CLUSTERPRO

CLUSTERPRO X SingleServerSafe 5.3 for Linux

設定ガイド

リリース *4*

日本電気株式会社

2026 年 07 月 13 日

目次:

第 1 章

はじめに

1.1 対象読者と目的

『CLUSTERPRO X SingleServerSafe for Linux 設定ガイド』は、システムの導入を行うシステムエンジニアと、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 X SingleServerSafe の構築作業の手順について説明します。

1.2 本書の構成

- 「2. *CLUSTERPRO X SingleServerSafe* について」: CLUSTERPRO X SingleServerSafe の製品概要について説明します。
- 「3. 構成情報を作成する」: Cluster WebUI の起動方法、および構成情報の作成手順をサンプルの構成例を用いて説明します。
- 「4. システムを確認する」: 作成したシステムが正常に動作するかを確認します。
- 「5. グループリソースの詳細」: CLUSTERPRO X SingleServerSafe でアプリケーションの制御を行う単位となるグループリソースについての詳細を説明します。
- 「6. モニタリソースの詳細」: CLUSTERPRO X SingleServerSafe で監視を実行する単位であるモニタリソースについての詳細を説明します。
- 「7. ハートビートリソースの詳細」: ハートビートの詳細について説明します。
- 「8. その他の設定の詳細」: その他、CLUSTERPRO X SingleServerSafe の設定項目についての詳細を説明します。
- 「9. 監視動作の詳細」: いくつかの障害パターンにより、どのように障害を検出するかの仕組みについての詳細を説明します。
- 「10. 注意制限事項」: 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。

1.3 本書で記述される用語

本書で説明する CLUSTERPRO X SingleServerSafe は、クラスタリングソフトウェアである CLUSTERPRO X との操作性などにおける親和性を高めるために、共通の画面・コマンドを使用しています。そのため、一部、クラスタとしての用語が使用されています。

以下ように用語の意味を解釈して本書を読み進めてください。

クラスタ、クラスタシステム

CLUSTERPRO X SingleServerSafe を導入した単サーバのシステム

クラスタシャットダウン/リブート

CLUSTERPRO X SingleServerSafe を導入したシステムのシャットダウン、リブート

クラスタリソース

CLUSTERPRO X SingleServerSafe で使用されるリソース

クラスタオブジェクト

CLUSTERPRO X SingleServerSafe で使用される各種リソースのオブジェクト

フェイルオーバグループ

CLUSTERPRO X SingleServerSafe で使用されるグループリソース（アプリケーション、サービスなど）をまとめたグループ

1.4 CLUSTERPRO X SingleServerSafe マニュアル体系

CLUSTERPRO X SingleServerSafe のマニュアルは、以下の 3 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 SingleServerSafe for Linux インストールガイド』 (Install Guide)

CLUSTERPRO X SingleServerSafe を使用した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 SingleServerSafe のインストール作業の手順について説明します。

『CLUSTERPRO X SingleServerSafe for Linux 設定ガイド』 (Configuration Guide)

CLUSTERPRO X SingleServerSafe を使用したシステムの導入を行うシステムエンジニアと、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 X SingleServerSafe の構築作業の手順について説明します。

『CLUSTERPRO X SingleServerSafe for Linux 操作ガイド』 (Operation Guide)

CLUSTERPRO X SingleServerSafe を使用した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 X SingleServerSafe の操作方法について説明します。

1.5 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。

注釈: この表記は、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: この表記は、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。

参考:

この表記は、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。	`clpstat -s[-h host_name]`
#	Linux ユーザが、root でログインしていることを示すプロンプト	`# clpcl -s -a`
モノスペースフォント	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	`/Linux/5.3/jp/server/`
太字	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。 **# clpcl -s -a**
斜体	ユーザが有効な値に置き換えて入力する項目	`rpm -i clusterprosss-<`**バージョン番号**`>-<`**リリース番号**`>.x86_64.rpm`


本書の図では、CLUSTERPRO X SingleServerSafe を表すために このアイコンを使用します。

1.6 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 2 章

CLUSTERPRO X SingleServerSafe について

本章では、CLUSTERPRO X SingleServerSafe の機能概要の説明と、監視可能な障害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。

2.1 CLUSTERPRO X SingleServerSafe とは?

CLUSTERPRO X SingleServerSafe は、サーバにセットアップすることで、サーバ上のアプリケーションやハードウェアの障害を検出し、障害発生時には、アプリケーションの再起動やサーバの再起動を自動的に実行することで、サーバの可用性を向上させる製品です。

通常のサーバでは、アプリケーションが異常終了した場合、アプリケーションの終了に気づいた時点で、アプリケーションの起動を手動で行う必要があります。また、アプリケーションは異常終了していないが、アプリケーション内部での動作が不安定になり正常に動作していない場合があります。このような異常状態になっていることは、通常では容易に知ることはできません。ハードウェア障害が発生した場合、一時的な障害であれば、サーバの再起動で正常に戻る可能性があります。しかし、ハードウェア障害に気づくのは困難で、アプリケーションの動作がどうもおかしいと調査を行った結果、ハードウェア障害であったということがよくあります。

CLUSTERPRO X SingleServerSafe では、異常を検出したいアプリケーション、ハードウェアを指定することで、自動的に障害を検出し、自動的にアプリケーション、サーバの再起動を行うことで、障害からの復旧処理を行います。

注釈: 上述のようにハードウェアの物理的な障害に関しては、サーバの再起動では復旧できないことが多いです。ハードウェアの物理的障害に備えるには、ハードウェアの二重化やクラスタリングソフトなどの導入を検討してください。

2.2 CLUSTERPRO X SingleServerSafe の障害監視のしくみ

CLUSTERPRO X SingleServerSafe では、各種監視を行うことで、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。

- 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 (アプリケーションリソース、サービスリソースと呼びます) により起動し、監視用のリソース (アプリケーションモニタリソース、サービス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。

  注釈: CLUSTERPRO X SingleServerSafe 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。

  注釈: 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。

- 監視オプションによるアプリケーション/プロトコルのストール/結果異常監視

  別途ライセンスの購入が必要となりますが、データベースアプリケーション (Oracle,DB2 等)、プロトコル (FTP,HTTP 等)、アプリケーションサーバ (WebSphere,WebLogic 等) のストール/結果異常監視を行うことができます。詳細は、「6. モニタリソースの詳細」を参照してください。

- リソースの監視

  CLUSTERPRO X SingleServerSafe のモニタリソースにより各種リソース (アプリケーション、サービスなど) や LAN の状態を監視します。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。

2.2.1 監視できる障害と監視できない障害

CLUSTERPRO X SingleServerSafe 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。

2.2.2 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
  - 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 X SingleServerSafe 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、再起動を発生させることは可能です。

第 3 章

構成情報を作成する

CLUSTERPRO X SingleServerSafe では、構成内容を記述するデータのことを、構成情報と呼びます。Cluster WebUI を用いて構成情報を作成します。本章では、Cluster WebUI の起動方法、および構成情報の作成手順をサンプルの構成例を用いて説明します。

本章で説明する項目は以下のとおりです。

3.1 設定値を確認する

Cluster WebUI を使用して実際に構成情報を作成する前に、構成情報として設定する値を確認します。値を書き出して、情報に漏れがないかを確認しておきましょう。

3.1.1 環境のサンプル

以下に、構成情報のサンプル値を記載します。以降のトピックでは、この条件で構成情報を作成する手順をステップ バイ ステップで説明します。実際に値を設定する際には、構築する構成情報と置き換えて入力してください。値の決定方法については、「5. グループリソースの詳細」「6. モニタリソースの詳細」を参照してください。

構成設定例

設定対象	設定パラメータ	設定値
サーバの情報	サーバ名	server1
	モニタ リソース数	3
	タイプ	フェイルオーバ
	グループ名	failover1
	起動サーバ	server1
1 つ目のグループリソース	タイプ	EXEC リソース
	グループ リソース名	exec1
	常駐タイプ	常駐
	開始パス	実行ファイルのパス
1 つ目のモニタリソース (デフォルト作成)	タイプ	ユーザ空間モニタ
	モニタ リソース名	userw1
2 つ目のモニタリソース	タイプ	IP モニタ
	モニタリソース名	ipw1
	監視 IP アドレス	192.168.0.254(ゲートウェイ)
	回復対象	LocalServer
	再活性しきい値	-
	最終動作	サービス停止と OS 再起動
3 つ目のモニタリソース	タイプ	PID モニタ
	モニタリソース名	pidw1
	対象リソース	exec1
	回復対象	failover1
	再活性しきい値	3
	最終動作	サービス停止と OS 再起動

注釈: 1 つ目のモニタリソースの「ユーザ空間モニタ」は自動的に設定されます。

3.2 Cluster WebUI を起動する

構成情報を作成するには、Cluster WebUI にアクセスする必要があります。ここでは、まず Cluster WebUI の概要を説明し、その後、Cluster WebUI にアクセスして、構成情報を作成する方法について説明します。

3.2.1 Cluster WebUI とは

Cluster WebUI とは、Web ブラウザ経由でサーバの状態監視、サーバ/グループの起動/停止及び、動作ログの収集などを行うための機能です。

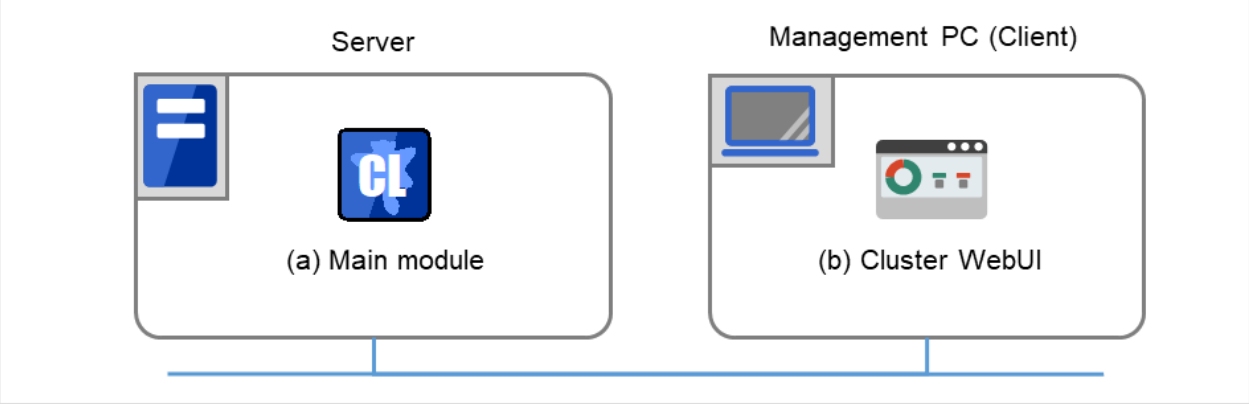


図 3.1　Cluster WebUI

3.2.2 Cluster WebUI を起動するには

Cluster WebUI を起動する手順を示します。

1. Web ブラウザを起動します。

   ブラウザのアドレス バーに、CLUSTERPRO X SingleServerSafe をインストールしたサーバの IP アドレスとポート番号を入力します。

   `http://ip-address:port/`

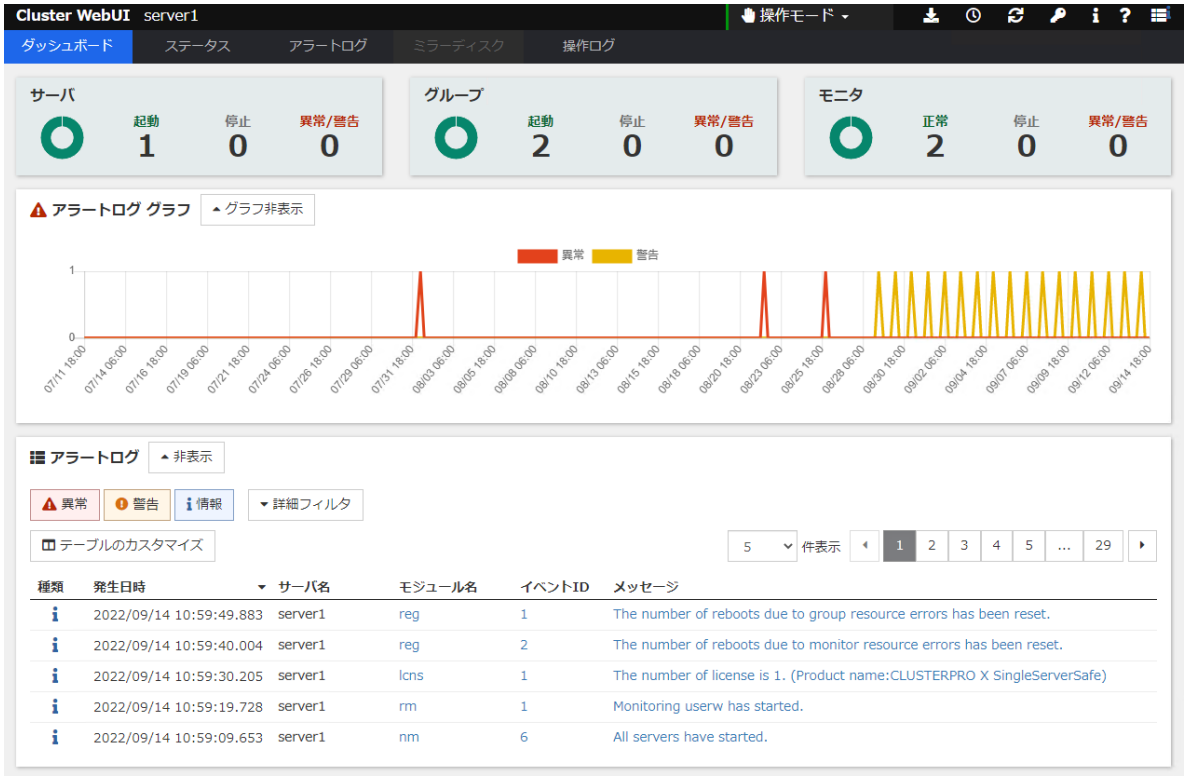
   ip-address

   CLUSTERPRO X SingleServerSafe をインストールしたサーバの IP アドレスを指定します。自サーバの場合は localhost でも問題ありません。

   port

   インストール時に指定した WebManager のポート番号と同じ番号を指定します （既定値 29003）。

2. Cluster WebUI が起動します。



3. ツールバーのドロップダウンメニューで [設定モード] を選択して、設定モードに切り替えます。

参考:

CLUSTERPRO サーバと暗号化通信を有効にして接続する場合は、「8. その他の設定の詳細」- 「8.1. クラスタプロパティ」 - 「8.1.11. *WebManager* タブ」を参照してください。暗号化通信を行う場合は下記を入力します。

https://192.168.0.3:29003/

3.3 構成情報の作成手順

構成情報を作成するには、サーバの設定、グループの作成、モニタリソースの作成の 3 つのステップを踏みます。新規に構成情報を作成する場合は、生成ウィザードを使います。以下に手順の流れを示します。

注釈: 作成した構成情報のほとんどは名称変更機能やプロパティ表示機能を使用して後から変更できます。

---

1. 「3.3.1. **サーバの設定**」

   CLUSTERPRO X SingleServerSafe を動作させるサーバを設定します。

   - 「3.3.1. **サーバを設定する**」
     構築するサーバ名などを設定します。

2. 「3.3.2. **グループの設定**」

   グループを作成します。グループでアプリケーションの起動・終了を制御します。必要な数のグループを作成します。通常、制御したいアプリケーション数ほど必要ですが、「スクリプトリソース」を使用した場合は、1 つのグループで複数のアプリケーションをまとめることもできます。

   - 「3.3.2. **グループを追加する**」
     グループを追加します。
   - 「3.3.2. **グループリソース *(EXEC* リソース*)* を追加する**」
     アプリケーションの起動・終了を行うリソースを追加します。

3. 「3.3.3. **モニタリソースの設定**」

   指定された監視対象を監視する、モニタリソースを追加します。
   監視したい数、作成します。

   - 「3.3.3. **モニタリソース *(IP* モニタリソース*)* を追加する**」
     監視を行うモニタリソース (IP モニタリソース) を追加します。
   - 「3.3.3. **モニタリソース *(PID* モニタリソース*)* を追加する**」
     監視を行うモニタリソース (PID モニタリソース) を追加します。

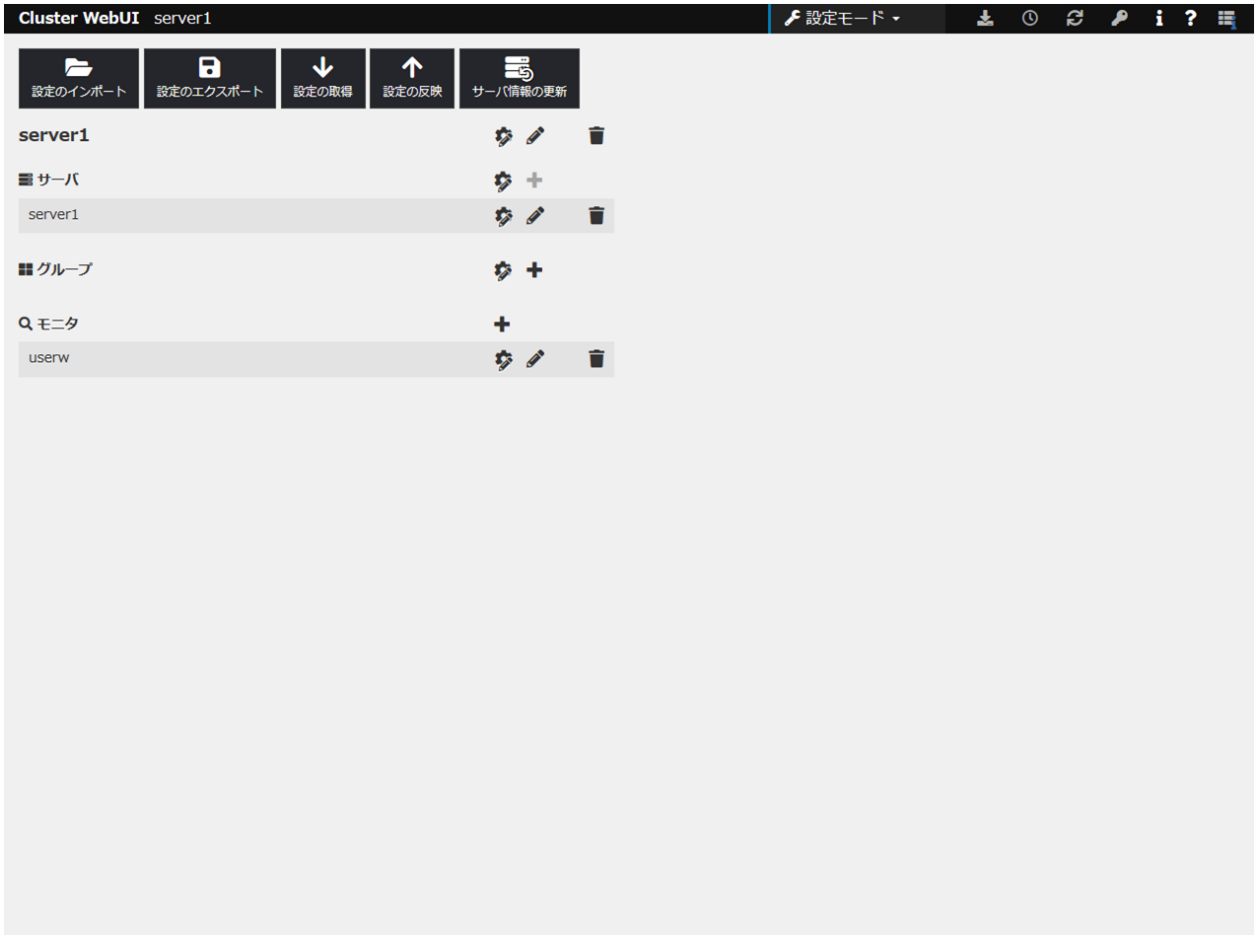
3.3.1 サーバの設定

サーバを設定します。

サーバを設定する

CLUSTERPRO X SingleServerSafe をインストール後、OS を再起動することで自動的に作成されます。Cluster WebUI の操作モードから設定モード画面に切り替えると既に作成済みの情報が表示されます。

画面は以下のようになっています。



3.3.2 グループの設定

グループとは、システム内のある 1 つの独立した業務を実行するために必要なサービスやプロセスの集まりのことです。

グループを追加する手順を説明します。

グループを追加する

グループの設定を行います。

1. [グループ] の [グループの追加] をクリックします。
2. [グループの定義] 画面が開きます。
   以下のタイプから、選択してください。

   タイプ

   - フェイルオーバ

     通常はこちらのタイプを選択します。

   [名前] ボックスにグループ名 (failover1) を入力し、[次へ] をクリックします。
3. [全てのサーバでフェイルオーバ可能] チェックボックスのチェックがオンになっていることを確認し、[次へ] をクリックします。

4. グループの各属性値を設定する画面です。そのまま [次へ] をクリックします。
5. [グループリソースの定義一覧] が表示されます。そのまま [完了] をクリックします。

グループリソース (EXEC リソース) を追加する

スクリプトによってアプリケーションの起動/終了を行う、EXEC リソースを追加します。

1. [failover1] の [リソースの追加] をクリックします。
2. [グループのリソース定義 | failover1] 画面が開きます。[タイプ] ボックスでグループリソースのタイプ (EXEC リソース) を選択し、[名前] ボックスにグループ名 (exec1) を入力します。[次へ] をクリックします。
3. 依存関係設定が表示されます。何も指定せず [次へ] をクリックします。
4. 復旧動作設定が表示されます。[次へ] をクリックします。
5. [ユーザアプリケーション] をチェックします。また、[Start path] に、実行ファイルのパスを指定します。
6. [調整] をクリックし、ダイアログボックスを開きます。[開始スクリプト] で、[非同期] をチェックし、[OK] をクリックします。
7. [完了] をクリックします。

3.3.3 モニタリソースの設定

指定した対象を監視するモニタリソースを追加します。

モニタリソース (IP モニタリソース) を追加する

1. [モニタ] の [モニタリソースの追加] をクリックします。[モニタリソースの定義] が表示されます。
2. [タイプ] ボックスでモニタリソースのタイプ (IP モニタ) を選択し、[名前] ボックスにモニタリソース名 (ipw1) を入力します。[次へ] をクリックします。

注釈:

タイプとして、モニタリソースが表示されるので、監視したいリソースを選択します。

オプション製品のライセンスがインストールされていない場合、ライセンスに対応するリソースおよびモニタリソースは Cluster WebUI の一覧に表示されません。

インストールされているライセンスが表示されない場合、[ライセンス情報取得] をクリックしてライセンス情報を取得してください。

---

3. 監視 (共通) 設定を入力します。ここではデフォルト値のまま変更せず、[次へ] をクリックします。
4. [IP アドレス一覧] が表示されます。[追加] をクリックします。
5. [IP アドレス] ボックスに監視 IP アドレス (192.168.0.254) を入力し [OK] をクリックします。

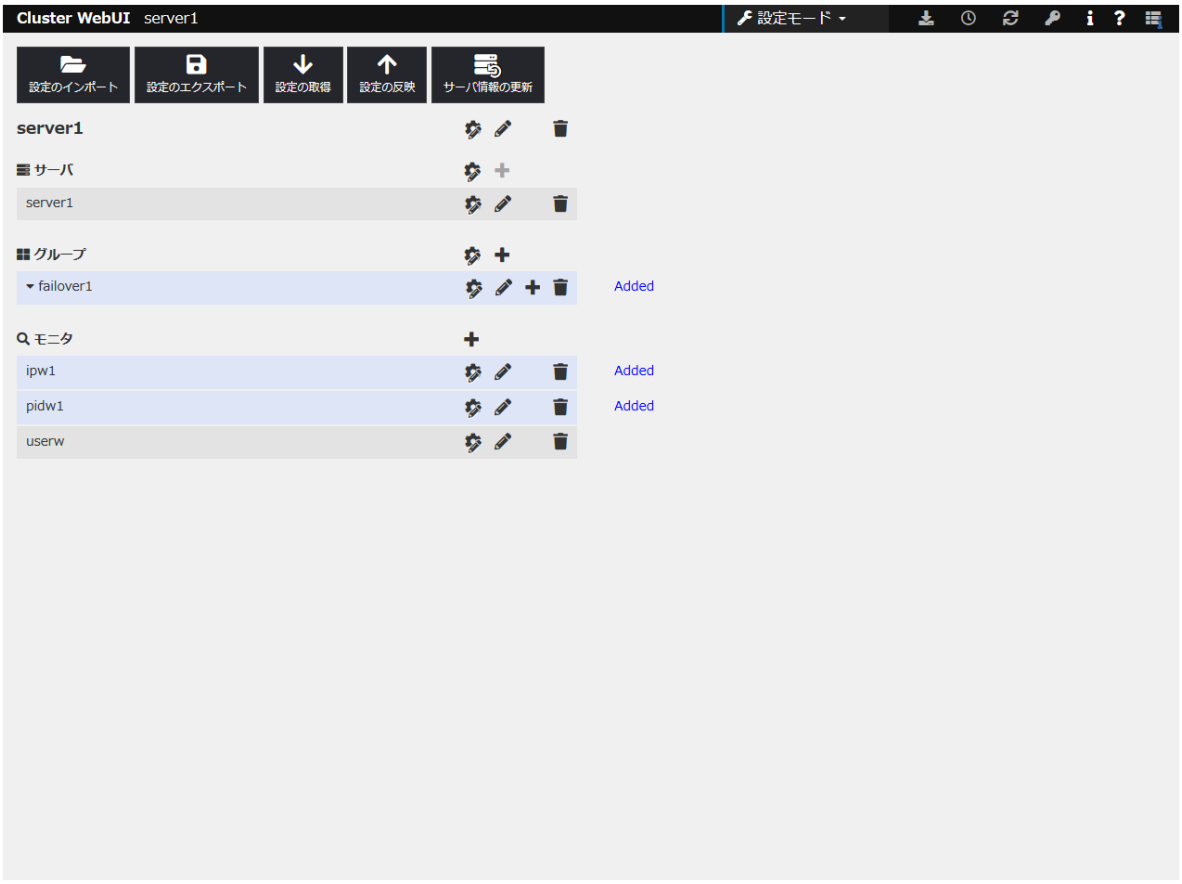
注釈: IP モニタリソースの監視対象には、LAN 上で、常時稼動が前提とされている機器 (例えば、ゲートウェイ) の IP アドレスを指定します。

6. 入力した IP アドレスが [IP アドレス一覧] に設定されます。[次へ] をクリックします。
7. 回復動作設定が表示されます。[参照] を押して LocalServer を選択します。[完了] をクリックします。

モニタリソース (PID モニタリソース) を追加する

このモニタリソースは EXEC リソースの開始スクリプトの種類が [非同期] の場合に設定可能です。

1. モニタ] の [モニタリソースの追加] をクリックします。
2. [タイプ] ボックスでモニタリソースのタイプ (PID モニタ) を選択し、[名前] ボックスにモニタリソース名 (pidw1) を入力します。[次へ] をクリックします。
3. 監視 (共通) 設定を入力します。[参照] をクリックします。
4. 表示されるツリービューで [exec1] をクリックし、[OK] をクリックします。[対象リソース] に [exec1] が設定されます。[次へ] をクリックします。
5. 回復対象を設定します。[参照] をクリックします。
6. 表示されるツリー ビューで [failover1] をクリックし、[OK] をクリックします。[回復対象] に [failover1] が設定されます。
7. [完了] をクリックします。
   設定後の画面は以下のようになります。



以上で構成情報の作成は終了です。次の「 3.4. 構成情報を保存する 」へ進んでください。

3.4 構成情報を保存する

構成情報は、使用中の PC のディレクトリ上または外部メディアに保存することができます。

構成情報を保存するには、以下の手順に従ってください。

1. Cluster WebUI の設定モードから [設定のエクスポート] をクリックします。
2. 保存先を選択し、保存します。

注釈: ファイル 1 点 (clp.conf) とディレクトリ 1 点 (scripts) を zip で圧縮したファイルが保存されます。これらのファイルとディレクトリがすべて揃っていない場合は構成情報の反映の実行が不成功に終わりますので、移動する場合はかならずこの 2 点をセットとして取り扱ってください。なお、新規作成した構成情報を変更した場合は、上記 2 点に加えて clp.conf.bak が作成されます。

注釈: CLUSTERPRO X SingleServerSafe インストール時に [通信ポート番号設定] 画面で既定値と異なるポート番号を指定した場合、構成情報を保存する前に [クラスタプロパティ] - [ポート番号] タブで [WebManager HTTP ポート番号] をインストール時と同じ値に設定してください。

3.5 構成情報をチェックする

Cluster WebUI で作成したクラスタ構成情報をクラスタサーバに反映する前に、設定したクラスタ構成情報のチェックを行うことができます。

1. Cluster WebUI の設定モードから [クラスタ構成情報チェック] をクリックします。
2. チェックが完了すると結果が別画面で表示されます。作成したクラスタ構成情報の設定内容によってはチェック完了まで時間がかかる場合があります。

以下に各チェック内容の詳細について記載します。

クラスタプロパティ

チェック内容	説明
ポート番号タブ：ポート番号チェック	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が、CLUSTERPRO が使用する通信ポート番号と重複していないかを確認します。
ポート番号 (ログ) タブ：ポート番号チェック	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が、CLUSTERPRO が使用する通信ポート番号と重複していないかを確認します。

ハートビートリソース

チェック内容	説明
hb の ping チェック	ハートビートリソースとして設定された IP アドレスに対して ping を実行し、該当 IP アドレスが使用可能であるかを確認します。

その他

チェック内容	説明
SELinux の設定チェック	SELinux が適切に設定されているか確認します。
カーネルチェック	カーネルのバージョンを確認します。
tar コマンドの存在チェック	tar コマンドがインストールされているか確認します。
zip コマンドの存在チェック	zip コマンドがインストールされているか確認します。
セキュアブートチェック	セキュアブートが無効になっているか確認します。

非推奨設定確認

チェック内容	説明
非活性異常時の復旧動作チェック	各グループリソースの非活性異常時の最終動作に、「何もしない」以外が設定されているかを確認します。

注釈: 出力されるメッセージについて「クラスタ構成情報チェックの詳細情報」を参照してください。

3.6 構成情報を反映する

Cluster WebUI で構成情報を作成したら、サーバに構成情報を反映させます。

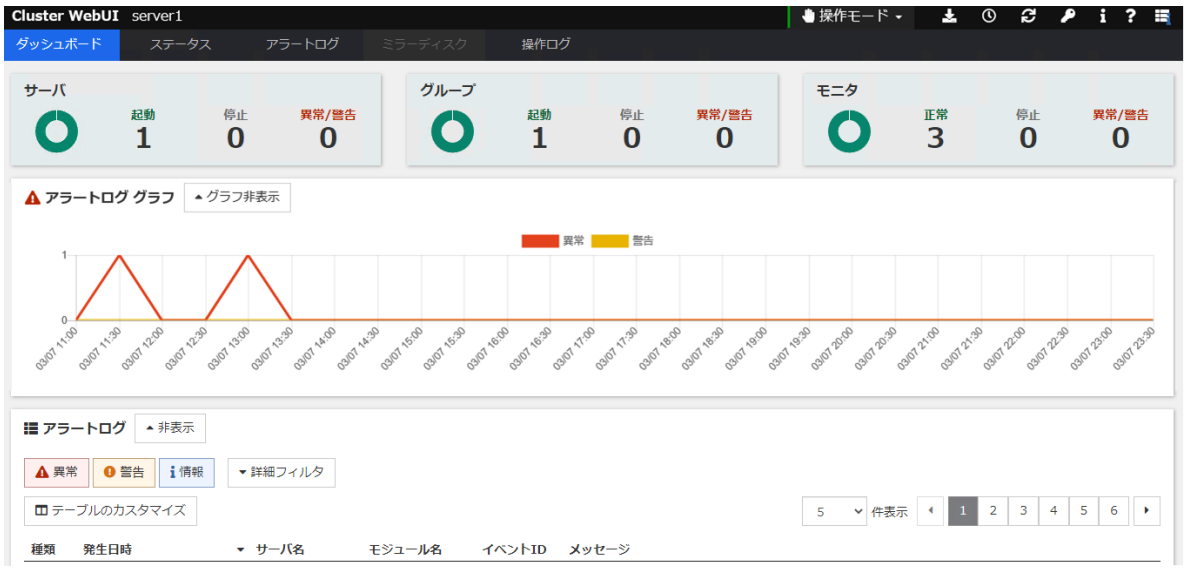
構成情報を反映するには、以下の手順に従ってください。

1. Cluster WebUI の設定モードから、[設定の反映] をクリックします。
2. 設定の反映前後の構成情報の差異によっては、ポップアップウィンドウに反映に必要な動作に関する確認が表示されます。

   動作内容に問題がなければ、[OK] をクリックします。

   アップロードに成功すると、[反映に成功しました。] のメッセージが表示されますので、[了解] をクリックします。

   アップロードに失敗した場合は、表示されるメッセージに従って操作を行ってください。
3. 状態が Cluster WebUI に表示されます。



Cluster WebUI の操作・確認方法についてはオンラインマニュアルを参照してください。

オンラインマニュアルは画面右上部の [?] から参照できます。

注釈: ファイアウォールの設定に、clpfwctrl コマンドを使用した場合には、構成情報の反映後にもコマンドの実行が必要です。

第 4 章

システムを確認する

本章では、作成したシステムが正常に起動するかどうかを確認します。

本章で説明する項目は以下のとおりです。

4.1 Cluster WebUI による動作確認

設定後のシステムの確認には、Cluster WebUI を使用して行う方法と、コマンドラインを使用して行う方法があります。本トピックでは、Cluster WebUI を使用してシステムの確認を行う方法について説明します。Cluster WebUI は、CLUSTERPRO Server と同時にインストールされます。新たにインストールを行う必要はありません。ここでは、まず Cluster WebUI の概要を説明し、その後、Cluster WebUI にアクセスし、サーバの状態を確認する方法について説明します。

参考:

Cluster WebUI の動作環境については、『インストールガイド』の「CLUSTERPRO X SingleServerSafe について」 - 「CLUSTERPRO X SingleServerSafe の動作環境を確認する」 - 「ソフトウェア」を参照してください。

Cluster WebUI を接続後、以下の手順で動作を確認します。

参考:

Cluster WebUI の操作方法についてはオンラインマニュアルを参照してください。

1. ハートビートリソース

   Cluster WebUI 上でサーバのステータスが起動済であることを確認します。

   サーバのハートビートリソースのステータスが正常であることを確認します。

2. モニタリソース

   Cluster WebUI 上で各モニタリソースのステータスが正常であることを確認します。

3. グループ起動

   グループを起動します。

   Cluster WebUI 上でグループのステータスが起動済であることを確認します。

4. EXEC リソース

   EXEC リソースを持つグループが起動しているサーバで、アプリケーションが動作していることを確認します。

5. グループ停止

   グループを停止します。

   Cluster WebUI 上でグループのステータスが停止済であることを確認します。

6. グループ起動

   グループを起動します。

   Cluster WebUI 上でグループのステータスが起動済であることを確認します。

7. サーバ シャットダウン

   サーバをシャットダウンします。サーバが正常にシャットダウンされることを確認します。

4.2 コマンドによるサーバの動作確認

生成後、コマンドラインを使用して構成するサーバ上から状態を確認するには、以下の手順で動作を確認します。

参考:

コマンドの操作方法については『操作ガイド』の「CLUSTERPRO X SingleServerSafe コマンドリファレンス」を参照してください。

clpstat コマンドを使用して、サーバのステータスが ONLINE であることを確認します。サーバのハートビート リソースのステータスが NORMAL で あることを確認します。

1. ハートビート リソース

   clpstat コマンドを使用して、サーバのステータスが ONLINE であることを確認します。

   サーバのハートビート リソースのステータスが NORMAL であることを確認します。

2. モニタ リソース

   clpstat コマンドを使用して、各モニタ リソースのステータスが NORMAL であることを確認します。

3. グループ起動

   clpgrp コマンドを使用して、グループを起動します。

   clpstat コマンドを使用して、グループのステータスが ONLINE であることを確認します。

4. EXEC リソース

   EXEC リソースを持つグループが起動しているサーバで、アプリケーションが動作していることを確認します。

5. グループ停止

   clpgrp コマンドを使用して、グループを停止します。

   clpstat コマンドを使用して、グループのステータスが OFFLINE であることを確認します。

6. グループ起動

   clpgrp コマンドを使用して、グループを起動します。

   clpstat コマンドを使用して、グループのステータスが ONLINE であることを確認します。

7. シャットダウン

   clpstdn コマンドを使用してサーバをシャットダウンします。サーバが正常にシャットダウンされることを確認します。

第 5 章

グループリソースの詳細

本章では、グループリソースについての詳細を説明します。

CLUSTERPRO X SingleServerSafe は、クラスタリングソフトウェアである CLUSTERPRO X との操作性などにおける親和性を高めるために、共通の画面を使用しています。

本章で説明する項目は以下のとおりです。

5.1 グループリソース一覧

グループリソースとして定義可能なリソースは以下の通りです。

グループリソース名	機能	略称
EXEC リソース	グループの起動時、終了時に実行されるアプリケーションやシェルスクリプトを登録します。	exec

5.2 EXEC リソースの設定

CLUSTERPRO では、CLUSTERPRO によって管理され、グループの起動時、終了時に実行されるアプリケーションやシェルスクリプトを登録できます。EXEC リソースには、ユーザ独自のプログラムやシェルスクリプトなども登録できます。シェルスクリプトは、sh のシェルスクリプトと同じ書式なので、それぞれのアプリケーションの事情にあわせた処理を記述できます。

5.2.1 EXEC リソースで使用するスクリプト

スクリプトの種類

EXEC リソースには、それぞれ開始スクリプトと終了スクリプトが用意されています。CLUSTERPRO は、サーバの状態遷移が必要な場面において、EXEC リソースごとのスクリプトを実行します。動作させたいアプリケーションの起動、終了、もしくは復旧の手順を、これらのスクリプトに記述する必要があります。

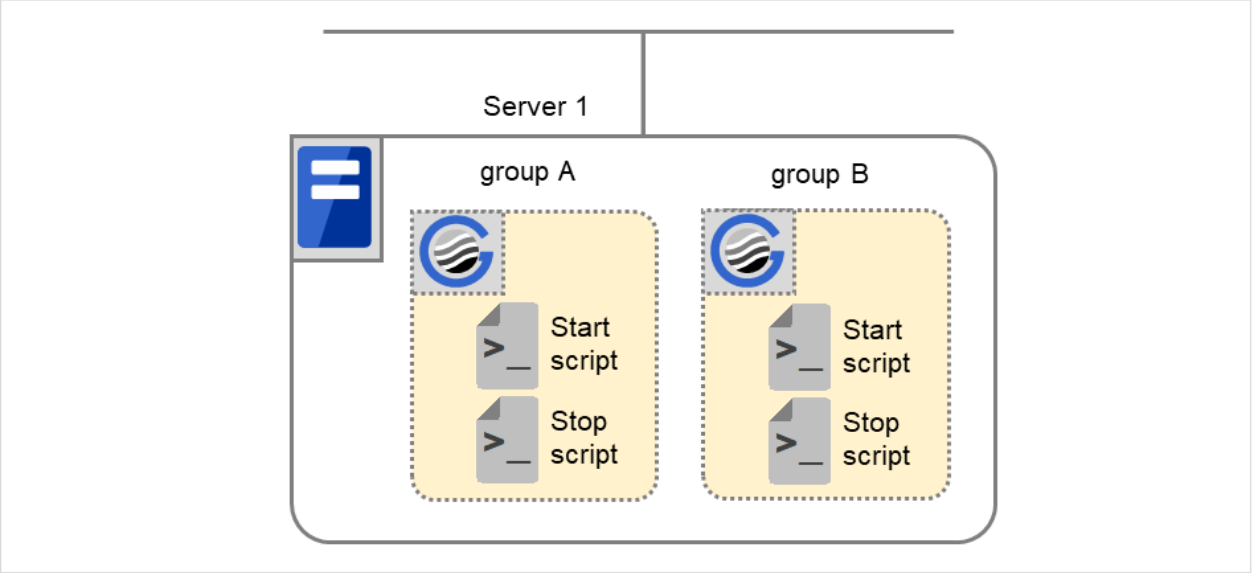


図 5.1　EXEC リソースで使用するスクリプト

Start

開始スクリプト

Stop

終了スクリプト

5.2.2 EXEC リソースのスクリプトで使用する環境変数

CLUSTERPRO は、スクリプトを実行する場合に、どの状態で実行したか (スクリプト実行要因) などの情報を環境変数にセットします。

スクリプト内で下図の環境変数を分岐条件として、システム運用にあった処理内容を記述できます。

終了スクリプトの環境変数は、直前に実行された開始スクリプトの内容を、値として返します。開始スクリプトでは CLP_FACTOR および CLP_PID の環境変数はセットされません。

CLP_LASTACTION の環境変数は、CLP_FACTOR の環境変数が CLUSTERSHUTDOWN または SERVERSHUTDOWN の場合にのみセットされます。

環境変数	環境変数の値	意味
CLP_EVENT …スクリプト実行要因	START	グループの起動により、実行された場合。 モニタリソースの異常検出によるグループの再起動により、同じサーバで実行された場合。 モニタリソースの異常検出によるグループリソースの再起動により、同じサーバで実行された場合。
	FAILOVER	使用しません。
CLP_FACTOR …グループ停止要因	CLUSTERSHUTDOWN	サーバ停止により、グループの停止が実行された場合。
	SERVERSHUTDOWN	サーバ停止により、グループの停止が実行された場合。
	GROUPSTOP	グループ停止により、グループの停止が実行された場合。
	GROUPMOVE	使用しません。
	GROUPFAILOVER	使用しません。
	GROUPRESTART	モニタリソースの異常検出により、グループの再起動が実行された場合。

次のページに続く

表 5.2 – 前のページからの続き

環境変数	環境変数の値	意味
	RESOURCERESTART	モニタリソースの異常検出により、グループリソースの再起動が実行された場合。
CLP_LASTACTION …停止後処理	REBOOT	OS を reboot (再起動) する場合。
	HALT	OS を halt (シャットダウン) する場合。
	NONE	何もしない。
CLP_SERVER	HOME	使用しません。
	OTHER	使用しません。
CLP_DISK	SUCCESS	使用しません。
	FAILURE	使用しません。
CLP_PRIORITY	1〜クラスタ内のサーバ数	使用しません。
CLP_GROUPNAME …グループ名	グループ名	スクリプトが属している、グループ名を示す。
CLP_RESOURCENAME …リソース名	リソース名	スクリプトが属している、リソース名を示す。
CLP_PID …プロセス ID	プロセス ID	プロパティとして開始スクリプトが非同期に設定されている場合、開始スクリプトのプロセス ID を示す。開始スクリプトが同期に設定されている場合、本環境変数は値を持たない。
CLP_VERSION_FULL …CLUSTERPRO フルバージョン	CLUSTERPRO フルバージョン	CLUSTERPRO のフルバージョンを示す。 （例） 5.3.1-1

次のページに続く

表 5.2 – 前のページからの続き

環境変数	環境変数の値	意味
CLP_VERSION_MAJOR …CLUSTERPRO メジャーバージョン	CLUSTERPRO メジャーバージョン	CLUSTERPRO のメジャーバージョンを示す。 （例）5
CLP_PATH …CLUSTERPRO インストールパス	CLUSTERPRO インストールパス	CLUSTERPRO がインストールされているパスを示す。 （例）/opt/nec/clusterpro
CLP_OSNAME …サーバ OS 名	サーバ OS 名	スクリプトが実行されたサーバの OS 名を示す。 （例） (1) OS 名が取得できた場合： Red Hat Enterprise Linux Server release 6.8 (Santiago) (2) OS 名が取得できなかった場合： Linux
CLP_OSVER …サーバ OS バージョン	サーバ OS バージョン	スクリプトが実行されたサーバの OS バージョンを示す。 （例） (1) OS バージョンが取得できた場合：6.8 (2) OS バージョンが取得できなかった場合：※値なし

EXEC リソース スクリプトの実行タイミング

開始、終了スクリプトの実行タイミングと環境変数の関連を、状態遷移図にあわせて説明します。

- 図中のサーバは以下の状態を表しています。

  - (例) 正常状態にある Server 1 において Group A が動作している。

- 定義されているグループは A、B の 2 つ。

【状態遷移図】

状態遷移について説明します。

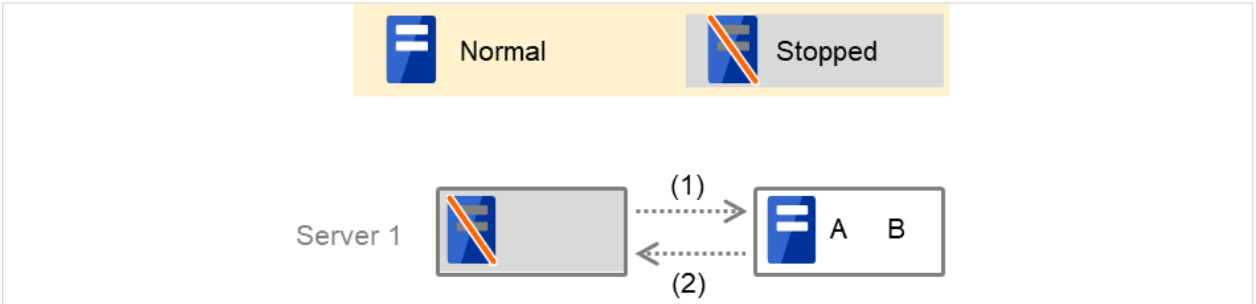


図 5.2　状態遷移図

図中の (1)～(2) は、以下の説明に対応しています。

(1) 通常立ち上げ

ここでいう通常立ち上げとは、開始スクリプトがサーバで正常に実行された時を指します。

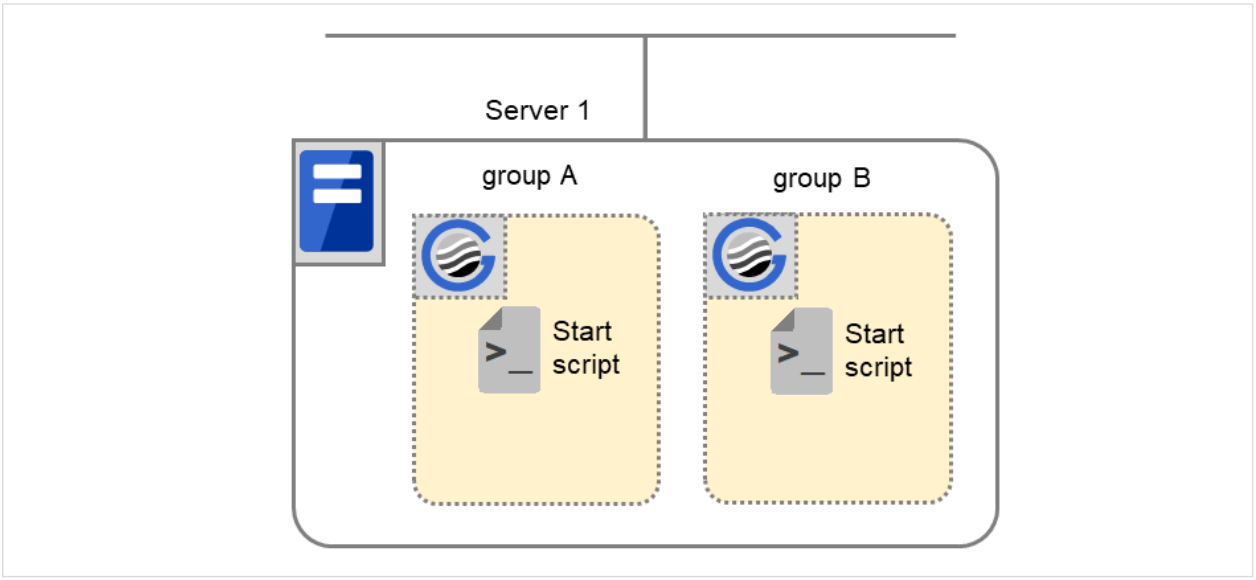


図 5.3　状態とスクリプト実行（通常立ち上げ）

Start に対する環境変数

	Group A	Group B
CLP_EVENT	START	START

(2) 通常シャットダウン

ここでいう通常シャットダウンとは、終了スクリプトに対応する開始スクリプトが、通常立ち上げにより実行されたシャットダウンを指します。

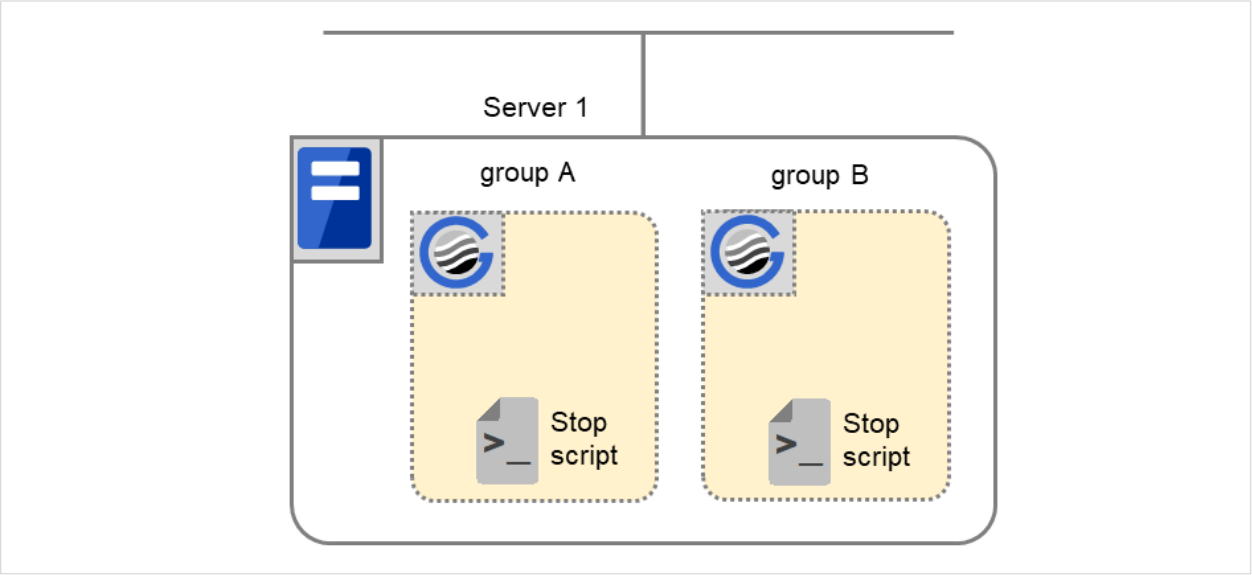


図 5.4　状態とスクリプト実行（通常シャットダウン）

Stop に対する環境変数

	Group A	Group B
CLP_EVENT	START	START

5.2.3 EXEC リソーススクリプトの記述の流れ

前のトピックの、スクリプトの実行タイミングと実際のスクリプト記述を関連付けて説明します。文中の (数字) は「5.2.2. *EXEC* リソース スクリプトの実行タイミング」の各動作をさします。

グループ A 開始スクリプト： start.sh の一例

```
#!/bin/sh
# ***************************************
# *              start.sh               *
# ***************************************

# スクリプト実行要因の環境変数を参照して処理の振り分けを行う。
if [ "$CLP_EVENT" = "START" ]
then
    # ここに、業務の通常起動処理を記述する。
    # この処理は以下のタイミングで実行される。
```

(次のページに続く)

(前のページからの続き)

```
    #
    # (1) 通常立ち上げ
    #

else
    # CLUSTERPRO は動作していない。

fi

# 終了コードが 0 の場合、EXEC リソースの活性処理は成功と判定される。
# スクリプト内でエラーが発生した場合には 0 以外の終了コードを返却するように記述する。
exit 0
```

グループ A 終了スクリプト： stop.sh の一例

```
#!/bin/sh
# ************************************
# *              stop.sh             *
# ************************************

# スクリプト実行要因の環境変数を参照して処理の振り分けを行う。
if [ "$CLP_EVENT" = "START" ]
then
    # ここに、業務の通常終了処理を記述する。以下のタイミングで実行される。
    #
    # (2) 通常シャットダウン
    #

else
    # CLUSTERPRO は動作していない。
fi

exit 0
```

5.2.4 EXEC リソーススクリプト作成のヒント

以下の点に注意して、スクリプトを作成してください。

- スクリプト中にて、実行に時間を必要とするコマンドを実行する場合には、コマンドの実行が完了したことを示すトレースを残すようにしてください。この情報は、問題発生時、障害の切り分けを行う場合に使用することができます。トレースを残す方法は下記の 2 つがあります。

- スクリプト中に echo コマンドを記述して EXEC リソースのログ出力先を設定する方法

  トレースを echo コマンドにて標準出力することができます。その上で、スクリプトが属しているリソースのプロパティでログ出力先を設定します。

デフォルトではログ出力されません。ログ出力先の設定については「5.2.6. 詳細タブ」の「EXEC リソース調整プロパティ」にある「メンテナンスタブ」を参照してください。[ローテートする] チェックボックスがオフの場合は、ログ出力先に設定されたファイルには、サイズが無制限に出力されますのでファイルシステムの空き容量に注意してください。

(例：スクリプト中のイメージ)

```
echo "appstart.."
appstart
echo "OK"
```

- スクリプト中に clplogcmd を記述する方法

  clplogcmd でアラートログや OS の syslog に、メッセージを出力できます。clplogcmd については、『操作ガイド』の「CLUSTERPRO X SingleServerSafe コマンドリファレンス」の「メッセージを出力する (clplogcmd コマンド)」を参照してください。

(例：スクリプト中のイメージ)

```
clplogcmd -m "appstart.."
appstart
clplogcmd -m "OK"
```

5.2.5 EXEC リソース 注意事項

- スクリプトのログローテート機能について

  スクリプトのログローテート機能を有効にした場合、ログ出力を仲介するプロセス (仲介プロセス) が生成されます。仲介プロセスは、「開始・停止スクリプト」および「開始・停止スクリプトから標準出力・標準エラー出力のいずれかまたは両方を継承した子孫プロセス」からのログ出力が全て停止 (ファイルディスクリプタがクローズ) するまで動作を継続します。子孫プロセスの出力をログから除外する場合は、スクリプトからのプロセス生成時に標準出力および標準エラー出力をリダイレクトしてください。

- 開始スクリプト/終了スクリプトは root ユーザで実行されます。
- 環境変数に依存するアプリケーションを起動する際には必要に応じてスクリプト側で環境変数の設定を行っていただく必要があります。

5.2.6 詳細タブ

ユーザアプリケーション

スクリプトとしてサーバ上の実行可能ファイル (実行可能なシェルスクリプトやバイナリファイル) を使用します。各実行可能ファイル名は、サーバ上のローカルディスクのパスで設定します。

Cluster WebUI の構成情報には含まれません。スクリプトファイルは Cluster WebUI では編集できません。

この製品で作成したスクリプト

スクリプトとして Cluster WebUI で準備したスクリプトファイルを使用します。必要に応じて Cluster WebUI でスクリプトファイルを編集できます。スクリプトファイルは、構成情報に含まれます。

表示

[この製品で作成したスクリプト] を選択した場合に、スクリプトファイルを表示します。

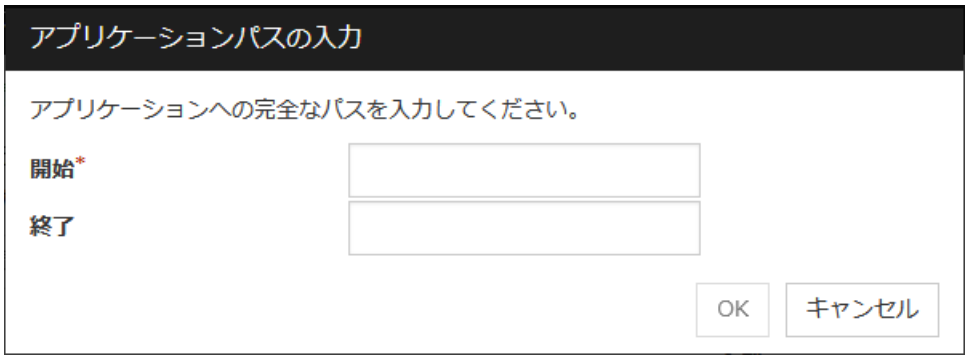
編集

[この製品で作成したスクリプト] を選択した場合に、スクリプトファイルを編集します。変更を反映するには [保存] をクリックしてください。スクリプトファイル名の変更はできません。

[ユーザアプリケーション] を選択している場合は [アプリケーション・パスの入力] ダイアログボックスが表示されます。

アプリケーション・パスの入力

EXEC リソースの実行可能ファイル名を設定します。



開始 (1023 バイト以内)

EXEC リソースの開始時の実行可能ファイル名を設定します。「/」 で始まる必要があります。引数を指定することも可能です。

終了 (1023 バイト以内)

EXEC リソースの終了時の実行可能ファイル名を設定します。「/」 で始まる必要があります。終了スクリプトは省略可能です。

実行可能ファイル名はサーバ上のファイルを「/」 から始まる完全なパス名で設定する必要があります。引数を指定することも可能です。

置換

[この製品で作成したスクリプト] を選択した場合に、[ファイル選択] ダイアログボックスが表示されます。

[リソースのプロパティ] で選択したスクリプトファイルの内容が、ファイル選択ダイアログ ボックスで選択したスクリプトファイルの内容に置換されます。スクリプトが表示中または編集中の場合は置換できません。ここではスクリプトファイルを選択してください。バイナリファイル (アプリケーションなど) は選択しないでください。

調整

EXEC リソース調整プロパティダイアログを表示します。EXEC リソースの詳細設定を行います。EXEC リソースを PID モニタリソースで監視するには、開始スクリプトの設定を非同期にする必要があります。

EXEC リソース調整プロパティ

パラメータタブ

[開始スクリプト]、[終了スクリプト] 全スクリプト共通

同期

スクリプトの実行時にスクリプトの終了を待ちます。常駐しない (実行後に処理がすぐ戻る) 実行可能ファイルの場合に選択します。

非同期

スクリプトの実行時にスクリプトの終了を待ちません。常駐する実行可能ファイルの場合に選択します。

EXEC リソースの開始スクリプトを非同期で実行する場合は、PID モニタリソースで監視できます。

タイムアウト (1～9999)

スクリプトの実行時に終了を待つ場合 ([同期]) のタイムアウトを設定します。[同期] を選択している場合のみ入力可能です。設定時間内にスクリプトが終了しないと、異常と判断します。

メンテナンスタブ

ログ出力先 (1023 バイト以内)

EXEC リソースのスクリプトや実行可能ファイルの標準出力と標準エラー出力のリダイレクト先を指定します。何も指定しない場合、/dev/null に出力されます。[/] で始まる必要があります。

[ローテートする] チェックボックスがオフの場合は無制限に出力されますのでファイルシステムの空き容量に注意してください。

[ローテートする] チェックボックスがオンの場合は、出力されるログファイルは、ローテートします。また、以下の注意事項があります。

- [ログの出力先] には 1009 バイト以内でログのパスを記述してください。1010 バイトを超えた場合、ログの出力が行えません。
- ログファイルの名前の長さは 31 バイト以内で記述してください。32 バイト以上の場合、ログの出力が行えません。
- EXEC リソースごとに異なるログファイル名を設定してください。

  複数の EXEC リソースでログローテートを行う場合、パス名が異なってもログファイルの名前が同じ場合 (ex. /home/foo01/log/exec.log, /home/foo02/log/exec.log)、複数の EXEC リソースのログが、いずれか 1 つのログファイルに出力されます。また、ローテートサイズが正しく反映されないことがあります。

ローテートする

EXEC リソースのスクリプトや実行可能ファイルの実行ログを、オフの場合は無制限のファイルサイズで、オンの場合はローテートして出力します。

ローテートサイズ (1～999999999)

[ローテートする] チェックボックスがオンの場合に、ローテートするサイズを指定します。

ローテート出力されるログファイルの構成は、以下のとおりです。

ファイル名	内容
[ログ出力先] 指定のファイル名	最新のログです。
[ログ出力先] 指定のファイル名.pre	ローテートされた以前のログです。

第 6 章

モニタリソースの詳細

本章では、CLUSTERPRO X SingleServerSafe で監視を実行する単位であるモニタリソースについての詳細を説明します。

CLUSTERPRO X SingleServerSafe は、クラスタリングソフトウェアである CLUSTERPRO X との操作性などにおける親和性を高めるために、共通の画面を使用しています。

本章で説明する項目は以下のとおりです。

6.1 モニタリソース一覧

モニタリソースとして定義可能なリソースは以下の通りです。

モニタリソース名	機能	監視タイミング (太字は既定値)	対象リソース
ディスクモニタリソース	ディスクデバイスの監視を行います。	**常時**/活性時	全て
IP モニタリソース	ping コマンドを使用して応答の有無により、IP アドレスおよび通信路の監視を行います。	**常時**/活性時	全て
NIC Link Up/Down モニタリソース	NIC の Link 状態を取得し、Link の Up/Down の監視を行います。	**常時**/活性時	全て
PID モニタリソース	活性に成功した EXEC リソースを監視します。	活性時 (固定)	exec
ユーザ空間モニタリソース	ユーザ空間のストールを異常として判断します。	常時 (固定)	-
マルチターゲットモニタリソース	複数のモニタリソースの状態の組み合わせで監視を行います。	**常時**/活性時	全て
ソフト RAID モニタリソース	ソフト RAID を行っているデバイスを監視します。	常時 (固定)	なし
カスタムモニタリソース	任意のスクリプトを実行することで監視を行います。	**常時**/活性時	全て
ボリュームマネージャモニタリソース	複数のストレージやディスクの監視機構を提供します。	常時/**活性時**	全て
外部連携モニタリソース	"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" を実現します。	**常時**/活性時	なし
プロセス名モニタリソース	任意のプロセス名のプロセスを監視します。	**常時**/活性時	全て
DB2 モニタリソース	IBM DB2 データベースへの監視機構を提供します。	活性時 (固定)	全て

次のページに続く

表 6.1 – 前のページからの続き

モニタリソース名	機能	監視タイミング (太字は既定値)	対象リソース
FTP モニタリソース	FTP サーバへの監視機構を提供します。	常時/**活性時**	全て
HTTP モニタリソース	HTTP サーバへの監視機構を提供します。	常時/**活性時**	全て
IMAP4 モニタリソース	IMAP サーバへの監視機構を提供します。	常時/**活性時**	全て
MySQL モニタリソース	MySQL データベースへの監視機構を提供します。	活性時 (固定)	全て
NFS モニタリソース	NFS のファイルサーバへの監視機構を提供します。	**常時**/活性時	全て
ODBC モニタリソース	ODBC データベースへの監視機構を提供します。	活性時 (固定)	全て
Oracle モニタリソース	Oracle データベースへの監視機構を提供します。	活性時 (固定)	全て
POP3 モニタリソース	POP サーバへの監視機構を提供します。	常時/**活性時**	全て
PostgreSQL モニタリソース	PostgreSQL データベースへの監視機構を提供します。	活性時 (固定)	全て
Samba モニタリソース	samba ファイルサーバへの監視機構を提供します。	**常時**/活性時	全て
SMTP モニタリソース	SMTP サーバへの監視機構を提供します。	常時/**活性時**	全て
SQL Server モニタリソース	SQL Server データベースへの監視機構を提供します。	活性時 (固定)	全て
Tuxedo モニタリソース	Tuxedo アプリケーションサーバへの監視機構を提供します。	活性時	全て
WebLogic モニタリソース	WebLogic アプリケーションサーバへの監視機構を提供します。	活性時	全て
WebSphere モニタリソース	WebSphere アプリケーションサーバへの監視機構を提供します。	活性時	全て

次のページに続く

表 6.1 – 前のページからの続き

モニタリソース名	機能	監視タイミング (太字は既定値)	対象リソース
WebOTX モニタリソース	WebOTX アプリケーションサーバへの監視機構を提供します。	活性時	全て
JVM モニタリソース	Java VM の監視を行います。	**常時**/活性時	exec
システムモニタリソース	システムリソースの監視を行います。	常時 (固定)	全て
プロセスリソースモニタリソース	プロセスリソースの監視を行います。	常時 (固定)	全て

6.1.1 モニタリソースの監視開始後のステータス

モニタリソースの監視開始後、監視開始準備のために一時的にステータスが警告となることがあります。
モニタステータスが警告となる可能性があるのは、下記のモニタリソースです。

- 外部連携モニタリソース
- カスタムモニタリソース (監視タイプが [非同期] の場合のみ)
- DB2 モニタリソース
- システムモニタリソース
- プロセスリソースモニタリソース
- JVM モニタリソース
- MySQL モニタリソース
- ODBC モニタリソース
- Oracle モニタリソース
- PostgreSQL モニタリソース
- プロセス名モニタリソース
- SQL Server モニタリソース

6.1.2 モニタリソースの監視タイミング

モニタリソースによる監視は、常時監視と活性時監視の 2 つのタイプがあります。モニタリソースによって設定可能な監視タイミングが異なります。

a. 常時

モニタリソースは常に監視を行います。

b. 活性時

特定のグループリソースが活性状態の間、監視を実行します。グループリソースが非活性状態の間は監視を実行しません。

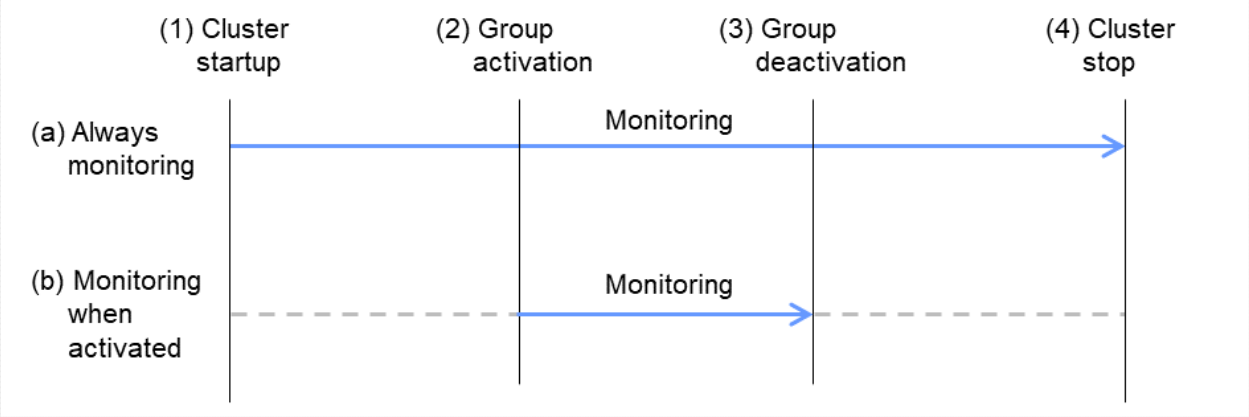


図 6.1　モニタリソースの常時監視と活性時監視

6.1.3 モニタリソースの一時停止/再開

モニタリソースは一時的に監視を停止したり再開したりすることが可能です。監視の一時停止/再開の方法は以下の 2 つの方法があります。

- Cluster WebUI による操作
- clpmonctrl コマンドによる操作

  clpmonctrl コマンドでは、コマンドの実行サーバ上のモニタリソースの制御のみ可能です

モニタリソースには、一時停止/再開の制御が可能なものと不可能なものがあります。モニタリソースによる制御の可否は下記を参照してください。

モニタリソース	制御可否
ディスクモニタリソース	可能
IP モニタリソース	可能

次のページに続く

表 6.2 – 前のページからの続き

モニタリソース	制御可否
ユーザ空間モニタリソース	可能
NIC Link Up/Down モニタリソース	可能
PID モニタリソース	可能
マルチターゲットモニタリソース	可能
カスタムモニタリソース	可能
ボリュームマネージャモニタリソース	可能
ソフト RAID モニタリソース	可能
プロセス名モニタリソース	可能
DB2 モニタリソース	可能
FTP モニタリソース	可能
HTTP モニタリソース	可能
IMAP4 モニタリソース	可能
MySQL モニタリソース	可能
NFS モニタリソース	可能
ODBC モニタリソース	可能
Oracle モニタリソース	可能
POP3 モニタリソース	可能
PostgreSQL モニタリソース	可能
Samba モニタリソース	可能
SMTP モニタリソース	可能
SQL Server モニタリソース	可能
Tuxedo モニタリソース	可能
WebLogic モニタリソース	可能
WebSphere モニタリソース	可能
WebOTX モニタリソース	可能
外部連携モニタリソース	可能
JVM モニタリソース	可能
システムモニタリソース	可能
プロセスリソースモニタリソース	可能

モニタリソースが一時停止状態で下記の操作を行った場合、モニタリソースの一時停止が解除されます。

- Cluster WebUI で、モニタリソースの「再開」を行った場合
- clpmonctrl コマンドに -r オプション を指定した場合
- クラスタを停止した場合
- クラスタをサスペンドした場合

6.1.4 モニタリソースの擬似障害 発生/解除

モニタリソースは擬似的に障害を発生させることが可能です。また、それを解除することもできます。擬似障害の発生/解除を行う方法は以下の 2 つの方法があります。

- Cluster WebUI (検証モード) による操作

  Cluster WebUI (検証モード) では、制御が不可能なモニタリソースの操作が無効になります。

- [clpmonctrl] コマンドによる操作

  [clpmonctrl] コマンドでは、コマンドを実行するサーバ上のモニタリソースに対して制御を行います。制御が不可能なモニタリソースに対して実行した場合、コマンドの実行自体は成功しますが、擬似障害を発生させることはできません。

モニタリソースには、擬似障害の発生/解除が可能なものと不可能なものがあります。『操作ガイド』 の 「CLUSTERPRO X SingleServerSafe コマンドリファレンス」の「モニタリソースを制御する (clpmonctrl コマンド)」を参照してください。

擬似障害発生状態で下記の操作を行った場合、モニタリソースの擬似障害が解除されます。

- Cluster WebUI (検証モード) で、モニタリソースの「擬似障害解除」を実行した場合
- Cluster WebUI のモードを、検証モード から 他のモードに変更する際に出力されるダイアログで「はい」を選択した場合
- clpmonctrl コマンドに -n オプション を指定した場合
- クラスタを停止した場合
- クラスタをサスペンドした場合

6.1.5 モニタリソースの監視プライオリティ

OS 高負荷時にモニタリソースへの監視を優先的に行うため、nice 値を設定することができます。

nice 値は 19(優先度低) ~ -20(優先度高) の範囲で指定することが可能です。

- nice 値の優先度を上げることで監視タイムアウトの検出を抑制することが可能です。

6.2 モニタリソースのプロパティ

6.2.1 情報タブ

名前

モニタリソース名を表示します。

コメント (127 バイト以内)

モニタリソースのコメントを設定します。半角英数字のみ入力可能です。

6.2.2 監視 (共通) タブ

インターバル (1～999)

監視対象の状態を確認する間隔を設定します。

タイムアウト (5～999[*1])

ここで指定した時間内に監視対象の正常状態が検出できない場合に異常と判断します。

タイムアウト発生時に監視プロセスのダンプを採取する

本機能を有効にした場合、モニタリソースがタイムアウトすると、タイムアウトしたモニタリソースのダンプが採取されます。ダンプ情報は最大 5 回採取されます。

タイムアウト発生時にリトライしない

本機能を有効にした場合、モニタリソースがタイムアウトすると即座に「タイムアウト発生時動作」を実行します。

タイムアウト発生時動作

[*1] ユーザ空間モニタリソースで監視方法に ipmi を設定している場合は、255 以下の値を設定する必要があります。

監視リソースタイムアウト発生時の動作を選択します。

また、タイムアウトが発生した場合にはリトライ回数の回数カウンタはリセットされます。

本機能は、[タイムアウト発生時にリトライしない] 機能を有効にしている場合のみ設定可能です。

- **[回復動作を実行する]**

  監視リソースがタイムアウトした場合に回復動作を実行します。

- **[回復動作を実行しない]**

  監視リソースがタイムアウトした場合に回復動作を実行しません。

- **[keepalive パニックを実行する]**

  keepalive パニックを実行します。

- **[sysrq パニックを実行する]**

  sysrq パニックを実行します。

注釈: 下記のモニタリソースでは、[タイムアウト発生時にリトライしない], [タイムアウト発生時動作] 機能は設定できません。

- ユーザ空間モニタリソース
- カスタムモニタリソース (監視タイプが [非同期] の場合のみ)
- マルチターゲットモニタリソース
- 外部連携モニタリソース
- JVM モニタリソース
- システムモニタリソース
- プロセスリソースモニタリソース

リトライ回数 (0～999)

異常状態を検出後、連続してここで指定した回数の異常を検出したときに異常と判断します。

0 を指定すると最初の異常検出で異常と判断します。

監視開始待ち時間 (0～9999)

監視を開始するまでの待ち時間を設定します。

監視タイミング

監視のタイミングを設定します。

- [常時]

監視を常時行います。

- [活性時]
  指定したリソースが活性するまで監視を行いません。

対象リソース

活性時監視を行う場合に対象となるリソースを表示します。

参照

対象リソースの選択ダイアログボックスを表示します。LocalServer とクラスタに登録されているグループ名、リソース名がツリー表示されます。対象リソースとして設定するリソースを選択して [OK] をクリックします。

nice 値

プロセスの nice 値を設定します。

監視処理時間メトリクスを送信する

モニタリソースの監視処理時間メトリクスの送信機能を設定します。

- チェックボックスがオン
  監視処理メトリクスを送信します。
- チェックボックスがオフ
  監視処理メトリクスを送信しません。

注釈:

Amazon CloudWatch 連携機能を使用する場合は、本機能を有効にすることで任意のモニタリソースの監視処理時間メトリクスが送信出来ます。

下記のモニタリソースでは、[監視処理時間メトリクスを送信する] 機能は設定できません。

- ユーザ空間モニタリソース
- カスタムモニタリソース (監視タイプが [非同期] の場合のみ)

- 外部連携モニタリソース
- JVM モニタリソース
- システムモニタリソース
- プロセスリソースモニタリソース

6.2.3 監視 (固有) タブ

モニタリソースによっては監視動作時のパラメータを設定する必要があります。パラメータは各リソースの説明に記述しています。

6.2.4 回復動作タブ

回復対象と異常検出時の動作を設定します。異常検出時にグループの再起動やリソースの再起動、サーバの再起動ができます。ただし、回復対象が非活性状態であれば回復動作は行われません。

回復動作

異常検出時の回復動作を選択します。

- [回復対象を再起動]

  回復対象として選択されたグループまたはグループリソースを再活性します。再活性が失敗するか、再活性後に同じ異常が検出された場合は、最終動作として選択された動作を実行します。

- [最終動作のみ実行]

  最終動作として選択された動作を実行します。

- [カスタム設定]

  回復対象として選択されたグループまたはグループリソースを最大再活性回数まで再活性します。再活性が失敗するか、再活性後に同じ異常が検出される状態が継続し、最大再活性回数に達した場合は、最終動作として選択された動作を実行します。

回復対象

リソースの異常とみなした時に回復を行う対象のオブジェクトが表示されます。

参照

回復対象の選択ダイアログ ボックスを表示します。LocalServer、All Groups とサーバに登録されているグループ名、リソース名がツリー表示されます。回復対象として設定するものを選択して [OK] をクリックします。

回復スクリプト実行回数 (0～99)

異常検出時に [スクリプト設定] で設定されたスクリプトを実行する回数を設定します。0 を設定するとスクリプトを実行しません。

再活性前にスクリプトを実行する

- チェックボックスがオン

  再活性化を実施する前にスクリプト/コマンドを実行します。スクリプト/コマンドの設定を 行うためには [スクリプト設定] をクリックしてください。

- チェックボックスがオフ

  スクリプト/コマンドを実行しません。

最大再活性回数 (0〜99)

異常検出時に再活性化を行う回数を設定します。0 を設定すると再活性化を行いません。回復対象にグループまたはグループリソースを選択した場合に設定可能です。

フェイルオーバ実行前にスクリプトを実行する

使用しません。

最大フェイルオーバ回数

使用しません。

最終動作前にスクリプトを実行する

最終動作を実行する前にスクリプトを実行するかどうかを指定します。

- チェックボックスがオン

  最終動作を実施する前にスクリプト/コマンドを実行します。スクリプト/コマンドの設定を行うためには [スクリプト設定] ボタンをクリックしてください。

- チェックボックスがオフ

  スクリプト/コマンドを実行しません。

[スクリプト設定] をクリックすると、[スクリプトの編集] ダイアログボックスが表示されます。実行するスクリプトまたは実行ファイルを設定して [OK] をクリックします。

スクリプト設定

[スクリプトの編集] ダイアログボックスを表示します。回復スクリプト、回復動作前に実行するスクリプト/コマンドを設定します。

ユーザアプリケーション

スクリプトとしてサーバ上の実行可能ファイル (実行可能なシェルスクリプトファイルや実行ファイル) を使用します。ファイル名にはサーバ上のローカルディスクの絶対パスまたは実行可能ファイル名を設定します。また、絶対パスやファイル名に空欄が含まれる場合は、下記のように、ダブルクォーテーション (") でそれらを囲ってください。

例:

```
"/tmp/user application/script.sh"
```

各実行可能ファイルは、Cluster WebUI の構成情報には含まれません。Cluster WebUI で編集やアップロードはできませんので、サーバ上に準備する必要があります。

この製品で作成したスクリプト

スクリプトとして Cluster WebUI で準備したスクリプトファイルを使用します。必要に応じて Cluster WebUI でスクリプトファイルを編集できます。スクリプトファイルは、構成情報に含まれます。

ファイル (1023 バイト以内)

[ユーザアプリケーション] を選択した場合に、実行するスクリプト（実行可能なシェルスクリプトファイルや実行ファイル）を設定します。

表示

[この製品で作成したスクリプト] を選択した場合に、スクリプトファイルを表示します。

編集

[この製品で作成したスクリプト] を選択した場合に、スクリプトファイルを編集します。変更を反映するには [保存] をクリックしてください。スクリプトファイル名の変更はできません。

置換

[この製品で作成したスクリプト] を選択した場合に、スクリプトファイルの内容を、ファイル選択ダイアログ ボックスで選択したスクリプトファイルの内容に置換します。スクリプトが既に表示中または編集中の場合は置換できません。ここではスクリプトファイルを選択してください。バイナリファイル (アプリケーションなど) は選択しないでください。

タイムアウト (1～9999)

スクリプトの実行完了を待ち合わせる最大時間を指定します。既定値は 5 秒です。

最終動作

再活性化による回復が失敗した後の回復動作を選択します。

最終動作は以下の動作が選択できます。

- 何もしない

  何も行いません。

注釈: [何もしない] の設定は

- 一時的に最終動作を抑止したい場合
- 異常を検出したときにアラートの表示のみを行いたい場合
- 実際の最終動作はマルチターゲットモニタリソースで行いたい場合

に使用してください。

- リソース停止

  回復対象としてグループリソースが選択されている場合、選択したグループリソースとそのグループリソースに依存するグループリソースを停止します。回復対象に "LocalServer" 、"All Groups"、グループが選択されている場合は選択できません。

- グループ停止

  回復対象としてグループが選択されている場合そのグループを、また回復対象としてグループリソースが選択されている場合そのグループリソースが所属するグループを停止します。"All Groups"が選択されている場合は、モニタリソースが異常を検出したサーバで起動している全てのグループを停止します。

- クラスタサービス停止

  CLUSTERPRO X SingleServerSafe を停止します。

- クラスタサービス停止と OS シャットダウン

  CLUSTERPRO X SingleServerSafe を停止し、OS をシャットダウンします。

- クラスタサービス停止と OS 再起動

CLUSTERPRO X SingleServerSafe を停止し、OS を再起動します。

- sysrq パニック

  sysrq のパニックを行います。

  注釈: sysrq パニックに失敗した場合、OS のシャットダウンを行います。

- keepalive リセット

  clpkhb ドライバ、clpka ドライバを使用し、OS をリセットします。

  注釈:

  keepalive リセットに失敗した場合、OS のシャットダウンを行います。
  clpkhb ドライバ、clpka ドライバが対応していない OS、kernel では設定しないでください。

- keepalive パニック

  clpkhb ドライバ、clpka ドライバを使用し、OS をパニックします。

  注釈:

  keepalive パニックに失敗した場合、OS のシャットダウンを行います。
  clpkhb ドライバ、clpka ドライバが対応していない OS、kernel では設定しないでください。

- BMC リセット

  サーバをハードウェアリセットします。

  注釈: BMC リセットに失敗した場合、OS のシャットダウンを行います。

- BMC パワーオフ

  サーバの電源をオフにします。OS の ACPI の設定により OS のシャットダウンが実行される場合があります。

  注釈: BMC パワーオフに失敗した場合、OS のシャットダウンを行います。

- BMC パワーサイクル

サーバでパワーサイクル（電源オフ/オン）を実行します。OS の ACPI の設定により OS のシャットダウンが実行される場合があります。

注釈: BMC パワーサイクルに失敗した場合、OS のシャットダウンを行います。

- BMC NMI

  サーバで NMI を発生させます。NMI 発生後の挙動は OS の設定に依存します。

注釈: BMC NMI に失敗した場合、OS のシャットダウンを行います。

6.3 ディスクモニタリソースの設定

ディスクモニタリソースは、ディスクデバイスの監視を行います。ディスクモニタリソース (TUR 方式) が使用できないディスクでは、READ(O_DIRECT) 方式での監視を推奨します。

6.3.1 監視 (固有) タブ

監視方法

ディスクデバイスを監視するときの監視方法を下記より選択します。

- TUR
- TUR(generic)
- TUR(legacy)
- READ
- READ (O_DIRECT)
- WRITE (FILE)
- READ (RAW)

監視先 (1023 バイト以内)

- 監視方法が WRITE (FILE) の場合

  監視用のファイルのパス名を指定します。[/] で始まる必要があります。

  ファイル名は絶対パスで指定してください。既存のファイルのファイル名を指定した場合には上書きされファイルの内容は失われます。

- 監視方法が READ(O_DIRECT) の場合

  監視用のデバイスファイルもしくはファイルのパス名を指定します。[/] で始まる必要があります。

  デバイスファイル名もしくはファイル名は絶対パスで指定してください。

  ファイル名を指定する場合は、指定するファイルを事前に作成しておく必要があります。

- 監視方法が READ(RAW) の場合

  監視先は空欄でもかまいません。ただし、監視対象 RAW デバイス名の入力は必須となります。バインドをして監視を行う場合のみ指定します。既に mount しているパーティションデバイスまたは mount する可能性のあるパーティションデバイスをデバイス名に設定して監視することはできません。

  また、既に mount しているパーティションデバイスまたは mount する可能性のあるパーティションデバイスの whole device (ディスク全体を示すデバイス) をデバイス名に設定して監視することもできません。監視専用のパーティションを用意してください。(監視用のパーティションサイズは、10MB 以上を割り当ててください) [/] で始まる必要があります。

- 監視方法が READ の場合

  ディスクデバイスを監視するときの監視先デバイス名もしくはファイル名を指定します。[/] で始まる必要があります。ファイル名を指定する場合は、指定するファイルを事前に作成しておく必要があります。

- 監視方法が上記以外の場合

  ディスクデバイスを監視するときの監視先デバイス名を指定します。[/] で始まる必要があります。

監視対象 RAW デバイス名 (1023 バイト以内)

監視方法に READ（RAW）を選択した場合のみ入力可能となります。

- 監視方法が READ(RAW) の場合

  raw アクセスするためのデバイス名を入力します。既にサーバプロパティの [ディスク I/F 一覧] に登録されている RAW デバイスは登録できません。

I/O サイズ (1～99999999)

監視処理で行う read または read/write のサイズを指定します。

- READ(RAW), READ(O_DIRECT) を指定した場合、I/O サイズの入力項目はグレーアウトされます
  対象のデバイスから 1 セクタ分の read を行います。
- TUR, TUR (generic), TUR (legacy) を指定した場合、本設定項目は無視されます。

ディスクフル検出時動作

ディスクフル (監視するディスクに空き容量がない状態) 検出時の動作を下記より選択します。

- 回復動作を実行する

  ディスクモニタリソースはディスクフル検出時に異常として扱います。

- 回復動作を実行しない

ディスクモニタリソースはディスクフル検出時に警告として扱います。

- READ, READ (RAW), READ (O_DIRECT), TUR, TUR (generic),
- TUR (legacy) を指定した場合、ディスクフル検出時動作の項目はグレーアウトされます

監視デバイス名にローカルディスクを設定すると、サーバのローカルディスク監視を行うことができます。

- ローカルディスク [/dev/sdb] を [READ 方式] で監視し、異常検出時に [OS 再起動] を行う設定例

設定項目	設定値	備考
監視デバイス名	/dev/sdb	2 台目の SCSI ディスク
監視方法	READ	READ 方式
回復対象	サーバ	-
最終動作	サービス停止と OS 再起動	OS 再起動

- ローカルディスク [/dev/sdb] を [TUR(generic) 方式] で監視し、異常検出時に [何もしない] (Cluster WebUI へアラートの表示のみを行う) 場合の設定例

設定項目	設定値	備考
監視デバイス名	/dev/sdb	2 台目の SCSI ディスク
監視方法	TUR(generic)	SG_IO 方式
最終動作	何もしない	

6.3.2 ディスクモニタリソースによる監視方法

ディスクモニタリソースの監視方法は大きく分けて TUR と READ があります。

- TUR の注意事項
  - SCSI の Test Unit Ready コマンドや SG_IO コマンドをサポートしていないディスク、ディスクインタフェース (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。
  - LVM 論理ボリューム (LV) のデバイスでは ioctl が正常に実行できない可能性があるため、LV の監視には READ を使用してください。
  - IDE インターフェイスのディスクの場合には、すべての TUR 方式は使用できません。
  - S-ATA インターフェイスのディスクの場合には、ディスクコントローラのタイプや使用するディストリビューションにより、OS に IDE インターフェイスのディスク (hd) として認識される場合と SCSI イ

ンターフェイスのディスク (sd) として認識される場合があります。IDE インターフェイスとして認識される場合には、すべての TUR 方式は使用できません。SCSI インターフェイスとして認識される場合には、TUR(legacy) が使用できます。TUR(generic) は使用できません。

- 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。
- ディスク上のパーティションを監視対象に設定して使用することはできません。whole device (ディスク全体を示すデバイス) を指定する必要があります。
- ディスク装置によっては TUR 発行時、装置の状態によって一時的に Unit Attention を返す場合があります。

  Unit Attention が一時的に返却されることは問題ではありませんが、TUR のリトライ回数を 0 回に設定している場合、上記をエラーと判断し、ディスクモニタリソースが異常となります。

  無用な異常検出を防ぐため、リトライ回数は 1 回以上を設定してください。

TUR の監視方法は、下記の 3 つが選択可能です。

- TUR
  - 指定されたデバイスへ以下の手順で ioctl を発行して、その結果で判断します。ioctl(SG_GET_VERSION_NUM) コマンドを実行します。この ioctl の戻り値と SG ドライバの version を見て判断します。
  - ioctl コマンド成功かつ SG ドライバの version が 3. 0 以上なら SG ドライバを使用した ioctl TUR(SG_IO) を実行します。
  - ioctl コマンド失敗または SG ドライバの version が 3.0 未満なら SCSI コマンドとして定義されている ioctl TUR を実行します。
- TUR(legacy)
  - ioctl(Test Unit Ready) を使って監視を行います。指定されたデバイスへ SCSI コマンドとして定義されている Test Unit Ready(TUR) コマンドを発行してその結果で判断します。
- TUR(generic)
  - ioctl TUR(SG_IO) を使って監視を行います。指定されたデバイスへ SCSI コマンドとして定義されている ioctl(SG_IO) コマンドを発行してその結果で判断します。SG_IO は SCSI ディスクであっても OS やディストリビューションによって動作しないことがあります。

READ の監視方法は、下記のとおりです。

- READ
  - 指定されたデバイス (ディスクデバイスまたはパーティションデバイス) もしくはファイル上の指定されたサイズを read してその結果 (read できたサイズ) で判断します。

  - 指定されたサイズが read できたことを判断します。read したデータの正当性は判断しません。
  - read するサイズを大きくすると OS やディスクへの負荷が大きくなります。
  - read するサイズについては「 6.3.3. ディスクモニタリソースで *READ* を選択した場合の *I/O* サイズ 」を留意して設定してください。

READ(O_DIRECT) の監視方法は、下記のとおりです。

- READ (O_DIRECT)
  - 指定されたデバイス (ディスクデバイスまたはパーティションデバイス) 上の 1 セクタ分もしくはファイルを、キャッシュを使用しない (O_DIRECT モード) で read してその結果 (read できたサイズ) で判断します。
  - read できたことを判断します。read したデータの正当性は判断しません。

READ (RAW) の監視方法は、下記のとおりです。

- READ (RAW)
  - 監視方法「READ(O_DIRECT)」と同様に OS のキャッシュを使用しないで指定されたデバイスの read の監視を行います。
  - read できたことを判断します。read したデータの正当性は判断しません。
  - 監視方法「READ(RAW)」を設定する場合、既に mount しているパーティションまたは mount する可能性のあるパーティションの監視はできません。また、既に mount しているパーティションまたは mount する可能性のあるパーティションの whole device(ディスク全体を示すデバイス) を監視することもできません。監視専用のパーティションを用意してディスクモニタリソースに設定してください。(監視用のパーティションサイズは、10MB 以上を割り当ててください)

WRITE (FILE) の監視方法は、下記のとおりです。

- WRITE (FILE)
  - 指定されたパス名のファイルを作成、書き込み、削除を行い判断します。
  - 書き込んだデータの正当性は判断しません。

6.3.3 ディスクモニタリソースで READ を選択した場合の I/O サイズ

監視方法で READ を選択した場合の read を行うサイズを指定します。

使用するディスクやインターフェイスにより、様々な read 用のキャッシュが実装されている場合があります。そのため I/O サイズが小さい場合にはキャッシュにヒットしてしまい read のエラーを検出できない場合があります。

READ の I/O のサイズはディスクの障害を発生させて障害の検出ができることを確認して指定してください。

以下の図は 2 台のサーバとそれに接続された共有ディスクの例です。
まず、サーバの（SCSI、Fibre Channel などの）インターフェイスアダプタ（図の HBA）にキャッシュがあります。
Shared disk には RAID サブシステム上のキャッシュがあります。
また、アレイディスク内部の各ディスクドライブ上にもキャッシュがあります。

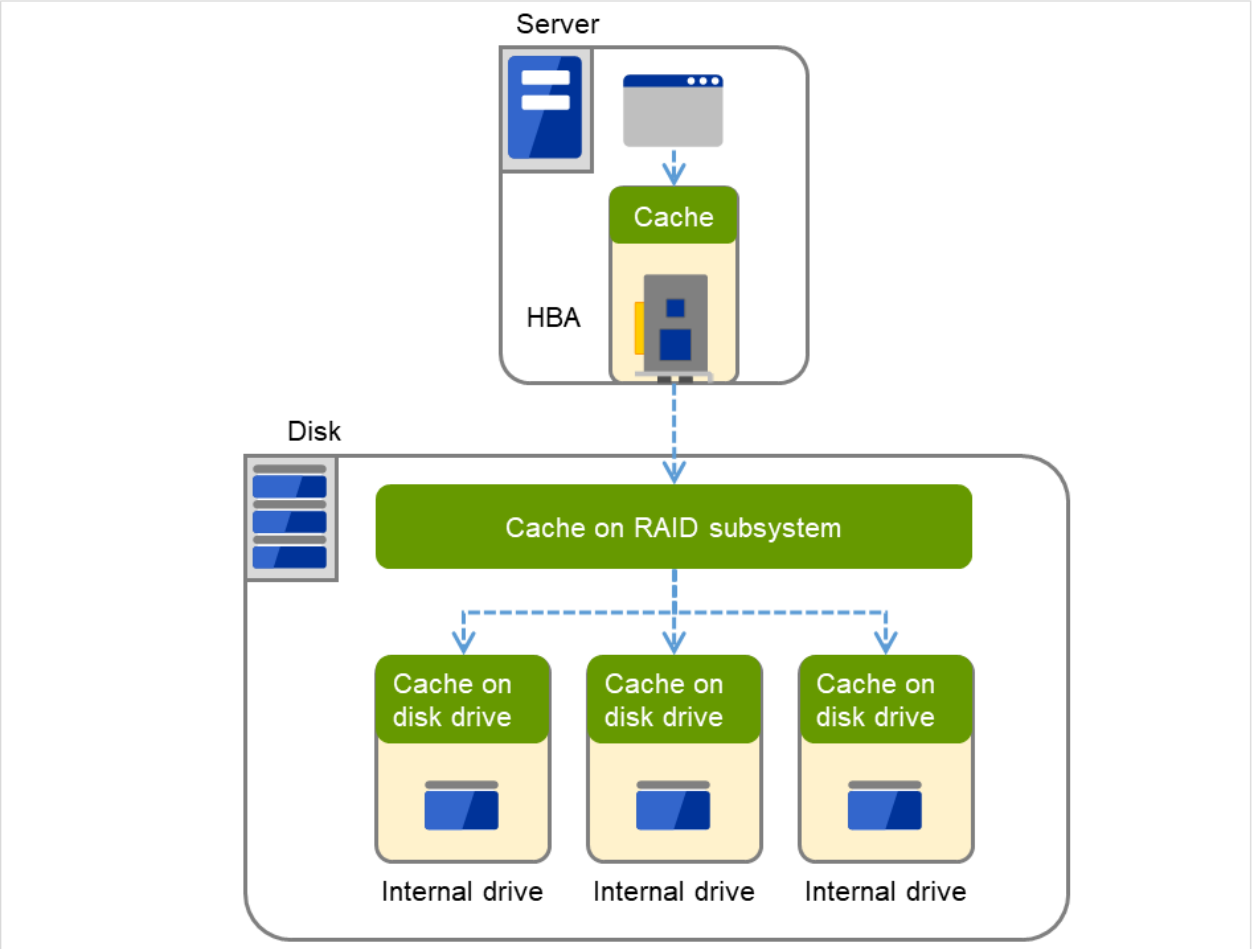


図 6.2　様々なキャッシュ

6.4 ディスクモニタリソースで READ(RAW) を選択した場合の設定例

ディスクモニタの設定例

- Disk モニタリソース (内蔵 HDD を「READ(RAW)」で監視)
- Disk モニタリソース (共有ディスクを「READ(RAW)」で監視)

図はサーバとそれに接続されたディスクの例を表しています。Server 1 の内蔵ディスクにおいて、/dev/sda3 を Disk モニタに指定しています。

注釈:

OS で使用しているパーティションは指定しないでください（swap も含む）。

既に mount しているパーティション、mount する可能性のあるパーティション、whole device も指定しないでください。

Disk モニタリソース専用のパーティションを確保してください。

また外部接続ディスク（Disk）において、/dev/sdb3 を Disk モニタに指定しています。

注釈:

既に mount しているパーティション、または mount する可能性のあるパーティションは指定しないでください。

また、既に mount しているパーティション、または mount する可能性のあるパーティションの whole device も指定しないでください。

Disk モニタリソース専用のパーティションを確保してください。

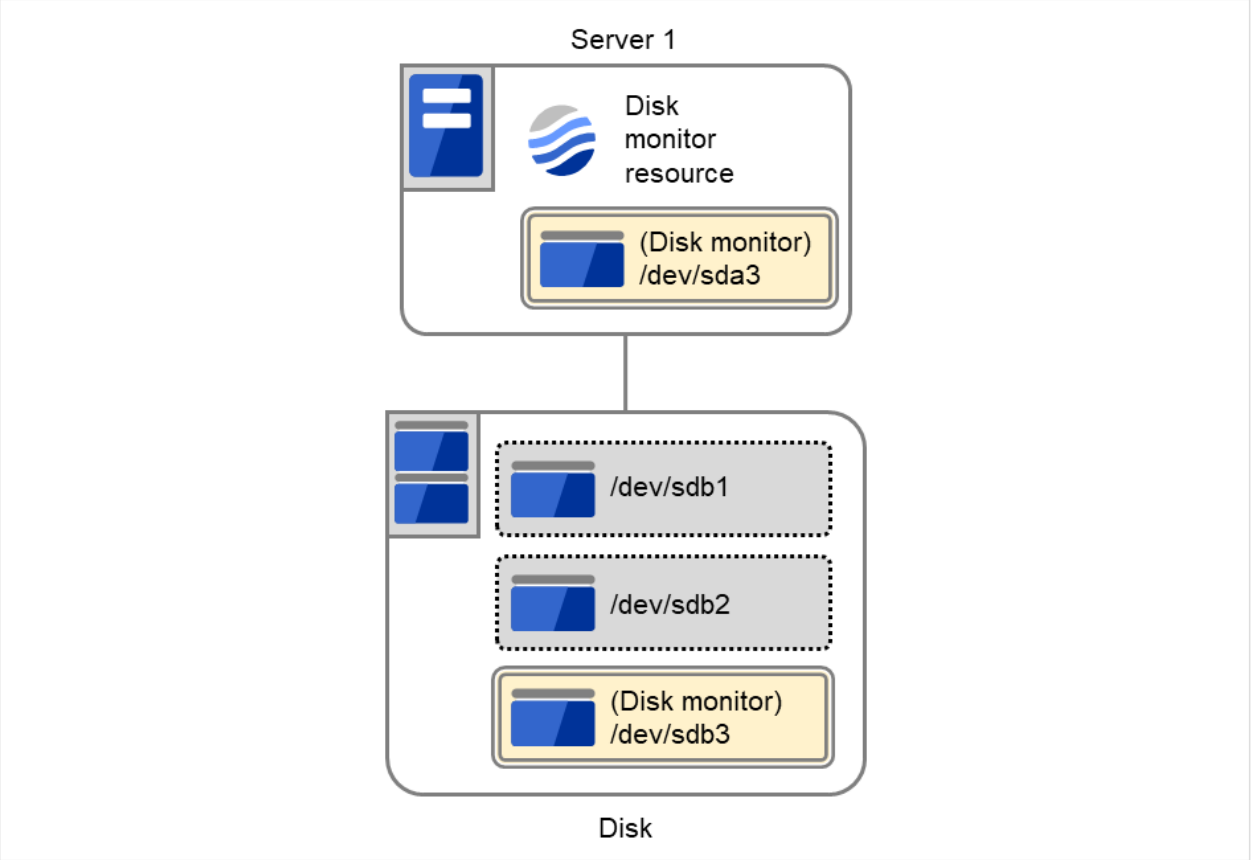


図 6.3　ディスクモニタの設定例

6.5 IP モニタリソースの設定

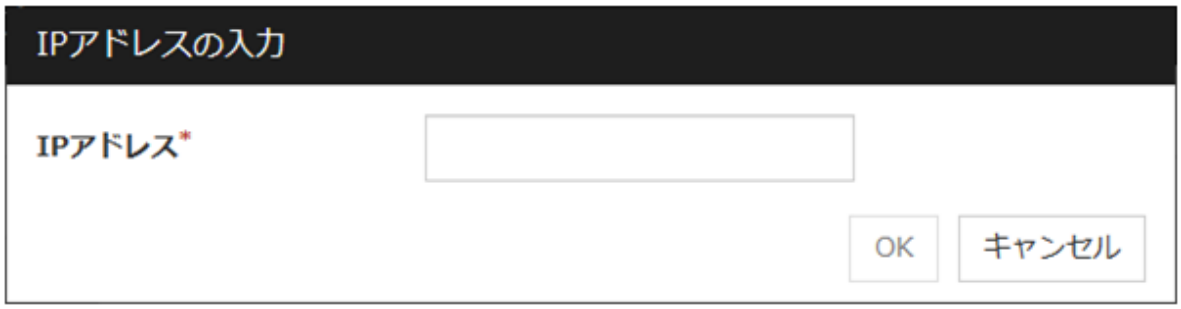
IP モニタリソースとは、ping コマンドを使用して、IP アドレスの監視を行うモニタリソースです。

6.5.1 監視 (固有) タブ

[IP アドレス一覧] には監視する IP アドレスの一覧が表示されます。

追加

監視する IP アドレスを追加します。IP アドレスの入力ダイアログボックスが表示されます。



IP アドレス (255 バイト以内)

監視を行う IP アドレスまたはホスト名を入力して [OK] を選択してください。パブリック LAN に存在する実 IP アドレスまたはホスト名を入力してください。ホスト名を設定する場合は、OS 側に名前解決の設定 (/etc/hosts へのエントリの追加など) をしてください。

削除

[IP アドレス一覧] で選択している IP アドレスを監視対象から削除します。

編集

IP アドレスの入力ダイアログボックスが表示されます。[IP アドレス一覧] で選択している IP アドレスが表示されるので、編集して [OK] を選択します。

6.5.2 IP モニタリソースの監視方法

指定した IP アドレスを ping コマンドで監視します。指定した IP アドレスすべての応答がない場合に異常と判断します。

IP アドレスの応答確認には ICMP の packet type 0 (Echo Reply) と 8 (Echo Request) が使用されます。

- 複数の IP アドレスについてすべての IP アドレスが異常時に異常と判断したい場合、1 つの IP モニタリソースにすべての IP アドレスを登録してください。

  以下の図は 1 つの IP モニタリソースに全ての IP アドレスを登録した場合の例です。指定した IP アドレスが一つでも正常な場合、IP monitor 1 は正常と判断します。

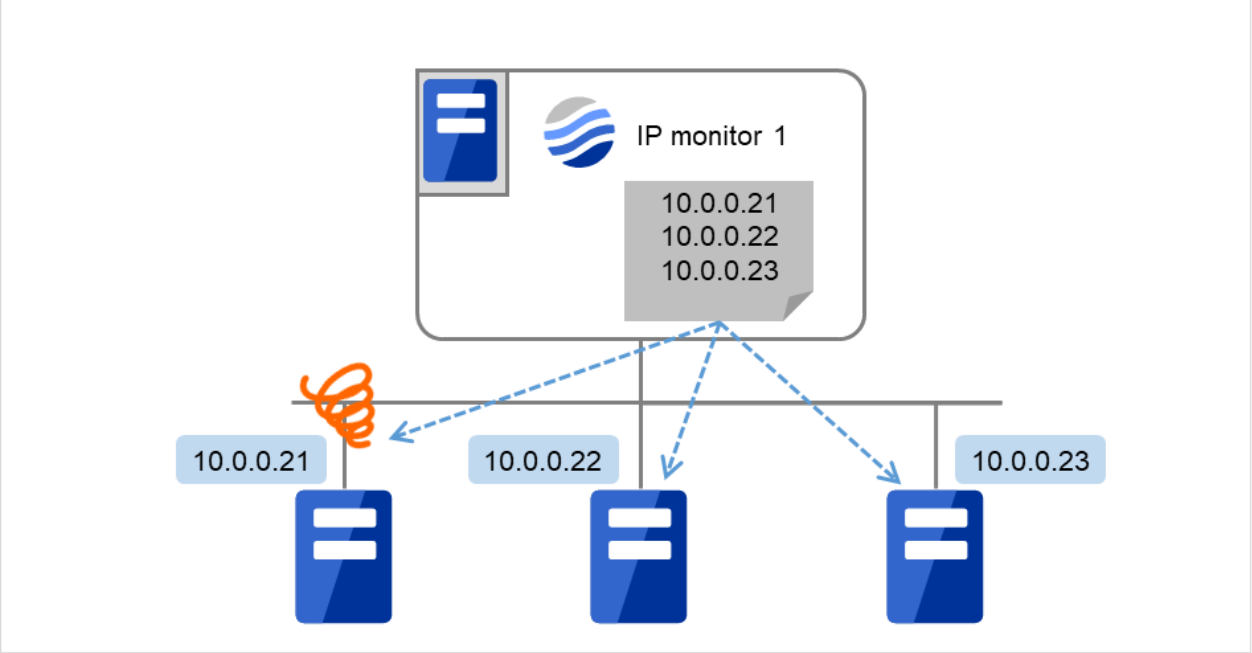


図 6.4　1 つの IP モニタリソースに全ての IP アドレスを登録（正常）

以下の図は 1 つの IP モニタリソースに全ての IP アドレスを登録した場合の例です。指定した IP アドレスが全て異常な場合、IP monitor 1 は異常と判断します。

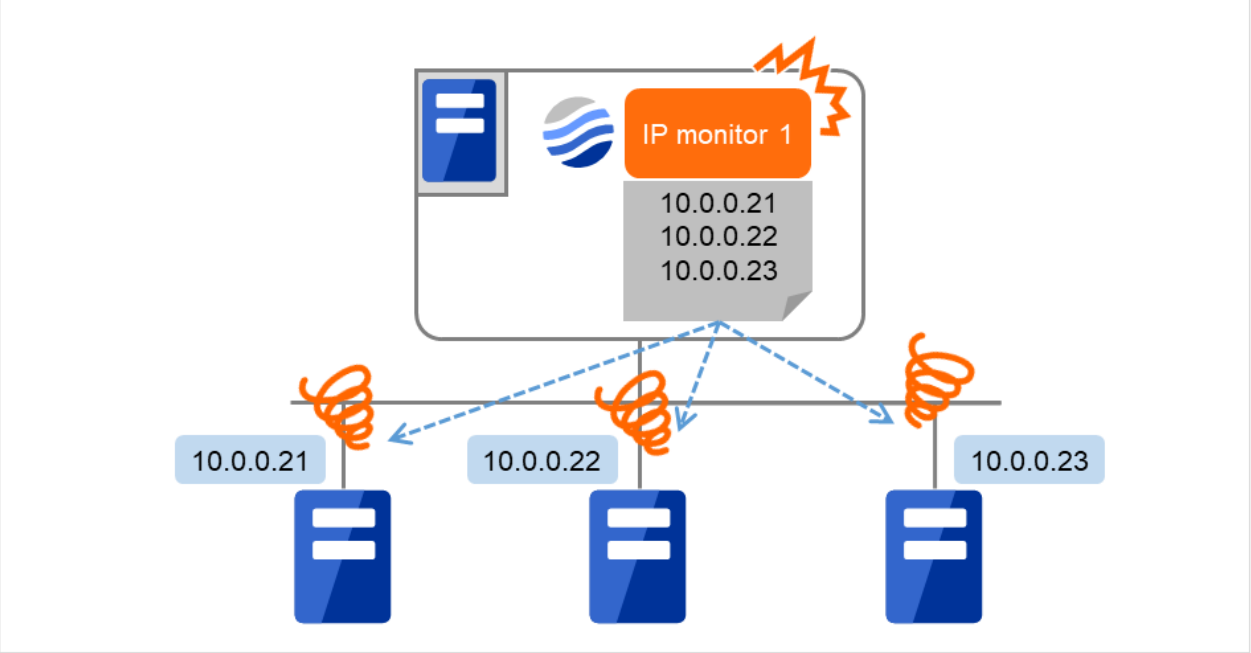


図 6.5　1 つの IP モニタリソースに全ての IP アドレスを登録（異常検出）

- 複数の IP アドレスについてどれか 1 つが異常時に異常と判断したい場合、個々の IP アドレスについて 1 つずつの IP モニタリソースを作成してください。

  図は各 IP モニタリソースに IP アドレスを一つずつ登録した場合の例です。指定した IP アドレスの異常を検出した場合、IP モニタ（図では IP monitor 1）は異常と判断します。

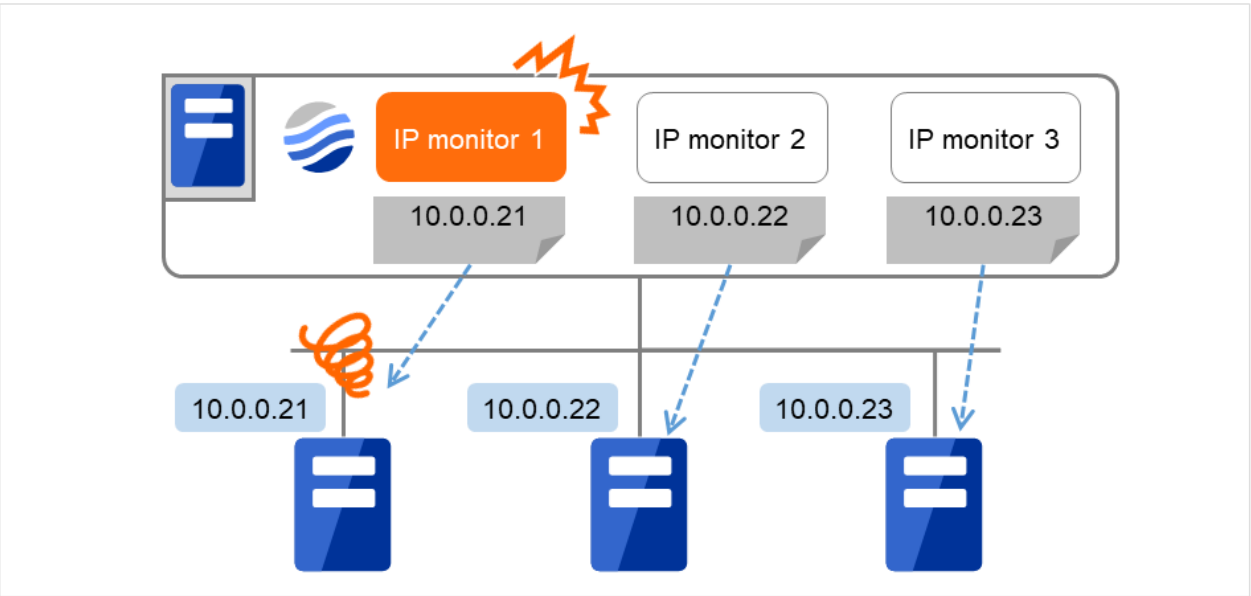


図 6.6　各 IP モニタリソースに IP アドレスを一つずつ登録（異常検出）

6.6 NIC Link Up/Down モニタリソースの設定

NIC Link Up/Down モニタリソースは、指定した NIC の Link 状態を取得し、Link の Up/Down を監視します。

6.6.1 監視 (固有) タブ

監視対象 (15 バイト以内)

監視を行う NIC のインターフェイス名を設定してください。ボンドデバイス (例：bond.600)、およびチームデバイス (例：team0) 共に監視可能です。VLAN, tagVLAN の監視も可能です (設定例:eth0.8)。

6.6.2 NIC Link UP/Down モニタリソースの動作環境

NIC Link UP/Down モニタリソースをサポートするネットワークインターフェイス

NIC Link UP/Down モニタリソースは、以下のネットワークインターフェイスで動作確認しています。

Ethernet Controller(Chip)	Bus	Driver version
Intel 82557/8/9	PCI	3.5.10-k2-NAPI
Intel 82546EB	PCI	7.2.9
Intel 82546GB	PCI	7.3.20-k2-NAPI 7.2.9
Intel 82573L	PCI	7.3.20-k2-NAPI
Intel 80003ES2LAN	PCI	7.3.20-k2-NAPI
Broadcom BCM5721	PCI	7.3.20-k2-NAPI

6.6.3 NIC Link UP/Down モニタリソースの注意事項

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。NIC Link Up/Down モニタリソースの動作可否は、各ディストリビュータが提供する ethtool コマンドで確認することができます。

```
ethtool eth0
Settings for eth0:
Supported ports: [ TP ]
Supported link modes: 10baseT/Half 10baseT/Full
100baseT/Half 100baseT/Full
1000baseT/Full
Supports auto-negotiation: Yes
Advertised link modes: 10baseT/Half 10baseT/Full
100baseT/Half 100baseT/Full
1000baseT/Full
Advertised auto-negotiation: Yes
Speed: 1000Mb/s
Duplex: Full
Port: Twisted Pair
PHYAD: 0
Transceiver: internal
Auto-negotiation: on
Supports Wake-on: umbg
Wake-on: g
Current message level: 0x00000007 (7)
Link detected: yes
```

- ethtool コマンドの結果で LAN ケーブルのリンク状況 ("Link detected: yes") が表示されない場合
  - CLUSTERPRO の NIC Link Up/Down モニタリソースが動作不可能な可能性が高いです。IP モニタリソースで代替してください。
- ethtool コマンドの結果で LAN ケーブルのリンク状況 ("Link detected: yes") が表示される場合
  - 多くの場合 CLUSTERPRO の NIC Link Up/Down モニタリソースが動作可能ですが、希に動作不可能な場合があります。
  - 特に以下のようなハードウェアでは動作不可能な場合があります。IP モニタリソースで代替してください。
  - ブレードサーバのように実際の LAN のコネクタと NIC のチップとの間にハードウェアが実装されてい

る場合

- 監視対象の NIC が Bonding 環境の場合、MII Polling Interval の設定値が 0 以上に設定されているか確認してください。

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. サーバ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。

6.6.4 NIC Link UP/Down 監視の構成および範囲

NIC Link Up/Down 監視が検知した異常には複数の要因が考えられます。サーバとネットワーク機器を LAN ケーブルで接続している時に異常が発生したのであれば、サーバ側のケーブルが抜けている可能性があります。また、その場合、ネットワーク機器側のケーブルが抜けている可能性もあります。さらに、ネットワーク機器の電源断の可能性も考えられます。

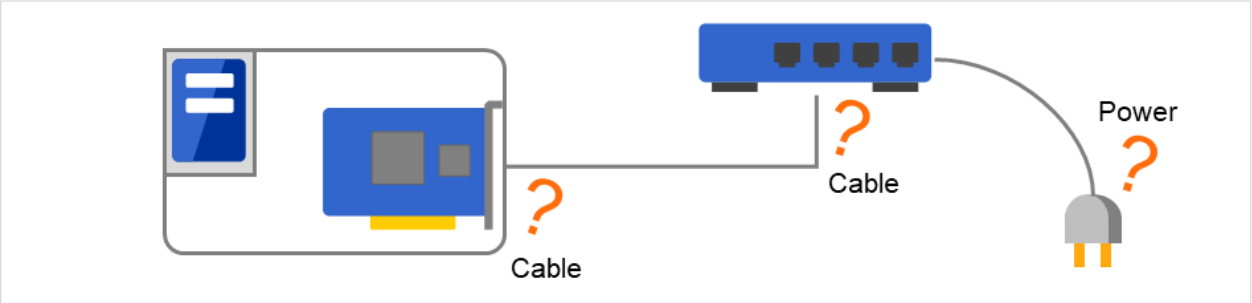


図 6.7　NIC Link Up/Down 監視と異常発生要因

- NIC のドライバへの ioctl( ) によりネットワーク (ケーブル) のリンク確立状態を検出します。
  (IP モニタの場合は、指定された IP アドレスへの ping の反応で判断をします。)
- 他サーバと LAN ケーブルで直結している NIC を監視する場合には、他サーバダウン時に (リンクが確立しないため) 異常を検出します。

また、ネットワークを bonding 化している場合には、bonding による可用性を活かしたまま下位のスレーブインターフェイス (eth0, eth1...) だけでなくマスタインターフェイス (bond0...) も監視することが可能です。その場合には、下記の設定を推奨します。

- スレーブインターフェイス
  - 異常検出時の回復動作：何もしない

    片方のネットワークケーブルのみ (eth0) の異常時には CLUSTERPRO は回復動作を実行せず、アラートのみ出力します。

    ネットワークの回復動作は、bonding が行います。
- マスタインターフェイス
  - 異常検出時の回復動作：シャットダウンなどを設定する

    全てのスレーブインターフェイスの異常時 (マスタインターフェイスがダウン状態) に CLUSTERPRO は、回復動作を実行します。

以下の図は、スレーブインターフェイス eth0、eth1 を bonding 化し、マスタインターフェイス bond0 とした場合を表しています。

eth0 の障害発生時には、bonding ドライバが縮退または切替を行います。

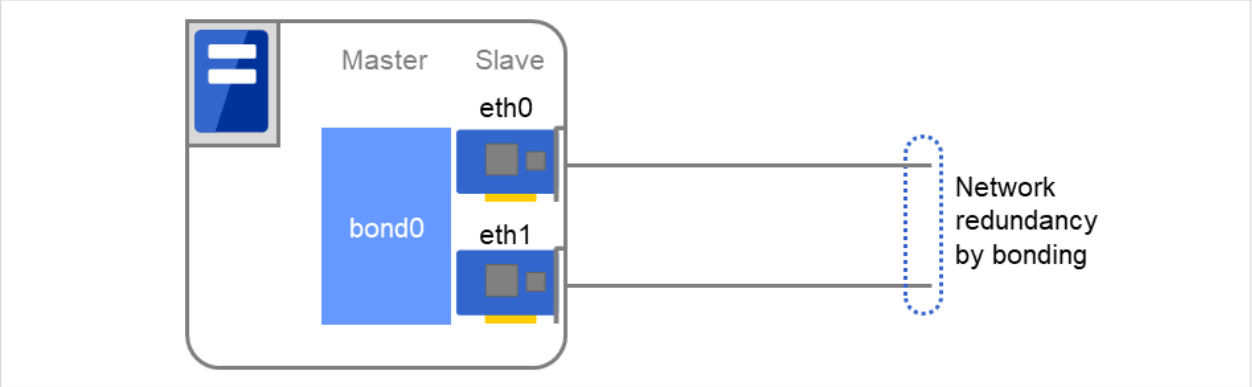


図 6.8　Network bonding の使用例

6.7 PID モニタリソースの設定

活性に成功した EXEC リソースを監視します。プロセス ID の有無を監視することによってプロセス ID の消滅時に異常と判断します。

監視を行う EXEC リソースは「 6.2. モニタリソースのプロパティ 」の [対象リソース] で設定します。EXEC リソースの起動時の設定が [非同期] の場合のみ監視できます。プロセスのストールを検出することは出来ません。

注釈: データベース、samba、apache、sendmail などのストール監視を行うには「CLUSTERPRO 監視オプション」を購入してください。

6.7.1 PID モニタリソースの注意事項

活性に成功した EXEC リソースを監視します。EXEC リソースの開始スクリプトの起動時の設定が [非同期] の場合のみ監視できます。

6.8 ユーザ空間モニタリソースの設定

ユーザ空間モニタリソースは、ユーザ空間のストールを異常として判断します。

本リソースは自動的に登録されます。監視方法は softdog のユーザ空間モニタリソースが自動登録されます。

6.8.1 監視 (固有) タブ

ハートビートのインターバル/タイムアウトを使用する

監視のインターバルとタイムアウトを、ハートビートのインターバルとタイムアウトを使用するかどうかを設定します。

- チェックボックスがオン

  ハートビートのインターバルとタイムアウトを使用します。

- チェックボックスがオフ

  ハートビートの設定は使用せず、監視タブで設定するインターバルとタイムアウトを使用します。タイムアウトはインターバルより大きい値を設定する必要があります。[監視方法] に ipmi を設定している場合、タイムアウトを 255 以下に設定する必要があります。

監視方法

ユーザ空間モニタリソースの監視方法を以下の中から選択します。既に他のユーザ空間モニタリソースで使用している監視方法は選択できません。

- softdog

softdog ドライバを使用します。

- ipmi

  OpenIPMI を使用します。

- keepalive

  clpkhb ドライバ、clpka ドライバを使用します。

- none

  何も使用しません。

タイムアウト発生時動作

最終動作を設定します。

- RESET

  サーバをリセットします。

- PANIC

  サーバをパニックさせます。監視方法が keepalive の場合にのみ設定可能です。

- NMI

  サーバへ NMI を発生させます。監視方法が ipmi の場合にのみ設定可能です。

ダミーファイルのオープンクローズ

監視を行う際、インターバルごとにダミーファイルのオープン/クローズを行うかどうかを設定します。

- チェックボックスがオン

  ダミーファイルのオープン/クローズを行います。

- チェックボックスがオフ

  ダミーファイルのオープン/クローズを行いません。

書き込みを行う

ダミーファイルのオープン/クローズを行う場合に、ダミーファイルに書き込みを行うかどうかを設定します。

- チェックボックスがオン

  ダミーファイルの書き込みを行います。

- チェックボックスがオフ

  ダミーファイルの書き込みを行いません。

サイズ (1～9999999)

ダミーファイルに書き込みを行う場合に書き込むサイズを設定します。

ダミースレッドの作成

監視を行う際にダミースレッドの作成を行うかどうかを設定します。

- チェックボックスがオン
  ダミースレッドの作成を行います。
- チェックボックスがオフ
  ダミースレッドの作成を行いません。

6.8.2 ユーザ空間モニタリソースが依存するドライバ

監視方式 softdog

softdog

- 監視方法が softdog の場合、このドライバが必要です。
- ローダブルモジュール構成にしてください。スタティックドライバでは動作しません。
- softdog ドライバが使用できない場合、監視を開始することはできません。

監視方式 keepalive

clpka clpkhb

- 監視方法が keepalive の場合、CLUSTERPRO の clpkhb ドライバ、clpka ドライバが必要です。
- clpka ドライバと clpkhb ドライバは CLUSTERPRO が提供するドライバです。サポート範囲については『インストールガイド』の「CLUSTERPRO X SingleServerSafe について」 - 「CLUSTERPRO X SingleServerSafe の動作環境を確認する」 - 「動作可能なディストリビューションと kernel」を参照してください。
- clpkhb ドライバ、clpka ドライバが使用できない場合、監視を開始することはできません。

6.8.3 ユーザ空間モニタリソースが依存する rpm

監視方式 ipmi

OpenIPMI

- 監視方法が ipmi の場合、この rpm をインストールしておく必要があります。
- この rpm がインストールされていない場合、監視を開始することはできません。

6.8.4 ユーザ空間モニタリソースの監視方法

ユーザ空間モニタリソースの監視方法は以下のとおりです。

監視方法 softdog

監視方法が softdog の場合、OS の softdog ドライバを使用します。

監視方法 ipmi

監視方法が ipmi の場合、OpenIPMI を使用します。

OpenIPMI がインストールされていない場合、インストールする必要があります。

監視方法 keepalive

監視方法が keepalive の場合、clpkhb ドライバと clpka ドライバを使用します。

注釈:

clpkhb ドライバ, clpka ドライバが動作するディストリビューション、kernel バージョンについては必ず『インストールガイド』の「CLUSTERPRO X SingleServerSafe について」の「動作可能なディストリビューションと kernel」で確認してください。

ディストリビュータがリリースするセキュリティパッチを既に運用中のサーバへ適用する場合 (kernel バージョンが変わる場合) にも確認してください。

監視方法 none

監視方法 none は、評価用の設定です。ユーザ空間モニタリソースの拡張設定の動作だけを実行します。本番環境では設定しないでください。

6.8.5 ユーザ空間モニタリソースの拡張設定

ユーザ空間モニタリソースを拡張させる設定として、ダミーファイルのオープン/クローズ、ダミーファイルへの書き込み、ダミースレッドの作成があります。各設定に失敗するとタイマの更新を行いません。設定したタイムアウト値またはハートビートタイムアウト時間内に各設定が失敗し続けると OS をリセットします。

ダミーファイルのオープン/クローズ

監視間隔ごとにダミーファイルの作成、ダミーファイルの open、ダミーファイルの close、ダミーファイルの削除を繰り返します。

- この拡張機能を設定している場合、ディスクの空き容量がなくなるとダミーファイルの open に失敗してタイマの更新が行われず、OS をリセットします。

ダミーファイルへの書き込み

監視間隔毎にダミーファイルに設定したサイズを書き込みます。

- この拡張機能は、ダミーファイルのオープン / クローズが設定されていないと設定できません。

ダミースレッドの作成

監視間隔ごとにダミースレッドを作成します。

6.8.6 ユーザ空間モニタリソースのロジック

監視方法の違いによる処理内容、特徴は以下の通りです。シャットダウン監視では各処理概要のうち 1 のみの挙動になります。

監視方法 ipmi

- 処理概要

  以下の 2〜7 の処理を繰り返します。

  1. IPMI タイマセット
  2. ダミーファイルの open()
  3. ダミーファイル write()
  4. ダミーファイル fdatasync()
  5. ダミーファイルの close()
  6. ダミースレッド作成
  7. IPMI タイマ更新

  処理概要 2〜6 は監視の拡張設定の処理です。各設定を行っていないと処理を行いません。

  - タイムアウトしない (上記 2〜7 が問題なく処理される) 場合の挙動
    リセットなどのリカバリ処理は実行されません
  - タイムアウトした (上記 2〜7 のいずれかが停止または遅延した) 場合の挙動
    BMC(サーバ本体のマネージメント機能) によりリセットを発生させます
  - メリット
    * BMC(サーバ本体のマネージメント機能) を使用するため kernel 空間の障害を受けにくく、リセットができる確率が高くなります。
  - デメリット
    * H/W に依存しているため IPMI をサポートしていないサーバ、OpenIPMI が動作しないサーバでは使用できません。

* ESMPRO/ServerAgent を使用しているサーバでは使用できません。
* その他サーバベンダが提供するサーバ監視ソフトウェアと共存できない可能性があります。

監視方法 softdog

- 処理概要

  以下の 2〜7 の処理を繰り返します。

  1. softdog セット
  2. ダミーファイルの open()
  3. ダミーファイル write()
  4. ダミーファイル fdatasync()
  5. ダミーファイルの close()
  6. ダミースレッド作成
  7. softdog タイマ更新

  処理概要 2〜6 は監視の拡張設定の処理です。各設定を行っていないと処理を行いません。

  - タイムアウトしない (上記 2〜7 が問題なく処理される) 場合の挙動
    リセットなどのリカバリ処理は実行されません
  - タイムアウトした (上記 2〜7 のいずれかが停止または遅延した) 場合の挙動
    softdog.ko によりリセットを発生させます
  - メリット
    * H/W に依存しないため softdog kernel モジュールがあれば使用できます。
      (一部のディストリビューションではデフォルトで softdog が用意されていないものもがありますので 設定する前に softdog の有無を確認してください)
  - デメリット
    * softdog が kerne l 空間のタイマロジックに依存しているため kernel 空間に障害が発生した場合にリセットされない場合があります。

監視方法 keepalive

- 処理概要

  以下の 2〜7 の処理を繰り返します。

  1. keepalive タイマセット
  2. ダミーファイルの open()

3. ダミーファイル write()
4. ダミーファイル fdatasync()
5. ダミーファイルの close()
6. ダミースレッド作成
7. keepalive タイマ更新

処理概要 2〜6 は監視の拡張設定の処理です。各設定を行っていないと処理を行いません。

- タイムアウトしない (上記 2〜7 が問題なく処理される) 場合の挙動
  リセットなどのリカバリ処理は実行されません
- タイムアウトした (上記 2〜7 のいずれかが停止または遅延した) 場合の挙動
- アクションの設定にしたがって、clpka.ko によりリセットまたはパニックを発生させます
  - メリット
    - アクションとしてパニックが設定できます。
  - デメリット
    - 動作できる (ドライバを提供している) ディストリビューション、アーキテクチャ、カーネルバージョンが制限されます。
    - clpka が kernel 空間のタイマロジックに依存しているため kernel 空間に障害が発生した場合にリセットされない場合があります。

6.8.7 ipmi 動作可否の確認方法

サーバ本体の OpenIPMI の対応状況を確認する方法は、以下の手順で簡易確認することができます。

1. OpenIPMI の rpm パッケージをインストールする。
2. /usr/bin/ipmitool を実行する。
3. 実行結果を確認する。

以下のように表示される場合 (/usr/bin/ipmitool bmc watchdog get の実行結果)

(以下は表示例です。H/W により表示される値が異なる場合があります。)

```
Watchdog Timer Use: SMS/OS (0x04)
Watchdog Timer Is: Stopped
Watchdog Timer Actions: No action (0x00)
```

(次のページに続く)

(前のページからの続き)

```
Pre-timeout interval: 0 seconds
Timer Expiration Flags: 0x00
Initial Countdown: 300 sec
Present Countdown: 0 sec
```

OpenIPMI は使用できます。監視方法に ipmi を選択することが可能です。

6.8.8 ユーザ空間モニタリソースの注意事項

全監視方法での共通の注意事項

- Cluster WebUI で設定情報を作成すると監視方法 softdog のユーザ空間モニタリソースが自動で作成されます。
- 監視方法の異なるユーザ空間モニタリソースを追加することができます。自動的に作成された監視方法 softdog のユーザ空間モニタリソースは削除することもできます。
- OS の softdog ドライバが存在しない、または CLUSTERPRO の clpkhb ドライバ、clpka ドライバが存在しない、OpenIPMI の rpm がインストールされていないなどの理由によりユーザ空間モニタリソースの活性に失敗した場合、Cluster WebUI のアラートログに "Monitor userw failed." というメッセージが表示されます。Cluster WebUI、clpstat コマンドでの表示ではリソースステータスは [正常] が表示され、サーバのステータスは [停止済] が表示されます。

ipmi による監視の注意事項

- ipmi に関する注意事項は『インストールガイド』の「注意制限事項」-「OS インストール後、CLUSTERPRO X SingleServerSafe インストール前」-「BMC (Baseboard Management Controller) による制御について」を参照してください。

注釈:

ESMPRO/ServerAgent などサーバベンダが提供するサーバ監視ソフトウェアを使用する場合には、監視方法に IPMI を選択しないでください。

これらのサーバ監視ソフトウェアと OpenIPMI は共にサーバ上の BMC(Baseboard Management Controller) をするため、競合が発生して正しく監視が行うことができなくなります。

6.9 カスタムモニタリソースの設定

カスタムモニタリソースは、任意のスクリプトを実行することによりシステムモニタを行うモニタリソースです。

6.9.1 監視 (固有) タブ

ユーザアプリケーション

スクリプトとしてサーバ上の実行可能ファイル (実行可能なシェルスクリプトファイルや実行ファイル) を使用します。各実行可能ファイル名は、サーバ上のローカルディスクの絶対パスで設定します。

各実行可能ファイルは、Cluster WebUI の構成情報には含まれません。Cluster WebUI で編集やアップロードはできませんので、サーバ上に準備する必要があります。

この製品で作成したスクリプト

スクリプトとして Cluster WebUI で準備したスクリプトファイルを使用します。必要に応じて Cluster WebUI でスクリプトファイルを編集できます。スクリプトファイルは、構成情報に含まれます。

ファイル (1023 バイト以内)

[ユーザアプリケーション] を選択した場合に、実行するスクリプト（実行可能なシェルスクリプトファイルや実行ファイル）を、サーバ上のローカルディスクの絶対パスで設定します。

表示

[この製品で作成したスクリプト] を選択した場合に、スクリプトファイルを表示します。

編集

[この製品で作成したスクリプト] を選択した場合に、スクリプトファイルを編集します。変更を反映するには [保存] をクリックしてください。スクリプトファイル名の変更はできません。

置換

[この製品で作成したスクリプト] を選択した場合に、スクリプトファイルの内容を、ファイル選択ダイアログ ボックスで選択したスクリプトファイルの内容に置換します。スクリプトが表示中または編集中の場合は置換できません。ここではスクリプトファイルを選択してください。バイナリファイル (アプリケーションなど) は選択しないでください。

監視タイプ

監視の方法を選択します。

- 同期 (既定値)

  定期的にスクリプトを実行し、そのエラーコードにより異常の有無を判断します。

- 非同期

  監視開始時にスクリプトを実行し、そのプロセスが消失した場合に異常と判断します。

アプリケーション/スクリプトの監視開始を一定時間待ち合わせる (0〜9999)

監視タイプが [非同期] の場合にアプリケーション/スクリプトを起動してから監視を開始するまでの待ち時間を設定します。この待ち時間は [監視 (共通)] タブで設定したタイムアウトの値より小さい値を設定する必要があります。

注釈: 本設定は次回モニタ起動時に有効になります。

既定値 ： 0

ログ出力先 (1023 バイト以内)

スクリプト内で出力するログの出力先を設定します。

[ローテートする] のチェックボックスがオフの場合は無制限に出力されますのでファイルシステムの空き容量に注意してください。

[ローテートする] のチェックボックスがオンの場合は、出力されるログファイルは、ローテートします。また、以下の注意事項があります。

[ログの出力先] には 1009 バイト以内でログのパスを記述してください。1010 バイトを超えた場合、ログの出力が行えません。

ログファイルの名前の長さは 31 バイト以内で記述してください。32 バイト以上の場合、ログの出力が行えません。

複数のカスタムモニタリソースでログローテートを行う場合、パス名が異なってもログファイルの名前が同じ場合、(ex. /home/foo01/log/genw.log, /home/foo02/log/genw.log) ローテートサイズが正しく反映されないことがあります。

ローテートする

スクリプトや実行可能ファイルの実行ログを、オフの場合は無制限のファイルサイズで、オンの場合はローテートして出力します。

ローテートサイズ (1〜999999999)

[ローテートする] チェックボックスがオンの場合に、ローテートするサイズを指定します。

ローテート出力されるログファイルの構成は、以下のとおりです。

ファイル名	内容
[ログ出力先] 指定のファイル名	最新のログです。
[ログ出力先] 指定のファイル名.pre	ローテートされた以前のログです。

正常な戻り値 (1023 バイト以内)

監視タイプが [同期] の場合にスクリプトのエラーコードがどのような値の場合に正常と判断するかを設定します。複数の値がある場合は、0,2,3 というようにカンマで区切るか、 0-3 のようにハイフンで値の範囲を指定します。

既定値 ： 0

警告戻り値 (1023 バイト以内)

監視タイプが [同期] の場合にスクリプトのエラーコードがどのような値の場合に警告と判断するかを設定します。複数の値がある場合は、0,2,3 というようにカンマで区切るか、 0-3 のようにハイフンで値の範囲を指定します。

[正常な戻り値] と [警告戻り値] に同じ値を設定した場合、正常と判断します。

クラスタ停止時に活性時監視の停止を待ち合わせる

クラスタ停止時にカスタムモニタリソースの停止を待ち合わせます。監視タイミングに [活性時] を設定している場合のみ有効となります。

6.9.2 カスタムモニタリソースの注意事項

監視タイプが [非同期] の場合、監視リトライ回数を 1 回以上に設定すると、正常に監視を 行うことができません。監視タイプを [非同期] に設定する場合は、監視リトライ回数を 0 回に設定してください。

スクリプトのログローテート機能を有効にした場合、ログ出力を仲介するプロセス (仲介プロセス) が生成されます。仲介プロセスは、「開始・停止スクリプト」および「開始・停止スクリプトから標準出力・標準エラー出力のいずれかまたは両方を継承した子孫プロセス」からのログ出力が全て停止 (ファイルディスクリプタがクローズ) するまで動作を継続します。子孫プロセスの出力をログから除外する場合は、スクリプトからのプロセス生成時に標準出力および標準エラー出力をリダイレクトしてください。

6.9.3 カスタムモニタリソースの監視方法

カスタムモニタリソースは、任意のスクリプトによりシステム監視を行います。

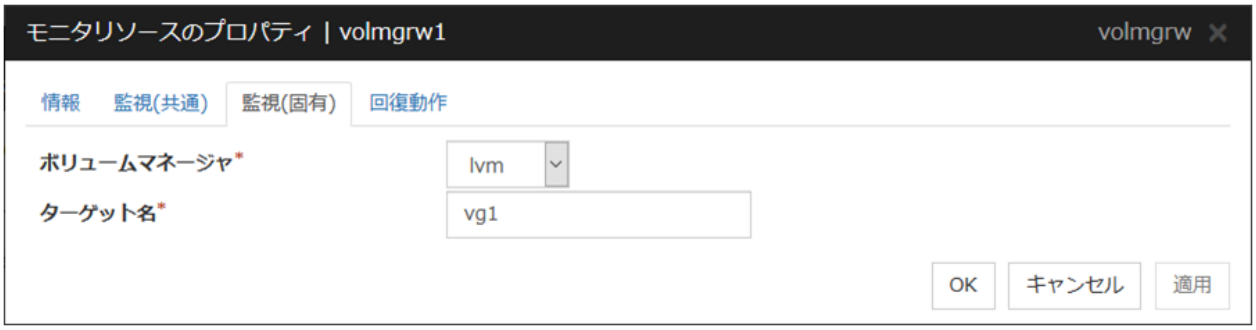
監視タイプが [同期] の場合、スクリプトを定期的に実行し、そのエラーコードにより異常の有無を判別します。

監視タイプが [非同期] の場合、スクリプトを監視開始時に実行し、このスクリプトのプロセスが消失した場合に異常と判断します。

6.10 ボリュームマネージャモニタリソースの設定

ボリュームマネージャモニタリソースは、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を行うモニタリソースです。

6.10.1 監視 (固有) タブ



ボリュームマネージャ

監視対象の論理ディスクを管理しているボリュームマネージャの種類を設定します。対応済みのボリュームマネージャは下記です。

- lvm (LVM ボリュームグループ)
- zfspool (ZFS ストレージプール)

ターゲット名 (1023 バイト以内)

監視対象の名前を設定します。ボリュームマネージャが [lvm] の場合、複数ボリュームをまとめて制御することができます。複数ボリュームを制御する場合は、ボリュームの名前を半角スペースで区切って設定します。

6.10.2 ボリュームマネージャモニタリソースの注意事項

ボリュームマネージャモニタリソースには既定値が設定されているため、必要があれば適切な値に変更してください。

6.10.3 ボリュームマネージャモニタリソースの監視方法

ボリュームマネージャモニタリソースは、監視する論理ディスクを管理するボリュームマネージャの種類によって監視方法が異なります。
対応済みのボリュームマネージャは下記です。

- lvm (LVM ボリュームグループ)
- zfspool (ZFS ストレージプール)

6.11 マルチターゲットモニタリソースの設定

マルチターゲットモニタリソースは、複数のモニタリソースの監視を行います。

6.11.1 監視 (固有) タブ

モニタリソースをグループ化して、そのグループの状態を監視します。[モニタリソース一覧] はモニタリソースを最大 64 個登録できます。

本リソースの [モニタリソース一覧] に唯一設定されているモニタリソースが削除された場合、本リソースは自動的に削除されます。

追加

選択しているモニタリソースを [モニタリソース一覧] に追加します。

削除

選択しているモニタリソースを [モニタリソース一覧] から削除します。

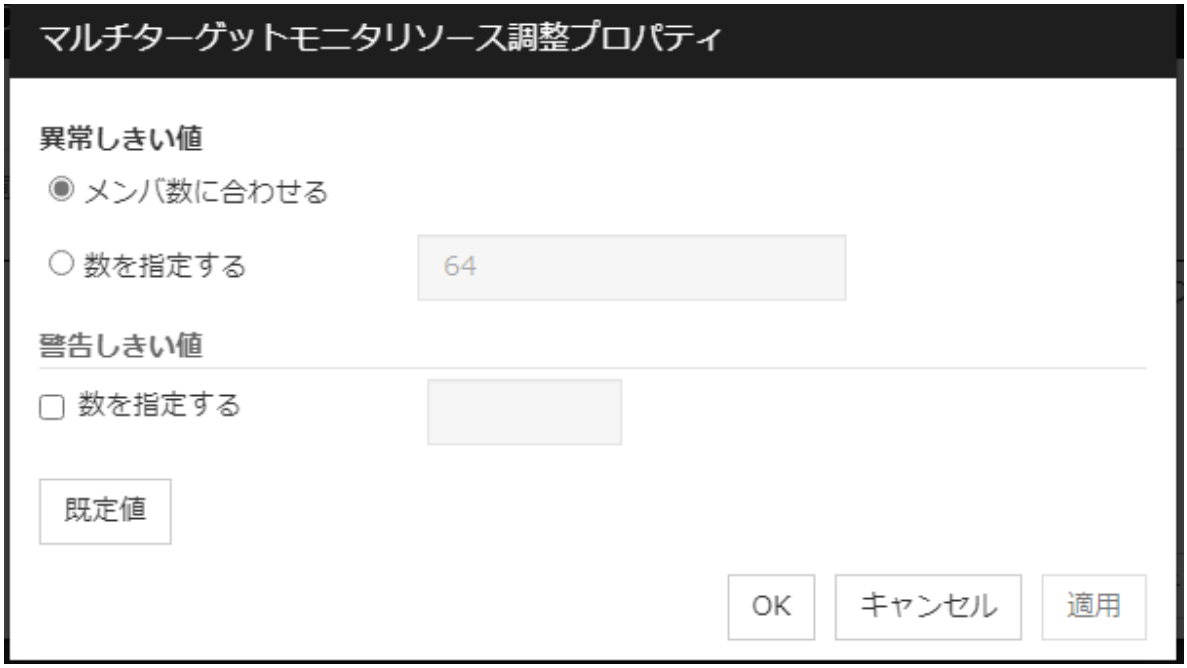
調整

[マルチターゲットモニタリソース調整プロパティ] ダイアログボックスを表示します。マルチターゲットモニタリソースの詳細設定を行います。

マルチターゲットモニタリソース調整プロパティ

パラメータタブ

パラメータに関する詳細設定が表示されます。



異常しきい値

マルチターゲットモニタが異常とする条件を選択します。

- メンバ数に合わせる

  マルチターゲットモニタの配下に指定したモニタリソースが全て異常となったとき、または異常と停止済が混在しているときにマルチターゲットモニタが異常になります。

  マルチターゲットモニタの配下に指定したモニタリソースの全てが停止済の場合には、正常になります。

- 数を指定する

  マルチターゲットモニタの配下に指定したモニタリソースのうち、異常しきい値に設定した数が異常または停止済となったときにマルチターゲットモニタが異常になります。

  マルチターゲットモニタの配下に指定したモニタリソースのうち、何個のモニタリソースが異常または停止済となったときにマルチターゲットモニタを異常とするかの個数を設定します。

  異常しきい値の選択が [数を指定する] のときに設定できます。

警告しきい値

- チェックボックスがオン

  マルチターゲットモニタの配下に指定したモニタリソースのうち、何個のモニタリソースが異常または停止済となったときにマルチターゲットモニタを警告とするかの個数を設定します。

- チェックボックスがオフ

  マルチターゲットモニタは警告のアラートを表示しません。

既定値

既定値に戻すときに使用します。[既定値] をクリックすると全ての項目に既定値が設定されます。

6.11.2 マルチターゲットモニタリソースの注意事項

- マルチターゲットモニタリソースは、登録されているモニタリソースのステータス 停止済み (offline) を異常として扱います。そのため、活性時監視のモニタリソースを登録した場合、モニタリソースが異常を検出していない状態でマルチターゲットモニタリソースが異常を検出してしまうことがあります。活性時監視のモニタリソースを登録しないでください。

6.11.3 マルチターゲットモニタリソースのステータス

マルチターゲットモニタリソースのステータスは登録されているモニタリソースのステータスによって判断します。
マルチターゲットモニタリソースが下記のように設定されている場合、

登録されているモニタリソース数 2
異常しきい値 2
警告しきい値 1

マルチターゲットモニタリソースのステータスは以下のようになります。

マルチターゲットモニタリソースステータス	モニタリソース 1 ステータス 正常 (normal)	モニタリソース 1 ステータス 異常 (error)	モニタリソース 1 ステータス 停止済 (offline)
モニタリソース 2 ステータス 正常 (normal)	正常 (normal)	警告 (caution)	警告 (caution)
モニタリソース 2 ステータス 異常 (error)	警告 (caution)	異常 (error)	異常 (error)
モニタリソース 2 ステータス 停止済 (offline)	警告 (caution)	異常 (error)	正常 (normal)

- マルチターゲットモニタリソースは、登録されているモニタリソースのステータスを監視しています。

  ステータスが異常 (error) であるモニタリソースの数が異常しきい値以上になった場合、マルチターゲットモニタリソースは異常 (error) を検出します。

  ステータスが異常 (error) であるモニタリソース数が警告しきい値を超えた場合、マルチターゲットモニタリソースの status は警告 (caution) となります。

  登録されている全てのモニタリソースのステータスが停止済み (offline) の場合、マルチターゲットモニタリソースのステータスは正常 (normal) となります。

  登録されている全てのモニタリソースのステータスが停止済み (offline) の場合を除いて、マルチターゲットモニタリソースは登録されているモニタリソースのステータス 停止済み (offline) を異常 (error) と判断します。

- 登録されているモニタリソースのステータスが異常 (error) となっても、そのモニタリソースの異常時アク

ションは実行されません。

マルチターゲットモニタリソースが異常 (error) になった場合のみ、マルチターゲットモニタリソースの異常時アクションが実行されます。

6.12 マルチターゲットモニタリソースの設定例

- Disk パス二重化ドライバの使用例

  ディスクデバイス (/dev/sdb, /dev/sdc など) が同時に異常となった場合にのみ、異常 (error) とする必要があります。

  以下の図は、2 つの HBA と Disk パス二重化ドライバを使ってパスを二重化した構成を表しています。
  片側の HBA の障害活性時には、Disk パス二重化ドライバがパスの縮退または切り替えを行います。

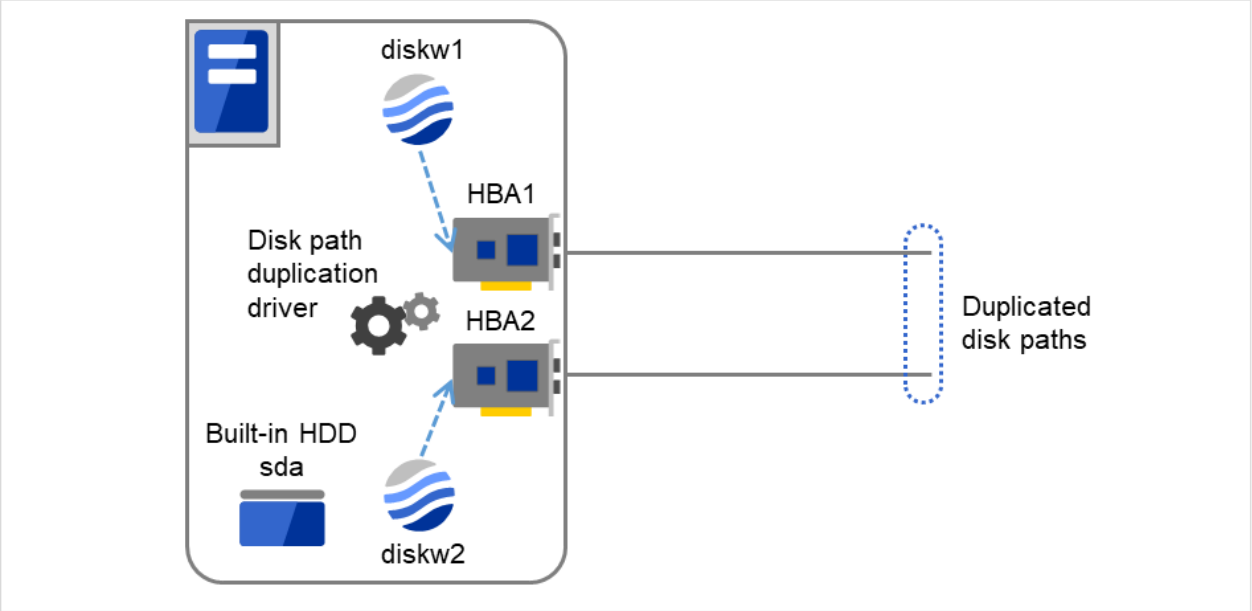


図 6.9　Disk パス二重化ドライバの使用例

  - マルチターゲットモニタリソース (mtw1) に登録するモニタリソース
    - diskw1
    - diskw2
  - マルチターゲットモニタリソース (mtw1) の異常しきい値、警告しきい値
    - 異常しきい値 2
    - 警告しきい値 0
  - マルチターゲットモニタリソース (mtw1) に登録するモニタリソースの詳細設定
    - ディスクモニタリソース (diskw1)

監視デバイス名 /dev/sdb

再活性しきい値 0

フェイルオーバしきい値 0

最終動作 何もしない

* ディスクモニタリソース (diskw2)

監視デバイス名 /dev/sdc

再活性しきい値 0

フェイルオーバしきい値 0

最終動作 何もしない

– 上記の設定の場合、マルチターゲットモニタリソースのモニタリソースに登録されている diskw1 と diskw2 のどちらかが異常を検出しても、異常となったモニタリソースの異常時アクションを行いません。

– diskw1 と diskw2 が共に異常となった場合、2 つのモニタリソースのステータスが異常 (error) と停止済み (offline) になった場合、マルチターゲットモニタリソースに設定された異常時アクションを実行します。

6.13 ソフト RAID モニタリソースの設定

ソフト RAID モニタリソースは、ソフト RAID を行っているデバイスを監視するモニタリソースです。

6.13.1 ソフト RAID モニタリソースの監視方法

ソフト RAID モニタリソースは、md ドライバを利用してソフト RAID を行っているデバイスを監視します。片方の DISK が異常になって、ソフト RAID が縮退している場合に WARNING を通知します。

注釈: 両方のディスクが異常になった場合は、異常を検出できませんので、縮退の通知時に DISK の復旧操作を行ってください。

6.13.2 監視 (固有) タブ

監視デバイス名 (1023 バイト以内)

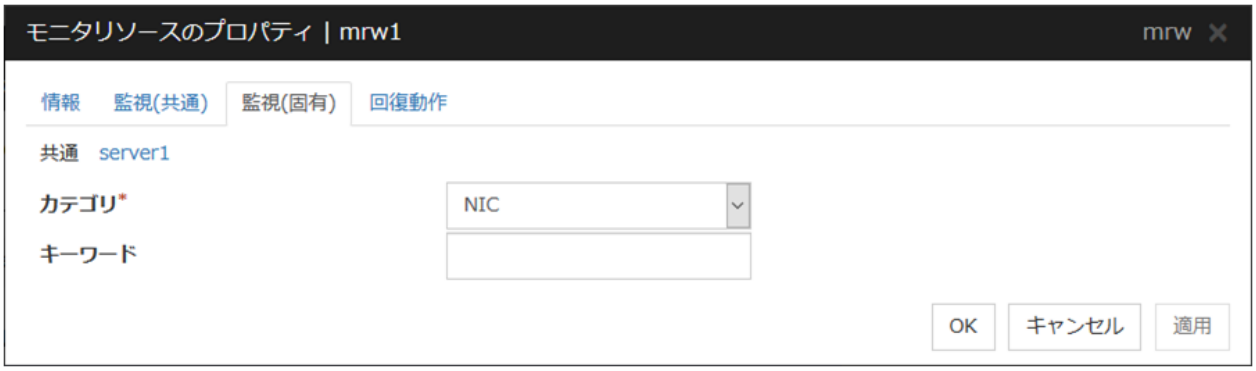
監視を行う md デバイス名を設定してください。

6.14 外部連携モニタリソースの設定

外部連携モニタリソースは受動的なモニタです。自身では監視処理を行いません。

CLUSTERPRO の外部から発行された異常発生通知を受信した場合に、外部連携モニタリソースのステータスの変更、異常発生時の回復動作を行うモニタリソースです。

6.14.1 監視 (固有) タブ



カテゴリとキーワードには、clprexec コマンドの引数 -k で渡すキーワードを設定します。キーワードは省略可能です。

カテゴリ (32 バイト以内)

clprexec コマンドの引数 -k で指定するカテゴリを指定します。

リストボックスでの既定文字列の選択または任意の文字列の指定が可能です。

キーワード (1023 バイト以内)

clprexec コマンドの引数 -k で指定するキーワードを指定します。

6.14.2 回復動作タブ

回復対象と異常検出時の動作を設定します。外部連携モニタリソースの場合、異常検出時の動作は、[回復対象を再起動]、[回復対象に対してフェイルオーバ実行]、または、[最終動作を実行] のいずれか 1 つを選択します。ただし、回復対象が非活性状態であれば回復動作は行われません。

回復動作

モニタ異常検出時に行う動作を選択します。

- 回復スクリプトを実行

  モニタ異常検出時に、回復スクリプトを実行します。

- 回復対象を再起動

  モニタ異常検出時に、回復対象に選択したグループまたはグループリソースの再起動を行います。

- 最終動作を実行

  モニタ異常検出時に、最終動作に選択した動作を行います。

回復動作前にスクリプトを実行する

回復動作を実行する前にスクリプトを実行するかどうかを指定します。

- チェックボックスがオン

  回復動作を実施する前にスクリプト/コマンドを実行します。スクリプト/コマンドの設定を 行うためには [スクリプト設定] をクリックしてください。

- チェックボックスがオフ

スクリプト/コマンドを実行しません。

※ 上記以外の設定項目については、「6. モニタリソースの詳細」 - 「6.2. モニタリソースのプロパティ」 - 「6.2.4. 回復動作タブ」を参照してください。

6.14.3 外部連携モニタリソースの監視方法

- 外部から異常発生通知を受信した場合、通知されたカテゴリとキーワード (キーワードは省略可能) が設定されている外部連携モニタリソースの異常発生時の回復動作を行います。通知されたカテゴリ、キーワードが設定されている外部連携モニタリソースが複数存在する場合は、各モニタリソースの回復動作を行います。

以下の図は外部連携モニタリソースを使用する構成の例です。clprexec コマンドから異常発生通知を受けた Server2 の外部連携モニタリソースは、自身のステータス変更と異常検出時の回復動作を実行します。

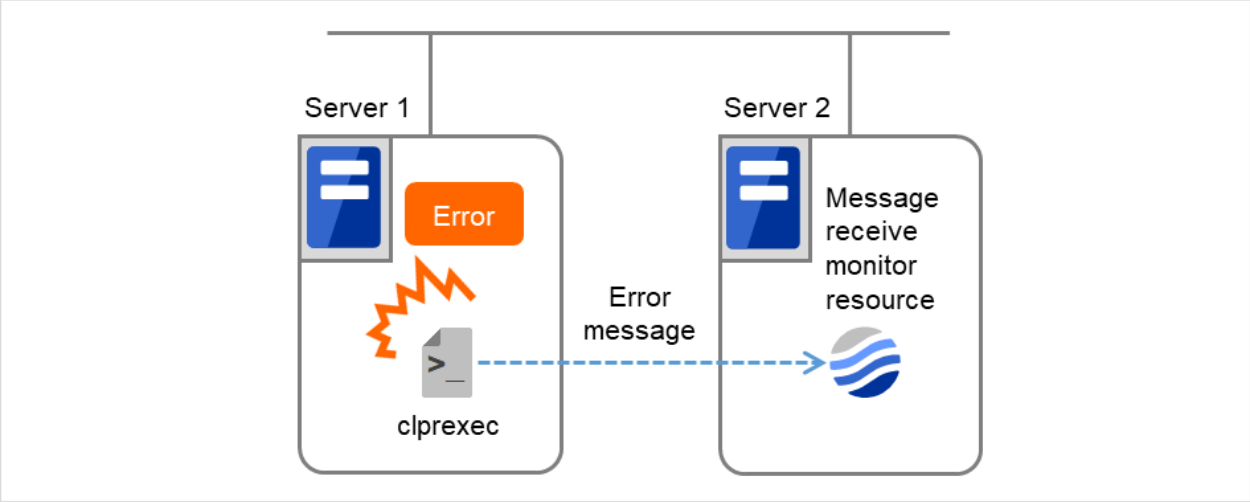


図 6.10　外部連携モニタリソースを使用する構成

6.14.4 外部連携モニタリソースに関する注意事項

- 外部連携モニタリソースが一時停止状態で外部からの異常発生通知を受信した場合、異常時動作は実行されません。
- 外部から異常発生通知を受信した場合、外部連携モニタリソースのステータスは"異常"になります。"異常"となった外部連携モニタリソースのステータスは、自動では"正常"に戻りません。ステータスを"正常"に戻したい場合は、clprexec コマンドを使用してください。clprexec コマンドについては『操作ガイド』の「CLUSTERPRO X SingleServerSafe コマンドリファレンス」を参照してください。
- 外部から異常発生通知を受信して外部連携モニタリソースのステータスが"異常"となっている状態で異常発生通知を受信した場合、異常発生時の回復動作は実行されません。

6.15 プロセス名モニタリソースの設定

プロセス名モニタリソースは、任意のプロセス名のプロセスを監視するモニタリソースです。

6.15.1 監視 (固有) タブ

プロセス名 (1023 バイト以内)

監視対象プロセスのプロセス名を設定します。プロセス名は ps(1) コマンドの出力結果などから確認します。

また、次の 3 つのパターンでプロセス名のワイルドカード指定が可能です。このパターン以外の指定はできません。

- 【前方一致】　＜プロセス名に含まれる文字列＞*
- 【後方一致】　*＜プロセス名に含まれる文字列＞
- 【部分一致】　*＜プロセス名に含まれる文字列＞*

プロセス数下限値 （1～999）

監視対象プロセスの監視個数を設定します。プロセス名に設定した監視対象プロセスの個数が設定値を下回った場合に異常と判断します。

6.15.2 プロセス名モニタリソースの注意事項

プロセス数下限値に 1 を設定した場合に監視対象に指定したプロセス名のプロセスが複数存在すると、次の条件で監視対象プロセスを一つ選択し監視します。

1. プロセス間に親子関係がある場合は、親プロセスを監視します。
2. プロセス間に親子関係がなければ、プロセスの起動時刻の最も古いものを監視します。
3. プロセス間に親子関係がなく、プロセスの起動時刻も同じであれば、もっともプロセス ID の小さいものを監視します。

同一名のプロセスが複数存在する場合にプロセスの起動個数によって監視を行う際には、プロセス数下限値に監視する個数を設定します。同一名のプロセスが設定された個数を下回ると異常と判断します。プロセス数下限値に指定できる個数は 1 から 999 個までです。プロセス数下限値に 1 を設定した場合は、監視対象プロセスを一つ選択して監視します。

監視対象プロセス名に指定できるプロセス名は 1023 バイトまでです。1023 バイトを超えるプロセス名を持つプロセスを監視対象として指定する場合は、ワイルドカード（*）を使って指定します。

監視対象プロセスのプロセス名が 1023 バイトより長い場合、プロセス名として認識できるのはプロセス名の先頭から 1023 バイトまでです。ワイルドカード（*）を使って指定する場合は、1023 バイトまでに含まれる文字列を指定してください。

監視対象のプロセス名が長い場合、ログ等に出力されるプロセス名情報は後半を省略して表示されます。

プロセス名の中に「"」（ダブルコーテーション）や「,」（カンマ）が含まれるプロセスを監視している場合、アラートメッセージにプロセス名が正しく表示できない場合があります。

監視対象プロセス名は、実際に動作しているプロセスのプロセス名を ps(1) コマンド等で確認し設定してください。

実行結果の例

```
# ps -eaf
UID        PID  PPID  C STIME TTY          TIME CMD
root         1     0  0 Sep12 ?        00:00:00 init [5]
    :
root      5314     1  0 Sep12 ?        00:00:00 /usr/sbin/acpid
root      5325     1  0 Sep12 ?        00:00:00 /usr/sbin/sshd
htt       5481     1  0 Sep12 ?        00:00:00 /usr/sbin/htt -retryonerror 0
```

上記のコマンド実行結果から /usr/sbin/htt を監視する場合、/usr/sbin/htt -retryonerror 0 を監視対象プロセス名に指定します。

監視対象プロセス名に指定したプロセス名はプロセスの引数もプロセス名の一部として監視対象のプロセスを特定します。監視対象プロセス名を指定する場合は、引数を含めたプロセス名を指定してください。引数を含めずプロセス名のみ監視したい場合は、ワイルドカード（*）を使い、引数を含めない前方一致または部分一致で指定してください。

6.15.3 プロセス名モニタリソースの監視方法

指定されたプロセス名のプロセスを監視します。プロセス数下限値に 1 を設定した場合、プロセス名からプロセス ID を特定し、そのプロセス ID の消滅時に異常と判断します。プロセスのストールを検出することはできません。

プロセス数下限値に 1 より大きい値を設定した場合、指定されたプロセス名のプロセスを個数によって監視します。プロセス名から監視対象プロセスの個数を算出し、下限値を下回った場合に異常と判断します。プロセスのストールを検出することはできません。

6.16 DB2 モニタリソースの設定

DB2 モニタリソースは、サーバ上で動作する DB2 のデータベースを監視するモニタリソースです。

6.16.1 監視 (固有) タブ

監視レベル

選択肢の中から 1 つを選択します。必ず設定してください。

- レベル 1 (select での監視)

  監視テーブルに対して参照のみを行う監視です。監視テーブルに対して実行する SQL 文は（ select ）です。

- レベル 2 (update/select での監視)

  監視テーブルに対して更新も行う監視です。監視テーブルに対して実行する SQL 文は（ update / select ）です。

  監視開始時に監視テーブルを自動で作成した場合、監視テーブルに対して実行する SQL 文は（ create / insert ）です。

- レベル 3 (毎回 create/drop も行う)

  監視テーブルに対しての更新に加え監視テーブルの作成・削除も毎回行います。監視テーブルに対して実行する SQL 文は（ create / insert / select / drop ）です。

既定値 ： レベル 2(update/select での監視)

データベース名 (255 バイト以内)

監視するデータベース名を設定します。必ず設定してください。

既定値 ： なし

インスタンス名 (255 バイト以内)

監視するデータベースのインスタンス名を設定します。必ず設定してください。

既定値 ： db2inst1

ユーザ名 (255 バイト以内)

データベースにログインする際のユーザ名を設定します。必ず設定してください。
指定したデータベースにアクセス可能な DB2 ユーザを指定してください。

既定値 ： db2inst1

パスワード (255 バイト以内)

データベースにログインする際のパスワードを設定します。必ず設定してください。

既定値 ： なし

監視テーブル名 (255 バイト以内)

データベース上に作成する監視用テーブルの名前を設定します。必ず設定してください。
テーブルの作成・削除を行いますので、運用に使用しているテーブル名と重ならないように注意してください。また、SQL 文の予約語と重ならないようにしてください。
データベースの仕様により監視テーブル名に設定できない文字があります。詳細はデータベースの仕様を確認してください。

既定値 ： db2watch

文字コード

DB2 のキャラクタ・セットを設定します。必ず設定してください。

既定値 ： なし

ライブラリパス (1023 バイト以内)

DB2 のライブラリパスを設定します。必ず設定してください。

既定値 ： /opt/ibm/db2/V11.1/lib64/libdb2.so

6.16.2 DB2 モニタリソースの注意事項

動作確認済みの DB2 のバージョンについては『インストールガイド』の「CLUSTERPRO X SingleServerSafe について」の「監視オプションの動作確認済アプリケーション情報」を参照してください。

本モニタリソースは、DB2 の CLI のライブラリを利用して、DB2 の監視を行っています。本モニタリソースが異常になる場合は、指定した DB2 の CLI のライブラリパスが存在することを確認してください。

データベースのコードページと本モニタリソースの「文字コード」の設定が異なると、本モニタリソースは、DB2 のデータベースに接続することができません。必要に応じて、適切な文字コードの設定を行ってください。データベースのコードページの確認は、「db2 get db cfg for データベース名」などで行ってください。詳細は、DB2 のマニュアルを参照してください。

パラメータで指定したデータベース名・インスタンス名・ユーザ名・パスワードなどの値が、監視を行う DB2 の環境と異なる場合、DB2 の監視を行うことができません。各エラー内容を示すメッセージが表示されますので、環境を確認してください。

次項の「 6.16.3. *DB2* モニタリソースの監視方法 」で説明する監視レベルについて、以下の点にご注意ください。
「レベル 1」で監視開始時に監視テーブルが無い場合、監視エラーになります。下記の監視テーブルの作成を行ってください。
「レベル 2」で監視開始時に監視テーブルが無い場合、CLUSTERPRO が監視テーブルを自動で作成します。このとき Cluster WebUI のアラートログに監視テーブルがない旨のメッセージが表示されます。
「レベル 3」での監視は毎回監視テーブルの作成・削除を行うため「レベル 1」「レベル 2」より監視の負荷が高くなります。

選択する監視レベル	監視テーブルの事前作成
レベル 1（select での監視）	必要あり
レベル 2（update/select での監視）	必要なし
レベル 3（毎回 create/drop も行う）	必要なし

監視テーブルの作成は以下の手順で行えます。

SQL 文で作成する場合（以下の例は監視テーブル名を db2watch とする場合）

```
sql> create table <ユーザ名>.db2watch (num int not null primary key)
sql> insert into db2watch values(0)
sql> commit
```

CLUSTERPRO のコマンドを利用する場合

前提条件として、モニタリソースの設定が完了している必要があります。

`clp_db2w --createtable -n <DB2 モニタリソース名>`

作成した監視テーブルを手動で削除する場合、下記のコマンドを実行してください：

`clp_db2w --deletetable -n <DB2 モニタリソース名>`

6.16.3 DB2 モニタリソースの監視方法

DB2 モニタリソースは、以下の監視レベルから選択した監視レベルに応じた監視を行います。

- レベル 1 (select での監視)

  監視テーブルに対して参照のみを行う監視です。監視テーブルに対して実行する SQL 文は（ select ）です。
  監視の結果以下の場合に異常とみなします。

  1. データベースへの接続や SQL 文の発行に対する応答で異常が通知された場合

- レベル 2 (update/select での監視)

  監視テーブルに対して更新も行う監視です。SQL 文の実行により最大 10 桁の数値データの書き込みと読み込みを実行します。監視テーブルに対して実行する SQL 文は（ update / select ）です。
  監視開始時に監視テーブルを自動で作成した場合、監視テーブルに対して実行する SQL 文は（ create / insert ）です。
  監視の結果以下の場合に異常とみなします。

  1. データベースへの接続や SQL 文の発行に対する応答で異常が通知された場合
  2. 書き込んだデータと読み込んだデータが一致していない場合

- レベル 3 (毎回 create/drop も行う)

  監視テーブルに対しての更新に加え監視テーブルの作成・削除も毎回行います。SQL 文の実行により最大 10 桁の数値データの書き込みと読み込みを実行します。監視テーブルに対して実行する SQL 文は（ create / insert / select / drop ）です。
  監視の結果以下の場合に異常とみなします。

1. データベースへの接続や SQL 文の発行に対する応答で異常が通知された場合

2. 書き込んだデータと読み込んだデータが一致していない場合

6.17 FTP モニタリソースの設定

FTP モニタリソースは、サーバ上で動作する FTP サービス監視するモニタリソースです。FTP プロトコルを監視するものであり、特定のアプリケーションの監視ではありません。そのため、FTP プロトコルを実装するさまざまなアプリケーションの監視を行うことができます。

6.17.1 監視 (固有) タブ

IP アドレス (79 バイト以内)

監視する FTP サーバの IP アドレスを設定します。必ず設定してください。

通常は自サーバ上で動作する FTP サーバに接続しますので、ループバックアドレス（127.0.0.1）を設定しますが、FTP サーバの設定で接続可能なアドレスを制限している場合は、接続可能なアドレス（フローティング IP アドレス等）を設定します。

既定値 ： 127.0.0.1

ポート番号 (1～65535)

監視する FTP のポート番号を設定します。必ず設定してください。

既定値 ： 21

ユーザ名 (255 バイト以内)

FTP にログインする際のユーザ名を設定します。

既定値 ： なし

パスワード (255 バイト以内)

FTP にログインする際のパスワードを設定します。

既定値 ： なし

プロトコル

FTP サーバとの通信に使用するプロトコルを設定します。通常は FTP を選択しますが、FTP over SSL/TLS で接続する必要がある場合は FTPS を選択します。

既定値 ： FTP

注釈: FTPS を利用するためには OpenSSL ライブラリが必要です

6.17.2 FTP モニタリソースの注意事項

監視の対象リソースには、FTP を起動する EXEC リソースなどを指定してください。対象リソースの活性後、監視を開始しますが、対象リソースの活性直後に FTP がすぐに動作できない場合などは、[監視開始待ち時間] で調整してください。

監視動作ごとに FTP サービス自体が動作ログなどを出力することがありますが、その制御は、FTP 側の設定で適宜行ってください。

FTP サーバの FTP メッセージ (バナー、ウェルカムメッセージなど) を既定から変更すると、監視異常とみなす場合があります。

6.17.3 FTP モニタリソースの監視方法

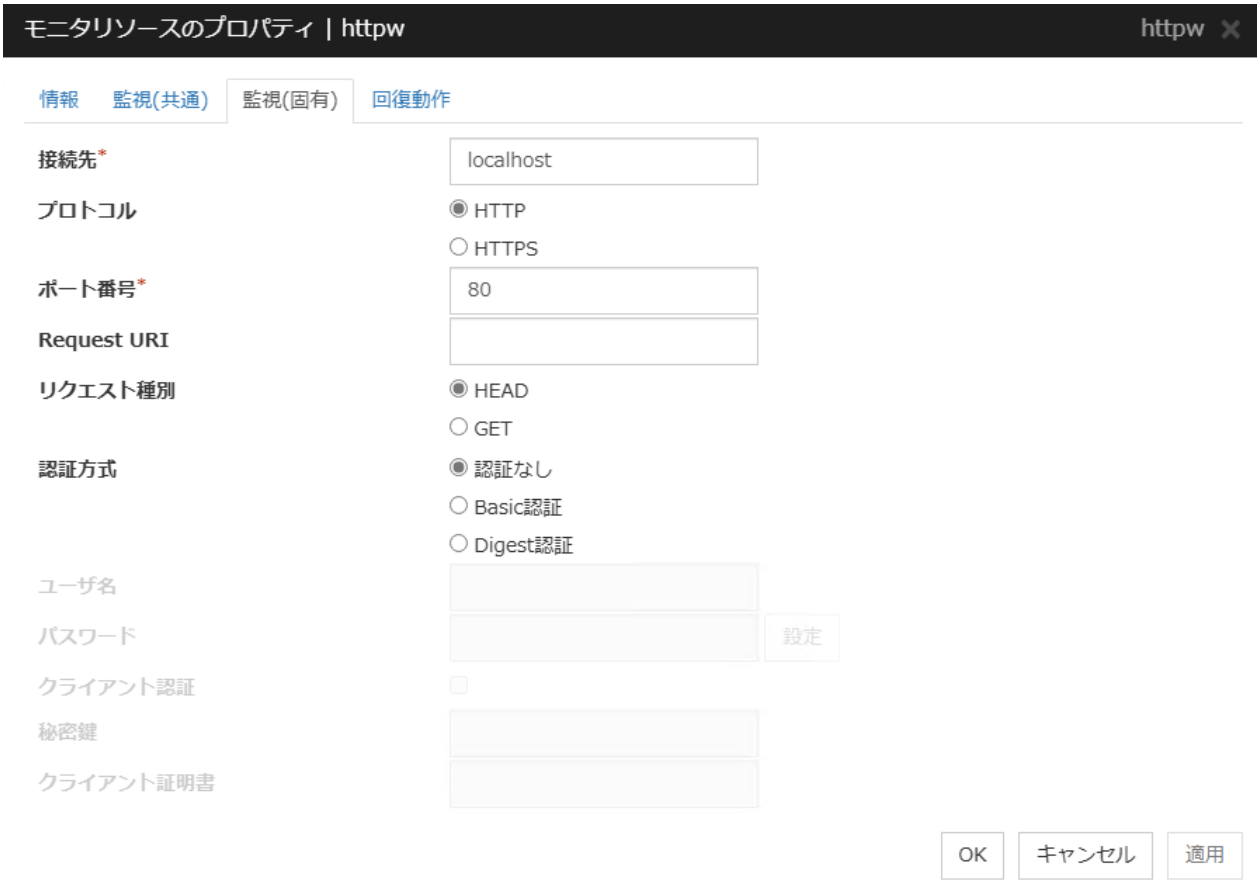
FTP モニタリソースは、以下の監視を行います。
FTP サーバに接続してファイル一覧取得コマンドを実行します。
監視の結果、以下の場合に異常とみなします。

1. FTP サービスへの接続に失敗した場合
2. FTP コマンドに対する応答で異常が通知された場合

6.18 HTTP モニタリソースの設定

HTTP モニタリソースは、サーバ上で動作する HTTP デーモンを監視するモニタリソースです。

6.18.1 監視 (固有) タブ



接続先 (255 バイト以内)

監視する HTTP サーバ名を設定します。必ず設定してください。

通常は自サーバ上で動作する HTTP サーバに接続しますので、ループバックアドレス（127.0.0.1） を設定しますが、HTTP サーバの設定で接続可能なアドレスを制限している場合は、接続可能なアドレスを設定します。

既定値 ： localhost

プロトコル

HTTP サーバとの通信に使用するプロトコルを設定します。通常は HTTP を選択しますが、HTTP over SSL で接続する必要がある場合は HTTPS を選択します。

既定値 ： HTTP

注釈: HTTPS を利用するためには OpenSSL ライブラリが必要です。

ポート番号 (1〜65535)

HTTP サーバに接続する際のポート番号を設定します。必ず設定してください。

既定値 ： 80 (HTTP の場合) 443 (HTTPS の場合)

Request URI(255 バイト以内)

Request URI（例："/index.html"） を設定します。

既定値 ： なし

リクエスト種別

HTTP サーバに接続する際の HTTP リクエストの種類を設定します。必ず設定してください。

既定値 ： HEAD

認証方式

HTTP サーバに接続する際の認証方式を設定します。

既定値 ： 認証なし

ユーザ名 (255 バイト以内)

HTTP にログインする際のユーザ名を設定します。

既定値 ： なし

パスワード (255 バイト以内)

HTTP にログインする際のパスワードを設定します。

既定値 ： なし

クライアント認証

本機能を有効にした場合、クライアント認証を行います。[プロトコル] に HTTPS が選択されている場合のみ選択可能です。

既定値 ： 無効

注釈: クライアント認証を行わない HTTP サーバに対して本機能を有効にしても動作に影響はありません。

秘密鍵 (1023 バイト以内)

クライアント認証で使用する秘密鍵ファイルのパスを設定します。[クライアント認証] を有効にした場合に必ず設定してください。

既定値 ： なし

クライアント証明書 (1023 バイト以内)

クライアント認証で使用するクライアント証明書ファイルのパスを設定します。[クライアント認証] を有効にした場合に必ず設定してください。

既定値 ： なし

6.18.2 HTTP モニタリソースの注意事項

動作確認済みの HTTP のバージョンについては、『インストールガイド』の「CLUSTERPRO X SingleServerSafe について」の「監視オプションの動作確認済アプリケーション情報」を参照してください。

HTTP モニタリソースの DIGEST 認証で使用可能なアルゴリズムは MD5 です。

HTTP モニタリソースのクライアント認証で監視可能な Web サーバは Apache HTTP Server です。

HTTP モニタリソースのクライアント認証の秘密鍵、クライアント証明書で対応しているエンコード形式は PEM 形式です。

HTTP モニタリソースの HTTP リクエストは、デフォルトのポート番号 (HTTP:80/HTTPS:443) で発行を行います。

[接続先] に IPv6 アドレスが紐づくホスト名を設定する場合は、カーネル起動オプションにて IPv6 を無効化していないことを確認してください。無効化している場合、監視が正常に行えない場合があります。

6.18.3 HTTP モニタリソースの監視方法

HTTP モニタリソースは、以下の監視を行います。
サーバ上の HTTP デーモンに接続し、HTTP リクエストの発行により、HTTP デーモンの監視を実行します。
監視の結果、以下の場合に異常とみなします。

1. HTTP デーモンへの接続で異常が通知された場合
2. HTTP リクエストの発行に対する応答メッセージが "HTTP/" で始まっていない場合
3. HTTP リクエストの発行に対する応答のステータスコードが 400、500 番台の場合 （Request URI に既定値以外の URI を指定した場合）

6.19 IMAP4 モニタリソースの設定

IMAP4 モニタリソースは、サーバ上で動作する IMAP4 のサービスを監視するモニタリソースです。IMAP4 プロトコルを監視するものであり、特定のアプリケーションの監視ではありません。そのため、IMAP4 プロトコルを実装するさまざまなアプリケーションの監視を行うことができます。

6.19.1 監視 (固有) タブ

IP アドレス (79 バイト以内)

監視する IMAP4 サーバの IP アドレスを設定します。必ず設定してください。

通常は自サーバ上で動作する IMAP4 サーバに接続しますので、ループバックアドレス（127.0.0.1）を設定しますが、IMAP4 サーバの設定で接続可能なアドレスを制限している場合は、接続可能なアドレスを設定します。

既定値 ： 127.0.0.1

ポート番号 (1〜65535)

監視する IMAP4 のポート番号を設定します。必ず設定してください。

既定値 ： 143

ユーザ名 (255 バイト以内)

IMAP4 にログインする際のユーザ名を設定します。

既定値 ： なし

パスワード (189 バイト以内)

IMAP4 にログインする際のパスワードを設定します。

既定値 ： なし

認証方式

IMAP4 にログインするときの認証方式を選択します。使用している IMAP4 の設定に合わせる必要があります。

- AUTHENTICATE LOGIN (既定値)
  AUTHENTICATE LOGIN コマンドを使用した暗号化認証方式です。
- LOGIN
  LOGIN コマンドを使用した平文方式です。

6.19.2 IMAP4 モニタリソースの注意事項

監視の対象リソースには、IMAP4 サーバを起動する EXEC リソースなどを指定してください。対象リソースの活性後、監視を開始しますが、対象リソースの活性直後に IMAP4 サーバがすぐに動作できない場合などは、[監視開始待ち時間] で調整してください。

監視動作ごとに IMAP4 サーバ自体が動作ログなどを出力することがありますが、その制御は、IMAP4 サーバ側の設定で適宜行ってください。

6.19.3 IMAP4 モニタリソースの監視方法

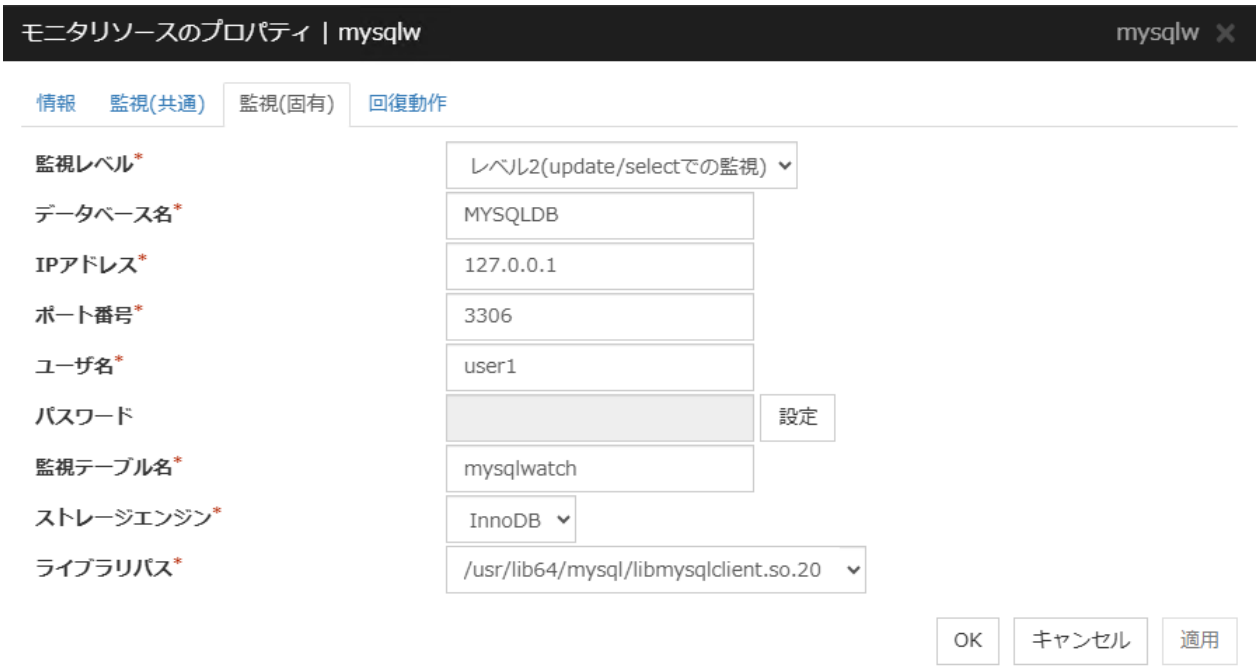
IMAP4 モニタリソースは、以下の監視を行います。
IMAP4 サーバに接続して動作確認コマンドを実行します。
監視の結果、以下の場合に異常とみなします。

1. IMAP4 サーバへの接続に失敗した場合
2. コマンドに対する応答で異常が通知された場合

6.20 MySQL モニタリソースの設定

MySQL モニタリソースは、サーバ上で動作する MySQL のデータベースを監視するモニタリソースです。

6.20.1 監視 (固有) タブ



監視レベル

選択肢の中から 1 つを選択します。必ず設定してください。

- レベル 1 (select での監視)

  監視テーブルに対して参照のみを行う監視です。監視テーブルに対して実行する SQL 文は（ select ）です。

- レベル 2 (update / select での監視)

  監視テーブルに対して更新も行う監視です。監視テーブルに対して実行する SQL 文は（ update / select ）です。

  監視開始時に監視テーブルを自動で作成した場合、監視テーブルに対して実行する SQL 文は（ create / insert ）です。

- レベル 3 (毎回 create / drop も行う)

  監視テーブルに対しての更新に加え監視テーブルの作成・削除も毎回行います。監視テーブルに対して実行する SQL 文は（ create / insert / select / drop ）です。

既定値 ： レベル 2 (update/select での監視)

データベース名 (255 バイト以内)

監視するデータベース名を設定します。必ず設定してください。

既定値 ： なし

IP アドレス (79 バイト以内)

接続するサーバの IP アドレスを設定します。必ず設定してください。

既定値 ： 127.0.0.1

ポート番号 (1～65535)

接続する際のポート番号を設定します。必ず設定してください。

既定値 ： 3306

ユーザ名 (255 バイト以内)

データベースにログインする際のユーザ名を設定します。必ず設定してください。

指定したデータベースにアクセス可能な MySQL ユーザを指定してください。

既定値 ： なし

パスワード (255 バイト以内)

データベースにログインする際のパスワードを設定します。

既定値 ： なし

監視テーブル名 (255 バイト以内)

データベース上に作成する監視用テーブルの名前を設定します。必ず設定してください。

テーブルの作成・削除を行いますので、運用に使用しているテーブル名と重ならないように注意してください。また、SQL 文の予約語と重ならないようにしてください。データベースの仕様により監視テーブル名に設定できない文字があります。詳細はデータベースの仕様を確認してください。

既定値 ： mysqlwatch

ストレージエンジン

監視用 Table の作成用ストレージエンジンを設定します。必ず設定してください。

既定値 ： InnoDB

ライブラリパス (1023 バイト以内)

MySQL のライブラリパスを設定します。必ず設定してください。

既定値 ： /usr/lib64/mysql/libmysqlclient.so.20

6.20.2 MySQL モニタリソースの注意事項

動作確認済みの MySQL のバージョンについては、『インストールガイド』の「CLUSTERPRO X SingleServerSafe について」の「監視オプションの動作確認済アプリケーション情報」を参照してください。

本モニタリソースは、MySQL の libmysqlclient のライブラリを利用して、MySQL の監視を行っています。本モニタリソースが異常になる場合は、MySQL のライブラリのインストールディレクトリに libmysqlclient.so.xx が存在することを確認してください。

パラメータ指定値が、監視を行う MySQL の環境と異なる場合、Cluster WebUI のアラートログに、エラー内容を示すメッセージが表示されますので、環境を確認してください。

次項の「6.20.3. *MySQL* モニタリソースの監視方法」で説明する監視レベルについて、以下の点にご注意ください。
「レベル 1」で監視開始時に監視テーブルが無い場合、監視エラーになります。下記の監視テーブルの作成を行ってください。
「レベル 2」で監視開始時に監視テーブルが無い場合、CLUSTERPRO が監視テーブルを自動で作成します。このとき Cluster WebUI のアラートログに監視テーブルがない旨のメッセージが表示されます。
「レベル 3」での監視は毎回監視テーブルの作成・削除を行うため「レベル 1」「レベル 2」より監視の負荷が高くなります。

選択する監視レベル	監視テーブルの事前作成
レベル 1 (select での監視)	必要あり
レベル 2 (update / select での監視)	必要なし
レベル 3 (毎回 create / drop も行う)	必要なし

監視テーブルの作成は以下の手順で行えます。

SQL 文で作成する場合（以下の例は監視テーブル名を mysqlwatch とする場合）

```
sql> create table mysqlwatch (num int not null primary key) ENGINE=<エンジン>;
sql> insert into mysqlwatch values(0);
sql> commit;
```

CLUSTERPRO のコマンドを利用する場合

前提条件として、モニタリソースの設定が完了している必要があります。

```
clp_mysqlw --createtable -n <MySQL モニタリソース名>
```

作成した監視テーブルを手動で削除する場合、下記のコマンドを実行してください：

```
clp_mysqlw --deletetable -n <MySQL モニタリソース名>
```

6.20.3 MySQL モニタリソースの監視方法

MySQL モニタリソースは、以下の監視レベルから選択した監視レベルに応じた監視を行います。

- レベル 1 (select での監視)

  監視テーブルに対して参照のみを行う監視です。監視テーブルに対して実行する SQL 文は（ select ）です。

  監視の結果以下の場合に異常とみなします。

  1. データベースへの接続や SQL 文の発行に対する応答で異常が通知された場合

- レベル 2 (update/select での監視)

  監視テーブルに対して更新も行う監視です。SQL 文の実行により最大 10 桁の数値データの書き込みと読み込みを実行します。監視テーブルに対して実行する SQL 文は（ update / select ）です。

  監視開始時に監視テーブルを自動で作成した場合、監視テーブルに対して実行する SQL 文は（ create / insert ）です。

  監視の結果以下の場合に異常とみなします。

  1. データベースへの接続や SQL 文の発行に対する応答で異常が通知された場合
  2. 書き込んだデータと読み込んだデータが一致していない場合

- レベル 3 (毎回 create / drop も行う)

  監視テーブルに対しての更新に加え監視テーブルの作成・削除も毎回行います。SQL 文の実行により最大 10 桁の数値データの書き込みと読み込みを実行します。監視テーブルに対して実行する SQL 文は（ create / insert / select / drop ）です。

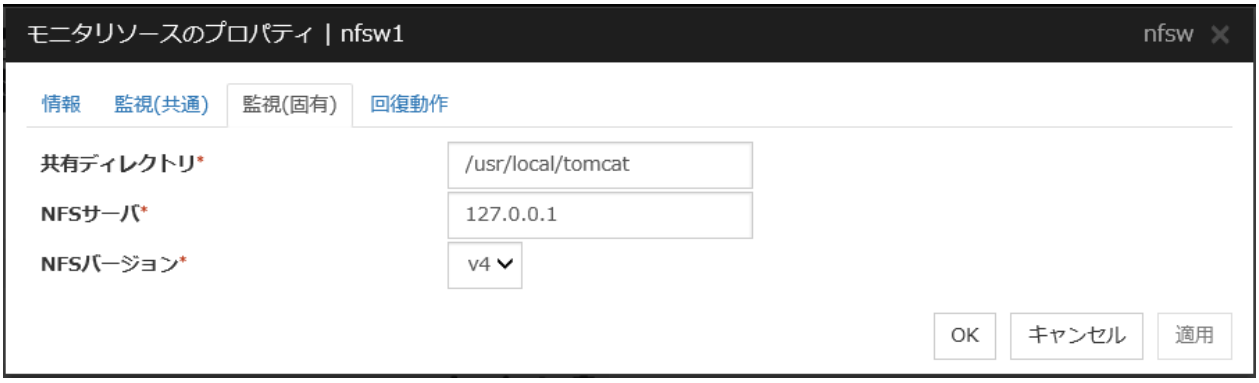
  監視の結果以下の場合に異常とみなします。

  1. データベースへの接続や SQL 文の発行に対する応答で異常が通知された場合
  2. 書き込んだデータと読み込んだデータが一致していない場合

6.21 NFS モニタリソースの設定

NFS モニタリソースは、サーバ上で動作する NFS のファイルサーバを監視するモニタリソースです。

6.21.1 監視 (固有) タブ



共有ディレクトリ (1023 バイト以内)

ファイル共有するディレクトリを設定します。必ず設定してください。

既定値 ： なし

NFS サーバ (255 バイト以内)

NFS 監視を行うサーバの IP アドレスを設定します。必ず設定してください。

既定値 ： 127.0.0.1

NFS バージョン

NFS 監視を行う NFS のバージョンを選択肢の中から 1 つ選択します。必ず設定してください。RHEL 7 では NFS バージョン v2 はサポートされていません。

- v2

  NFS バージョン v2 を監視します。

- v3

  NFS バージョン v3 を監視します。

- v4

  NFS バージョン v4 を監視します。

既定値 ： v4

6.21.2 NFS モニタリソースの動作環境

NFS モニタリソースを利用するためには、以下のサービスが起動している必要があります。

<Red Hat Enterprise Linux 7 の場合>

- nfs
- rpcbind
- nfslock (NFS v4 では不要)

<Red Hat Enterprise Linux 8 / 9 の場合>

- nfs-server
- rpcbind

NFS バージョン v4 を監視する場合は各サーバ上に nfs-utils パッケージが必要です。

6.21.3 NFS モニタリソースの注意事項

動作確認済みの NFS のバージョンについては、『インストールガイド』の「CLUSTERPRO X SingleServerSafe について」の「監視オプションの動作確認済アプリケーション情報」を参照してください。

監視する共有ディレクトリについては、自サーバから接続できるように exports ファイルを設定してください。

[監視 (固有)] タブ - [NFS バージョン] で指定したバージョンの nfsd およびその nfsd に対応する mountd の消滅を検出すると異常とみなします。nfsd に対応する mountd は以下の通りです。

nfsd バージョン	mountd バージョン
v2(udp)	v1(tcp) あるいは v2(tcp)
v3(udp)	v3(tcp)
v4(tcp)	-

6.21.4 NFS モニタリソースの監視方法

NFS モニタリソースは、以下の監視を行います。

NFS サーバに接続して [NFS] テストコマンドを実行します。

NFS バージョン v4 の export されている領域の監視は [mount] コマンドを実行します。

監視の結果、以下の場合に異常とみなします。

1. NFS サービスへの要求に対する応答結果が異常な場合
2. mountd が消滅した場合 (NFS v2/v3 の場合)
3. nfsd が消滅した場合
4. rpcbind サービスが停止した場合
5. export されている領域が消滅した場合

6.22 ODBC モニタリソースの設定

ODBC モニタリソースは、サーバ上で動作する ODBC のデータベースを監視するモニタリソースです。

6.22.1 監視 (固有) タブ

監視レベル

選択肢の中から 1 つを選択します。必ず設定してください。

- レベル 1 (select での監視)

  監視テーブルに対して参照のみを行う監視です。監視テーブルに対して実行する SQL 文は（ select ）です。

- レベル 2 (update/select での監視)

  監視テーブルに対して更新も行う監視です。監視テーブルに対して実行する SQL 文は（ update / select ）です。

  監視開始時に監視テーブルを自動で作成した場合、監視テーブルに対して実行する SQL 文は（ create / insert ）です。

- レベル 3 (毎回 create/drop も行う)

  監視テーブルに対しての更新に加え監視テーブルの作成・削除も毎回行います。監視テーブルに対して実行する SQL 文は（ create / insert / select / drop ）です。

既定値 ： レベル 2(update/select での監視)

データソース名 (255 バイト以内)

監視するデータソースを設定します。必ず設定してください。

既定値 ： なし

ユーザ名 (255 バイト以内)

データベースにログインする際のユーザ名を設定します。odbc.ini でユーザ名を設定している場合は、指定する必要はありません。

既定値 ： なし

パスワード (255 バイト以内)

データベースにログインする際のパスワードを設定します。

既定値 ： なし

監視テーブル名 (255 バイト以内)

データベース上に作成する監視用テーブルの名前を設定します。必ず設定してください。

テーブルの作成・削除を行いますので、運用に使用しているテーブル名と重ならないように注意してください。また、SQL 文の予約語と重ならないようにしてください。

データベースの仕様により監視テーブル名に設定できない文字があります。詳細はデータベースの仕様を確認してください。

既定値 ： odbcwatch

メッセージ文字コード

データベースのメッセージの文字コードを設定します。

既定値 ： UTF-8

6.22.2 ODBC モニタリソースの注意事項

監視処理は unixODBC ドライバマネージャを利用しているため、あらかじめ監視するデータベースの ODBC ドライバをインストールと odbc.ini へデータソースの設定を行ってください。

パラメータ指定値が、監視を行うデータベースの環境と異なる場合、Cluster WebUI のアラートログにエラー内容を示すメッセージが表示されますので、環境を確認してください。

ODBC モニタリソースでは、unixODBC ドライバマネージャの共有ライブラリへのシンボリックリンクとして以下を利用しています。

- libodbc.so

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、上記のシンボリックリンクが存在しない場合があります。ODBC モニタリソースでは、上記のシンボリックリンクが見つけられない場合は、以下のような警告が発生します。

```
Warn monitoring odbcw. (190 : Can not open library. (path=libodbc.so, msg=libodbc.
↪so: cannot open shared object file: No such file or directory))
```

このため、上記の警告が発生した場合は、/usr/lib64 配下に共有ライブラリへのシンボリックリンクが存在しているか確認をお願いします。また、シンボリックリンクが存在しない場合は、下記のコマンド例のようにシンボリックリンク libodbc.so を作成頂きますようお願いします。

コマンド例：

```
cd /usr/lib64                    # /usr/lib64 へ移動
ln -s libodbc.so.X libodbc.so    # シンボリックリンクの作成

X の部分は整数値を表します。環境により異なりますので確認して指定してください。
```

次項の「ODBC モニタリソースの監視方法」で説明する監視レベルについて、以下の点にご注意ください。

「レベル 1」で監視開始時に監視テーブルが無い場合、監視エラーになります。下記の監視テーブルの作成を行ってください。

「レベル 2」で監視開始時に監視テーブルが無い場合、CLUSTERPRO が監視テーブルを自動で作成します。このとき Cluster WebUI のアラートログに監視テーブルがない旨のメッセージが表示されます。

「レベル 3」での監視は毎回監視テーブルの作成・削除を行うため「レベル 1」「レベル 2」より監視の負荷が高くなります。

選択する監視レベル	監視テーブルの事前作成
レベル 1 (select での監視)	必要あり
レベル 2 (update/select での監視)	必要なし
レベル 3 (毎回 create/drop も行う)	必要なし

監視テーブルの作成は以下の手順で行えます。

監視テーブル名は英数字、一部記号 (アンダースコア等) が指定できます。

（以下の例は監視テーブル名を odbcwatch とする場合）

```
sql> create table odbcwatch (num int not null primary key);
sql> insert into odbcwatch values(0);
```

(次のページに続く)

(前のページからの続き)

```
sql> commit;
```

CLUSTERPRO のコマンドを利用する場合

前提条件として、モニタリソースの設定が完了している必要があります。

`clp_odbcw --createtable -n <ODBC モニタリソース名>`

作成した監視テーブルを手動で削除する場合、下記のコマンドを実行してください：

`clp_odbcw --deletetable -n <ODBC モニタリソース名>`

6.22.3 ODBC モニタリソースの監視方法

ODBC モニタリソースは、以下の監視レベルから選択した監視レベルに応じた監視を行います。

- レベル 1 (select での監視)
  監視テーブルに対して参照のみを行う監視です。監視テーブルに対して実行する SQL 文は（ select ）です。
  監視の結果以下の場合に異常とみなします。
  1. データベースへの接続や SQL 文の発行に対する応答で異常が通知された場合
- レベル 2 (update/select での監視)
  監視テーブルに対して更新も行う監視です。SQL 文の実行により最大 10 桁の数値データの書き込みと読み込みを実行します。監視テーブルに対して実行する SQL 文は（ update / select ）です。
  監視開始時に監視テーブルを自動で作成した場合、監視テーブルに対して実行する SQL 文は（ create / insert ）です。
  監視の結果以下の場合に異常とみなします。
  1. データベースへの接続や SQL 文の発行に対する応答で異常が通知された場合
  2. 書き込んだデータと読み込んだデータが一致していない場合
- レベル 3 (毎回 create/drop も行う)
  監視テーブルに対しての更新に加え監視テーブルの作成・削除も毎回行います。SQL 文の実行により最大 10 桁の数値データの書き込みと読み込みを実行します。監視テーブルに対して実行する SQ L 文は（ create / insert / select / drop ）です。
  監視の結果以下の場合に異常とみなします。
  1. データベースへの接続や SQL 文の発行に対する応答で異常が通知された場合
  2. 書き込んだデータと読み込んだデータが一致していない場合

6.23 Oracle モニタリソースの設定

Oracle モニタリソースは、サーバ上で動作する Oracle のデータベースを監視するモニタリソースです。

6.23.1 監視 (固有) タブ

監視方式

監視対象とする Oracle の機能を選択します。

- リスナーとインスタンスを監視 (既定値)

  監視レベルに設定されたレベルに応じ、データベースへの接続、参照、更新の動作を監視します。

- リスナーのみ監視

  リスナーが動作しているかを Oracle のコマンド（ tnsping ）を実行し監視します。モニタリソースプロパティで ORACLE_HOME を設定しておく必要があります。

  ORACLE_HOME が設定されていない場合、接続文字列に指定されている先に対して接続処理の動作のみ監視します。接続異常時にリスナーのサービス再起動による復旧を試みる場合に使用します。

本設定を選択した場合、監視レベルの設定は無視されます。

- インスタンスのみ監視

  データベースに対しリスナーを経由せず直接接続（BEQ 接続）を行い、監視レベルに設定されたレベルに応じ、データベースへの接続、参照、更新の動作を監視します。モニタリソースプロパティで ORACLE_HOME を設定しておく必要があります。この方式はリスナーを経由せずインスタンスを直接監視し復旧動作を設定するために使用します。

  監視対象が Oracle12c のマルチテナント構成のデータベースの場合、BEQ 接続での監視はできません。

  ORACLE_HOME が設定されていない場合、接続文字列に指定されている先に対して接続を行い、接続処理で異常があった場合は無視します。この方式は、[リスナーのみ監視] 方式の Oracle モニタリソースと併用して、接続処理以外の異常に対する復旧動作を設定するために使用します。

監視レベル

選択肢の中から 1 つを選択します。監視方式を「リスナーのみ監視」としている場合には本設定は無視されます。

- レベル 0 (データベースステータス)

  Oracle の管理テーブル （V$INSTANCE 表） を参照し DB の状態 （インスタンスの状態）を確認します。監視テーブルに対しての SQL 文実行は行わない簡易的な監視です。監視テーブルに対しての SQL 文実行は行わない簡易的な監視です。

- レベル 1 (select での監視)

  監視テーブルに対して参照のみを行う監視です。監視テーブルに対して実行する SQL 文は（ select ）です。

- レベル 2 (update/select での監視)

  監視テーブルに対して更新も行う監視です。監視テーブルに対して実行する SQL 文は（ update / select ）です。

  監視開始時に監視テーブルを自動で作成した場合、監視テーブルに対して実行する SQL 文は（ create / insert ）です。

- レベル 3 (毎回 create / drop も行う)

  監視テーブルに対しての更新に加え監視テーブルの作成・削除も毎回行います。監視テーブルに対して実行する SQL 文は（ create / insert / select / drop ）です。

既定値 ： レベル 2 (update / select での監視)

接続文字列 (255 バイト以内)

監視するデータベースに対応する接続文字列を設定します。必ず設定してください。

監視方式を「インスタンスのみの監視」とした場合には ORACLE_SID を設定します。

監視方式	ORACLE_HOME	接続文字列	監視レベル
リスナーとインスタンスを監視	入力不要	接続文字列を指定	設定に応じたレベルの監視
リスナーのみ監視	入力した場合、Oracle のコマンドを使用した監視	接続文字列を指定	レベル設定は無視される
	未入力の場合、リスナーを経由したインスタンスへの接続確認	接続文字列を指定	レベル設定は無視される
インスタンスのみ監視	入力した場合、BEQ 接続によるインスタンスの確認	ORACLE_SID を指定する	設定に応じたレベルの監視
	未入力の場合、リスナーを経由したインスタンスの確認となる	接続文字列を指定	設定に応じたレベルの監視

既定値 ： 接続文字列の既定値はなし

ユーザ名 (255 バイト以内)

データベースにログインする際のユーザ名を設定します。必ず設定してください。

指定したデータベースにアクセス可能な Oracle ユーザを指定してください。

既定値 ：sys

パスワード (255 バイト以内)

データベースにログインする際のパスワードを設定します。

既定値 ： なし

認証方式

データベースの認証方式を設定します。

既定値 ： SYSDBA

監視テーブル名 (255 バイト以内)

データベース上に作成する監視用テーブルの名前を設定します。必ず設定してください。

テーブルの作成・削除を行いますので、運用に使用しているテーブル名と重ならないように注意してください。また、SQL 文の予約語と重ならないようにしてください。

データベースの仕様により監視テーブル名に設定できない文字があります。詳細はデータベースの仕様を確認してください。

既定値 ： orawatch

ORACLE_HOME (255 バイト以内)

ORACLE_HOME に設定しているパス名を指定します。[/] で始まる必要があります。監視方式で「リスナーのみ監視」「インスタンスのみ監視」を選択したときに使用されます。

既定値 ： なし

文字コード

Oracle のキャラクタ・セットを設定します。必ず設定してください。

既定値 ： JAPANESE_JAPAN.JA16EUC

ライブラリパス (1023 バイト以内)

Oracle Call Interface(OCI) 用のライブラリパスを設定します。必ず設定してください。

既定値 ： /u01/app/oracle/product/12.2.0/dbhome_1/lib/libclntsh.so.12.1

障害発生時にアプリケーションの詳細情報を採取する

本機能を有効にした場合、Oracle モニタリソースが異常を検出すると、Oracle の詳細情報が採取されます。詳細情報は最大 5 回採取されます。

注釈: 採取中にクラスタ停止などにより、oracle サービスを停止させた場合、正しい情報が取得できない可能性があります。

既定値 ： 無効

採取タイムアウト

詳細情報採取時のタイムアウト値を設定します。

既定値 ： 600

Oracle の初期化中またはシャットダウン中をエラーにする

本機能を有効にした場合、Oracle の初期化中またはシャットダウン中の状態を検出すると、直ちに監視エラーになります。Oracle Clusterware 等の連携で Oracle が運用中に自動再起動される場合、本機能を無効にしてください。Oracle の初期化中またはシャットダウン中の状態でも監視正常になります。ただし 1 時間以上 Oracle の初期化中またはシャットダウン中の状態が継続すると監視エラーになります。

既定値 ： 無効

6.23.2 Oracle モニタリソースの注意事項

動作確認済みの Oracle のバージョンについては、『インストールガイド』の「CLUSTERPRO X SingleServerSafe について」の「監視オプションの動作確認済アプリケーション情報」を参照してください。

本モニタリソースは、Oracle のインターフェイス (Oracle Call Interface) を利用して、Oracle の監視を行っています。そのため、監視を行うサーバ上に、インターフェイス用のライブラリ (libclntsh.so) がインストールされている必要があります。

パラメータで指定した接続文字列・ユーザ名・パスワードなどの値が、監視を行う Oracle の環境と異なる場合、Oracle の監視を行うことができません。各エラー内容を示すメッセージが表示されますので、環境を確認してください。

パラメータのユーザ名に指定するユーザについて、デフォルトでは sys となっていますが、別途監視用ユーザを作成する場合、各監視レベルにおいて以下のアクセス権付与が必要です。(sysdba 権限を与えない場合)

監視レベル	必要な権限
レベル 0(データベースステータス)	V$INSTANCE への SELECT 権限
レベル 1(select での監視)	監視テーブルへの SELECT 権限
レベル 2(update/select での監視)	CREATE TABLE ／ DROP ANY TABLE ／監視テーブルへの INSERT 権限／監視テーブルへの UPDATE 権限／監視テーブルへの SELECT 権限
レベル 3(毎回 create/drop も行う)	CREATE TABLE ／ DROP ANY TABLE ／監視テーブルへの INSERT 権限／監視テーブルへの UPDATE 権限／監視テーブルへの SELECT 権限

管理者ユーザの認証方式が初期化パラメータ・ファイルで REMOTE_LOGIN_PASSWORDFILE を NONE に設定した OS 認証のみである場合、パラメータのユーザ名には SYSDBA 権限のないデータベースユーザ名を指定して下さい。
SYSDBA 権限のあるデータベースユーザを指定した場合、本モニタリソース起動時にエラーとなり監視を行うことができません。

ユーザ名に sys を指定すると Oracle の監査ログが出力されることがあります。監査ログを大量に出力したくない場合、 sys 以外のユーザ名を指定してください。

データベース作成時のキャラクタ・セットは、OS でサポートされているキャラクタ・セットに合わせてください。本モニタリソースの「文字コード」は、Oracle からのエラーメッセージが発生したときに、CLUSTERPRO の

Cluster WebUI のアラートログや OS の messages(syslog) に表示させる言語を選択してください。

ただし、データベース接続時のエラー （ユーザ名不正など） については、上記の対応を行っても正しく表示されないことがあります。

NLS パラメータ、NLS_LANG の設定、詳細な内容については、Oracle 社のマニュアル「グローバリゼーション・サポート・ガイド」を参照してください。

「文字コード」の設定は Oracle 自体の動作には影響を与えません。

CLUSTERPRO が OS の messages(syslog) へ 1 バイト文字以外 (ANK 文字以外) をエントリするときには常に EUC コードでエントリします。従ってご使用のディストリビューションによっては messages(syslog) の文字コードが EUC でないため文字化けが発生し正しく表示されないことがあります。

(Cluster WebUI のアラートログについては問題ありません。)

文字化けを発生させたくない場合には「文字コード」の設定に AMERICAN_AMERICA.US7ASCII または AMERICAN_AMERICA.UTF8 (ANK 文字を使用する言語) を選択してください。

設定例

- 日本語で表示させたい場合

  JAPANESE_JAPAN で始まる文字セットを選択してください。

- 英語で表示させたい場合

  AMERICAN_AMERICA で始まる文字セットを選択してください。

次項の「Oracle モニタリソースの監視方法」で説明する監視レベルについて、以下の点にご注意ください。

「レベル 1」で監視開始時に監視テーブルが無い場合、監視エラーになります。下記の監視テーブルの作成を行ってください。

「レベル 2」で監視開始時に監視テーブルが無い場合、CLUSTERPRO が監視テーブルを自動で作成します。このとき Cluster WebUI のアラートログに監視テーブルがない旨のメッセージが表示されます。

「レベル 3」での監視は毎回監視テーブルの作成・削除を行うため「レベル 1」「レベル 2」より監視の負荷が高くなります。また Oracle のリソースの使用量が増え続けるため、定期的に Oracle インスタンスを再起動する運用以外での「レベル 3」の監視は推奨しません。

選択する監視レベル	監視テーブルの事前作成
レベル 0 (データベースステータス)	必要なし
レベル 1 (select での監視)	必要あり
レベル 2 (update/select での監視)	必要なし
レベル 3 (毎回 create/drop も行う)	必要なし

監視テーブルの作成は以下の手順で行えます。

SQL 文で作成する場合（以下の例は監視テーブル名を orawatch とする場合）

```
sql> create table orawatch (num number(11,0) primary key);
sql> insert into orawatch values(0);
sql> commit;
```

※パラメータのユーザ名に指定するユーザのスキーマに作成してください。

CLUSTERPRO のコマンドを利用する場合

前提条件として、モニタリソースの設定が完了している必要があります。

clp_oraclew --createtable -n *<Oracle* モニタリソース名>

※パラメータのユーザ名に指定するユーザが sys 以外で sysdba 権限を付与しないユーザの場合は CREATE TABLE 権限が必要です。

作成した監視テーブルを手動で削除する場合、下記のコマンドを実行してください：

clp_oraclew --deletetable -n *<Oracle* モニタリソース名>

6.23.3 Oracle モニタリソースの監視方法

Oracle モニタリソースは、以下の監視レベルから選択した監視レベルに応じた監視を行います。

- レベル 0 (データベースステータス)

  Oracle の管理テーブル（V$INSTANCE 表）を参照し DB の状態（インスタンスの状態）を確認します。監視テーブルに対しての SQL 文実行は行わない簡易的な監視です。

  監視の結果以下の場合に異常とみなします。

  1. Oracle の管理テーブル (V$INSTANCE 表) のステータス (status) が未起動状態 (MOUNTED,STARTED) の場合
  2. Oracle の管理テーブル (V$INSTANCE 表) のデータベースステータス (database_status) が未起動 (SUSPENDED,INSTANCE RECOVERY) の場合

- レベル 1 (select での監視)

監視テーブルに対して参照のみを行う監視です。監視テーブルに対して実行する SQL 文は（ select ）です。
監視の結果以下の場合に異常とみなします。

1. データベースへの接続や SQL 文の発行に対する応答で異常が通知された場合

- レベル 2 (update/select での監視)

  監視テーブルに対して更新も行う監視です。SQL 文の実行により最大 11 桁の数値データの書き込みと読み込みを実行します。監視テーブルに対して実行する SQL 文は（ update / select ）です。
  監視開始時に監視テーブルを自動で作成した場合、監視テーブルに対して実行する SQL 文は（ create / insert ）です。
  監視の結果以下の場合に異常とみなします。

  1. データベースへの接続や SQL 文の発行に対する応答で異常が通知された場合
  2. 書き込んだデータと読み込んだデータが一致していない場合

- レベル 3 (毎回 create/drop も行う)

  監視テーブルに対しての更新に加え監視テーブルの作成・削除も毎回行います。SQL 文の実行により最大 11 桁の数値データの書き込みと読み込みを実行します。監視テーブルに対して実行する SQL 文は（ create / insert / select / drop ）です。
  監視の結果以下の場合に異常とみなします。

  1. データベースへの接続や SQL 文の発行に対する応答で異常が通知された場合
  2. 書き込んだデータと読み込んだデータが一致していない場合

6.24 POP3 モニタリソースの設定

POP3 モニタリソースは、サーバ上で動作する POP3 のサービスを監視するモニタリソースです。POP3 プロトコルを監視するものであり、特定のアプリケーションの監視ではありません。そのため、POP3 プロトコルを実装するさまざまなアプリケーションの監視を行うことができます。

6.24.1 監視 (固有) タブ

IP アドレス (79 バイト以内)

監視する POP3 サーバの IP アドレスを設定します。必ず設定してください。

通常は自サーバ上で動作する POP3 サーバに接続しますので、ループバックアドレス（127.0.0.1）を設定しますが、POP3 サーバの設定で接続可能なアドレスを制限している場合は、接続可能なアドレス（フローティング IP アドレス等）を設定します。

既定値 ： 127.0.0.1

認証方式

POP3 にログインするときの認証方式を選択します。使用している POP3 の設定に合わせる必要があります。

- APOP (既定値)

  APOP コマンドを使用した暗号化認証方式です。

- USER/PASS

  USER/PASS コマンドを使用した平文方式です。

- POP3S

  SSL/TLS を使用した暗号化認証方式です。

注釈: POP3S を利用するためには OpenSSL ライブラリが必要です。

ポート番号 (1〜65535)

監視する POP3 のポート番号を設定します。必ず設定してください。

既定値 ：

110

995 (POP3S の場合)

ユーザ名 (255 バイト以内)

POP3 にログインする際のユーザ名を設定します。

既定値 ： なし

パスワード (255 バイト以内)

POP3 にログインする際のパスワードを設定します。

既定値 ： なし

6.24.2 POP3 モニタリソースの注意事項

監視の対象リソースには、POP3 サーバを起動する EXEC リソースなどを指定してください。対象リソースの活性後、監視を開始しますが、対象リソースの活性直後に POP3 がすぐに動作できない場合などは、[監視開始待ち時間] で調整してください。

監視動作ごとに POP3 自体が動作ログなどを出力することがありますが、その制御は、POP3 側の設定で適宜行ってください。

6.24.3 POP3 モニタリソースの監視方法

POP3 モニタリソースは、以下の監視を行います。

POP3 サーバに接続して動作確認コマンドを実行します。

監視の結果、以下の場合に異常とみなします。

1. POP3 サーバへの接続に失敗した場合

2. コマンドに対する応答で異常が通知された場合

6.25 PostgreSQL モニタリソースの設定

PostgreSQL モニタリソースは、サーバ上で動作する PostgreSQL のデータベースを監視するモニタリソースです。

6.25.1 監視 (固有) タブ

監視レベル

選択肢の中から 1 つを選択します。必ず設定してください。

- レベル 1 (select での監視)

  監視テーブルに対して参照のみを行う監視です。監視テーブルに対して実行する SQL 文は（ select ）です。

- レベル 2 (update/select での監視)

  監視テーブルに対して更新も行う監視です。監視テーブルに対して実行する SQL 文は（ update / select / reindex / vacuum ）です。

  監視開始時に監視テーブルを自動で作成した場合、監視テーブルに対して実行する SQL 文は（ create / insert ）です。

- レベル 3 (毎回 create / drop も行う)

  監視テーブルに対しての更新に加え監視テーブルの作成・削除も毎回行います。監視テーブルに対して実行する SQL 文は（ create / insert / select / reindex / drop / vacuum ）です。

既定値 ： レベル 2 (update/select での監視)

データベース名 (255 バイト以内)

監視するデータベース名を設定します。必ず設定してください。

既定値 ： なし

IP アドレス (79 バイト以内)

接続するサーバの IP アドレスを設定します。必ず設定してください。

既定値 ： 127.0.0.1

ポート番号 (1〜65535)

接続する際のポート番号を設定します。必ず設定してください。

既定値 ： 5432

ユーザ名 (255 バイト以内)

データベースにログインする際のユーザ名を設定します。必ず設定してください。
指定したデータベースにアクセス可能な PostgreSQL ユーザを指定してください。

既定値 ： postgres

パスワード (255 バイト以内)

データベースにログインする際のパスワードを設定します。

既定値 ： なし

監視テーブル名 (255 バイト以内)

データベース上に作成する監視用テーブルの名前を設定します。必ず設定してください。
テーブルの作成・削除を行いますので、運用に使用しているテーブル名と重ならないように注意してください。
また、SQL 文の予約語と重ならないようにしてください。
データベースの仕様により監視テーブル名に設定できない文字があります。詳細はデータベースの仕様を確認してください。

既定値 ： psqlwatch

ライブラリパス (1023 バイト以内)

PostgreSQL のライブラリパスを設定します。必ず設定してください。

既定値 ： /opt/PostgreSQL/10/lib/libpq.so.5.10

PostgreSQL の初期化中またはシャットダウン中をエラーにする

本機能を有効にした場合、PostgreSQL の初期化中またはシャットダウン中の状態を検出すると、直ちに監視エラーになります。本機能を無効にした場合、PostgreSQL の初期化中またはシャットダウン中の状態でも監視正常になります。ただし 1 時間以上 PostgreSQL の初期化中またはシャットダウン中の状態が継続すると監視エラーになります。

既定値 ： 有効

6.25.2 PostgreSQL モニタリソースの注意事項

動作確認済みの PostgreSQL のバージョンについては、『インストールガイド』の「CLUSTERPRO X SingleServerSafe について」の「監視オプションの動作確認済アプリケーション情報」を参照してください。

本モニタリソースは、PostgreSQL の libpq のライブラリを利用して、PostgreSQL の監視を行っています。本モニタリソースが異常になる場合は、PostgreSQL の libpq ライブラリが存在するパスへアプリケーションのライブラリパスを設定してください。

パラメータ指定値が、監視を行う PostgreSQL の環境と異なる場合、Cluster WebUI のアラートログにエラー内容を示すメッセージが表示されますので、環境を確認してください。

クライアント認証について、本モニタリソースでは pg_hba.conf ファイルに設定可能な以下の認証方式が動作確認済みとなっています。trust、md5、password

本モニタリソースを利用すると PostgreSQL 側のログに下記のようなメッセージが出力されます。監視処理に伴って出力されるメッセージで、問題はありません。

```
YYYY-MM-DD hh:mm:ss JST moodle moodle LOG: statement: DROP TABLE psqlwatch
YYYY-MM-DD hh:mm:ss JST moodle moodle ERROR: table "psqlwatch" does not exist
YYYY-MM-DD hh:mm:ss JST moodle moodle STATEMENT: DROP TABLE psqlwatch
YYYY-MM-DD hh:mm:ss JST moodle moodle LOG: statement: CREATE TABLE psqlwatch (num␣
↪INTEGER NOT NULL PRIMARY KEY)
YYYY-MM-DD hh:mm:ss JST moodle moodle NOTICE: CREATE TABLE / PRIMARY KEY will create␣
↪implicit index "psqlwatch_pkey" for table "psql watch"
YYYY-MM-DD hh:mm:ss JST moodle moodle LOG: statement: DROP TABLE psqlwatch
```

次項の「PostgreSQL モニタリソースの監視方法」で説明する監視レベルについて、以下の点にご注意ください。

「レベル 1」で監視開始時に監視テーブルが無い場合、監視エラーになります。下記の監視テーブルの作成を行ってください。

「レベル 2」で監視開始時に監視テーブルが無い場合、CLUSTERPRO が監視テーブルを自動で作成します。このとき Cluster WebUI のアラートログに監視テーブルがない旨のメッセージが表示されます。

「レベル 3」での監視は毎回監視テーブルの作成・削除を行うため「レベル 1」「レベル 2」より監視の負荷が高くなります。

選択する監視レベル	監視テーブルの事前作成
レベル 1(select での監視)	必要あり
レベル 2(update/select での監視)	必要なし
レベル 3(毎回 create/drop も行う)	必要なし

監視テーブルの作成は以下の手順で行えます。

SQL 文で作成する場合（以下の例は監視テーブル名を psqlwatch とする場合）

```
sql> CREATE TABLE psqlwatch (num INTEGER NOT NULL PRIMARY KEY);
sql> INSERT INTO psqlwatch VALUES(0) ;
sql> COMMIT;
```

CLUSTERPRO のコマンドを利用する場合

前提条件として、モニタリソースの設定が完了している必要があります。

`clp_psqlw --createtable -n <PostgreSQL モニタリソース名>`

作成した監視テーブルを手動で削除する場合、下記のコマンドを実行してください：

`clp_psqlw --deletetable -n <PostgreSQL モニタリソース名>`

6.25.3 PostgreSQL モニタリソースの監視方法

PostgreSQL モニタリソースは、以下の監視レベルから選択した監視レベルに応じた監視を行います。

- レベル 1 (select での監視)
  監視テーブルに対して参照のみを行う監視です。監視テーブルに対して実行する SQL 文は（ select ）です。
  監視の結果以下の場合に異常とみなします。
  1. データベースへの接続や SQL 文の発行に対する応答で異常が通知された場合
- レベル 2 (update / select での監視)
  監視テーブルに対して更新も行う監視です。SQL 文の実行により最大 10 桁の数値データの書き込みと読み込みを実行します。監視テーブルに対して実行する SQL 文は（ update / select / reindex / vacuum ）です。
  監視開始時に監視テーブルを自動で作成した場合、監視テーブルに対して実行する SQL 文は（ create / insert ）です。
  監視の結果以下の場合に異常とみなします。
  1. データベースへの接続や SQL 文の発行に対する応答で異常が通知された場合
  2. 書き込んだデータと読み込んだデータが一致していない場合

- レベル 3 (毎回 create / drop も行う)

  監視テーブルに対しての更新に加え監視テーブルの作成・削除も毎回行います。SQL 文の実行により最大 10 桁の数値データの書き込みと読み込みを実行します。監視テーブルに対して実行する SQL 文は（ create / insert / select / reindex / drop / vacuum ）です。

  監視の結果以下の場合に異常とみなします。

  1. データベースへの接続や SQL 文の発行に対する応答で異常が通知された場合
  2. 書き込んだデータと読み込んだデータが一致していない場合

6.26 Samba モニタリソースの設定

Samba モニタリソースは、サーバ上で動作する samba のファイルサーバを監視するモニタリソースです。

6.26.1 監視 (固有) タブ

共有名 (255 バイト以内)

監視を行う samba サーバの共有名を設定します。必ず設定してください。

既定値 ： なし

IP アドレス (79 バイト以内)

samba サーバの IP アドレスを設定します。必ず設定してください。

既定値 ： 127.0.0.1

ポート番号 (1～65535)

samba デーモンが使用しているポート番号を設定します。必ず設定してください。libsmbclient のバージョンが 3 以下の場合（例.RHEL 6 に同梱の libsmbclient.so)、[ポート番号] は 139 もしくは 445 しか指定できません。smb.conf の smb ports も同じ値を指定してください。

既定値 ： 139

ユーザ名 (255 バイト以内)

samba サービスにログインする際のユーザ名を設定します。必ず設定してください。

既定値 ： なし

パスワード (255 バイト以内)

samba サービスにログインする際のパスワードを設定します。

既定値 ： なし

6.26.2 Samba モニタリソースの注意事項

動作確認済みの samba のバージョンについては、『インストールガイド』の「CLUSTERPRO X SingleServerSafe について」の「監視オプションの動作確認済アプリケーション情報」を参照してください。

本モニタリソースが異常になる場合は、パラメータの設定値と samba の環境が一致していない可能性がありますので、環境を確認してください。

監視する共有名については、自サーバから接続できるように smb.conf を設定してください。また、smb.conf ファイルの security パラメータが share の場合は、ゲスト接続を有効にしてください。

ファイル共有、プリンタ共有以外の samba の機能に関しては監視を行いません。

samba の認証モードが Domain もしくは Server の場合、監視サーバ上で smbmount を実行すると、本モニタリソースのパラメータで指定したユーザ名で mount されることがあります。

6.26.3 Samba モニタリソースの監視方法

Samba モニタリソースは、内部バージョン 4.1.0-1 より共有ライブラリの libsmbclient.so.0 を利用しています。
Samba モニタリソースは、以下の監視を行います。
samba サーバに接続して samba サーバのリソースに対する tree connection の確立を確認します。
監視の結果、以下の場合に異常とみなします。

1. samba サービスへの要求に対する応答内容が不正な場合

6.27 SMTP モニタリソースの設定

SMTP モニタリソースは、サーバ上で動作する SMTP デーモンを監視するモニタリソースです。

6.27.1 監視 (固有) タブ

IP アドレス (79 バイト以内)

監視する SMTP サーバの IP アドレスを設定します。必ず設定してください。

既定値 ： 127.0.0.1

ポート番号 (1～65535)

SMTP サーバに接続する際のポート番号を設定します。必ず設定してください。

既定値 ： 25

6.27.2 SMTP モニタリソースの注意事項

動作確認済みの SMTP のバージョンについては、『インストールガイド』の「CLUSTERPRO X SingleServerSafe について」の「監視オプションの動作確認済アプリケーション情報」を参照してください。

ロードアベレージが、sendmail.def ファイルで設定されている RefuseLA の値よりも超えた状態が一定時間続くと、本モニタリソースで異常とみなすことがあります。

6.27.3 SMTP モニタリソースの監視方法

SMTP モニタリソースは、以下の監視を行います。

サーバ上の SMTP デーモンに接続し、NOOP コマンドの発行により、SMTP デーモンの監視を実行します。

監視の結果、以下の場合に異常とみなします。

1. SMTP デーモンへの接続や NOOP コマンドの発行に対する応答で異常が通知された場合

6.28 SQL Server モニタリソースの設定

SQL Server モニタリソースは、サーバ上で動作する SQL Server のデータベースを監視するモニタ リソースです。

6.28.1 監視 (固有) タブ

監視レベル

選択肢の中から 1 つを選択します。必ず設定してください。

- レベル 0 (データベースステータス)

  SQL Server の管理テーブルを参照し DB の状態を確認します。監視テーブルに対して SQL 文の発行は行わない簡易的な監視です。

- レベル 1 (select での監視)

  監視テーブルに対して参照のみを行う監視です。監視テーブルに対して実行する SQL 文は（ select ）です。

- レベル 2 (update/select での監視)

  監視テーブルに対して更新も行う監視です。監視テーブルに対して実行する SQL 文は（ update / select ）です。

  監視開始時に監視テーブルを自動で作成した場合、監視テーブルに対して実行する SQL 文は（ create / insert ）です。

- レベル 3 (毎回 create/drop も行う)

  監視テーブルに対しての更新に加え監視テーブルの作成・削除も毎回行います。監視テーブルに対して実行する SQL 文は（ create / insert / select / drop ）です。

既定値 ： レベル 2 (update/select での監視)

データベース名 (255 バイト以内)

監視するデータベース名を設定します。必ず設定してください。

既定値 ： なし

サーバ名 (255 バイト以内)

監視するデータベースのサーバ名を設定します。必ず設定してください。

既定値 ： localhost

ユーザ名 (255 バイト以内)

データベースにログインする際のユーザ名を設定します。必ず設定してください。
指定したデータベースにアクセス可能な SQL Server ユーザを指定してください。

既定値 ： SA

パスワード (255 バイト以内)

データベースにログインする際のパスワードを設定します。

既定値 ： なし

監視テーブル名 (255 バイト以内)

データベース上に作成する監視用テーブルの名前を設定します。必ず設定してください。

テーブルの作成・削除を行いますので、運用に使用しているテーブル名と重ならないように注意してください。また、SQL 文の予約語と重ならないようにしてください。データベースの仕様により監視テーブル名に設定できない文字があります。詳細はデータベースの仕様を確認してください。

既定値 ： sqlwatch

ODBC ドライバ名 (255 バイト以内)

SQL Server の ODBC ドライバ名を設定します。必ず設定してください。

既定値 ： ODBC Driver 13 for SQL Server

6.28.2 SQL Server モニタリソースの注意事項

動作確認済みの SQL Server のバージョンについては、『インストールガイド』の「CLUSTERPRO X SingleServerSafe について」の「監視オプションの動作確認済アプリケーション情報」を参照してください。

本モニタリソースは、Microsoft ODBC Driver for SQL Server を使用して、SQL Server の監視を行っています。

パラメータ指定値が、監視を行う SQL Server の環境と異なる場合、Cluster WebUI のアラートログにエラー内容を示すメッセージが表示されますので、環境を確認してください。

次項の「SQL Server モニタリソースの監視方法」で説明する監視レベルについて、以下の点にご注意ください。
「レベル 1」で監視開始時に監視テーブルが無い場合、監視エラーになります。下記の監視テーブルの作成を行ってください。
「レベル 2」で監視開始時に監視テーブルが無い場合、CLUSTERPRO が監視テーブルを自動で作成します。このとき Cluster WebUI のアラートログに監視テーブルがない旨のメッセージが表示されます。
「レベル 3」での監視は毎回監視テーブルの作成・削除を行うため「レベル 1」「レベル 2」より監視の負荷が高くなります。

選択する監視レベル	監視テーブルの事前作成
レベル 0(データベースステータス)	必要なし
レベル 1(select での監視)	必要あり
レベル 2(update/select での監視)	必要なし
レベル 3(毎回 create/drop も行う)	必要なし

監視テーブルの作成は以下の手順で行えます。監視テーブル名は英数字、一部記号 (アンダースコア等) が指定できます。

SQL 文で作成する場合 （以下の例は監視テーブル名を sqlwatch とする場合）

- SET IMPLICIT_TRANSACTIONS がオフの場合

```
sql> CREATE TABLE sqlwatch (num INT NOT NULL PRIMARY KEY)
sql> GO
sql> INSERT INTO sqlwatch VALUES(0)
sql> GO
```

- SET IMPLICIT_TRANSACTIONS がオンの場合

```
sql> CREATE TABLE sqlwatch (num INT NOT NULL PRIMARY KEY)
sql> GO
sql> INSERT INTO sqlwatch VALUES(0)
sql> GO
sql> COMMIT
sql> GO
```

CLUSTERPRO のコマンドを利用する場合

前提条件として、モニタリソースの設定が完了している必要があります。

`clp_sqlserverw --createtable -n <SQL Server モニタリソース名>`

作成した監視テーブルを手動で削除する場合、下記のコマンドを実行してください：

`clp_sqlserverw --deletetable -n <SQL Server モニタリソース名>`

6.28.3 SQL Server モニタリソースの監視方法

SQL Server モニタリソースは、以下の監視レベルから選択した監視レベルに応じた監視を行います。

- レベル 0 (データベースステータス)

  SQL Server の管理テーブルを参照し DB の状態を確認します。監視テーブルに対して SQL 文の発行は行わない簡易的な監視です。

  監視の結果以下の場合に異常とみなします。

  1. データベースのステータスがオンラインでない場合

- レベル 1 (select での監視)

  監視テーブルに対して参照のみを行う監視です。監視テーブルに対して実行する SQL 文は（ select ）です。

  監視の結果以下の場合に異常とみなします。

  1. データベースへの接続や SQL 文の発行に対する応答で異常が通知された場合

- レベル 2 (update/select での監視)

  監視テーブルに対して更新も行う監視です。SQL 文の実行により最大 10 桁の数値データの書き込みと読み込みを実行します。監視テーブルに対して実行する SQL 文は（ update / select ）です。

  監視開始時に監視テーブルを自動で作成した場合、監視テーブルに対して実行する SQL 文は（ create / insert ）です。

  監視の結果以下の場合に異常とみなします。

  1. データベースへの接続や SQL 文の発行に対する応答で異常が通知された場合
  2. 書き込んだデータと読み込んだデータが一致していない場合

- レベル 3 (毎回 create/drop も行う)

  監視テーブルに対しての更新に加え監視テーブルの作成・削除も毎回行います。SQL 文の実行により最大 10 桁の数値データの書き込みと読み込みを実行します。監視テーブルに対して実行する SQL 文は（ create / insert / select / drop ）です。

  監視の結果以下の場合に異常とみなします。

  1. データベースへの接続や SQL 文の発行に対する応答で異常が通知された場合
  2. 書き込んだデータと読み込んだデータが一致していない場合

6.29 Tuxedo モニタリソースの設定

Tuxedo モニタリソースは、サーバ上で動作する Tuxedo を監視するモニタリソースです。

6.29.1 監視 (固有) タブ

アプリケーションサーバ名 (255 バイト以内)

監視するアプリケーションサーバ名を設定します。必ず設定してください。

既定値 ： BBL

TUXCONFIG ファイル (1023 バイト以内)

Tuxedo の配置ファイル名を設定します。必ず設定してください。

既定値 ： なし

ライブラリパス (1023 バイト以内)

Tuxedo のライブラリパスを設定します。必ず設定してください。

既定値 ： /home/Oracle/tuxedo/tuxedo12.1.3.0.0/lib/libtux.so

6.29.2 Tuxedo モニタリソースの注意事項

動作確認済みの Tuxedo のバージョンについては、『インストールガイド』の「CLUSTERPRO X SingleServerSafe について」の「監視オプションの動作確認済アプリケーション情報」を参照してください。

Tuxedo のライブラリ (libtux.so など) が存在しない場合、監視を行うことができません。

6.29.3 Tuxedo モニタリソースの監視方法

Tuxedo モニタリソースは、以下の監視を行います。

Tuxedo の API を利用して、アプリケーションサーバの監視を実行します。

監視の結果、以下の場合に異常とみなします。

1. アプリケーションサーバへの接続や状態取得に対する応答で異常が通知された場合

6.30 WebLogic モニタリソースの設定

WebLogic モニタリソースは、サーバ上で動作する WebLogic を監視するモニタリソースです。

6.30.1 監視 (固有) タブ

IP アドレス (79 バイト以内)

監視するサーバの IP アドレスを設定します。必ず設定してください。

既定値 ： 127.0.0.1

ポート番号 (1～65535)

サーバに接続する際のポート番号を設定します。必ず設定してください。

既定値 ： 7002

監視方式

サーバの監視方式を設定します。必ず設定してください。

既定値 ： RESTful API

プロトコル

監視するサーバのプロトコルを設定します。[監視方式] に RESTful API を選択した場合に必ず選択してください。

既定値 ： HTTP

ユーザ名 (255 バイト以内)

WebLogic のユーザ名を設定します。[監視方式] に RESTful API を選択した場合に必ず入力してください。

既定値 ： weblogic

パスワード (255 バイト以内)

WebLogic のパスワードを設定します。[監視方式] に RESTful API を選択した場合に必要に応じて入力してください。

既定値 ： なし

アカウントの隠蔽

ユーザ名とパスワードを直接指定する場合は「しない」を、ファイル内に記述する場合は「する」を指定してください。必ず設定してください。

既定値 ： しない

コンフィグファイル (1023 バイト以内)

ユーザ情報を保持しているファイル名を設定します。アカウントの隠蔽「する」の場合、必ず設定してください。

既定値 ： なし

キーファイル名 (1023 バイト以内)

コンフィグファイルパスにアクセスするためのパスワードを保存しているファイル名を、フルパスで設定します。アカウントの隠蔽「する」の場合、必ず設定してください。

既定値 ： なし

ユーザ名 (255 バイト以内)

WebLogic のユーザ名を設定します。アカウントの隠蔽「しない」の場合、必ず設定してください。

既定値 ：weblogic

パスワード (255 バイト以内)

WebLogic のパスワードを設定します。

既定値 ： なし

認証方式

アプリケーションサーバに接続する際の認証方式を設定します。必ず設定してください。

SSL 通信を用いた監視を行いたい場合、[認証方式] に [DemoTrust] または [CustomTrust] を指定してください。

[DemoTrust]、[CustomTrust] のいずれを選択するかは、WebLogic Administration Console 上の設定により異なります。

WebLogic Administration Console の [キーストア] が [デモ・アイデンティティとデモ信頼] の場合、[DemoTrust] を指定してください。この場合、[キーストアファイル] の設定は不要です。

WebLogic Administration Console の [キーストア] が [カスタム・アイデンティティとカスタム信頼] の場合、[CustomTrust] を指定してください。この場合、[キーストアファイル] の設定が必要です

既定値 ： DemoTrust

キーストアファイル (1023 バイト以内)

SSL 認証時の認証ファイルを設定します。認証方式が「CustomTrust」の場合、必ず設定してください。WebLogic Administration Console 上の [カスタム・アイデンティティ・キーストア] で指定しているファイルを設定してください。

既定値 ： なし

ドメイン環境ファイル (1023 バイト以内)

WebLogic のドメイン環境ファイル名を設定します。必ず設定してください。

既定値 ：/home/Oracle/product/Oracle_Home/user_projects/domains/base_domain/bin/setDomainEnv.sh

追加コマンドオプション (1023 バイト以内)

[webLogic.WLST] コマンドへ渡すオプションを変更する場合に設定します。

既定値 ： -Dwlst.offline.log=disable -Duser.language=en_US

6.30.2 WebLogic モニタリソースの注意事項

動作確認済みの WebLogic のバージョンについては、『インストールガイド』の「CLUSTERPRO X SingleServerSafe について」の「監視オプションの動作確認済アプリケーション情報」を参照してください。

本モニタリソースで 監視方式 に [WLST] を選択した場合は、監視を行うために JAVA 環境が必要です。アプリケーションサーバシステムは JAVA の機能を利用しているため、JAVA のストールなどが発生した場合も異常とみなすことがあります。

WebLogic 起動時にすぐに動作できない場合は異常とみなしてしまうため、[監視開始待ち時間] で調整してください。もしくは、WebLogic を先に起動するようにしてください (例：監視の対象リソースに、WebLogic を起動する EXEC リソースを指定)。

6.30.3 WebLogic モニタリソースの監視方法

WebLogic モニタリソースは、以下の監視を行います。

- 監視方式：RESTful API を選択した場合

  WebLogic では WebLogic RESTful 管理サービス という RESTful API が用意されています。

  この RESTful API を通して アプリケーションサーバの監視を実行します。

  監視の結果、以下の応答で異常が通知された場合に異常とみなします。

  1. RESTful API の応答で異常が通知された場合

  注釈: 監視方式：WLST と比較して、監視時のアプリケーションサーバの CPU 負荷を低減できます。

- 監視方式：WLST を選択した場合

  [weblogic.WLST] コマンドを利用して connect を行うことで、アプリケーションサーバの監視を実行します。

  監視の結果、以下の場合に異常とみなします。

  1. connect の応答で異常が通知された場合

  [認証方式] により以下の動作となります。

  - DemoTrust: WebLogic のデモ用認証ファイルを使用した SSL 認証方式
  - CustomTrust: ユーザ作成認証ファイルを使用した SSL 認証方式
  - Not Use SSL: SSL 認証を行わない

6.31 WebSphere モニタリソースの設定

WebSphere モニタリソースは、サーバ上で動作する WebSphere を監視するモニタリソースです。

6.31.1 監視 (固有) タブ

アプリケーションサーバ名 (255 バイト以内)

監視するアプリケーションサーバ名を設定します。必ず設定してください。

既定値 ： server1

プロファイル名 (1023 バイト以内)

監視するアプリケーションサーバのプロファイル名を設定します。必ず設定してください。

既定値 ： default

ユーザ名 (255 バイト以内)

WebSphere のユーザ名を設定します。必ず設定してください。

既定値 ：なし

パスワード (255 バイト以内)

WebSphere のパスワードを設定します。

既定値 ： なし

インストールパス (1023 バイト以内)

WebSphere のインストールパスを設定します。必ず設定してください。

既定値 ： /opt/IBM/WebSphere/AppServer

6.31.2 WebSphere モニタリソースの注意事項

動作確認済みの WebSphere のバージョンについては、『インストールガイド』の「CLUSTERPRO X SingleServerSafe について」の「監視オプションの動作確認済アプリケーション情報」を参照してください。

本モニタリソースで監視を行うためには JAVA 環境が必要です。アプリケーションサーバシステムは JAVA の機能を利用しているため、JAVA のストールなどが発生した場合も異常とみなすことがあります。

6.31.3 WebSphere モニタリソースの監視方法

WebSphere モニタリソースは、以下の監視を行います。
WebSphere の serverStatus.sh コマンドを利用して、アプリケーションサーバの監視を実行します。
監視の結果、以下の場合に異常とみなします。

1. 取得したアプリケーションサーバの状態で異常が通知された場合

6.32 WebOTX モニタリソースの設定

WebOTX モニタリソースは、サーバ上で動作する WebOTX を監視するモニタリソースです。

6.32.1 監視 (固有) タブ

接続先 (255 バイト以内)

監視するサーバのサーバ名を設定します。必ず設定してください。

既定値 ： localhost

ポート番号 (1～65535)

サーバに接続する際のポート番号を設定します。必ず設定してください。

WebOTX ユーザドメインを監視する場合、WebOTX ドメインの管理ポート番号を設定してください。管理ポート番号とは、ドメイン作成時に <ドメイン名>.properties の domain.admin.port にて設定したポート番号です。<ドメイン名>.properties の詳細については WebOTX のドキュメントを参照してください。

既定値 ： 6212

ユーザ名 (255 バイト以内)

WebOTX のユーザ名を設定します。必ず設定してください。
WebOTX ユーザドメインを監視する場合、WebOTX ドメインのログインユーザ名を設定してください。

既定値 ：なし

パスワード (255 バイト以内)

WebOTX のパスワードを設定します。

既定値 ： なし

インストールパス (1023 バイト以内)

WebOTX のインストールパスを設定します。必ず設定してください。

既定値 ： /opt/WebOTX

6.32.2 WebOTX モニタリソースの注意事項

動作確認済みの WebOTX のバージョンについては、『インストールガイド』の「CLUSTERPRO X SingleServerSafe について」の「監視オプションの動作確認済アプリケーション情報」を参照してください。

本モニタリソースで監視を行うためには JAVA 環境が必要です。アプリケーションサーバシステムは JAVA の機能を利用しているため、JAVA のストールなどが発生した場合も異常とみなすことがあります。

6.32.3 WebOTX モニタリソースの監視方法

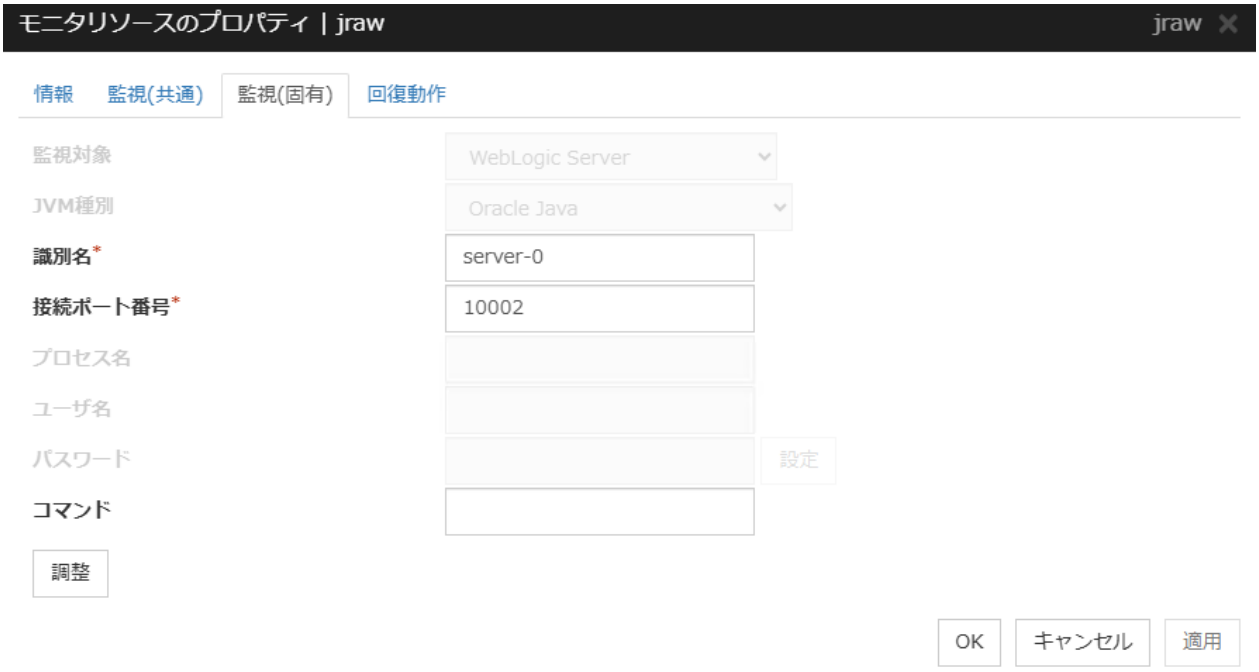
WebOTX モニタリソースは、以下の監視を行います。
WebOTX の otxadmin.sh コマンドを利用して、アプリケーションサーバの監視を実行します。
監視の結果、以下の場合に異常とみなします。

1. 取得したアプリケーションサーバの状態で異常が通知された場合

6.33 JVM モニタリソースの設定

JVM モニタリソースは、サーバ上で動作する Java VM やアプリケーションサーバが使用するリソースの利用情報を監視するモニタリソースです。

6.33.1 監視 (固有) タブ



監視対象

監視対象をリストから選択します。WebSAM SVF for PDF、WebSAM Report Director Enterprise、WebSAM Universal Connect/X を監視する場合は、[WebSAM SVF] を選択してください。自製の Java アプリケーションを監視する場合は、[Java アプリケーション] を選択してください。

JBoss Enterprise Application Platform のスタンドアローンモードを監視する場合は [JBoss]、JBoss Enterprise Application Platform のドメインモードを監視する場合は「JBoss ドメインモード」を選択してください。

既定値 ： なし

JVM 種別

監視対象のアプリケーションが動作する Java VM をリストから選択します。

Java 8 および OpenJDK 8 以降の場合は、[Oracle Java(usage monitoring)] を選択してください。Java 8 では以下の仕様変更がありました。

- 非ヒープ領域における各メモリの最大値が取得できなくなりました。

- Perm Gen は Metaspace に変更されました。
- Compressed Class Space が追加されました。

そのため、Java 8 では [メモリ] タブの監視項目は以下に変更となります。

- 使用率監視は使用量監視に変更となります。
- [Perm Gen]、Perm Gen[shared-ro]、Perm Gen[shared-rw] は監視できません。チェックボックスはオフにしてください。
- [Metaspace]、[Compressed Class Space] を監視可能です。

Java 9 では以下の仕様変更がありました。

- Code Cache が分割されました。

そのため、Java 9 では [メモリ] タブの監視項目は以下に変更となります。

- [Code Cache] は監視できません。チェックボックスはオフにしてください。
- [CodeHeap non-nmethods]、[CodeHeap profiled]、[CodeHeap non-profiled] を監視可能です。

監視対象別では以下を指定可能です。

- 監視対象が [WebLogic Server] の場合

  [Oracle Java]、[Oracle Java(usage monitoring)]、[Oracle JRockit] が選択可能です。
- 監視対象が [Tomcat] の場合

  [Oracle Java]、[Oracle Java(usage monitoring)]、[OpenJDK] が選択可能です。
- 監視対象が [WebLogic Server] [Tomcat] 以外の場合

  [Oracle Java]、[Oracle Java(usage monitoring)] が選択可能です。

既定値 ： なし

識別名 (255 バイト以内)

識別名とは、JVM モニタリソースの JVM 運用ログに監視対象の情報を出力する際に、別の JVM モニタリソースと識別するために設定します。そのため、JVM モニタリソース間で一意の文字列を設定してください。必ず設定してください。

- 監視対象が「WebLogic Server」の場合

  「6.33.18. *WebLogic Server* を監視するには 」の 2 を参照して、監視対象のサーバインスタンス名を設定してください。
- 監視対象が「WebOTX プロセスグループ」の場合

  プロセスグループ名を設定してください。
- 監視対象が「WebOTX ドメインエージェント」の場合

ドメイン名を設定してください。

- 監視対象が「JBoss」「JBoss ドメインモード」の場合
  「 6.33.23. *JBoss* を監視するには 」を参照して設定してください。
- 監視対象が「Tomcat」の場合
  「 6.33.24. *Tomcat* を監視するには 」を参照して設定してください。
- 監視対象が「WebOTX ESB」の場合
  「WebOTX プロセスグループ」の場合と同じです。
- 監視対象が「WebSAM SVF」の場合
  「 6.33.25. *SVF* を監視するには 」を参照して設定してください。
- 監視対象が「Java アプリケーション」の場合
  監視対象の Java VM プロセスを一意に識別可能な文字列を指定してください。

既定値 ： なし

接続ポート番号 (1024〜65535)

JVM モニタリソースが、監視対象 Java VM と JMX 接続を行う際に使用するポート番号を設定します。JVM モニタリソースは監視対象 Java VM に JMX 接続を行うことにより情報を取得します。そのため JVM モニタリソースを登録する場合は、監視対象 Java VM に JMX 接続用ポートを開放する設定を行う必要があります。必ず設定してください。42424〜61000 は推奨しません。

- 監視対象が「WebLogic Server」の場合
  接続ポート番号は「 6.33.18. *WebLogic Server* を監視するには 」の 6 を参照して設定してください。
- 監視対象が「WebOTX プロセスグループ」の場合
  「 6.33.21. *WebOTX* プロセスグループの *Java* プロセスを監視するには 」を参照して設定してください。
- 監視対象が「WebOTX ドメインエージェント」の場合
  "(WebOTX インストールパス)/<ドメイン名>.properties"の"domain.admin.port"を設定してください。
- 監視対象が「JBoss」の場合
  「 6.33.23. *JBoss* を監視するには 」を参照して設定してください。
- 監視対象が「JBoss ドメインモード」の場合
  設定不要です。
- 監視対象が「Tomcat」の場合
  「 6.33.24. *Tomcat* を監視するには 」を参照して設定してください。
- 監視対象が「WebOTX ESB」の場合
  「WebOTX プロセスグループ」の場合と同じです。

- 監視対象が「WebSAM SVF」の場合

  「 6.33.25. *SVF* を監視するには 」を参照して設定してください。

- 監視対象が「Java アプリケーション」の場合

  接続ポート番号は監視対象である Java アプリケーションに確認の上、設定してください。

既定値 ： なし

プロセス名 (1024 バイト以内)

プロセス名とは、JVM モニタリソースが、監視対象 Java VM と JMX 接続を行う際に別の JVM モニタリソースと識別するために設定します。そのため、JVM モニタリソース間で一意の文字列を設定してください。

- 監視対象が「JBoss ドメインモード」以外の場合

  接続ポート番号] により監視対象 Java VM が識別可能なため、設定不要です。内部バージョン 3.3.5-1 までは仮想メモリ使用量を取得する際や JVM 運用ログに監視対象の情報を出力する際にも本パラメータを使用し識別していたため、指定が必要でした。しかし、内部バージョン 4.0.0-1 以降は [仮想メモリ使用量を監視する] が削除となったため、設定できません。

- 監視対象が「JBoss ドメインモード」の場合

  「 6.33.23. *JBoss* を監視するには 」を参照して設定してください。

既定値 ： なし

ユーザ名 (255 バイト以内)

監視対象の Java VM に接続する管理ユーザ名を設定します。

- 監視対象に [WebOTX ドメインエージェント] を選択した場合

  "/opt/WebOTX/<**ドメイン名**>.properties"の"domain.admin.user"の値を設定してください。

- 監視対象が [WebOTX ドメインエージェント] 以外の場合

  設定できません。

既定値 ：なし

パスワード (255 バイト以内)

監視対象の Java VM に接続する管理ユーザのパスワードを設定します。

- 監視対象に [WebOTX ドメインエージェント] を選択した場合

  "/opt/WebOTX/<**ドメイン名**>.properties"の"domain.admin.passwd"の値を設定してください。

- 監視対象が [WebOTX ドメインエージェント] 以外の場合

  設定できません。

既定値 ： なし

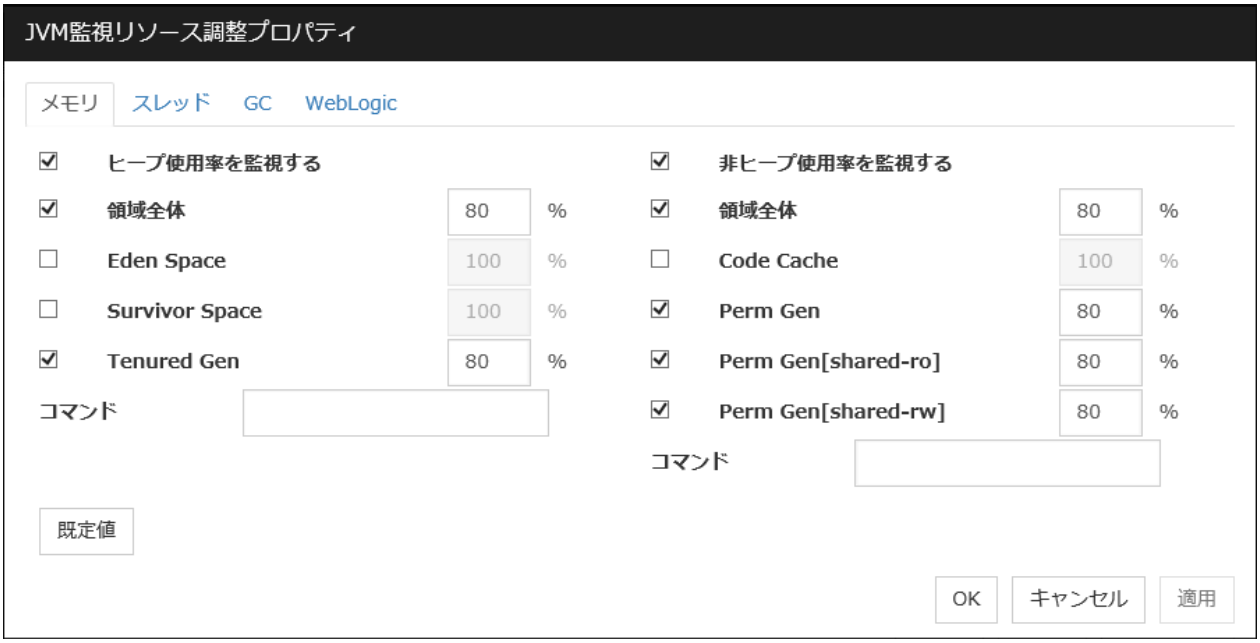
コマンド (255 バイト以内)

監視対象の Java VM 異常検出時に、実行するコマンドを設定します。異常の原因別に実行するコマンドおよび引数の指定が可能です。絶対パスで指定してください。また、実行ファイル名は二重引用符 ("") で括ってください。例)"/usr/local/bin/command" arg1 arg2 ここでは監視対象 Java VM に接続できない場合や使用リソース量の取得における異常検出時に、実行するコマンドを設定します。「 6.33.17. 異常検出時に障害原因別にコマンドを実行するには 」も参照してください。

既定値 ： なし

さらに [調整] ボタンを選択すると以下の内容がポップアップダイアログに表示されます。以下の説明に従い詳細設定を行います。

6.33.2 メモリタブ（[JVM 種別] で [Oracle Java]、[OpenJDK] 選択時）



ヒープ使用率を監視する

監視対象の Java VM が使用する Java ヒープ領域の使用率の監視設定をします。

- チェックボックスがオン (既定値)

  監視します。

- チェックボックスがオフ

  監視しません。

領域全体 (1～100)

監視対象の Java VM が使用する Java ヒープ領域の使用率のしきい値を設定します。

既定値 ： 80[%]

Eden Space (1〜100)

監視対象の Java VM が使用する Java Eden Space の使用率のしきい値を設定します。GC 方式として G1 GC を指定している場合、G1 Eden Space と読み替えてください。

既定値 ： 100[%]

Survivor Space (1〜100)

監視対象の Java VM が使用する Java Survivor Space の使用率のしきい値を設定します。GC 方式として G1 GC を指定している場合、G1 Survivor Space と読み替えてください。

既定値 ： 100[%]

Tenured Gen (1〜100)

監視対象の Java VM が使用する Java Tenured(Old) Gen 領域の使用率のしきい値を設定します。GC 方式として G1 GC を指定している場合、G1 Old Gen と読み替えてください。

既定値 ： 80[%]

非ヒープ使用率を監視する

監視対象の Java VM が使用する Java 非ヒープ領域の使用率の監視設定をします。

- チェックボックスがオン (既定値)
  監視します。
- チェックボックスがオフ
  監視しません。

領域全体 (1〜100)

監視対象の Java VM が使用する Java 非ヒープ領域の使用率のしきい値を設定します。

既定値 ： 80[%]

Code Cache (1〜100)

監視対象の Java VM が使用する Java Code Cache 領域の使用率のしきい値を設定します。

既定値 ： 100[%]

Perm Gen (1〜100)

監視対象の Java VM が使用する Java Perm Gen 領域の使用率のしきい値を設定します。

既定値 ： 80[%]

Perm Gen[shared-ro] (1〜100)

監視対象の Java VM が使用する Java Perm Gen [shared-ro] 領域の使用率のしきい値を設定します。

Java Perm Gen [shared-ro] 領域は監視対象 Java VM の起動オプションに -client -Xshare:on -XX:+UseSerialGC を付与して起動している場合に使用される領域です。

既定値 ： 80[%]

Perm Gen[shared-rw] (1〜100)

監視対象の Java VM が使用する Java Perm Gen [shared-rw] 領域の使用率のしきい値を設定します。

Java Perm Gen [shared-rw] 領域は監視対象 Java VM の起動オプションに -client -Xshare:on -XX:+UseSerialGC を付与して起動している場合に使用される領域です。

既定値 ： 80[%]

コマンド (255 バイト以内)

監視対象の Java VM 異常検出時に、実行するコマンドを設定します。異常の原因別に実行するコマンドおよび引数の指定が可能です。絶対パスで指定してください。また、実行ファイル名は二重引用符 ("") で括ってください。例)"/usr/local/bin/command" arg1 arg2

ここでは監視対象 Java VM の Java ヒープ領域、Java 非ヒープ領域における異常検出時に、実行するコマンドを設定します。

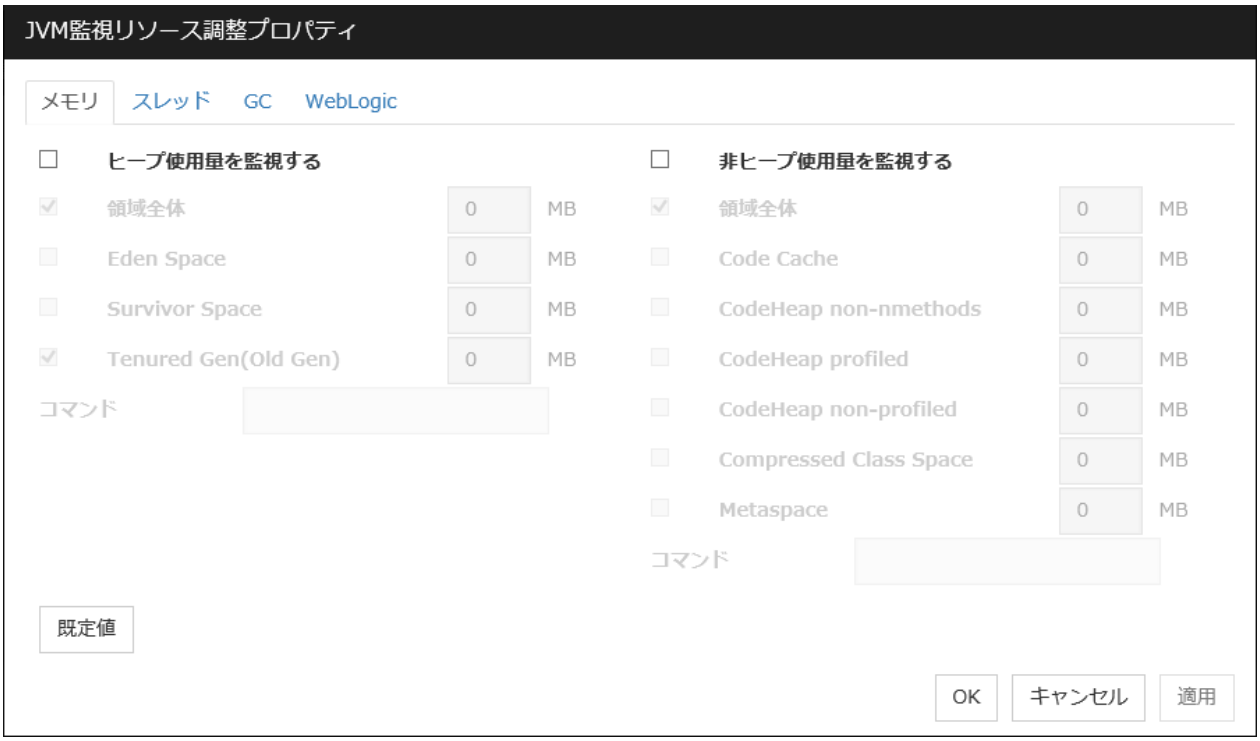
「 6.33.17. 異常検出時に障害原因別にコマンドを実行するには 」も参照してください。

既定値 ： なし

既定値

[既定値] ボタンをクリックすると全ての項目に既定値が設定されます。

6.33.3 メモリタブ（[JVM 種別] で [Oracle Java(usage monitoring)] 選択時）



ヒープ使用量を監視する

監視対象の Java VM が使用する Java ヒープ領域の使用量の監視設定をします。

- チェックボックスがオン

  監視します。

- チェックボックスがオフ (既定値)

  監視しません。

領域全体 (0〜102400)

監視対象の Java VM が使用する Java ヒープ領域の使用量のしきい値を設定します。0 の場合、監視しません。

既定値 ： 0[MB]

Eden Space (0〜102400)

監視対象の Java VM が使用する Java Eden Space の使用量のしきい値を設定します。0 の場合、監視しません。GC 方式として G1 GC を指定している場合、G1 Eden Space と読み替えてください。

既定値 ： 0[MB]

Survivor Space (0〜102400)

監視対象の Java VM が使用する Java Survivor Space の使用量のしきい値を設定します。0 の場合、監視しません。GC 方式として G1 GC を指定している場合、G1 Survivor Space と読み替えてください。

既定値 ： 0[MB]

Tenured Gen (0〜102400)

監視対象の Java VM が使用する Java Tenured(Old) Gen 領域の使用量のしきい値を設定します。0 の場合、監視しません。GC 方式として G1 GC を指定している場合、G1 Old Gen と読み替えてください。

既定値 ： 0[MB]

非ヒープ使用量を監視する

監視対象の Java VM が使用する Java 非ヒープ領域の使用量の監視設定をします。

- チェックボックスがオン
  監視します。
- チェックボックスがオフ (既定値)
  監視しません。

領域全体 (0〜102400)

監視対象の Java VM が使用する Java 非ヒープ領域の使用量のしきい値を設定します。0 の場合、監視しません。

既定値 ： 0[MB]

Code Cache (0〜102400)

監視対象の Java VM が使用する Java Code Cache 領域の使用量のしきい値を設定します。0 の場合、監視しません。

既定値 ： 0[MB]

CodeHeap non-nmethods (0〜102400)

監視対象の Java VM が使用する Java CodeHeap non-nmethods 領域の使用量のしきい値を設定します。0 の場合、監視しません。

既定値 ： 0[MB]

CodeHeap profiled (0〜102400)

監視対象の Java VM が使用する Java CodeHeap profiled nmethods 領域の使用量のしきい値を設定します。0 の場合、監視しません。

既定値 ： 0[MB]

CodeHeap non-profiled (0〜102400)

監視対象の Java VM が使用する Java CodeHeap non-profiled nmethods 領域の使用量のしきい値を設定します。0 の場合、監視しません。

既定値 ： 0[MB]

Compressed Class Space (0〜102400)

監視対象の Java VM が使用する Compressed Class Space 領域の使用量のしきい値を設定します。0 の場合、監視しません。

既定値 ： 0[MB]

Metaspace (0〜102400)

監視対象の Java VM が使用する Metaspace 領域の使用量のしきい値を設定します。0 の場合、監視しません。

既定値 ： 0[MB]

コマンド (255 バイト以内)

監視対象の Java VM 異常検出時に、実行するコマンドを設定します。異常の原因別に実行するコマンドおよび引数の指定が可能です。絶対パスで指定してください。また、実行ファイル名は二重引用符 ("") で括ってください。例)"/usr/local/bin/command" arg1 arg2

ここでは監視対象 Java VM の Java ヒープ領域、Java 非ヒープ領域における異常検出時に、実行するコマンドを設定します。

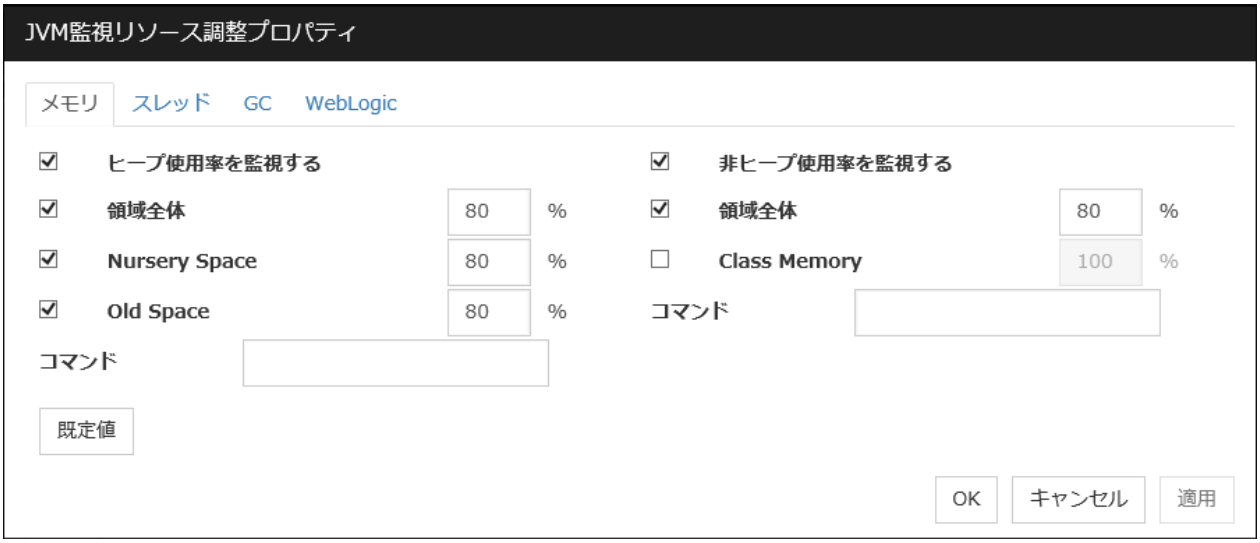
「 6.33.17. 異常検出時に障害原因別にコマンドを実行するには 」も参照してください。

既定値 ： なし

既定値

[既定値] ボタンをクリックすると全ての項目に既定値が設定されます。

6.33.4 メモリタブ（Oracle JRockit 選択時）



[JVM 種別] で [JRockit] 選択時のみ表示されます。

ヒープ使用率を監視する

監視対象の Java VM が使用する Java ヒープ領域の使用率の監視設定をします。

- チェックボックスがオン (既定値)
  監視します。
- チェックボックスがオフ
  監視しません。

領域全体 (1～100)

監視対象の Java VM が使用する Java ヒープ領域の使用率のしきい値を設定します。

既定値 ： 80[%]

Nursery Space (1～100)

監視対象の JRockit JVM が使用する Java Nursery Space の使用率のしきい値を設定します。

既定値 ： 80[%]

Old Space (1～100)

監視対象の JRockit JVM が使用する Java Old Space の使用率のしきい値を設定します。

既定値 ： 80[%]

非ヒープ使用率を監視する

監視対象の Java VM が使用する Java 非ヒープ領域の使用率の監視設定をします。

- チェックボックスがオン (既定値)
  監視します。
- チェックボックスがオフ
  監視しません。

領域全体 (1〜100)

監視対象の Java VM が使用する Java ヒープ領域の使用率のしきい値を設定します。

既定値 ： 80[%]

Class Memory (1〜100)

監視対象の JRockit JVM が使用する Java Class Memory の使用率のしきい値を設定します。

既定値 ： 100[%]

コマンド (255 バイト以内)

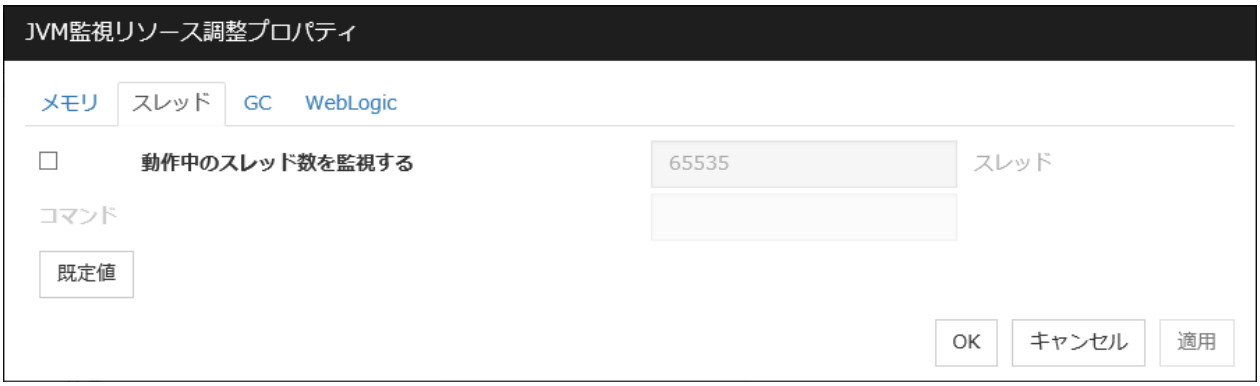
監視対象の Java VM 異常検出時に、実行するコマンドを設定します。異常の原因別に実行するコマンドおよび引数の指定が可能です。絶対パスで指定してください。また、実行ファイル名は二重引用符 ("") で括ってください。例)"/usr/local/bin/command" arg1 arg2 ここでは監視対象 Java VM の Java ヒープ領域、Java 非ヒープ領域における異常検出時に、実行するコマンドを設定します。「6.33.17. 異常検出時に障害原因別にコマンドを実行するには」も参照してください。

既定値 ： なし

既定値

[既定値] ボタンをクリックすると全ての項目に既定値が設定されます。

6.33.5 スレッドタブ



動作中のスレッド数を監視する (1〜65535)

監視対象の Java VM で現在動作中のスレッド上限数のしきい値を設定します。

既定値 ： 65535[スレッド]

コマンド (255 バイト以内)

監視対象の Java VM 異常検出時に、実行するコマンドを設定します。異常の原因別に実行するコマンドおよび引数の指定が可能です。絶対パスで指定してください。また、実行ファイル名は二重引用符 ("") で括ってください。例)"/usr/local/bin/command" arg1 arg2 ここでは監視対象 Java VM で現在動作中のスレッド数における異常検出時に、実行するコマンドを設定します。「 6.33.17. 異常検出時に障害原因別にコマンドを実行するには 」も参照してください。

既定値 ： なし

既定値

[既定値] ボタンをクリックすると全ての項目に既定値が設定されます。

6.33.6 GC タブ

Full GC 実行時間を監視する (1〜65535)

監視対象の Java VM において、前回計測以降の Full GC 実行時間のしきい値を設定します。Full GC 実行時間とは、前回計測以降の Full GC 発生回数で割った平均値です。

前回計測以降の Full GC 実行時間 3000 ミリ秒、Full GC 発生回数 3 回の場合を異常と判定したい場合、1000 ミリ秒以下を設定してください。

既定値 ： 65535[ミリ秒]

Full GC 発生回数を監視する (1〜65535)

監視対象の Java VM において、前回計測以降の Full GC 発生回数のしきい値を設定します。

既定値 ： 1(回)

コマンド (255 バイト以内)

監視対象の Java VM 異常検出時に、実行するコマンドを設定します。異常の原因別に実行するコマンドおよび引数の指定が可能です。絶対パスで指定してください。また、実行ファイル名は二重引用符 ("") で括ってください。例)"/usr/local/bin/command" arg1 arg2 ここでは監視対象 Java VM の Full GC 実行時間や Full GC 発生回数における異常検出時に、実行するコマンドを設定します。「 6.33.17. 異常検出時に障害原因別にコマンドを実行するには 」も参照してください。

既定値 ： なし

既定値

[既定値] ボタンをクリックすると全ての項目に既定値が設定されます。

6.33.7 WebLogic タブ

[監視対象] で [WebLogic Server] 選択時のみ表示されます。

ワークマネージャのリクエストを監視する

WebLogic Server でワークマネージャの待機リクエスト状態の監視設定をします。

- チェックボックスがオン
  監視します。
- チェックボックスがオフ (既定値)
  監視しません。

監視対象ワークマネージャ

監視対象の WebLogic Server に対して監視したいアプリケーションのワークマネージャ名を設定します。

ワークマネージャ監視を実施する場合、必ず設定してください。

*App*1[*WM1,WM2*,…];*App*2[*WM1,WM2*,…];…

App と *WM* にて指定可能な文字は ASCII 文字です。(Shift_JIS コード 0x005C と 0x00A1～0x00DF を除く)

アプリケーション アーカイブのバージョンを持つアプリケーションを指定する場合、*App* には「アプリケーション名#バージョン」を指定してください。

アプリケーション名に"["や"]"が付いている場合、"["や"]"の直前に「¥¥」を追加してください。

(例) アプリケーション名が app[2] の場合、app¥¥　[2¥¥　]

既定値 ： なし

リクエスト数 (1～65535)

監視対象の WebLogic Server のワークマネージャにおいて、待機リクエスト数のしきい値を設定します。

既定値 ： 65535

平均値 (1～65535)

監視対象の WebLogic Server のワークマネージャにおいて、待機リクエスト数の平均値のしきい値を設定します。

既定値 ： 65535

前回計測値からの増加率 (1～1024)

監視対象の WebLogic Server のワークマネージャにおいて、待機リクエスト数の前回計測以降の増分に対するしきい値を設定します。

既定値 ： 80[%]

スレッドプールのリクエストを監視する

監視対象の WebLogic Server のスレッドプールにおいて、待機リクエスト数 、実行リクエスト数の監視設定をします。リクエスト数とは、WebLogic Server 内部で処理待ちや実行した HTTP リクエスト数や、EJB の呼び出しや WebLogic Server 内部で行われる処理のリクエスト数を含みます。ただし、増加しても異常な状態とは判断できません。JVM 統計ログの採取をする場合に指定してください。

- チェックボックスがオン (既定値)
  監視します。
- チェックボックスがオフ
  監視しません。

待機リクエスト リクエスト数 (1～65535)

待機リクエスト数のしきい値を設定します。

既定値 ： 65535

待機リクエスト 平均値 (1〜65535)

待機リクエスト数の平均値のしきい値を設定します。

既定値 ： 65535

待機リクエスト 前回計測値からの増加率 (1〜1024)

待機リクエスト数の前回計測以降の増分に対するしきい値を設定します。

既定値 ： 80[%]

実行リクエスト リクエスト数 (1〜65535)

単位時間あたりに実行したリクエスト数のしきい値を設定します。

既定値 ： 65535

実行リクエスト 平均値 (1〜65535)

単位時間あたりに実行したリクエスト数の平均値のしきい値を設定します。

既定値 ： 65535

実行リクエスト 前回計測値からの増加率 (1〜1024)

単位時間あたりに実行したリクエスト数の前回計測以降の増分に対するしきい値を設定します。

既定値 ： 80[%]

コマンド (255 バイト以内)

監視対象の Java VM 異常検出時に、実行するコマンドを設定します。異常の原因別に実行するコマンドおよび引数の指定が可能です。絶対パスで指定してください。また、実行ファイル名は二重引用符 ("") で括ってください。例)"/usr/local/bin/command" arg1 arg2 ここでは WebLogic Server のワークマネージャのリクエストやスレッドプールのリクエストにおける異常検出時に、実行するコマンドを設定します。「 6.33.17. 異常検出時に障害原因別にコマンドを実行するには 」も参照してください。

既定値 ： なし

既定値

[既定値] ボタンをクリックすると全ての項目に既定値が設定されます。

6.33.8 JVM モニタリソースの注意事項

JVM モニタリソースを作成する前に [クラスタのプロパティ] の [JVM 監視] タブの [Java インストールパス] を前もって設定しておく必要があります。

監視対象のリソースには、WebLogic Server や WebOTX など Java VM 上で動作するアプリケーションサーバを指定してください。JVM モニタリソースの活性後、Java Resource Agent は監視を開始しますが、JVM モニタリソースの活性直後に監視対象 (WebLogic Server や WebOTX) がすぐに動作できない場合は、[監視開始待ち時間] で調整してください。

[監視 (共通)] - [リトライ回数] の設定は無効です。異常の検出を遅らせたい場合は、[クラスタ] プロパティ - [JVM 監視] タブ - [リソース計測設定] - [共通] - [リトライ回数] の設定を変更してください。

6.33.9 JVM モニタリソースの監視方法

JVM モニタリソースは、以下の監視を行います。

JMX(Java Management Extensions) を利用して、アプリケーションサーバの監視を実行します。

監視の結果、以下の場合に異常とみなします。

- 監視対象の Java VM やアプリケーションサーバに接続できない場合
- 取得した Java VM やアプリケーションサーバのリソース使用量がお客様定義のしきい値を規定回数 (異常判定しきい値) 連続して超えた場合

監視の結果、以下の場合に異常から正常へ復帰したとみなします。

- 回復動作後の監視を再開時にしきい値を下回った場合

注釈: Cluster WebUI の [クラスタログ収集] では、監視対象 (WebLogic Server や WebOTX) の設定ファイルおよびログファイルは収集されません。

図は JVM モニタリソースによる監視動作を表しています。

a) で監視対象の Java VM の監視を開始します。Java VM の監視には JMX（Java Management Extensions）を利用します。Java Resource Agent が JMX を通じて Java VM に対して定期的に使用リソース量を取得することで Java VM の状態をチェックします。

状態が正常から異常へ変化した場合、b) で Java VM の異常を検出したことを Cluster WebUI に表示します。状態とアラートを確認することができます。さらに c) で、障害があったことを syslog や JVM 運用ログへ通知します。アラートサービスをご利用の場合、E メール通報も可能です。

a) の後、状態が異常から正常に変化した場合、d) で Java VM の正常復帰を検出したことを Cluster WebUI に表示します。さらに e) で正常復旧した旨を syslog や JVM 運用ログへ通知します。

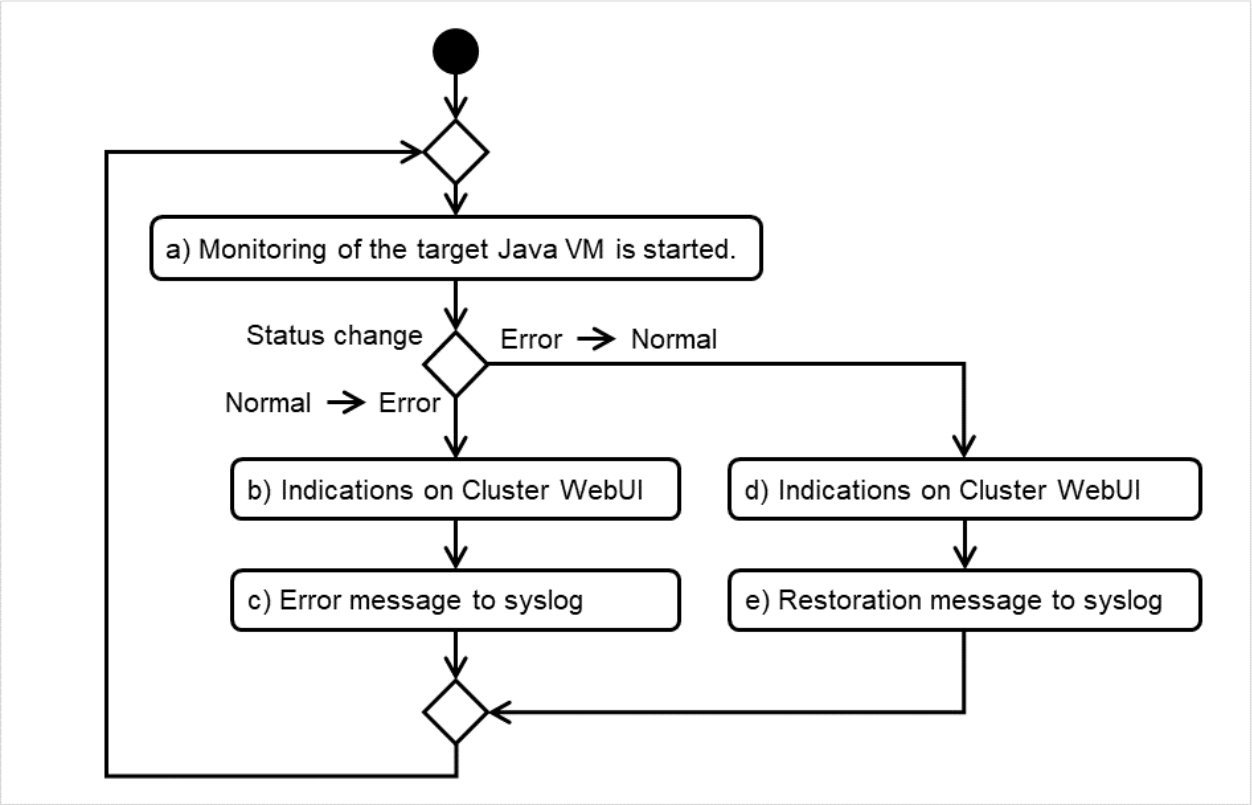


図 6.11　JVM モニタリソースによる監視フロー

基本的なしきい値超過時の動作は以下の通りです。

図の横軸は時間の経過を表しており、縦軸は監視のしきい値を超えた（Exceeded）か超えていない（Not exceeded）かを表しています。
ここで、監視時のしきい値を超える状態が異常判定しきい値回（図では 5 回）以上連続すると、異常と判断します。

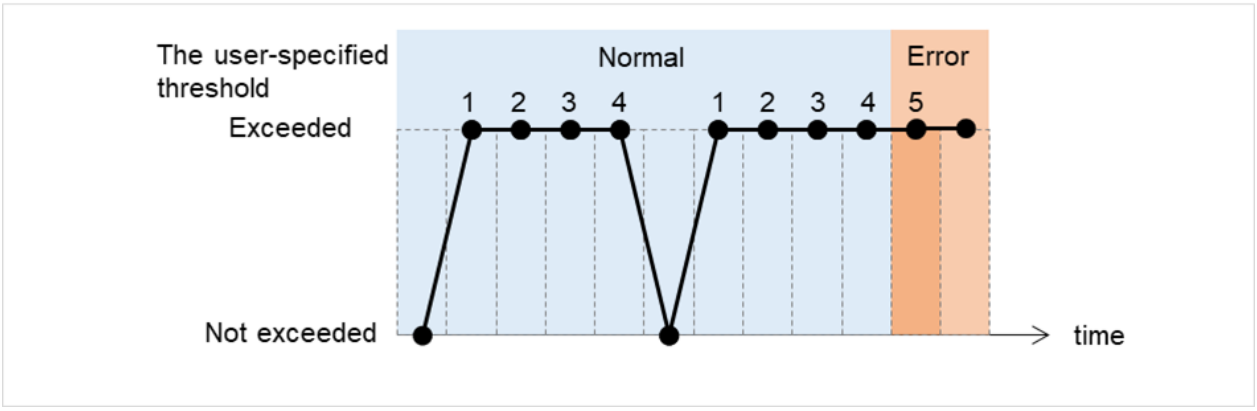


図 6.12　しきい値超過時の動作

異常が継続する場合は以下の通りです

しきい値の超過が異常判定しきい値回連続して発生した場合、異常状態と判断します。
異常状態と判断後、再度異常判定しきい値回連続してしきい値を超過していても、Cluster WebUI には再度アラートは表示されません。

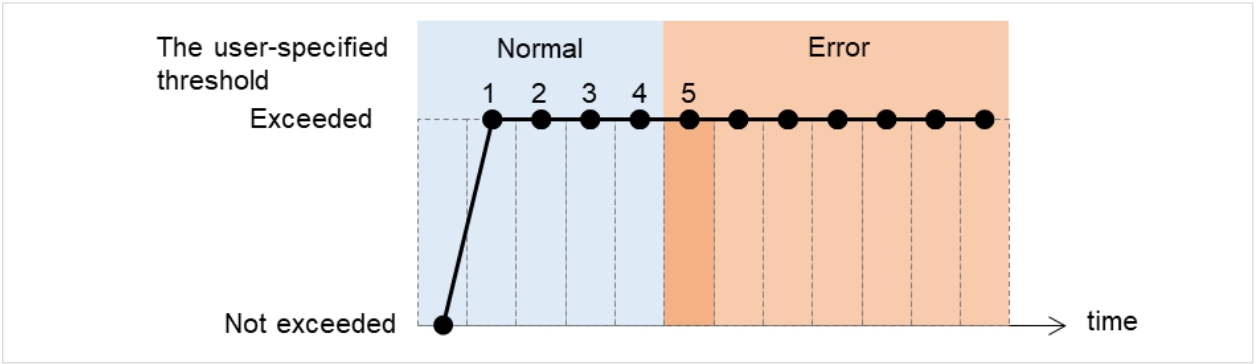


図 6.13　異常継続時の動作

Full GC(Garbage Collection) を監視する場合を例に説明します。

図の横軸は時間の経過を表しています。そして、図の上段は各監視タイミングで GC の発生を検出したか否かを示し、下段はそれぞれの時点で Full GC 検出が何回連続しているかを示しています。JVM モニタリソースは、異常判定しきい値回連続して Full GC が発生すると、モニタ異常を検出します。異常判定しきい値を 5 回に設定しているので、 Full GC 検出が 5 回に達した時点でモニタ異常を検出します。

Full GC はシステムに与える影響が大きいため、異常判定しきい値は 1 回に設定することを推奨します。

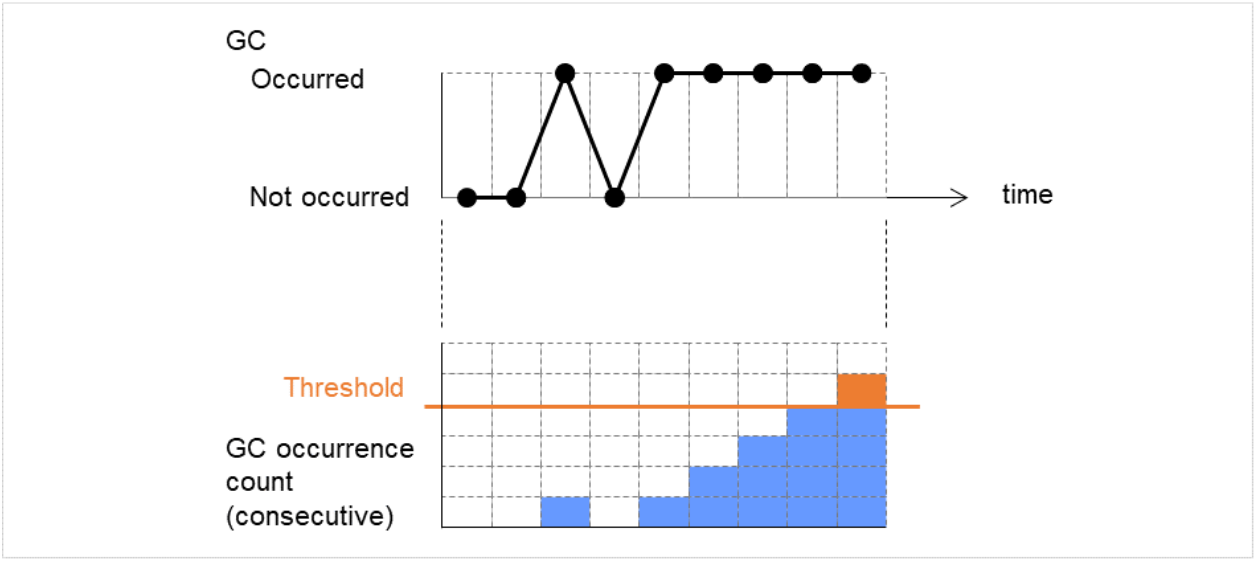


図 6.14　監視イメージ（異常判定しきい値を 5 回に設定した場合）

6.33.10 JVM 統計ログとは

JVM モニタリソースが収集する監視対象 Java VM の統計情報を保存したファイルが、JVM 統計ログです。ファイル形式は csv 形式です。作成場所は以下のとおりです。

<CLUSTERPRO インストールパス>/log/ha/jra/*.stat

下記の「監視項目」とは、JVM モニタリソースの [プロパティ]-[監視 (固有)] タブ内の設定項目を表します。

それぞれの監視項目について、[監視する] をチェックし、かつ閾値を設定した場合に統計情報を採取し、JVM 統計ログに情報を出力します。[監視する] をチェックしない場合、および [監視する] をチェックしたが閾値を設定しない場合は、JVM 統計ログには情報は出力されません。

監視項目と該当する JVM 統計ログは以下の通りです。

監視項目	該当する JVM 統計ログ
[メモリ] タブ-[ヒープ使用率を監視する] [メモリ] タブ-[非ヒープ使用率を監視する] [メモリ] タブ-[ヒープ使用量を監視する] [メモリ] タブ-[非ヒープ使用量を監視する]	jramemory.stat
[スレッド] タブ-[動作中のスレッド数を監視する]	jrathread.stat

次のページに続く

表 6.17 – 前のページからの続き

監視項目	該当する JVM 統計ログ
[GC] タブ-[Full GC 実行時間を監視する] [GC] タブ-[Full GC 発生回数を監視する]	jragc.stat
[WebLogic] タブ-[ワークマネージャのリクエストを監視する] [WebLogic] タブ-[スレッドプールのリクエストを監視する] 上記のいずれかがチェックされている場合、wlworkmanager.stat と wlthreadpool.stat の両方出力します。	wlworkmanager.stat wlthreadpool.stat

6.33.11 監視対象 Java VM の Java メモリ領域の使用量を確認する (jramemory.stat)

監視対象 Java VM の Java メモリ領域の使用量を記録するログファイルです。ファイル名はログ出力設定のローテーション方式により以下のいずれかになります。

- [クラスタのプロパティ] - [JVM 監視] タブ - [ログ出力設定] - [ローテーション方式] - [ファイルサイズ] を選択した場合：`jramemory<0 から始まる整数>.stat`
- [クラスタのプロパティ] - [JVM 監視] タブ - [ログ出力設定] - [ローテーション方式] - [時間] を選択した場合：`jramemory<YYYYMMDDhhmm>.stat`

フォーマットは以下の通りです。

No	フォーマット	説明
1	yyyy/mm/dd hh:mm:ss.SSS	ログを記録した日時を示します。
2	半角英数字記号	監視対象 Java VM の名称を示します。JVM モニタリソースの [プロパティ]-[監視固有] タブ-[識別名] で設定した値です。
3	半角英数字記号	Java メモリプールの名称です。詳細は「6.33.16. *Java* メモリプール名について」を参照してください。
4	半角英数字記号 Java メモリプールのタイプです。 Heap、Non-Heap	

次のページに続く

表 6.18 – 前のページからの続き

No	フォーマット	説明
5	半角数字	Java VM が起動時に OS に要求するメモリ量です。単位はバイトです。(init) 監視対象 Java VM の起動時、以下の Java VM 起動時オプションでサイズの指定が可能です。 ・HEAP：-Xms ・NON_HEAP パーマネント領域 (Perm Gen)：-XX:PermSize ・NON_HEAP コードキャッシュ領域 (Code Cache)：-XX:InitialCodeCacheSize
6	半角数字	Java VM が現在使用しているメモリ量です。単位はバイトです。(used)
7	半角数字	Java VM が現在使用することを保証しているメモリ量です。単位はバイトです。(committed) メモリの使用状況により増減しますが、必ず used 以上、max 以下になります。

次のページに続く

表 6.18 – 前のページからの続き

No	フォーマット	説明
8	半角数字	Java VM が使用できる最大メモリ量です。単位はバイトです。(max) 以下の Java VM 起動時オプションでサイズの指定が可能です。 ・HEAP：-Xmx ・NON_HEAP パーマネント領域 (Perm Gen)：-XX:MaxPermSize ・NON_HEAP コードキャッシュ領域 (Code Cache)：-XX:ReservedCodeCacheSize 例） java -XX:MaxPermSize=128m -XX:ReservedCodeCacheSize=128m javaAP 上記例では NON_HEAP の max は 128m+128m=256m になります。 (注意) -Xms と-Xmx に同じ値を指定すると、(init)>(max) となることがあります。これは HEAP の max が、-Xmx の指定によって確保される領域サイズから Survivor Space のサイズの半分を除いたサイズを示すためです。
9	半角数字	計測対象の Java VM が起動してから使用したメモリ量のピーク値です。Java メモリプールの名称が HEAP、NON_HEAP の場合、Java VM が現在使用しているメモリ量 (used) と同じになります。単位はバイトです。

次のページに続く

表 6.18 – 前のページからの続き

No	フォーマット	説明
10	半角数字	[JVM 種別] で [Oracle Java(usage monitoring)] 選択時は無視してください。 [JVM 種別] で [Oracle Java(usage monitoring)] 以外を選択時、Java メモリプールのタイプ (No.4 のフィールド) が HEAP の場合、max(No.8 のフィールド) ×しきい値 (%) のメモリ量です。単位はバイトです。Java メモリプールのタイプが HEAP 以外の場合、0 固定です。

6.33.12 監視対象 Java VM のスレッド稼働状況を確認する (jrathread.stat)

監視対象 Java VM のスレッド稼働状況を記録するログファイルです。ファイル名はログ出力設定のローテーション方式により以下のいずれかになります。

- [クラスタのプロパティ] - [JVM 監視] タブ - [ログ出力設定] - [ローテーション方式] - [ファイルサイズ] を選択した場合：`jrathread<0 から始まる整数>.stat`
- [クラスタのプロパティ] - [JVM 監視] タブ - [ログ出力設定] - [ローテーション方式] - [時間] を選択した場合：`jrathread<YYYYMMDDhhmm>.stat`

フォーマットは以下の通りです。

No	フォーマット	説明
1	yyyy/mm/dd hh:mm:ss.SSS	ログを記録した日時を示します。
2	半角英数字記号	監視対象 Java VM の名称を示します。JVM モニタリソースの [プロパティ]-[監視固有] タブ-[識別名] で設定した値です。
3	半角英数字記号	監視対象 Java VM で現在実行中のスレッド数を示します。
4	[半角数字: 半角数字:...]	監視対象 Java VM でデッドロックしているスレッド ID を示します。デッドロック数分 ID を繰り返します。

次のページに続く

表 6.19 – 前のページからの続き

No	フォーマット	説明
5	半角英数字記号	監視対象 Java VM でデッドロックしているスレッドの詳細情報を示します。スレッド数分、以下の形式で繰り返します。 スレッド名, スレッド ID, スレッド状態, UserTime, CpuTime, WaitedCount, WaitedTime, isInNative, isSuspended <改行> stacktrace<改行> : stacktrace<改行> stacktrace=ClassName, FileName, LineNumber, MethodName, isNativeMethod

6.33.13 監視対象 Java VM の GC 稼働状況を確認する (jragc.stat)

監視対象 Java VM の GC 稼働状況を記録するログファイルです。ファイル名はログ出力設定のローテーション方式により以下のいずれかになります。

- [クラスタのプロパティ] - [JVM 監視] タブ - [ログ出力設定] - [ローテーション方式] - [ファイルサイズ] を選択した場合：`jragc<0 から始まる整数>.stat`
- [クラスタのプロパティ] - [JVM 監視] タブ - [ログ出力設定] - [ローテーション方式] - [時間] を選択した場合：`jragc<YYYYMMDDhhmm>.stat`

JVM モニタリソースではコピー GC と Full GC の 2 種類の GC の情報を出力しています。
JVM モニタリソースでは、Oracle Java の場合は以下の GC について、Full GC として発生回数の増分をカウントしています。

- MarkSweepCompact
- PS MarkSweep
- ConcurrentMarkSweep
- G1 Old Generation

フォーマットは以下の通りです。

No	フォーマット	説明
1	yyyy/mm/dd hh:mm:ss.SSS	ログを記録した日時を示します。
2	半角英数字記号	監視対象 Java VM の名称を示します。JVM モニタリソースの [プロパティ]-[監視固有] タブ-[識別名] で設定した値です。
3	半角英数字記号	監視対象 Java VM の GC 名称を示します。 **監視対象 Java VM が Oracle Java の場合** 以下があります。 Copy MarkSweepCompact PS Scavenge PS MarkSweep ParNew ConcurrentMarkSweep G1 Young Generation G1 Old Generation G1 Concurrent GC(Java 20 以降の場合のみ出力) **監視対象 Java VM が Oracle JRockit の場合** 以下があります。 Garbage collection optimized for throughput Old Collector Garbage collection optimized for short pausetimes Old Collector Garbage collection optimized for deterministic pausetimes Old Collector Static Collector Static Old Collector Garbage collection optimized for throughput Young Collector

次のページに続く

表 6.20 – 前のページからの続き

No	フォーマット	説明
4	半角数字	監視対象 Java VM の起動直後から計測時点までの GC 発生回数を示します。JVM モニタリソースが監視を開始する前に発生した GC の発生回数も値に含みます。
5	半角数字	監視対象 Java VM の起動直後から計測時点までの GC 総実行時間を示します。単位はミリ秒です。JVM モニタリソースが監視を開始する前に発生した GC の実行時間も値に含みます。

6.33.14 WebLogic Server のワークマネージャの稼働状況を確認する (wlworkmanager.stat)

WebLogic Server のワークマネージャの稼働状況を記録するログファイルです。ファイル名はログ出力設定のローテーション方式により以下のいずれかになります。

- [クラスタのプロパティ] - [JVM 監視] タブ - [ログ出力設定] - [ローテーション方式] - [ファイルサイズ] を選択した場合：`wlworkmanager<0 から始まる整数>.stat`
- [クラスタのプロパティ] - [JVM 監視] タブ - [ログ出力設定] - [ローテーション方式] - [時間] を選択した場合：`wlworkmanager<YYYYMMDDhhmm>.stat`

フォーマットは以下の通りです。

No	フォーマット	説明
1	yyyy/mm/dd hh:mm:ss.SSS	ログを記録した日時を示します。
2	半角英数字記号	監視対象 Java VM の名称を示します。JVM モニタリソースの [プロパティ]-[監視固有] タブ-[識別名] で設定した値です。
3	半角英数字記号	アプリケーション名を示します。
4	半角英数字記号	ワークマネージャ名を示します。
5	半角数字	実行したリクエストの数を示します。
6	半角数字	待機しているリクエストの数を示します。

6.33.15 WebLogic Server のスレッドプールの稼働状況を確認する (wlthreadpool.stat)

WebLogic Server のスレッドプールの稼働状況を記録するログファイルです。ファイル名はログ出力設定のローテーション方式により以下のいずれかになります。

- [クラスタのプロパティ] - [JVM 監視] タブ - [ログ出力設定] - [ローテーション方式] - [ファイルサイズ] を選択した場合：`wlthreadpool<0 から始まる整数>.stat`
- [クラスタのプロパティ] - [JVM 監視] タブ - [ログ出力設定] - [ローテーション方式] - [時間] を選択した場合：`wlthreadpool<YYYYMMDDhhmm>.stat`

フォーマットは以下の通りです。

No	フォーマット	説明
1	yyyy/mm/dd hh:mm:ss.SSS	ログを記録した日時を示します。
2	半角英数字記号	監視対象 Java VM の名称を示します。JVM モニタリソースの [プロパティ]-[監視固有] タブ-[識別名] で設定した値です。
3	半角数字	実行したリクエストの総数を示します。
4	半角数字	処理待ちとなっているリクエスト数を示します。
5	半角数字	単位時間（秒）あたりのリクエスト処理数を示します。
6	半角数字	アプリケーションを実行するためのスレッドのトータル数を示します。
7	半角数字	アイドル状態となっているスレッドの数を示します。
8	半角数字	実行中のスレッド数を示します。
9	半角数字	スタンバイ状態となっているスレッド数を示します。

6.33.16 Java メモリプール名について

JVM 運用ログに出力するメッセージ中の memory_name として出力する Java メモリプール名、および JVM 統計ログ jramemory.stat 中に出力する Java メモリプール名について説明します。

Java メモリプール名として出力する文字列は、JVM モニタリソースで決定しているのではなく、監視対象 Java VM から受け取った文字列を出力しています。

また、Java VM としては仕様を公開していないため、Java VM のバージョンアップにより、予告なく変更される可能性があります。

そのため、メッセージ中の Java メモリプール名をメッセージ監視することは推奨いたしません。

下記の監視項目とは JVM モニタリソースの [プロパティ]-[監視 (固有)] タブ-[メモリ] タブ内の設定項目を表します。

以下に記載している Java メモリプール名は Oracle Java 、JRockit において実機確認した結果です。

[JVM 種別] に [Oracle Java] を選択、かつ監視対象 Java VM の起動オプションに「-XX:+UseSerialGC」が付加されている場合、jramemory.stat における No3 の Java メモリプール名は以下の通りです。

監視項目	memory_name として出力する文字列
[ヒープ使用率を監視する]-[領域全体]	HEAP
[ヒープ使用率を監視する]-[Eden Space]	Eden Space
[ヒープ使用率を監視する]-[Survivor Space]	Survivor Space
[ヒープ使用率を監視する]-[Tenured Gen]	Tenured Gen
[非ヒープ使用率を監視する]-[領域全体]	NON_HEAP
[非ヒープ使用率を監視する]-[Code Cache]	Code Cache
[非ヒープ使用率を監視する]-[Perm Gen]	Perm Gen
[非ヒープ使用率を監視する]-[Perm Gen[shared-ro]]	Perm Gen [shared-ro]
[非ヒープ使用率を監視する]-[Perm Gen[shared-rw]]	Perm Gen [shared-rw]

[JVM 種別] に [Oracle Java] を選択、かつ監視対象 Java VM の起動オプションに「-XX:+UseParallelGC」、「-XX:+UseParallelOldGC」が付加されている場合、jramemory.stat における No3 の Java メモリプール名は以下の通りです。

監視項目	memory_name として出力する文字列
[ヒープ使用率を監視する]-[領域全体]	HEAP
[ヒープ使用率を監視する]-[Eden Space]	PS Eden Space
[ヒープ使用率を監視する]-[Survivor Space]	PS Survivor Space
[ヒープ使用率を監視する]-[Tenured Gen]	PS Old Gen
[非ヒープ使用率を監視する]-[領域全体]	NON_HEAP
[非ヒープ使用率を監視する]-[Code Cache]	Code Cache
[非ヒープ使用率を監視する]-[Perm Gen]	PS Perm Gen
[非ヒープ使用率を監視する]-[Perm Gen[shared-ro]]	Perm Gen [shared-ro]
[非ヒープ使用率を監視する]-[Perm Gen[shared-rw]]	Perm Gen [shared-rw]

[JVM 種別] に [Oracle Java] を選択、かつ監視対象 Java VM の起動オプションに「-XX:+UseConcMarkSweepGC」が付加されている場合、jramemory.stat における No3 の Java メモリプール名は以下の通りです。

監視項目	memory_name として出力する文字列
[ヒープ使用率を監視する]-[領域全体]	HEAP
[ヒープ使用率を監視する]-[Eden Space]	Par Eden Space

次のページに続く

表 6.25 – 前のページからの続き

監視項目	memory_name として出力する文字列
[ヒープ使用率を監視する]-[Survivor Space]	Par Survivor Space
[ヒープ使用率を監視する]-[Tenured Gen]	CMS Old Gen
[非ヒープ使用率を監視する]-[領域全体]	NON_HEAP
[非ヒープ使用率を監視する]-[Code Cache]	Code Cache
[非ヒープ使用率を監視する]-[Perm Gen]	CMS Perm Gen
[非ヒープ使用率を監視する]-[Perm Gen[shared-ro]]	Perm Gen [shared-ro]
[非ヒープ使用率を監視する]-[Perm Gen[shared-rw]]	Perm Gen [shared-rw]

[JVM 種別] に [Oracle Java(usage monitoring)] を選択、かつ監視対象 Java VM の起動オプションに「-XX:+UseSerialGC」が付加されている場合、jrammemory.stat における No3 の Java メモリプール名は以下の通りです。

監視項目	memory_name として出力する文字列
[ヒープ使用量を監視する]-[領域全体]	HEAP
[ヒープ使用量を監視する]-[Eden Space]	Eden Space
[ヒープ使用量を監視する]-[Survivor Space]	Survivor Space
[ヒープ使用量を監視する]-[Tenured Gen]	Tenured Gen
[非ヒープ使用量を監視する]-[領域全体]	NON_HEAP
[非ヒープ使用量を監視する]-[Code Cache]	Code Cache(Java 9 以降の場合、出力なし)
[非ヒープ使用量を監視する]-[Metaspace]	Metaspace
[非ヒープ使用量を監視する]-[CodeHeap non-nmethods]	CodeHeap non-nmethods
[非ヒープ使用量を監視する]-[CodeHeap profiled]	CodeHeap profiled nmethods
[非ヒープ使用量を監視する]-[CodeHeap non-profiled]	CodeHeap non-profiled nmethods
[非ヒープ使用量を監視する]-[Compressed Class Space]	Compressed Class Space

[JVM 種別] に [Oracle Java(usage monitoring)] を選択、かつ監視対象 Java VM の起動オプションに「-XX:+UseParallelGC」が付加されている場合、jrammemory.stat における No3 の Java メモリプール名は以下の通りです。

監視項目	memory_name として出力する文字列
[ヒープ使用量を監視する]-[領域全体]	HEAP
[ヒープ使用量を監視する]-[Eden Space]	PS Eden Space
[ヒープ使用量を監視する]-[Survivor Space]	PS Survivor Space
[ヒープ使用量を監視する]-[Tenured Gen]	PS Old Gen
[非ヒープ使用量を監視する]-[領域全体]	NON_HEAP

次のページに続く

表 6.27 – 前のページからの続き

監視項目	memory_name として出力する文字列
[非ヒープ使用量を監視する]-[Code Cache]	Code Cache(Java 9 以降の場合、出力なし)
[非ヒープ使用量を監視する]-[Metaspace]	Metaspace
[非ヒープ使用量を監視する]-[CodeHeap non-nmethods]	CodeHeap non-nmethods
[非ヒープ使用量を監視する]-[CodeHeap profiled]	CodeHeap profiled nmethods
[非ヒープ使用量を監視する]-[CodeHeap non-profiled]	CodeHeap non-profiled nmethods
[非ヒープ使用量を監視する]-[Compressed Class Space]	Compressed Class Space

[JVM 種別] に [Oracle Java(usage monitoring)] を選択、かつ監視対象 Java VM の起動オプションに「-XX:+UseParNewGC」が付加されている場合、jramemory.stat における No3 の Java メモリプール名は以下の通りです。Java 9 以降の場合、「-XX:+UseParNewGC」を付加すると、監視対象 Java VM は起動しません。

監視項目	memory_name として出力する文字列
[ヒープ使用量を監視する]-[領域全体]	HEAP
[ヒープ使用量を監視する]-[Eden Space]	Par Eden Space
[ヒープ使用量を監視する]-[Survivor Space]	Par Survivor Space
[ヒープ使用量を監視する]-[Tenured Gen]	Tenured Gen
[非ヒープ使用量を監視する]-[領域全体]	NON_HEAP
[非ヒープ使用量を監視する]-[Code Cache]	Code Cache
[非ヒープ使用量を監視する]-[Metaspace]	Metaspace
[非ヒープ使用量を監視する]-[CodeHeap non-nmethods]	CodeHeap non-nmethods
[非ヒープ使用量を監視する]-[CodeHeap profiled]	CodeHeap profiled nmethods
[非ヒープ使用量を監視する]-[CodeHeap non-profiled]	CodeHeap non-profiled nmethods
[非ヒープ使用量を監視する]-[Compressed Class Space]	Compressed Class Space

[JVM 種別] に [Oracle Java(usage monitoring)] を選択、かつ監視対象 Java VM の起動オプションに「-XX:+UseG1GC」が付加されている場合、jramemory.stat における No3 の Java メモリプール名は以下の通りです。

監視項目	memory_name として出力する文字列
[ヒープ使用量を監視する]-[領域全体]	HEAP
[ヒープ使用量を監視する]-[Eden Space]	G1 Eden Space
[ヒープ使用量を監視する]-[Survivor Space]	G1 Survivor Space
[ヒープ使用量を監視する]-[Tenured Gen(Old Gen)]	G1 Old Gen
[非ヒープ使用量を監視する]-[領域全体]	NON_HEAP
[非ヒープ使用量を監視する]-[Code Cache]	Code Cache(Java 9 以降の場合、出力なし)

次のページに続く

表 6.29 – 前のページからの続き

監視項目	memory_name として出力する文字列
[非ヒープ使用量を監視する]-[Metaspace]	Metaspace
[非ヒープ使用量を監視する]-[CodeHeap non-nmethods]	CodeHeap non-nmethods
[非ヒープ使用量を監視する]-[CodeHeap profiled]	CodeHeap profiled nmethods
[非ヒープ使用量を監視する]-[CodeHeap non-profiled]	CodeHeap non-profiled nmethods
[非ヒープ使用量を監視する]-[Compressed Class Space]	Compressed Class Space

監視対象 Java VM が Oracle JRockit の場合 ([JVM 種別] で [JRockit] 選択時)、jramemory.stat における No3 の Java メモリプール名は以下の通りです。

監視項目	memory_name として出力する文字列
[ヒープ使用率を監視する]-[領域全体]	HEAP memory
[ヒープ使用率を監視する]-[Nursery Space]	Nursery
[ヒープ使用率を監視する]-[Old Space]	Old Space
[非ヒープ使用率を監視する]-[領域全体]	NON_HEAP
[非ヒープ使用率を監視する]-[Class Memory]	Class Memory

JVM 統計ログ jramemory.stat における Java メモリプール名と、Java VM メモリ空間の関係は以下の通りです。

- Oracle Java 8/Oracle Java 9/Oracle Java 11/Oracle Java 17/Oracle Java 21 の場合

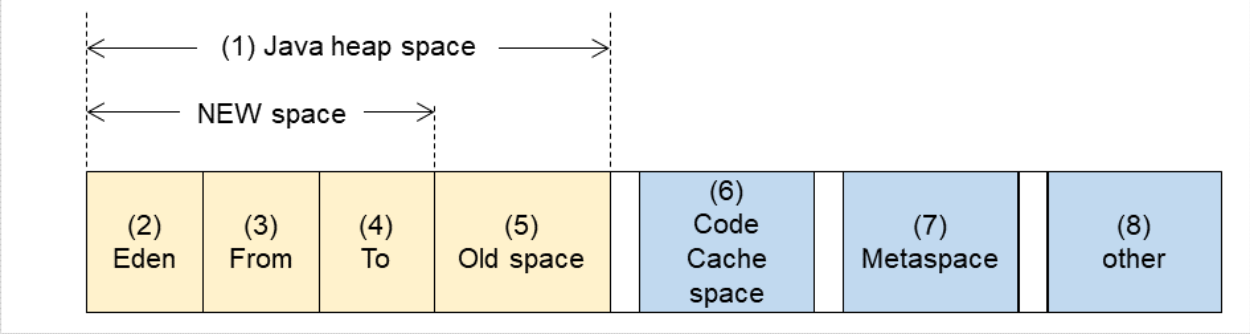


図 6.15　Java VM メモリ空間（Oracle Java 8/Oracle Java 9/Oracle Java 11/Oracle Java 17/Oracle Java 21）

図中の No	監視項目	jramemory.stat の Java メモリプール名
(1)	[ヒープ使用量を監視する]-[領域全体]	HEAP

次のページに続く

表 6.31 – 前のページからの続き

図中の No	監視項目	jramemory.stat の Java メモリプール名
(2)	[ヒープ使用量を監視する]-[Eden Space]	EdenSpace PS Eden Space Par Eden Space G1 Eden Space
(3)+(4)	[ヒープ使用量を監視する]-[Survivor Space]	Survivor Space PS Survivor Space Par Survivor Space G1 Survivor Space
(5)	[ヒープ使用量を監視する]-[Tenured Gen]	Tenured Gen PS Old Gen G1 Old Gen
(6)	[非ヒープ使用量を監視する]-[Code Cache]	Code Cache(Java 9 以降の場合、出力なし)
(6)	[非ヒープ使用量を監視する]-[CodeHeap non-nmethods]	CodeHeap non-nmethods(Java 9 以降の場合のみ出力)
(6)	[非ヒープ使用量を監視する]-[CodeHeap profiled]	CodeHeap profiled nmethods(Java 9 以降の場合のみ出力)
(6)	[非ヒープ使用量を監視する]-[CodeHeap non-profiled]	CodeHeap non-profiled nmethods(Java 9 以降の場合のみ出力)
(7)	[非ヒープ使用量を監視する]-[Metaspace]	Metaspace
(8)	[非ヒープ使用量を監視する]-[Compressed Class Space]	Compressed Class Space
(6)+(7)+(8)	[非ヒープ使用量を監視する]-[領域全体]	NON_HEAP

- Oracle JRockit の場合

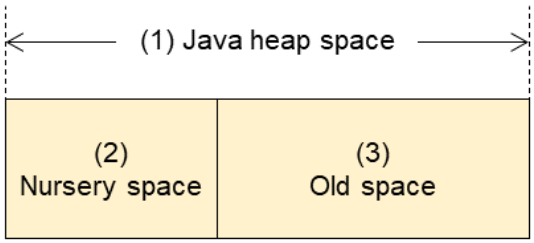


図 6.16　Java VM メモリ空間（Oracle JRockit）

図中の No	監視項目	jrammemory.stat の Java メモリプール名
(1)	[ヒープ使用率を監視する]-[領域全体]	HEAP memory
(2)	[ヒープ使用率を監視する]-[Nursery Space]	Nursery
(3)[*2]	[ヒープ使用率を監視する]-[Old Space]	Old Space
-	[非ヒープ使用率を監視する]-[領域全体]	NON_HEAP
-	[非ヒープ使用率を監視する]-[Class Memory]	Class Memory

6.33.17 異常検出時に障害原因別にコマンドを実行するには

モニタリソースの異常検出時、CLUSTERPRO では障害原因別に異なるコマンドを区別して実行する手段を提供していません。
JVM モニタリソースでは障害原因別にコマンドを区別して実行可能です。異常検出時に実行します。

障害原因別に実行するコマンドの設定項目は以下の通りです。

障害原因	設定項目
・監視対象の Java VM へ接続失敗 ・リソース計測失敗	[監視 (固有)] タブ-[コマンド]

次のページに続く

[*2] jrammemory.stat の Java メモリプール名"Old Space"については、HEAP 内の old 領域の値ではなく、"HEAP memory"全体と同値となります。(3) のみの計測はできません。

表 6.33 – 前のページからの続き

障害原因	設定項目
・ヒープ使用率 ・非ヒープ使用率 ・ヒープ使用量 ・非ヒープ使用量	[監視 (固有)] タブ-[調整] プロパティ-[メモリ] タブ-[コマンド]
・動作中のスレッド数	[監視 (固有)] タブ-[調整] プロパティ-[スレッド] タブ-[コマンド]
・Full GC 実行時間 ・Full GC 発生回数	[監視 (固有)] タブ-[調整] プロパティ-[GC] タブ-[コマンド]
・WebLogic のワークマネージャのリクエスト ・WebLogic のスレッドプールのリクエスト	[監視 (固有)] タブ-[調整] プロパティ-[WebLogic] タブ-[コマンド]

[コマンド] は障害原因の詳細をコマンドの引数として渡します。引数は [コマンド] の最後に結合して渡します。スクリプトなどを自身で作成し [コマンド] へ設定することにより、更に障害原因に特化した動作が可能です。引数として渡す文字列は以下の通りです。

引数として渡す文字列が複数記載している場合は、監視対象 Java VM の GC 方式によりいずれかを渡します。差異の詳細は「6.33.16. *Java* メモリプール名について」を参照してください。

(Oracle Java の場合) (Oracle JRockit の場合) と記載がある場合は、JVM 種別により異なります。記載がない場合、JVM 種別による区別はありません。

障害原因の詳細	引数として渡す文字列
・監視対象の Java VM へ接続失敗 ・リソース計測失敗	なし

次のページに続く

表 6.34 – 前のページからの続き

障害原因の詳細	引数として渡す文字列
[監視 (固有)] タブ-[調整] プロパティ-[メモリ] タブ-[ヒープ使用率を監視する]-[領域全体] (Oracle Java の場合)	HEAP
[メモリ] タブ- [ヒープ使用率を監視する]-[Eden Space] (Oracle Java の場合)	EdenSpace PSEdenSpace ParEdenSpace
[メモリ] タブ- [ヒープ使用率を監視する]-[Survivor Space] (Oracle Java の場合)	SurvivorSpace PSSurvivorSpace ParSurvivorSpace
[メモリ] タブ- [ヒープ使用率を監視する]-[Tenured Gen] (Oracle Java の場合)	TenuredGen PSOldGen CMSOldGen
[メモリ] タブ- [非ヒープ使用率を監視する]-[領域全体] (Oracle Java の場合)	NON_HEAP
[メモリ] タブ- [非ヒープ使用率を監視する]-[Code Cache] (Oracle Java の場合)	CodeCache

次のページに続く

表 6.34 – 前のページからの続き

障害原因の詳細	引数として渡す文字列
[メモリ] タブ- [非ヒープ使用率を監視する]-[PermGen] (Oracle Java の場合)	PermGen PSPermGen CMSPermGen
[メモリ] タブ- [非ヒープ使用率を監視する]-[PermGen[shared-ro]] (Oracle Java の場合)	PermGen[shared-ro]
[メモリ] タブ- [非ヒープ使用率を監視する]-[PermGen[shared-rw]] (Oracle Java の場合)	PermGen[shared-rw]
[メモリ] タブ- [ヒープ使用量を監視する]-[領域全体](Oracle Java(usage monitoring) の場合)	HEAP
[メモリ] タブ- [ヒープ使用量を監視する]-[Eden Space](Oracle Java(usage monitoring) の場合)	EdenSpace PSEdenSpace ParEdenSpace G1EdenSpace
[メモリ] タブ- [ヒープ使用量を監視する]-[Survivor Space](Oracle Java(usage monitoring) の場合)	SurvivorSpace PSSurvivorSpace ParSurvivorSpace G1SurvivorSpace

次のページに続く

表 6.34 – 前のページからの続き

障害原因の詳細	引数として渡す文字列
[メモリ] タブ- [ヒープ使用量を監視する]-[Tenured Gen](Oracle Java(usage monitoring) の場合)	TenuredGen PSOldGen CMSOldGen G1OldGen
[メモリ] タブ- [非ヒープ使用量を監視する]-[領域全体](Oracle Java(usage monitoring) の場合)	NON_HEAP
[メモリ] タブ- [非ヒープ使用量を監視する]-[Code Cache](Oracle Java(usage monitoring) の場合)	CodeCache
[メモリ] タブ- [非ヒープ使用量を監視する]-[Metaspace](Oracle Java(usage monitoring) の場合)	Metaspace
[メモリ] タブ - [非ヒープ使用量を監視する]-[CodeHeap non-nmethods](Oracle Java(usage monitoring) の場合)	non-nmethods
[メモリ] タブ - [非ヒープ使用量を監視する]-[CodeHeap profiled](Oracle Java(usage monitoring) の場合)	profilednmethods
[メモリ] タブ - [非ヒープ使用量を監視する]-[CodeHeap non-profiled](Oracle Java(usage monitoring) の場合)	non-profilednmethods
[メモリ] タブ - [非ヒープ使用量を監視する]-[Compressed Class Space](Oracle Java(usage monitoring) の場合)	CompressedClassSpace
[メモリ] タブ- [ヒープ使用率を監視する]-[領域全体] (Oracle JRockit の場合)	HEAP Heap
[メモリ] タブ- [ヒープ使用率を監視する]-[Nursery Space] (Oracle JRockit の場合)	Nursery

次のページに続く

表 6.34 – 前のページからの続き

障害原因の詳細	引数として渡す文字列
[メモリ] タブ- [ヒープ使用率を監視する]-[Old Space] (Oracle JRockit の場合)	OldSpace
[メモリ] タブ- [非ヒープ使用率を監視する]-[領域全体] (Oracle JRockit の場合)	NON_HEAP
[メモリ] タブ- [非ヒープ使用率を監視する]-[Class Memory] (Oracle JRockit の場合)	ClassMemory
[スレッド] タブ-[動作中のスレッド数を監視する]	Count
[GC] タブ-[Full GC 実行時間を監視する]	Time
[GC] タブ-[Full GC 発生回数を監視する]	Count
[WebLogic] タブ-[ワークマネージャのリクエストを監視する]-[待機リクエスト リクエスト数]	WorkManager_PendingRequests
[WebLogic] タブ-[スレッドプールのリクエストを監視する]-[待機リクエスト リクエスト数]	ThreadPool_PendingUserRequestCount
[WebLogic] タブ-[スレッドプールのリクエストを監視する]-[実行リクエスト リクエスト数]	ThreadPool_Throughput

以下に実行例に示します。

例 1)

設定項目	設定内容
[監視 (固有)] タブ-[調整] プロパティ-[GC] タブ-[コマンド]	/usr/local/bin/downcmd
[監視 (固有)] タブ-[調整] プロパティ-[GC] タブ-[Full GC 発生回数を監視する]	1

次のページに続く

表 6.35 – 前のページからの続き

設定項目	設定内容
[クラスタ] プロパティ-[JVM 監視] タブ-[リソース計測設定]-[共通] タブ-[異常判定しきい値]	3

JVM モニタリソースは、異常判定しきい値回 (3 回) 連続して Full GC が発生すると、モニタ異常を検出し、「/usr/local/bin/downcmd Cont」としてコマンドを実行します。

例 2)

設定項目	設定内容
[監視 (固有)] タブ-[調整] プロパティ-[GC] タブ-[コマンド]	"/usr/local/bin/downcmd" GC
[監視 (固有)] タブ-[調整] プロパティ-[GC] タブ-[Full GC 実行時間を監視する]	65536
[クラスタ] プロパティ-[JVM 監視] タブ-[リソース計測設定]-[共通] タブ-[異常判定しきい値]	3

JVM モニタリソースは、異常判定しきい値回 (3 回) 連続して Full GC 実行時間が 65535 ミリ秒超過すると、モニタ異常を検出し、「/usr/local/bin/downcmd GC Time」としてコマンドを実行します。

例 3)

設定項目	設定内容
[監視 (固有)] タブ-[調整] プロパティ-[メモリ] タブ-[コマンド]	"/usr/local/bin/downcmd" memory
[監視 (固有)] タブ-[調整] プロパティ-[メモリ] タブ-[ヒープ使用率を監視する]	オン
[監視 (固有)] タブ-[調整] プロパティ-[メモリ] タブ-[Eden Space]	80
[監視 (固有)] タブ-[調整] プロパティ-[メモリ] タブ-[Survivor Space]	80
[クラスタ] プロパティ-[JVM 監視] タブ-[リソース計測設定]-[共通] タブ-[異常判定しきい値]	3

JVM モニタリソースは、異常判定しきい値回 (3 回) 連続して Java Eden Space の使用率および Java Survivor Space の使用率が 80% を超過すると、モニタ異常を検出し、「/usr/local/bin/downcmd memory EdenSpace SurvivorSpace」としてコマンドを実行します。

[コマンド] で設定したコマンドの終了を待つタイムアウト (秒) は、[クラスタのプロパティ] - [JVM 監視]

タブ - [コマンドタイムアウト] で設定します。これは上記各タブの [コマンド] で同じ値を適用します。[コマンド] 個別には設定できません。

タイムアウトした場合、[コマンド] プロセスを強制終了させるような処理は実行しません。[コマンド] プロセスの後処理 (例：強制終了) は、お客様が実行してください。タイムアウトした場合は、以下のメッセージを JVM 運用ログへ出力します。

action thread execution did not finish. action is alive = **<コマンド>**

注意事項は以下の通りです。

- Java VM の正常復帰検出時 (異常 → 正常時) には [コマンド] は実行しません。
- [コマンド] は Java VM 異常検出時 (しきい値の超過が異常判定しきい値回連続して発生した場合) を契機として実行します。しきい値の超過毎には実行しません。
- 複数のタブにて [コマンド] を設定すると、同時に障害が発生した場合は複数の [コマンド] が実行されます。そのため、システム負荷にはご注意ください。
- [監視 (固有)] タブ - [調整] プロパティ - [WebLogic] タブ - [ワークマネージャのリクエストを監視する] - [待機リクエスト リクエスト数]、[監視 (固有)] タブ - [調整] プロパティ - [WebLogic] タブ - [ワークマネージャのリクエストを監視する]-[待機リクエスト 平均値] を両方監視している場合、[コマンド] が同時に 2 回実行される可能性があります。

  これは、[クラスタ] プロパティ - [JVM 監視] タブ - [リソース計測設定] - [WebLogic] タブ- [インターバル リクエスト数] と [クラスタ] プロパティ -[JVM 監視] タブ-[リソース計測設定]-[WebLogic] タブ-[インターバル 平均値] の異常検出が同時に発生する可能性があるためです。回避策としては、どちらか一方のみ監視するようにしてください。以下の監視項目の組み合わせも同様です。
- [監視 (固有)] タブ-[調整] プロパティ -[WebLogic] タブ-[スレッドプールのリクエストを監視する]-[待機リクエスト リクエスト数] と、[監視 (固有)] タブ-[調整] プロパティ -[WebLogic] タブ-[スレッドプールのリクエストを監視する]-[待機リクエスト 平均値]
- [監視 (固有)] タブ-[調整] プロパティ -[WebLogic] タブ-[スレッドプールのリクエストを監視する]-[実行リクエスト リクエスト数] と、[監視 (固有)] タブ-[調整] プロパティ -[WebLogic] タブ-[スレッドプールのリクエストを監視する]-[実行リクエスト 平均値]

6.33.18 WebLogic Server を監視するには

監視対象の WebLogic Server の設定が終了しアプリケーションサーバとして稼動させる手順は、WebLogic Server のマニュアルを参照してください。

本章では、JVM モニタリソースで監視するために必要な設定のみについて記述します。

1. WebLogic Server Administration Console を起動します。

起動方法は、WebLogic Server マニュアルの「Administration Console の概要」を参照してください。

ドメインコンフィグレーション－ドメイン－コンフィグレーション－全般を選択します。ここで**「管理ポートの有効化」のチェックがオフ**になっていることを確認してください

2. ドメインコンフィグレーション-サーバを選択し、監視対象のサーバ名を選択します。選択したサーバ名は Cluster WebUI の設定モードから選択可能な [プロパティ]-[監視 (固有)] タブの識別名に設定します。CLUSTERPRO X の『リファレンスガイド』-「モニタリソースの詳細」-「JVM モニタリソースを理解する」を参照してください。

3. 監視対象のサーバのコンフィグレーション－全般で**「リスンポート」**で管理接続するポート番号を確認します。

4. WebLogic Server を停止します。停止方法は、WebLogic Server マニュアルの「WebLogic Server の起動と停止」を参照してください。

5. WebLogic Server の管理サーバ起動スクリプト (startWebLogic.sh) を開きます。

6. 開いたスクリプトに以下の内容を記述します。

- 監視対象が WebLogic Server の管理サーバの場合

```
JAVA_OPTIONS="${JAVA_OPTIONS}
-Dcom.sun.management.jmxremote.port=n
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.authenticate=false
-Djavax.management.builder.initial=weblogic.management.jmx.mbeanserver.
↪WLSMBeanServerBuilder"
```

※ 上記内容は実際には 1 行で記述してください。

- 監視対象が WebLogic Server の管理対象サーバの場合

```
if [ "${SERVER_NAME}" = "SERVER_NAME" ]; then
    JAVA_OPTIONS="${JAVA_OPTIONS}
    -Dcom.sun.management.jmxremote.port=n
    -Dcom.sun.management.jmxremote.ssl=false
    -Dcom.sun.management.jmxremote.authenticate=false
    -Djavax.management.builder.initial=weblogic.management.jmx.mbeanserver.
↪WLSMBeanServerBuilder"
fi
```

※ 上記で if 文の中は実際には 1 行で記述してください。

注釈: *n* は、監視のために使用するポート番号を指定します。指定するポート番号は**監視対象の Java VM のリスンポート番号とは別の番号を指定してください。**また同一のマシンに複数の監視対象の WebLogic Server が存在する場合、そのリスニング・ポート番号や他のアプリケーションのポート番号と重複しないポート番号を指定してください。

注釈: **SERVER_NAME** は、「監視対象サーバ選択」で確認した監視対象となるサーバ名を指定します。監視対象のサーバが複数の場合、同様の設定 (1〜6 行目) に対してサーバ名を変更し、繰り返し設定してください。

注釈: 上記の記述内容の追加箇所は、以下の記述より前に記述するようにしてください。

```
${JAVA_HOME}/bin/java ${JAVA_VM} ${MEM_ARGS} ${JAVA_OPTIONS} -Dweblogic.Name=${SERVER_
↪NAME} -Djava.security.policy=${WL_HOME}/server/lib/weblogic.policy ${PROXY_SETTINGS} $
↪{SERVER_CLASS}
```

※ 上記内容は実際には 1 行で記述してください

※ WebLogic のバージョンによって、上記の java 引数の内容が異なっている場合がありますが、java の実行前に JAVA_OPTIONS を記述していただければ問題ありません。

注釈: [メモリタブ] の [Perm Gen[shared-ro]] や [Perm Gen[shared-rw]] を監視する場合、以下を追加してください。

```
-client -Xshare:on -XX:+UseSerialGC
```

7. ワークマネージャやスレッドプールのリクエストを監視する場合は、以下の設定を行ってください。
   監視対象の WebLogic Server の WLST(wlst.sh) を起動します。表示されたコンソール画面上で、以下のコマンドを実行してください。

   ```
   > connect('USERNAME','PASSWORD','t3://SERVER_ADDRESS:SERVER_PORT')
   > edit()
   > startEdit()
   > cd('JMX/DOMAIN_NAME')
   > set('PlatformMBeanServerUsed','true')
   ```

```
> activate()
> exit()
```

上記の **USERNAME**、**PASSWORD**、**SERVER_ADDRESS**、**SERVER_PORT**、**DOMAIN_NAME** はドメイン環境に応じた値に置き換えてください

8. 監視対象の WebLogic Server を再起動します

6.33.19 WebOTX を監視するには

本ガイドでは、JVM モニタリソースで監視する対象の WebOTX の設定手順について記述します。

WebOTX 統合運用管理コンソールを起動します。起動方法は「WebOTX 運用編（Web 版統合運用管理ツール）」マニュアルの「統合運用管理ツールの起動と終了」を参照してください。

以降の設定は、WebOTX 上の JMX エージェントの Java プロセスに対する監視を行う場合と、プロセスグループ上の Java プロセスに対する監視を行う場合とで設定内容が異なります。監視する対象に合わせて、設定してください。

6.33.20 WebOTX ドメインエージェントの Java プロセスを監視するには

特に設定作業は不要です。

6.33.21 WebOTX プロセスグループの Java プロセスを監視するには

1. 統合運用管理ツールよりドメインと接続します。
2. ツリービューより [<ドメイン名>]-[TP システム]-[アプリケーショングループ]-[<アプリケーショングループ名>]-[プロセスグループ]-[<プロセスグループ名>] を選択します。
3. 右側に表示される [JVM オプション] タブ内の [その他の引数] 属性に、次の Java オプションを 1 行で指定します。**n** は、ポート番号を指定します。同一のマシンに複数の監視対象の Java VM が存在する場合、重複しないポート番号を指定してください。ここで指定するポート番号は、Cluster WebUI ([モニタリソースのプロパティ]→[監視 (固有)] タブ →[接続ポート番号]) でも設定します。

```
-Dcom.sun.management.jmxremote.port=n
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.authenticate=false
-Djavax.management.builder.initial=com.nec.webotx.jmx.mbeanserver.
↪JmxMBeanServerBuilder
```

※ WebOTX V9.2 以降では -Djavax.management.builder.initial の指定は不要です。

4. 設定後、[更新] ボタンを押します。設定が完了したら、プロセスグループを再起動します。

   本設定は、WebOTX 統合運用管理ツールの [Java システムプロパティ] タブ内の [Java システムプロパティ] 属性にて指定することも可能です。その場合は、"-D"は指定せず、また、"="より前の文字列を「名前」に、"="より後ろの文字列を「値」に指定してください。

設定タブ名	項目名	設定値
監視 (共通)	監視タイミング	常時
回復動作	回復動作	最終動作のみ実行
回復動作	最終動作	何もしない

注釈: WebOTX プロセスグループの機能でプロセス障害時の再起動を設定されている場合、CLUSTERPRO からの復旧動作でプロセスグループの再起動を実行すると、WebOTX プロセスグループの機能が正常に動作しない場合があります。そのため、WebOTX プロセスグループを監視する場合は Cluster WebUI から JVM モニタリソースに対して以下のように設定してください。

6.33.22 WebOTX notification 通知を受信するには

特定のリスナクラスを登録することにより、WebOTX が障害を検出すると notification が発行されます。JVM モニタリソースはその notification を受信し、JVM 運用ログへ以下のメッセージを通知します。

```
%1$s:Notification received. %2$s.
```

%1$s、%2$s の意味は以下のとおりです。

```
%1$s：監視対象 Java VM
%2$s：notification の通知メッセージ (ObjectName=**,type=**,message=**)
```

現在、監視可能なリソースの MBean の詳細情報は以下のとおりです。

ObjectName	[domainname]:j2eeType=J2EEDomain,name=[domainname],category=runtime
notification タイプ	nec.webotx.monitor.alivecheck.not-alive
メッセージ	failed

6.33.23 JBoss を監視するには

スタンドアローンモードに対する監視を行う場合と、ドメインモードに対する監視を行う場合とで設定内容が異なります。監視する対象に合わせて、設定してください。

JVM モニタリソースで監視する対象の JBoss の設定手順について記述します。

スタンドアローンモードの場合

1. JBoss を停止し、(*JBoss* **インストールパス**)/bin/standalone.conf をエディタから開きます。
2. 開いた設定ファイルに、設定する JDK のバージョンに応じて以下の内容を記述します。**n** は、ポート番号を指定します。同一のマシンに複数の監視対象の Java VM が存在する場合、重複しないポート番号を指定してください。ここで指定するポート番号は、Cluster WebUI ([モニタリソースのプロパティ]→[監視 (固有)] タブ →[接続ポート番号]) でも設定します。

   JDK10 以前を使用する場合は、以下の修正を行う。

   「if ["x$JBOSS_MODULES_SYSTEM_PKGS" = "x"]; then」より前に以下を追加

```
JBOSS_MODULES_SYSTEM_PKGS="org.jboss.logmanager"
```

   「if ["x$JAVA_OPTS" = "x"]; then … fi:」より後に以下を追加

```
JAVA_OPTS="$JAVA_OPTS -Xbootclasspath/p:$JBOSS_HOME/modules/org/jboss/logmanager/
↪main/jboss-logmanager-1.3.2.Final-redhat-1.jar"
JAVA_OPTS="$JAVA_OPTS -Djava.util.logging.manager=org.jboss.logmanager.LogManager"
JAVA_OPTS="$JAVA_OPTS -Dcom.sun.management.jmxremote.port=n -Dcom.sun.management.
↪jmxremote.ssl=false -Dcom.sun.management.jmxremote.authenticate=false"
```

   JDK11 以降を使用する場合は、以下の修正を行う。

   「if ["x$JBOSS_MODULES_SYSTEM_PKGS" = "x"]; then」より前に以下を追加

```
JBOSS_MODULES_SYSTEM_PKGS="org.jboss.logmanager"
```

   「if ["x$JAVA_OPTS" = "x"]; then … fi:」より後に以下を追加

```
JAVA_OPTS="$JAVA_OPTS -Xbootclasspath/a:$JBOSS_HOME/modules/org/jboss/logmanager/
↪main/jboss-logmanager-1.3.2.Final-redhat-1.jar"
JAVA_OPTS="$JAVA_OPTS -Djava.util.logging.manager=org.jboss.logmanager.LogManager"
JAVA_OPTS="$JAVA_OPTS -Dcom.sun.management.jmxremote.port=n -Dcom.sun.management.
↪jmxremote.ssl=false -Dcom.sun.management.jmxremote.authenticate=false"
JAVA_OPTS="$JAVA_OPTS -Dsun.util.logging.disableCallerCheck=true"
```

※ jboss-logmanager-*.jar は JBoss のバージョンによって格納ディレクトリ、ファイル名が異なりますため、インストールしている環境に合わせてパスを指定してください。

3. 上記設定を保存した後、JBoss を起動します。
4. Cluster WebUI (JVM モニタリソース名 →[プロパティ]→[監視 (固有)] タブ →[識別名]) には他の監視対象と重ならない任意の文字列 (例：JBoss) を設定してください。

ドメインモードの場合

1. Cluster WebUI (JVM モニタリソース名 →[プロパティ]→[監視 (固有)] タブ →[識別名]) には他の監視対象と重ならない任意の文字列 (例：JBoss) を設定してください。また、Cluster WebUI (JVM モニタリソース名 →[プロパティ]→[監視 (固有)] タブ →[プロセス名]) では、ユニークに特定できるよう Java VM 起動時オプションを全て指定してください。

6.33.24 Tomcat を監視するには

JVM モニタリソースで監視する対象の Tomcat の設定手順について記述します。

1. Tomcat を rpm パッケージでインストールした場合、Tomcat を停止し、/etc/sysconfig/tomcat6 または /etc/sysconfig/tomcat を開きます。Tomcat を rpm パッケージでインストールしていない場合、Tomcat を停止し、(*Tomcat* **インストールパス**)/bin/setenv.sh を作成します。
2. 開いた設定ファイルの Java オプションに以下の内容を 1 行で記述します。**n** は、ポート番号を指定します。同一のマシンに複数の監視対象の Java VM が存在する場合、重複しないポート番号を指定してください。ここで指定するポート番号は、Cluster WebUI ([モニタリソースのプロパティ]→[監視 (固有)] タブ →[接続ポート番号]) でも設定します。

```
CATALINA_OPTS="${CATALINA_OPTS}
-Dcom.sun.management.jmxremote.port=n
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.authenticate=false"
```

3. 上記設定を保存した後、Tomcat を起動します。
4. Cluster WebUI (JVM モニタリソース名 →[プロパティ]→[監視 (固有)] タブ →[識別名]) には他の監視対象

と重ならない任意の文字列 (例：tomcat) を設定してください。

6.33.25 SVF を監視するには

JVM モニタリソースで監視する対象の SVF の設定手順について記述します。

監視対象が Tomcat の場合:

OS の SVF ユーザの環境変数を以下のように変更してください。**n** は、ポート番号を指定します。同一のマシンに複数の監視対象の Java VM が存在する場合、重複しないポート番号を指定してください。ここで指定するポート番号は、Cluster WebUI([モニタリソースのプロパティ]→[監視 (固有)] タブ →[接続ポート番号]) でも設定します。

```
JAVA_OPTS="-Xms512m -Xmx512m -Dcom.sun.management.jmxremote.port=n -Dcom.sun.
↪management.jmxremote.ssl=false -Dcom.sun.management.jmxremote.authenticate=false"
export JAVA_OPTS
```

監視対象が Tomcat 以外の場合:

1. 監視対象を下記より選択し、該当するスクリプトをエディタから開きます。

監視対象	編集するスクリプト
Simple Httpd Service(8.x の場合)	<SVF インストールパス>/bin/SimpleHttpd
UCX Server Service(9.x 以降の場合)	<SVF インストールパス>/bin/UCXServer
RDE Service	<SVF インストールパス>/rdjava/rdserver/rd_server_startup.sh
	<SVF インストールパス>/rdjava/rdserver/svf_server_startup.sh
RD Spool Balancer	<SVF インストールパス>/rdjava/rdbalancer/rd_balancer_startup.sh
SVF Print Spooler Service	<SVF インストールパス>/bin/spooler

2. Java オプション指定箇所に下記の内容を 1 行で記述します。**n** は、ポート番号を指定します。同一のマシン

に複数の監視対象の Java VM が存在する場合、重複しないポート番号を指定してください。ここで指定するポート番号は、Cluster WebUI ([モニタリソースのプロパティ]→[監視 (固有)] タブ →[接続ポート番号]) でも設定します。

```
JAVA_OPTIONS="${JAVA_OPTIONS} -Dcom.sun.management.jmxremote.port=n -Dcom.sun.
↪management.jmxremote.ssl=false -Dcom.sun.management.jmxremote.authenticate=false"
```

3. 監視対象が RDE Service の場合、下記の起動パス中および rd_balancer_startup.sh に${JAVA_OPTIONS}を追記します。

```
java -Xmx256m -Xms256m -Djava.awt.headless=true ${JAVA_OPTIONS} -classpath
↪$CLASSPATH jp.co.fit.vfreport.RdSpoolPlayerServer &
```

6.33.26 自製の Java アプリケーションを監視するには

JVM モニタリソースで監視する対象の Java アプリケーションの設定手順について記述します。監視対象の Java アプリケーションが停止した状態で、Java アプリケーションの起動時オプションに次の Java オプションを 1 行で指定します。n は、監視のために使用するポート番号を指定します。同一のマシンに複数の監視対象の Java VM が存在する場合、重複しないポート番号を指定してください。ここで指定するポート番号は、Cluster WebUI([モニタリソースのプロパティ]→[監視 (固有)] タブ →[接続ポート番号]) でも設定します。

```
-Dcom.sun.management.jmxremote.port=n
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.authenticate=false
```

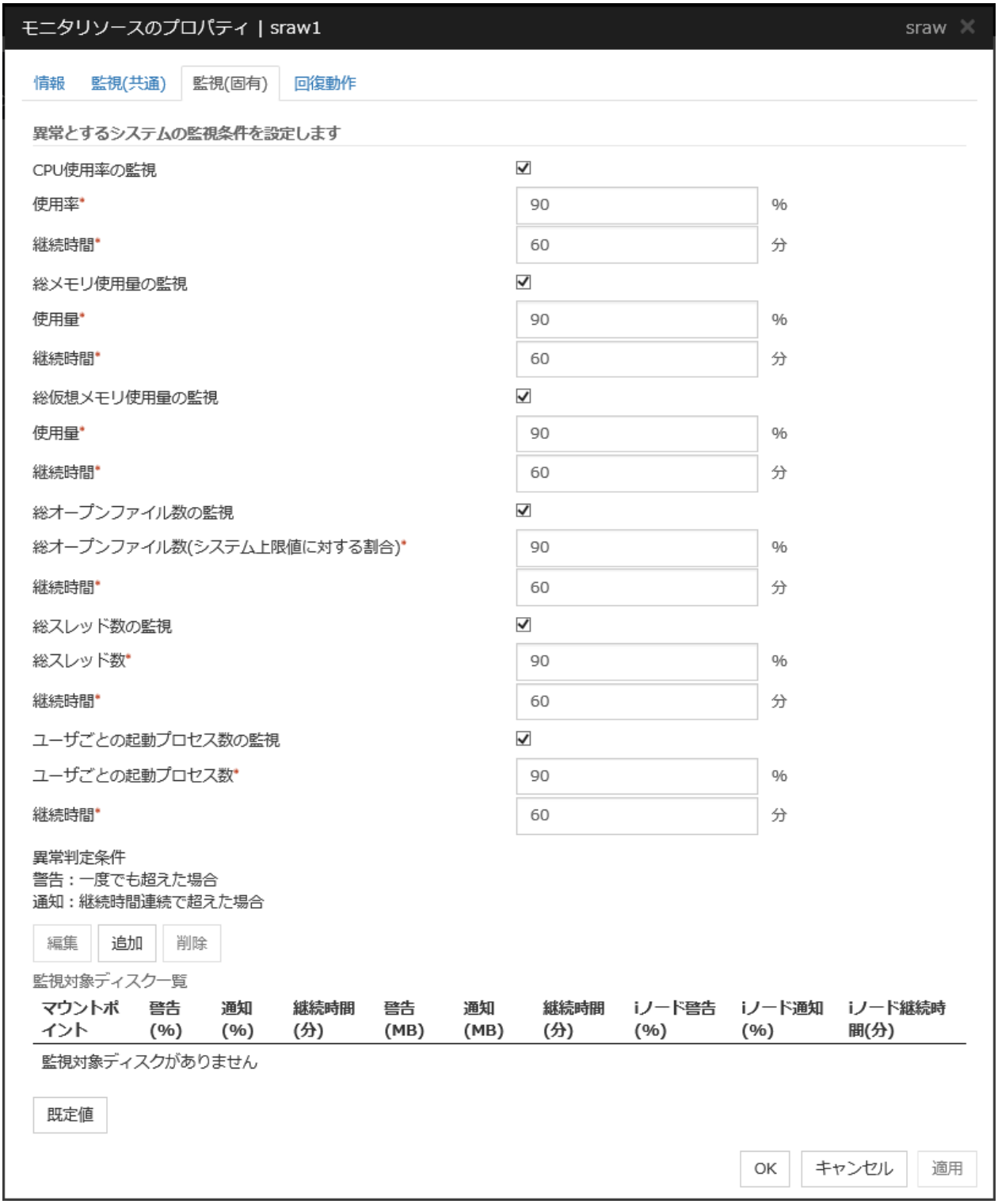
Java アプリケーションによっては以下も追加で指定必要です。

-Djavax.management.builder.initial=<*MBeanServerBuilder* のクラス名>

6.34 システムモニタリソースの設定

システムモニタリソースは、システムリソースの統計情報を継続的に収集し、一定のナレッジ情報にしたがい解析を行います。解析の結果からリソース枯渇の発生を早期検出する機能を提供します。

6.34.1 監視 (固有) タブ



CPU 使用率の監視

CPU 使用率の監視を行うかどうかを設定します。

- チェックボックスがオン

  CPU 使用率の監視を行います。

- チェックボックスがオフ

  CPU 使用率の監視を行いません。

使用率 (1〜100)

CPU 使用率の異常を検出するしきい値を設定します。

継続時間 (1〜1440)

CPU 使用率の異常を検出する時間を設定します。

指定した時間以上連続してしきい値を超過した場合、異常を検出します。

総メモリ使用量の監視

総メモリ使用量の監視を行うかどうかを設定します。

- チェックボックスがオン

  総メモリ使用量の監視を行います。

- チェックボックスがオフ

  総メモリ使用量の監視を行いません。

使用量 (1〜100)

メモリの使用量の異常を検出するしきい値 (システムのメモリ搭載量に対する割合) を設定します。

継続時間 (1〜1440)

総メモリ使用量の異常を検出する時間を設定します。

指定した時間以上連続してしきい値を超過した場合、異常を検出します。

総仮想メモリ使用量の監視

総仮想メモリ使用量の監視を行うかどうかを設定します。

- チェックボックスがオン

  総仮想メモリ使用量の監視を行います。

- チェックボックスがオフ

  総仮想メモリ使用量の監視を行いません。

使用量 (1〜100)

仮想メモリの使用量の異常を検出するしきい値を設定します。

継続時間 (1〜1440)

総仮想メモリ使用量の異常を検出する時間を設定します。

指定した時間以上連続してしきい値を超過した場合、異常を検出します。

総オープンファイル数の監視

総オープンファイル数の監視を行うかどうかを設定します。

- チェックボックスがオン

  総オープンファイル数の監視を行います。

- チェックボックスがオフ

  総オープンファイル数の監視を行いません。

総オープンファイル数 (1〜100)

オープンしているファイルの総数の異常を検出するしきい値 (システム上限値に対する割合) を設定します。

継続時間 (1〜1440)

総オープンファイル数の異常を検出する時間を設定します。

指定した時間以上連続してしきい値を超過した場合、異常を検出します。

総スレッド数の監視

総スレッド数の監視を行うかどうかを設定します。

- チェックボックスがオン

  総スレッド数の監視を行います。

- チェックボックスがオフ

  総スレッド数の監視を行いません。

総スレッド数 (1〜100)

起動しているスレッドの総数の異常を検出するしきい値 (システム上限値に対する割合) を設定します。

継続時間 (1〜1440)

総スレッド数の異常を検出する時間を設定します。

指定した時間以上連続してしきい値を超過した場合、異常を検出します。

ユーザごとの起動プロセス数の監視

ユーザごとの起動プロセス数の監視を行うかどうかを設定します。

- チェックボックスがオン

  ユーザごとの起動プロセス数の監視を行います。

- チェックボックスがオフ

ユーザごとの起動プロセス数の監視を行いません。

ユーザごとの起動プロセス数 (1〜100)

ユーザごとの起動プロセス数の異常を検出するしきい値 (システム上限値に対する割合) を設定します。

継続時間 (1〜1440)

ユーザごとの起動プロセス数の異常を検出する時間を設定します。

指定した時間以上連続してしきい値を超過した場合、異常を検出します。

追加

監視するディスクを追加します。[監視条件の入力] ダイアログボックスが表示されます。

[監視条件の入力] ダイアログの説明に従い異常とする監視条件の詳細設定を行います。

削除

[ディスク一覧] で選択しているディスクを監視対象から削除します。

編集

[監視条件の入力] ダイアログボックスが表示されます。[ディスク一覧] で選択しているディスクの監視条件が表示されるので、編集して [OK] を選択します。

マウントポイント (1024 バイト以内)

監視を行うマウントポイントを設定します。[/] で始まる必要があります。

使用率

ディスク使用率の監視を行うかどうかを設定します。

- チェックボックスがオン
  ディスク使用率の監視を行います。
- チェックボックスがオフ

ディスク使用率の監視を行いません。

警告レベル (1〜100)

ディスク使用率の警報レベルの異常を検出するしきい値を設定します。

通知レベル (1〜100)

ディスク使用率の通知レベルの異常を検出するしきい値を設定します。

継続時間 (1〜43200)

ディスク使用率の通知レベルの異常を検出する時間を設定します。
指定した時間以上連続してしきい値を超過した場合、異常を検出します。

空き容量

ディスク空き容量の監視を行うかどうかを設定します。

- チェックボックスがオン
  ディスク空き容量の監視を行います。
- チェックボックスがオフ
  ディスク空き容量の監視を行いません。

警告レベル (1〜4294967295)

ディスク空き容量の警報レベルの異常を検出する容量（MB）を設定します。

通知レベル (1〜4294967295)

ディスク空き容量の通知レベルの異常を検出する容量（MB）を設定します。

継続時間 (1〜43200)

ディスク空き容量の通知レベルの異常を検出する時間を設定します。
指定した時間以上連続してしきい値を超過した場合、異常を検出します。

i ノード使用率

i ノード使用率の監視を行うかどうかを設定します。

- チェックボックスがオン
  i ノード使用率の監視を行います。
- チェックボックスがオフ
  i ノード使用率の監視を行いません。

警告レベル (1〜100)

i ノード使用率の警報レベルの異常を検出するしきい値を設定します。

通知レベル (1〜100)

i ノード使用率の通知レベルの異常を検出するしきい値を設定します。

継続時間 (1〜43200)

i ノード使用率の通知レベルの異常を検出する時間を設定します。
指定した時間以上連続してしきい値を超過した場合、異常を検出します。

6.34.2 システムモニタリソースの注意事項

回復対象には System Resource Agent がリソース監視の異常を検出した際のフェイルオーバ対象リソースを指定してください。

System Resource Agent の設定値は、デフォルトで使用することを推奨します。

以下のような場合には、リソース監視の異常を検出できないことがあります。

- システム全体のリソース監視で、しきい値をはさんで増減を繰り返している場合

動作中に OS の日付/時刻を変更した場合、10 分間隔で行っている解析処理のタイミングが日付/時刻変更後の最初の一回だけずれてしまいます。以下のようなことが発生するため、必要に応じてクラスタのサスペンド・リジュームを行ってください。

- 異常として検出する経過時間を過ぎても、異常検出が行われない。
- 異常として検出する経過時間前に、異常検出が行われる。

クラスタのサスペンド・リジュームを行った場合、その時点から情報の収集を開始します。

システムリソースの使用量の解析は 10 分間隔で行います。そのため、監視継続時間を経過してから最大 10 分後に異常を検出する場合があります。

ディスクリソースの使用量の解析は 60 分間隔で行います。そのため、監視継続時間を経過してから最大 60 分後に異常を検出する場合があります。

ディスクリソースの空き容量監視にて指定するディスクサイズは、実際のディスクサイズより小さい値を指定してください。大きい値を指定した場合、空き容量不足として異常検出します。

監視中のディスクを交換した場合、交換前と交換後のディスクにて以下のいずれかが異なる場合、それまでの解析情報はクリアします。

- ディスクの総容量
- ファイルシステム

スワップ領域を割り当てていないマシンでは、システムの総仮想メモリ使用量の監視のチェックを外してください。

ディスクリソース監視機能は、ディスクデバイス以外は監視対象外です。

System Resource Agent で収集しているディスク使用率は、ディスク総容量とディスク使用可能容量で計算しています。df(1) コマンドで表示されるディスク使用率とは算出方法の違いにより、値が若干異なる場合があります。

ディスクリソース監視機能で同時に監視できる最大のディスク数は 64 台です。

システムモニタリソースは収集した統計情報および解析情報をファイル出力します。これらのファイル数が下記最大個数に達した場合には、古いファイルから削除を行います。(下記文中の <*data* **パス**> は <**インストールディレクトリ**>/ha/sra/data/ となります。)

- システムリソースの統計情報

  パス: <*data* **パス**>/hasrm_monitor_list.xml.*YYYYMMDDhhmmss*.tar.gz

  最大個数: 1500 個

- システムリソースの解析情報

  パス: <*data* **パス**>/hasrm_analyze_list.xml.*YYYYMMDDhhmmss*.tar.gz

  最大個数: 3 個

- ディスクリソースの統計情報

  パス: <*data* **パス**>/hasrm_diskcapacity_monitor_list.xml.*YYYYMMDDhhmmss*.tar.gz

  最大個数: 10 個

- ディスクリソースの解析情報

  パス: <*data* **パス**>/hasrm_diskcapacity_analyze_list.xml.*YYYYMMDDhhmmss*.tar.gz

  最大個数: 3 個

6.34.3 システムモニタリソースの監視方法

システムモニタリソースは、以下の監視を行います。
システムおよびディスクのリソースの使用量を継続的に収集し、解析します。
リソースの使用量があらかじめ設定したしきい値以上になった場合、異常を検出します。
異常を検出した状態が監視継続時間連続すると、リソース監視の異常を通知します。

システムリソース監視をデフォルト値で運用した場合、リソースの使用量が 90% 以上の状態が連続すると、 60 分後にリソース監視の異常を通知します。

以下に、システムリソース監視をデフォルト値で運用した場合の総メモリ使用量の異常検出の例を示します。

- 総メモリ使用量が経過時間と共に総メモリ使用量のしきい値以上の状態が続き、一定時間以上になった

以下の図では、総メモリ使用量がしきい値（90%）以上の状態が続き、連続して監視継続時間（60 分）以上になったため、総メモリ使用量の異常を検出します。

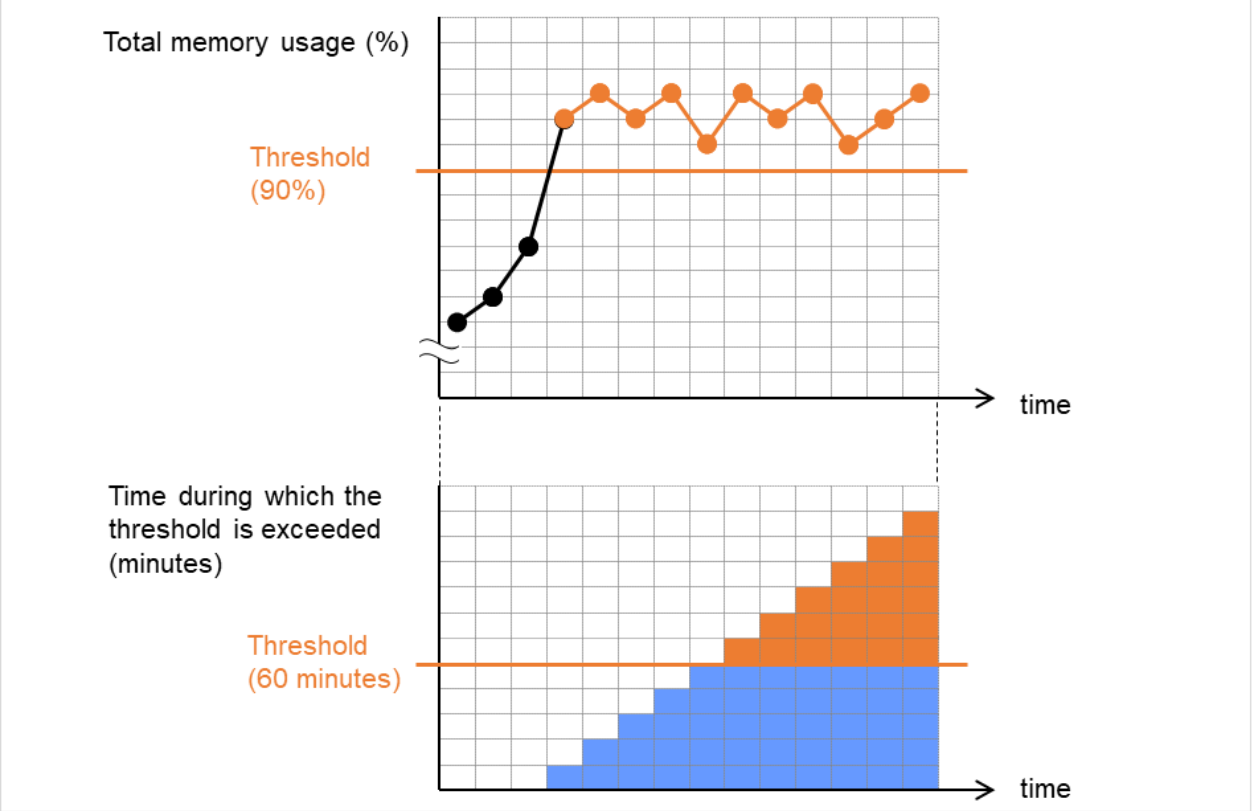


図 6.17　総メモリ使用量のしきい値以上の状態が一定時間続いた場合（異常検出する）

- 総メモリ使用量が経過時間と共に総メモリ使用のしきい値の前後で増減し、連続して総メモリ使用量のしきい値以上にならない

  以下の図では、総メモリ使用量は一時的に総メモリ使用量のしきい値（90%）以上になります。しかし、そのしきい値を超える状態も監視継続時間（60 分）連続することなく推移しているため、総メモリ使用量の異常を検出しません。

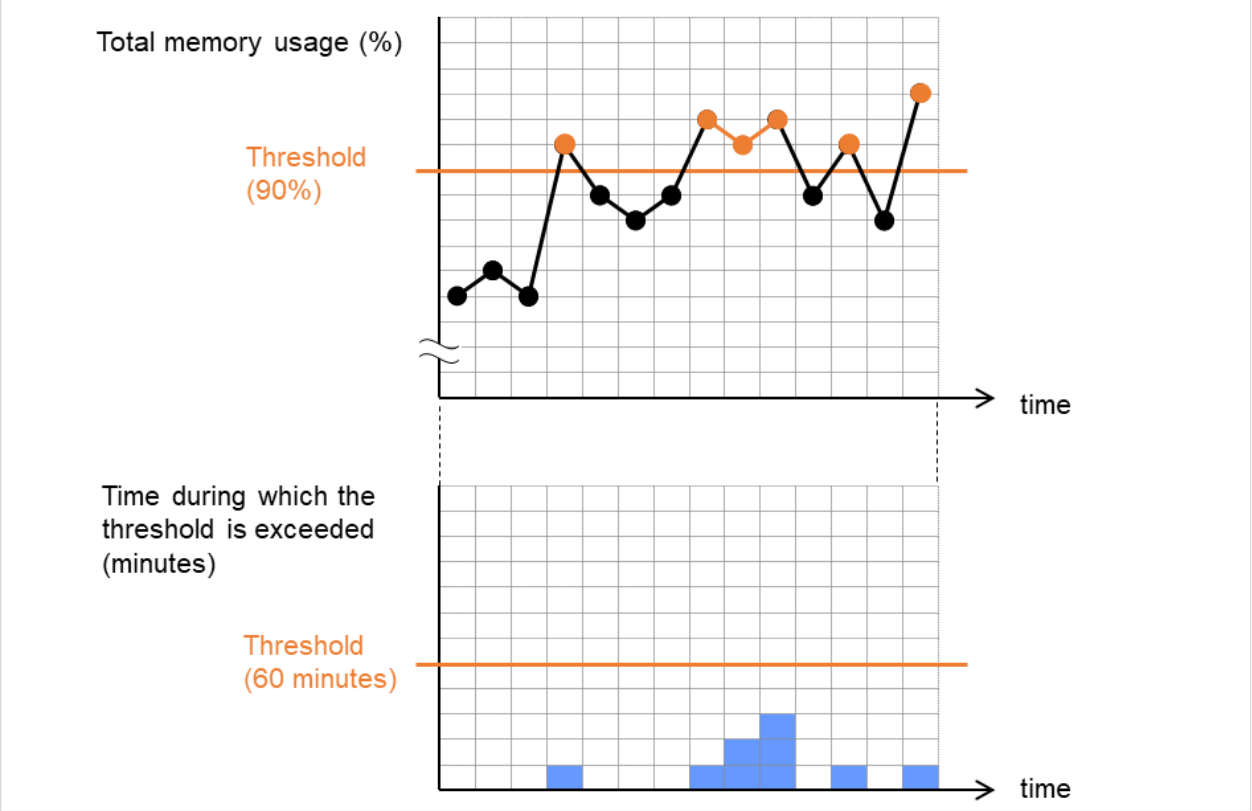


図 6.18　総メモリ使用量のしきい値以上の状態が一定時間続かない場合（異常検出しない）

ディスクリソース監視をデフォルト値で運用した場合、 24 時間後に通知レベルの異常を通知します。

以下に、ディスクリソース監視をデフォルト値で運用した場合のディスク使用率の異常検出の例を示します。

警告レベルのディスク容量監視

- ディスク使用率が警告レベル上限値で指定された一定のしきい値以上になった

  ディスク使用率が警告レベル上限値を超えたため、ディスク容量監視異常と判定します。

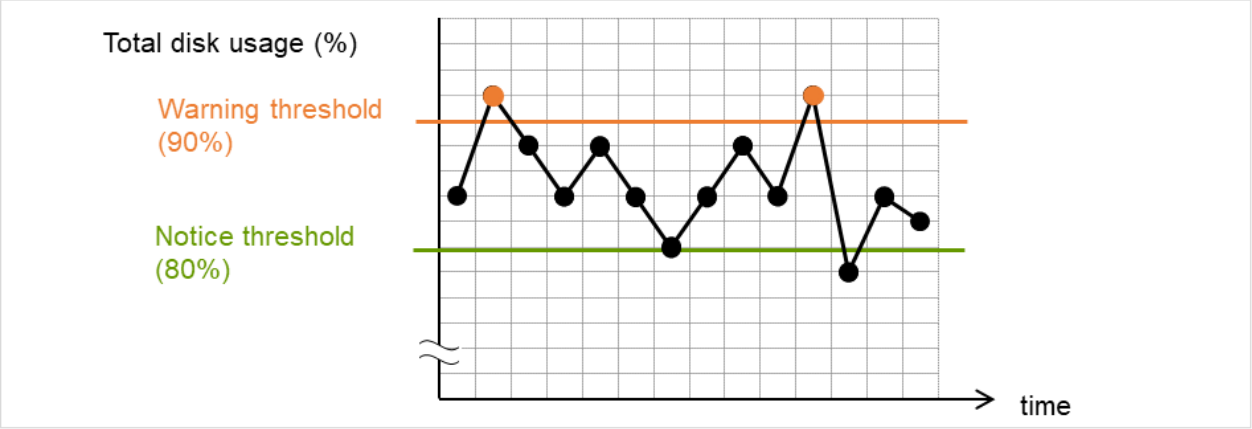


図 6.19　ディスク使用率が警告レベル上限値以上になった場合（異常検出する）

- ディスク使用率が一定の範囲内で増減し、警告レベル上限値で指定された一定のしきい値以上にならない

  ディスク使用率は警告レベル上限値を超えない範囲で増減しているため、ディスク容量監視異常と判定しません。

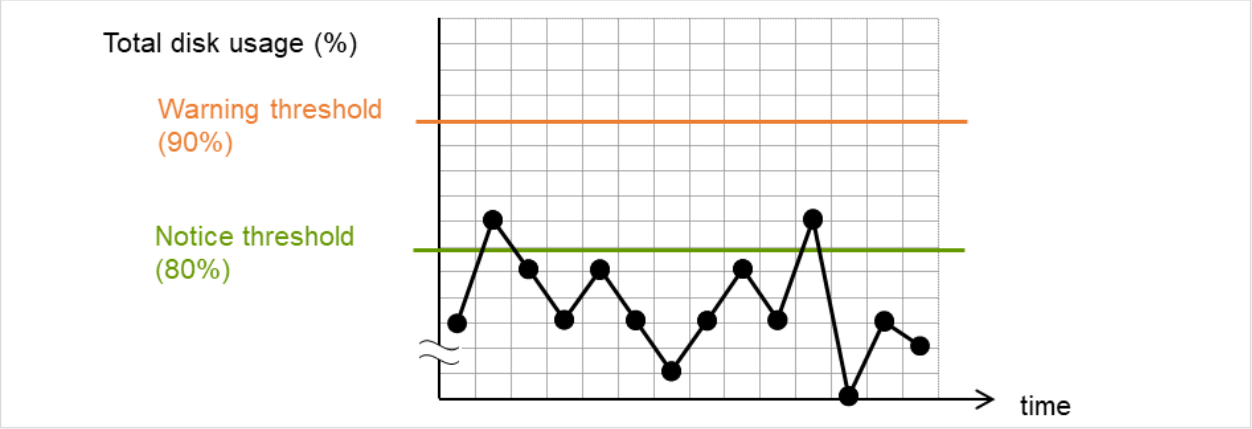


図 6.20　ディスク使用率が警告レベル上限値以上にならない場合（異常検出しない）

通知レベルのディスク容量監視

- ディスク使用率が経過時間と共に通知レベル上限値で指定された一定のしきい値以上の状態が続き、一定時間以上になった

  ディスク使用率が通知レベル上限値を連続して超えたため、ディスク容量監視異常と判定します。

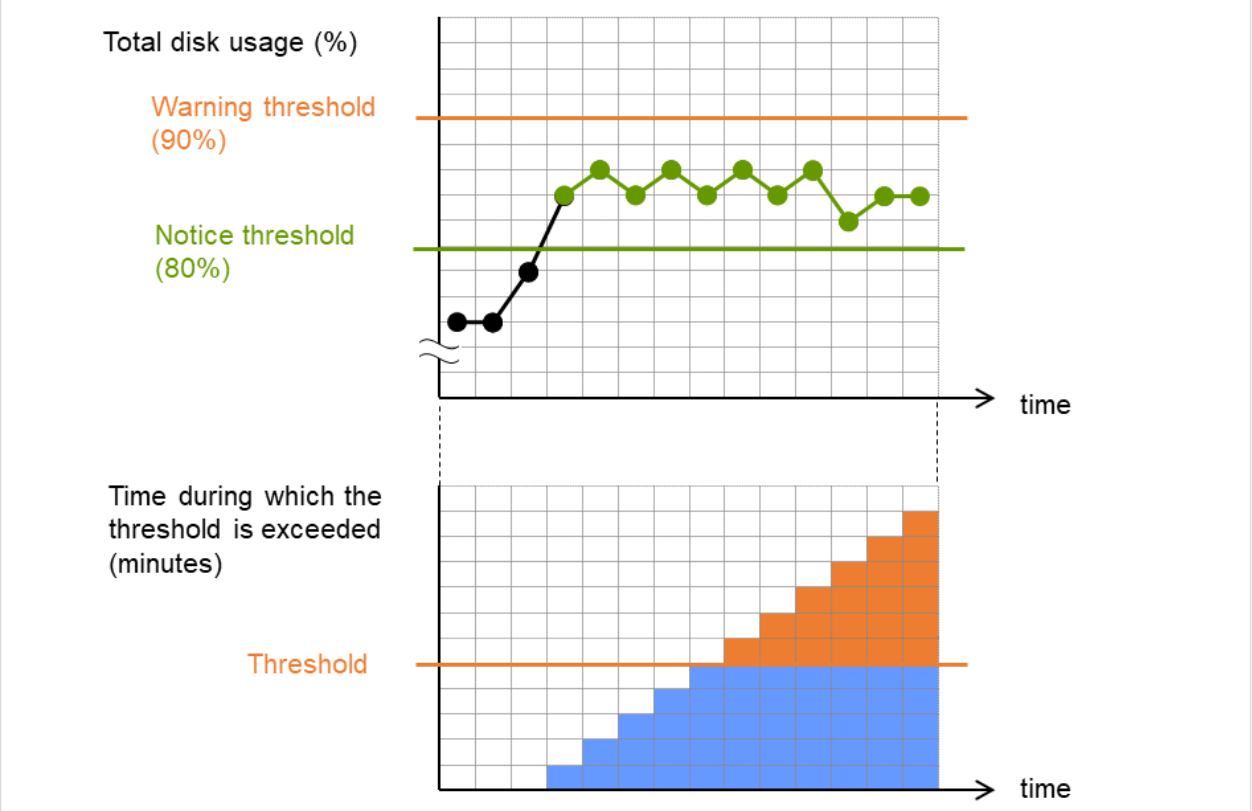


図 6.21　ディスク使用率において、通知レベル上限値以上の状態が一定時間続いた場合（異常検出する）

- ディスク使用率が一定の範囲内で増減し、通知レベル上限値で指定された一定のしきい値以上にならない

  ディスク使用率は通知レベル上限値の前後で増減しているため、ディスク容量監視異常と判定しません。

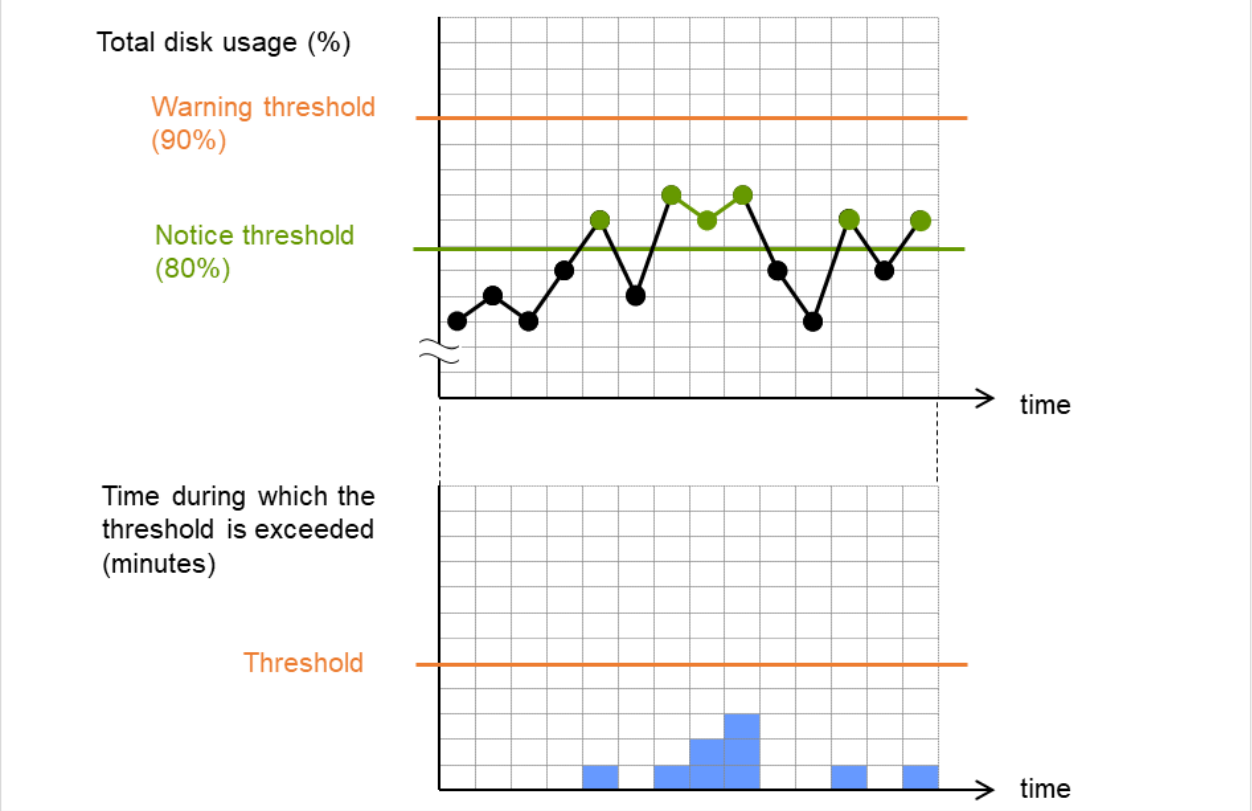


図 6.22　ディスク使用率において、通知レベル上限値以上の状態が一定時間続かない場合（異常検出しない）

6.35 プロセスリソースモニタリソースの設定

プロセスリソースモニタリソースは、プロセスが使用するリソースの統計情報を継続的に収集し、一定のナレッジ情報にしたがい解析を行います。解析の結果からリソース枯渇の発生を早期検出する機能を提供します。

6.35.1 監視 (固有) タブ

プロセス名 (1023 バイト以内)

監視対象プロセスのプロセス名を設定します。プロセス名を設定しない場合、起動中のすべてのプロセスが対象となります。

また、次の 3 つのパターンでプロセス名のワイルドカード指定が可能です。このパターン以外の指定はでき

ません。

【前方一致】 ＜プロセス名に含まれる文字列＞*

【後方一致】 *＜プロセス名に含まれる文字列＞

【部分一致】 *＜プロセス名に含まれる文字列＞*

監視対象プロセス名に指定できるプロセス名は 1023 バイトまでです。1023 バイトを超えるプロセス名を持つプロセスを監視対象として指定する場合は、ワイルドカード（＊）を使って指定します。

監視対象プロセスのプロセス名が 1023 バイトより長い場合、プロセス名として認識できるのはプロセス名の先頭から 1023 バイトまでです。ワイルドカード（＊）を使って指定する場合は、1024 バイトまでに含まれる文字列を指定してください。

監視対象プロセス名は、実際に動作しているプロセスのプロセス名を ps(1) コマンド等で確認し設定してください。

- 実行結果の例

```
UID        PID  PPID  C STIME TTY          TIME CMD
root         1     0  0 Sep12 ?        00:00:00 init [5]
:
root      5314     1  0 Sep12 ?        00:00:00 /usr/sbin/acpid
root      5325     1  0 Sep12 ?        00:00:00 /usr/sbin/sshd
htt       5481     1  0 Sep12 ?        00:00:00 /usr/sbin/htt -retryonerror 0
```

上記のコマンド実行結果から /usr/sbin/htt を監視する場合、

/usr/sbin/htt -retryonerror 0 を監視対象プロセス名に指定します。

監視対象プロセス名に指定したプロセス名はプロセスの引数もプロセス名の一部として監視対象のプロセスを特定します。監視対象プロセス名を指定する場合は、引数を含めたプロセス名を指定してください。引数を含めずプロセス名のみ監視したい場合は、ワイルドカード（＊）を使い、引数を含めない前方一致または部分一致で指定してください。

CPU 使用率の監視

CPU 使用率の監視を行うかどうかを設定します。

- チェックボックスがオン
  CPU 使用率の監視を行います。
- チェックボックスがオフ

CPU 使用率の監視を行いません。

使用率（1〜100）

CPU 使用率の異常を検出するしきい値を設定します。

継続時間（1〜129600）

CPU 使用率の異常を検出する時間を設定します。

指定した時間以上連続してしきい値を超過した場合、異常を検出します。

メモリ使用量の監視

メモリ使用量の監視を行うかどうかを設定します。

- チェックボックスがオン

  メモリ使用量の監視を行います。

- チェックボックスがオフ

  メモリ使用量の監視を行いません。

初回監視時からの増加率（1〜1000）

メモリ使用量の異常を検出するしきい値を設定します。

最大更新回数（1〜129600）

メモリ使用量の異常を検出する更新回数を設定します。

指定した更新回数以上連続してしきい値を超過した場合、異常を検出します。

オープンファイル数の監視（最大値）

オープンファイル数の監視（最大値）を行うかどうかを設定します。

- チェックボックスがオン

  オープンファイル数の監視を行います。

- チェックボックスがオフ

  オープンファイル数の監視を行いません。

更新回数（1〜1024）

オープンファイル数の異常を検出する更新回数を設定します。

オープンファイル数の最大値を指定した回数以上更新した場合、異常を検出します。

オープンファイル数の監視（カーネル上限値）

オープンファイル数の監視（カーネル上限値）を行うかどうかを設定します。

- チェックボックスがオン

オープンファイル数の監視を行います。

- チェックボックスがオフ

  オープンファイル数の監視を行いません。

割合（1～100）

オープンファイル数の異常を検出するしきい値（カーネル上限値に対する割合）を設定します。

スレッド数の監視

スレッド数の監視を行うかどうかを設定します。

- チェックボックスがオン

  スレッド数の監視を行います。

- チェックボックスがオフ

  スレッド数の監視を行いません。

継続時間（1～129600）

スレッド数の異常を検出する時間を設定します。

スレッド数が増加し、指定した時間以上経過したプロセスがある場合、異常を検出します。

ゾンビプロセスの監視

ゾンビプロセスの監視を行うかどうかを設定します。

- チェックボックスがオン

  ゾンビプロセスの監視を行います。

- チェックボックスがオフ

  ゾンビプロセスの監視を行いません。

継続時間（1～129600）

ゾンビプロセスを検出する時間を設定します。

ゾンビプロセスとなって指定時間以上経過したプロセスがある場合、異常を検出します。

同一名プロセスの監視

同一名プロセスの監視を行うかどうかを設定します。

- チェックボックスがオン

  同一名プロセスの監視を行います。

- チェックボックスがオフ

  同一名プロセスの監視を行いません。

個数（1〜10000）

同一名プロセスの異常を検出する個数を設定します。
同一名プロセスが指定した個数以上存在する場合、異常を検出します。

6.35.2 プロセスリソースモニタリソースの注意事項

プロセスリソースモニタリソースの設定値は、デフォルトで使用することを推奨します。

スワップアウトされているプロセスについては、リソース異常の検出対象になりません。

動作中に OS の日付/時刻を変更した場合、10 分間隔で行っている解析処理のタイミングが日付/時刻変更後の最初の一回だけずれてしまいます。以下のようなことが発生するため、必要に応じてクラスタのサスペンド・リジュームを行ってください。

- 異常として検出する経過時間を過ぎても、異常検出が行われない。
- 異常として検出する経過時間前に、異常検出が行われる。

クラスタのサスペンド・リジュームを行った場合、その時点から情報の収集を開始します。

プロセスリソースの使用量の解析は 10 分間隔で行います。そのため、監視継続時間を経過してから最大 10 分後に異常を検出する場合があります。

プロセスリソースモニタリソースは収集した統計情報および解析情報をファイル出力します。これらのファイル数が下記最大個数に達した場合には、古いファイルから削除を行います。(下記文中の <data パス> は <インストールディレクトリ>/ha/sra/data/ となります。)

- プロセスリソースの統計情報
  パス: <data パス>/hasrm_monitor_list.xml.YYYYMMDDhhmmss.tar.gz
  最大個数: 1500 個
- プロセスリソースの解析情報
  パス: <data パス>/hasrm_analyze_list.xml.YYYYMMDDhhmmss.tar.gz
  最大個数: 3 個

プロセスリソースモニタリソースのステータスを異常から正常に戻すには、以下のいずれかを実施してください。

- クラスタのサスペンド・リジューム
- クラスタの停止・開始

6.35.3 プロセスリソースモニタリソースの監視方法

プロセスリソースモニタリソースは、以下の監視を行います。

プロセスリソースの使用量を継続的に収集し、解析します。

リソースの使用量があらかじめ設定したしきい値以上になった場合、異常を検出します。

異常を検出した状態が監視継続時間連続すると、リソース監視の異常を通知します。

プロセスリソース監視（CPU、メモリ、オープンファイル数、ゾンビプロセス）をデフォルト値で運用した場合、24 時間後にリソース監視の異常を通知します。

以下に、プロセスリソース監視のメモリ使用量の異常検出の例を示します。

- メモリ使用量が経過時間と共に増減しながら、規定回数以上最大値を更新し、増加率が初期値の 10% 以上になった最大値更新回数が 24 時間（デフォルト）以上になり、増加率も初期値の 10 %を上回っているため、メモリリークと判定します。

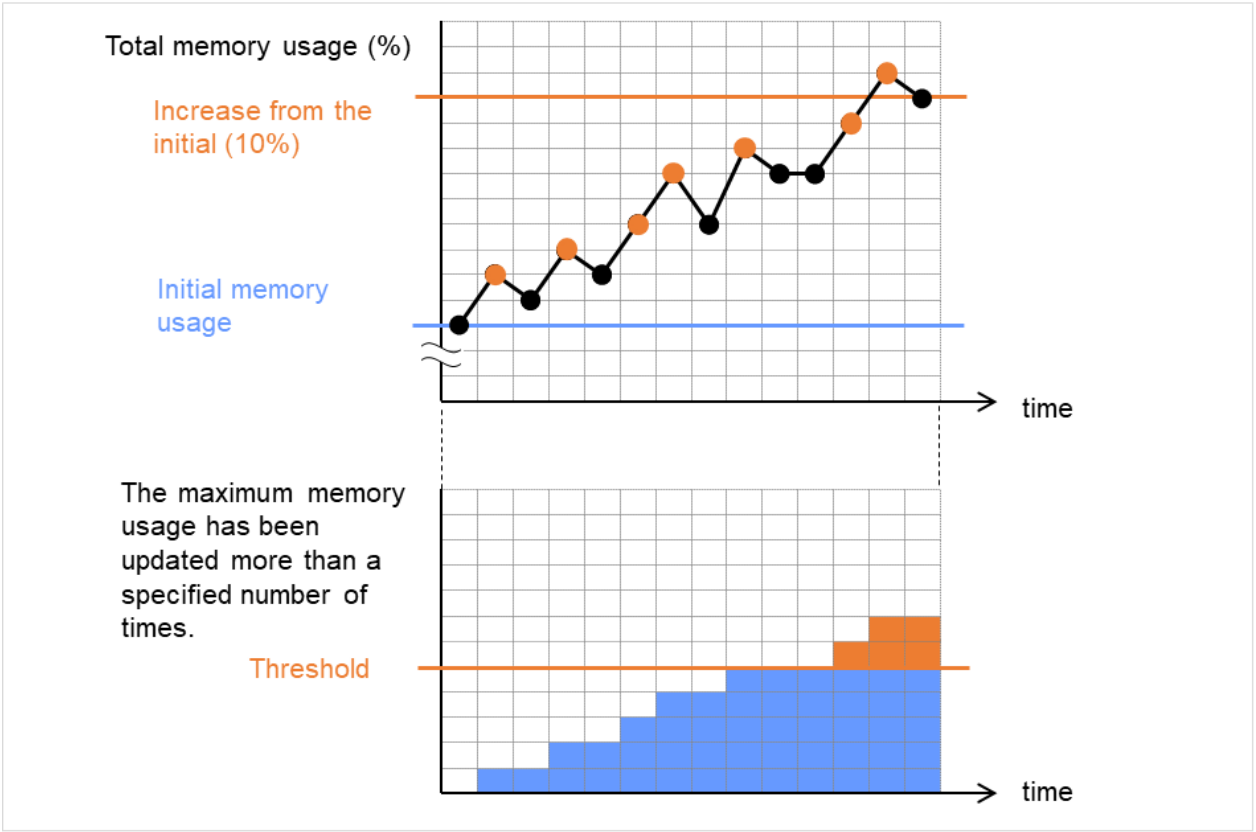


図 6.23　メモリ使用量が規定回数以上最大値を更新し、増加率が初期値の 10% を超過（異常検出する）

- メモリ使用量が経過時間と共に一定の範囲内で増減

  メモリ使用量は、一定の値未満の範囲で増減しているため、メモリリークと判定しません。

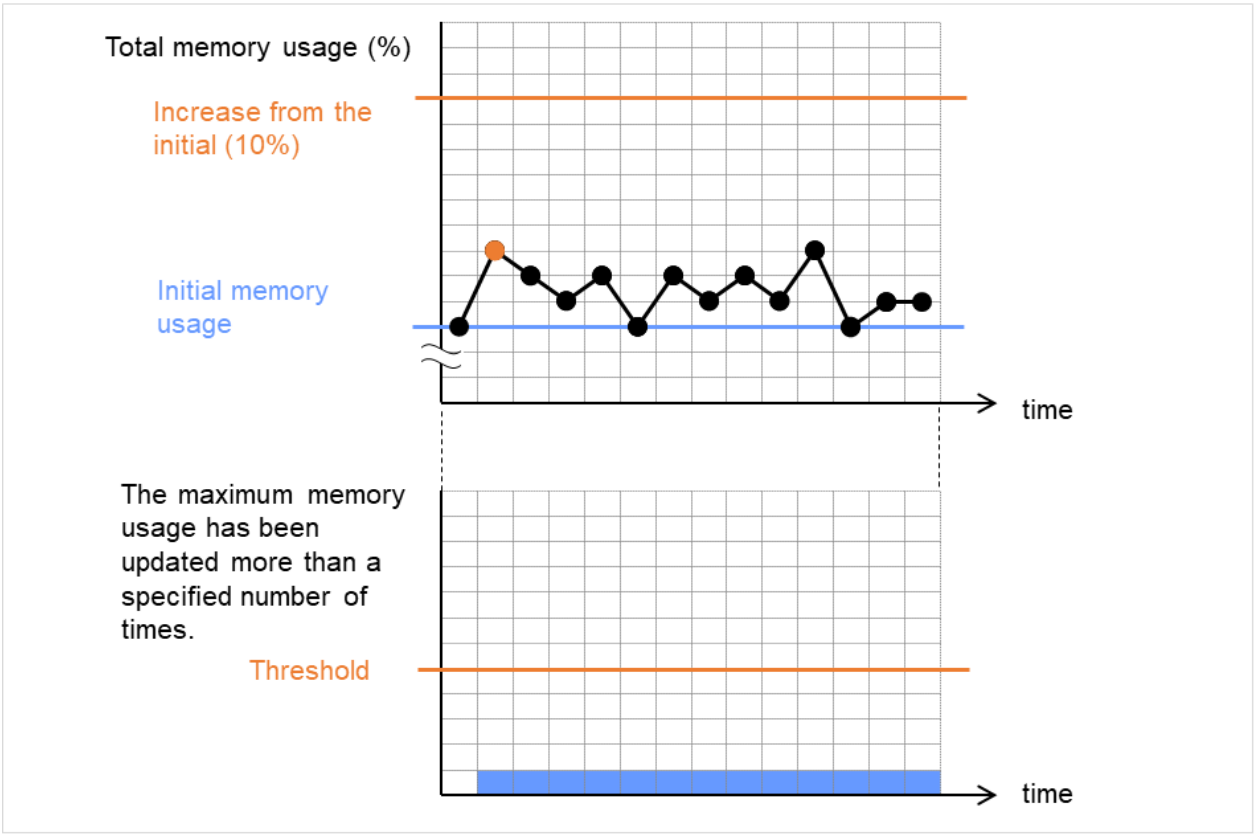


図 6.24　メモリ使用量が一定の範囲内で増減（異常検出しない）

第 7 章

ハートビートリソースの詳細

本章では、ハートビートリソースの詳細について説明します。

CLUSTERPRO X SingleServerSafe は、クラスタリングソフトウェアである CLUSTERPRO X との操作性などにおける親和性を高めるために、共通の画面を使用しています。

本章で説明する項目は以下のとおりです。

7.1 ハートビートリソース一覧

サーバの死活監視を行います。ハートビートデバイスには以下の種類があります。

ハートビートリソース名	略称	機能概要
LAN ハートビートリソース	lanhb	LAN を使用してサーバの死活監視を行います

- LAN ハートビートは 1 つ設定する必要があります。

7.2 LAN ハートビートリソースの設定

7.2.1 LAN ハートビートリソースの注意事項

- LAN ハートビートリソースは 1 つ設定する必要があります。

第 8 章

その他の設定の詳細

本章では、CLUSTERPRO X SingleServerSafe のその他の項目についての詳細を説明します。

CLUSTERPRO X SingleServerSafe は、クラスタリングソフトウェアである CLUSTERPRO X との操作性などにおける親和性を高めるために、共通の画面を使用しています。

本章で説明する項目は以下のとおりです。

8.1 クラスタプロパティ

「クラスタのプロパティ」では、CLUSTERPRO X SingleServerSafe の詳細情報の表示や設定変更ができます。

8.1.1 情報タブ

クラスタ名の表示、コメントの登録、変更を行います。

クラスタ名

クラスタ名を表示します。ここでは名前の変更はできません。

コメント (127 バイト以内)

コメントを設定します。半角英数字のみ入力可能です。

言語

表示言語を以下の中から選択します。Cluster WebUI を動作させる OS の言語 (ロケール) に設定してください。

- 英語
- 日本語

8.1.2 インタコネクトタブ

使用しません。

8.1.3 フェンシングタブ

使用しません。

8.1.4 タイムアウトタブ

タイムアウトなどの値を設定します。

サービス起動遅延時間 (0 ～ 9999)

OS 起動時にクラスタサービスの起動を遅延させる時間です。

同期待ち時間 (0 ～ 99)

使用しません。

ハートビート

ハートビート間隔および、ハートビートタイムアウトです。

- インターバル (1 ～ 99)

  ハートビートの間隔です。

- タイムアウト (2 ～ 9999)

  ハートビートタイムアウトです。ここで設定された時間の間無応答が続くとサーバダウンとみなします。

  - インターバルより大きい値である必要があります。

内部通信タイムアウト (1 ～ 9999)

CLUSTERPRO のコマンドを実行する際や、Cluster WebUI での操作、画面表示する際などに行われる CLUSTERPRO サーバの内部通信で使うタイムアウトです。

なお、以下のコマンドでは [--apito] オプションを使用することで、一時的に内部通信タイムアウトを変更することが可能です：

- clpgrp
- clprsc

- clpdown
- clpstdn
- clpcl

注釈:

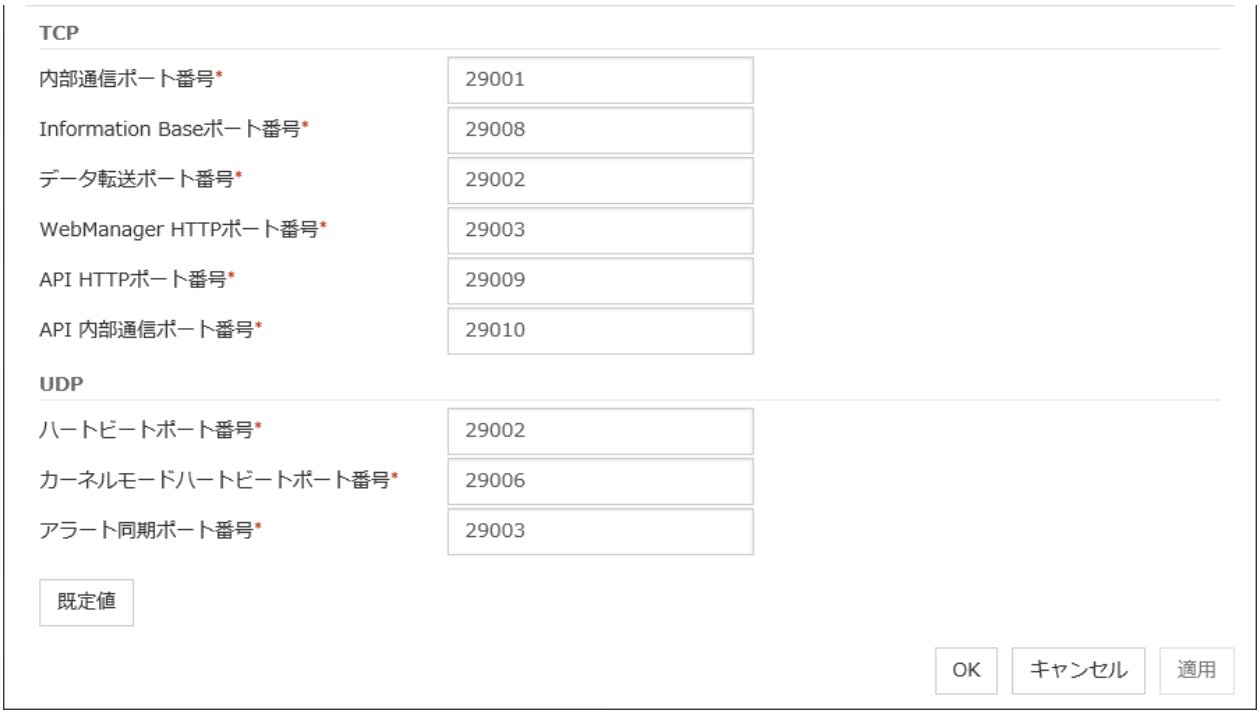
内部通信タイムアウトを極端に大きな値に設定すると、ハートビートが途絶した場合に clpstat コマンドの実行や Cluster WebUI の表示に要する時間に大きく影響します。
既定値を設定することを推奨します。

既定値

既定値に戻すときに使用します。[既定値] をクリックすると全ての項目に既定値が設定されます。

8.1.5 ポート番号タブ

TCP ポート番号、UDP ポート番号を設定します。



TCP

TCP の各ポート番号は重複できません。

- 内部通信ポート番号 (1〜65535[*3])
  内部通信で使うポート番号です。
- Information Base ポート番号 (1〜65535[*3])
  クラスタ情報管理で使うポート番号です。
- データ転送ポート番号 (1〜65535[*3])
  トランザクション (構成情報反映/バックアップ、ライセンス情報送受信、コマンド実行) で使うポート番号です。
- WebManager HTTP ポート番号 (1〜65535[*3])
  ブラウザが CLUSTERPRO サーバと通信するときに使うポート番号です。
- API HTTP ポート番号 (1〜65535[*3])
  Restful API クライアントが CLUSTERPRO サーバと通信するときに使うポート番号です。
- API 内部通信ポート番号 (1〜65535[*3])
  Restful API の内部通信で使うポート番号です。

UDP

UDP の各ポート番号は重複できません。

- カーネルモードハートビートポート番号 (1〜65535[*3])
  カーネルモードハートビートで使うポート番号です。
- アラート同期ポート番号 (1〜65535[*3])
  サーバ間でアラートメッセージを同期するときに使うポート番号です。

既定値

既定値に戻すときに使用します。[既定値] をクリックすると全ての項目に既定値が設定されます。

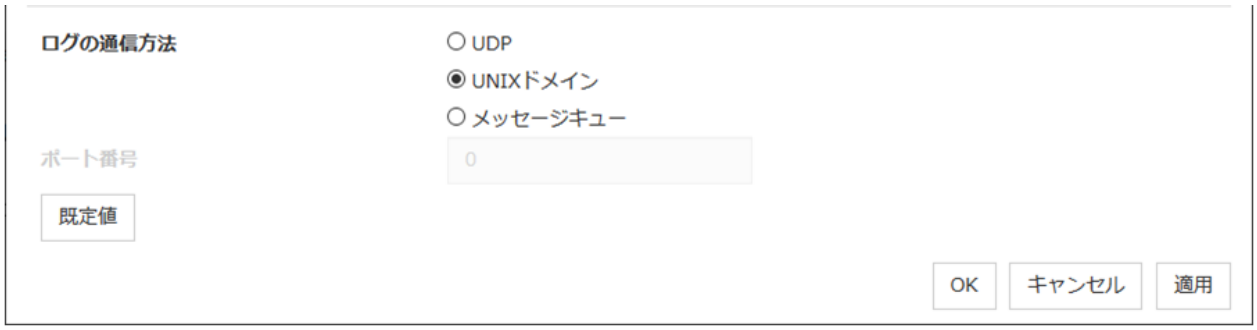
8.1.6 ポート番号 (ミラー) タブ

使用しません。

[*3] Well-known ポート、特に 1〜1023 番の予約ポートの使用は推奨しません。

8.1.7 ポート番号 (ログ) タブ

ログの通信方法を設定します。



ログの通信方法

- UDP

  ログの通信方法に UDP を使用します。

- UNIX ドメイン

  ログの通信方法に UNIX ドメインを使用します。

- メッセージキュー

  ログの通信方法に メッセージキューを使用します。

ポート番号 (1〜65535)

ログの通信方法で UDP を選択した場合に使うポート番号です。[ポート番号] タブの UDP の各ポート番号と重複することはできません。

既定値

既定値に戻すときに使用します。[既定値] をクリックすると全ての項目に既定値が設定されます。

8.1.8 監視タブ

監視に関する設定をします。

シャットダウン監視

CLUSTERPRO のコマンドでサーバシャットダウンを実行したときに、OS がストールしているか否か監視します。

クラスタサービスは OS がストールしていると判断すると強制的にサーバをリセットまたはパニックします。サーバのパニックは、監視方法 keepalive の場合のみ設定可能です。

- 常に実行する

  常にシャットダウン監視をします。

- グループ非活性処理に失敗した場合のみ実行する

  グループの非活性に失敗した場合のみシャットダウン監視をします。

- 実行しない

  シャットダウン監視をしません。

監視方法

シャットダウン監視を行う場合の監視方法を以下の中から選択します。

- softdog
- ipmi
- keepalive

タイムアウト発生時動作

OS がストールしていると判断した場合の動作を以下の中から選択します。

- RESET

  サーバをリセットします。

- PANIC

  サーバをパニックさせます。監視方法に keepalive を選択した場合のみ設定できます。

- NMI

  サーバへ NMI を発生させます。監視方法に ipmi を選択した場合のみ設定できます。

SIGTERM を有効にする

シャットダウン監視を行う場合に SIGTERM を有効にするかどうかを設定します。

注釈: [監視方法] で ipmi を選択して、[SIGTERM を有効にする] をオフに設定にしている場合、OS のシャットダウンが正常に終了してもリセットすることがあります。

ハートビートのタイムアウトを使用する

シャットダウン監視のタイムアウト値をハートビートタイムアウト値と連動させます。

タイムアウトを指定する (2〜9999)

シャットダウン監視のタイムアウト値としてハートビートタイムアウト値を使用しない場合にタイムアウト値を指定します。

8.1.9 リカバリタブ

リカバリに関する設定をします。

クラスタサービスのプロセス異常時動作

クラスタサービスのプロセス異常時におけるアクションを指定します。

- OS シャットダウン

  OS をシャットダウンします。

- OS 再起動

  OS を再起動します。

- sysrq パニック

  sysrq のパニックを行います。

- keepalive リセット

  clpkhb ドライバ、clpka ドライバを使用し、OS をリセットします。

- keepalive パニック

  clpkhb ドライバ、clpka ドライバを使用し、OS をパニックします。

- BMC リセット

  サーバをハードウェアリセットします。

- BMC パワーオフ

  サーバの電源をオフにします。OS の ACPI の設定により OS のシャットダウンが実行される場合があります。

- BMC パワーサイクル

  サーバのパワーサイクル （電源オフ/オン） を実行します。OS の ACPI の設定により OS のシャットダウンが実行される場合があります。

- BMC NMI

  サーバで NMI を発生させます。NMI 発生後の挙動は OS の設定に依存します。

注釈: CLUSTERPRO デーモン停止処理でグループリソースの非活性に失敗した場合も、この設定に従った動作が実行されます。

HA プロセス異常時動作

- プロセス起動リトライ回数 (0～99)

  HA プロセス異常時の再起動回数を指定します。

- リトライオーバ時の動作

  HA プロセス異常時における動作を指定します。

- クラスタサービス停止

  クラスタサービスを停止します。

- クラスタサービス停止 と OS シャットダウン

  クラスタサービスを停止し、OS をシャットダウンします。

- クラスタサービス停止と OS 再起動

  クラスタサービスを停止し、OS を再起動します。

注釈: HA プロセスは、システムモニタリソースやプロセスリソースモニタリソース、JVM モニタリソース、システムリソース情報収集機能で使用されるプロセスです。

グループリソースの活性/非活性ストール発生時動作

グループリソースの活性/非活性ストール発生時における動作を指定します。

- クラスタサービス停止と OS シャットダウン

  ストールが発生したサーバのクラスタサービスを停止し、OS をシャットダウンします。

- クラスタサービス停止と OS 再起動

  ストールが発生したサーバのクラスタサービスを停止し、OS を再起動します。

- 緊急シャットダウン

  ストールが発生したサーバをクラスタサービス停止を待ち合わせずにシャットダウンします。

- sysrq パニック

  ストールが発生したサーバで sysrq のパニックを行います。

- keepalive リセット

  ストールが発生したサーバで clpkhb ドライバ、clpka ドライバを使用し、OS をリセットします。

- keepalive パニック

  ストールが発生したサーバで clpkhb ドライバ、clpka ドライバを使用し、OS をパニックします。

- BMC リセット

  ストールが発生したサーバをハードウェアリセットします。

- BMC パワーオフ

  ストールが発生したサーバの電源をオフにします。OS の ACPI の設定により OS のシャットダウンが実行される場合があります。

- BMC パワーサイクル

  ストールが発生したサーバでパワーサイクル （電源オフ/オン） を実行します。OS の ACPI の設定により OS のシャットダウンが実行される場合があります。

- BMC NMI

  ストールが発生したサーバで NMI を発生させます。NMI 発生後の挙動は OS の設定に依存します。

- 何もしない (活性/非活性異常として扱う)

  グループリソースの活性/非活性異常検出時の復旧動作を行います。

注釈:

「何もしない (活性/非活性異常として扱う)」を指定してストールが発生した場合、グループリソースへの影響が不定となりますので、「何もしない (活性/非活性異常として扱う)」への設定変更は推奨しません。

「何もしない (活性/非活性異常として扱う)」を指定する場合は、グループリソースの活性/非活性異常検出時の復旧動作の設定を以下のようにしてください。

- 活性/非活性リトライしきい値 ： 0 回
- フェイルオーバしきい値 ： 0 回
- 最終動作 ： OS 停止を伴う動作

異常検出時の OS 停止を伴う最終動作を抑制する

[詳細設定] をクリックし、異常検出時の OS 停止を伴う最終動作の抑制を設定します。

- グループリソースの活性異常検出時

  グループリソースの活性異常検出時の最終動作が OS 停止を伴うものに設定されている場合、活性異常検出時の最終動作が抑制されます。

- グループリソースの非活性異常検出時

  グループリソースの非活性異常検出時の最終動作が OS 停止を伴うものに設定されている場合、非活性異常検出時の最終動作が抑制されます。

- モニタリソースの異常検出時

モニタリソースの異常検出時の最終動作が OS 停止を伴うものに設定されている場合、異常検出時の最終動作が抑制されます。

注釈:

- 外部連携モニタリソースは異常検出時の最終動作の抑止の対象にはなりません。
- グループリソースの活性/非活性異常検出時の最終動作、およびモニタリソースの異常検出時の最終動作で OS 停止を伴うものは以下の通りです。
  - クラスタサービス停止と OS シャットダウン
  - クラスタサービス停止と OS 再起動
  - sysrq パニック
  - keepalive リセット
  - keepalive パニック
  - BMC リセット
  - BMC パワーオフ
  - BMC パワーサイクル
  - BMC NMI

両系活性検出時のシャットダウンを抑制する

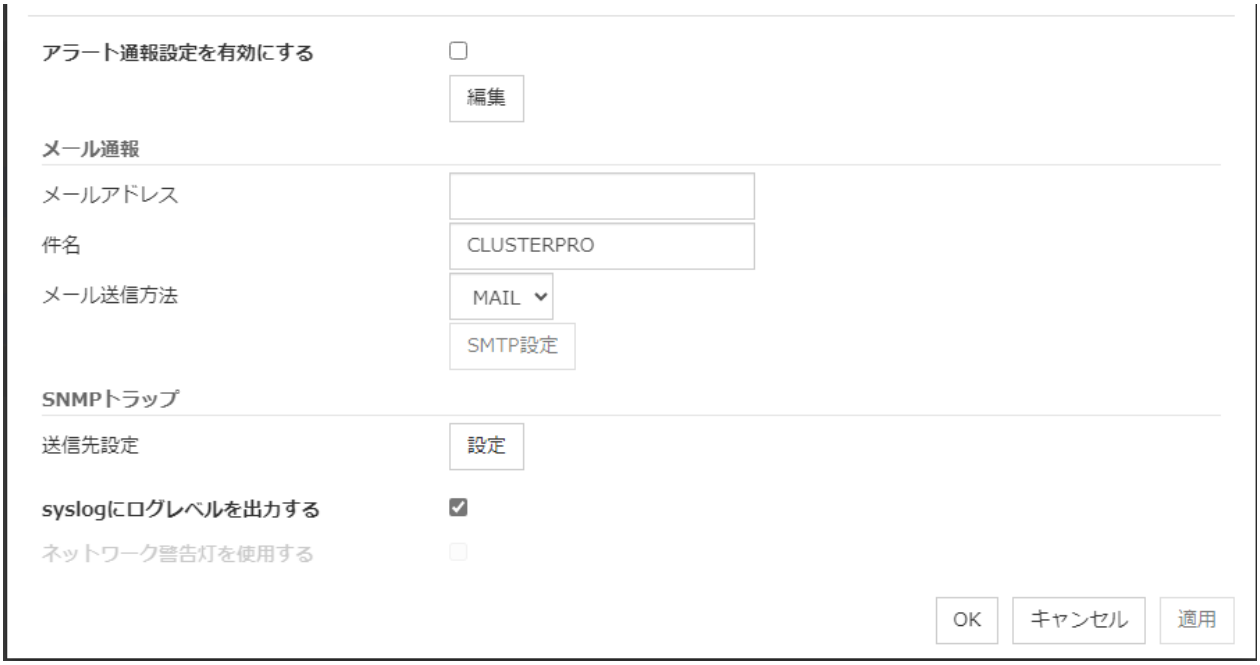
使用しません。

8.1.10 アラートサービスタブ

アラート通報の設定を行います。

メール通報の機能を使用する場合は、Alert Service のライセンスを登録してください。

注釈: メール通報機能を使用するためには CLUSTERPRO X Alert Service 5.3 for Linux を購入し、ライセンスを登録してください。



アラート通報設定を有効にする

アラート通報の設定を既定値から変更する/しない の設定をします。変更をする場合には、[編集] をクリックし、[アラート送信先の変更] ダイアログにて設定をしてください。

チェックボックスをオフにすると 変更した出力先を一時的に既定値に戻すことができます。

既定の通報先は、『操作ガイド』の「エラーメッセージ一覧」の「syslog、アラート、メール通報、SNMP トラップメッセージ、Message Topic」を参照してください。

メールアドレス (255 バイト以内)

通報先のメールアドレスを入力します。メールアドレスを複数設定する場合は、メールアドレスをセミコロンで区切ってください。

件名 (127 バイト以内)

メールの件名を入力します。

メール送信方法

メールの送信方法の設定をします。メールの送信方法として SMTP を使用する場合は、 [SMTP 設定] をクリックし、[SMTP 設定] ダイアログにて設定をしてください。

- MAIL

  mail コマンドを使います。事前に mail コマンドでメールアドレスにメールが送信されることを確認してください。

- SMTP

  SMTP サーバと直接通信をしてメール通報します。

送信先設定

SNMP トラップ送信機能の設定をします。SNMP トラップの送信先を設定する場合には [設定] をクリックし、[送信先設定] ダイアログにて送信先の設定をしてください。

syslog にログレベルを出力する

CLUSTERPRO X SingleServerSafe が動作中に出力する syslog のメッセージにレベルを付加します。

ネットワーク警告灯を使用する

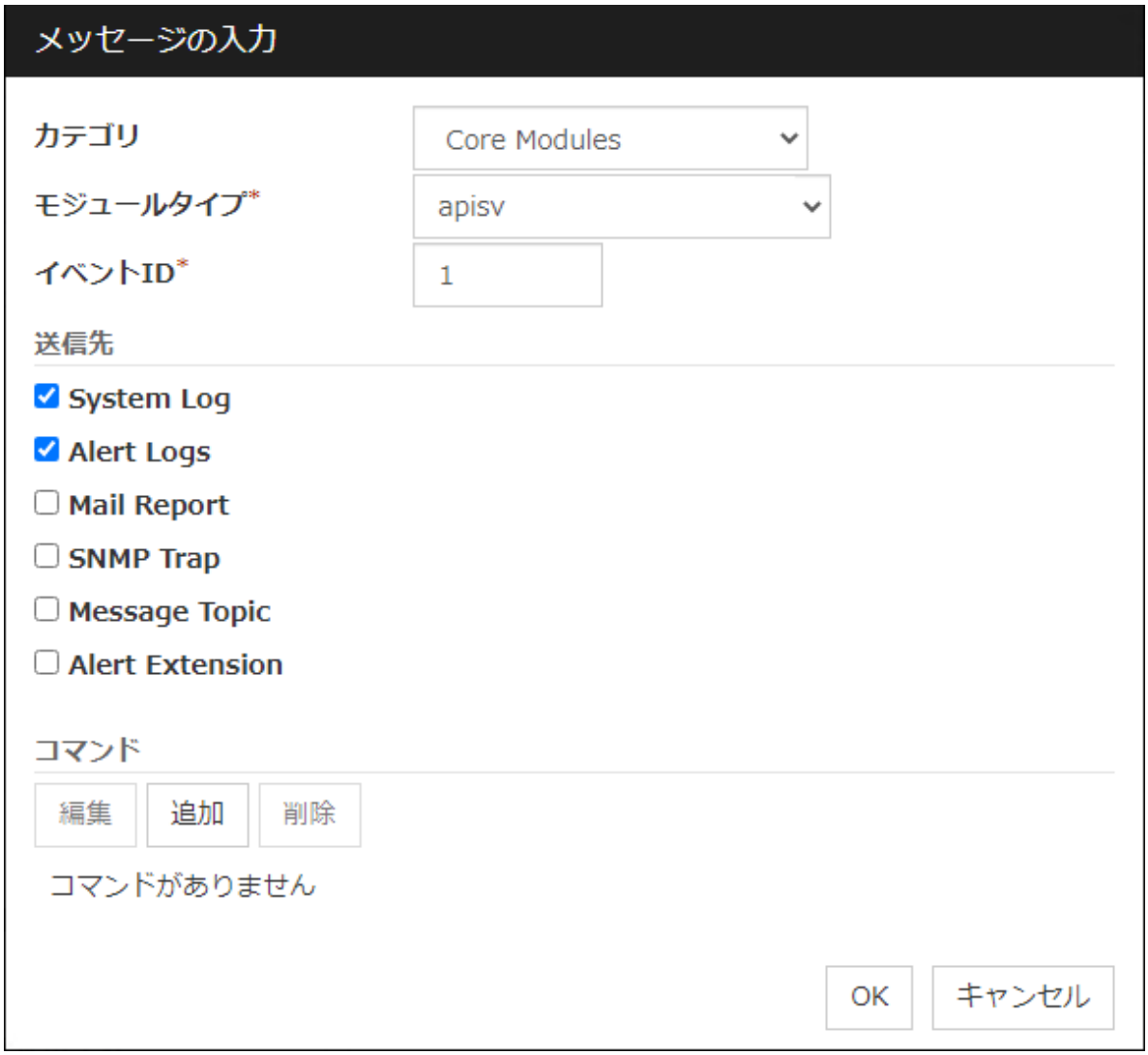
使用しません。

アラート送信先の変更

[編集] をクリックすると アラート送信先の変更ダイアログボックスが表示されます。

追加

送信先をカスタマイズしたいモジュールタイプ、イベント ID を追加します。[追加] ボタンを押すとメッセージの入力のダイアログが表示されます。



カテゴリ

モジュールタイプの大分類を選択します。

モジュールタイプ (31 バイト以内)

送信先を変更するモジュールタイプ名を選択します。

イベント ID

送信先を変更するモジュールタイプのイベント ID を入力します。イベント ID は『操作ガイド』の「エラーメッセージ一覧」の「syslog、アラート、メール通報、SNMP トラップメッセージ、Message Topic」を参照してください。

送信先

メッセージの送信として実行する処理を選択します。

- System Log

  OS の syslog へ送信します

- Alert Logs

  アラートログにメッセージを表示します。

- Mail Report

  メール通報機能で送信します。

- SNMP Trap

  SNMP トラップ送信機能で送信します。

- Message Topic

  Amazon SNS へ送信します。

- Alert Extension

  指定されたコマンドを実行します（アラート拡張機能)。 [追加] ボタン、[編集] ボタンで実行するコマンドを設定・変更します。(最大 4 つのコマンドラインを指定することが出来ます)。

追加

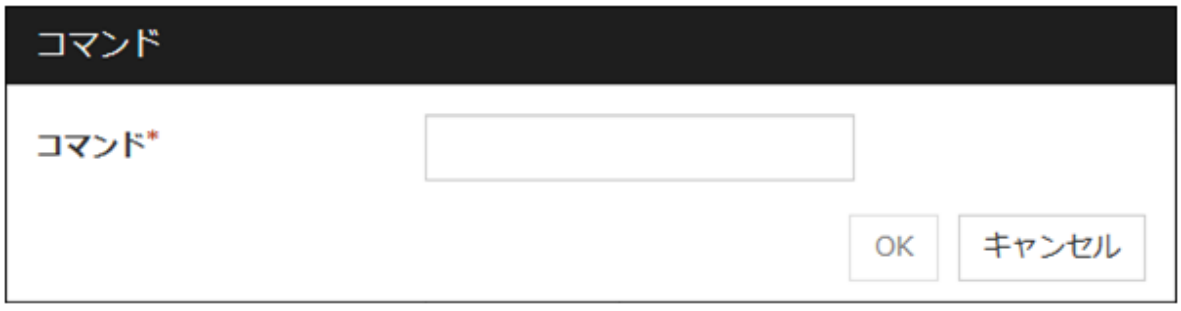
アラート拡張機能のコマンドを追加します。[追加] ボタンを押すとコマンドの入力のダイアログが表示されます。コマンドは 1 つのイベント ID について 4 個まで登録できます。

削除

アラート拡張機能のコマンドを削除する場合に使用します。コマンドを選択して、[削除] をクリックしてください。

編集

アラート拡張機能のコマンドを変更する場合に使用します。コマンドを選択して、[編集] をクリックしてください。



コマンド (511 バイト以内)

SNMP trap など通報を実行するコマンドを入力します。絶対パスで指定してください。指定したコマンドの実行結果は参照できません。

- キーワードについて

  %%MSG%% を指定すると、該当のイベント ID のメッセージ本文が挿入されます。

  1 つのコマンドに対して複数の %%MSG%% を使用することはできません。

  %%MSG%% の内容を含めて 511 バイト以内になるように設定してください。また、%%MSG%% 内に空白文字が含まれることがありますので、コマンドの引数として指定する場合には、"%%MSG%%" と指定してください。

  設定例

```
/usr/local/bin/snmptrap -v1 -c HOME 10.0.0.2 0 10.0.0.1 1 0 '' 1 s "%%MSG%%"
```

SMTP 設定

[SMTP 設定] をクリックするとメール通報で使用する [SMTP 設定] ダイアログボックスが表示されます。

メール送信文書の文字コード (127 バイト以内)

メール通報で送信するメールの文字コードを設定します。

通信応答待ち時間 (1～999)

SMTP サーバとの通信のタイムアウトを設定します。

件名のエンコードをする

メールの件名のエンコードをする/しない を設定します。

SMTP サーバ一覧

設定されている SMTP サーバを表示します。本バージョンで設定できる SMTP サーバは 1 台です。

追加

SMTP サーバを追加します。[追加] ボタンを押すと SMTP サーバの入力のダイアログが表示されます。

削除

SMTP サーバの設定を削除する場合に使用します。

編集

SMTP サーバの設定を変更する場合に使用します。

SMTP サーバ (255 バイト以内)

SMTP サーバの IP アドレスまたはホスト名を設定します。

SSL を使用する

SMTP サーバとの通信に SSL を使用するか設定します。チェックボックスがオンの場合は SSL を使用し、オフの場合は SSL を使用しません。

SSL を使用する場合は、クラスタプロパティの暗号化タブで [SSL ライブラリ] および [Crypto ライブラリ] を設定してください。

対応している OpenSSL のバージョンは『インストールガイド』 - 「CLUSTERPRO X SingleServerSafe の動作環境を確認する」 - 「ソフトウェア」 - 「暗号化を有効にする場合の動作環境」を参照してください。

接続方式

- SMTPS

  SMTP サーバとの通信に SMTPS を使用します。

- STARTTLS

  SMTP サーバとの通信に STARTTLS を使用します。

SMTP ポート番号 (1〜65535)

SMTP サーバのポート番号を設定します。

差出人メールアドレス (255 バイト以内)

メール通報で送信されるメールの送信元アドレスを設定します。

SMTP 認証を有効にする

SMTP の認証をする/しない の設定をします。

認証方式

SMTP の認証の方式を選択します。

ユーザ名 (255 バイト以内)

SMTP の認証で使用するユーザ名を設定します。

パスワード (255 バイト以内)

SMTP の認証で使用するパスワードを設定します。

送信先一覧

設定されている SNMP トラップ送信先を表示します。本バージョンで設定できる SNMP トラップ送信先は 32 件です。

追加

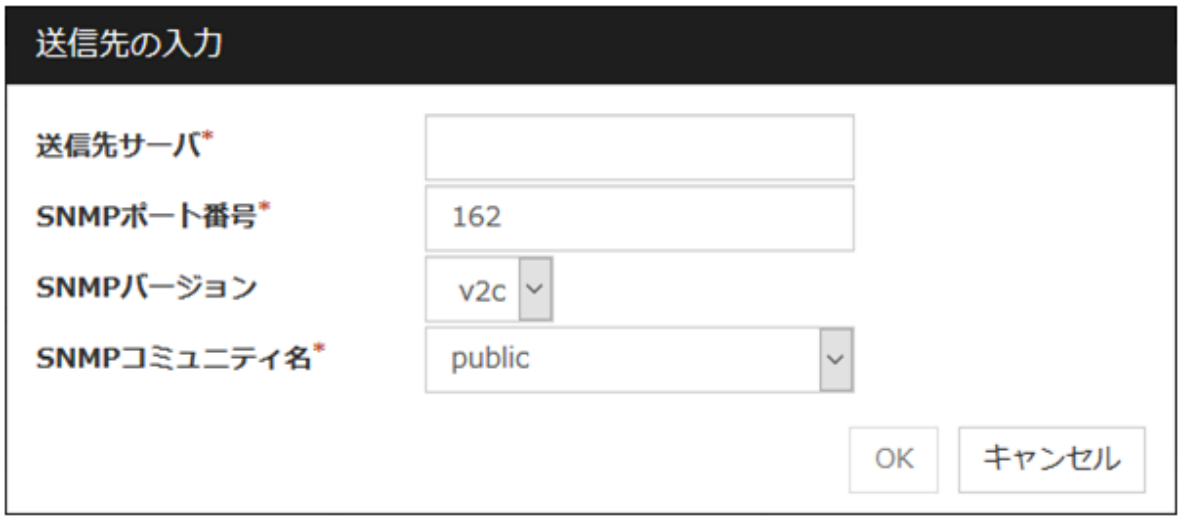
SNMP トラップ送信先を追加します。[追加] をクリックすると 送信先の入力ダイアログが表示されます。

削除

SNMP トラップ送信先の設定を削除する場合に使用します。

編集

SNMP トラップ送信先の設定を変更する場合に使用します。



送信先サーバ (255 バイト以内)

SNMP トラップ送信先のサーバ名を設定します。

SNMP ポート番号 (1-65535)

SNMP トラップ送信先のポート番号を設定します。

SNMP バージョン

SNMP トラップ送信先の SNMP バージョンを設定します。

SNMP コミュニティ名 (255 バイト以内)

SNMP トラップ送信先の SNMP コミュニティ名を設定します。

8.1.11 WebManager タブ

WebManager サーバを設定します。

WebManager サービスを有効にする

WebManager サービスを有効にします。

- チェックボックスがオン

  WebManager サービスを有効にします。

- チェックボックスがオフ

  WebManager サービスを無効にします。

通信方式

- HTTP

  クライアントとの通信に暗号化を使用しません。

- HTTPS

  クライアントとの通信に暗号化を使用します。

同時接続セッション数 (10～999)

クライアントからの同時リクエスト数を設定します。本設定を超える同時リクエストが発生した場合、リクエストは破棄されます。

パスワードによって接続を制御する

[設定] をクリックすると [パスワード] ダイアログボックスが表示されます。

クラスタパスワード方式 / OS 認証方式

Cluster WebUI にログインする方法を下記より選択します。

- クラスタパスワード方式

  設定した操作用パスワード、参照用パスワードで認証する方式です。

- OS 認証方式

  OS のユーザ、パスワードで認証する方式です。

クラスタパスワード方式

- 操作用パスワード

  Cluster WebUI に操作モード、設定モード、検証モードで接続するためのパスワードを設定します。

  [変更] をクリックすると [パスワードの変更] ダイアログボックスが表示されます。

- 参照用パスワード

  Cluster WebUI に参照モードで接続するためのパスワードを設定します。

  [変更] をクリックすると [パスワードの入力] ダイアログボックスが表示されます。

  - 古いパスワード (255 バイト以内)

    変更前のパスワードを入力します。

    古いパスワードが設定されていない場合は何も入力しません。

  - 新しいパスワード (255 バイト以内)

    新しいパスワードを入力します。

    パスワードを削除する場合は何も入力しません。

  - パスワードの確認入力 (255 バイト以内)

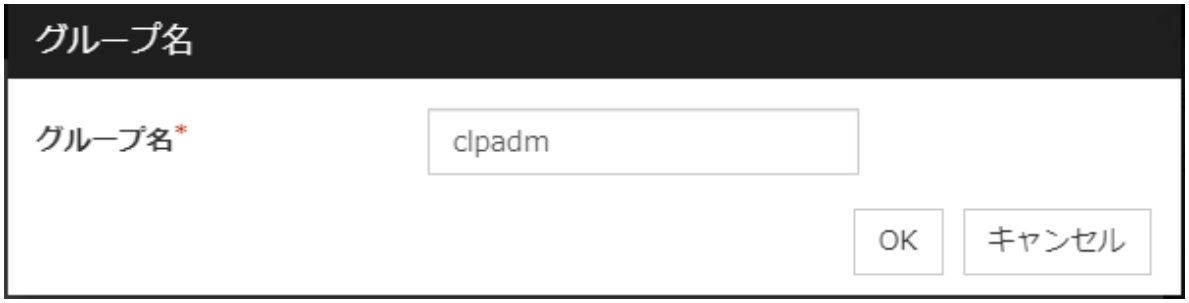
    新しいパスワードをもう一度入力します。

OS 認証方式

Cluster WebUI にログインするユーザを事前にサーバに登録しておく必要があります。また、クラスタの操作権限はグループ単位に設定するため、グループをサーバに登録し、ユーザを所属させておく必要があります。

追加

[権限を与えるグループ一覧] にグループを追加する場合に使用します。[追加] をクリックすると [グループ名] ダイアログボックスが表示されます。新規に追加するグループは [操作権] のチェックボックスがオンの状態で追加されます。



- グループ名 (255 バイト以内)

  権限を与えるグループ名を入力します。指定したグループに所属しているユーザに権限を与えます。

  グループは事前にサーバに登録しておく必要があります。

削除

[権限を与えるグループ一覧] からグループを削除する場合に使用します。

[権限を与えるグループ一覧] から削除するグループを選択して、[削除] をクリックしてください。

編集

グループを編集する場合に使用します。[権限を与えるグループ一覧] から編集するグループを選択して、[編集] をクリックします。選択されたグループが入力されている [グループ名] ダイアログボックスが表示されます。編集したグループの操作権は変わりません。

操作権

[権限を与えるグループ一覧] に登録されているグループに操作権を設定します。

- チェックボックスがオン

  グループに所属しているユーザはクラスタの操作と状態表示が行えます。

- チェックボックスがオフ

  グループに所属しているユーザはクラスタの状態表示のみ行えます。

ログインセッションの有効時間 (0～525600)

ログインセッションの有効時間です。0 に設定すると無期限となります。

自動ログアウト時間 (0～99999)

Cluster WebUI と WebManager サーバとの通信がない場合に自動的にログアウトする時間です。0 に設定すると自動ログアウトすることはありません。

ロックアウトのしきい値 (0～999)

連続してログインに失敗したクライアント IP アドレスをロックアウトするためのしきい値です。ロックアウトされたクライアント IP アドレスからは、ロックアウト期間が過ぎるまでログインできません。0 に設定すると、クライアント IP アドレスがロックアウトされることはありません。

ロックアウト期間 (1～99999)

ロックアウトされたクライアント IP アドレスが自動的にロック解除されるまでの時間です。

既定値

既定値に戻すときに使用します。[既定値] をクリックすると **ログインセッションの有効時間**、**自動ログアウト時間**、**ロックアウトのしきい値**、**ロックアウト期間** に既定値が設定されます。

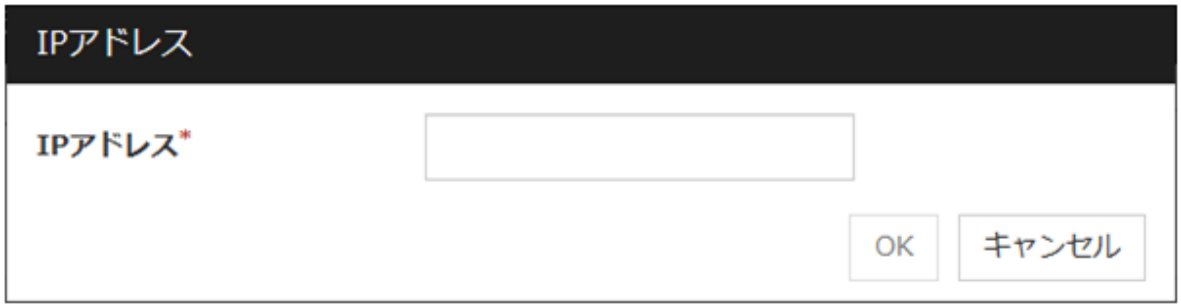
クライアント IP アドレスによって接続を制御する

クライアント IP アドレスによって接続を制御します。

- チェックボックスがオン
  [追加]、[削除]、[編集] ボタンが表示されます。
- チェックボックスがオフ
  [追加]、[削除]、[編集] ボタンが表示されません。

追加

[接続を許可するクライアント IP アドレス一覧] に IP アドレスを追加する場合に使用します。[追加] をクリックすると IP アドレスの入力ダイアログボックスが表示されます。新規に追加する IP アドレスは操作権ありで追加されます。



- IP アドレス (80 バイト以内)
  接続を許可するクライアント IP アドレスを入力します。
  - IP アドレスの場合の例 ： 10.0.0.21
  - ネットワークアドレスの場合の例 ： 10.0.1.0/24

削除

[接続を許可するクライアント IP アドレス一覧] から IP アドレスを削除する場合に使用します。[接続を許可するクライアント IP アドレス一覧] から削除したい IP アドレスを選択して、[削除] をクリックしてください。

編集

IP アドレスを編集する場合に使用します。[接続を許可するクライアント IP アドレス一覧] から編集したい IP アドレスを選択して、[編集] をクリックします。選択された IP アドレスが入力されている IP アドレスの入力ダイアログボックスが表示されます。編集した IP アドレスの操作権は変わりません。

注釈: この接続を許可するクライアント IP アドレスは clprexec による外部操作に対する接続制限にも使用されます。

操作権

[接続を許可するクライアント IP アドレス一覧] に登録されている IP アドレスに操作権を設定します。

- チェックボックスがオン

  クライアントは CLUSTERPRO X SingleServerSafe の操作と状態表示が行えます。

- チェックボックスがオフ

  クライアントは CLUSTERPRO X SingleServerSafe の状態表示のみ行えます。

Cluster WebUI の操作ログを出力する

Cluster WebUI の操作ログを出力します。

- チェックボックスがオン

  Cluster WebUI の操作ログを出力します。

- チェックボックスがオフ

  Cluster WebUI の操作ログを出力しません。

ログ出力先 (255 バイト以内)

Cluster WebUI 操作ログの出力先ディレクトリを指定します。絶対パスかつ ASCII 文字で指定してください。

ログ出力先を省略した場合、<インストールパス>/log 配下に Cluster WebUI 操作ログが出力されます。

ファイルサイズ (1〜10)

Cluster WebUI 操作ログのサイズを指定します。

指定したファイルサイズに達した場合はローテートが行われます。最大で 5 世代のログファイルが保存されます。

接続用 IP アドレス

[設定] をクリックすると 統合 Cluster WebUI 用 IP アドレスダイアログ ボックスが表示されます。

- 追加

  統合 Cluster WebUI 用 IP アドレスを追加します。各サーバの IP アドレスは、各サーバの列のセルをクリックして IP アドレスを選択または入力して設定します。

- 削除

  通信経路を削除します。削除したい通信経路の列を選択して [削除] をクリックすると、選択していた経路が削除されます

- 優先度

  統合 Cluster WebUI 用 IP アドレスを複数設定する場合、[優先度] 列の番号が小さい通信経路が優先的にクラスタ サーバ間の内部通信に使用されます。優先度を変更する場合は、矢印をクリックして、選択行の順位を変更します。

調整

WebManager サーバの調整を行う場合に使用します。[調整] をクリックすると [WebManager 調整プロパティ] ダイアログボックスが表示されます。

- クライアントセッションタイムアウト (1〜999)

  WebManager サーバが Cluster WebUI と通信しなくなってからのタイムアウト時間です。

- 画面データ更新インターバル (0〜999)

  Cluster WebUI の画面データが更新される間隔です。

- ミラーエージェントタイムアウト（1〜999）

  使用しません。

- ログファイルダウンロード有効期限 (60〜43200)

  サーバ上に一時保存したログ収集情報を削除するまでの有効期限です。ログ収集情報の保存ダイアログが表示されてから、保存を実行しないまま有効期限が経過するとサーバ上のログ収集情報は削除されます。

- 時刻情報表示機能を使用する

  時刻情報表示機能の有効/無効を設定します。

  - チェックボックスがオン

    時刻情報表示機能を有効にします。

  - チェックボックスがオフ

    時刻情報表示機能を無効にします。

- 既定値

  既定値に戻すときに使用します。[既定値] をクリックすると全ての項目に既定値が設定されます。

8.1.12 API タブ

API サービスの設定をおこないます。

API サービスを有効にする

API サービスを有効にします。

- チェックボックスがオン

  API サービスを有効にします。

- チェックボックスがオフ

  API サービスを無効にします。

通信方式

- HTTP

  クライアントとの通信に暗号化を使用しません。

- HTTPS

  クライアントとの通信に暗号化を使用します。

グループ単位で権限を設定する

クラスタの操作権限をグループ単位に設定、制御します。

- チェックボックスがオン

[追加]、[削除]、[編集] が表示されます。

- チェックボックスがオフ

  [追加]、[削除]、[編集] が表示されません。

リクエストを発行するサーバにログインするユーザを事前にサーバに登録しておく必要があります。また、クラスタの操作権限はグループ単位に設定するため、グループをサーバに登録し、ユーザを所属させておく必要があります。

- サーバがワークグループに所属している場合

  リクエストを発行するサーバ全てにユーザ、グループを同一名で登録します。

- サーバがドメインに所属している場合

  ドメインにユーザ、グループを登録します。

追加

[権限を与えるグループ一覧] にグループを追加する場合に使用します。[追加] をクリックすると [グループ名] ダイアログボックスが表示されます。新規に追加するグループは [操作権] のチェックボックスがオンの状態で追加されます。

- グループ名 (255 バイト以内)

  権限を与えるグループ名を入力します。指定したグループに所属しているユーザに権限を与えます。

  グループは事前にサーバに登録しておく必要があります。

削除

[権限を与えるグループ一覧] からグループを削除する場合に使用します。

[権限を与えるグループ一覧] から削除するグループを選択して、[削除] をクリックしてください。

編集

グループを編集する場合に使用します。[権限を与えるグループ一覧] から編集するグループを選択して、[編集] をクリックします。選択されたグループが入力されている [グループ名] ダイアログボックスが表示されます。編集したグループの操作権は変わりません。

操作権

[権限を与えるグループ一覧] に登録されているグループに操作権を設定します。

- チェックボックスがオン

  グループに所属しているユーザはクラスタ操作と各種ステータスの取得が行えます。

- チェックボックスがオフ

  グループに所属しているユーザは各種ステータスの取得のみ行えます。

クライアント IP アドレスによって接続を制御する

クライアント IP アドレスによって接続を制御します。

- チェックボックスがオン

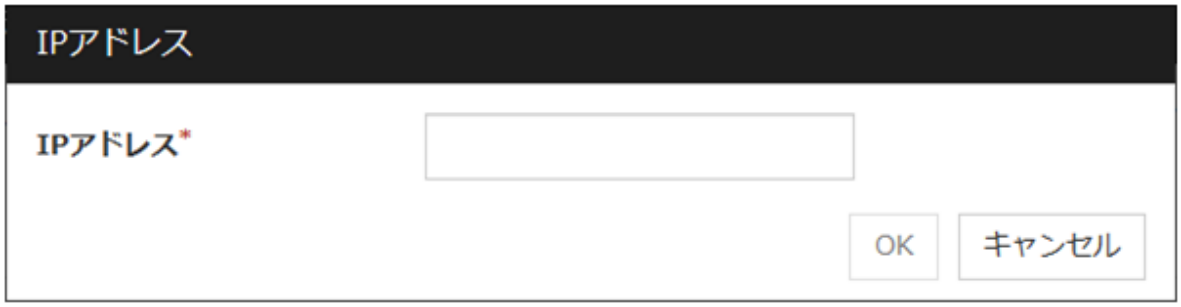
  [追加]、[削除]、[編集] が表示されます。

- チェックボックスがオフ

  [追加]、[削除]、[編集] が表示されません。

追加

[接続を許可するクライアント IP アドレス一覧] に IP アドレスを追加する場合に使用します。[追加] をクリックすると IP アドレスの入力ダイアログボックスが表示されます。新規に追加する IP アドレスは操作権ありで追加されます。



- IP アドレス (80 バイト以内)

  接続を許可するクライアント IP アドレスを入力します。

  - IP アドレスの場合の例 ： 10.0.0.21
  - ネットワークアドレスの場合の例 ： 10.0.1.0/24

削除

[接続を許可するクライアント IP アドレス一覧] から IP アドレスを削除する場合に使用します。[接続を許可するクライアント IP アドレス一覧] から削除したい IP アドレスを選択して、[削除] をクリックしてください。

編集

IP アドレスを編集する場合に使用します。[接続を許可するクライアント IP アドレス一覧] から編集したい IP アドレスを選択して、[編集] をクリックします。選択された IP アドレスが入力されている [IP アドレス] ダイアログボックスが表示されます。

操作権

[接続を許可するクライアント IP アドレス一覧] に登録されている IP アドレスに操作権を設定します。

- チェックボックスがオン

  グループに所属しているユーザはクラスタ操作と各種ステータスの取得が行えます。

- チェックボックスがオフ

  グループに所属しているユーザは各種ステータスの取得のみ行えます。

API サービスの操作ログを出力する

API サービスの操作ログを出力します。

- チェックボックスがオン

  API サービスの操作ログを出力します。

- チェックボックスがオフ

  API サービスの操作ログを出力しません。

ログ出力先 (255 バイト以内)

API サービス操作ログの出力先ディレクトリを指定します。絶対パスかつ ASCII 文字で指定してください。

ログ出力先を省略した場合、<インストールパス>/log 配下に API サービス操作ログが出力されます。

ファイルサイズ (1〜10)

API サービス操作ログのサイズを指定します。

指定したファイルサイズに達した場合はローテートが行われます。最大で 5 世代のログファイルが保存されます。

調整

API サービスの調整を行う場合に使用します。[調整] をクリックすると、[API 調整プロパティ] ダイアログボックスが表示されます。

- 認証ロックアウトのしきい値

  HTTP サーバへの認証に連続して失敗した場合にロックアウトと判断する回数を設定します。

- HTTP サーバ起動リトライ回数

  API サービスが HTTP サーバの起動に失敗した時の起動リトライ回数を設定します。

- HTTP サーバ起動インターバル

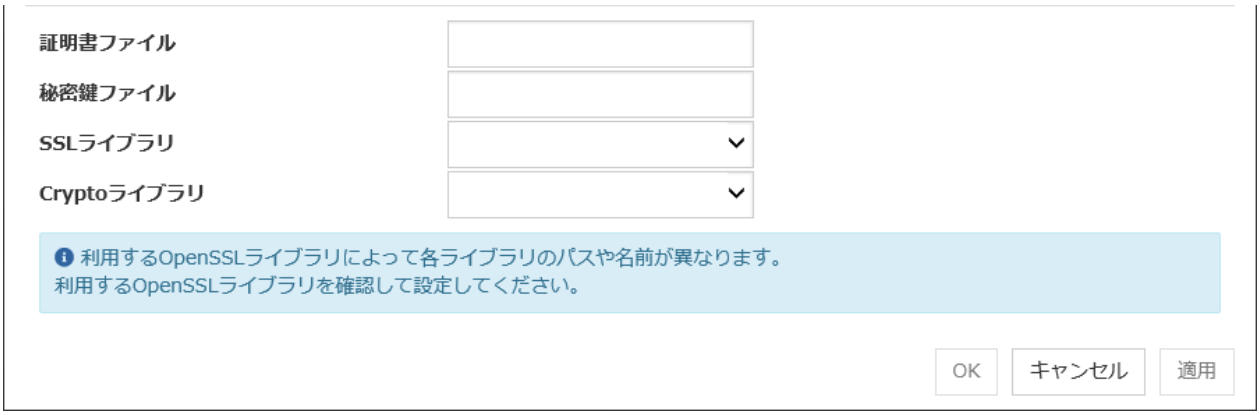
  API サービスが HTTP サーバの起動に失敗した時から次の起動をリトライするまでの間隔を設定します。

- 既定値

  既定値に戻すときに使用します。[既定値] をクリックすると全ての項目に既定値が設定されます。

8.1.13 暗号化 タブ

クラスタ関連サービスの暗号化で使用するファイルおよびライブラリに関する設定を行います。



証明書ファイル

クライアント接続時に利用されるサーバ証明書ファイルをフルパスで設定します。サーバ証明書ファイルは独自に用意する必要があります。

秘密鍵ファイル

クライアント接続時に利用される秘密鍵ファイルをフルパスで設定します。秘密鍵ファイルは独自に用意する必要があります。

SSL ライブラリ

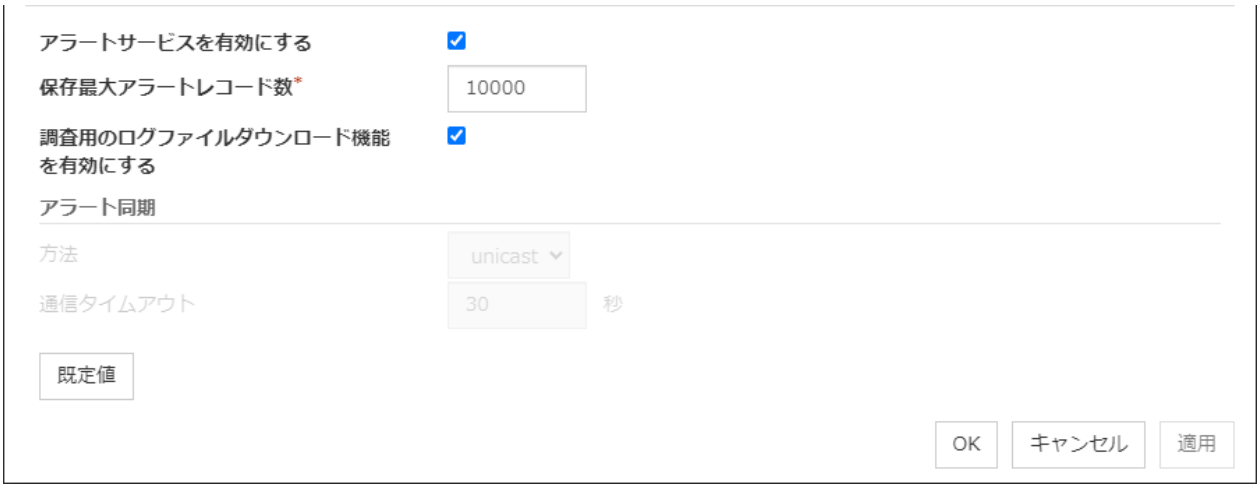
暗号化に利用する SSL ライブラリファイルを設定します。OpenSSL に含まれる SSL ライブラリファイルを選択します。インストールフォルダなど環境に応じて変更する必要があります。

Crypto ライブラリ

暗号化に利用する Crypto ライブラリファイルを設定します。OpenSSL に含まれる Crypto ライブラリファイルを選択します。インストールフォルダなど環境に応じて変更する必要があります。

8.1.14 アラートログタブ

アラートログを設定します。



アラートサービスを有効にする

サーバのアラートサービスを起動するかどうかの設定です。

- チェックボックスがオン

  アラートサービスを有効にします。

- チェックボックスがオフ

  アラートサービスを無効にします。

保存最大アラートレコード数 (1～99999)

サーバのアラートサービスが保存できる最大のアラートメッセージ数です。

調査用のログファイルダウンロード機能を有効にする

異常発生時の調査ログを WebUI からダウンロード可能にするか設定します。調査用のログファイルの詳細については『CLUSTERPRO X メンテナンスガイド』 - 「保守情報」 - 「調査ログ収集機能」を参照してください。

- チェックボックスがオン

  調査ログが Cluster WebUI 上でダウンロードできるようになります。

- チェックボックスがオフ

  調査ログが Cluster WebUI 上でダウンロードできなくなります。

アラート同期 方法

使用しません。

アラート同期 通信タイムアウト (1～300)

使用しません。

既定値

既定値に戻すときに使用します。[既定値] をクリックすると全ての項目に既定値が設定されます。

8.1.15 遅延警告タブ

遅延警告を設定します。遅延警告の詳細については「9. 監視動作の詳細」の「9.7. モニタリソースの遅延警告」を参照してください。

ハートビート遅延警告 (0～100)

ハートビートの遅延警告の割合を設定します。ハートビートタイムアウト時間のここで指定した割合の時間内にハートビートの応答がない場合にアラートログに警告を表示します。100 を設定すると警告を表示しません。

モニタ遅延警告 (0〜100)

モニタの遅延警告の割合を設定します。モニタタイムアウト時間のここで指定した割合の時間内にモニタの応答がない場合にアラートログに警告を表示します。100 を設定すると警告を表示しません。

注釈:

遅延警告で 0% を指定するとハートビートインターバル、モニタインターバルごとにアラートログを表示します。
アラートログで監視にかかった時間を確認することができるので、テスト運用などで監視の時間を確認する場合は、0% を設定します。
本番環境では 0% などの低い値は設定しないでください。

8.1.16 ミラーエージェントタブ

使用しません。

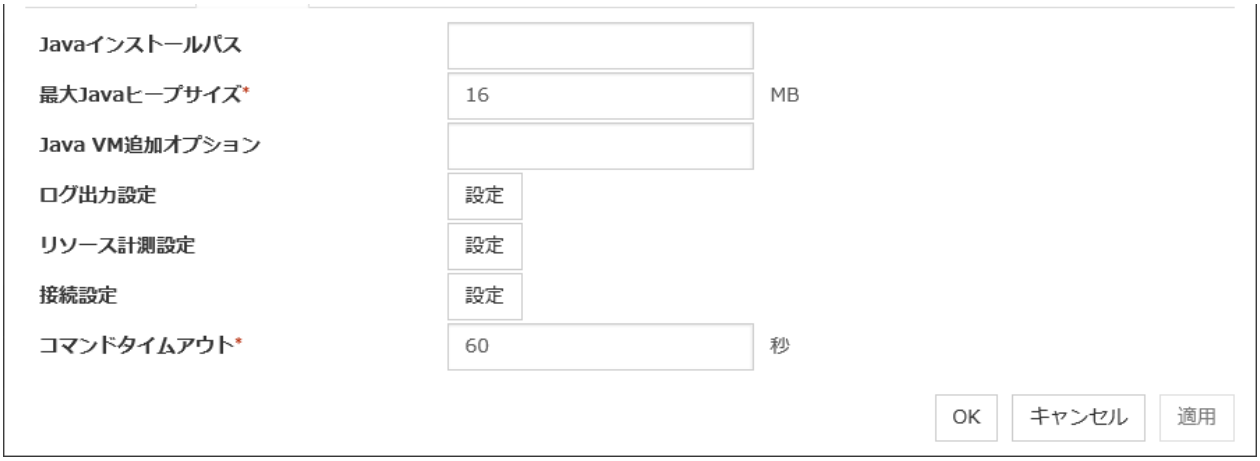
8.1.17 ミラードライバタブ

使用しません。

8.1.18 JVM 監視タブ

JVM 監視で用いる詳細なパラメータを設定します。

注釈: Cluster WebUI で JVM 監視タブを表示するためには、Java Resource Agent のライセンスが登録されている状態で [サーバ情報の更新] を実行する必要があります。



Java インストールパス (255 バイト以内)

JVM 監視が使用する Java VM のインストールパスを設定します。絶対パスかつ ASCII 文字で指定してください。末尾に"/"はつけないでください。指定例：/usr/java/jdk-9

最大 Java ヒープサイズ (7～4096)

JVM 監視が使用する Java VM の最大ヒープサイズをメガバイトで設定します (Java VM 起動時オプションの-Xmx に相当)。

Java VM 追加オプション (1024 バイト以内)

JVM 監視が使用する Java VM の起動時オプションを設定します。ただし、-Xmx は [最大 Java ヒープサイズ] で指定してください。指定例：-XX:+UseSerialGC

ログ出力設定

[設定] ボタンを押すとログ出力設定入力のダイアログが表示されます。

リソース計測設定

[設定] ボタンを押すとリソース計測設定入力のダイアログが表示されます。

接続設定

[設定] ボタンを押すと接続設定入力のダイアログが表示されます。

コマンドタイムアウト (30〜300)

JVM 監視の各画面で指定する [コマンド] のタイムアウト値を設定します。[コマンド] 共通の設定となります。

ログ出力設定

[設定] ボタンを押すとログ出力設定入力のダイアログが表示されます。

ログレベル

JVM 監視が出力するログのログレベルを選択します。

保持する世代数 (2〜100)

JVM 監視が出力するログについて保持する世代数を設定します。[ローテーション方式] にて [時間] を指定している場合、クラスタサスペンドを実行するとローテーション回数がリセットされるため、クラスタサスペンドごとに <CLUSTERPRO インストールパス>/log/ha/jra 配下のログファイルが増加することに注意してください。

ローテーション方式

JVM 監視が出力するログのローテーション方式を選択します。ファイルサイズによるログローテーションの場合、JVM 運用ログなどログ 1 ファイルあたりの最大サイズをキロバイトで設定します (範囲は 200〜2097151)。時間によるログローテーションの場合、ログローテーション開始時刻を"hh:mm"の形式 (hh: 時間を 0〜23、mm: 分を 0〜59 で指定)、ローテーションのインターバルを時間 (範囲は 1〜8784) で設定します。

既定値

ログレベル、保持する世代数、ローテーション方式を既定値の設定に戻します。

リソース計測設定 [共通]

[設定] ボタンを押すとリソース計測設定入力のダイアログが表示されます。JVM 監視が異常と判断する仕組みについては、「6. モニタリソースの詳細」を参照してください。

リトライ回数 (1～1440)

JVM 監視がリソース計測失敗した時のリソース計測リトライ回数を設定します。

異常判定しきい値 (1～10)

JVM 監視がリソース計測により取得した Java VM やアプリケーションサーバのリソース使用量が、お客様定義のしきい値を連続して超えた場合に異常と判断する回数を設定します。

インターバル メモリ使用量・動作スレッド数 (15～600)

JVM 監視がメモリ使用量および動作スレッド数を計測するインターバルを設定します。

インターバル Full GC 発生回数・実行時間 (15～600)

JVM 監視が Full GC 発生回数および発生時間を計測するインターバルを設定します。

既定値

リトライ回数、異常判定しきい値、インターバルを既定値の設定に戻します。

リソース計測設定 [WebLogic]

[設定] ボタンを押すとリソース計測設定入力のダイアログが表示されます。JVM 監視が異常と判断する仕組みについては、「6. モニタリソースの詳細」を参照してください。

リトライ回数 (1～5)

JVM 監視がリソース計測失敗した時のリソース計測リトライ回数を設定します。

異常判定しきい値 (1～10)

JVM 監視がリソース計測により取得した Java VM やアプリケーションサーバのリソース使用量が、お客様定義のしきい値を連続して超えた場合に異常と判断する回数を設定します。

インターバル リクエスト数 (15～600)

JVM 監視が WebLogic 監視におけるワークマネージャおよびスレッドプールのリクエスト数を計測するインターバルを設定します。

インターバル 平均値 (15～600)

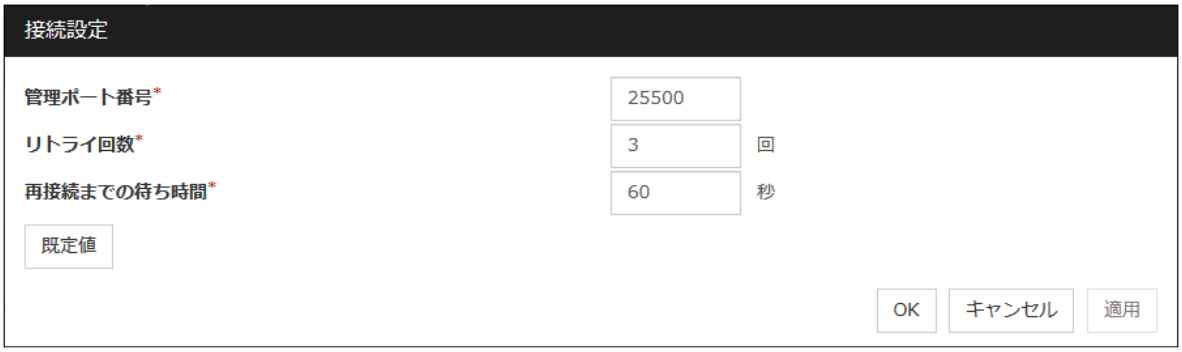
JVM 監視が WebLogic 監視におけるワークマネージャおよびスレッドプールのリクエスト数平均値を計測するインターバルを設定します。インターバル リクエスト数で設定されている整数倍の値を設定してください。

既定値

リトライ回数、異常判定しきい値、インターバルを既定値の設定に戻します。

接続設定

[設定] ボタンを押すと監視対象の Java VM への接続設定入力のダイアログが表示されます。



管理ポート番号 (1〜65535)

JVM モニタリソースが内部で使用するためのポート番号を設定します。他のポート番号と被らないようにしてください。32768〜61000 は非推奨です。

リトライ回数 (1〜5)

監視対象の Java VM へ接続失敗時のリトライ回数を設定します。

再接続までの待ち時間 (15〜60)

監視対象の Java VM へ接続失敗時に接続をリトライするまでのインターバルを設定します。

既定値

管理ポート番号、リトライ回数、再接続までの待ち時間を既定値の設定に戻します。

8.1.19 クラウドタブ

クラウド環境で用いる機能を設定します。

Amazon SNS 連携機能を有効にする

Amazon SNS 連携機能の設定をします。

- チェックボックスがオン

  Amazon SNS 連携機能を有効にします。

  CLUSTERPRO のメッセージを Amazon SNS のトピックにサブスクライブされている各エンドポイントに配信します。

  既定では、『操作ガイド』の「エラーメッセージ一覧」の「syslog、アラート、メール通報、SNMP トラップメッセージ、Message Topic」の [5] に●印のあるメッセージを送信します。

  その他のメッセージを送信する場合は、

  [クラスタプロパティ]-[アラートサービス] タブ-[アラート送信先の変更] で [送信先] に [Message Topic] を設定してください。

- チェックボックスがオフ

  Amazon SNS 連携機能を無効にします。

TopicArn

Amazon SNS 連携機能で使用する TopicArn を設定します。

Amazon CloudWatch 連携機能を有効にする

Amazon CloudWatch 連携機能の設定をします。

- チェックボックスがオン

  Amazon CloudWatch 連携機能を有効にします。

Amazon CloudWatch にモニタリソースの監視処理時間を送信します。

- チェックボックスがオフ

  Amazon CloudWatch 連携機能を無効にします。

注釈: Amazon CloudWatch 連携機能を使用する場合は、[Amazon CloudWatch 連携機能を有効にする] をオンにし、対象となるモニタリソースの [監視 (共通)] タブ-[監視処理時間メトリクスを送信する] の設定を有効にする必要があります。

Namespace

Amazon CloudWatch 連携機能で使用する Namespace を設定します。

メトリクスの送信インターバル

Amazon CloudWatch にモニタリソースの監視処理時間を送信する頻度を設定します。

AWS CLI コマンドラインオプション

[設定] をクリックすると AWS のサービスごとにテキストボックスが表示されます。

AWS のサービスごとに反映したい AWS CLI のコマンドラインオプションを設定します。

AWS 関連機能実行時の環境変数

[設定] をクリックすると環境変数一覧のダイアログが表示されます。

環境変数一覧

[編集] をクリックすると選択済みの環境変数入力のダイアログが表示されます。

[追加] をクリックすると新規の環境変数入力のダイアログが表示されます。

[削除] をクリックすると選択済みの環境変数が削除されます。

環境変数の入力

環境変数の名前と値を入力します。

- 名前 (259 バイト以内)

  環境変数の名前を設定します。

- 値 (2047 バイト以内)

  環境変数の値を設定します。

8.1.20 統計情報タブ

統計情報に関する設定をします。

クラスタ統計情報

グループのフェイルオーバに要した時間やリソースの活性処理時間などクラスタの動作に関する情報を採取し、参照することができます。

詳細は『CLUSTERPRO X メンテナンスガイド』-「保守情報」-「クラスタ統計情報採取機能」を参照してください。

- チェックボックスがオン

  クラスタ統計情報の採取を行います。

  - ファイルサイズ (タイプによって設定可能な値が異なります)

    クラスタ統計情報ファイルのサイズを指定します。

    指定したファイルサイズに達した場合はローテートが行われます。最大で 2 世代の情報が保存されます。

- チェックボックスがオフ

  クラスタ統計情報の採取を行いません。

注釈:

クラスタ統計情報のファイルサイズに設定可能な値は以下の通りです。

- ハートビートリソース : 1〜50 (MB)

- グループ : 1〜5 (MB)
- グループリソース : 1〜5 (MB)
- モニタリソース : 1〜10 (MB)

ミラー統計情報

使用しません。

システムリソース

システムリソース情報を収集する/しないを設定します。

運用性向上のためにシステムリソース情報を定期的に収集します。システムリソース情報は、CLUSTERPRO の動作状況の調査に役立ち、システムリソース不足を起因とする障害の原因特定が容易になります。

詳細は 『CLUSTERPRO X メンテナンスガイド』 -「保守情報」 -「システムリソース統計情報採取機能」 および 「プロセスリソース統計情報採取機能」 を参照してください。

- チェックボックスがオン

  サーバ動作中に CPU やメモリ、プロセスなどのシステムリソース情報を定期的に収集します。

  収集したシステムリソース情報は clplogcc コマンドや Cluster WebUI によるログ収集で収集されます。

  clplogcc コマンドでのログ収集時には type2 を、Cluster WebUI でのログ収集時にはパターン 2 を指定してください。

  プロセスの起動数などのシステム稼働状況に依存しますが、リソース情報の保存には 450MB 以上のディスク領域が必要となります。

- チェックボックスがオフ

  システムリソース情報を収集しません。

既定値

既定値に戻すときに使用します。[既定値] をクリックすると全ての項目に既定値が設定されます。

8.1.21 拡張タブ

その他のクラスタの機能を設定します。

再起動制限

グループリソースとモニタリソースの異常検出時の最終動作として、OS の再起動を伴うような設定をしている場合、永遠に再起動を繰り返してしまうことがあります。再起動の回数を設定することによって再起動の繰り返しを制限できます。

- 最大再起動回数 (0～99)

  再起動の制限回数を設定します。ここで指定する回数はグループリソース、モニタリソースで別々にカウントされます。

  [最大再起動回数] に 0 を設定した場合、再起動の繰り返しを制限しません。

- 最大再起動回数をリセットする時間 (0～999)

  最大再起動回数を指定している場合に、クラスタ起動時からの正常動作がここで指定した時間続いた時、それまでの再起動回数はリセットされます。ここで指定する時間はグループリソース、モニタリソースで別々にカウントされます。

注釈: [最大再起動回数をリセットする時間] に 0 を設定した場合、再起動回数はリセットされません。再起動回数をリセットする場合は、clpregctrl コマンドを使用してください。

ダウン後自動起動する

クラスタシャットダウンやクラスタ停止以外の方法でサーバを停止した場合やクラスタシャットダウンやクラスタ停止が正常に終了しなかった場合に、次回 OS 起動時にクラスタサービスを自動起動するかどうかを設定します。

マウント、アンマウントコマンドを排他する

使用しません。

サーバグループ間のフェイルオーバ時の猶予時間 (0～99999)

使用しません。

OS 停止動作を OS 再起動動作に変更する

OS 停止動作を一括して OS 再起動動作に変更します。

- チェックボックスがオン
  動作変更を行います。
- チェックボックスがオフ
  動作変更を行いません。

動作変更を設定した場合、下記の動作が変更されます。
下記以外の動作に関しては変更されません。

- NP 解決時動作
  - 「クラスタサービスの停止と OS シャットダウン」設定時
    クラスタサービスの停止と OS 再起動に変更します。
  - 「緊急シャットダウン」設定時
    緊急シャットダウン後、OS 再起動に変更します。
  - 「BMC パワーオフ」設定時
    BMC パワーサイクルに変更します。
- クラスタサービスのプロセス異常時動作
  - 「OS シャットダウン」設定時

OS 再起動に変更します。

– 「BMC パワーオフ」設定時

BMC パワーサイクルに変更します。

- グループリソース活性/非活性ストール発生時動作

– 「クラスタサービスの停止と OS シャットダウン」設定時

クラスタサービスの停止と OS 再起動に変更します。

– 「緊急シャットダウン」設定時

緊急シャットダウン後、OS 再起動に変更します。

– 「BMC パワーオフ」設定時

BMC パワーサイクルに変更します。

- グループリソース活性非活性異常時最終動作

– 「クラスタサービスの停止と OS シャットダウン」設定時

クラスタサービスの停止と OS 再起動に変更します。

– 「BMC パワーオフ」設定時

BMC パワーサイクルに変更します。

- モニタリソース異常時最終動作

– 「クラスタサービスの停止と OS シャットダウン」設定時

クラスタサービスの停止と OS 再起動に変更します。

– 「BMC パワーオフ」設定時

BMC パワーサイクルに変更します。

注釈: 以下のモニタリソースは動作変更の対象にはなりません。

- 外部連携モニタリソース
- ユーザ空間モニタリソース

クラスタ動作の無効化

- グループ自動起動

– チェックボックスがオン

グループの自動起動を無効化します。

– チェックボックスがオフ

グループの自動起動を無効化しません。

- グループリソースの活性異常検出時の復旧動作
  - チェックボックスがオン

    グループリソース活性異常検出による復旧動作を無効化します。
  - チェックボックスがオフ

    グループリソース活性異常検出による復旧動作を無効化しません。
- グループリソースの非活性異常検出時の復旧動作
  - チェックボックスがオン

    グループリソース非活性異常検出による復旧動作を無効化します。
  - チェックボックスがオフ

    グループリソース非活性異常検出による復旧動作を無効化しません。
- モニタリソースの異常検出時の回復動作
  - チェックボックスがオン

    モニタリソース異常検出による回復動作を無効化します。
  - チェックボックスがオフ

    モニタリソース異常検出による回復動作を無効化しません。
- サーバダウン時のフェイルオーバ
  - 使用しません

注釈:

モニタリソース異常検出による回復動作の無効化は、ユーザ空間モニタリソースでは有効になりません。
外部連携モニタリソースはモニタリソース異常検出による回復動作の無効化の対象にはなりません。

ログ保存期間設定

- ログ保存期間設定機能を使用する

  以下のフォルダにおいて、ローテート時に古いログファイル (拡張子が pre のファイル) を削除する代わりに「ファイル最終更新日時_タイプ名.log」にリネームします。
  - <インストールパス>/log
  - <インストールパス>/perf

「ファイル最終更新日時_タイプ名.log」のログファイルは、指定した時刻に圧縮ファイルにまとめられ、「圧縮を実行した日付_サーバ名.tar.gz」としてログ保存先に保存されます。

- ログ保存期間 (1 ～ 9999)

  保存期間を指定します。最長 9999 日まで指定できます。保存期間を過ぎたログファイルは自動的に削除されます。

- ログ保存先 (170 文字以内)

  保存先のフォルダを指定します。絶対パスかつ ASCII 文字で指定してください。

  指定するフォルダは、インストールパス外に予め作成しておく必要があります。

  充分な空き容量と書き込み性能があることを事前に確認してください。

- ログ保存タイミング

  毎日指定した時刻に保存処理を行います。時計ボタンをクリックし、ポップアップ画面から時刻を指定してください。

既定値

既定値に戻すときに使用します。[既定値] をクリックすると全ての項目に既定値が設定されます。

8.2 サーバプロパティ

「サーバのプロパティ」では、サーバ固有の設定を行います。

8.2.1 情報タブ

サーバ名の表示、コメントの登録、変更を行います。

名前

サーバ名を表示しています。ここでは名前の変更はできません。

コメント (127 バイト以内)

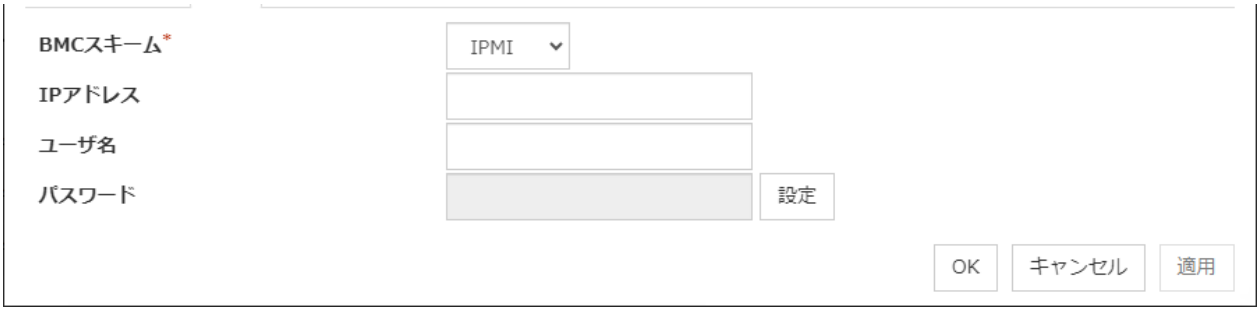
サーバのコメントを設定します。半角英数字のみ入力可能です。

8.2.2 警告灯タブ

使用しません。

8.2.3 BMC タブ

BMC 情報を設定します。



BMC スキーム

BMC の実行方法をを設定します。

IPMI : IPMI コマンドを使用する

Redfish : Redfish API を使用する

IP アドレス (80 バイト以内)

BMC のマネージメント用 LAN ポートに設定している IP アドレスを入力します。

ユーザ名 (255 バイト以内)

BMC に設定されているユーザ名のうち root 権限を持っているユーザ名を入力します。

パスワード (255 バイト以内)

上記で設定したユーザのパスワードを入力します。

BMC のユーザ名、パスワードについてはサーバのマニュアルを参照してください。

8.2.4 Proxy タブ

Proxy 情報を設定します。

Proxy スキーム

使用するプロトコルを設定します。

なし : Proxy を使用しない

HTTP : HTTP を使用する

Proxy サーバ

接続先の DNS ホスト名または IP アドレスを設定します。

Proxy ポート

接続先のポート番号を設定します。

8.3 登録最大数一覧

	Version	登録最大数
サーバ	4.0.0-1 以降	1
グループ	4.0.0-1 以降	128
グループリソース （1 グループにつき）	4.0.0-1 以降	256
モニタリソース	4.0.0-1 以降	512

第 9 章

監視動作の詳細

本章では、監視における監視インターバル、監視タイムアウト、監視リトライ回数をどうのように設定すればよいか検討するために、いくつかの障害パターンにより、どのように障害を検出するかの仕組みについての詳細を説明します。

本章で説明する項目は以下のとおりです。

9.1 常時監視と活性時監視について

常時監視では、サーバが起動して、CLUSTERPRO X SingleServerSafe が動作可能になった時点から監視を始めます。

活性時監視では、指定されたグループが活性してから、そのグループが非活性 (停止) する間で監視が行われます。

モニタリソースにより、いずれかに固定されているもの、いずれかを選択できるものがあります。

(1) Server startup: サーバ起動

(2) Group activation: グループ活性

(3) Group deactivation: グループ非活性

(4) Server stops: サーバ停止

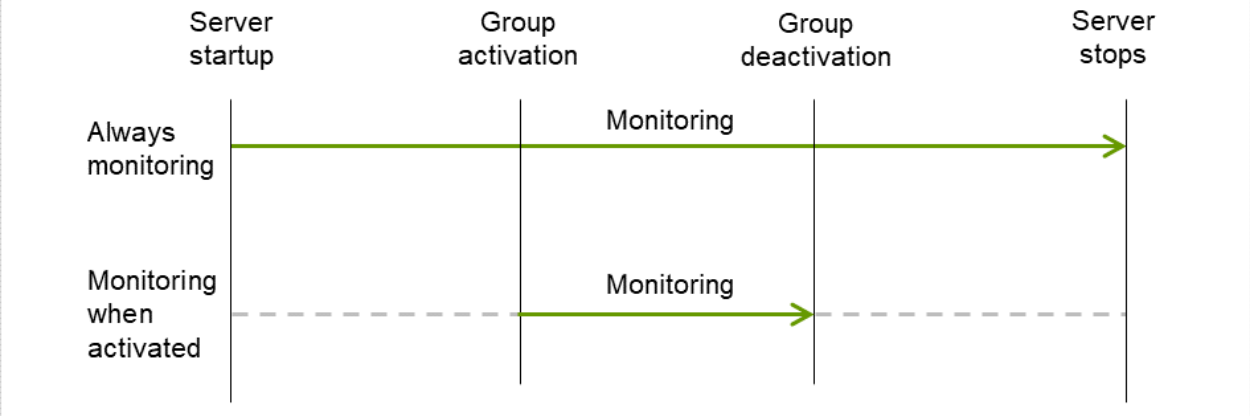


図 9.1　モニタリソースの常時監視と活性時監視

9.2 モニタリソースの監視インターバルのしくみ

全てのモニタリソースは、監視インターバル毎に監視が行われます。

以下は、この監視インターバルの設定による正常または、異常時におけるモニタリソースの監視の流れを時系列で表した説明です。

監視正常検出時

図は、サーバ起動後に監視を開始または再開した際の動作を表しています。監視メインプロセス（Main monitoring process）が監視結果を受け取ると、監視インターバル（Monitor interval）の時間を空けて、繰り返し、監視が起動されます。

下記の値が設定されている場合の挙動の例：

<監視>
監視インターバル 30 秒
監視タイムアウト 60 秒
監視リトライ回数 0 回

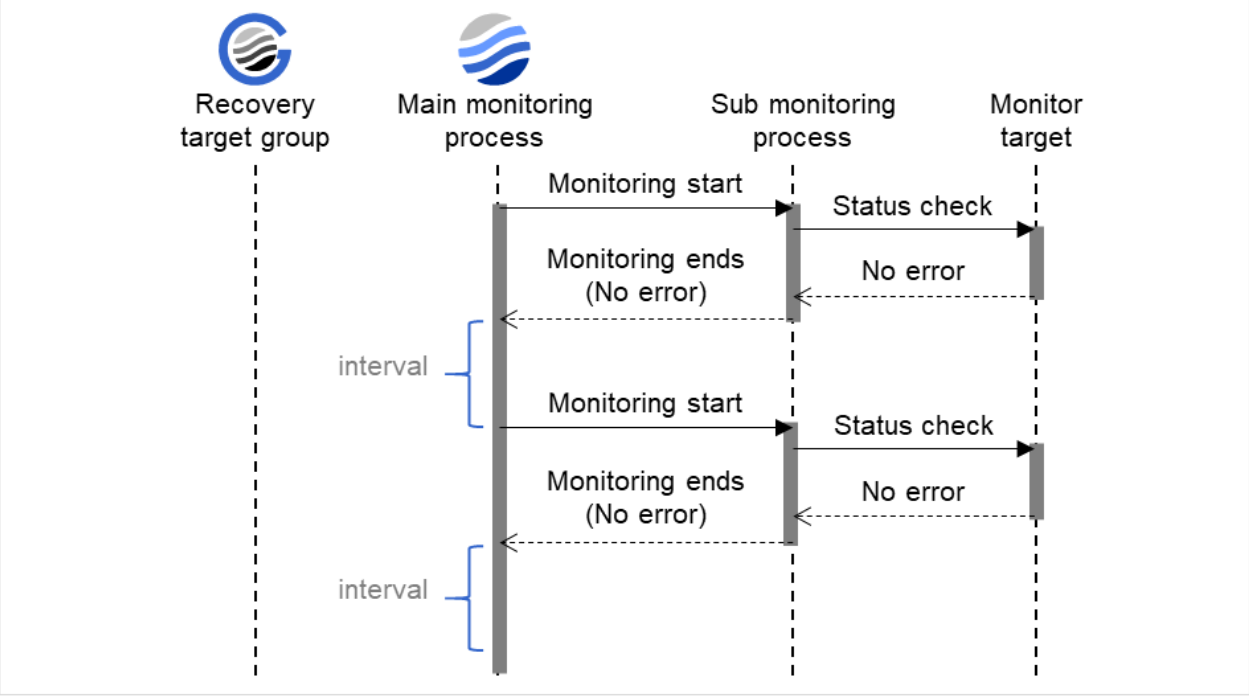


図 9.2　監視インターバル（監視正常検出時）

監視異常検出時 (監視リトライ設定なし)

図は、監視対象（Monitor target）で異常が発生し、それが検出された後の動作を表しています。監視メインプロセス（Main monitoring process）が監視結果（異常）を受け取ると、回復対象グループに対してフェイルオーバを実行します。

監視異常発生後、次回監視で監視異常を検出し回復対象に対して再活性化が行われます。

下記の値が設定されている場合の挙動の例：

<監視>
監視インターバル 30 秒
監視タイムアウト 60 秒
監視リトライ回数 0 回

<異常検出>
回復動作 回復対象を再起動
回復対象 グループ
回復スクリプト実行回数 0 回
再活性化しきい値 1 回
最終動作 何もしない

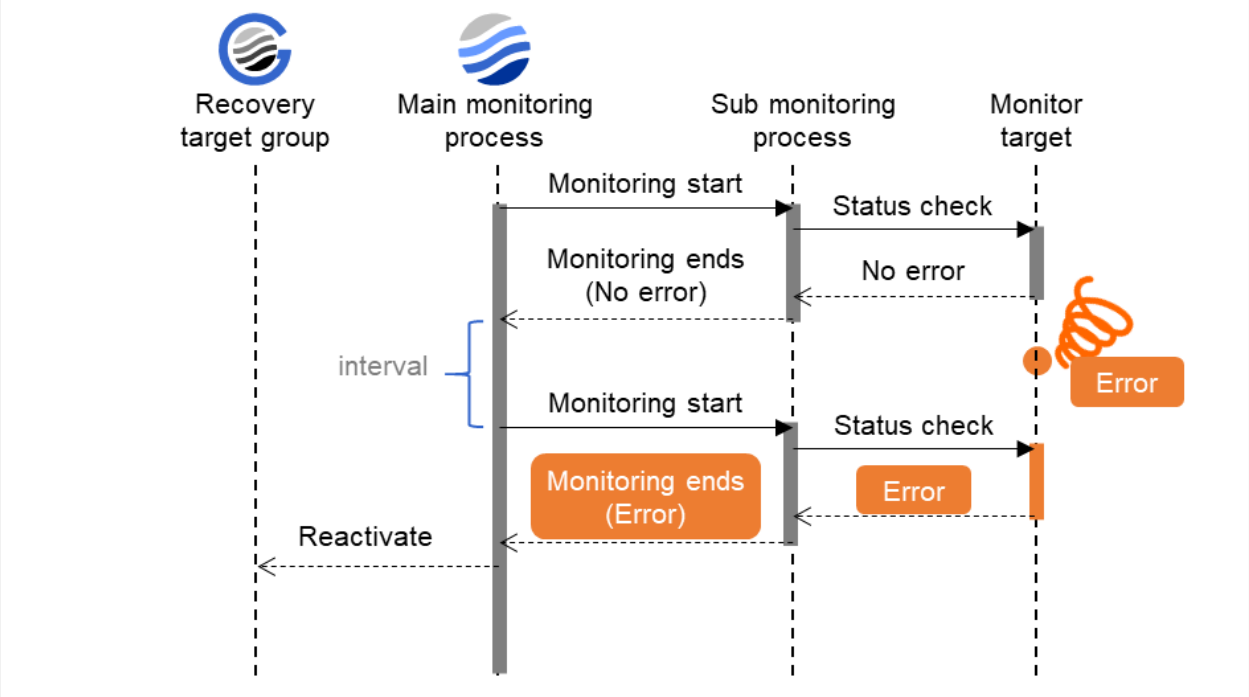


図 9.3　監視インターバル（監視異常検出時 ・監視リトライ設定なし）

監視異常検出時 (監視リトライ設定あり)

図は、監視対象（Monitor target）で異常が発生し、それが検出された後の動作を表しています。監視メインプロセス（Main monitoring process）が監視結果（異常）を受け取ると、設定された監視リトライ回数に達するまで、監視動作を実行します。それでも監視対象が回復しない場合、回復対象グループに対してフェイルオーバを実行します。

監視異常発生後、次回監視で監視異常を検出し監視リトライ以内で回復しなければ、回復対象に対して再活性化が行われます。

下記の値が設定されている場合の挙動の例：

<監視>
監視インターバル 30 秒
監視タイムアウト 60 秒
監視リトライ回数 2 回

<異常検出>
回復動作 回復対象を再起動
回復対象 グループ

回復スクリプト実行回数 0 回

再活性化しきい値 1 回

最終動作 何もしない

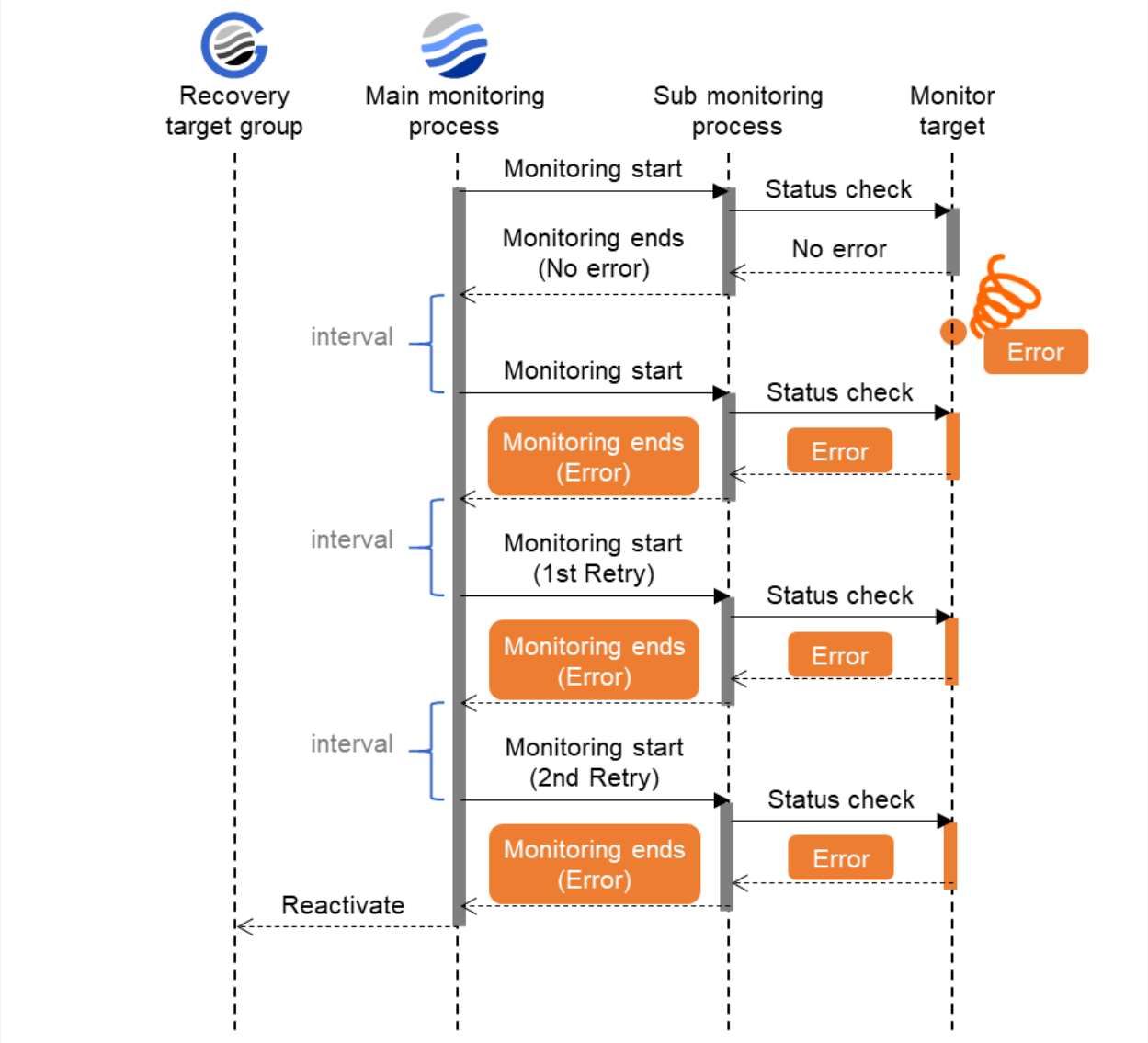


図 9.4　監視インターバル（監視異常検出時 ・監視リトライ設定あり）

監視タイムアウト検出時 (監視リトライ設定なし)

図は、設定された時間内に監視処理が終わらなかった場合の動作を表しています。監視メインプロセス（Main monitoring process）が監視を起動した後、監視タイムアウトに設定された時間内に監視結果が得られなかった場合、回復対象グループに対してフェイルオーバを実行します。

監視タイムアウト発生後、直ぐに回復対象への回復動作に対して再活性化が行われます。

下記の値が設定されている場合の挙動の例：

<監視>
監視インターバル 30 秒
監視タイムアウト 60 秒
監視リトライ回数 0 回

<異常検出>
回復動作 回復対象を再起動
回復対象 グループ
回復スクリプト実行回数 0 回
再活性化しきい値 1 回
最終動作 何もしない

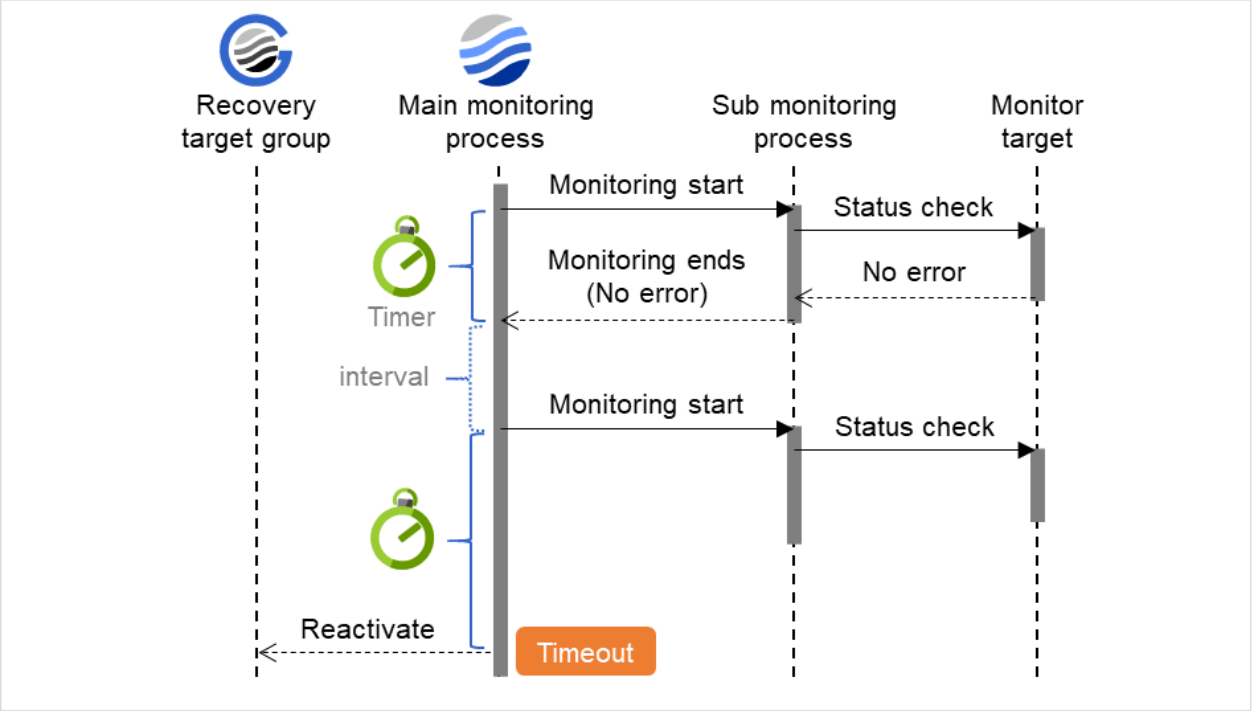


図 9.5　監視インターバル（監視タイムアウト検出時 ・監視リトライ設定なし）

監視タイムアウト検出時 (監視リトライ設定あり)

図は、設定された時間内に監視処理が終わらなかった場合の動作を表しています。監視メインプロセス（Main monitoring process）が監視を起動した後、監視タイムアウトに設定された時間内に監視結果が得られなかった場合、設定された監視リトライ回数に達するまで、監視動作を実行します。それでも監視結果が得られなかった場合、回復対象グループに対してフェイルオーバを実行します。

監視タイムアウト発生後、監視リトライを行い回復対象に対して再活性化が行われます。

下記の値が設定されている場合の挙動の例：

<監視>
監視インターバル 30 秒
監視タイムアウト 60 秒
監視リトライ回数 1 回

<異常検出>
回復動作 回復対象を再起動
回復対象 グループ
回復スクリプト実行回数 0 回
再活性化しきい値 1 回
最終動作 何もしない

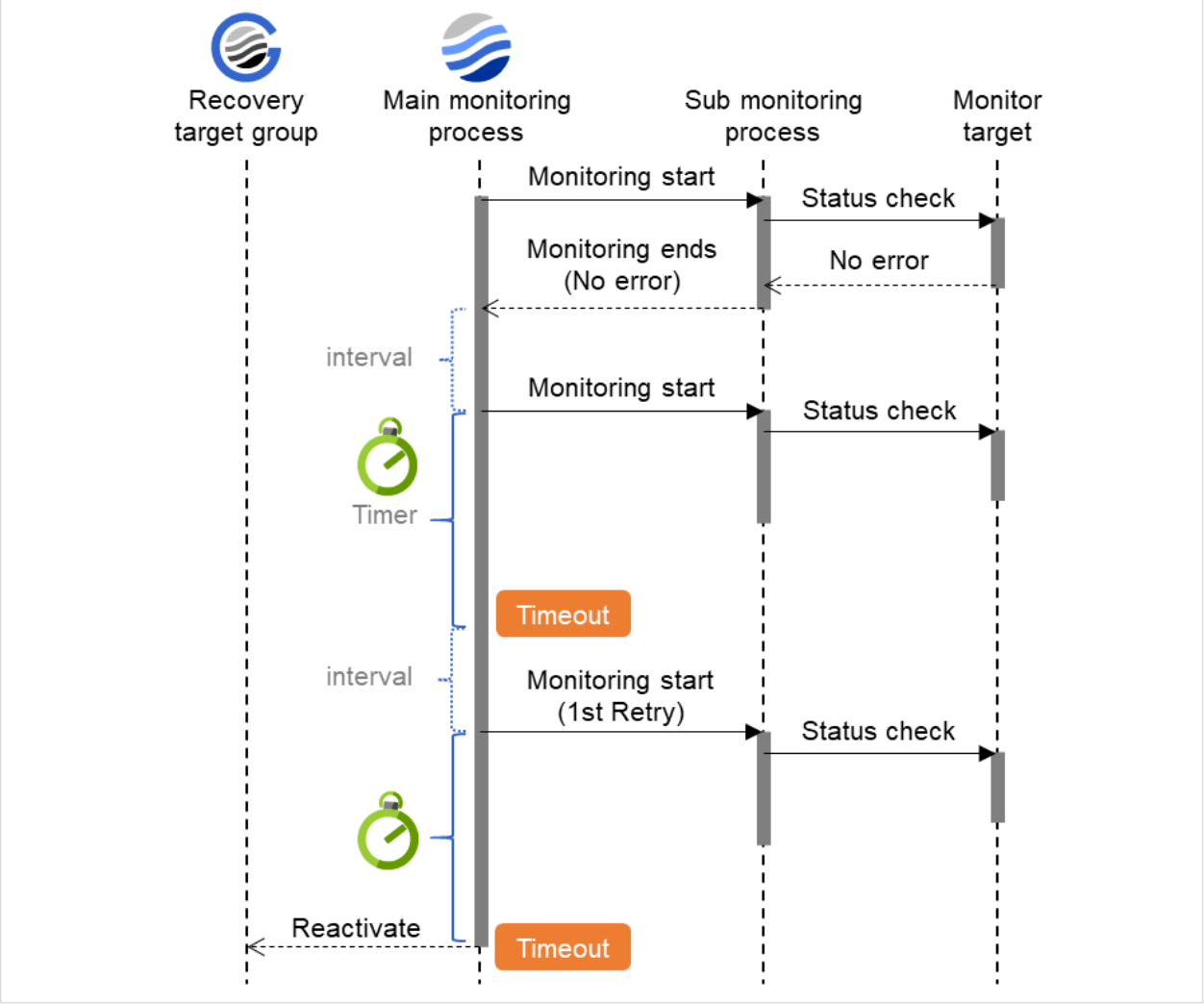


図 9.6　監視インターバル（監視タイムアウト検出時 ・監視リトライ設定あり）

9.3 モニタリソースによる異常検出時の動作

異常検出時には回復対象に対して以下の回復動作が行われます。

- 監視対象の異常を検出すると回復スクリプトを実行します。
- 回復スクリプト実行回数の回復スクリプト実行後、回復対象の再活性化を行います。再活性前スクリプト実行が設定されている場合はスクリプトを実行後に再活性化を行います。
- 監視対象の異常を検出すると回復対象の再活性化を行います（回復動作が [最終動作のみ実行] の場合、及び [カスタム設定] で最大再活性回数が 0 に設定されている場合は再活性化を行いません）。
- 再活性化に失敗した場合、あるいは再活性化を行っても異常を検出する場合、最終動作を行います（[カスタム設定] で最大再活性回数が 2 以上に設定されている場合は、指定回数まで再活性化をリトライします）。

回復動作が実行されるか否かは、回復対象の状態によって変わります。

回復対象	状態	再活性化[p. 308, *4]	最終動作[*5]
グループ/グループリソース	停止済	No	No
	起動/停止中	No	No
	起動済	Yes	Yes
	異常	Yes	Yes
LocalServer	-	-	Yes

Yes：回復動作が行われる No：回復動作が行われない

注釈: 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 (例: 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 → 最終動作) には、以下のコマンドまたは Cluster WebUI から以下の操作を行わないでください。

- サーバの停止 / サスペンド
- グループの開始 / 停止

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。

[*4] 再活性化しきい値に 1 以上が設定されている場合のみ有効になります。
[*5] 最終動作に"何もしない"以外が設定されている場合のみ有効になります。

モニタリソースの状態が異常から復帰 (正常) した場合は、再活性化回数、最終動作の実行要否はリセットされます。ただし、回復対象としてグループ/グループリソースが指定されている場合は、同一の回復対象が指定されている全てのモニタリソースの状態が正常状態になった場合のみ、これらのカウンタがリセットされます。

回復動作の再活性化回数は、回復動作に失敗した場合でも 1 回としてカウントされることに注意してください。

9.4 監視異常からの復帰 (正常)

監視異常を検出し、回復動作遷移中または全ての回復動作を完了後にモニタリソースの復帰を検出すると、そのモニタリソースが保持している以下のしきい値に対する回数カウンタはリセットされます。

- 回復スクリプト実行回数
- 再活性化回数

最終動作については、実行要否がリセットされます。

9.5 回復動作時の回復対象活性/非活性異常

モニタリソースの監視先と回復対象のグループリソースが同一のデバイスの場合で監視異常を検出すると、回復動作中にグループリソースの活性/非活性異常を検出する場合があります。

9.6 回復スクリプト、回復動作前スクリプトについて

モニタリソースの異常検出時に、回復スクリプトを実行させることが可能です。また、回復対象の再活性化、最終動作を実行する前に回復動作前スクリプトを実行させることも可能です。

いずれの場合でも共通のスクリプトファイルが実行されます。

回復スクリプト、回復動作前スクリプトで使用する環境変数

CLUSTERPRO はスクリプトを実行する場合に、どの状態で実行したか (回復動作種別) などの情報を環境変数にセットします。

スクリプト内で下図の環境変数を分岐条件として、システム運用にあった処理内容を記述できます。

環境変数	環境変数の値	意味
CLP_MONITORNAME …モニタリソース名	モニタリソース名	回復スクリプト、回復動作前スクリプトを実行する原因となる異常を検出したモニタリソース名を示します。
CLP_VERSION_FULL …CLUSTERPRO フルバージョン	CLUSTERPRO フルバージョン	CLUSTERPRO のフルバージョンを示す。 （例） 5.3.1-1
CLP_VERSION_MAJOR …CLUSTERPRO メジャーバージョン	CLUSTERPRO メジャーバージョン	CLUSTERPRO のメジャーバージョンを示す。 （例）5
CLP_PATH …CLUSTERPRO インストールパス	CLUSTERPRO インストールパス	CLUSTERPRO がインストールされているパスを示す。 （例）/opt/nec/clusterpro

次のページに続く

表 9.2 – 前のページからの続き

環境変数	環境変数の値	意味
CLP_OSNAME …サーバ OS 名	サーバ OS 名	スクリプトが実行されたサーバの OS 名を示す。 (例) (1) OS 名が取得できた場合： Red Hat Enterprise Linux Server release 6.8 (Santiago) (2) OS 名が取得できなかった場合： Linux
CLP_OSVER …サーバ OS バージョン	サーバ OS バージョン	スクリプトが実行されたサーバの OS バージョンを示す。 (例) (1) OS バージョンが取得できた場合：6.8 (2) OS バージョンが取得できなかった場合：※値なし
CLP_ACTION …回復動作種別	RECOVERY	回復スクリプトとして実行された場合。
	RESTART	再起動前に実行された場合。
	FINALACTION	最終動作前に実行された場合。
CLP_RECOVERYCOUNT …回復スクリプトの実行回数	回復スクリプト実行回数	何回目の回復スクリプト実行回数かを示す。

次のページに続く

表 9.2 – 前のページからの続き

環境変数	環境変数の値	意味
CLP_RESTARTCOUNT …再活性化回数	再活性化回数	何回目の再活性化回数かを示す。
CLP_FAILOVERCOUNT …フェイルオーバ回数	フェイルオーバ回数	使用しません。

回復スクリプト、回復動作前スクリプトの記述の流れ

前のトピックの、環境変数と実際のスクリプト記述を関連付けて説明します。

回復スクリプト、回復動作前スクリプトの一例

```
#!/bin/sh

# ***************************************
# *           preactaction.sh
# ***************************************

# スクリプト実行要因の環境変数を参照して、処理の振り分けを行う。
if [ "$CLP_ACTION" = "RECOVERY" ]
then
    # ここに回復処理を記述する。
    # この処理は以下のタイミングで実行される。
    #
    # 回復動作: 回復スクリプト

elif [ "$CLP_ACTION" = "RESTART" ]
then
    # ここに再活性化前処理を記述する。
    # この処理は以下のタイミングで実行される。
    #
    # 回復動作: 再活性化

elif [ "$CLP_ACTION" = "FINALACTION" ]
```

(次のページに続く)

(前のページからの続き)

```
then
    # ここに回復処理を記述する。
    # この処理は以下のタイミングで実行される。
    #
    # 回復動作: 最終動作

fi
exit 0
```

回復スクリプト、回復動作前スクリプト作成のヒント

以下の点に注意して、スクリプトを作成してください。

- スクリプト中にて、実行に時間を必要とするコマンドを実行する場合には、コマンドの実行が完了したことを示すトレースを残すようにしてください。この情報は、問題発生時、障害の切り分けを行う場合に使用することができます。clplogcmd を使用してトレースを残す方法があります。
- スクリプト中に clplogcmd を使用して記述する方法

  clplogcmd で Cluster WebUI のアラートログや OS の syslog に、メッセージを出力できます。
  clplogcmd については、『操作ガイド』 の 「CLUSTERPRO X SingleServerSafe コマンドリファレンス」の「メッセージを出力する (clplogcmd コマンド)」を参照してください。

(例：スクリプト中のイメージ)

```
clplogcmd -m "recoverystart.."
recoverystart
clplogcmd -m "OK"
```

回復スクリプト、回復動作前スクリプト 注意事項

- スクリプトから起動されるコマンド、アプリケーションのスタックサイズについて

  スタックサイズが 2MB に設定された状態で回復スクリプト、回復動作前スクリプトが実行されます。このため、スクリプトから起動されるコマンドやアプリケーションで 2MB 以上のスタックサイズが必要な場合には、スタックオーバーフローが発生します。

  スタックオーバーフローが発生する場合には、コマンドやアプリケーションを起動する前にスタック サイズを設定してください。

9.7 モニタリソースの遅延警告

モニタリソースは、業務アプリケーションの集中などにより、サーバが高負荷状態になり監視タイムアウトを検出する場合があります。監視タイムアウトを検出する前に監視の監視処理時間 (実測時間) が監視タイムアウト時間の何割かに達した場合、アラート通報させることが可能です。

以下は、モニタリソースが遅延警告されるまでの流れを時系列で表した説明です。

監視タイムアウトに 60 秒、遅延警告割合には、既定値の 80% を指定します。

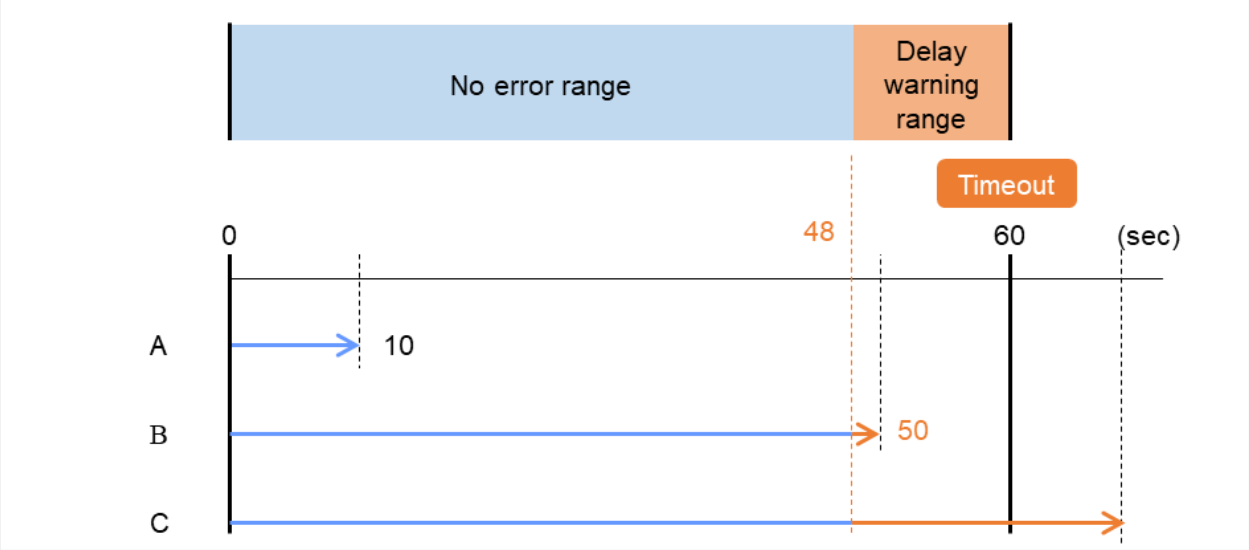


図 9.7　監視ポーリング時間と遅延警告

A. 監視の監視処理時間は 10 秒で、モニタリソースは正常状態。

   この場合、アラート通報は行いません。

B. 監視の監視処理時間は 50 秒で、監視の遅延を検出し、モニタリソースは正常状態。

   この場合、遅延警告割合の 80% を超えているためアラート通報を行います。

C. 監視の監視処理時間は監視タイムアウト時間の 60 秒を越え、監視タイムアウトを検出し、モニタリソースは異常状態。

   この場合、アラート通報は行いません。

また、遅延警告割合を 0 または、100 に設定すれば以下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

  監視ごと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モニタリソースへの監視処理時間を算出し、モニタ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。

注釈: テスト運用以外で、0% などの低い値を設定しないように注意してください。

参考:

モニタリソースの遅延警告は [クラスタのプロパティ]→[遅延警告] タブの [モニタ遅延警告] で設定します。

9.8 モニタリソースの監視開始待ち

監視開始待ちとは、監視を指定した監視開始待ち時間後から開始することをいいます。

以下は、監視開始待ちを 0 秒に指定した場合と 30 秒に指定した場合の監視の違いを時系列で表した説明です。

監視開始待ち時間が 0 秒の場合、サーバ起動または監視再開後に監視リソースポーリングを開始します。

[モニタリソース構成]

<監視>

インターバル 30 秒

タイムアウト 60 秒

リトライ回数 0 回

監視開始待ち時間 0 秒

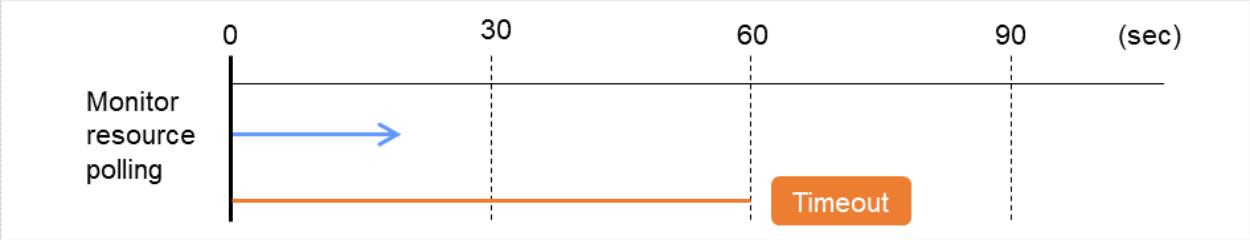


図 9.8　モニタリソースの監視開始待ち（監視開始待ち時間 0 秒）

監視開始待ち時間が 30 秒の場合、サーバ起動または監視再開後に 30 秒待ってから監視リソースポーリングを開始します。

[モニタリソース構成]

<監視>

インターバル 30 秒

タイムアウト 60 秒

リトライ回数 0 回

監視開始待ち時間 30 秒

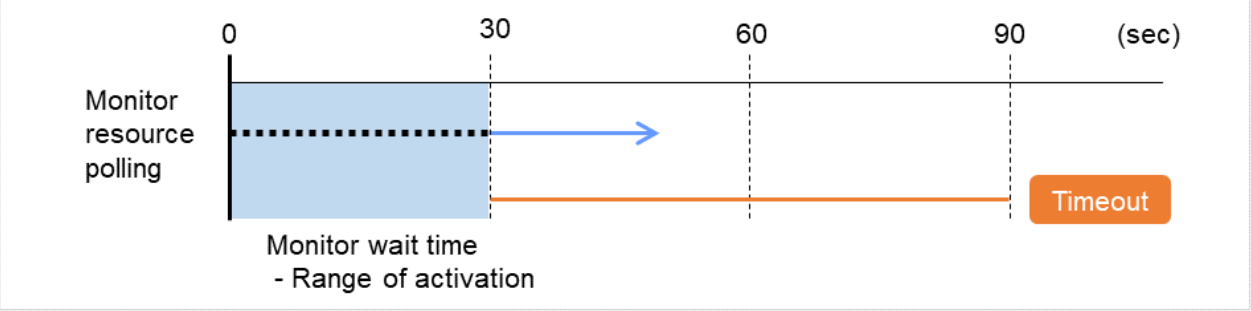


図 9.9　モニタリソースの監視開始待ち（監視開始待ち時間 30 秒）

注釈: 監視制御コマンドによるモニタリソースの一時停止/再開を行った場合も、指定された監視開始待ち時間後に再開します。

注釈: 外部連携モニタリソースでは監視開始待ち時間機能は機能しません。

監視開始待ち時間は、PID モニタリソースが監視する EXEC リソースのようにアプリケーションの設定ミスなどにより監視開始後すぐに終了する可能性があり、再活性化では回復できない場合に使用します。

たとえば、以下のように監視開始待ち時間を 0 に設定すると回復動作を無限に繰り返す場合があります。

このケースにおいて、アプリケーションは一旦起動します。さらに PID モニタによる監視が開始され、PID モニタによるポーリングが一度正常終了します。しかしその後、アプリケーションは何らかの理由で異常終了します。

[PID モニタリソース構成]

<監視>

インターバル 5 秒

タイムアウト 60 秒

リトライ回数 0 回

監視開始待ち時間 0 秒

<異常検出>

回復動作 回復対象を再起動

回復対象 exec

再活性化しきい値 1 回

最終動作 グループ停止

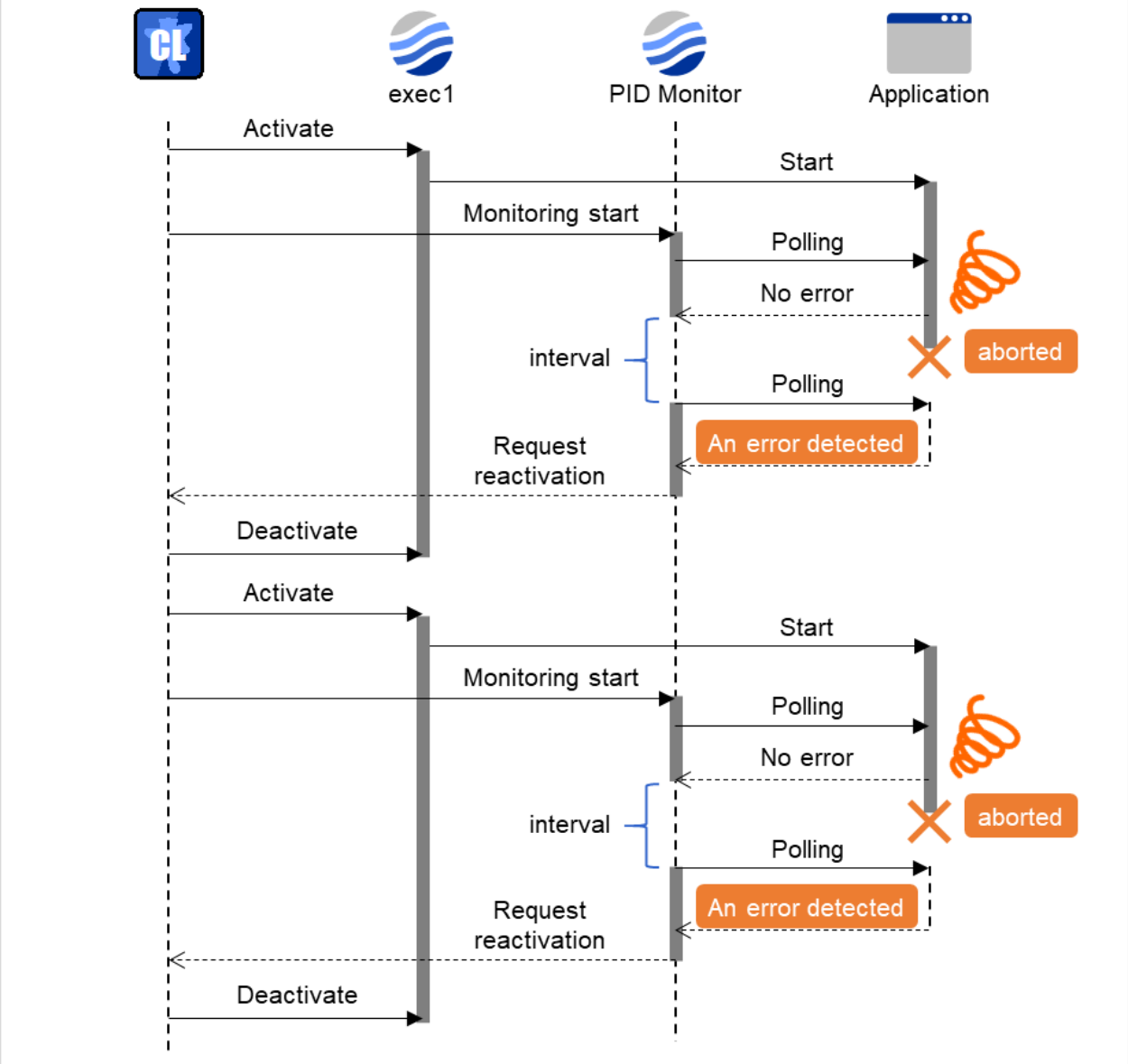


図 9.10　モニタリソースの監視開始待ち（監視開始待ち時間 0 秒）

この回復動作を無限に繰り返す原因は、初回の監視処理が正常終了することにあります。モニタリソースの回復動作の現在回数は、モニタリソースが正常状態になればリセットされます。そのため、現在回数が常に 0 リセットされ再活性化の回復動作を無限に繰り返すことになります。

上記の現象は、監視開始待ち時間を設定することで回避できます。

監視開始待ち時間には、アプリケーションが起動後、終了しうる時間として既定値で 60 秒を設定しています。

このケースにおいて、アプリケーションは一旦起動します。その後、設定された開始監視待ち時間待ちあわせた後に、PID モニタによる監視が開始されます。その後、アプリケーションは何らかの理由で異常終了しますが、それは PID モニタによる初回のポーリングで検出されます。

[PID モニタリソース構成]

<監視>
インターバル 5 秒
タイムアウト 60 秒
リトライ回数 0 回
監視開始待ち時間 60 秒

<異常検出>
回復動作 回復対象を再起動
回復対象 exec
再活性化しきい値 1 回
最終動作 グループ停止

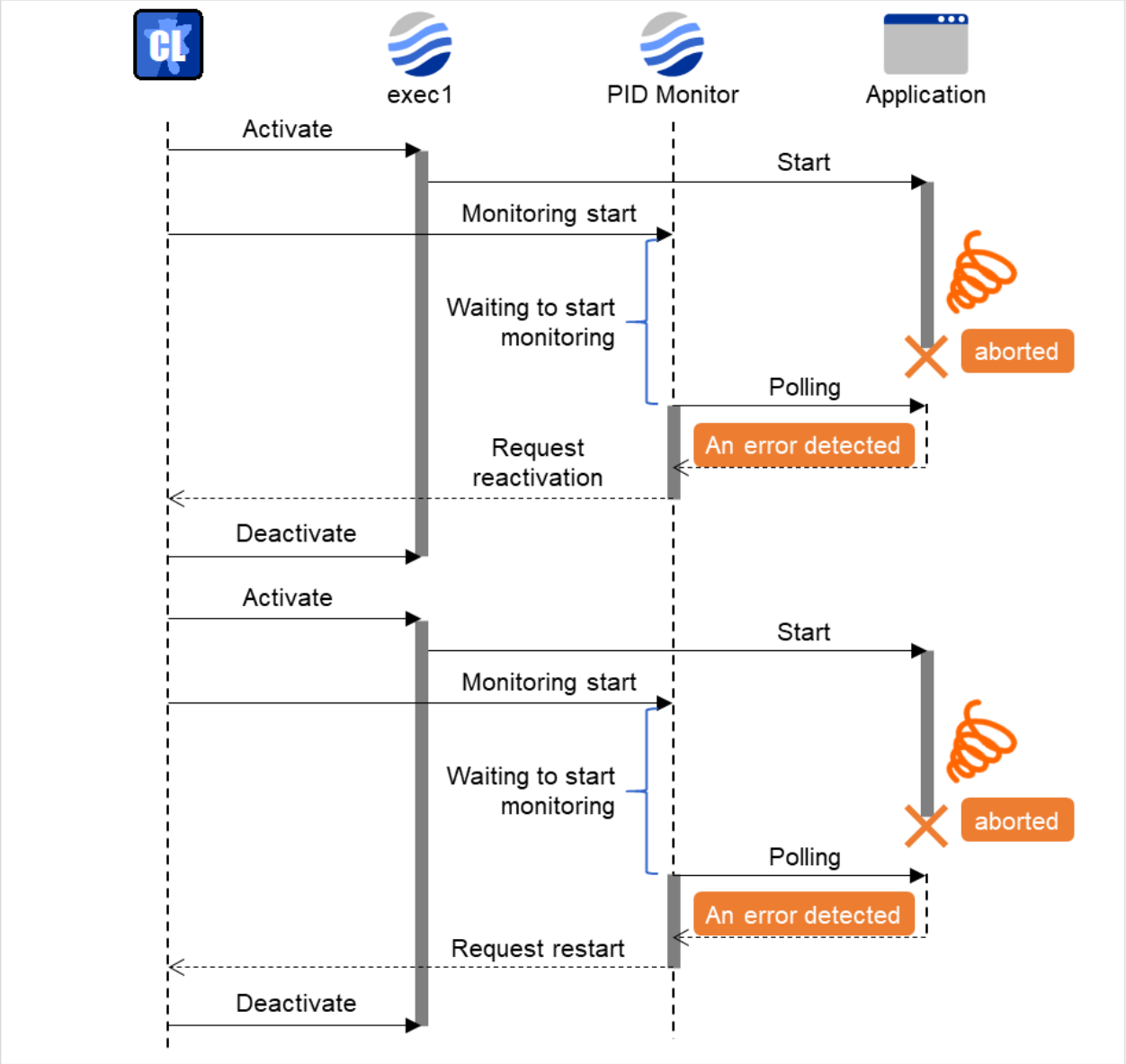


図 9.11　モニタリソースの監視開始待ち（監視開始待ち時間 60 秒）

9.9 再起動回数制限について

活性異常、非活性異常検出時の最終動作、またはモニタリソース異常検出時の最終動作として OS の再起動を伴うような設定をしている場合に、シャットダウン回数、または再起動回数を制限することができます。

注釈: 再起動回数はサーバごとに記録されるため、最大再起動回数はサーバごとの再起動回数の上限になります。

また、グループ活性、非活性異常検出時の最終動作による再起動回数とモニタリソース異常の最終動作による再起動回数は別々に記録されます。

最大再起動回数をリセットする時間に 0 を設定した場合には、再起動回数はリセットされません。リセットする場合は clpregctrl コマンドを使用する必要があります。

第 10 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。

10.1 システム構成検討時

システム構成時に留意すべき事項について説明します。

10.1.1 JVM モニタリソースについて

- 同時に監視可能な Java VM は最大 25 個です。同時に監視可能な Java VM とは Cluster WebUI ([監視 (固有)] タブ-[識別名]) で一意に識別する Java VM 数のことです。
- Java VM と JVM モニタリソース間のコネクションは SSL には対応していません。
- スレッドのデッドロックは検出できない場合があります。これは、Java VM の既知で発生している不具合です。詳細は、Oracle の Bug Database の「Bug ID: 6380127 」を参照してください。
- JVM モニタリソースが監視できる Java VM は、JVM モニタリソースが動作中のサーバと同じサーバ内のみです。
- JVM モニタリソースが監視できる JBoss のサーバインスタンスは、1 サーバに 1 つまでです。
- x86_64 版 OS 上において IA32 版の監視対象のアプリケーションを動作させている場合、監視を行うことはできません。
- Cluster WebUI ([クラスタのプロパティ] - [JVM 監視] タブ - [最大 Java ヒープサイズ]) で設定した最大 Java ヒープサイズを 3000 など大きな値に設定すると、JVM モニタリソースが起動に失敗します。システム環境に依存するため、システムのメモリ搭載量を元に決定してください。
- 監視対象 Java VM の起動オプションに「-XX:+UseG1GC」が付加されている場合、Java 7 以前では JVM モニタリソースの [プロパティ] - [監視 (固有)] タブ - [調整] プロパティ-[メモリ] タブ内の設定項目は監視できません。

  Java 8 以降では JVM モニタリソースの [プロパティ] - [監視 (固有)] タブ - [JVM 種別] に [Oracle Java(usage monitoring)] を選択することで監視可能です。

10.1.2 Cluster WebUI について

Cluster WebUI を使用する際は、よりセキュアに使用するため、通信方式として HTTPS の使用を推奨しています。

設定方法については「**その他の設定の詳細**」 - 「**クラスタプロパティ**」 - 「*WebManager* **タブ**」 および 「**暗号化 タブ**」 を参照ください。

10.2 CLUSTERPRO X SingleServerSafe の情報作成時

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。

10.2.1 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

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 X SingleServerSafe 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 X SingleServerSafe 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。

10.2.2 環境変数

環境変数が 256 個以上設定されている環境では、下記のスクリプトが実行できません。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。

- 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

10.2.3 サーバのリセット、パニック、パワーオフ

CLUSTERPRO X SingleServerSafe 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

「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
  - sysrq パニック
  - 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
  - sysrq パニック
  - 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 softdog
  - 監視方法 ipmi
  - 監視方法 keepalive

注釈: 「サーバのパニック」は監視方法が keepalive の場合のみ設定可能です。

- シャットダウン監視
  - 監視方法 softdog
  - 監視方法 ipmi
  - 監視方法 keepalive

注釈: 「サーバのパニック」は監視方法が keepalive の場合のみ設定可能です。

10.2.4 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。

10.2.5 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モニタリソースへのポーリング時間を算出し、モニタ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。

10.2.6 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 コマンドや SG_IO 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。

- S-ATA インターフェイスのディスクの場合には、ディスクコントローラのタイプや使用するディストリビューションにより、OS に IDE インターフェイスのディスク (hd) として認識される場合と SCSI インターフェイスのディスク (sd) として認識される場合があります。

  IDE インターフェイスとして認識される場合には、すべての TUR 方式は使用できません。

  SCSI イ ンターフェイスとして認識される場合には、TUR(legacy) が使用できます。TUR(generic) は使用できません。

- 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。

10.2.7 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、Linux 環境で編集されたスクリプトは EUC、Windows 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。

10.2.8 スクリプトの文字コードと改行コードについて

- Cluster WebUI 以外で作成したスクリプトを clpcfctrl コマンドで設定反映する場合、構成情報ファイル (clp.conf) とスクリプトの文字コードと改行コードが同じであることを確認してから設定反映してください。文字コードまたは改行コードが異なる場合、スクリプトが正常に動作しない可能性があります。

10.2.9 システムモニタリソースの設定について

- リソース監視の検出パターン

  System Resource Agent では、「しきい値」、「監視継続時間」という 2 つのパラメータを組み合わせて検出を行います。

  各システムリソース (オープンファイル数、ユーザプロセス数、スレッド数、メモリ使用量、CPU 使用率、仮想メモリ使用量) を継続して収集し、一定時間（継続時間として指定した時間）しきい値を超えていた場合に異常を検出します。

10.2.10 外部連携モニタリソースの設定について

- 外部連携モニタリソースに異常を通知するには、[clprexec] コマンドを用いる方法があります。
- [clprexec] コマンドを用いる場合は CLUSTERPRO CD に同梱されているファイルを利用します。通知元サーバの OS やアーキテクチャに合わせて利用してください。また、通知元サーバと通知先サーバの通信が可能である必要があります。

10.2.11 JVM 監視の設定について

- 監視対象が WebLogic Server の場合、JVM モニタリソースの以下の設定値については、システム環境 (メモリ搭載量など) により、設定範囲の上限に制限がかかることがあります。
  - [ワークマネージャのリクエストを監視する]-[リクエスト数]
  - [ワークマネージャのリクエストを監視する]-[平均値]
  - [スレッドプールのリクエストを監視する]-[待機リクエスト リクエスト数]

  - [スレッドプールのリクエストを監視する]-[待機リクエスト 平均値]
  - [スレッドプールのリクエストを監視する]-[実行リクエスト リクエスト数]
  - [スレッドプールのリクエストを監視する]-[実行リクエスト 平均値]

- 監視対象の JRockit JVM が 64bit 版の場合、JRockit JVM から取得した各最大メモリ量がマイナスとなり使用率が計算できないため、以下のパラメータが監視できません。
  - [ヒープ使用率を監視する]- [領域全体]
  - [ヒープ使用率を監視する]- [Nursery Space]
  - [ヒープ使用率を監視する]- [Old Space]
  - [非ヒープ使用率を監視する]- [領域全体]
  - [非ヒープ使用率を監視する]- [ClassMemory]
- Java Resource Agent を使用するには、『インストールガイド』の「JVM モニタリソースの動作環境」に記載している JRE(Java Runtime Environment) をインストールしてください。監視対象（WebLogic Server や WebOTX）が使用する JRE と同じ物件を使用することも、別の物件を使用することも可能です。
- モニタリソース名に空白を含まないでください。

10.2.12 AWS CLI コマンドラインオプション

AWS 関連機能では AWS CLI を実行しています。

クラスタプロパティのクラウドタブで [AWS CLI コマンドラインオプション] を設定することで、これらの処理に反映するコマンドラインオプションを指定することができます。
AWSCLI 実行時にリクエストを送信するエンドポイントの URL を指定する場合などに有効です。

複数のコマンドラインオプションを指定する場合はスペース区切りで指定してください。

AWS のサービスごとにコマンドラインオプションを指定することができます。
[AWS CLI コマンドラインオプション] の設定が有効になる機能は以下の通りです。

aws cloudwatch

- Amazon CloudWatch 連携

aws ec2

- Cluster WebUI によるクラウド環境情報の取得

aws sns

- Amazon SNS 連携

AWS CLI のコマンドラインオプションの詳細については AWS のドキュメントをご参照ください。

注釈:

特殊文字である「;」「&&」「||」「`」を指定すると AWS CLI コマンドラインオプションは無効になります。
--output オプションを指定すると AWS CLI コマンドラインオプションは無効になります。

10.2.13 AWS 関連機能実行時の環境変数

AWS 関連機能では AWS CLI やインスタンスメタデータへのアクセスを実行します。

クラスタプロパティのクラウドタブで [AWS 関連機能実行時の環境変数] を設定することで、これらの処理に反映する環境変数を指定することができます。AWS 環境にてプロキシサーバを利用する場合や、AWS CLI の設定ファイルや認証情報ファイルを指定する場合などに有効です。

[AWS 関連機能実行時の環境変数] の設定が有効になる機能は以下の通りです。

- Amazon SNS 連携
- Amazon CloudWatch 連携
- Cluster WebUI によるクラウド環境情報の取得

また、環境変数設定ファイルを使用することで環境変数を指定することもできます。この場合、[AWS 関連機能実行時の環境変数] は設定しないでください。[AWS 関連機能実行時の環境変数] を設定した場合は環境変数設定ファイルは使用できません。

注釈: 環境変数設定ファイルは旧バージョンとの互換性維持のための機能です。環境変数の設定には [AWS 関連機能実行時の環境変数] の使用を推奨します。

環境変数設定ファイルは、以下に配置しています。

<*CLUSTERPRO* インストールパス>/cloud/aws/clpaws_setting.conf

環境変数設定ファイルのフォーマットは、以下のとおりです。

環境変数名 = 値

記載例)

```
[ENVIRONMENT]
HTTP_PROXY = http://10.0.0.1:3128
HTTPS_PROXY = http://10.0.0.1:3128
NO_PROXY = 169.254.169.254,ec2.ap-northeast-1.amazonaws.com
```

環境変数設定ファイルの仕様は、以下のとおりです。

- 一行目は [ENVIRONMENT] を記載してください。記載がない場合は環境変数が設定されないことがあります。
- 環境変数設定ファイルが存在しない場合や読み取り権限がない場合は無視します。活性異常や監視異常にはなりません。
- 同名の環境変数が既に設定されている場合、値を上書きします。
- 環境変数名の前にスペースやタブがある場合または = の両側にタブがある場合、設定が反映されないことがあります。
- 環境変数名は大文字・小文字を区別します。
- 値にスペースが入る場合、""(ダブルクォート) で括る必要はありません。
- 環境変数はグループリソースやモニタリソースの共通スクリプト (例. 最終動作前スクリプト、活性/非活性前後スクリプト) には反映されません。

10.2.14 AWS 関連機能実行時に使用する設定ファイルと認証情報ファイルについて

AWS 関連機能から実行される AWS CLI は以下のフォルダに保存されている設定ファイルと認証情報ファイルを使用しています。

```
/root/.aws
```

上記のフォルダ以外に保存されている設定ファイルと認証情報ファイルを使用したい場合、環境変数を指定する必要があります。

AWS 関連機能から実行される AWS CLI に環境変数を指定するには「**注意制限事項**」 - 「*CLUSTERPRO X SingleServerSafe* **の情報作成時**」 - 「*AWS* **関連機能実行時の環境変数**」を参照してください。

設定ファイルと認証情報ファイルを指定する環境変数は以下になります。

設定ファイルと認証情報ファイルのパスを環境変数に指定してください。

```
AWS_CONFIG_FILE
AWS_SHARED_CREDENTIALS_FILE
```

AWS CLI の環境変数の詳細については AWS のドキュメントをご参照ください。

10.3 CLUSTERPRO X SingleServerSafe 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。

10.3.1 リソースプロパティの依存関係について

リソースの依存関係を変更した場合、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。

リソースの依存関係と反映方法としてリソース停止が必要な設定変更をした場合、リジューム後のリソースの起動状態が依存関係を考慮したものになっていない場合があります。

次回グループ起動時から正しく依存関係の制御が行われるようになります。

10.3.2 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。

10.3.3 ポート番号の変更について

サーバのファイアウォールを有効にしており、ポート番号を変更した場合、ファイアウォールの設定の変更が必要です。clpfwctrl.sh コマンドでファイアウォールの設定を行うことができます。詳細は『CLUSTERPRO X SingleServerSafe for Linux 操作ガイド』 -「CLUSTERPRO X SingleServerSafe コマンドリファレンス」 -「ファイアウォールの規則を追加する (clpfwctrl.sh コマンド)」を参照してください。

第 11 章

免責・法的通知

11.1 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、一切責任をおいません。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。
-

11.2 商標情報

- CLUSTERPRO ® は、日本電気株式会社の登録商標です。
- Linux は、Linus Torvalds 氏の米国およびその他の国における登録商標です。
- RPM は、米国およびその他の国における Red Hat, Inc. またはその子会社の商標です。
- Intel、Pentium、Xeon は、米国およびその他の国における Intel Corporation またはその子会社の商標です。
- 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。
- 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。
- VMware は Broadcom Inc. の米国および各国での登録商標または商標です。
- Citrix、Citrix XenServer および Citrix Essentials は、Citrix Systems, Inc. の米国あるいはその他の国における登録商標または商標です。
- WebOTX は、日本電気株式会社の登録商標です。
- JBoss は、米国およびその他の国における Red Hat, Inc. またはその子会社の登録商標です。
- Apache Tomcat、Tomcat、Apache は、Apache Software Foundation の登録商標または商標です。
- SVF は、ウイングアークテクノロジーズ株式会社の登録商標です。
- F5、F5 Networks、BIG-IP、および iControl は、米国および他の国における F5 Networks, Inc. の商標または登録商標です。
- IBM、DB2、WebSphere は、International Business Machines 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。
- PostgreSQL は、PostgreSQL Global Development Group の登録商標です。
- WebSAM は、日本電気株式会社の登録商標です。
- 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。

第 12 章

改版履歴

版数	改版日付	内容
1	2025/04/08	新規作成
2	2025/09/22	誤記修正等
3	2026/01/30	誤記修正等
4	2026/07/13	誤記修正等