アプリケーションは双方向スタンバイ運用をサポートしているものでなければなりません。ある業務データを複数に分割できる場合に、アクセスしようとしているデータによってクライアントからの接続先サーバを変更することで、データ分割単位での負荷分散システムを構築できます。

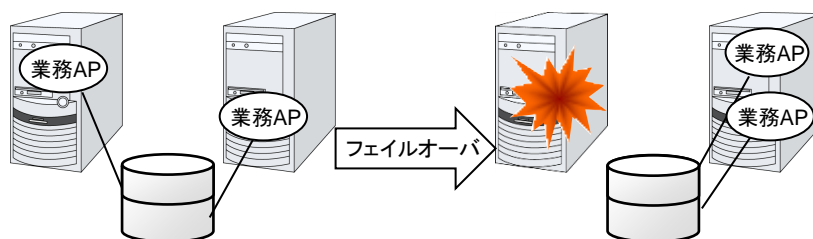


- ※ 図の業務APIは同一アプリケーション
- ※ フェイルオーバー後にひとつのサーバ上で複数の業務APインスタンスが動く

図 2-6 同一アプリケーション双方向スタンバイクラスタ

異種アプリケーション双方向スタンバイクラスタ

複数の種類の業務アプリケーションをそれぞれ異なるサーバで稼働させ相互に待機する運用形態です。アプリケーションが双方向スタンバイ運用をサポートしている必要はありません。業務単位での負荷分散システムを構築できます。

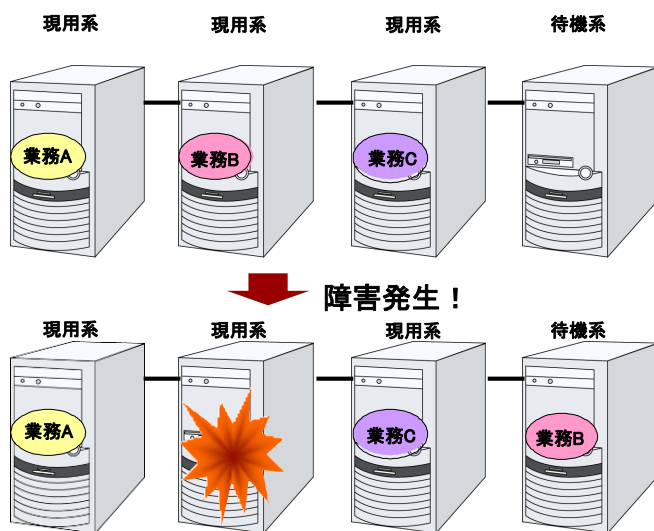


- ※ 業務1と業務2は異なるアプリケーションを使用

図 2-7 異種アプリケーション双方向スタンバイクラスタ

N + N 構成

ここまでの構成を応用し、より多くのノードを使用した構成に拡張することも可能です。下図は、3 種の業務を 3 台のサーバで実行し、いざ問題が発生した時には 1 台の待機系にその業務を引き継ぐという構成です。片方向スタンバイでは、正常時のリソースの無駄は 1/2 でしたが、この構成なら正常時の無駄を 1/4 まで削減でき、かつ、1 台までの異常発生であればパフォーマンスの低下もありません。

**図 2-8 N + N 構成**

共有ディスク型のハードウェア構成

共有ディスク構成の CLUSTERPRO の HW 構成は下図のようになります。

サーバ間の通信に

- ◆ NICを 2 枚 (1枚は外部との通信と流用、1枚はCLUSTERPRO専用)
- ◆ RS232Cクロスケーブルで接続されたCOMポート
- ◆ 共有ディスクの特定領域

を利用する構成が一般的です。

共有ディスクとの接続インターフェイスは SCSI や Fibre Channel、iSCSI ですが、最近では Fibre Channel か iSCSI による接続が一般的です。

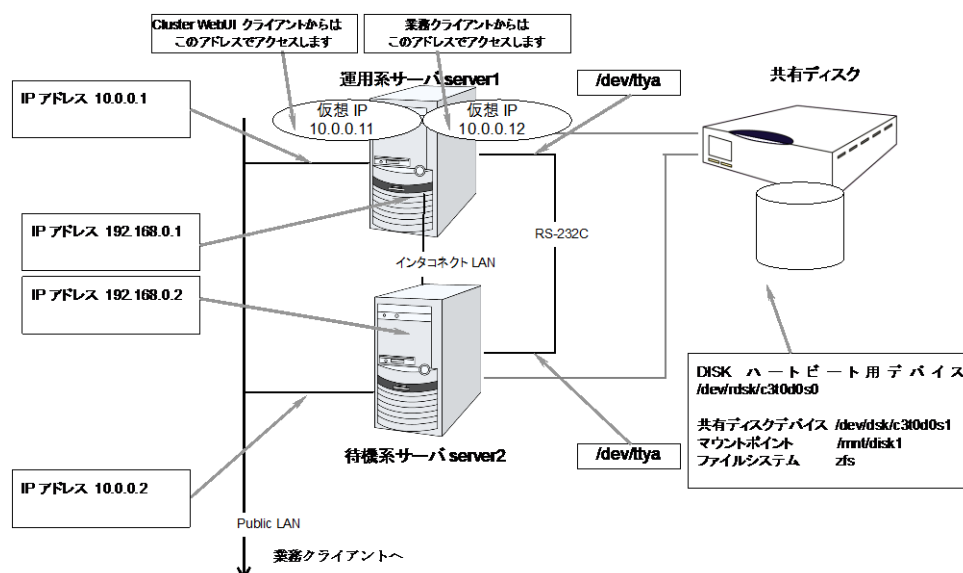


図 2-9 共有ディスク使用時のクラスタ環境のサンプル

クラスタオブジェクトとは？

CLUSTERPRO では各種リソースを下のような構成で管理しています。

- ◆ クラスタオブジェクト
クラスタの構成単位となります。
- ◆ サーバオブジェクト
実体サーバを示すオブジェクトで、クラスタオブジェクトに属します。
- ◆ ハートビートリソースオブジェクト
実体サーバのNW部分を示すオブジェクトで、サーバオブジェクトに属します。
- ◆ ネットワークパーティション解決リソースオブジェクト
ネットワークパーティション解決機構を示すオブジェクトで、サーバオブジェクトに属します。
- ◆ グループオブジェクト
仮想サーバを示すオブジェクトで、クラスタオブジェクトに属します。
- ◆ グループリソースオブジェクト
仮想サーバの持つリソース(NW、ディスク)を示すオブジェクトでグループオブジェクトに属します。
- ◆ モニタリソースオブジェクト
監視機構を示すオブジェクトで、クラスタオブジェクトに属します。

リソースとは？

CLUSTERPRO では、監視する側とされる側の対象をすべてリソースと呼び、分類して管理します。このことにより、より明確に監視/被監視の対象を区別できるほか、クラスタ構築や障害検出時の対応が容易になります。リソースはハートビートリソース、ネットワークパーティション解決リソース、グループリソース、モニタリソースの 4 つに分類されます。以下にその概略を示します。

ハートビートリソース

サーバ間で、お互いの生存を確認するためのリソースです。

以下に現在サポートされているハートビートリソースを示します。

- ◆ LANハートビートリソース
Ethernetを利用した通信を示します。
- ◆ COMハートビートリソース
RS232C(COM)を利用した通信を示します。
- ◆ ディスクハートビートリソース
共有ディスク上の特定パーティション(ディスクハートビート用パーティション)を利用した通信を示します。共有ディスク構成の場合のみ利用可能です。
- ◆ Witness ハートビートリソース
Witness サーバサービスが動作している外部サーバから取得した各サーバとの通信状態を示します。

ネットワークパーティション解決リソース

ネットワークパーティション状態を解決するためのリソースを示します。

- ◆ PING ネットワークパーティション解決リソース
PING 方式によるネットワークパーティション解決リソースです。
- ◆ HTTP ネットワークパーティション解決リソース
HTTP 方式によるネットワークパーティション解決リソースです。

グループリソース

フェイルオーバーを行う際の単位となる、フェイルオーバーグループを構成するリソースです。

以下に現在サポートされているグループリソースを示します。

- ◆ フローティングIPリソース (fip)
仮想的なIPアドレスを提供します。クライアントからは一般のIPアドレスと同様にアクセス可能です。
- ◆ EXECリソース (exec)
業務(DB、httpd、etc..)を起動/停止するための仕組みを提供します。
- ◆ ディスクリソース (disk)
共有ディスク上の指定パーティションを提供します。(共有ディスク)構成の場合のみ利用可能です。
- ◆ NASリソース (nas)

NASサーバ上の共有リソースへ接続します。(クラスタサーバがNASのサーバ側として振る舞うリソースではありません。)

- ◆ 仮想 IP リソース (vip)
仮想的な IP アドレスを提供します。クライアントからは一般の IP アドレスと同様にアクセス可能です。ネットワークアドレスの異なるセグメント間で遠隔クラスタを構成する場合に使用します。
- ◆ ボリュームマネージャリソース (volmgr)
ボリュームマネージャリソースは、ボリュームマネージャによって管理される論理ディスクを制御します。
- ◆ 仮想マシンリソース (vm)
仮想マシンの起動、停止、マイグレーションを行います。
- ◆ ダイナミック DNS リソース (ddns)
Dynamic DNS サーバに仮想ホスト名と活性サーバの IP アドレスを登録します。

モニタリソース

クラスタシステム内で、監視を行う主体であるリソースです。

以下に現在サポートされているモニタリソースを示します。

- ◆ IPモニタリソース (ipw)
外部のIPアドレスの監視機構を提供します。
- ◆ ディスクモニタリソース (diskw)
ディスクの監視機構を提供します。共有ディスクの監視にも利用されます。
- ◆ PIDモニタリソース (pidw)
EXECリソースで起動したプロセスの死活監視機能を提供します。
- ◆ ユーザ空間モニタリソース (userw)
ユーザ空間のストール監視機構を提供します。
- ◆ NIC Link Up/Downモニタリソース (miiw)
LANケーブルのリンクステータスの監視機構を提供します。
- ◆ マルチターゲットモニタリソース (mtw)
複数のモニタリソースを束ねたステータスを提供します。
- ◆ 仮想IPモニタリソース (vipw)
仮想IPリソースのRIPパケットを送出する機構を提供します。
- ◆ カスタムモニタリソース (genw)
監視処理を行うコマンドやスクリプトがある場合に、その動作結果によりシステムを監視する機構を提供します。
- ◆ MySQL モニタリソース (mysqlw)
MySQL データベースへの監視機構を提供します。
- ◆ NFS モニタリソース (nfs w)
NFS ファイルサーバへの監視機構を提供します。
- ◆ Oracle モニタリソース (oraclew)
Oracle データベースへの監視機構を提供します。
- ◆ PostgreSQL モニタリソース (psqlw)
PostgreSQL データベースへの監視機構を提供します。

- ◆ Samba モニタリソース (sambaw)
Samba ファイルサーバへの監視機構を提供します。
- ◆ ボリュームマネージャモニタリソース (volmgrw)
ボリュームマネージャにより管理されている論理ディスクの監視機構を提供します。
- ◆ 仮想マシンモニタリソース (vmw)
仮想マシンの生存確認を行います。
- ◆ 外部連携モニタリソース (mrw)
”異常発生通知受信時に実行する異常時動作の設定”と”異常発生通知の Cluster WebUI 表示”を実現するためのモニタリソースです。
- ◆ ダイナミック DNS モニタリソース (ddnsw)
定期的に Dynamic DNS サーバに仮想ホスト名と活性サーバの IP アドレスを登録します。
- ◆ プロセス名モニタリソース (psw)
プロセス名を指定することで、任意のプロセスの死活監視機能を提供します。

CLUSTERPRO を始めよう!

以上で CLUSTERPRO の簡単な説明が終了しました。

以降は、以下の流れに従い、対応するガイドを読み進めながら CLUSTERPRO を使用したクラスタシステムの構築を行ってください。

最新情報の確認

本ガイドの「第 3 章 CLUSTERPRO の動作環境」、「第 4 章 最新バージョン情報」、「第 5 章 注意制限事項」、「第 6 章 アップグレード手順」を参照してください。

クラスタシステムの設計

『インストール&設定ガイド』の「第 1 章 システム構成を決定する」、「第 2 章 クラスタシステムを設計する」および

『リファレンスガイド』の「第 2 章 グループリソースの詳細」、「第 3 章 モニタリソースの詳細」、「第 4 章 ハートビートリソースの詳細」、「第 5 章 ネットワークパーティション解決リソースの詳細」、「第 6 章 その他の設定情報」および

『ハードウェア連携ガイド』を参照してください。

クラスタシステムの構築

『インストール&設定ガイド』の全編を参照してください。

クラスタシステムの運用開始後の障害対応

『メンテナンスガイド』の「第 1 章 保守情報」および

『リファレンスガイド』の「第 8 章 トラブルシューティング」、「第 9 章 エラーメッセージ一覧」を参照してください。

第 3 章 CLUSTERPRO の動作環境

本章では、CLUSTERPRO の動作環境について説明します。

本章で説明する項目は以下の通りです。

- ハードウェア 48
- ソフトウェア 49
- Cluster WebUI の動作環境 52

ハードウェア

CLUSTERPRO は以下のアーキテクチャのサーバで動作します。

- ◆ i86pc(x86_64)

スペック

CLUSTERPRO Server で必要なスペックは下記の通りです。

- ◆ RS-232Cポート 1 つ (3 ノード以上のクラスタを構築する場合は不要)
- ◆ Ethernetポート 2 つ以上
- ◆ 共有ディスク
- ◆ CD-ROMドライブ

ソフトウェア

CLUSTERPRO Serverの動作環境

動作可能なバージョン

CLUSTERPRO には下記の独自ドライバモジュールがあります。

独自ドライバモジュール	説明
Keepaliveドライバ	ユーザ空間モニタリソースの監視方法としてkeepaliveを選択した場合に使用します。 シャットダウン監視の監視方法としてkeepaliveを選択した場合に使用します。

動作確認を行ったバージョン情報を下記に提示します。

i86pc(x86_64)

バージョン	clpka 動作可否	CLUSTERPROVersion	備考
Solaris11.2	○	4.0.0-1~	
Solaris11.3	○	4.0.0-1~	
Solaris11.4	○	4.1.0-1~	

監視オプションの動作確認済アプリケーション情報

モニタリソースの監視対象のアプリケーションのバージョンの情報

i86pc(x86_64)

モニタリソース	監視対象のアプリケーション	CLUSTERPRO Version	備考
Oracleモニタ	Oracle Database 12c Release 1 (12.1)	4.0.0-1~	
	Oracle Database 12c Release 2 (12.2)	4.0.0-1~	
	Oracle Database 18c (18.3)	4.1.0-1~	
PostgreSQLモニタ	PostgreSQL 9.3	4.0.0-1~	
	PostgreSQL 9.4	4.0.0-1~	
	PostgreSQL 9.5	4.0.0-1~	
	PostgreSQL 9.6	4.0.0-1~	
	PostgreSQL 10	4.0.0-1~	
	PostgreSQL 11	4.1.0-1~	
MySQLモニタ	MySQL 5.5	4.0.0-1~	
	MySQL 5.6	4.0.0-1~	
	MySQL 5.7	4.0.0-1~	
	MySQL 8.0	4.1.0-1~	
Sambaモニタ	Samba 3.6	4.0.0-1~	
NFSモニタ	nfsd 2 (udp)	4.0.0-1~	
	nfsd 3 (udp)	4.0.0-1~	
	nfsd 4 (tcp)	4.0.0-1~	
	mountd 1(tcp)	4.0.0-1~	

	mountd 2(tcp)	4.0.0-1~	
	mountd 3(tcp)	4.0.0-1~	

必要メモリ容量とディスクサイズ

必要メモリサイズ		必要ディスクサイズ		備考
ユーザモード	kernel モード	インストール直後	運用時	
200MB(*1)	キープアライブドライバの場合 8MB	300MB	5.0GB	

(*1) オプション類を除く

Cluster WebUI の動作環境

動作確認済OS、ブラウザ

現在の対応状況は下記の通りです。

ブラウザ	言語
Internet Explorer 11	日本語/英語/中国語
Internet Explorer 10	日本語/英語/中国語
Firefox	日本語/英語/中国語
Google Chrome	日本語/英語/中国語

注: IPアドレスで接続する場合、事前に該当のIPアドレスを [ローカル イントラネット] の [サイト] に登録する必要があります。

注: Internet Explorer 11 にて Cluster WebUI に接続すると、Internet Explorer が停止することがあります。本事象回避のために、Internet Explorer のアップデート (KB4052978 以降) を適用してください。なお、Windows 8.1/Windows Server 2012R2 に KB4052978 以降を適用するためには、事前に KB2919355 の適用が必要となります。詳細は Microsoft より展開されている情報をご確認ください。

注: タブレットやスマートフォンなどのモバイルデバイスには対応していません。

必要メモリ容量/ディスク容量

必要メモリ容量 500MB 以上

必要ディスク容量 50MB 以上

第 4 章 最新バージョン情報

本章では、CLUSTERPRO の最新情報について説明します。新しいリリースで強化された点、改善された点などをご紹介します。

- CLUSTERPRO とマニュアルの対応一覧 54
- 機能強化 55
- 修正情報 57

CLUSTERPRO とマニュアルの対応一覧

本書では下記のバージョンの CLUSTERPRO を前提に説明してあります。CLUSTERPRO のバージョンとマニュアルの版数に注意してください。

CLUSTERPROの 内部バージョン	マニュアル	版数	備考
4.1.1-1	スタートアップガイド	第 2 版	
	インストール&設定ガイド	第 1 版	
	リファレンスガイド	第 1 版	
	メンテナンスガイド	第 1 版	
	互換機能ガイド	第 1 版	

機能強化

各バージョンにおいて以下の機能強化を実施しています。

項番	内部バージョン	機能強化項目
1	4.0.0-1	デザインを刷新した管理 GUI (Cluster WebUI) を実装しました。
2	4.0.0-1	WebManager が HTTPS プロトコルに対応しました。
3	4.0.0-1	期限付きライセンスが利用可能になりました。
4	4.0.0-1	モニタリソースにおけるエラー判定およびタイムアウト判定の精度を改善しました。
5	4.0.0-1	両系活性検出時に生存させるサーバグループを選択できるようにしました。
6	4.0.0-1	フェイルオーバー属性に[完全排他]が設定されているグループにて、排他の対象とする組み合わせを設定できるようになりました。
7	4.0.0-1	フェイルオーバー属性に[完全排他]が設定されているグループにて、排他の対象とする組み合わせを設定できるようになりました。
8	4.0.0-1	内部プロセス間通信で消費される TCP ポート量を削減しました。
9	4.0.0-1	ログ収集で収集する項目を強化しました。
10	4.0.1-1	WebManager において、設定不備により HTTPS を使用できない場合に、syslog およびアラートログヘッメッセージを出力するようにしました。
11	4.1.0-1	Solaris11.4 に対応しました。
12	4.1.0-1	Oracle モニタリソースが Oracle Database 18c に対応しました。
13	4.1.0-1	MySQL モニタリソースが MySQL8.0 に対応しました。
14	4.1.0-1	Cluster WebUI でクラスタの構築、構成変更が可能になりました。
15	4.1.0-1	Witness ハートビートリソースを追加しました。
16	4.1.0-1	HTTP ネットワークパーティション解決リソースを追加しました。
17	4.1.0-1	クラスタ構成の変更時、業務を停止せずに変更を反映可能な設定項目を拡充しました。
18	4.1.0-1	フェイルオーバーグループの起動時に、フローティング IP アドレスの重複チェックを行う機能を追加しました。
19	4.1.0-1	遠隔クラスタ構成で、サーバグループ間のハートビートタイムアウトを検出しても、設定された時間だけ自動フェイルオーバーを猶予する機能を追加しました。
20	4.1.0-1	EXEC リソースの開始 / 終了スクリプトで利用できる環境変数を拡充しました。
21	4.1.0-1	強制停止スクリプトの実行結果を判定し、フェイルオーバーを抑制する機能を追加しました。

項番	内部バージョン	機能強化項目
22	4.1.0-1	強制停止機能および筐体 ID 連携機能で実行する IPMI コマンドラインを編集できるようにしました。
23	4.1.0-1	フェイルオーバーグループ、グループリソース、モニタリソースの稼働状況をクラスタ統計情報として保存する機能を追加しました。
24	4.1.0-1	ログ収集のパターンに、ミラー統計情報とクラスタ統計情報を追加しました。
25	4.1.0-1	カスタムモニタリソースに、非同期スクリプトの監視開始を待ち合わせる機能を追加しました。
26	4.1.0-1	クラスタ停止の実行時、グループリソースの停止前にカスタムモニタリソースの停止完了を待ち合わせる設定を追加しました。
27	4.1.0-1	clpmonctrl コマンドに処理を要求する先のサーバを指定するためのオプションを追加しました。
28	4.1.0-1	WebManager サーバに対する HTTPS 接続において、SSL および TLS 1.0 を無効化しました。
29	4.1.0-1	共有ディスクデバイスが使用可能となるまでクラスタの起動を待ち合わせる機能を追加しました。
30	4.1.0-1	シャットダウン監視の既定値を「常に実行する」から「グループ非活性処理に失敗した場合のみ実行する」に変更しました。
31	4.1.1-1	Cluster WebUI の表示および操作を改善しました。

修正情報

各バージョンにおいて以下の修正を実施しています。

項番	修正バージョン / 発生バージョン	修正項目	致命度	発生条件 発生頻度	原因
1	4.0.1-1 / 4.0.0-1	同一製品の期限付きライセンスが2つ有効化されることがある。	小	ライセンス期限切れの際にストックされた未使用のライセンスを自動的に有効化する処理と、ライセンス登録コマンドによる新規ライセンスの登録操作が同時に行われた場合に、稀に発生する。	ライセンス情報を操作する際の排他処理に不備があったため。
2	4.0.1-1 / 4.0.0-1	clpgrp コマンドによるグループの起動が失敗する。	小	排他ルールが設定された構成で、起動対象のグループ名を指定せずにclpgrpコマンドを実行した場合に発生する。	グループ名が省略された場合の処理に不備があったため。
3	4.0.1-1 / 4.0.0-1	CPUライセンスとVMノードライセンスが混在する構成で、CPUライセンスの不足を示す警告メッセージが出力される。	小	CPUライセンスとVMノードライセンスが混在する場合に発生する。	ライセンスのカウンタ処理に不備があったため。
4	4.1.0-1 / 4.0.0-1	Database Agent で監視異常時の回復動作が30秒遅れて実行される。	小	回復動作実行時に必ず発生する。	回復動作実行時の処理に不備があったため。
5	4.1.0-1 / 4.0.0-1	クラスタサスペンドがタイムアウトすることがある。	中	クラスタリジューム処理中にクラスタサスペンド操作を実行した場合に、稀に発生する。	クラスタサスペンド・リジューム操作が競合した場合の処理に不備があったため。
6	4.1.0-1 / 4.0.0-1	手動起動に設定されたフェイルオーバーグループのフェイルオーバー時に、フェイルオーバー元で起動されていなかったグループリソースが、フェイルオーバー先で起動されることがある。	小	下記の状態遷移により発生する。 (1) クラスタ停止 (2) クラスタ起動 (3) 手動起動に設定されたフェイルオーバーグループの一部のグループリソースを単体起動 (4) グループリソースが起動されているサーバをシャットダウン	グループリソースの状態を保持する情報の初期化に不備があったため。

項番	修正バージョン / 発生バージョン	修正項目	致命度	発生条件 発生頻度	原因
7	4.1.0-1 / 4.0.0-1	clpstat コマンドで、クラスタ停止処理中のステータスが適切に表示されない。	小	クラスタ停止実行直後からクラスタ停止完了までの間で clpstat コマンドを実行した場合に発生する。	クラスタ停止処理中のステータス判定処理に不備があったため。
8	4.1.0-1 / 4.0.0-1	停止処理の完了していないグループリソースのステータスが停止状態となる場合がある。	中	停止処理が失敗した状態のグループリソースに対し、下記の操作を行うと発生する場合がある。 ・起動操作 ・停止操作	異常状態のグループリソースに対する起動・停止操作によるステータス変更処理に不備があったため。
9	4.1.0-1 / 4.0.0-1	シャットダウン監視によるサバリセットよりも前にフェイルオーバーが開始されることがある。	大	システム高負荷により、シャットダウン監視の動作が遅延した場合に、稀に発生する。	ハートビートを停止するタイミングに考慮漏れがあったため。
10	4.1.0-1 / 4.0.0-1	強制停止機能の設定変更時に、適切な反映方法（クラスタのサスペンド / リジューム）が実行されない場合がある。	小	仮想マシン強制停止設定の初回反映時に発生する。	仮想マシン強制停止設定が追加された場合の反映方法を判定するための定義情報に誤りがあったため。
11	4.1.0-1 / 4.0.0-1	クラスタプロパティの「ログの通信方法」の設定変更が反映されないことがある。	小	クラスタの初回構築時に、「ログの通信方法」を「UNIXドメイン」以外へ変更した場合に発生する。	設定変更時の反映方法の判定処理に不備があったため。
12	4.1.0-1 / 4.0.0-1	exec リソース、カスタムモニタリソースのスク립トログにて下記の問題が発生する。 ・非同期スク립トのログ出力時刻が全てプロセス終了時刻になる。 ・ログの一時保存ファイルが残存することがある。	小	スク립トのログローテート機能が有効である場合に発生する。	ログ出力処理に不備があったため。
13	4.1.0-1 / 4.0.0-1	ディスクモニタリソースにおいて、タイムアウトを検出しても異常とならず警告となる。	中	ディスクモニタリソースでタイムアウトを検出した場合に発生することがある。	タイムアウト検出時の判定処理に不備があったため。
14	4.1.1-1 / 4.1.0-1	Cluster WebUI の設定モードへの切替に失敗する。	小	特定のブラウザから HTTPS で Cluster WebUI に接続すると発生する。	特定ブラウザからのデータ送信パターンに対応できていない箇所があったため。

第 5 章 注意制限事項

本章では、注意事項や既知の問題とその回避策について説明します。

本章で説明する項目は以下の通りです。

• システム構成検討時.....	60
• OS インストール前、OS インストール時.....	63
• OS インストール後、CLUSTERPRO インストール前.....	64
• CLUSTERPRO の情報作成時.....	69
• CLUSTERPRO 運用後.....	72
• CLUSTERPRO の構成変更時.....	75
• CLUSTERPRO バージョンアップ時.....	76

システム構成検討時

HW の手配、システム構成、共有ディスクの構成時に留意すべき事項について説明します。

機能一覧と必要なライセンス

下記オプション製品はサーバ台数分必要となります。

使用したい機能	必要なライセンス
Oracleモニタリソース	CLUSTERPRO X Database Agent 4.1
PostgreSQLモニタリソース	CLUSTERPRO X Database Agent 4.1
MySQLモニタリソース	CLUSTERPRO X Database Agent 4.1
sambaモニタリソース	CLUSTERPRO X File Server Agent 4.1
nfsモニタリソース	CLUSTERPRO X File Server Agent 4.1

共有ディスクの要件について

- ◆ 共有ディスクはSolarisのmdlによるストライプセット、ボリュームセット、ミラーリング、パリティ付ストライプセットの機能はサポートしていません。

IPv6 環境について

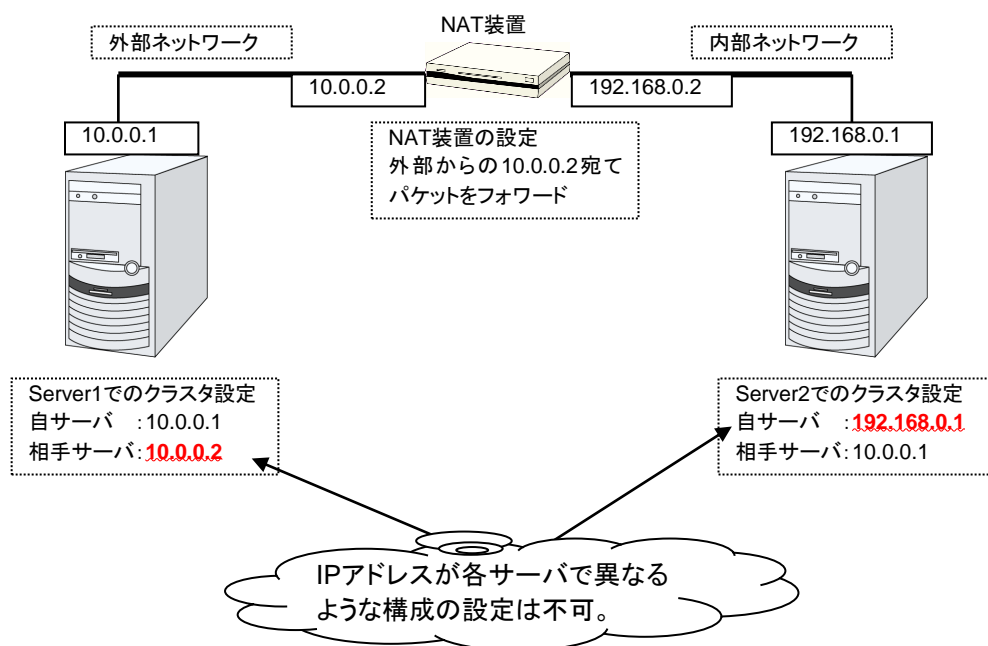
下記の機能はリンクローカルアドレスを使用できません。

- ◆ LANハートビートリソース
- ◆ カーネルモードLANハートビートリソース
- ◆ PINGネットワークパーティション解決リソース
- ◆ FIPリソース
- ◆ VIPリソース

ネットワーク構成について

NAT 環境等のように、自サーバの IP アドレスおよび相手サーバの IP アドレスが、各サーバで異なるような構成においては、クラスタ構成を構築/運用できません。

《不可な構成の例》



モニタリソース回復動作の「最終動作前にスクリプトを実行する」について

バージョン 3.1.0-1 以降から、再活性前とフェイルオーバ前にもスクリプトを実行することが可能になりました。

いずれの場合も同じスクリプトが実行されます。そのため、3.1.0-1 より前のバージョンで「最終動作前スクリプトを実行する」を設定している場合にはスクリプトファイルの編集が必要になる場合があります。

再活性前、フェイルオーバ前にスクリプトを実行するように追加設定する場合には、スクリプトを編集し、回復動作による切り分け処理を記述する必要があります。

回復動作の切り分けについては、『リファレンスガイド』の「第 3 章 モニタリソースの詳細」に記載されている、「回復スクリプト、回復動作前スクリプトについて」を参照してください。

NIC Link Up/Down モニタリソース

NIC のボード、ドライバによっては、必要な `ioctl()` がサポートされていない場合があります。

実機で CLUSTERPRO を使用して NIC Link Up/Down モニタリソースの使用可否を確認する場合には以下の手順で動作確認を行ってください。

1. NIC Link Up/Down モニタリソースを構成情報に登録してください。
NIC Link Up/Down モニタリソースの異常検出時回復動作の設定は「何もしない」を選択してください。
2. クラスタを起動してください。
3. NIC Link Up/Down モニタリソースのステータスを確認してください。
LAN ケーブルのリンク状態が正常状態時に NIC Link Up/Down モニタリソースのステータスが異常となった場合、NIC Link Up/Down モニタリソースは動作不可です。
4. LAN ケーブルのリンク状態を異常状態(リンクダウン状態)にしたときに NIC Link Up/Down モニタリソースのステータスが異常となった場合、NIC Link Up/Down モニタリソースは動作可能です。
ステータスが正常のまま変化しない場合、NIC Link Up/Down モニタリソースは動作不可です。

メール通報について

メール通報機能は、STARTTLS や SSL に対応していません。

ネットワーク警告灯の要件について

- ◆ 「警子ちゃんミニ」、「警子ちゃん 4G」を使用する場合、警告灯にパスワードを設定しないで下さい。
- ◆ 音声ファイルの再生による警告を行う場合、あらかじめ音声ファイル再生に対応したネットワーク警告灯に音声ファイルを登録しておく必要があります。
音声ファイルの登録に関しては、各ネットワーク警告灯の取扱説明書を参照して下さい。
- ◆ ネットワーク警告灯にクラスタ内のサーバからの `rsh` コマンド実行を許可するように設定してください。

OS インストール前、OS インストール時

OS をインストールするときに決定するパラメータ、リソースの確保、ネーミングルールなどで留意して頂きたいことです。

/opt/nec/clusterpro のファイルシステムについて

システムの対障害性の向上のために、ジャーナル機能を持つファイルシステムを使用することを推奨します。ジャーナリングシステムに対応していないファイルシステムを使用した場合、サーバや OS の停止(正常なシャットダウンが行えなかった場合)から再起動した場合、インタラクティブなコマンドの実行(root ファイルシステムの fsck の実行)が必要になります。

依存するライブラリ

SUNWlxml

OS インストール後、CLUSTERPRO インストール前

OS のインストールが完了した後、OS やディスクの設定を行うときに留意して頂きたいことです。

通信ポート番号

CLUSTERPRO では、以下のポート番号を使用します。このポート番号については Cluster WebUI での変更が可能です。

下記ポート番号には、CLUSTERPRO 以外のプログラムからアクセスしないようにしてください。

サーバにファイアウォールの設定を行う場合には、下記のポート番号にアクセスできるようにしてください。

[サーバ・サーバ間][サーバ内ループバック]

From			To		備考
サーバ	自動割り当て ¹	→	サーバ	29001/TCP	内部通信
サーバ	自動割り当て	→	サーバ	29002/TCP	データ転送
サーバ	自動割り当て	→	サーバ	29002/UDP	ハートビート
サーバ	自動割り当て	→	サーバ	29003/UDP	アラート同期
サーバ	自動割り当て	→	サーバ	icmp	FIP/VIP リソースの重複確認
サーバ	自動割り当て	→	サーバ	XXXX ² /UDP	内部ログ用通信

[サーバ・Cluster WebUI 間]

From			To		備考
Cluster WebUI	自動割り当て	→	サーバ	29003/TCP	http 通信

[その他]

From			To		備考
サーバ	自動割り当て	→	ネットワーク警告灯	各製品のマニュアルを参照	ネットワーク警告灯制御
サーバ	自動割り当て	→	サーバの BMC の管理 LAN	623/UDP	BMC 制御 (強制停止/筐体ランプ連携)
サーバ	自動割り当て	→	Witness サーバ	Cluster WebUI で設定した通信ポート番号	Witness ハートビートリソースの接続先ホスト
サーバ	自動割り当て	→	監視先	icmp	IP モニタ
サーバ	自動割り当て	→	NFS サーバ	icmp	NAS リソースの NFS サーバ死活確認

サーバ	自動割り当て	→	監視先	icmp	Ping 方式ネットワークパーティション解決リソースの監視先
サーバ	自動割り当て	→	監視先	Cluster WebUI で設定した通信ポート番号	HTTP 方式ネットワークパーティション解決リソースの監視先

1. 自動割り当てでは、その時点で使用されていないポート番号が割り当てられます。
2. クラスタプロパティ、ポート番号(ログ)タブでログの通信方法に[UDP]を選択し、ポート番号で設定したポート番号を使用します。デフォルトのログの通信方法 [UNIX ドメイン]では通信ポートは使用しません。

通信ポート番号の自動割り当て範囲の変更

- ◆ OSが管理している通信ポート番号の自動割り当ての範囲とCLUSTERPROが使用する通信ポート番号と重複する場合があります。
- ◆ 通信ポート番号の自動割り当ての範囲とCLUSTERPROが使用する通信ポート番号が重複する場合には、重複ないようにOSの設定を変更してください。

OS の設定状態の確認例/表示例

TCP の通信ポート番号の自動割り当ての範囲は以下のコマンドで確認することができます。

```
#ndd -get /dev/tcp tcp_smallest_anon_port
32768

#ndd -get /dev/tcp tcp_largest_anon_port
65535
```

これは、TCP 通信を行うアプリケーションが OS へ通信ポート番号の自動割り当てを要求した場合、32768～65535 の範囲でアサインされる状態です。

同様に、UDP の通信ポート番号の自動割り当ての範囲は以下のコマンドで確認することができます。

```
#ndd -get /dev/udp udp_smallest_anon_port
32768

#ndd -get /dev/udp udp_largest_anon_port
65535
```

これは、UDP 通信を行うアプリケーションが OS へ通信ポート番号の自動割り当てを要求した場合、32768～65535 の範囲でアサインされる状態です。

OS の設定の変更例

TCP ポートの自動割り当て範囲を 30000～65000 に変更する場合、以下のコマンドを実行します。

```
#ndd -set /dev/tcp tcp_smallest_anon_port 30000
#ndd -set /dev/tcp tcp_largest_anon_port 65000
```

ポート数不足を回避する設定について

CLUSTERPRO の構成において、多数のサーバ、多数のリソースを使用している場合、CLUSTERPRO の内部通信に使用する一時ポートが不足して、クラスタサーバとして正常に動作できなくなる可能性があります。

一時ポートとして使用できる範囲や、一時ポートが解放されるまでの時間を必要に応じて調整してください。

時刻同期の設定

クラスタシステムでは、複数のサーバの時刻を定期的に同期する運用を推奨します。ntp などを使用してサーバの時刻を同期させてください。

共有ディスクについて

- ◆ サーバの再インストール時等で共有ディスク上のデータを引き続き使用する場合、パーティションの確保やファイルシステムの作成はしないでください。
- ◆ パーティションの確保やファイルシステムの作成を行うと共有ディスク上のデータは削除されます。
- ◆ 共有ディスク上のファイルシステムはCLUSTERPROが制御します。共有ディスクのファイルシステムをOSの/etc/vfstabにエントリしないでください。
- ◆ 共有ディスクの設定手順は『インストールガイド&設定ガイド』を参照してください。

OS 起動時間の調整

電源が投入されてから、OS が起動するまでの時間が、下記の 2 つの時間より長くなるように調整してください。

- ◆ 共有ディスクを使用する場合に、ディスクの電源が投入されてから使用可能になるまでの時間
- ◆ ハートビートタイムアウト時間

設定手順は『インストールガイド&設定ガイド』を参照してください。

ネットワークの確認

- ◆ インタコネクトで使用するネットワークの確認をします。クラスタ内のすべてのサーバで確認します。
- ◆ 設定手順は『インストールガイド&設定ガイド』を参照してください。

ipmiutil, OpenIPMI について

- ◆ 以下の機能で [ipmitool] コマンドを使用します。
 - ・ グループリソースの活性異常時/非活性異常時の最終アクション
 - ・ モニタリソースの異常時アクション
 - ・ 強制停止機能
 - ・ 筐体 ID ランプ連携
- ◆ [ipmitool]コマンドに関する以下の事項について、弊社は対応いたしません。ユーザー様の判断、責任にてご使用ください。
 - ・ [ipmitool] コマンド自体に関するお問い合わせ
 - ・ [ipmitool] コマンドの動作保証
 - ・ [ipmitool] コマンドの不具合対応、不具合が原因の障害
 - ・ 各サーバの [ipmitool] コマンドの対応状況のお問い合わせ
- ◆ ご使用予定のサーバ（ハードウェア）の [ipmitool] コマンド対応可否についてはユーザー様にて事前に確認ください。
- ◆ ハードウェアとしてIPMI規格に準拠している場合でも実際には [ipmitool] コマンドが動作しない場合がありますので、ご注意ください。

nsupdate,nslookup について

- ◆ 以下の機能でnsupdateとnslookupを使用します。
 - ・ グループリソースのダイナミック DNS リソース(ddns)
 - ・ モニタリソースのダイナミック DNS モニタリソース(ddnsw)
- ◆ CLUSTERPROにnsupdateとnslookupは添付しておりません。ユーザー様ご自身で別途nsupdate と nslookup をインストールしてください。
- ◆ nsupdate、nslookupに関する以下の事項について、弊社は対応いたしません。ユーザー様の判断、責任にてご使用ください。
 - ・ nsupdate、nslookup 自体に関するお問い合わせ
 - ・ nsupdate、nslookup の動作保証
 - ・ nsupdate、nslookup の不具合対応、不具合が原因の障害
 - ・ 各サーバの nsupdate、nslookup の対応状況のお問い合わせ

Samba モニタリソースについて

- ◆ Samba モニタリソースは、監視のためにSMBプロトコルバージョン1.0 を使用しています。そのため、Sambaサーバ側で受け入れるSMBプロトコルのバージョンをSMB2.0 以降に限定(例:smb.conf の server min protocol = SMB2)すると監視異常となります。Samba モニタリソースを利用する場合は、SMBプロトコルバージョン1.0を許可してください。
- ◆ Samba モニタリソースは、SMB署名には未対応です。Sambaサーバ側でSMB署名を有効(例:smb.conf の client signing = mandatory)にすると、監視異常となります。SMB署名は無効にしてください。

- ◆ Samba モニタリソースは、監視のために NTLMv1 認証を使用しています。そのため、Sambaサーバ側で NTLMv1 認証を無効(例:smb.conf の lanman auth = no, ntlm auth = no)にすると監視異常となります。Samba モニタリソースを利用する場合は、NTLMv1 認証を許可してください。Samba 4.5.0 以降は NTLMv1 認証の既定値が無効になっていますので、注意してください。

HTTP ネットワークパーティション解決リソース、Witness ハートビートリソースについて

- ◆ HTTP ネットワークパーティション解決リソース、Witness ハートビートリソースでは、SSL を使用する場合に OpenSSL 1.0 の共有ライブラリを利用しています。

以下の共有ライブラリを検索します。

- libssl.so.1.0.0

OS のディストリビューションやバージョン、およびパッケージのインストール状況によっては、上記のファイルまたはシンボリックリンクが存在しない場合があります。その場合は下記のコマンド例のようにシンボリックリンクを作成してください。

コマンド例:

```
cd /usr/lib/amd64 # /usr/lib/amd64 へ移動
ln -s libssl.so.1.0.1e libssl.so.1.0.0 # シンボリックリンクの作成
```

CLUSTERPRO の情報作成時

CLUSTERPRO の構成情報の設計、作成前にシステムの構成に依存して確認、留意が必要な事項です。

CLUSTERPRO インストールパス配下のディレクトリ、ファイルについて

CLUSTERPRO インストールパス配下にあるディレクトリやファイルは、CLUSTERPRO 以外から操作(編集/作成/追加/削除など)しないでください。

CLUSTERPRO 以外からディレクトリやファイルを操作した場合の影響についてはサポート対象外とします。

環境変数

環境変数が 256 個以上設定されている環境では、下記の処理を実行できません。下記の機能またはリソースを使用する場合は、環境変数を 255 個以下に設定してください。

- ◆ グループの起動/停止処理
- ◆ execリソースが活性/非活性時に実行する開始/停止スクリプト
- ◆ カスタムモニタリソースが監視時に実行するスクリプト
- ◆ グループリソース、モニタリソース異常検出後の最終動作実行前スクリプト
- ◆ グループリソースの活性/非活性前後スクリプト
- ◆ 強制停止スクリプト

注: システムに設定されている環境変数と CLUSTERPRO で設定される環境変数を合わせて 255 個以下になるように設定してください。CLUSTERPRO が設定する環境変数は約 30 個です。

強制停止機能、筐体 ID ランプ連携

強制停止機能、筐体 ID ランプ連携を使用する場合、各サーバの BMC の IP アドレス、ユーザ名、パスワードの設定が必須です。ユーザ名には必ずパスワード登録されているものを設定してください。

サーバのリセット、パニック、パワーオフ

CLUSTERPRO が「サーバのリセット」または「サーバのパニック」、または「サーバのパワーオフ」を行う場合、サーバが正常にシャットダウンされません。そのため下記のリスクがあります。

- ◆ マウント中のファイルシステムへのダメージ
- ◆ 保存していないデータの消失
- ◆ OSのダンプ採取の中断

「サーバのリセット」または「サーバのパニック」が発生する設定は下記です。

- ◆ グループリソース活性時/非活性時異常時の動作
 - keepalive リセット
 - keepalive パニック

- BMC リセット
- BMC パワーオフ
- BMC サイクル
- BMC NMI
- ◆ モニタリソース異常検出時の最終動作
 - keepalive リセット
 - keepalive パニック
 - BMC リセット
 - BMC パワーオフ
 - BMC サイクル
 - BMC NMI
- ◆ ユーザ空間監視のタイムアウト検出時動作
 - 監視方法 keepalive
- ◆ シャットダウン監視
 - 監視方法 keepalive
- ◆ 強制停止機能の動作
 - BMC リセット
 - BMC パワーオフ
 - BMC サイクル
 - BMC NMI

グループリソースの非活性異常時の最終アクション

非活性異常検出時の最終動作に「何もしない」を選択すると、グループが非活性失敗のまま停止しません。
本番環境では「何もしない」は設定しないように注意してください。

遅延警告割合

遅延警告割合を 0 または、100 に設定すれば以下のようなことを行うことが可能です。

- ◆ 遅延警告割合に 0 を設定した場合

監視毎に遅延警告がアラート通報されます。
この機能を利用し、サーバが高負荷状態での監視リソースへのポーリング時間を算出し、監視リソースの監視タイムアウト時間を決定することができます。

- ◆ 遅延警告割合に 100 を設定した場合
遅延警告の通報を行いません。

テスト運用以外で、0%等の低い値を設定しないように注意してください。

ディスクモニタリソースの監視方法TURについて

- ◆ SCSIの[Test Unit Ready]コマンドをサポートしていないディスク、ディスクインターフェイス(HBA)では使用できません。
ハードウェアがサポートしている場合でもドライバがサポートしていない場合があるのでドライバの仕様も合わせて確認してください。
- ◆ Read方式に比べてOSやディスクへの負荷は小さくなります。
- ◆ Test Unit Readyでは、実際のメディアへのI/Oエラーは検出できない場合があります。

LAN ハートビートの設定について

- ◆ LANハートビートリソースは最低 1 つ設定する必要があります。
- ◆ インタコネクト専用のLANをLANハートビートリソースとして登録し、さらにパブリックLANもLANハートビートリソースとして登録することを推奨します (LANハートビートリソースを2つ以上設定することを推奨します)。

COM ハートビートの設定について

- ◆ ネットワークが断線した場合に両系で活性することを防ぐため、COMが使用できる環境であればCOMハートビートリソースを使用することを推奨します。

スクリプトのコメントなどで取り扱える 2 バイト系文字コードについて

- ◆ CLUSTERPROでは、Solaris環境で編集されたスクリプトはEUC、Window環境で編集されたスクリプトはShift-JISとして扱われます。その他の文字コードを利用した場合、環境によっては文字化けが発生する可能性があります。

仮想マシングループのフェイルオーバー排他属性の設定について

- ◆ 仮想マシングループに設定したグループは排他ルールへ設定しないでください。

CLUSTERPRO 運用後

クラスタとして運用を開始した後に発生する事象で留意して頂きたい事項です。

回復動作中の操作制限

モニタリソースの異常検出時の設定で回復対象にグループリソース(ディスクリソース、EXEC リソース、...)を指定し、モニタリソースが異常を検出した場合の回復動作遷移中(再活性化 → フェイルオーバー → 最終動作)には、以下のコマンドまたは、Cluster WebUI からのクラスタ及びグループへの制御は行わないでください。

- ◆ クラスタの停止/サスペンド
- ◆ グループの開始/停止/移動

モニタリソース異常による回復動作遷移中に上記の制御を行うと、そのグループの他のグループリソースが停止しないことがあります。

また、モニタリソース異常状態であっても最終動作実行後であれば上記制御を行うことが可能です。

コマンド編に記載されていない実行形式ファイルやスクリプトファイルについて

インストールディレクトリ配下にコマンド編に記載されていない実行形式ファイルやスクリプトファイルがありますが、CLUSTERPRO 以外からは実行しないでください。

実行した場合の影響については、サポート対象外となります。

EXEC リソースで使用するスクリプトファイルについて

EXEC リソースで使用するスクリプトファイルは各サーバ上の下記のディレクトリに配置されます。

`/インストールパス/scripts/グループ名/EXEC リソース名/`

クラスタ構成変更時に下記の変更を行った場合、変更前のスクリプトファイルはサーバ上からは削除されません。

- EXEC リソースを削除した場合や EXEC リソース名を変更した場合
- EXEC リソースが所属するグループを削除した場合やグループ名を変更した場合

変更前のスクリプトファイルが必要ない場合は、削除しても問題ありません。

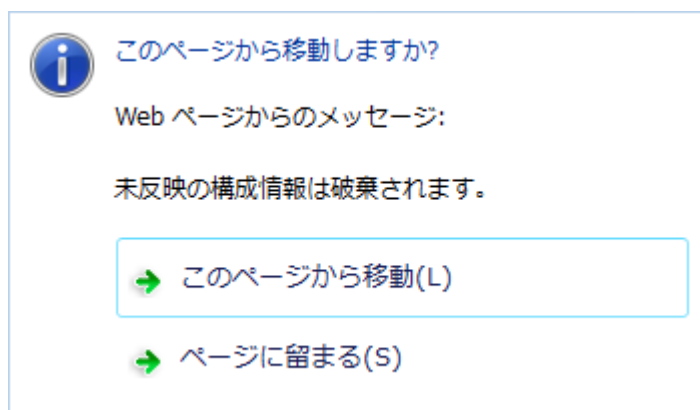
活性時監視設定のモニタリソースについて

活性時監視設定のモニタリソースの一時停止/再開には下記の制限事項があります。

- ◆ モニタリソースの一時停止後、監視対象リソースを停止させた場合モニタリソースは停止状態となります。そのため、監視の再開はできません。
- ◆ モニタリソースを一時停止後、監視対象リソースを停止/起動させた場合、監視対象リソースが起動したタイミングで、モニタリソースによる監視が開始されます。

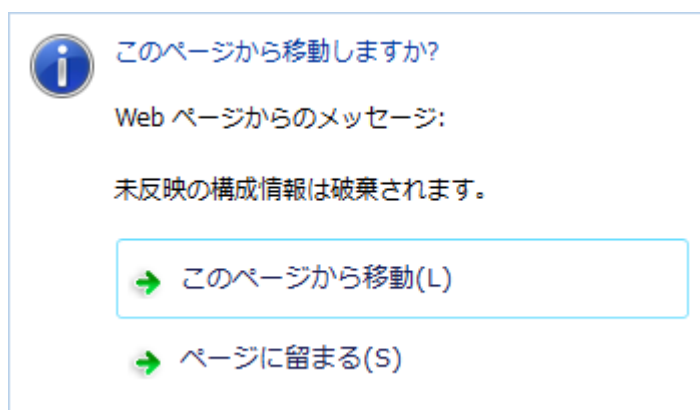
Cluster WebUI について

- ◆ 接続先と通信できない状態で操作を行うと、制御が戻ってくるまでしばらく時間が必要な場合があります。
- ◆ Proxyサーバを経由する場合は、Cluster WebUI のポート番号を中継できるように、Proxyサーバの設定をしてください。
- ◆ Reverse Proxy サーバを経由する場合、Cluster WebUI は正常に動作しません。
- ◆ CLUSTERPRO のアップデートを行った場合、起動している全てのブラウザを一旦終了してください。
ブラウザ側のキャッシュをクリアして、ブラウザを起動してください。
- ◆ 本製品より新しいバージョンで作成されたクラスタ構成情報は、本製品で利用することはできません。
- ◆ Webブラウザを終了すると(ウィンドウフレームの[X]等)、確認ダイアログが表示される場合があります。



設定を続行する場合は [ページに留まる] を選択してください。

- ◆ Webブラウザをリロードすると(メニューの[最新の情報に更新]やツールバーの[現在のページを再読み込み]等)、確認ダイアログが表示される場合があります。



設定を続行する場合は [ページに留まる] を選択してください。

- ◆ 上記以外の Cluster WebUI の注意制限事項についてはオンラインマニュアルを参照してください。

サービス起動時間について

CLUSTERPRO の各サービスは、起動時の待ち合わせ処理の有無により時間がかかる場合があります。

- ◆ clusterpro_evt
マスタサーバ以外のサーバは、マスタサーバの構成情報をダウンロードする処理を最大 2 分間待ち合わせます。マスタサーバが起動済みの場合、通常数秒以内に終了します。マスタサーバはこの処理で待ち合わせは発生しません。
- ◆ clusterpro_trn
特に待ち合わせ処理はありません。通常数秒以内に終了します。
- ◆ clusterpro
特に待ち合わせ処理はありませんが、CLUSTERPRO の起動に時間がかかる場合数十秒かかります。通常数秒以内に終了します。
- ◆ clusterpro_webmgr
特に待ち合わせ処理はありません。通常数秒以内に終了します。
- ◆ clusterpro_alertsync
特に待ち合わせ処理はありません。通常数秒以内に終了します。

さらに、CLUSTERPRO デーモン起動後は、クラスタ起動同期待ち処理があり、デフォルト設定では、5 分間の待ち合わせがあります。

これに関しては『メンテナンスガイド』の「第 1 章 保守情報」の「クラスタ起動同期待ち時間について」を参照してください。

ログ収集について

- ◆ 各サーバでログの総サイズが2GBを超えた場合、ログ収集が失敗することがあります。

フローティング IP、仮想 IP リソースについて

- ◆ フローティング IP リソースまたは仮想 IP リソースを設定している場合、これらのリソースが活性しているサーバでネットワーク再起動は実行しないでください。ネットワークを再起動すると各リソースによって追加された IP アドレスが削除されます。

CLUSTERPRO の構成変更時

クラスタとして運用を開始した後に構成を変更する場合に発生する事象で留意して頂きたい事項です。

グループ共通プロパティの排他ルールについて

排他ルールの排他属性を変更した場合、クラスタサスペンド、リジュームにより変更が反映されます。

排他属性が「完全排他」に設定されている排他ルールに、新たに排他対象のグループを追加した場合、サスペンド前のグループの起動状態により完全排他のグループが同一サーバ上で複数起動した状態になることがあります。

次回グループ起動時から正しく排他制御が行われるようになります。

グループリソースの追加、削除について

同一グループリソース名を別のグループへ移す設定変更を行う場合、以下の手順にて行ってください。

以下の手順にて行わなかった場合、正常に動作できなくなる可能性があります。

例) フローティング IP リソース fip1 をグループ failover1 から別のグループ failover2 に移す場合

1. グループ failover1 から fip1 を削除します。
2. 設定の反映を行います。
3. fip1 をグループ failover2 へ追加します。
4. 設定の反映を行います。

外部連携モニタリソースのクラスタ統計情報の設定について

モニタリソースのクラスタ統計情報の設定を変更した場合、サスペンド・リジュームを実行しても外部連携モニタリソースにはクラスタ統計情報の設定が反映されません。外部連携モニタリソースにもクラスタ統計情報の設定を反映させる場合は、OS の再起動を行ってください。

CLUSTERPRO バージョンアップ時

クラスタとして運用を開始した後に CLUSTERPRO をバージョンアップする際に留意して頂きたい事項です。

機能変更一覧

各バージョンで変更された機能について、以下に示します。

内部バージョン 4.0.0-1

- ◆ 管理ツールについて

既定の管理ツールを Cluster WebUI に変更しました。従来の WebManager をご利用の場合は、[http://管理用グループの管理IPアドレスまたは CLUSTERPRO Server をインストールしたサーバの実IPアドレス:ポート番号 \(既定値29003\)/main.htm](http://管理用グループの管理IPアドレスまたは CLUSTERPRO Server をインストールしたサーバの実IPアドレス:ポート番号 (既定値29003)/main.htm) を Web ブラウザに指定してください。

内部バージョン 4.1.0-1

- ◆ 設定ツールについて

既定の設定ツールを Cluster WebUI に変更しました。Cluster WebUI によるクラスタの管理および設定を可能にしました。

- ◆ クラスタ統計情報採取機能について

クラスタ統計情報採取機能により、既定値の動作では統計情報ファイルがインストールパス配下に保存されます。ディスク容量の都合等で統計情報ファイルを保存したくない場合は、クラスタ統計情報採取機能をオフにしてください。本機能の設定値については『リファレンスガイド』の「第 1 章 パラメータの詳細」を参照してください。

削除機能一覧

各バージョンで削除された機能について、以下に示します。

内部バージョン 4.0.0-1

- ◆ WebManager Mobile

パラメータ削除一覧

Cluster WebUI で設定可能なパラメータのうち、各バージョンで削除されたものについて、以下の表に示します。

内部バージョン 4.0.0-1

クラスタ

パラメータ	既定値
クラスタのプロパティ	
アラートサービスタブ	
アラート拡張機能を使用する	オフ
WebManager タブ	
WebManager Mobile の接続を許可する	オフ
WebManager Mobile 用パスワード	
操作用パスワード	-
参照用パスワード	-

内部バージョン 4.1.0-1

クラスタ

パラメータ	既定値
クラスタのプロパティ	
WebManager タブ	
WebManager 調整プロパティ	
動作タブ	
アラートビューア最大レコード数	300
クライアントデータ更新方法	Real Time

既定値変更一覧

Cluster WebUI で設定可能なパラメータのうち、各バージョンで既定値が変更されたものについて、以下の表に示します。

- ◆ バージョンアップ後も [変更前の既定値] の設定を継続したい場合は、バージョンアップ後に改めてその値に再設定してください。
- ◆ [変更前の既定値] 以外の値を設定していた場合、バージョンアップ後もそれ以前の設定値が継承されます。再設定の必要はありません。

内部バージョン 4.0.0-1

ディスクリソース

パラメータ	変更前の既定値	変更後の既定値
ディスクリソースのプロパティ		
詳細タブ		
ディスクリソース調整プロパティ		
マウントタブ		
タイムアウト	60[秒]	180[秒]

仮想 IP モニタリソース

パラメータ	変更前の既定値	変更後の既定値
仮想IPモニタリソースのプロパティ		
監視(共通)タブ		
タイムアウト	30[秒]	180[秒]

PID モニタリソース

パラメータ	変更前の既定値	変更後の既定値
PIDモニタリソースのプロパティ		
監視(共通)タブ		
監視開始待ち時間	0[秒]	3[秒]
タイムアウト発生時にリトライしない	オフ	オン
タイムアウト発生時に回復動作を実行しない	オフ	オン

NIC Link Up/Down モニタリソース

パラメータ	変更前の既定値	変更後の既定値
NIC Link Up/Downモニタリソースのプロパティ		
監視(共通)タブ		
タイムアウト	60[秒]	180[秒]
タイムアウト発生時にリトライしない	オフ	オン
タイムアウト発生時に回復動作を実行しない	オフ	オン

ダイナミック DNS モニタリソース

パラメータ	変更前の既定値	変更後の既定値
ダイナミックDNSモニタリソースのプロパティ		
監視(共通)タブ		
タイムアウト	100[秒]	180[秒]

プロセス名モニタリソース

パラメータ	変更前の既定値	変更後の既定値
プロセス名モニタリソースのプロパティ		
監視(共通)タブ		
監視開始待ち時間	0[秒]	3[秒]
タイムアウト発生時にリトライしない	オフ	オン
タイムアウト発生時に回復動作を実行しない	オフ	オン

MySQL モニタリソース

パラメータ	変更前の既定値	変更後の既定値
MySQLモニタリソースのプロパティ		
監視(固有)タブ		
ストレージエンジン	MyISAM	InnoDB
ライブラリパス	/usr/lib/mysql/libmysqlclient.so.15	/usr/lib64/mysql/libmysqlclient.so.20

Oracle モニタリソース

パラメータ	変更前の既定値	変更後の既定値
Oracleモニタリソースのプロパティ		
監視(固有)タブ		
パスワード	change_on_install	-
ライブラリパス	/opt/app/oracle/product/10.2.0/db_1/lib/libclntsh.so.10.1	/u01/app/oracle/product/12.2.0/dbhome_1/lib/libclntsh.so.12.1

PostgreSQL モニタリソース

パラメータ	変更前の既定値	変更後の既定値
PostgreSQLモニタリソースのプロパティ		
監視(固有)タブ		
ライブラリパス	/usr/lib/libpq.so.3.0	/opt/PostgreSQL/10/lib/libpq.so.5.10

フローティング IP モニタリソース

パラメータ	変更前の既定値	変更後の既定値
フローティングIPモニタリソースのプロパティ		
監視(共通)タブ		
タイムアウト	60[秒]	180[秒]
タイムアウト発生時にリトライしない	オフ	オン
タイムアウト発生時に回復動作を実行しない	オフ	オン

内部バージョン 4.1.0-1

クラスタ

パラメータ	変更前の既定値	変更後の既定値
クラスタのプロパティ		
監視タブ		
シャットダウン監視	常に実行する	グループ非活性処理に失敗した場合のみ実行する

パラメータ移動一覧

Cluster WebUI で設定可能なパラメータのうち、各バージョンで設定箇所が変更されたものについて、以下の表に示します。

変更前の設定箇所	変更後の設定箇所
[クラスタのプロパティ]-[リカバリタブ]-[最大再起動回数]	[クラスタのプロパティ]-[拡張タブ]-[最大再起動回数]
[クラスタのプロパティ]-[リカバリタブ]-[最大再起動回数をリセットする時間]	[クラスタのプロパティ]-[拡張タブ]-[最大再起動回数をリセットする時間]
[クラスタのプロパティ]-[リカバリタブ]-[強制停止機能を使用する]	[クラスタのプロパティ]-[拡張タブ]-[強制停止機能を使用する]
[クラスタのプロパティ]-[リカバリタブ]-[強制停止アクション]	[クラスタのプロパティ]-[拡張タブ]-[強制停止アクション]
[クラスタのプロパティ]-[リカバリタブ]-[強制停止タイムアウト]	[クラスタのプロパティ]-[拡張タブ]-[強制停止タイムアウト]
[クラスタのプロパティ]-[リカバリタブ]-[仮想マシン強制停止設定]	[クラスタのプロパティ]-[拡張タブ]-[仮想マシン強制停止設定]
[クラスタのプロパティ]-[リカバリタブ]-[強制停止スクリプトを実行する]	[クラスタのプロパティ]-[拡張タブ]-[強制停止スクリプトを実行する]
[クラスタのプロパティ]-[リカバリタブ]-[ダウン後自動起動する]	[クラスタのプロパティ]-[拡張タブ]-[ダウン後自動起動する]
[クラスタのプロパティ]-[排他タブ]-[マウント、アンマウントコマンド排他]	[クラスタのプロパティ]-[拡張タブ]-[マウント、アンマウントコマンドを排他する]
[グループのプロパティ]-[属性タブ]-[フェイルオーバー排他属性]	[グループ共通のプロパティ]-[排他タブ]

第 6 章 アップグレード手順

本章では、CLUSTERPRO のアップグレード手順について説明します。

本章で説明する項目は以下の通りです。

- CLUSTERPRO X のアップグレード手順 82

CLUSTERPRO X のアップグレード手順

X 3.0/3.1/3.2/3.3 から X 4.0/4.1 へのアップグレード

CLUSTERPRO Server パッケージは root ユーザでアップグレードしてください。

1. アップグレードを開始する前に、クラスタ運用中の各サーバの状態、および全リソースの状態が正常状態であることを WebManager またはコマンドから確認してください。
2. クラスタ構成情報をバックアップします。クラスタ構成情報は作成時に Builder で保存する他に、clpcfctrl コマンドでバックアップを作成することもできます。詳細は『リファレンスガイド』の「第 7 章 CLUSTERPRO コマンドリファレンス」 - 「クラスタ生成、クラスタ構成情報バックアップを実行する (clpcfctrl コマンド)」 - 「クラスタ構成情報をバックアップする」を参照してください。
3. クラスタを構成する全サーバで CLUSTERPRO をアンインストールします。アンインストール手順は『インストール&設定ガイド』の「第 10 章 CLUSTERPRO をアンインストール/再インストールする」 - 「アンインストール手順」 - 「CLUSTERPRO Server のアンインストール」を参照してください。
4. クラスタを構成するサーバで CLUSTERPRO を新規インストールします。新規インストール手順は『インストール&設定ガイド』の「第 3 章 CLUSTERPRO をインストールする」および「第 4 章 ライセンスを登録する」を参照してください。
5. 以下にアクセスしWebManagerを起動します。
http://インストールしたサーバの実 IP アドレス :29003/main.htm
クラスタ構成情報をインポートし、バックアップした構成情報を読み込みます。
6. 構成情報を反映します。
7. Cluster WebUI を起動し、クラスタを開始します。
8. グループを起動し、各リソースが正常に起動することを確認します。
9. 以上で CLUSTERPRO Server のアップグレードは完了です。Cluster WebUI または clpstat コマンドで、各サーバの [内部バージョン]、クラスタとして正常に動作していることを確認してください。

付録 A 用語集

あ

インタコネクト クラスタサーバ間の通信パス
(関連) プライベート LAN、パブリック LAN

か

仮想IPアドレス 遠隔地クラスタを構築する場合に使用するリソース (IPアドレス)

管理クライアント Cluster WebUI が起動されているマシン

起動属性 クラスタ起動時、自動的にフェイルオーバーグループを起動するか、手動で起動するかを決定するフェイルオーバーグループの属性
管理クライアントより設定が可能

共有ディスク 複数サーバよりアクセス可能なディスク

共有ディスク型クラスタ 共有ディスクを使用するクラスタシステム

切替パーティション 複数のコンピュータに接続され、切り替えながら使用可能なディスクパーティション
(関連) ディスクハートビート用パーティション

クラスタシステム 複数のコンピュータを LAN などをつないで、1 つのシステムのように振る舞わせるシステム形態

クラスタシャットダウン クラスタシステム全体 (クラスタを構成する全サーバ) をシャットダウンさせること

現用系 ある 1 つの業務セットについて、業務が動作しているサーバ
(関連) 待機系

さ

セカンダリ (サーバ) 通常運用時、フェイルオーバーグループがフェイルオーバーする先のサーバ
(関連) プライマリ サーバ

た

待機系	現用系ではない方のサーバ (関連) 現用系
ディスクハートビート用パーティション	共有ディスク型クラスタで、ハートビート通信に使用するためのパーティション
データパーティション	共有ディスクの切替パーティションのように使用することが可能なローカルディスク

な

ネットワークパーティション	全てのハートビートが途切れてしまうこと (関連) インタコネクト、ハートビート
ノード	クラスタシステムでは、クラスタを構成するサーバを指す。ネットワーク用語では、データを他の機器に経由することのできる、コンピュータやルータなどの機器を指す。

は

ハートビート	サーバの監視のために、サーバ間で定期的にお互いに通信を行うこと (関連) インタコネクト、ネットワークパーティション
パブリック LAN	サーバ/クライアント間通信パスのこと (関連) インタコネクト、プライベート LAN
フェイルオーバー	障害検出により待機系が、現用系上の業務アプリケーションを引き継ぐこと
フェイルバック	あるサーバで起動していた業務アプリケーションがフェイルオーバーにより他のサーバに引き継がれた後、業務アプリケーションを起動していたサーバに再び業務を戻すこと
フェイルオーバーグループ	業務を実行するのに必要なクラスタリソース、属性の集合
フェイルオーバーグループの移動	ユーザが意図的に業務アプリケーションを現用系から待機系に移動させること
フェイルオーバーポリシー	フェイルオーバー可能なサーバリストとその中でのフェイルオーバー優先順位を持つ属性
プライベート LAN	クラスタを構成するサーバのみが接続された LAN (関連) インタコネクト、パブリック LAN

プライマリ (サーバ)	フェイルオーバーグループでの基準で主となるサーバ (関連) セカンダリ (サーバ)
フローティング IP アドレス	フェイルオーバーが発生したとき、クライアントのアプリケーションが接続先サーバの切り替えを意識することなく利用できる IP アドレス クラスタサーバが所属する LAN と同一のネットワークアドレス内で、他に使用されていないホストアドレスを割り当てる

ま

マスタサーバ	Cluster WebUI の設定モード の [サーバ共通のプロパティ]-[マスタサーバ] で先頭に表示されているサーバ
--------	--

付録 B 索引

C

Cluster WebUI, 47, 52, 73
CLUSTERPRO, 27, 28
CLUSTERPRO インストールパス配下のディレクトリ、
ファイル, 69
COM ハートビート, 71

H

HA クラスタ, 15
HTTP ネットワークパーティション解決リソース, 68

I

ipmiutil, 67
IPv6 環境, 60

L

LAN ハートビート, 71

N

NIC Link Up/Down モニタリソース, 62
nslookup, 67
nsupdate, 67

O

OpenIPMI, 67
OS, 52
OS 起動時間, 66

S

Samba モニタリソース, 67
Single Point of Failure (SPOF), 13, 23

T

TUR, 70

W

Witness/ハートビートリソース, 68

あ

アプリケーションの引き継ぎ, 22

い

依存するライブラリ, 63

か

外部連携モニタリソースのクラスタ統計情報, 75
活性時監視設定のモニタリソース, 72
環境変数, 69
監視できる障害と監視できない障害, 32

き

既定値変更一覧, 77
機能強化, 55
機能変更一覧, 76
強制停止機能、筐体 ID ランプ連携, 69
業務監視, 32
共有ディスク, 66
共有ディスクの要件, 60

く

クラスタオブジェクト, 41
クラスタシステム, 13, 14
クラスタリソースの引き継ぎ, 21
グループリソース, 42, 70
グループリソースの追加、削除, 75

け

検出できる障害とできない障害, 32, 33

さ

サーバ監視, 31
サーバのリセット、パニック, 69
サービス起動時間, 74
最終アクション, 70
最終動作前スクリプト, 61
削除機能一覧, 76

し

時刻同期, 66
システム構成, 37
実行形式ファイル, 72
修正情報, 57
障害監視のしくみ, 30
障害検出, 13, 19
障害の監視, 26

す

スクリプトファイル, 72
スペック, 48

<p>せ</p> <p>製品構成, 29</p>	<p>は</p> <p>ハードウェア, 48 ハードウェア構成, 40 ハートビートリソース, 42 排他ルール, 75 パラメータ移動一覧, 80 パラメータ削除一覧, 76</p>
<p>そ</p> <p>ソフトウェア, 49 ソフトウェア構成, 30</p>	
<p>ち</p> <p>遅延警告割合, 70</p>	<p>ふ</p> <p>ファイルシステム, 63 フェイルオーバー, 22, 35 フェイルオーバー排他属性, 71 フェイルオーバーリソース, 36 ブラウザ, 52</p>
<p>つ</p> <p>通信ポート番号, 64</p>	
<p>て</p> <p>ディスクサイズ, 51 ディスク容量, 52 データの引き継ぎ, 21</p>	<p>ほ</p> <p>ポート数不足を回避する設定, 66</p>
<p>と</p> <p>動作確認済アプリケーション情報, 50 動作可能なバージョン, 49</p>	<p>め</p> <p>メール通報, 62 メモリ容量, 51, 52</p>
<p>な</p> <p>内部監視, 32</p>	<p>も</p> <p>文字コード, 71 モニタリソース, 43</p>
<p>ね</p> <p>ネットワーク, 66 ネットワーク警告灯, 62 ネットワーク構成, 61 ネットワークパーティション解決, 34 ネットワークパーティション解決リソース, 42 ネットワークパーティション症状, 20</p>	<p>り</p> <p>リソース, 27, 42</p> <p>ろ</p> <p>ログ収集, 74</p>