CLUSTERPRO X SingleServerSafe 5.3 for Windows

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
1.1 対象読者と目的 . . . 1
1.2 本書の構成 . . . 2
1.3 本書で記述される用語 . . . 3
1.4 CLUSTERPRO X SingleServerSafe マニュアル体系 . . . 4
1.5 本書の表記規則 . . . 5
1.6 最新情報の入手先 . . . 6

第 2 章 CLUSTERPRO X SingleServerSafe について 7
2.1 CLUSTERPRO X SingleServerSafe とは? . . . 8
2.2 CLUSTERPRO X SingleServerSafe の障害監視のしくみ . . . 9

第 3 章 構成情報を作成する 11
3.1 設定値を確認する . . . 12
3.2 Cluster WebUI を起動する . . . 14
3.3 構成情報の作成手順 . . . 16
3.4 構成情報を保存する . . . 22
3.5 構成情報をチェックする . . . 23
3.6 構成情報を反映する . . . 24

第 4 章 グループリソースの詳細 25
4.1 グループリソース一覧 . . . 26
4.2 アプリケーションリソースの設定 . . . 27
4.3 スクリプトリソースの設定 . . . 33
4.4 サービスリソースの設定 . . . 42

第 5 章 モニタリソースの詳細 47
5.1 モニタリソース一覧 . . . 49
5.2 モニタリソースのプロパティ . . . 56
5.3 アプリケーション監視リソースの設定 . . . 66
5.4 サービス監視リソースの設定 . . . 67
5.5 ディスク RW 監視リソースの設定 . . . 68
5.6 IP 監視リソースの設定 . . . 71

5.7 NIC Link Up/Down 監視リソースの設定 74
5.8 カスタム監視リソースの設定 76
5.9 マルチターゲット監視リソースの設定 80
5.10 外部連携監視リソースの設定 85
5.11 プロセス名監視リソースの設定 87
5.12 DB2 監視リソースの設定 90
5.13 FTP 監視リソースの設定 94
5.14 HTTP 監視リソースの設定 96
5.15 IMAP4 監視リソースの設定 100
5.16 ODBC 監視リソースの設定 102
5.17 Oracle 監視リソースの設定 105
5.18 POP3 監視リソースの設定 113
5.19 PostgreSQL 監視リソースの設定 116
5.20 SMTP 監視リソースの設定 121
5.21 SQL Server 監視リソースの設定 124
5.22 Tuxedo 監視リソースの設定 128
5.23 WebLogic 監視リソースの設定 130
5.24 WebOTX 監視リソースの設定 134
5.25 WebSphere 監視リソースの設定 137
5.26 JVM 監視リソースの設定 139
5.27 システム監視リソースの設定 182
5.28 プロセスリソース監視リソースの設定 193
5.29 ユーザ空間監視リソースの設定 200

第 6 章 その他の設定の詳細 203
6.1 クラスタプロパティ 204
6.2 サーバプロパティ 249
6.3 登録最大数一覧 251

第 7 章 監視動作の詳細 253
7.1 常時監視と活性時監視について 254
7.2 モニタリソースの擬似障害 発生/解除 255
7.3 モニタリソースの監視インターバルのしくみ 256
7.4 モニタリソースによる異常検出時の動作 262
7.5 監視異常からの復帰 (正常) 264
7.6 回復動作時の回復対象活性/非活性異常 265
7.7 回復スクリプト、回復動作前スクリプトについて 266
7.8 モニタリソースの遅延警告 270
7.9 モニタリソースの監視開始待ち 271
7.10 モニタリソース異常検出時の再起動回数制限 276

第 8 章 注意制限事項 277

8.1 システム構成検討時 278
8.2 CLUSTERPRO X SingleServerSafe の構成情報作成時 279
8.3 CLUSTERPRO X SingleServerSafe の構成変更時 284

第 9 章 免責・法的通知 285
9.1 免責事項 285
9.2 商標情報 286

第 10 章 改版履歴 287

第 1 章

はじめに

1.1 対象読者と目的

『CLUSTERPRO X SingleServerSafe 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. 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。
- 「5. 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。
- 「6. 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。
- 「7. 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。
- 「8. 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 Windows インストールガイド』 (Installation 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 Windows 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 Windows 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]`
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	`C:\Program Files\CLUSTERPRO`
太字	ユーザが実際にコマンドプロンプト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	`clpstat -s [-h host_name]`


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*?*
- 2.2. *CLUSTERPRO X SingleServerSafe* の障害監視のしくみ

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。

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 (アプリケーション監視リソース、サービス監視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、「5. 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。

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
- 3.2. *Cluster WebUI* を起動する
- 3.3. 構成情報の作成手順
- 3.4. 構成情報を保存する
- 3.5. 構成情報をチェックする
- 3.6. 構成情報を反映する

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、「4. グループリソースの詳細」 「5. 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
	システムドライブ	C:
グループ	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	アプリケーションリソース
	グループリソース名	appli1
	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	タイプ	ユーザ空間監視
	モニタリソース名	userw
	ハートビートのインターバル/タイムアウトを使用する	する
	監視方法	keepalive
	タイムアウト発生時動作	意図的なストップエラーの発生
	ダミースレッドの作成	する
2 つ目のモニタリソース	タイプ	IP 監視
	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	server1 (サーバ名)
	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	アプリケーション監視
	モニタリソース名	appliw1
	対象リソース	appli1

次のページに続く

表 3.1 – 前のページからの続き

設定対象	設定パラメータ	設定値
	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 「ユーザ空間監視」 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。

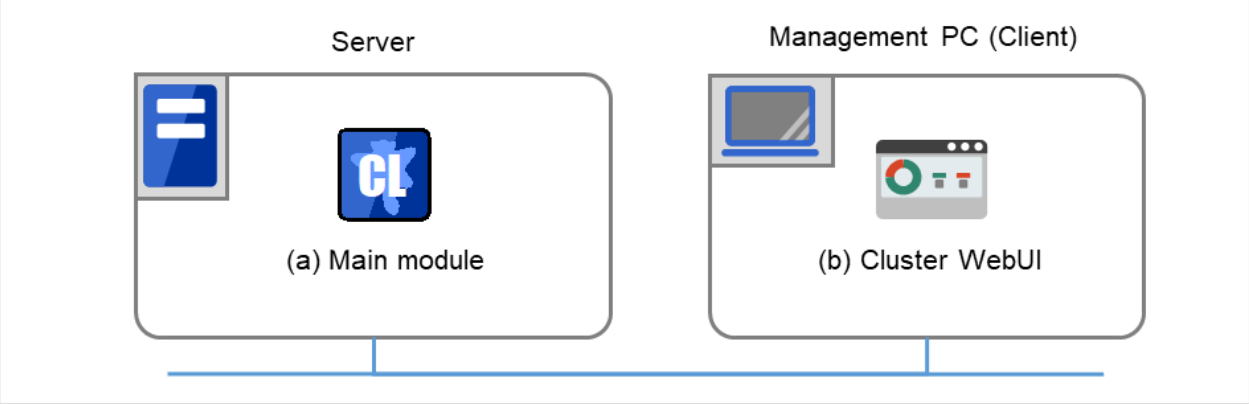


図 3.1　Cluster WebUI

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/`

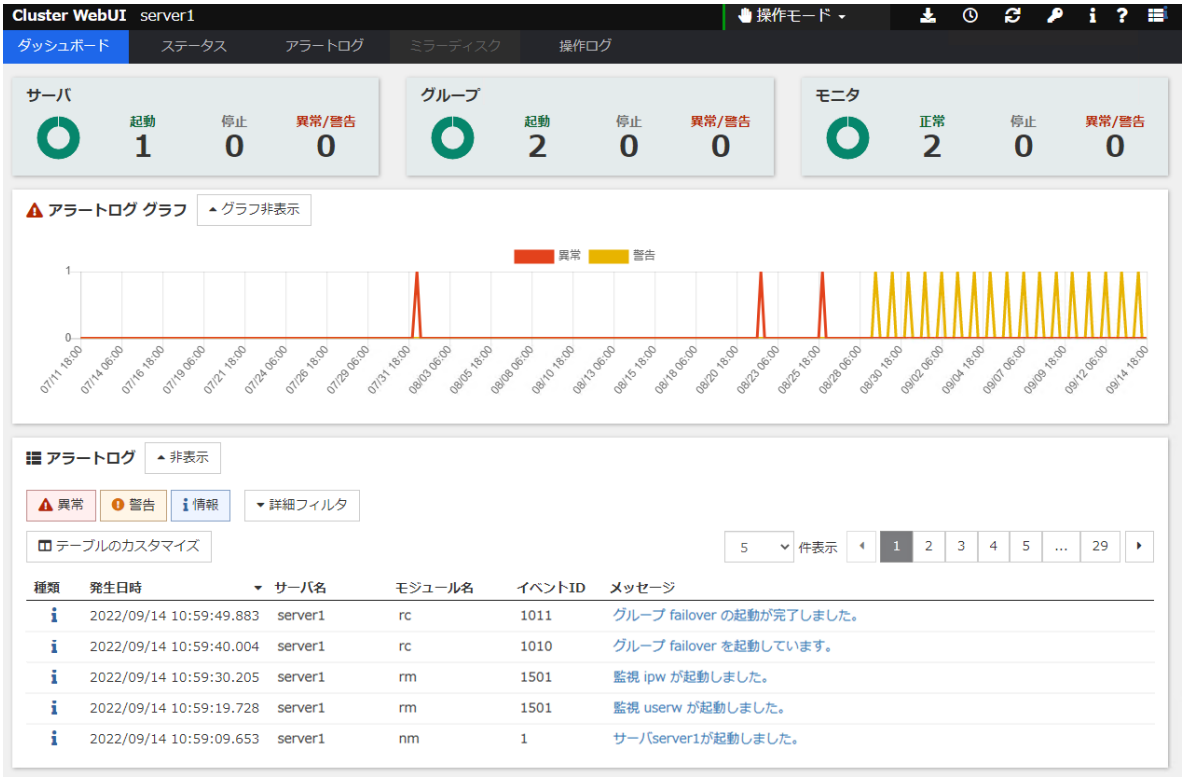
   ip-address

   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、「6. その他の設定の詳細」 - 「6.1. クラスタプロパティ」 - 「6.1.8. *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://192.168.0.1:29003/

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 *(アプリケーションリソース)* 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。
   監視したい数ほど、作成します。

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

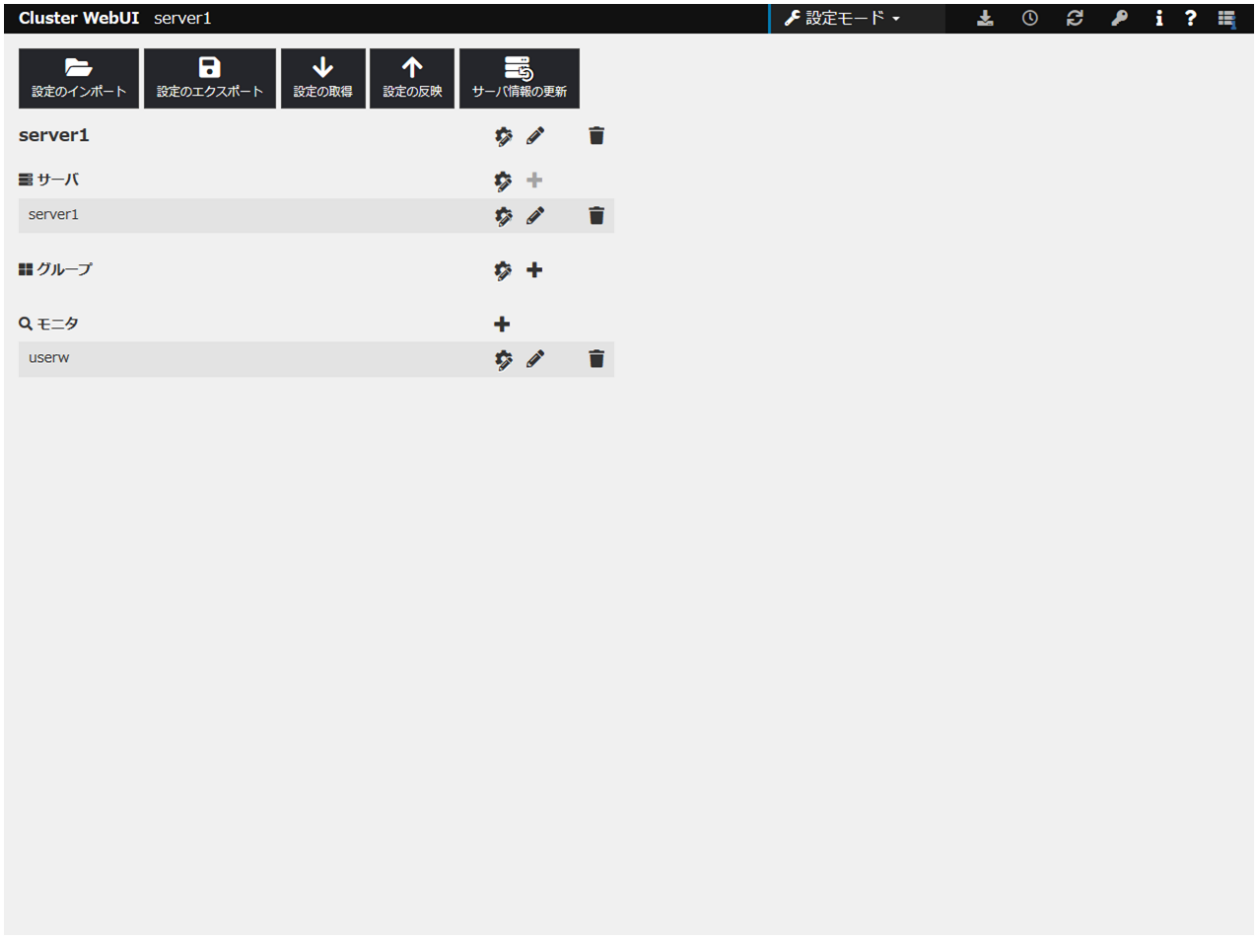
3.3.1 サーバの設定

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。[グループリソース一覧] が表示されます。

グループリソース (アプリケーションリソース) を追加する

アプリケーションの起動 / 終了を行う、アプリケーションリソースを追加します。

1. [グループリソース一覧] で、[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 (アプリケーションリソース) を選択し、[名前] ボックスにグループリソース名 (appli1) を入力します。[次へ] をクリックします。

   注釈: タイプとして、「アプリケーションリソース」「スクリプトリソース」「サービスリソース」 を選択することができます。

3. 依存関係設定のページが表示されます。何も指定せず [次へ] をクリックします。
4. [活性異常検出時の復旧動作]、[非活性異常検出時の復旧動作] が表示されます。
   [次へ] をクリックします。
5. [常駐タイプ] で [常駐] を選択します。また、[開始パス] に、実行ファイルのパスを指定します。

   注釈: [開始パス]、および [終了パス] には実行可能ファイル名の絶対パス、あるいは環境変数で設定されたパスの通った実行可能ファイル名を設定します。相対パスは指定しないでください。相対パスを指定した場合、アプリケーションリソースの起動に失敗する可能性があります。

6. [完了] をクリックします。
   [グループリソース一覧] にアプリケーションリソースが追加されました。

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 監視リソース) 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 監視) 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監視リソースは 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。

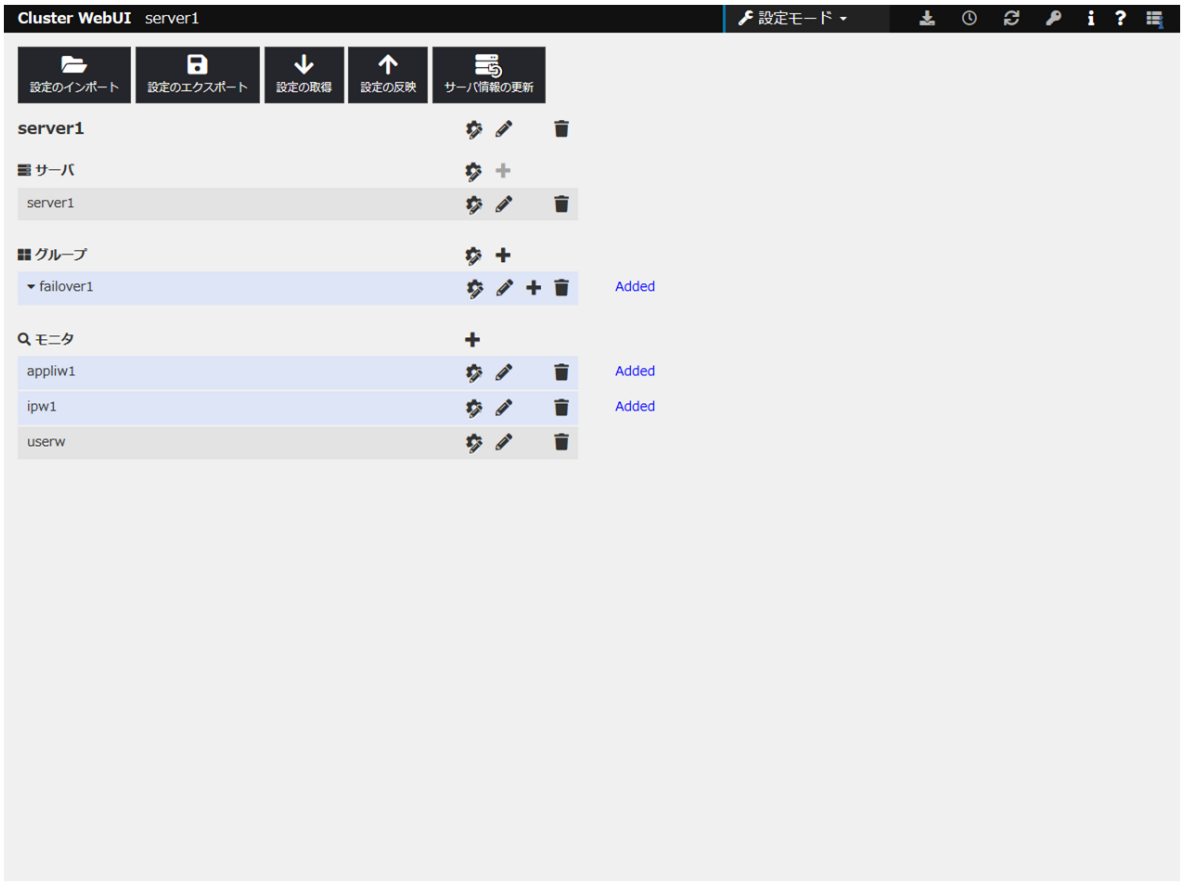
---

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 監視リソースの監視対象には、パブリック 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. 回復対象を設定します。[参照] をクリックします。
8. 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。
9. [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。

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。

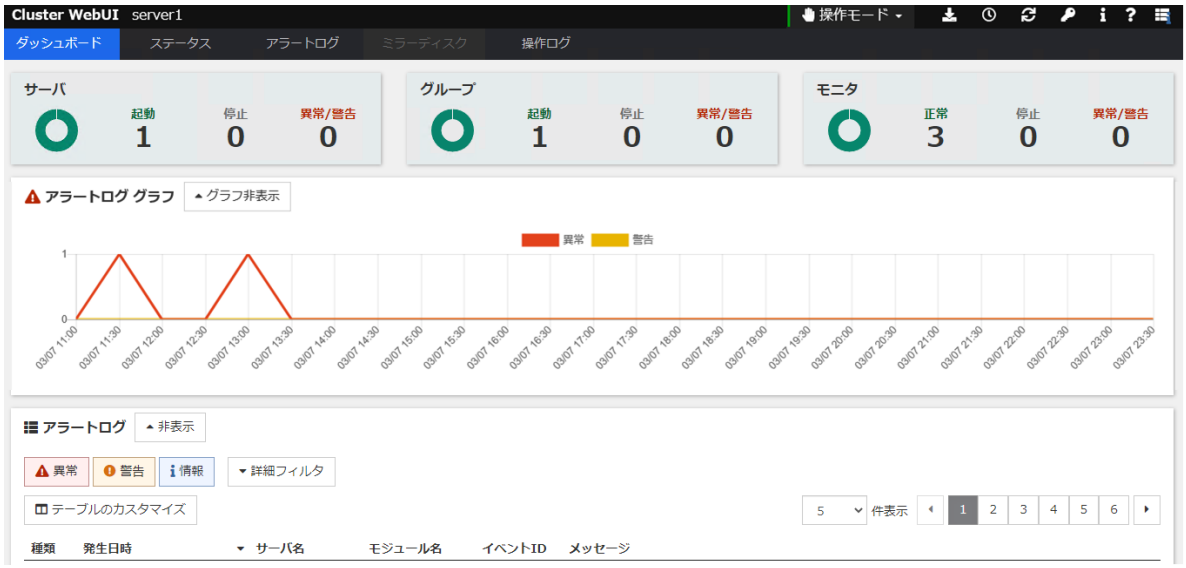
構成情報を反映するには、以下の手順に従ってください。

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. アップロード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アップロード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. クラスタの状態が 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

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。

- 4.1. グループリソース一覧
- 4.2. アプリケーションリソースの設定
- 4.3. スクリプトリソースの設定
- 4.4. サービスリソースの設定

4.1 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
アプリケーションリソース	アプリケーション (ユーザ作成アプリケーションを含む) を起動 / 停止するための仕組みを提供します。	appli
スクリプトリソース	ユーザ作成スクリプト等のスクリプト (BAT) を起動 / 停止するための仕組みを提供します。	script
サービスリソース	データベースや Web などのサービスを起動 / 停止するための仕組みを提供します。	service

4.2 アプリケーションリソースの設定

CLUSTERPRO X SingleServerSafe 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を登録できます。アプリケーションリソースには、ユーザ独自のアプリケーションも登録できます。

アプリケーションとは、ファイルの拡張子が exe/cmd/bat などのファイルが、コマンドラインなどから実行可能なプログラムを指します。

4.2.1 詳細タブ

常駐タイプ (既定値：常駐)

アプリケーションのタイプを設定します。以下の中から選択します。

- 常駐

  アプリケーションが常駐する場合に選択します。

- 非常駐

  アプリケーションが常駐しない (実行後に処理がすぐ戻る) 場合に選択します。

開始パス (1023 バイト以内)

アプリケーションリソースの開始時の実行可能ファイル名を設定します。

終了パス (1023 バイト以内)

アプリケーションリソースの終了時の実行可能ファイル名を設定します。常駐タイプが常駐の場合以下の動作となります。

- 終了パスを指定しなかった場合

  非活性時に CLUSTERPRO より起動しているアプリケーションの終了処理を行います。

- 終了パスを指定した場合

非活性時に終了パスで指定したアプリケーションを実行することにより起動しているアプリケーションの終了処理を行います。

注釈: [開始パス]、および [終了パス] には実行可能ファイル名の絶対パス、あるいは環境変数で設定されたパスの通った実行可能ファイル名を設定します。相対パスは指定しないでください。相対パスを指定した場合、アプリケーションリソースの起動に失敗する可能性があります。

調整

[アプリケーション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。アプリケーションリソースの詳細設定を行います。

アプリケーション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。

同期 （開始）

常駐型アプリケーションの場合、本設定は無視されます。

非常駐型アプリケーションの場合、アプリケーションの実行時にアプリケーションの終了を待ちます。

非同期 （開始）

常駐型アプリケーションの場合、本設定は無視されます。

非常駐型アプリケーションの場合、アプリケーションの実行時にアプリケーションの終了を待ちません。

正常な戻り値 (開始）(1023 バイト以内)

「非同期」 を選んだ場合、入力欄は入力できません。

常駐タイプが非常駐の場合に開始パスで設定した実行可能ファイル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。

- 値がない場合

  戻り値は無視します。

- 値がある場合

  以下の入力規則に従ってください。

  – 0,2,3 のようにカンマで区切る

  – 0-3 のようにハイフンで指定

注釈: 実行可能ファイルとしてバッチファイルを指定している場合、バッチファイルを実行する cmd.exe で異常が発生した場合に 「1」 が返却されますので、正常な戻り値として 「1」 を指定すると異常を検出できなくなります。

同期 （終了）

常駐型アプリケーションの場合、終了パスを指定しなかったときは起動しているアプリケーションの終了を待ちます。終了パスを指定したときは終了パスで指定したアプリケーションの終了を待ちます。

非常駐型アプリケーションの場合、アプリケーションの実行時にアプリケーションの終了を待ちます。

非同期 （終了）

常駐型アプリケーションの場合、起動しているアプリケーションまたは終了パスで指定したアプリケーションの終了を待ちません。

非常駐型アプリケーションの場合、アプリケーションの実行時にアプリケーションの終了を待ちません。

正常な戻り値 （終了）(1023 バイト以内)

「非同期」 を選んだ場合、入力欄は入力できません。

常駐タイプが非常駐の場合に終了パスで設定した実行可能ファイル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。

- 値がない場合

  戻り値は無視します。

- 値がある場合

  以下の入力規則に従ってください。

  – 0,2,3 のようにカンマで区切る

  – 0-3 のようにハイフンで指定

注釈: 実行可能ファイルとしてバッチファイルを指定している場合、バッチファイルを実行する cmd.exe で異常が発生した場合に 「1」 が返却されますので、正常な戻り値として 「1」 を指定すると異常を検出できなくなります。

タイムアウト （開始）(1〜9999)

常駐型アプリケーションの場合、本設定は無視されます。

非常駐型アプリケーションの場合、アプリケーション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。設定時間内にアプリケーションが終了しないと、異常と判断します。

タイムアウト （終了）(1〜9999)

常駐型アプリケーションの場合、起動しているアプリケーションまたは終了パスで指定したアプリケーションの終了を待つ場合 ([同期]) のタイムアウトを設定します。

非常駐型アプリケーションの場合、アプリケーション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。設定時間内にアプリケーションが終了しないと、異常と判断します。

対象 VCOM リソース名

使用しません。

終了時アプリケーションを強制終了する

非活性時の終了処理としてアプリケーションを強制終了するかどうかを設定します。設定した場合、通常の終了処理を行わず強制終了によりアプリケーションを終了させます。常駐タイプに「常駐」を設定しており、かつ終了パスを指定していない場合のみ有効となります。

実行ユーザ

アプリケーションを実行するユーザを指定します。実行ユーザは [クラスタのプロパティ] の [アカウント] タブに登録されたユーザの中から選択可能です。

「個別指定する」を指定している場合、開始タブ/終了タブにおける実行ユーザの設定が使用されます。

「個別指定する」以外を指定している場合、開始タブ/終了タブの設定は使用されなくなり、本パラメータで指定した実行ユーザの設定が使用されます。

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。

開始タブ / 終了タブ 共通

開始 / 終了に関する詳細設定が表示されます。

カレントディレクトリ (1023 バイト以内)

アプリケーションを実行する時のディレクトリを設定します。

オプションパラメータ (1023 バイト以内)

アプリケーションに対する入力パラメータを設定します。入力パラメータが複数ある場合は、スペース

区切りで設定します。スペースを含む入力パラメータがある場合は、入力パラメータをダブルクオート（"） で括ります。

例: "param 1" param2

ウィンドウサイズ

アプリケーションを実行する時のウィンドウサイズを以下の中から選択します。

- **[非表示]**

  アプリケーションは表示されません。

- **[通常]**

  アプリケーションは通常のウィンドウで表示されます。

- **[最大化]**

  アプリケーションは最大化のウィンドウで表示されます。

- **[最小化]**

  アプリケーションは最小化のウィンドウで表示されます。

実行ユーザ ドメイン

アプリケーションを実行するユーザアカウントの所属するドメインを指定します。

[終了] タブの場合、グループの停止・再開は不要です。

実行ユーザ アカウント

アプリケーションを実行するユーザアカウントを指定します。[*1]

[終了] タブの場合、グループの停止・再開は不要です。

実行ユーザ パスワード

アプリケーションを実行するユーザアカウントのパスワードを指定します。

[終了] タブの場合、グループの停止・再開は不要です。

コマンドプロンプトから実行する

アプリケーションをコマンドプロンプト (cmd.exe) から実行するかどうかを設定します。ファイルの拡張子が、exe/cmd/bat 以外のアプリケーション (JavaScript や VBScript 等) を実行する場合に指定します。

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。

[*1] 実行ユーザアカウントを指定しなかった場合、アプリケーションはローカルシステムアカウントとして実行されます。

4.3 スクリプトリソースの設定

CLUSTERPRO X SingleServerSafe 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スクリプトを登録できます。スクリプトリソースには、ユーザ独自のスクリプトなども登録できます。

スクリプトリソース用に、開始スクリプトと終了スクリプトが用意されています。それぞれ、グループの開始時・終了時に実行されます。ファイル名固定です。

start.bat 開始スクリプト

stop.bat 終了スクリプト

グループ A 開始スクリプト： start.bat の一例

```
rem ********************************************************************
rem *                              START.BAT                             *
rem ********************************************************************

rem 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" GOTO NORMAL
IF "%CLP_EVENT%"=="FAILOVER" GOTO FAILOVER
IF "%CLP_EVENT%"=="RECOVER" GOTO RECOVER


rem CLUSTERPRO は動作していない
GOTO no_clp


:NORMAL
IF "%CLP_DISK%"=="FAILURE" GOTO ERROR_DISK

    rem ここに、業務の通常起動処理を記述する。
    rem この処理は以下のタイミングで実行される。
    rem
    rem 通常立ち上げ
    rem


rem 実行サーバ環境変数を参照して、処理の振り分けを行う。
IF "%CLP_SERVER%"=="OTHER" GOTO ON_OTHER1
```

(次のページに続く)

(前のページからの続き)

```
    rem プライマリサーバで、業務が通常起動される場合のみ
    rem 行いたい処理を記述する。
    rem この処理は以下のタイミングで実行される。
    rem
    rem 通常立ち上げ
    rem

GOTO EXIT


:ON_OTHER1

rem プライマリサーバ以外で、業務が通常起動される場合のみ
rem 行いたい処理を記述する。
rem
rem SingleServerSafe ではこの処理は実行されない。
rem

GOTO EXIT


:FAILOVER

rem DISK 接続情報環境変数を参照して、エラー処理を行う。
IF "%CLP_DISK%"=="FAILURE" GOTO ERROR_DISK

    rem 業務の起動処理を記述する。
    rem
    rem SingleServerSafe ではこの処理は実行されない。
    rem


rem 実行サーバ環境変数を参照して、処理の振り分けを行う。
IF "%CLP_SERVER%"=="OTHER" GOTO ON_OTHER2

    rem プライマリサーバで業務が起動される場合のみ
    rem 行いたい処理を記述する。
    rem
```

(次のページに続く)

(前のページからの続き)

```
    rem SingleServerSafe ではこの処理は実行されない。
    rem

GOTO EXIT


:ON_OTHER2

rem 非プライマリサーバで業務が起動される場合のみ
rem 行いたい処理を記述する。
rem
rem SingleServerSafe ではこの処理は実行されない。
rem


GOTO EXIT


:RECOVER

rem クラスタ復帰後のリカバリ処理を記述する。
rem この処理は以下のタイミングで実行される。
rem
rem クラスタ復帰
rem

GOTO EXIT


:ERROR_DISK

rem ディスク関連のエラー処理を記述する。

:no_clp

:EXIT
exit
```

グループ A 終了スクリプト： stop.bat の一例

```
rem ************************************************************
rem *                          STOP.BAT                        *
rem ************************************************************

rem 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" GOTO NORMAL
IF "%CLP_EVENT%"=="FAILOVER" GOTO FAILOVER


rem CLUSTERPRO は動作していない
GOTO NO_CLP


:NORMAL
rem DISK 接続情報環境変数を参照して、エラー処理を行う。
IF "%CLP_DISK%"=="FAILURE" GOTO ERROR_DISK

    rem ここに、業務の通常終了処理を記述する。
    rem この処理は以下のタイミングで実行される。
    rem
    rem 通常シャットダウン
    rem


rem 実行サーバ環境変数を参照して、処理の振り分けを行う。
IF "%CLP_SERVER%"=="OTHER" GOTO ON_OTHER1

    rem プライマリサーバで、業務が通常処理される場合のみ
    rem 行いたい処理を記述する。
    rem この処理は以下のタイミングで実行される。
    rem
    rem 通常シャットダウン
    rem

GOTO EXIT


:ON_OTHER1
```

(次のページに続く)

(前のページからの続き)

```
rem プライマリサーバ以外で、業務が通常終了される場合のみ
rem 行いたい処理を記述する。
rem
rem SingleServerSafe ではこの処理は実行されない。
rem

GOTO EXIT


:FAILOVER

rem DISK 接続情報環境変数を参照して、エラー処理を行う。
IF "%CLP_DISK%"=="FAILURE" GOTO ERROR_DISK

    rem フェイルオーバ後の通常終了処理を記述する。
    rem
    rem SingleServerSafe ではこの処理は実行されない。
    rem


rem 実行サーバ環境変数を参照して、処理の振り分けを行う。
IF "%CLP_SERVER%"=="OTHER" GOTO ON_OTHER2

    rem フェイルオーバ後、プライマリサーバで業務が終了
    rem される場合のみ行いたい処理を記述する。
    rem
    rem SingleServerSafe ではこの処理は実行されない。
    rem

GOTO EXIT


:ON_OTHER2

rem フェイルオーバ後、非プライマリサーバで業務が終了
rem される場合のみ行いたい処理を記述する。
rem
rem SingleServerSafe ではこの処理は実行されない。
rem
```

(次のページに続く)

(前のページからの続き)

```
GOTO EXIT


:ERROR_DISK

rem ディスク関連のエラー処理を記述する。

:NO_CLP

:EXIT
exit
```

4.3.1 スクリプト作成のヒント

- アラートログに、メッセージを出力できる clplogcmd コマンドがありますのでご活用ください。

4.3.2 スクリプトリソースに関する注意事項

開始/終了スクリプト内で start コマンドを利用している場合には、start コマンド経由で起動するスクリプト側で exit コマンドを使用して処理を終了するようにしてください。

4.3.3 詳細タブ

[スクリプト一覧] に既定のスクリプトファイル名 [start.bat]、[stop.bat] が表示されます。

追加

スクリプトの追加ダイアログが表示されます。[start.bat]、[stop.bat] 以外のスクリプトを追加します。

注釈:

追加するスクリプトのファイル名に 2 バイト文字は使用しないでください。
追加するスクリプトのファイル名に「&(アンパサンド)」、「=(等号)」は使用しないでください。

削除

スクリプトを削除します。[start.bat]、[stop.bat] は削除できません。

表示

選択したスクリプトファイルを表示します。表示しようとしているスクリプトファイルが表示中または編集中の場合は表示できません。

編集

選択したスクリプトファイルを編集できます。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

ファイル選択ダイアログボックスが表示されます。

注釈: Cluster WebUI から [削除] を実行しスクリプトファイルを削除しても、実ファイルは削除されません。またスクリプトファイルの削除後、Cluster WebUI を再起動するなどして構成情報を読込みなおした場合、削除したスクリプトファイルが [スクリプト一覧] に表示されます。

[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

スクリプトリソース調整プロパティダイアログを表示します。スクリプトリソースの詳細設定を行います。

スクリプト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。

[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。

非同期

選択できません。

正常な戻り値 (1023 バイト以内)

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。

- 値がない場合
  戻り値は無視します。
- 値がある場合
  以下の入力規則に従ってください。
  - 0,2,3 のようにカンマで区切る
  - 0-3 のようにハイフンで指定

注釈:

値を設定する場合、開始スクリプトと終了スクリプトに同じ値を設定してください。

スクリプトを実行する cmd.exe で異常が発生した場合、「1」 が返却されますので、正常な戻り値として 「1」 を設定すると異常が検出できなくなります。

リカバリ処理を実行する

以下のタイミングで開始スクリプトを実行するか否かを設定します。

- サーバの復帰時
- モニタリソースの異常検出時
- グループリソース活性処理の異常終了時

リカバリ処理として実行される場合は環境変数 CLP_EVENT に RECOVER が設定されます。

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。

対象 VCOM リソース名

使用しません。

実行ユーザ

スクリプトを実行するユーザを指定します。実行ユーザは [クラスタのプロパティ] の [アカウント] タブに登録されたユーザの中から選択可能です。

実行ユーザを指定しなかった場合、スクリプトはローカルシステムアカウントとして実行されます。

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。

4.4 サービスリソースの設定

CLUSTERPRO X SingleServerSafe 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サービスを登録できます。サービスリソースには、ユーザ独自のサービスも登録できます。

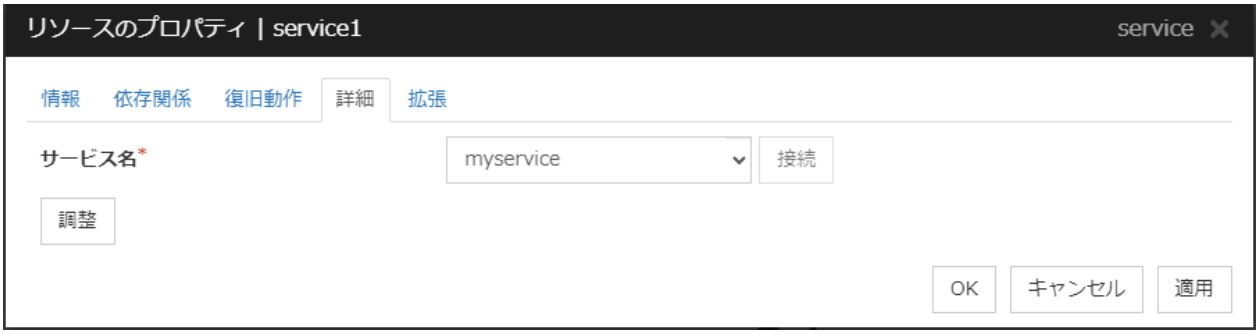
サービスとは、OS のサービス制御マネージャによって管理されるサービスを指します。

4.4.1 サービスリソースに関する注意事項

- 通常、サービスリソースで実行されるサービスは手動起動に設定します。自動起動で起動するサービスや、サービスリソース以外によって起動される可能性があるサービスの場合は、後述するサービスリソース調整プロパティダイアログの [サービス] タブの [サービスが起動済みの場合、エラーとしない] チェックボックスをオンにする必要があります。このチェックボックスがオフの場合、既に起動されているサービスに対してサービスリソースでサービス開始処理が実行されると、活性失敗となります。
- サービスリソースで実行されるサービスは CLUSTERPRO 以外から制御させないため、サービス制御マネージャによる回復動作は設定しないことを推奨します。

  サービス制御マネージャによる回復動作でサービスの再起動を設定している場合、CLUSTERPRO による回復動作と重複して予期せぬ挙動となる可能性があります。

4.4.2 詳細タブ



サービス名 (1023 バイト以内)

サービスリソースで使用するサービス名または、サービス表示名を設定します。

コンボボックスの選択肢はサーバから取得したサービスのサービス表示名一覧が表示されます。

接続

サーバからサービス一覧を取得し、[サービス名] コンボボックスに表示するサービス表示名一覧を更新します。

調整

サービスリソース調整プロパティダイアログを表示します。サービスリソースの詳細設定を行います。

サービス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。

同期

サービス開始時は、サービスの状態が 「起動済」 状態になるまで待ち合せを行います。通常、サービスを開始すると、「起動中」→「起動済」 のように状態が遷移します。

サービス停止時は、サービスの状態が 「停止」 状態になるまで待ち合せを行います。通常、サービスを停止すると、「停止中」→「停止」 のように状態が遷移します。

非同期

待ち合せを行いません。

タイムアウト (1～9999)

サービス開始時は、サービスの状態が「起動」状態になるまで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。設定時間内にサービスが 「起動」 状態にならない場合は、異常と判断します。

サービス停止時は、サービスの状態が 「停止」 状態になるまで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。設定時間内にサービスが 「停止」 状態にならない場合は、異

常と判断します。

対象 VCOM リソース名

使用しません。

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。

サービスタブ

サービスに関する詳細設定が表示されます。

開始パラメータ (1023 バイト以内)

サービスに対する入力パラメータを設定します。入力パラメータが複数ある場合は、スペース区切りで設定します。スペースを含む入力パラメータがある場合は、入力パラメータをダブルクオート （") で括ります。エスケープシークエンス \ を使用することはできません。

例: "param 1" param2

サービスが起動済みの場合、エラーとしない

- **チェックボックスがオン**

  サービス開始時に、すでにサービスが開始済みの場合、そのまま活性状態にします。

- **チェックボックスがオフ**

  サービス開始時に、すでにサービスが開始済みの場合、活性異常とします。

サービス開始後の待ち合わせ (0～9999)

サービスが起動状態になった後、待ち合わせる時間を指定します。指定された時間分、待ち合わせた後、サービスリソースの活性が完了した状態となります。

サービス停止後の待ち合わせ (0〜9999)

サービスが停止状態になった後、待ち合わせる時間を指定します。指定された時間分、待ち合わせた後、サービスリソースの非活性が完了した状態となります。

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。

第 5 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。

- 5.1. モニタリソース一覧
- 5.2. モニタリソースのプロパティ
- 5.3. アプリケーション監視リソースの設定
- 5.4. サービス監視リソースの設定
- 5.5. ディスク *RW* 監視リソースの設定
- 5.6. *IP* 監視リソースの設定
- 5.7. *NIC Link Up/Down* 監視リソースの設定
- 5.8. カスタム監視リソースの設定
- 5.9. マルチターゲット監視リソースの設定
- 5.10. 外部連携監視リソースの設定
- 5.11. プロセス名監視リソースの設定
- 5.12. *DB2* 監視リソースの設定
- 5.13. *FTP* 監視リソースの設定
- 5.14. *HTTP* 監視リソースの設定
- 5.15. *IMAP4* 監視リソースの設定

- 5.16. *ODBC* 監視リソースの設定
- 5.17. *Oracle* 監視リソースの設定
- 5.18. *POP3* 監視リソースの設定
- 5.19. *PostgreSQL* 監視リソースの設定
- 5.20. *SMTP* 監視リソースの設定
- 5.21. *SQL Server* 監視リソースの設定
- 5.22. *Tuxedo* 監視リソースの設定
- 5.23. *WebLogic* 監視リソースの設定
- 5.24. *WebOTX* 監視リソースの設定
- 5.25. *WebSphere* 監視リソースの設定
- 5.26. *JVM* 監視リソースの設定
- 5.27. システム監視リソースの設定
- 5.28. プロセスリソース監視リソースの設定
- 5.29. ユーザ空間監視リソースの設定

5.1 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
アプリケーション監視リソース	アプリケーションリソースの監視を行います。	活性時 (固定)	appli
サービス監視リソース	サービスリソースの監視を行います。	常時 / **活性時**	全て
ディスク RW 監視リソース	ファイルシステムへのダミーデータ書込みによりディスクデバイスの監視を行います。	常時 / **活性時**	全て
IP 監視リソース	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 監視リソース	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
カスタム監視リソース	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
マルチターゲット監視リソース	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
外部連携監視リソース	異常発生通知受信時に実行する異常時動作の設定と、異常発生通知を Cluster WebUI に表示するためのモニタリソースです。	常時 (固定)	なし
プロセス名監視リソース	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 監視リソース	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 5.1 – 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 監視リソース	FTP サーバへの監視機構を提供します。	活性時 (固定)	全て
HTTP 監視リソース	HTTP サーバへの監視機構を提供します。	活性時 (固定)	全て
IMAP4 監視リソース	IMAP サーバへの監視機構を提供します。	活性時 (固定)	全て
ODBC 監視リソース	ODBC でアクセス可能な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 監視リソース	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 監視リソース	POP サーバへの監視機構を提供します。	活性時 (固定)	全て
PostgreSQL 監視リソース	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
SMTP 監視リソース	SMTP サーバへの監視機構を提供します。	活性時 (固定)	全て
SQL Server 監視リソース	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 監視リソース	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 (固定)	全て
WebLogic 監視リソース	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 (固定)	全て
WebOTX 監視リソース	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 (固定)	全て
WebSphere 監視リソース	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 (固定)	全て

次のページに続く

表 5.1 – 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
JVM 監視リソース	Java VM の監視を行います。	**常時** / 活性時	全て
システム監視リソース	システムリソースの監視を行います。	常時 (固定)	全て
プロセスリソース監視リソース	プロセスリソースの監視を行います。	常時 (固定)	全て
ユーザ空間監視リソース	ユーザ空間のストール監視機構を提供します。	常時 (固定)	なし

5.1.1 ライセンスが必要なモニタリソース

以下の表に記述されているモニタリソースは、オプション製品になるため、ライセンスが必要になります。
ご使用になる場合は、製品ライセンスを入手してライセンスを登録してください。

オプション製品名	モニタリソース名
CLUSTERPRO X Database Agent 5.3 for Windows	DB2 監視リソース ODBC 監視リソース Oracle 監視リソース PostgreSQL 監視リソース SQL Server 監視リソース

次のページに続く

表 5.2 – 前のページからの続き

オプション製品名	モニタリソース名
CLUSTERPRO X Internet Server Agent 5.3 for Windows	FTP 監視リソース HTTP 監視リソース IMAP4 監視リソース POP3 監視リソース SMTP 監視リソース
CLUSTERPRO X Application Server Agent 5.3 for Windows	Tuxedo 監視リソース WebSphere 監視リソース WebLogic 監視リソース WebOTX 監視リソース
CLUSTERPRO X Java Resource Agent 5.3 for Windows	JVM 監視リソース
CLUSTERPRO X System Resource Agent 5.3 for Windows	システム監視リソース プロセスリソース監視リソース

ライセンスの登録手順については、『インストールガイド』 を参照してください。

5.1.2 監視オプションの動作確認済アプリケーション情報

監視オプションは、下記のアプリケーションを監視対象として動作確認しています。

x86_64 版

モニタリソース	監視対象のアプリケーション	CLUSTERPRO Version	備考
Oracle 監視	Oracle Database 19c (19.3)	13.00~	
DB2 監視	DB2 V11.5	13.00~	
	DB2 V12.1	13.31~	
PostgreSQL 監視	PostgreSQL 14.1	13.00~	
	PostgreSQL 15.1	13.10~	
	PostgreSQL 16.3	13.21~	
	PostgreSQL 17.2	13.30~	
	PowerGres on Windows V13	13.00~	
SQL Server 監視	SQL Server 2019	13.00~	
	SQL Server 2022	13.10~	
Tuxedo 監視	Tuxedo 12c Release 2 (12.1.3)	12.00~	
	Tuxedo 22c (22.1.0)	13.20~	
WebLogic 監視	WebLogic Server 11g R1	12.00~	
	WebLogic Server 11g R2	12.00~	
	WebLogic Server 12c R2 (12.2.1)	12.00~	
	WebLogic Server 14c (14.1.1)	12.20~	
WebSphere 監視	WebSphere Application Server 8.5	12.00~	
	WebSphere Application Server 8.5.5	12.00~	
	WebSphere Application Server 9.0	12.00~	
WebOTX 監視	WebOTX Application Server V9.1	12.00~	
	WebOTX Application Server V9.2	12.00~	
	WebOTX Application Server V9.3	12.00~	

次のページに続く

表 5.3 – 前のページからの続き

モニタリソース	監視対象のアプリケーション	CLUSTERPRO Version	備考
	WebOTX Application Server V9.4	12.00~	
	WebOTX Application Server V9.5	12.00~	
	WebOTX Application Server V10.1	12.00~	
	WebOTX Application Server V10.3	12.30~	
	WebOTX Application Server V11.1	13.20~	
JVM 監視	WebLogic Server 11g R1	12.00~	
	WebLogic Server 12c R2 (12.2.1)	12.00~	
	WebLogic Server 14c (14.1.1)	12.20~	
	WebOTX Application Server V9.1	12.00~	
	WebOTX Application Server V9.2	12.00~	
	WebOTX Application Server V9.3	12.00~	
	WebOTX Application Server V9.4	12.00~	
	WebOTX Application Server V9.5	12.00~	
	WebOTX Application Server V10.1	12.00~	
	WebOTX Application Server V10.3	12.30~	
	WebOTX Application Server V11.1	12.20~	
	WebOTX Enterprise Service Bus V8.4	12.00~	

次のページに続く

表 5.3 – 前のページからの続き

モニタリソース	監視対象のアプリケーション	CLUSTERPRO Version	備考
	WebOTX Enterprise Service Bus V8.5	12.00~	
	WebOTX Enterprise Service Bus V10.3	12.30~	
	WebOTX Enterprise Service Bus V11.1	13.20~	
	Apache Tomcat 8.5	12.00~	
	Apache Tomcat 9.0	12.00~	
	Apache Tomcat 10.0	13.02~	
	Apache Tomcat 10.1	13.30~	
	WebSAM SVF for PDF 9.1	12.00~	
	WebSAM SVF for PDF 9.2	12.00~	
	WebSAM SVF PDF Enterprise 10.1	13.10~	
	WebSAM Report Director Enterprise 9.1	12.00~	
	WebSAM Report Director Enterprise 9.2	12.00~	
	WebSAM RDE SUITE 10.1	13.10~	
	WebSAM Universal Connect/X 9.1	12.00~	
	WebSAM Universal Connect/X 9.2	12.00~	
	WebSAM SVF Connect SUITE Standard 10.1	13.10~	
システム監視	バージョン指定無し	12.00~	
プロセスリソース監視	バージョン指定無し	12.10~	

5.2 モニタリソースのプロパティ

5.2.1 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。

5.2.2 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)

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 (Oracle 監視リソースの場合のみ)

タイムアウト発生時に、CLUSTERPRO の監視プロセスのダンプファイルを採取するかどうかを指定します。

採取されたダンプファイルは CLUSTERPRO インストールフォルダ配下の work\rm\リソース名\errinfo.cur フォルダに保存されます。採取が複数回実行された場合は、過去の採取情報のフォルダ名が errinfo.1、errinfo.2 とリネームされ、最新の情報から 5 世代分まで保存されます。

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

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。
- **[意図的なストップエラーを発生させる]**
  意図的なストップエラーを発生させます。

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。

- カスタム監視リソース (監視タイプが [非同期] の場合のみ)
- マルチターゲット監視リソース
- 外部連携監視リソース
- JVM 監視リソース
- システム監視リソース

- プロセスリソース監視リソース
- ユーザ空間監視リソース

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

  監視対象のリソースが活性した時に監視を開始し、リソースが停止するときに監視を停止します。

  [監視タイミング] が [活性時] の場合、監視対象のリソースを設定する必要があります。[参照] をクリックし、監視対象を設定してください。

  監視対象のリソースを選択して、[OK] をクリックします。

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。サーバ名、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。

監視を行うサーバを選択する

使用しません。

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。

- 外部連携監視リソース

5.2.3 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。

5.2.4 回復動作タブ

通常の監視リソース (外部監視連携リソース以外) の場合

外部連携監視リソースの場合

回復対象と異常検出時の動作を設定します。異常検出時にリソースの再起動やクラスタ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

異常検出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 とクラスタに登録されているクラスタ名、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

再活性化を行う前にスクリプトを実行するかどうかを指定します。

最大再活性回数 (0～99)

回復動作がカスタム設定の場合に回復対象の再活性を行う回数の上限を設定します。0 を設定すると再活性化を行いません。外部連携監視リソースではこの値は設定できません。

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。

フェイルオーバ先サーバ

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 [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。

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。
外部連携監視リソースのみ設定できます。

- 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 [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。

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 / 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 (実行可能なバッチ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。ただし、実行可能ファイル名のみを設定する場合、あらかじめ環境変数にパスを設定しておく必要があります。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：

```
"C:\Program Files\script.bat"
```

また VB スクリプトを実行させるには下記のように入力してください。

例：

```
cscript script.vbs
```

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（実行可能なバッチ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。

実行ユーザ

スクリプトを実行するユーザを指定します。実行ユーザは [クラスタのプロパティ] の [アカウント] タブに登録されたユーザの中から選択可能です。

実行ユーザを指定しなかった場合、スクリプトはローカルシステムアカウントとして実行されます。

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。

最終動作に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監視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。回復対象に LocalServer が選択されている場合は選択できません。

- 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。

- 意図的なストップエラーの発生

  意図的にストップエラーを発生させます。

5.3 アプリケーション監視リソースの設定

アプリケーション監視リソースはアプリケーションリソースの監視を行います。アプリケーションリソースが活性した時点から監視を開始します。アプリケーションリソースの常駐タイプの設定が [常駐] の場合のみ監視できます。

5.3.1 アプリケーション監視リソースによる監視方法

アプリケーションの死活監視を定期的に行い、アプリケーションの消滅を検出した場合に異常と判断します。

5.3.2 アプリケーション監視リソースに関する注意事項

活性に成功したアプリケーションリソースを監視します。アプリケーションリソースの常駐タイプの設定が [常駐] の場合のみ監視できます。

本リソースはアプリケーションリソースを追加時、常駐タイプを「常駐」としていた場合に自動的に登録されます。各アプリケーションリソースに対応するアプリケーション監視リソースが自動登録されます。

アプリケーション監視リソースには既定値が設定されているので、必要があれば適切な値に変更してください。

アプリケーションリソースを追加時、常駐タイプを「非常駐」としていた場合、本リソースを追加することはできません。

5.4 サービス監視リソースの設定

サービス監視リソースはサービスリソースの監視、またはサービスの監視を行います。

5.4.1 サービス監視リソースによる監視方法

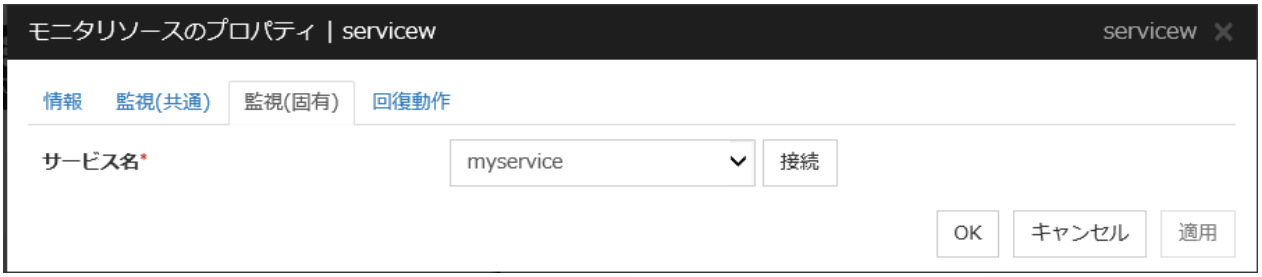
サービスの状態をサービス制御マネージャに対して定期的に問合せ、状態が 「停止」 状態となった場合に異常と判断します。

5.4.2 サービス監視リソースに関する注意事項

[監視タイミング]-[活性時] を選択し、[対象リソース] にサービスリソースを設定している場合、サービス監視リソースの [サービス名] はサービスリソースの [サービス名] が設定されます。

本リソースはサービスリソースを追加した時に自動的に登録されます。各サービスリソースに対応するサービス監視リソースが自動登録されます。

5.4.3 監視 (固有) タブ



サービス名 (1023 バイト以内)

サービスリソースで使用するサービス名または、サービス表示名を設定します。

コンボボックスの選択肢はすべてのサーバから取得したサービスのサービス表示名一覧が表示されます。

サービス名は [監視タイミング]-[活性時]-[対象リソース] にサービスリソースを設定している場合、設定変更は行えません。

接続

すべてのサーバからサービス一覧を取得し、[サービス名] コンボボックスに表示するサービス表示名一覧を更新します。

5.5 ディスク RW 監視リソースの設定

ディスク RW 監視リソースは、ファイルシステムへのダミーデータ書込みによりディスクデバイスの監視を行います。

5.5.1 ディスク RW 監視リソースによる監視方法

指定されたファイルシステム (ベーシックボリュームまたはダイナミックボリューム) 上を指定された I/O サイズで write し、その結果 (write できたサイズ) を判断します （作成したファイルは write 後に削除されます)。

指定された I/O サイズが write できたことのみを判断し、書込みデータの正当性は判断しません。

Write する I/O 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。

使用するディスクやインターフェイスにより、様々な write 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 write のエラーを検出できない場合があります。

I/O サイズについては、ディスクの障害等を発生させ障害の検出ができることを確認してください。

注釈: 監視対象ディスクのディスクパス障害発生時に、ディスクパス冗長化ソフトウェアなどの機能でパスフェイルオーバを行う場合、監視タイムアウトの時間 （既定値 300 秒） を、パスフェイルオーバにかかる時間よりも長く設定する必要があります。

5.5.2 監視 (固有) タブ

ファイル名 (1023 バイト以内)

アクセスするためのファイル名を入力します。このファイルは監視処理の際に作成され、I/O 完了後に削除

されます。

注釈: ファイル名には絶対パスを指定して下さい。相対パスを指定した場合、予期しない場所を監視する可能性があります。

重要: ファイル名には既に存在するファイルを指定しないで下さい。既に存在するファイルを指定した場合、そのファイルの情報は失われます。

I/O サイズ (1〜9999999 既定値：2000000)

監視するディスクに行う I/O サイズを指定します。

ストール異常検出時動作

ストール異常検出時の動作を指定します。

[監視 (共通)] タブの [タイムアウト] で指定した時間内に、I/O の制御が OS から戻らない場合にストール異常とみなします。

- 何もしない
  何も行いません。
- HW リセット[*2]
  ハードウェアをリセットします。
- 意図的なストップエラーの発生 (既定値)
  ストップエラーを発生させます。

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） 検出時の動作を指定します。

- 回復動作を実行する
  ディスク RW 監視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 RW 監視リソースはディスクフル検出時に警告として扱います。

Write Through 方式を有効にする

監視 I/O の方式に Write Through 方式を適用します。

- 有効にした場合、ディスク RW 監視の異常検出精度が向上しますが、

[*2] 本機能を使用する場合、強制停止機能とは異なり、ipmiutil は必要ありません。

システムの I/O 負荷が上昇する場合があります。

5.6 IP 監視リソースの設定

IP 監視リソースは、ping コマンドを使用して応答の有無により、IP アドレスの監視を行うモニタリソースです。

5.6.1 IP 監視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。

- 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 監視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 監視リソースに全ての 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。

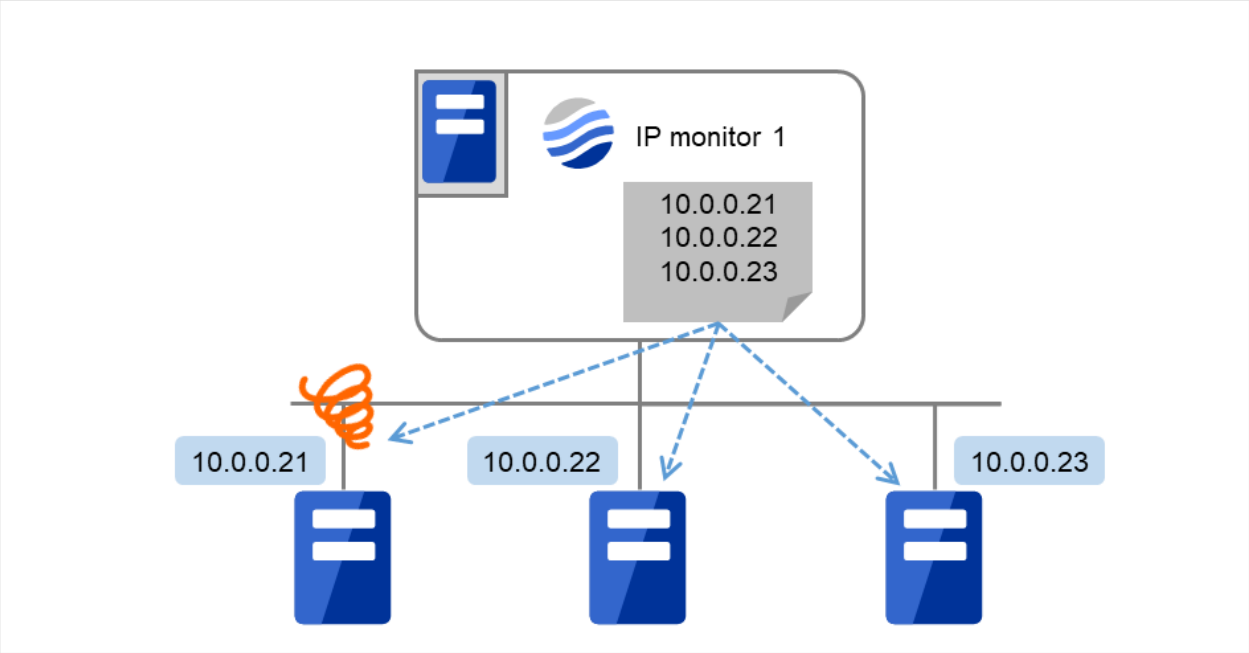


図 5.1　1 つの IP 監視リソースに全ての IP アドレスを登録（正常）

以下の図は 1 つの IP 監視リソースに全ての 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。

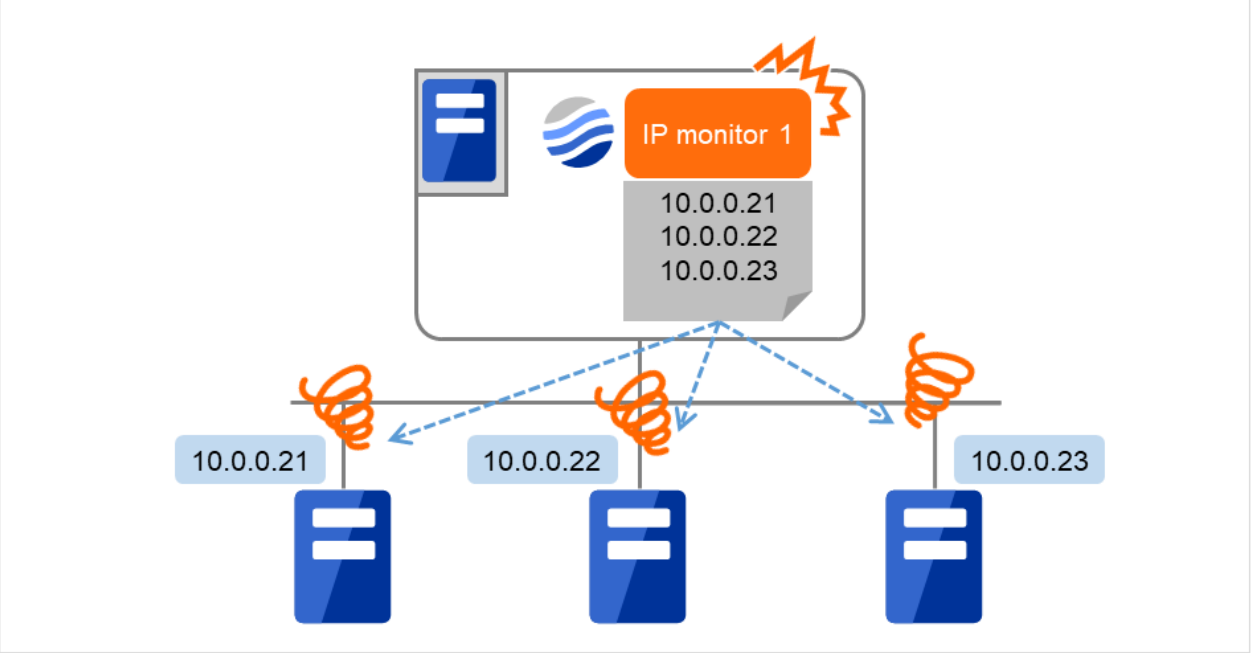


図 5.2　1 つの IP 監視リソースに全ての IP アドレスを登録（異常検出）

- 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 監視リソースを作成してください。

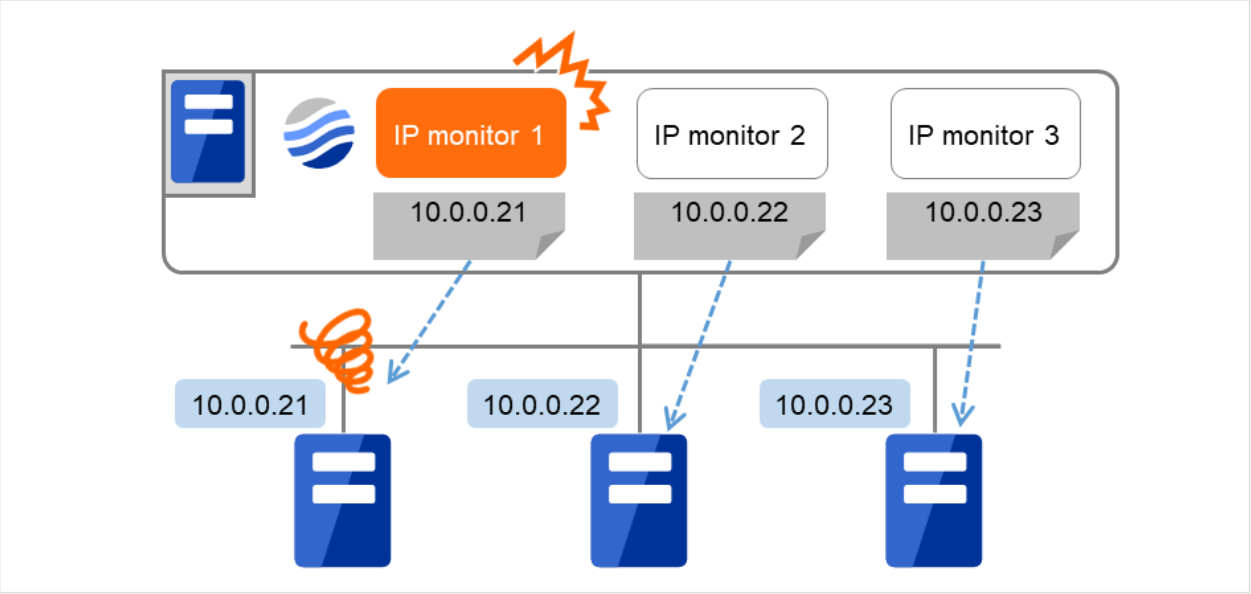


図 5.3　各 IP 監視リソースに IP アドレスを一つずつ登録（異常検出）

5.6.2 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。

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

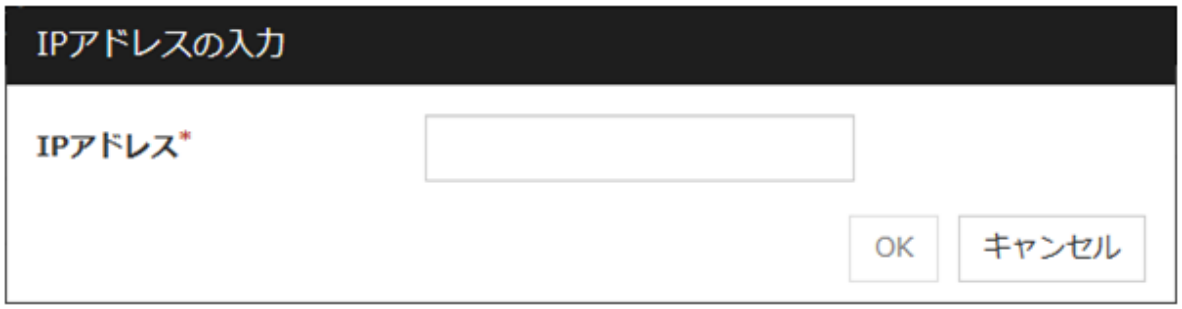
IP アドレスの入力ダイアログボックスが表示されます。[IP アドレス一覧] で選択している IP アドレスが表示されるので、編集して [OK] を選択します。

Ping タイムアウト (1～999999 既定値：1000)

監視する IP アドレスへの Ping のタイムアウトをミリ秒単位で設定します。

IP アドレスの入力

インタフェースに関する詳細設定が表示されます。



IP アドレス (255 バイト以内)

監視を行う IP ドレス入力して [OK] を選択してください。常時通信可能な IP アドレスを入力してください。

5.7 NIC Link Up/Down 監視リソースの設定

NIC Link Up/Down 監視リソースは、指定した NIC の Link 状態を取得し、Link の Up/Down の監視を行います。

5.7.1 NIC Link UP/Down 監視の構成および範囲

- 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。

5.7.2 監視 (固有) タブ

追加

監視を行うサーバを一覧に追加します。IP アドレスの入力ダイアログボックスが表示されます。

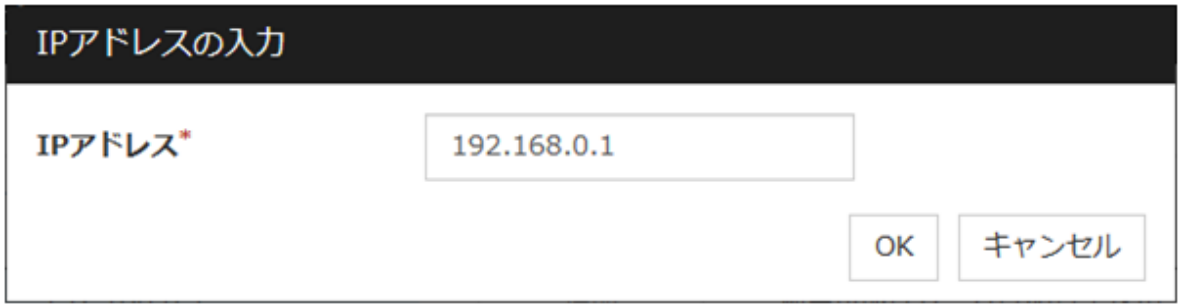
削除

監視を行うサーバを一覧から削除します。

編集

監視を行うサーバの NIC の IP アドレスを編集します。

IP アドレスの入力



IP アドレス (47 バイト以内)

監視を行う NIC の IP アドレスを設定してください。

5.8 カスタム監視リソースの設定

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

5.8.1 カスタム監視リソースに関する注意事項

- バッチファイル内でプロンプトへのメッセージ出力 (標準出力、エラー出力) を行うコマンドを実行する場合は、コマンドを実行した際にバッチファイルが停止する可能性があるため、メッセージ出力先にファイルもしくは nul を指定 (リダイレクト) してください。
- 監視タイプが [非同期] の場合は、タイムアウトに監視開始待ち時間より大きい値を設定してください。

5.8.2 カスタム監視リソースの監視方法

カスタム監視リソースは、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。

5.8.3 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 (実行可能なバッチ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（実行可能なバッチ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。ただし、スクリプトの後に引数は指定できません。

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。

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。

終了時アプリケーションを強制終了する

監視停止時の終了処理としてアプリケーションを強制終了するかどうかを設定します。設定した場合、通常の終了処理を行わず強制終了によりアプリケーションを終了させます。監視タイプに「非同期」を設定している場合のみ有効となります。

実行ユーザ

スクリプトを実行するユーザを指定します。実行ユーザは [クラスタのプロパティ] の [アカウント] タブに登録されたユーザの中から選択可能です。

実行ユーザを指定しなかった場合、スクリプトはローカルシステムアカウントとして実行されます。

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監視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。

5.9 マルチターゲット監視リソースの設定

マルチターゲット監視リソースは、複数のモニタリソースの監視を行います。

5.9.1 マルチターゲット監視リソースの注意事項

- マルチターゲット監視リソースは、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。

5.9.2 マルチターゲット監視リソースのステータス

マルチターゲット監視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

マルチターゲット監視リソースのステータスは以下のようになります。

マルチターゲット監視リソース 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 停止済み (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)

次のページに続く

表 5.4 – 前のページからの続き

マルチターゲット監視リソース 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 停止済み (offline)
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 停止済み (offline)	警告 (caution)	異常 (error)	正常 (normal)

- マルチターゲット監視リソースは、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、マルチターゲット監視リソースは異常 (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、マルチターゲット監視リソースの 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、マルチターゲット監視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、マルチターゲット監視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。

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

5.9.3 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。

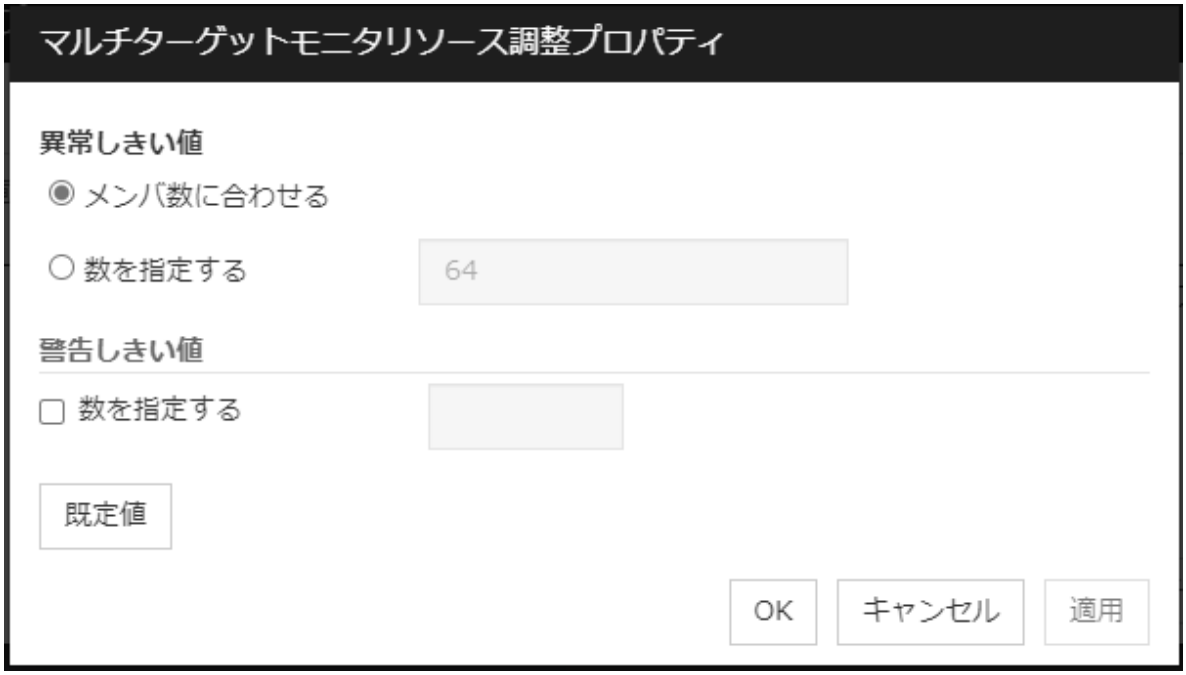
調整

[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。マルチターゲット監視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。

5.10 外部連携監視リソースの設定

外部連携監視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。

外部から clprexec コマンドを使って発行された異常発生通知を受信した場合に、外部連携監視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。

5.10.1 外部連携監視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、通知された監視タイプと監視対象 (監視対象は省略可能) が設定されている外部連携監視リソースの異常発生時の回復動作を行います。

通知された監視タイプ、監視対象が設定されている外部連携監視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。

図は外部連携監視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 Server 2 の外部連携監視リソースは、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。

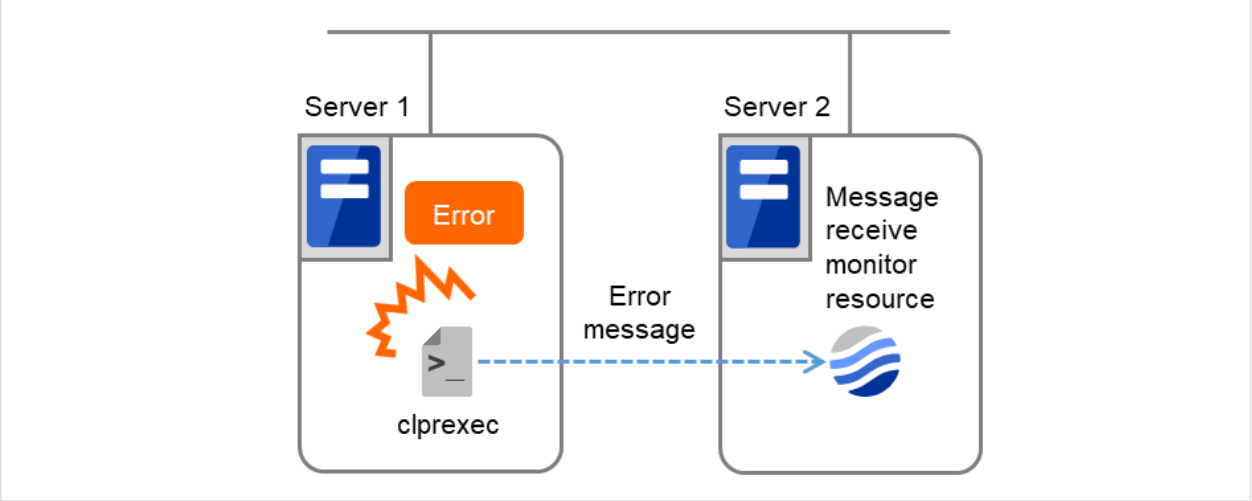


図 5.4　外部連携監視リソースを使用する構成

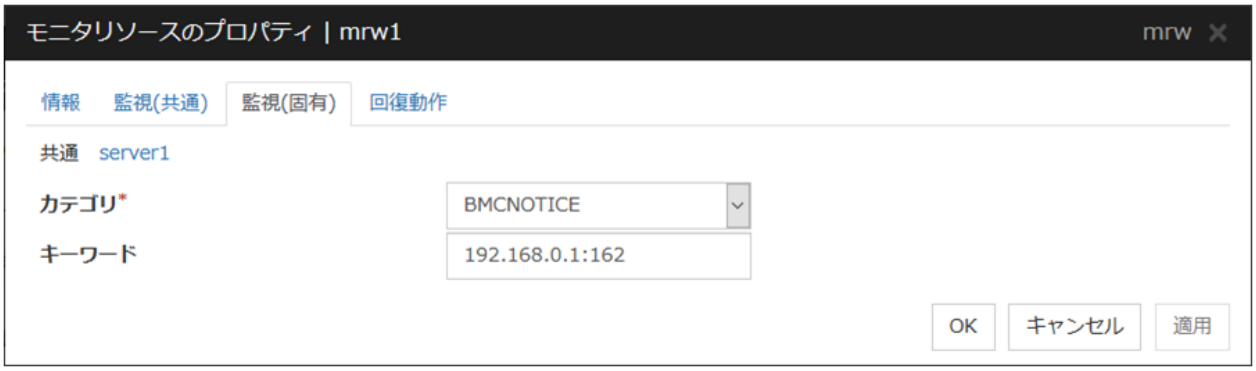
5.10.2 外部連携監視リソースに関する注意事項

- 外部連携監視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、外部連携監視リソースのステータスは "異常" になります。"異常" となった外部連携監視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監視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。

5.10.3 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。監視対象は省略可能です。

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。

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。

5.11 プロセス名監視リソースの設定

プロセス名監視リソースは、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。

5.11.1 プロセス名監視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 「"」（ダブルクォーテーション） 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以下のコマンドで確認し設定してください。

CLUSTERPRO インストールパス\bin\GetProcess.vbs

上記コマンドを実行すると、コマンドを実行したフォルダ配下に GetProcess_Result.txt が出力されます。GetProcess_Result.txt を開き、表示されているプロセスの CommandLine 部分を指定してください。出力情報に 「"」(ダブルクォーテーション) がある場合は、「"」 も含めて指定してください。

出力ファイルの例

```
20XX/07/26 12:03:13
Caption     CommandLine
services.exe    C:\WINDOWS\system32\services.exe
svchost.exe     C:\WINDOWS\system32\svchost -k rpcss
explorer.exe    C:\WINDOWS\Explorer.EXE
```

上記のコマンド出力情報から svchost.exe を監視する場合、

`C:\WINDOWS\system32\svchost -k rpcss` を監視対象プロセス名に指定します。

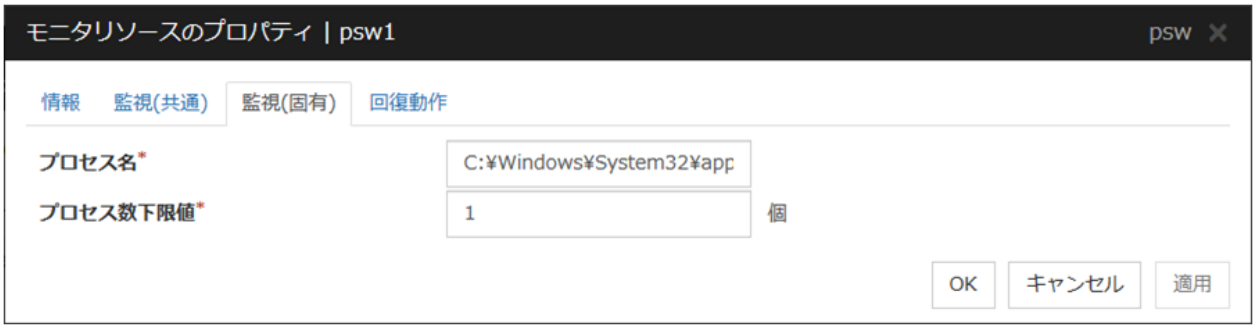
監視対象プロセス名に指定したプロセス名はプロセスの引数もプロセス名の一部として監視対象のプロセスを特定します。監視対象プロセス名を指定する場合は、引数を含めたプロセス名を指定してください。引数を含めずプロセス名のみ監視したい場合は、ワイルドカード （*） を使い、引数を含めない前方一致または部分一致で指定してください。

5.11.2 プロセス名監視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。

5.11.3 監視 (固有) タブ



プロセス名 (1023 バイト以内)

監視するプロセス名を設定します。必ず設定してください。

既定値 ： なし

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。

5.12 DB2 監視リソースの設定

DB2 監視リソースは、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。

5.12.1 DB2 監視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、「5. モニタリソースの詳細」 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。

監視処理は、DB2 の CLI を利用しているため、監視を行うサーバ上に、インターフェイス用の DLL(DB2CLI.DLL/DB2CLI64.DLL) がインストールされている必要があります。

監視の対象リソースには、DB2 を起動するサービスリソースやスクリプト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データベース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。

監視開始時に監視テーブルを作成します。グループが停止することにより監視が停止する場合に、監視テーブルを削除します。監視の一時中断などの場合は、監視テーブルを削除しません。また、システム異常などで、グループの停止する前にサーバダウンなどが発生した場合は、監視テーブルは削除されませんので、次回監視開始時に、「テーブルが存在する」 旨のアラートメッセージが表示されることがありますが、異常ではありません。

監視動作ごとに DB2 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、DB2 側の設定で適宜行ってください。

次項の 「 5.12.2. *DB2* 監視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。

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

監視テーブルの作成は以下の手順で行えます。

（以下の例は監視テーブル名を DB2WATCH とする場合）

```
sql> create table DB2WATCH (num int not null primary key)
sql> insert into DB2WATCH values(0)
sql> commit
```

5.12.2 DB2 監視リソースの監視方法

DB2 監視リソースは、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発行する 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に失敗した場合
  2. 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 文の発行により最大 10 桁の数値データの書き込みと読み込みを実行します。監視の開始時・終了時に監視テーブルの作成・削除が行われます。監視テーブルに対して発行する SQL 文は（create / update / 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に失敗した場合
  2. SQL 文の発行に対する応答で異常が通知された場合
  3. 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

5.12.3 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発行する 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発行する SQL 文は （create / update / 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 ： DB2

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。

既定値 ： db2admin

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 ： DB2WATCH

5.13 FTP 監視リソースの設定

FTP 監視リソースは、サーバ上で動作する FTP サービスを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。

5.13.1 FTP 監視リソースの注意事項

監視の対象リソースには、FTP を起動するサービスリソースやスクリプト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、接続時のメッセージなど) 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。

[プロトコル] に FTPS を選択した場合、[クラスタプロパティ] の [暗号化] タブに OpenSSL ライブラリのインストールパスを設定する必要があります。

5.13.2 FTP 監視リソースの監視方法

FTP 監視リソースは、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

5.13.3 監視 (固有) タブ

IP アドレス (255 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

5.14 HTTP 監視リソースの設定

HTTP 監視リソースは、サーバ上で動作する HTTP のサービスを監視するモニタリソースです。HTTP 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、HTTP 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。

5.14.1 HTTP 監視リソースの注意事項

監視の対象リソースには、HTTP サービスを起動するサービスリソースやスクリプト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 HTTP 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 HTTP 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、HTTP 側の設定で適宜行ってください。

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

HTTP 監視リソースのクライアント認証で監視可能な Web サーバは IIS です。

[プロトコル] に HTTP を指定している場合、HTTP 監視リソースの HTTP リクエストは、デフォルトのポート番号 (80) で発行を行います。

5.14.2 HTTP 監視リソースの監視方法

HTTP 監視リソースは、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）

5.14.3 監視 (固有) タブ

接続先 (255 バイト以内)

監視する HTTP 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 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 ： 127.0.0.1

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。

注釈: [HTTPS] を選択した場合は、リクエスト種別の選択肢のうち、どちらを選択しても、GET リクエストを発行します。

ポート番号 (1～65535)

監視する HTTP 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）
443 (HTTPS)

監視 URI (255 バイト以内)

監視する HTTP の URI を設定します。
指定しない場合は、ドキュメントルートに対して監視を行います。監視用のページを作成する必要はありません。
指定した場合は、指定した特定の URI に対して監視を行います。指定する URI は、匿名アクセスが可能な権限である必要があります。

記述は、以下のようにドキュメントルートからの URI で行います。

(例) 監視対象とする Web ページの URL が
http://WebServer:80/watch/sample.htm
の場合

```
/watch/sample.htm
```

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。

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。

既定値 ： 無効

クライアント証明書サブジェクト名 (64 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のサブジェクト名を設定します。[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。

注釈: [クライアント証明書サブジェクト名] に設定したサブジェクト名でローカルコンピューターの証明書ストアの「個人」に格納されているクライアント証明書を検索します。

既定値 ： なし

5.15 IMAP4 監視リソースの設定

IMAP4 監視リソースは、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。

5.15.1 IMAP4 監視リソースの注意事項

監視の対象リソースには、IMAP4 サーバを起動するサービスリソースやスクリプト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。

5.15.2 IMAP4 監視リソースの監視方法

IMAP4 監視リソースは、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

5.15.3 監視 (固有) タブ

IP アドレス (255 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。

5.16 ODBC 監視リソースの設定

ODBC 監視リソースは、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。

5.16.1 ODBC 監視リソースの注意事項

監視処理は、ODBC ドライバを利用しているため、あらかじめ、Windows の ODBC データソースアドミニストレータを使用して、データソースの設定を行ってください。データソースは、システムデータソースに追加します。

監視の対象リソースには、データベースを起動するサービスリソースやスクリプト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データベース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。

監視開始時に監視テーブルを作成します。グループが停止することにより監視が停止する場合に、監視テーブルを削除します。監視の一時中断などの場合は、監視テーブルを削除しません。また、システム異常などで、グループの停止する前にサーバダウンなどが発生した場合は、監視テーブルは削除されませんので、次回監視開始時に、「テーブルが存在する」 旨のアラートメッセージが表示されることがありますが、異常ではありません。

監視動作ごとにデータベー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、データベース側の設定で適宜行ってください。

次項の 「5.16.2. *ODBC* 監視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。

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

監視テーブルの作成は以下の手順で行えます。

（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);
sql> commit;
```

5.16.2 ODBC 監視リソースの監視方法

ODBC 監視リソースは、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発行する 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に失敗した場合
  2. 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 文の発行により最大 10 桁の数値データの書き込みと読み込みを実行します。監視の開始時・終了時に監視テーブルの作成・削除が行われます。監視テーブルに対して発行する SQL 文は （create / update / 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に失敗した場合
  2. SQL 文の発行に対する応答で異常が通知された場合
  3. 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

5.16.3 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発行する 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発行する SQL 文は （create / update / 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名を設定します。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。データソースの設定で、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

5.17 Oracle 監視リソースの設定

Oracle 監視リソースは、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。

5.17.1 Oracle 監視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、「5. モニタリソースの詳細」の「5.1.2. 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。

監視処理は、Oracle の OCI を利用しているため、監視を行うサーバ上に、インターフェイス用の DLL (OCI.DLL) がインストールされている必要があります。

監視の対象リソースには、Oracle を起動するサービスリソースやスクリプト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データベース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。

監視開始時に監視テーブルを作成します。グループが停止することにより監視が停止する場合に、監視テーブルを削除します。監視の一時中断などの場合は、監視テーブルを削除しません。また、システム異常などで、グループの停止する前にサーバダウンなどが発生した場合は、監視テーブルは削除されませんので、次回監視開始時に、「テーブルが存在する」旨のアラートメッセージが表示されることがありますが、異常ではありません。

パラメータの OS 認証のチェックがオフの場合、通常はパスワード認証で Oracle 監視を行いますが以下の条件の場合は OS 認証で Oracle 監視が行われ、パラメータで指定したユーザ名およびパスワードは無視されます。

- パラメータの認証方式が SYSDBA に指定されている。
- Windows OS の ora_dba グループに Administrator ユーザが所属している。

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$PROCESS への SELECT 権限／ V$INSTANCE への SELECT 権限
レベル 1(select での監視)	V$PROCESS への SELECT 権限／監視テーブルへの SELECT 権限
レベル 2(update/select での監視)	V$PROCESS への SELECT 権限／ 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

監視動作ごとに Oracle 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、Oracle 側の設定で適宜行ってください。

次項の「 5.17.2. *Oracle* 監視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。

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

監視テーブルの作成は以下の手順で行えます。

（以下の例は監視テーブル名を ORAWATCH とする場合）

```
sql> create table ORAWATCH (num int 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。

5.17.2 Oracle 監視リソースの監視方法

Oracle 監視リソースは、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 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. DB(インスタンス) のステータスが未起動状態（MOUNTED,STARTED）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発行する 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に失敗した場合
2. 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 文の発行により最大１０桁の数値データの書き込みと読み込みを実行します。監視の開始時・終了時に監視テーブルの作成・削除が行われます。監視テーブルに対して発行する SQL 文は（ create / update / 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に失敗した場合
  2. SQL 文の発行に対する応答で異常が通知された場合
  3. 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

5.17.3 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

  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 監視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。

既定値 ： リスナーとインスタンスを監視

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)

  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 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発行する 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発行する SQL 文は（ create / update / 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の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

次のページに続く

表 5.9 – 前のページからの続き

監視方式	ORACLE_HOME	接続文字列	監視レベル
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。監視方式として [リスナーのみ監視] 以外を選択している場合、および OS 認証を使用する場合は、必ず設定してください。

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

OS 認証

Oracle にログインするときの認証方式を指定します。Oracle の設定に合わせる必要があります。

- チェックボックスがオン
  OS 認証を使用します。
- チェックボックスがオフ (既定値)
  データベース認証を使用します。

認証方式

Oracle にログインするときのユーザの権限を選択します。指定したユーザ名の権限に合わせる必要があります。

- SYSDBA(既定値)
  SYSDBA 権限で接続します。
- DEFAULT
  一般ユーザ権限で接続します。

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・セットを選択します。

- (Following the setting of the application) (既定値)

  サーバにインストールされた Oracle のキャラクタセットを使用します。

- AMERICAN_AMERICA.US7ASCII

  Oracle の言語が日本語および英語以外の場合、AMERICAN_AMERICA.US7ASCII を選択してください。

障害発生時にアプリケーションの詳細情報を採取する

Oracle データベースの異常を検出した場合に Oracle の詳細情報を採取するかどうかを指定します。

- チェックボックスがオン

  Oracle の詳細情報を採取します。

- チェックボックスがオフ (既定値)

  Oracle の詳細情報を採取しません。

  この機能を使用する場合、情報採取のためのデータベース処理をローカル システム アカウントで実行するため、ローカル システム アカウントに DBA 権限が必要です。採取した情報は CLUSTERPRO インストールフォルダ配下の `work\rm\リソース名\errinfo.cur` フォルダに保存されます。採取が複数回実行された場合は、過去の採取情報のフォルダ名が errinfo.1、errinfo.2 とリネームされ、最大 5 世代分まで保存されます。

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。

採取中はグループ停止など手動での操作は行わないでください。手動での操作を行うタイミングによっては、その後の監視処理が正常に動作しない可能性があります。

採取タイムアウト (1～9999)

詳細情報採取時のタイムアウト時間を秒単位で指定します。

既定値：120

Oracle の初期化中またはシャットダウン中をエラーにする

本機能をオンにした場合、Oracle の初期化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 が運用中に自動で再起動される場合、本機能
をオフにしてください。Oracle の初期化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 の初期化またはシャットダウン中の状態が続くと監視エラーになります。

既定値：オフ

5.18 POP3 監視リソースの設定

POP3 監視リソースは、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。

5.18.1 POP3 監視リソースの注意事項

監視の対象リソースには、POP3 サーバを起動するサービスリソースやスクリプト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。

[認証方式] に POP3S を選択した場合、[クラスタプロパティ] の [暗号化] タブに OpenSSL ライブラリのインストールパスを設定する必要があります。

5.18.2 POP3 監視リソースの監視方法

POP3 監視リソースは、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

5.18.3 監視 (固有) タブ

IP アドレス（255 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。

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

5.19 PostgreSQL 監視リソースの設定

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

5.19.1 PostgreSQL 監視リソースの注意事項

動作確認済みの PostgreSQL/PowerGres のバージョンについては、「5. モニタリソースの詳細」の「5.1.2. 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。

監視処理は、PostgreSQL/PowerGres のライブラリを利用しているため、監視を行うサーバ上に、インターフェイス用の DLL(LIBPQ.DLL) がインストールされている必要があります。PostgreSQL の監視を行う際は、この DLL のパスを環境変数に設定してください。

監視の対象リソースには、PostgreSQL/PowerGres を起動するサービスリソースやスクリプト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データベース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。

監視開始時に監視テーブルを作成します。グループが停止することにより監視が停止する場合に、監視テーブルを削除します。監視の一時中断などの場合は、監視テーブルを削除しません。また、システム異常などで、グループの停止する前にサーバダウンなどが発生した場合は、監視テーブルは削除されませんので、次回監視開始時に、「テーブルが存在する」旨のアラートメッセージが表示されることがありますが、異常ではありません。

監視動作ごとに PostgreSQL/PowerGres 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、PostgreSQL/PowerGres 側の設定で適宜行ってください。

PostgreSQL は、オープンソースソフトウェア (OSS) のため、動作確認はしますが、動作保証はしません。各自で評価を行った後、運用してください。

OS 及び PostgreSQL のバージョンによっては、PostgreSQL 監視を行うと、ライブラリが見つからないエラーが出力されることがあります。この場合は、システム環境変数の PATH に PostgreSQL の bin を追加してください。その後、クラスタ再起動を行ってください。

環境変数に PATH を追加する場合（以下は PostgreSQL9.6 の bin の PATH の例）

```
C:\Program Files\PostgreSQL\9.6\bin
```

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␣
```

(次のページに続く)

(前のページからの続き)

```
↪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 監視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。

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

監視テーブルの作成は以下の手順で行えます。

(以下の例は監視テーブル名を PSQLWATCH とする場合)

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

5.19.2 PostgreSQL 監視リソースの監視方法

PostgreSQL 監視リソースは、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発行する 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に失敗した場合

2. 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 文の発行により最大 10 桁の数値データの書き込みと読み込みを実行します。監視の開始時・終了時に監視テーブルの作成・削除が行われます。監視テーブルに対して発行する SQL 文は（ create / update / 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に失敗した場合
  2. SQL 文の発行に対する応答で異常が通知された場合
  3. 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

5.19.3 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発行する 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発行する SQL 文は（ create / update / 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

監視するデータベースサーバの 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

監視する PostgreSQL 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。

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

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

5.20 SMTP 監視リソースの設定

SMTP 監視リソースは、サーバ上で動作する SMTP のサービスを監視するモニタリソースです。SMTP 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、SMTP 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。

5.20.1 SMTP 監視リソースの注意事項

監視の対象リソースには、SMTP を起動するサービスリソースやスクリプト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データベース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 SMTP 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、SMTP 側の設定で適宜行ってください。

5.20.2 SMTP 監視リソースの監視方法

SMTP 監視リソースは、以下の監視を行います。

SMTP 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. SMTP 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

5.20.3 監視 (固有) タブ

IP アドレス

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

監視する SMTP 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

ユーザ名 (255 バイト以内)

SMTP にログインする際のユーザ名を設定します。ユーザ名が指定されていない場合は、SMTP 認証を行いません。

既定値 ： なし

パスワード (255 バイト以内)

SMTP 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

SMTP 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 SMTP の設定に合わせる必要があります。

- CRAM-MD5(既定値)

  CRAM-MD5 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。

メールアドレス (255 バイト以内)

監視する際のメールアドレスを設定します。

指定しない場合は、動作確認コマンドのみで監視を行います。内部では、ダミーのメールアドレスを使用したコマンドを実行します。

指定した場合は、指定したメールアドレスに対して SMTP コマンドを実行し、その結果を確認することによって監視を行います。指定する場合は、監視専用のメールアドレスを用意することを推奨します。

既定値 ： なし

5.21 SQL Server 監視リソースの設定

SQL Server 監視リソースは、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。

5.21.1 SQL Server 監視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、「5. モニタリソースの詳細」の「5.1.2. 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。

監視の対象リソースには、SQL Server を起動するサービスリソースやスクリプト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データベース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。

監視開始時に監視テーブルを作成します。グループが停止することにより監視が停止する場合に、監視テーブルを削除します。監視の一時中断などの場合は、監視テーブルを削除しません。また、システム異常などで、グループの停止する前にサーバダウンなどが発生した場合は、監視テーブルは削除されませんので、次回監視開始時に、「テーブルが存在する」旨のアラートメッセージが表示されることがありますが、異常ではありません。

監視動作ごとに SQL Server 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、SQL Server 側の設定で適宜行ってください。

次項の「 5.21.2. *SQL Server* 監視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。

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

監視テーブルの作成は以下の手順で行えます。

（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
```

5.21.2 SQL Server 監視リソースの監視方法

SQL Server 監視リソースは、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発行する 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に失敗した場合
  2. 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 文の発行により最大 10 桁の数値データの書き込みと読み込みを実行します。監視の開始時・終了時に監視テーブルの作成・削除が行われます。監視テーブルに対して発行する SQL 文は（ create / update / 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に失敗した場合
  2. SQL 文の発行に対する応答で異常が通知された場合

3. 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

5.21.3 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発行する 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発行する SQL 文は（ create / update / 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 ： MSSQLSERVER

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。ユーザ名を指定しなかった場合は、Windows 認証として動作します。

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)

[スタート] メニュー → [管理ツール] → [データ ソース (ODBC)] の [ドライバ] タブに表示される対象データベースのドライバ名を設定します。

SQL Server 2014 の場合は SQL Server Native Client 11.0

SQL Server 2016、SQL Server 2017 の場合は ODBC Driver 13 for SQL Server

SQL Server 2019 の場合は ODBC Driver 17 for SQL Server

を選択、または直接入力してください。

既定値 ： ODBC Driver 13 for SQL Server

5.22 Tuxedo 監視リソースの設定

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

5.22.1 Tuxedo 監視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、「5. モニタリソースの詳細」の「5.1.2. 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。

監視の対象リソースには、Tuxedo を起動するスクリプトリソース、アプリケーションリソース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 Tuxedo 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 Tuxedo 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、Tuxedo 側の設定で適宜行ってください。

5.22.2 Tuxedo 監視リソースの監視方法

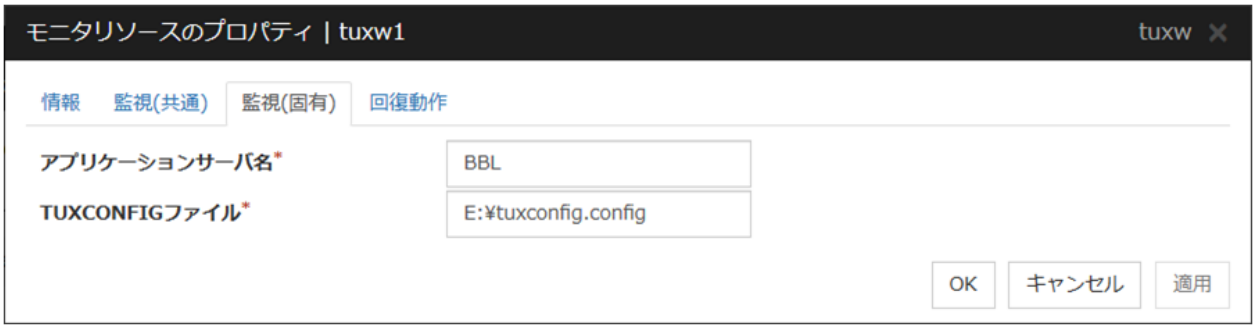
Tuxedo 監視リソースは、以下の監視を行います。

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

5.22.3 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

5.23 WebLogic 監視リソースの設定

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

5.23.1 WebLogic 監視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、「5. モニタリソースの詳細」の「5.1.2. 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。

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 を起動するスクリプトリソース、アプリケーションリソースを指定)。

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。

監視動作ごとに WebLogic 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、WebLogic 側の設定で適宜行ってください。

5.23.2 WebLogic 監視リソースの監視方法

WebLogic 監視リソースは、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

5.23.3 監視 (固有) タブ

IP アドレス (80 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

インストールパス (255 バイト以内)

WebLogic 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 ： `C:\Oracle\Middleware\Oracle_Home\wlserver`

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

5.24 WebOTX 監視リソースの設定

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

5.24.1 WebOTX 監視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、「5. モニタリソースの詳細」の「5.1.2. 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。

監視の対象リソースには、WebOTX を起動するサービスリソースやスクリプト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 WebOTX 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。

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。

監視動作ごとに WebOTX 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、WebOTX 側の設定で適宜行ってください。

WebOTX 監視リソースは WebOTX が提供する otxadmin.bat コマンドを利用して、アプリケーションサーバの監視を行います。WebOTX V10.1 以降では otxadmin.bat コマンドが配置されている `${AS_INSTALL}\bin` が環境変数 PATH に含まれなくなりました。WebOTX V10.1 以降を監視する場合は、以下のいずれかの設定をしてください。

- システム環境変数 PATH に [otxadmin.bat] コマンドが配置されているパスを追加。
- [インストールパス] に WebOTX Application Server のインストールパスを設定 (例. `C:\WebOTX`)。

5.24.2 WebOTX 監視リソースの監視方法

WebOTX 監視リソースは、以下の監視を行います。

WebOTX の otxadmin.bat 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

5.24.3 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 (255 バイト以内)

WebOTX Application Server のインストールパスを設定します。WebOTX Application Server V10.1 以降を監視する場合は必ず設定してください。

既定値 ： なし

5.25 WebSphere 監視リソースの設定

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

5.25.1 WebSphere 監視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、「5. モニタリソースの詳細」の「5.1.2. 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。

監視の対象リソースには、WebSphere を起動するサービスリソースやスクリプト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 WebSphere 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。

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。

監視動作ごとに WebSphere 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、WebSphere 側の設定で適宜行ってください。

5.25.2 WebSphere 監視リソースの監視方法

WebSphere 監視リソースは、以下の監視を行います。

WebSphere の serverStatus.bat 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

5.25.3 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)

WebSphere 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 (255 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 ： `C:\Program Files\IBM\WebSphere\AppServer`

5.26 JVM 監視リソースの設定

JVM 監視リソースは、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。

5.26.1 JVM 監視リソースの注意事項

JVM 監視 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 監視リソースの活性後、Java Resource Agent は監視を開始しますが、JVM 監視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。

JVM 監視リソースの監視開始から、実際に監視処理を行うまでの間、JVM 監視リソースのステータスは"警告"になります。

5.26.2 JVM 監視リソースの監視方法

JVM 監視リソースは、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 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 監視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イベントログや 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イベントログや JVM 運用ログへ通知します。

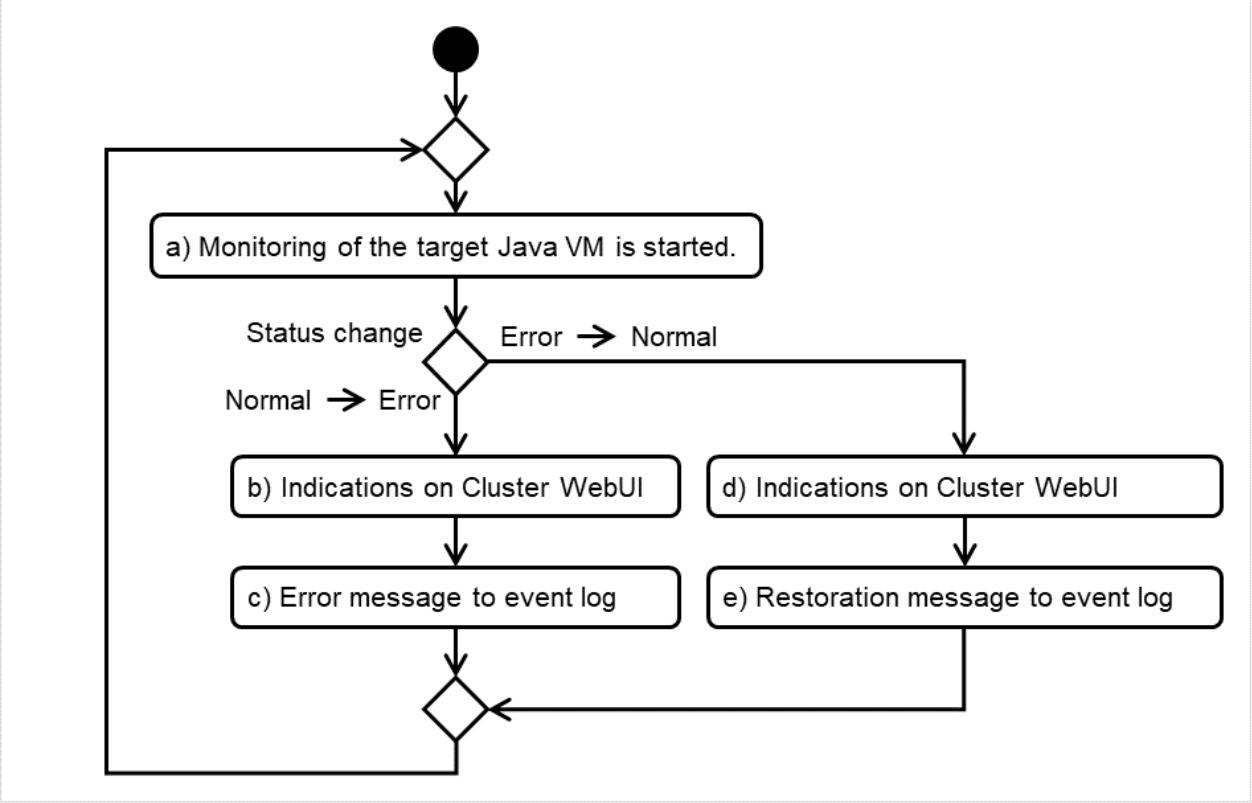


図 5.5　JVM 監視リソースによる監視フロー

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。

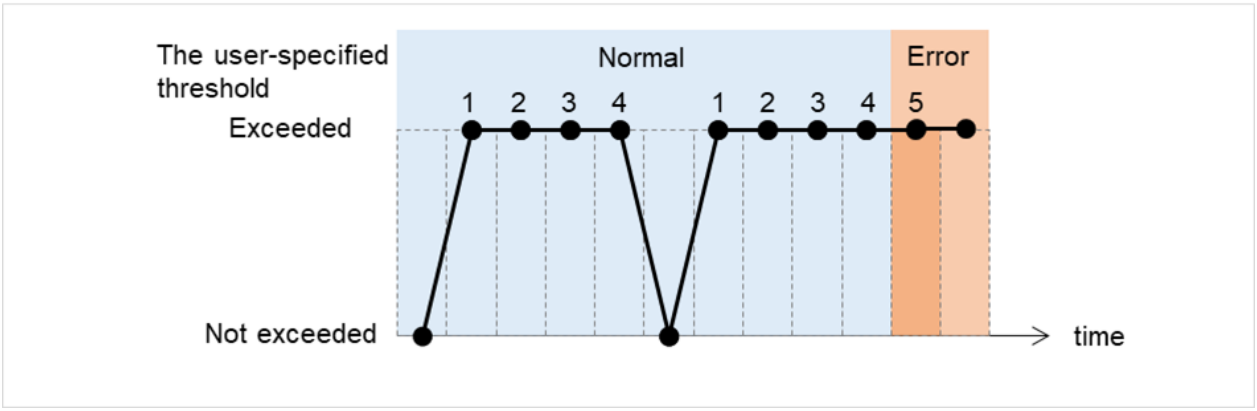


図 5.6　しきい値超過時の動作

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。

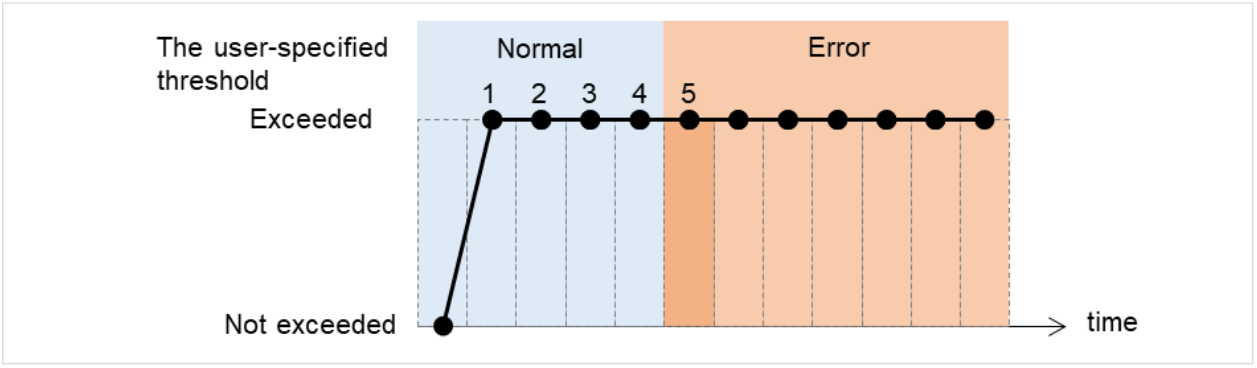


図 5.7　異常継続時の動作

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。

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 監視リソースは、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。

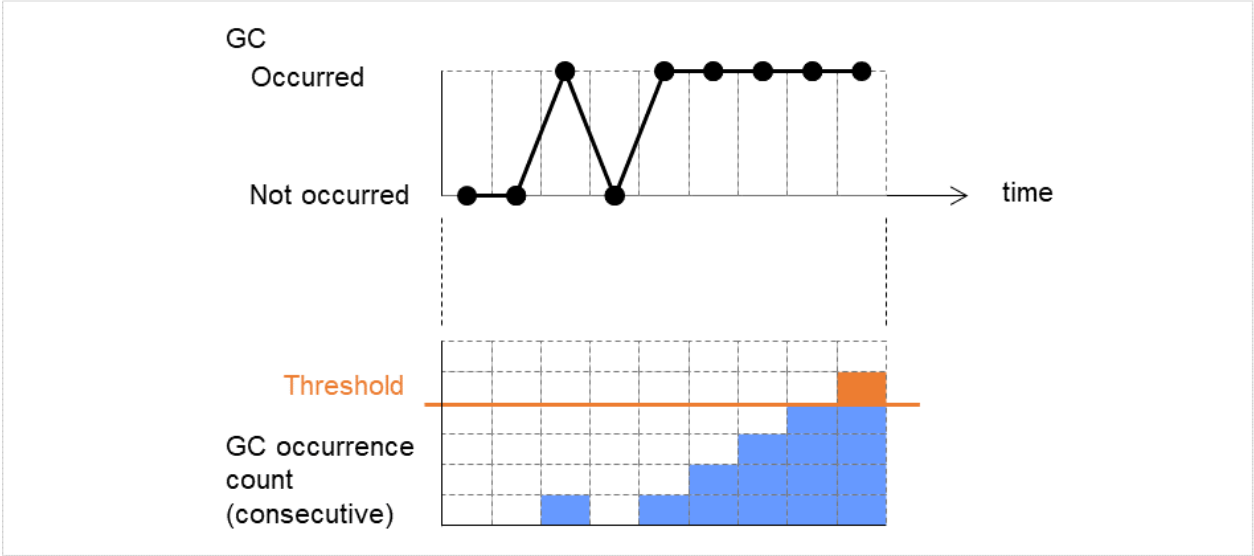


図 5.8　監視イメージ（異常判定しきい値を 5 回に設定した場合）

5.26.3 JVM 統計ログとは

JVM 監視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 監視リソースの [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
[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 の両方を出力します。一方のみ出力する設定は提供しておりません。	wlworkmanager.stat wlthreadpool.stat

5.26.4 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。

次のページに続く

表 5.13 – 前のページからの続き

No	フォーマット	説明
2	半角英数字記号	監視対象 Java VM の名称を示します。JVM 監視リソースの [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「5.26.9. *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
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 5.13 – 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 5.13 – 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。

5.26.5 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 監視リソースの [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 5.14 – 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

5.26.6 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 監視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 監視リソースでは、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 監視リソースの [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)
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 監視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 監視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。

5.26.7 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 監視リソースの [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。

5.26.8 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 監視リソースの [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。

5.26.9 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 監視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 監視リソースの [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 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

次のページに続く

表 5.19 – 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]-[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、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
[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

次のページに続く

表 5.21 – 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]-[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、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]	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
[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

次のページに続く

表 5.23 – 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]-[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)
[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 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

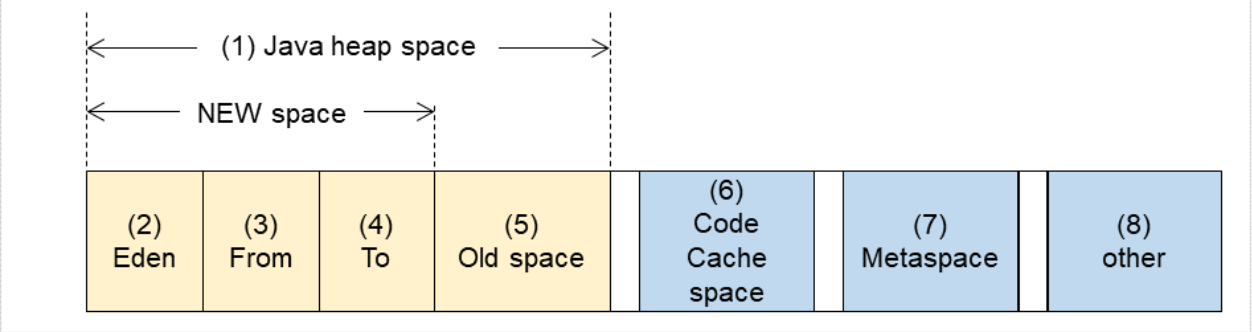


図 5.9　Java VM メモリ空間（Oracle Java 8/Oracle Java 9/Oracle Java 11/Oracle Java 17/Oracle Java 21）

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
(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)

次のページに続く

表 5.25 – 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
(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

5.26.10 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 監視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]
・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]

次のページに続く

表 5.26 – 前のページからの続き

障害原因	設定項目
・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「5.26.9. *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 Java(usage monitoring) 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
[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

次のページに続く

表 5.27 – 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]-[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
[メモリ] タブ- [非ヒープ使用率を監視する]-[Perm Gen] (Oracle Java の場合)	PermGen PSPermGen CMSPermGen

次のページに続く

表 5.27 – 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]-[Perm Gen[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]-[Perm Gen[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
[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

次のページに続く

表 5.27 – 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
[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]	\Program Files\bin\command.bat
[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
[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 監視リソースは、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、「\Program Files\bin\command.bat 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]	"\Program Files\bin\command.bat" 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 監視リソースは、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、「"\Program Files\bin\command.bat" 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]	"\Program Files\bin\command.bat" 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 監視リソースは、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、「\Program Files\bin\command.bat 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]

5.26.11 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。

本書では、JVM 監視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。
3. 監視対象のサーバのコンフィグレーション－全般で「リスニング・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 の起動スクリプトを開きます。
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

```
set 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。

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「リスニング・ポート」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。

   - 監視対象が WebLogic Server の管理対象サーバの場合

```
if "%SERVER_NAME%" == "SERVER_NAME"(
    set 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
)
```

※ 上記で if 文の中は実際には 1 行で記述してください。

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%
-Dweblogic.Name=%SERVER_NAME%
-Djava.security.policy=%WL_HOME%\server\lib\weblogic.policy %JAVA_OPTIONS
% %PROXY_SETTINGS% %SERVER_CLASS%
```

※ 上記内容は実際には 1 行で記述してください

---

7. 監視対象の WebLogic Server の WLST(wlst.cmd) を起動します。

   起動方法は [スタート] メニューの [Oracle WebLogic]-[WebLogic Server <**バージョン番号**>]-[Tools]-[WebLogic Scripting Tool] を選択します。

8. 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.cmd) を起動します。

   起動方法は [スタート] メニューの [Oracle WebLogic]-[WebLogic Server <**バージョン番号**>]-[Tools]-[WebLogic Scripting Tool] を選択します。

   表示されたプロンプト画面上で、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。

9. 監視対象の WebLogic Server を再起動します

5.26.12 WebOTX を監視するには

本書では、JVM 監視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 版統合運用管理コンソール）」マニュアルの「コンソールの実行」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。

5.26.13 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。

5.26.14 WebOTX プロセスグループの Java プロセスを監視するには

1. 統合運用管理コンソ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 [JavaVM 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
```

(次のページに続く)

(前のページからの続き)

```
-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 統合運用管理コンソールの [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。

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 監視リソースに対して以下のように設定してください。

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

5.26.15 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 監視リソースはその 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

5.26.16 Tomcat を監視するには

JVM 監視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 を停止し、[スタート]-(Tomcat のプログラムフォルダ)-[Configure Tomcat] を開きます。
2. 開いたウィンドウの [Java] タブの「Java Options」に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。

```
-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 監視 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。

5.26.17 SVF を監視するには

JVM 監視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。

1. 監視対象を下記より選択し、該当するファイルをエディタから開きます。

監視対象	編集するファイル
UCX Server Service(9.x 以降の場合)	<SVF インストールパス>\launcher\UCXServer.run

次のページに続く

表 5.33 – 前のページからの続き

監視対象	編集するファイル
Report Director EnterpriseServer	<SVF インストールパス>\launcher\ReportDirectorEnterpriseServer.run
Report Director Svf Server	<SVF インストールパス>\launcher\ReportDirectorSvfServer.run
Report Director Spool Balancer	<SVF インストールパス>\launcher\ReportDirectorSpoolBalancer.run
Tomcat	%FIT_PRODUCTS_BASE%\SetupUtils\setup_tomcat.bat
SVF Print Spooler services	<SVF インストールパス>\svfjpd\launcher\SpoolerDaemon.run

2. (監視対象が Tomcat の場合)

   setup_tomcat.bat 内の :install の --JvmOption の箇所に、以下のように追記します。**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。

   変更前：

```
--JvmOptions=...
```

   変更後：

```
--JvmOptions=...;-Dcom.sun.management.jmxremote.port=n;-Dcom.sun.management.
↪jmxremote.ssl=false;-Dcom.sun.management.jmxremote.authenticate=false
```

3. (監視対象が Tomcat 以外の場合)Arguments を指定している箇所に下記の内容を「-Xms」の設定箇所直後に挿入します。**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
```

5.26.18 自製の Java アプリケーションを監視するには

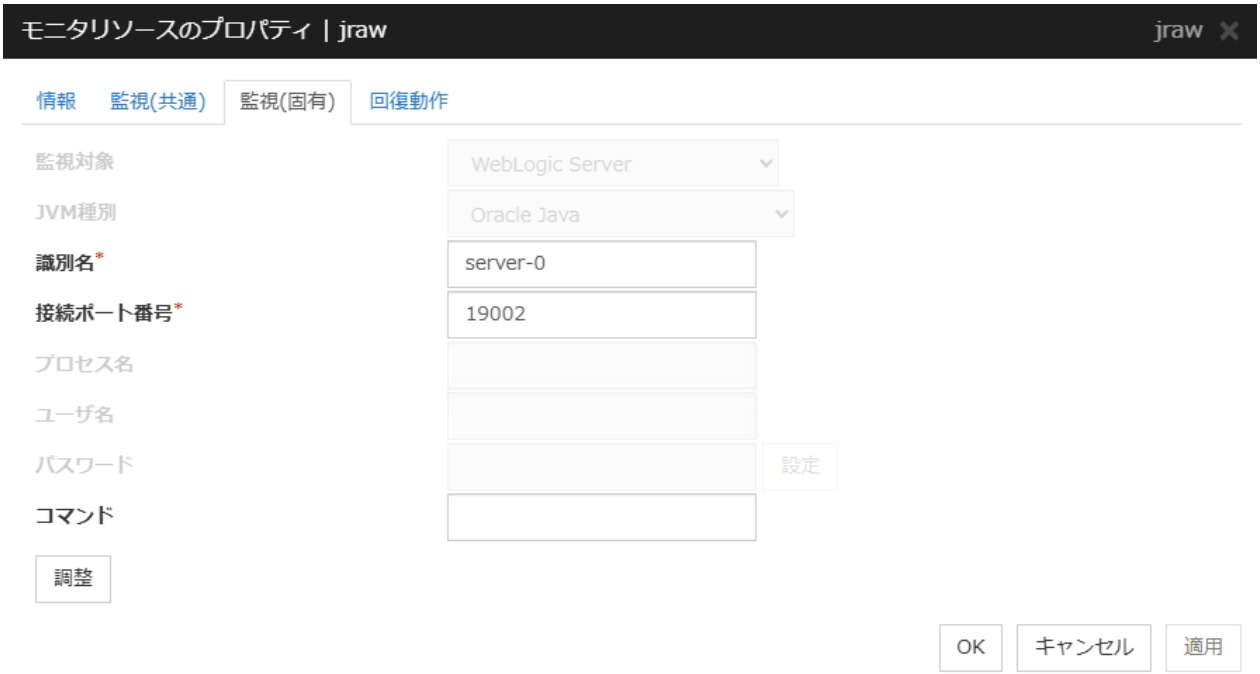
JVM 監視リソースで監視する対象の Java アプリケーションの設定手順について記述します。監視対象の Java アプリケーションが停止した状態で、Java アプリケーションの起動時オプションに次の Java オプションを 1 行で指定します。**n** は、監視のために使用するポート番号を指定します。同一のマシンに複数の監視対象の Java VM が存在する場合、重複しないポート番号を指定してください。ここで指定するポート番号は、Cluster WebUI([モニタリソースのプロパティ]→[監視 (固有)] タブ →[接続ポート番号]) でも設定します。

```
-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>
```

5.26.19 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。

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 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。

既定値 ： なし

識別名 (255 バイト以内)

識別名とは、JVM 監視の JVM 運用ログに監視対象の情報を出力する際に、別の JVM 監視リソースと識別するために設定します。そのため、JVM 監視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
  「5.26.11. *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「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「Tomcat」の場合

  「 5.26.16. *Tomcat* を監視するには 」の 4 を参照して設定してください。

- 監視対象が「WebSAM SVF」の場合

  「 5.26.17. *SVF* を監視するには 」の 4 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 監視リソースが、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 監視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 監視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「 5.26.11. *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

  「 5.26.14. *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「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「Tomcat」の場合

  「 5.26.16. *Tomcat* を監視するには 」の 2 を参照して設定してください。

- 監視対象が「WebSAM SVF」の場合

  「 5.26.17. *SVF* を監視するには 」の 2 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 (255 バイト以内)

[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 11.35 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 12.00 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。

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、"(WebOTX インストールパス)\<**ドメイン名**>.properties"の"domain.admin.user"の値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)

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、"(WebOTX インストールパス)\<**ドメイン名**>.properties"の"domain.admin.passwd"の値を設定してください。

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) `"\Program Files\bin\command.bat" 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。

「 5.26.10. **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。

5.26.20 メモリタブ ([JVM 種別] で [Oracle Java] 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。監視対象 Java VM の 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。監視対象 Java VM の 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。監視対象 Java VM の 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) `"\Program Files\bin\command.bat" 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。

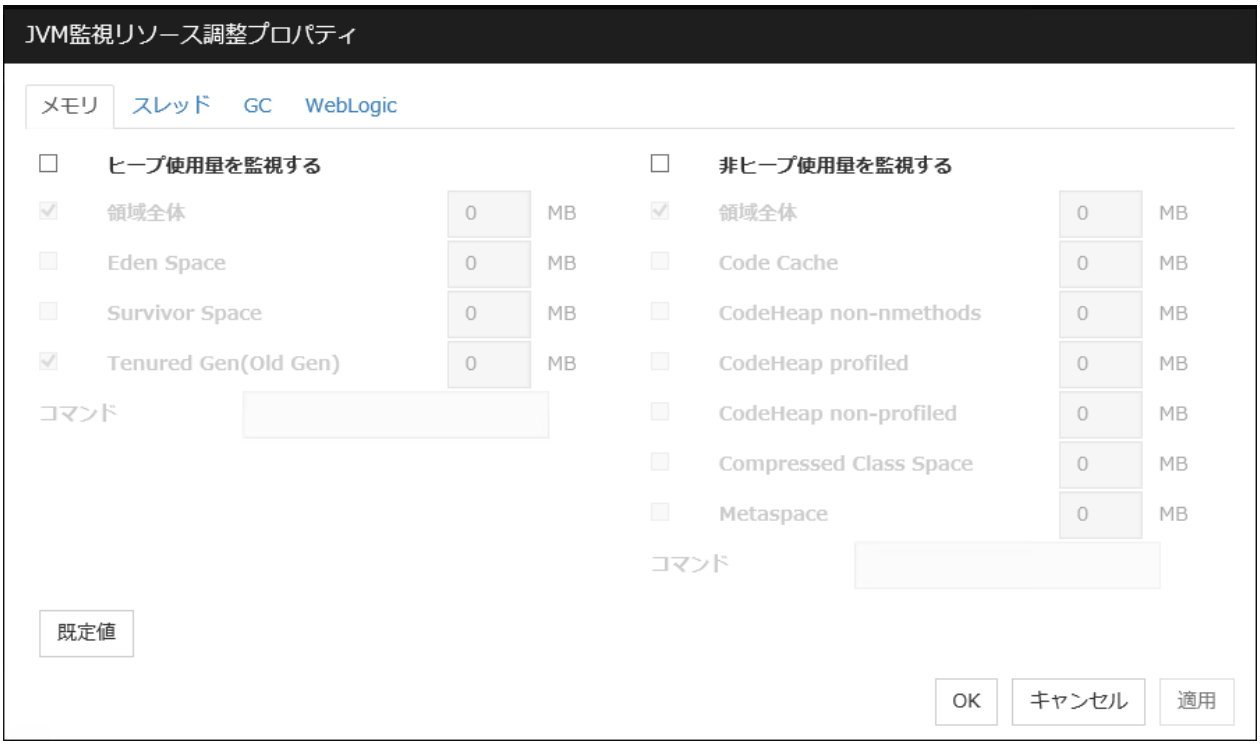
「 5.26.10. 異常検出時に障害原因別にコマンドを実行するには 」も参照してください。

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。

5.26.21 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。監視対象 Java VM の 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。監視対象 Java VM の 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。監視対象 Java VM の 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。

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) `"\Program Files\bin\command.bat" 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。

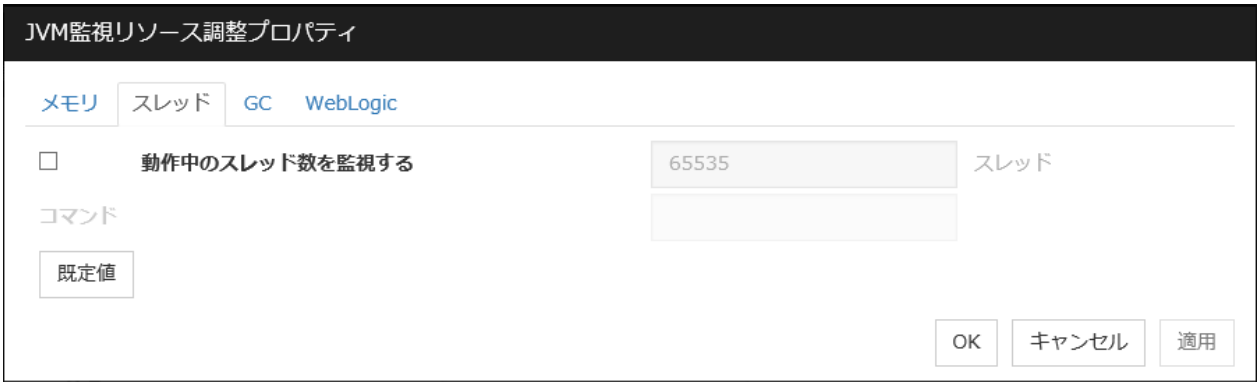
「 5.26.10. 異常検出時に障害原因別にコマンドを実行するには 」も参照してください。

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。

5.26.22 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) `"\Program Files\bin\command.bat" 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。

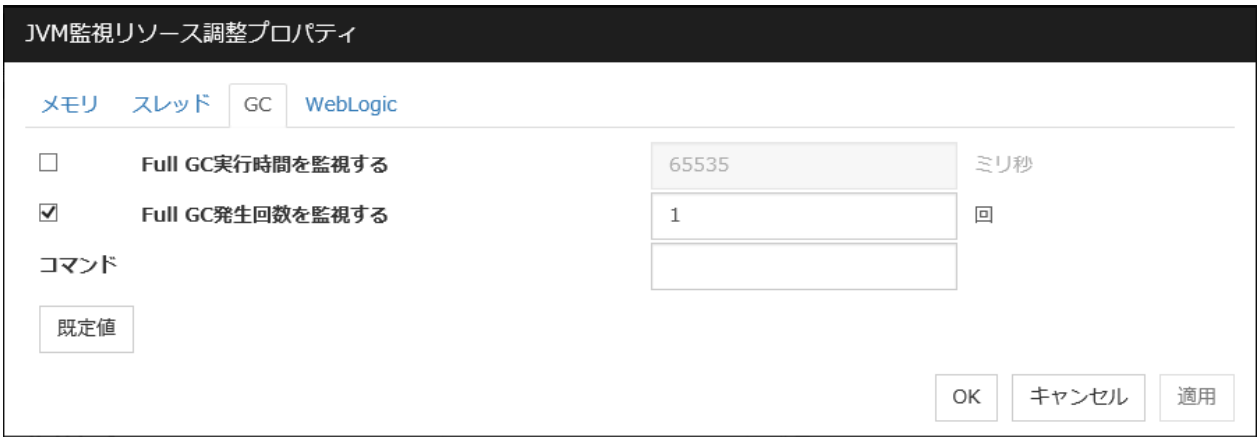
「 5.26.10. 異常検出時に障害原因別にコマンドを実行するには 」も参照してください。

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。

5.26.23 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) `"\Program Files\bin\command.bat" 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。

「 5.26.10. 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。

5.26.24 WebLogic タブ

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 (255 バイト以内)

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[*WM*1,*WM*2,…];*App*2[*WM*1,*WM*2,…];…

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 (WebLogic Server 内部で処理待ちとなっている HTTP リクエスト数)、実行リクエスト数 (WebLogic Server 内部で単位時間当たり実行した HTTP リクエスト数) 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。

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) `"\Program Files\bin\command.bat" 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。

「 5.26.10. 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。

5.27 システム監視リソースの設定

システム監視リソースは、システムリソースを監視するモニタリソースです。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。

5.27.1 システム監視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、リソース監視異常を検出できないことがあります。

- システムリソースがしきい値をはさんで増減を繰り返している場合

システムが高負荷な場合などでは、統計情報収集に時間がかかり統計情報収集間隔での情報収集ができない場合があります。

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 1 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際、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、[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。

[総仮想メモリ使用量の監視] チェックボックスをオンにすると、物理メモリを除いたスワップ領域の使用量の監視が有効になります。

ディスクリソース監視機能は、固定ディスク以外は監視対象外です。

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 26 台です。

モニタリソースの定義画面のタイプ欄に「システム監視」が表示されない場合は、[ライセンス情報取得] を選択し、ライセンス情報を取得してください。

システム監視リソースの監視開始から、実際に監視処理を行うまでの間、システム監視リソースのステータスは "警告" になります。

システム監視リソース、プロセスリソース監視リソースの登録数が多い場合は、下記メッセージがアラートログに出力され異常を検出する場合があります。
本メッセージが出力された場合は [監視 (共通)] タブからタイムアウトの設定を見直してください。

```
監視 sraw は異常を検出しました。(99 : monitor was timeout)
```

5.27.2 システム監視リソースの監視方法

システム監視リソースは、以下の監視を行います。
システムおよびディスクのシステム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

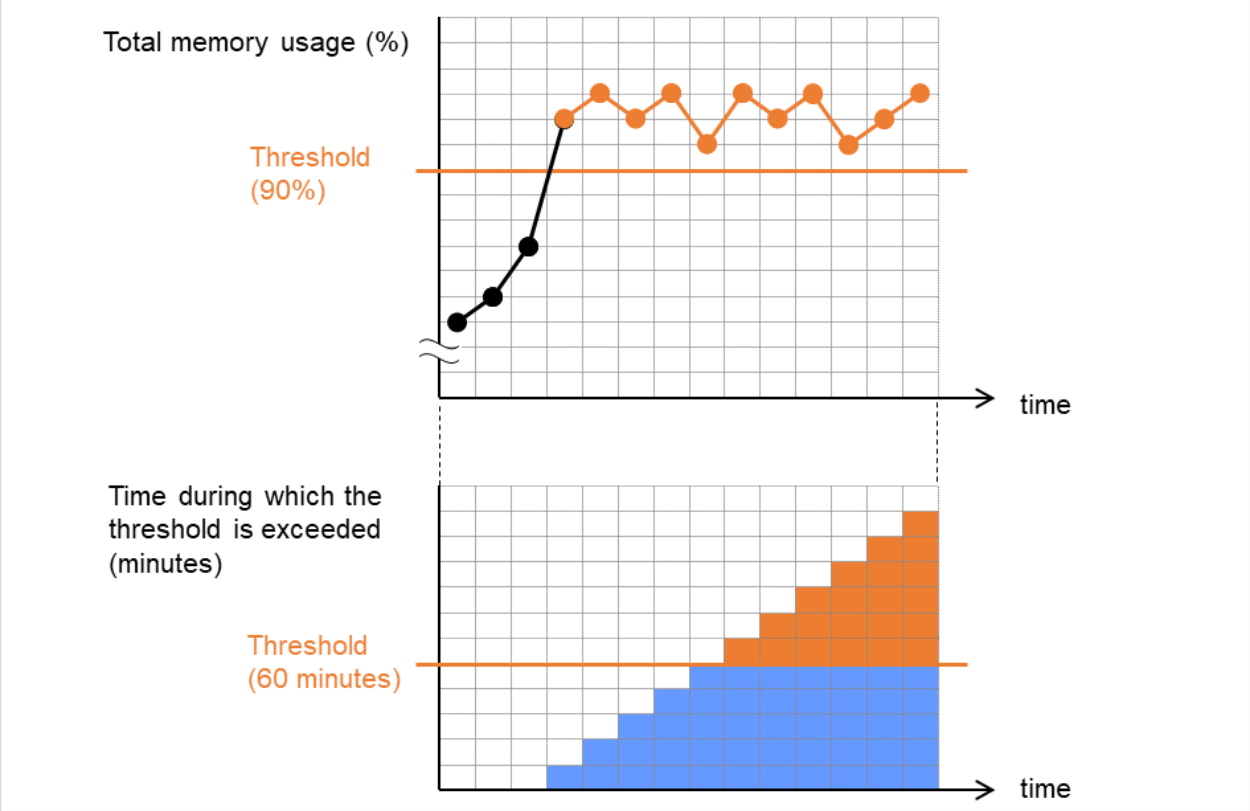


図 5.10　総メモリ使用量のしきい値以上の状態が一定時間続いた場合（異常検出する）

- 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。

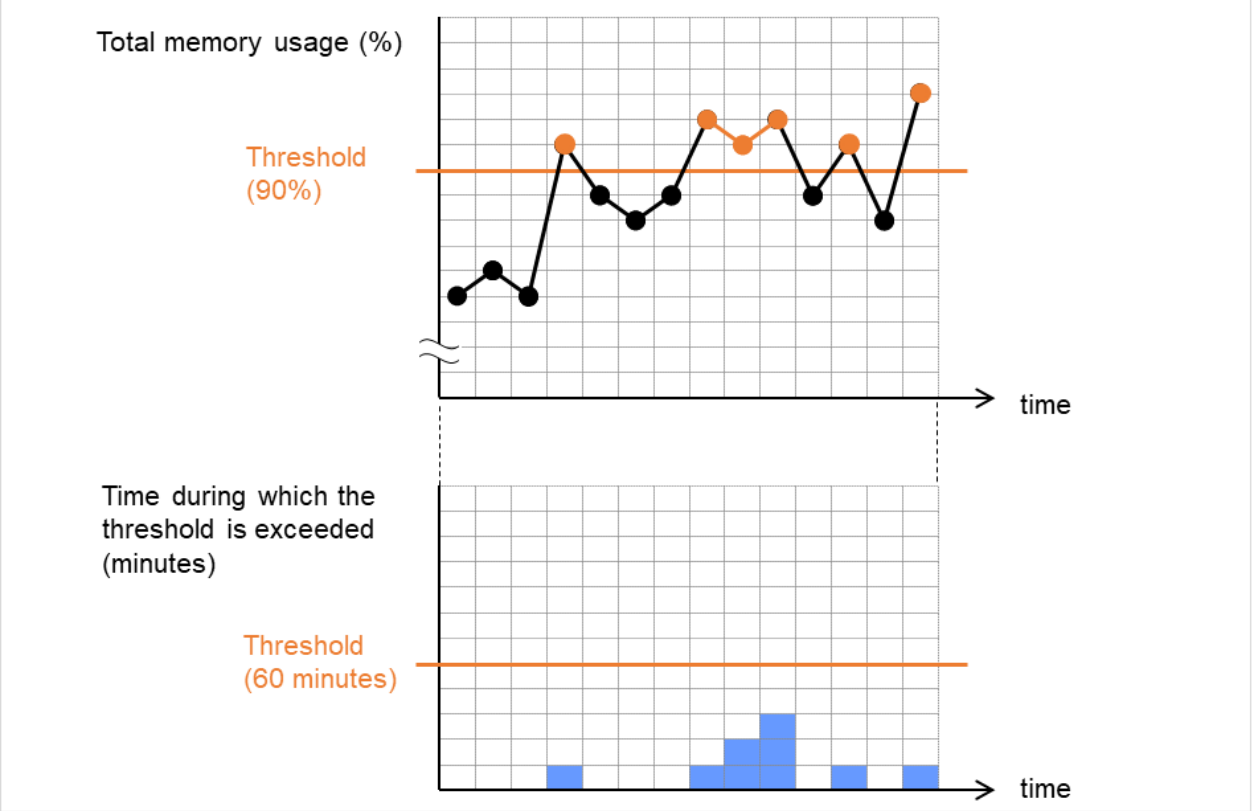


図 5.11　総メモリ使用量のしきい値以上の状態が一定時間続かない場合（異常検出しない）

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

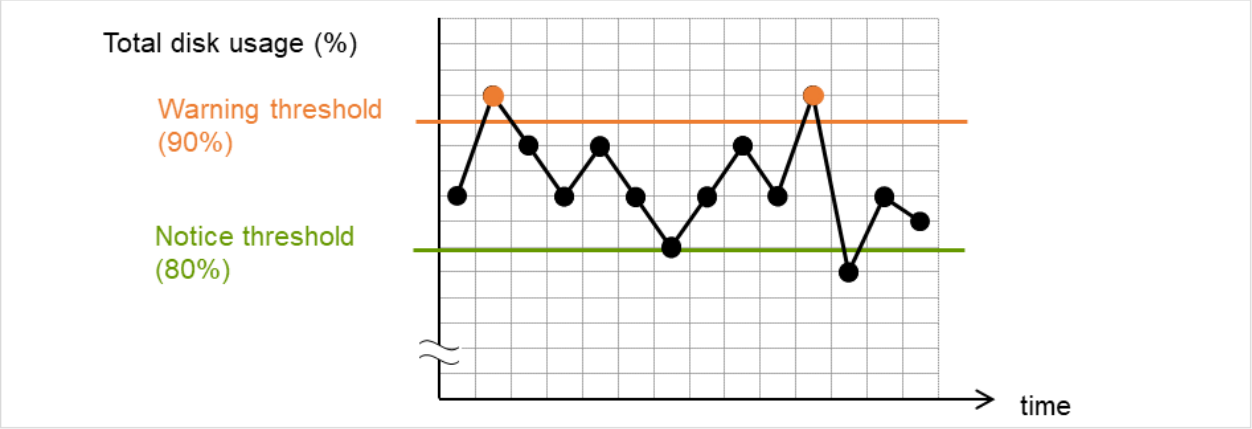


図 5.12　ディスク使用率が警告レベル上限値以上になった場合（異常検出する）

- 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。

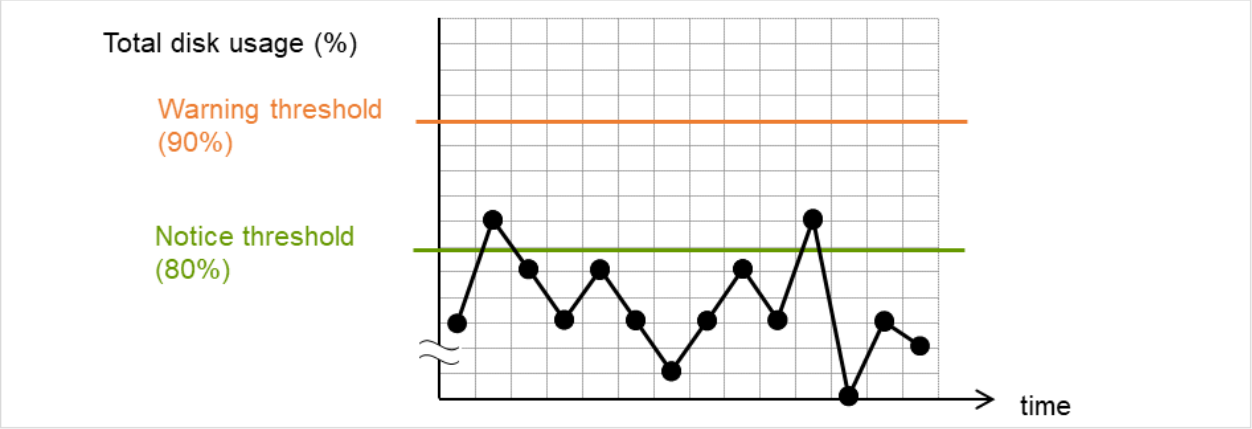


図 5.13　ディスク使用率が警告レベル上限値以上にならない場合（異常検出しない）

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。

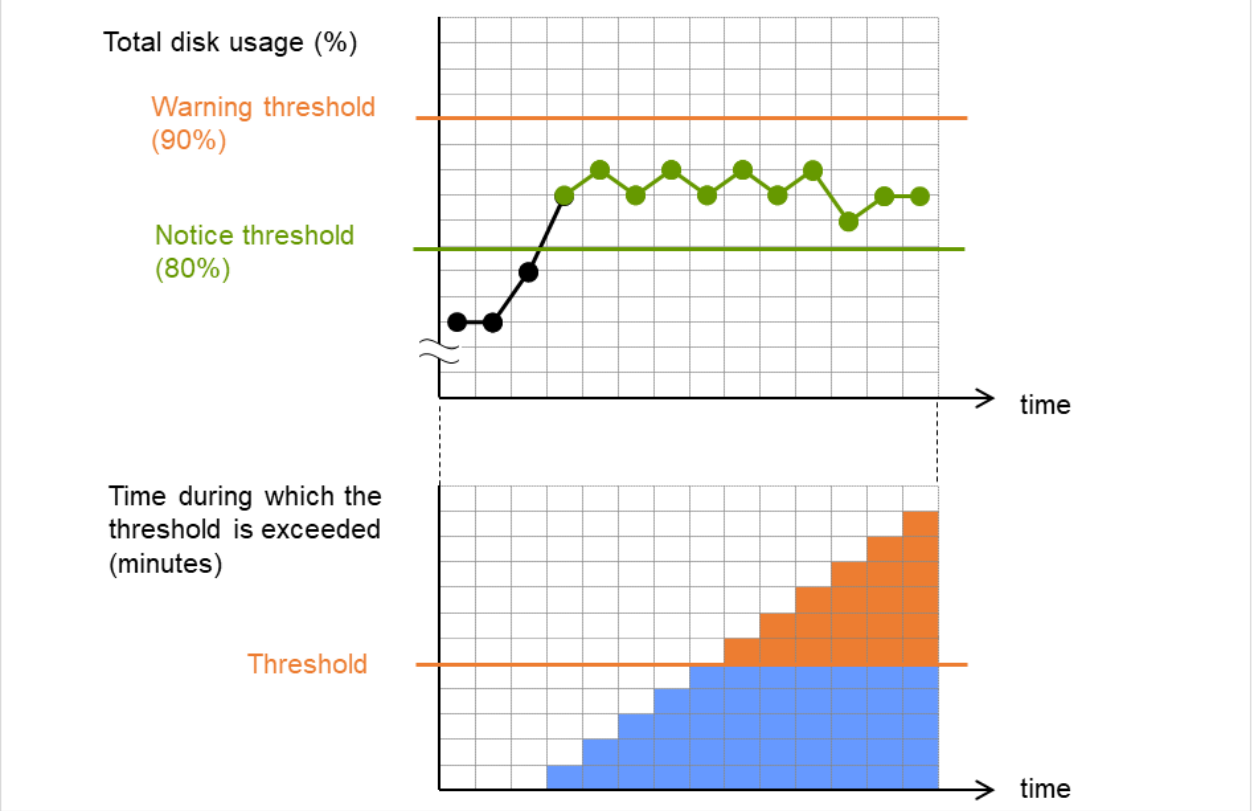


図 5.14　ディスク使用率において、通知レベル上限値以上の状態が一定時間続いた場合（異常検出する）

- 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。

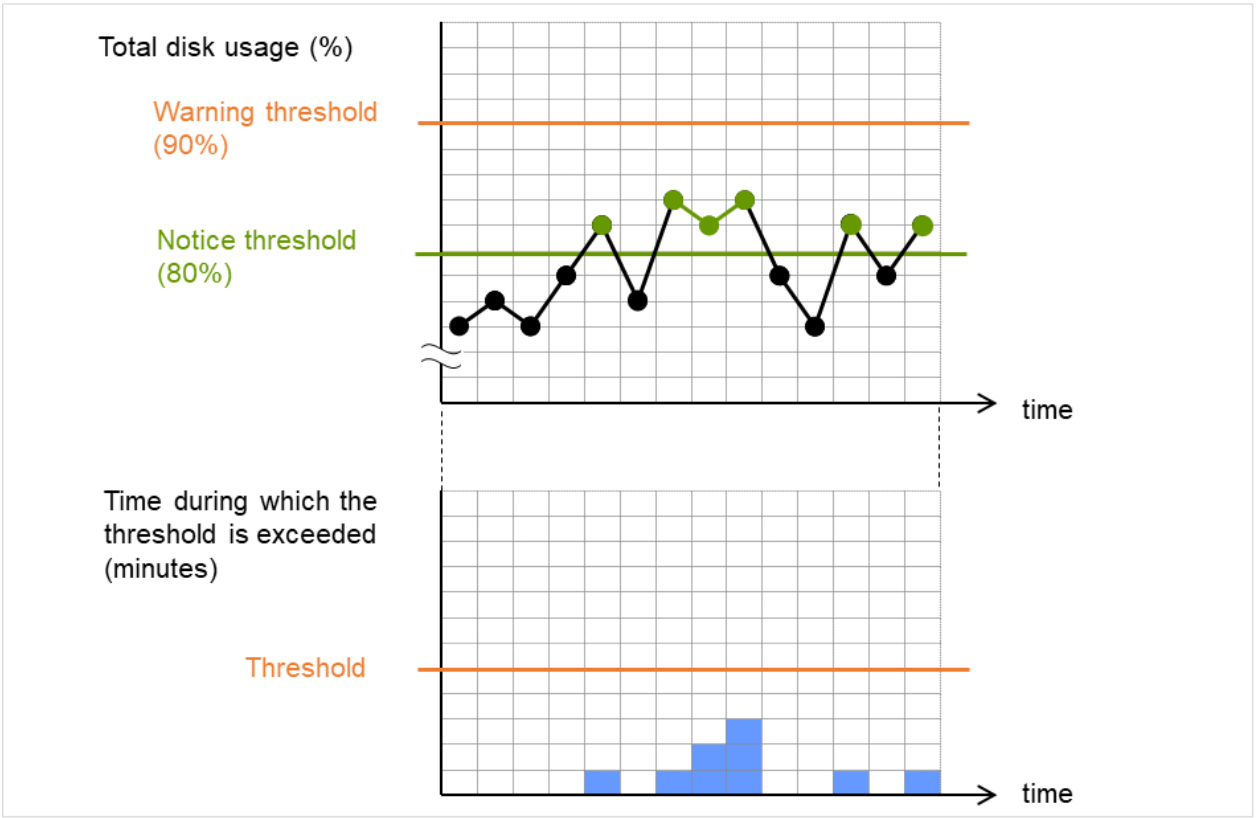


図 5.15　ディスク使用率において、通知レベル上限値以上の状態が一定時間続かない場合（異常検出しない）

5.27.3 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。

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。

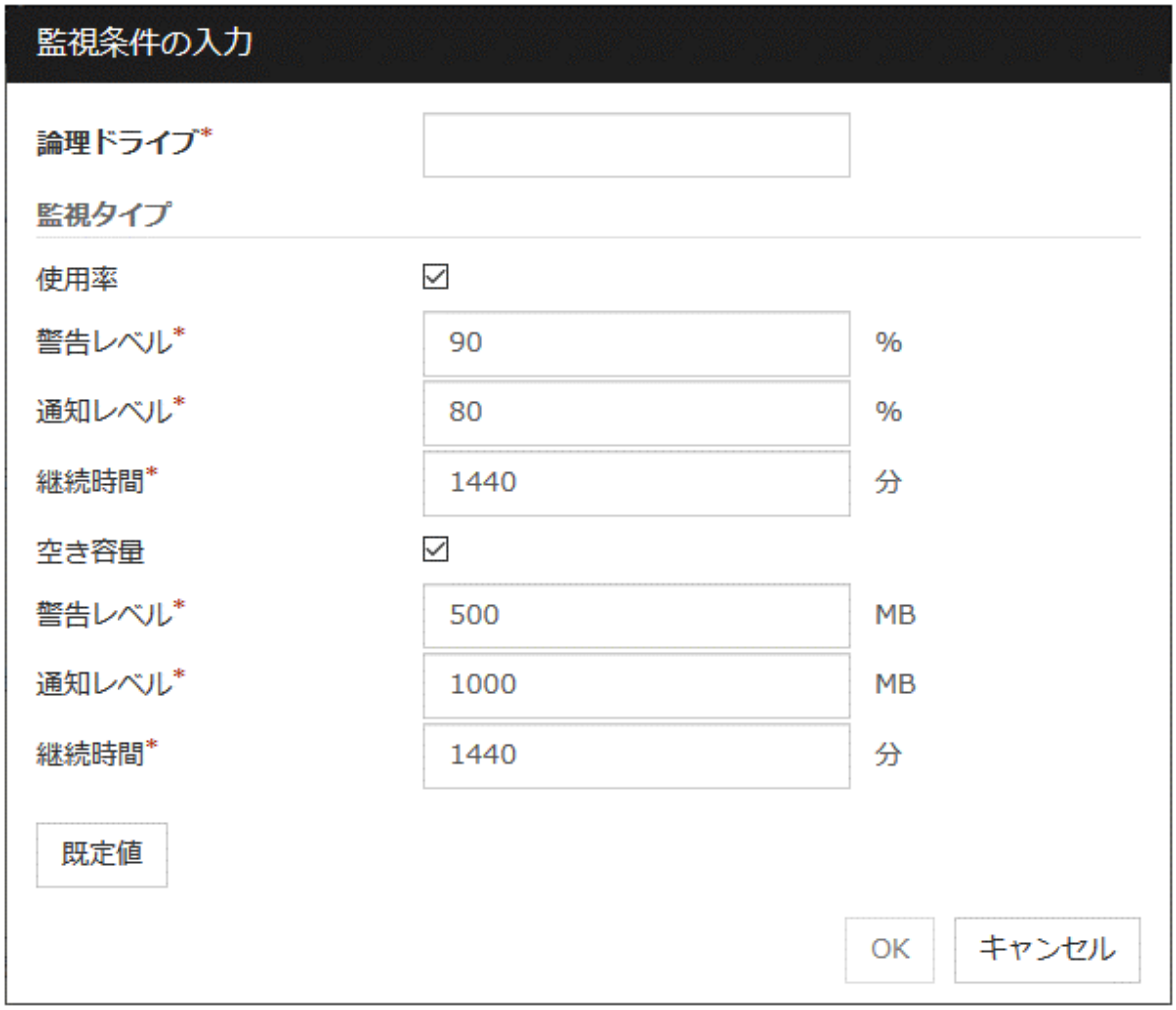
[監視条件の入力] ダイアログの説明に従い異常とする監視条件の詳細設定を行います。

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。



論理ドライブ

監視を行う論理ドライブを設定します。

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。

5.28 プロセスリソース監視リソースの設定

プロセスリソース監視リソースは、プロセスが使用するリソースを監視するモニタリソースです。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。

5.28.1 プロセスリソース監視リソースの注意事項

プロセスリソース監視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。

システムが高負荷な場合などでは、統計情報収集に時間がかかり統計情報収集間隔での情報収集ができない場合があります。

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 1 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
モニタリソースの定義画面のタイプ欄に「プロセスリソース監視」が表示されない場合は、[ライセンス情報取得]を選択し、ライセンス情報を取得してください。

プロセスリソース監視リソースの監視開始から、実際に監視処理を行うまでの間、プロセスリソース監視リソースのステータスは "警告" になります。

プロセスリソース監視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

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以下のコマンドで確認し設定してください。

CLUSTERPRO **インストールパス**\bin\GetProcess.vbs

上記コマンドを実行すると、コマンドを実行したフォルダ配下に GetProcess_Result.txt が出力されます。GetProcess_Result.txt を開き、表示されているプロセスの CommandLine 部分を指定してください。出力情報に 「"」(ダブルクォーテーション) がある場合は、「"」 も含めて指定してください。

出力ファイルの例

```
20XX/07/26 12:03:13
Caption     CommandLine
services.exe    C:\WINDOWS\system32\services.exe
svchost.exe     C:\WINDOWS\system32\svchost -k rpcss
explorer.exe    C:\WINDOWS\Explorer.EXE
```

上記のコマンド出力情報から svchost.exe を監視する場合、

`C:\WINDOWS\system32\svchost -k rpcss` 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。

システム監視リソース、プロセスリソース監視リソースの登録数が多い場合は、下記メッセージがアラートログに出力され異常を検出する場合があります。
本メッセージが出力された場合は [監視 (共通)] タブからタイムアウトの設定を見直してください。

```
監視 psrw は異常を検出しました。(99 : monitor was timeout)
```

5.28.2 プロセスリソース監視リソースの監視方法

プロセスリソース監視リソースは、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、リソース監視異常を通知します。
プロセスリソース監視（CPU、メモリ、スレッド数）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。

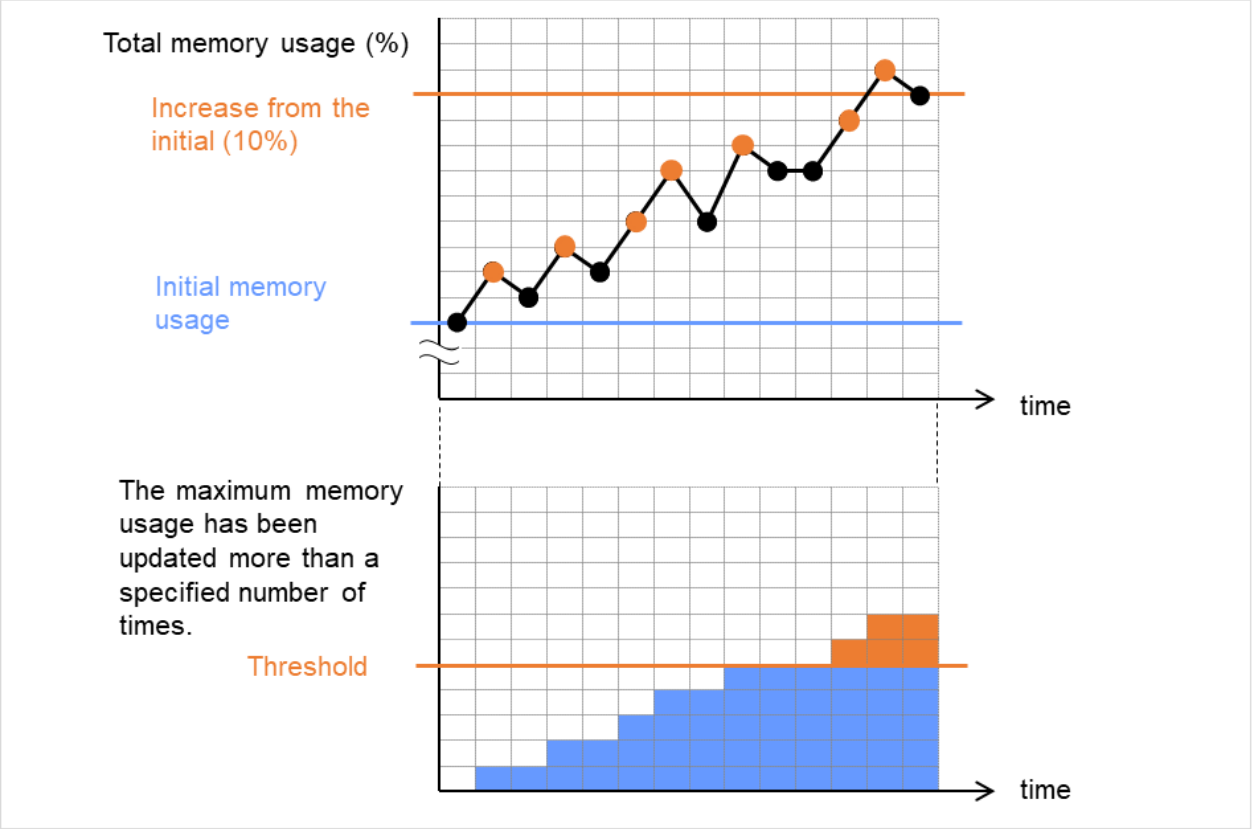


図 5.16　メモリ使用量が規定回数以上最大値を更新し、増加率が初期値の 10% を超過（異常検出する）

- 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。

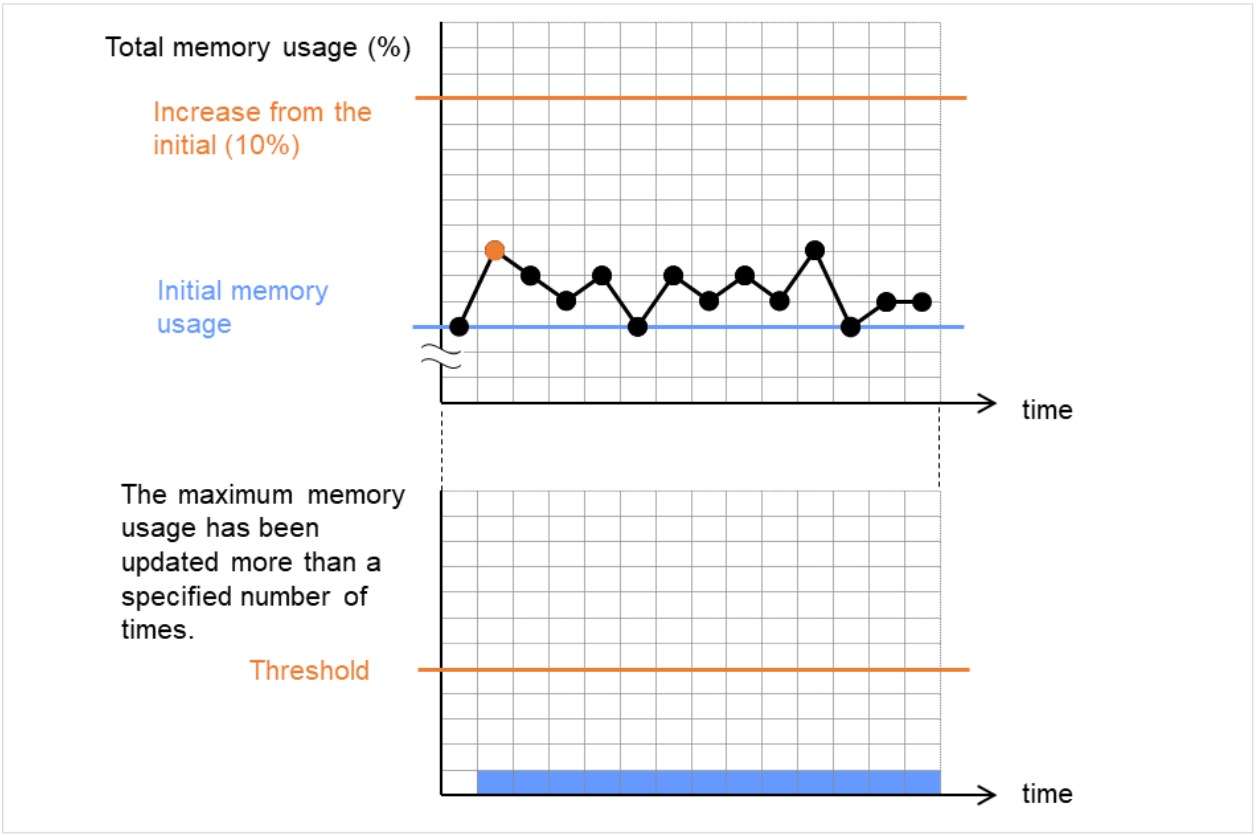
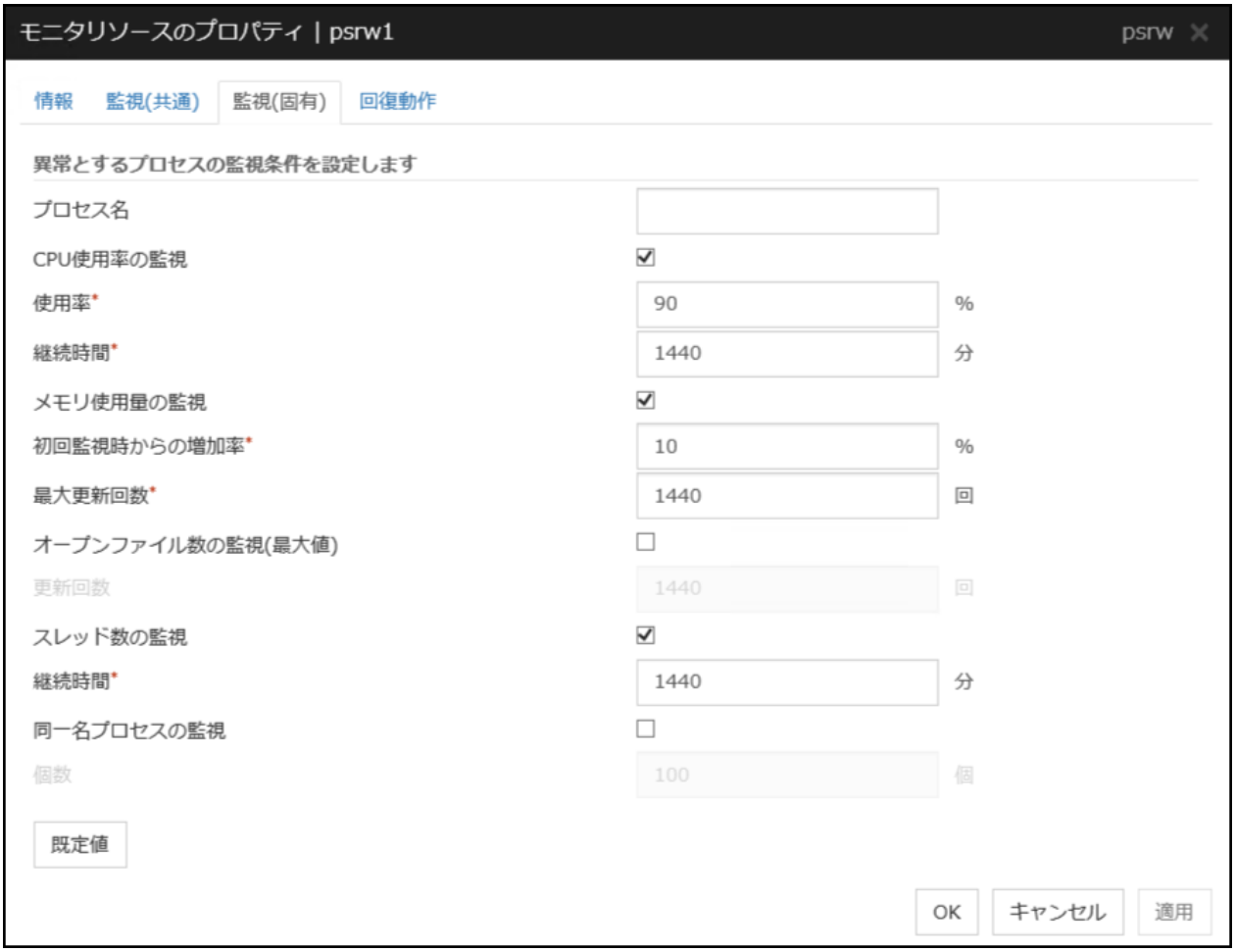


図 5.17　メモリ使用量が一定の範囲内で増減（異常検出しない）

5.28.3 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＞＊

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（1～4320）

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（1～4320）

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

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

  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（1～4320）

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。

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（1～4320）

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。

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。

5.29 ユーザ空間監視リソースの設定

ユーザ空間監視リソースは、ユーザ空間のストールを監視するモニタリソースです。

ユーザ空間監視リソースはデフォルトで登録されています。

5.29.1 ユーザ空間監視リソースの監視方法

ユーザ空間監視リソースは以下の監視を行います。

監視開始時に keepalive タイマを起動し、以降、監視間隔ごとに keepalive タイマの更新を行います。ユーザ空間のストールによって、一定時間以上タイマの更新が行われなかった場合に異常を検出します。

監視処理を拡張させる設定として、ダミースレッドの作成があります。設定が有効な場合は、監視間隔ごとにダミースレッドの作成を行います。ダミースレッドの作成に失敗した場合は keepalive タイマの更新を行いません。

ユーザ空間監視リソースの処理ロジックは以下の通りです。

- 処理概要

  以下の 2〜3 の処理を繰り返します。

  1. keepalive タイマセット
  2. ダミースレッド作成
  3. keepalive タイマ更新

  処理 2 は監視の拡張設定の処理です。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 2〜3 が問題無く処理される） 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 2〜3 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、CLUSTERPRO のカーネルモジュールにより、HW リセットまたは意図的なストップエラーを発生させます。

5.29.2 監視 (固有) タブ

監視方法

ユーザ空間の監視方法を指定します。

- keepalive

clphb ドライバを使用します。

タイムアウト発生時動作

タイムアウト発生時の動作を指定します。

- 何もしない

  何も行いません。

- HW リセット

  ハードウェアをリセットします。

- 意図的なストップエラーの発生

  ストップエラーを発生させます。

注釈: タイムアウト発生時動作に関しては、擬似障害を発生させることができません。

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 (既定値)

  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。

第 6 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。

- 6.1. クラスタプロパティ
- 6.2. サーバプロパティ
- 6.3. 登録最大数一覧

6.1 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。

6.1.1 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。

クラスタ名

サーバ名を表示します。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

6.1.2 インタコネクトタブ

使用しません。

6.1.3 フェンシングタブ

使用しません。

6.1.4 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。

ネットワーク初期化完了待ち時間 (0〜99)

サーバ起動時に自サーバの NIC が有効となるまで待ち合わせる時間です。

同期待ち時間 (0〜99)

使用しません。

ハートビート

- 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:

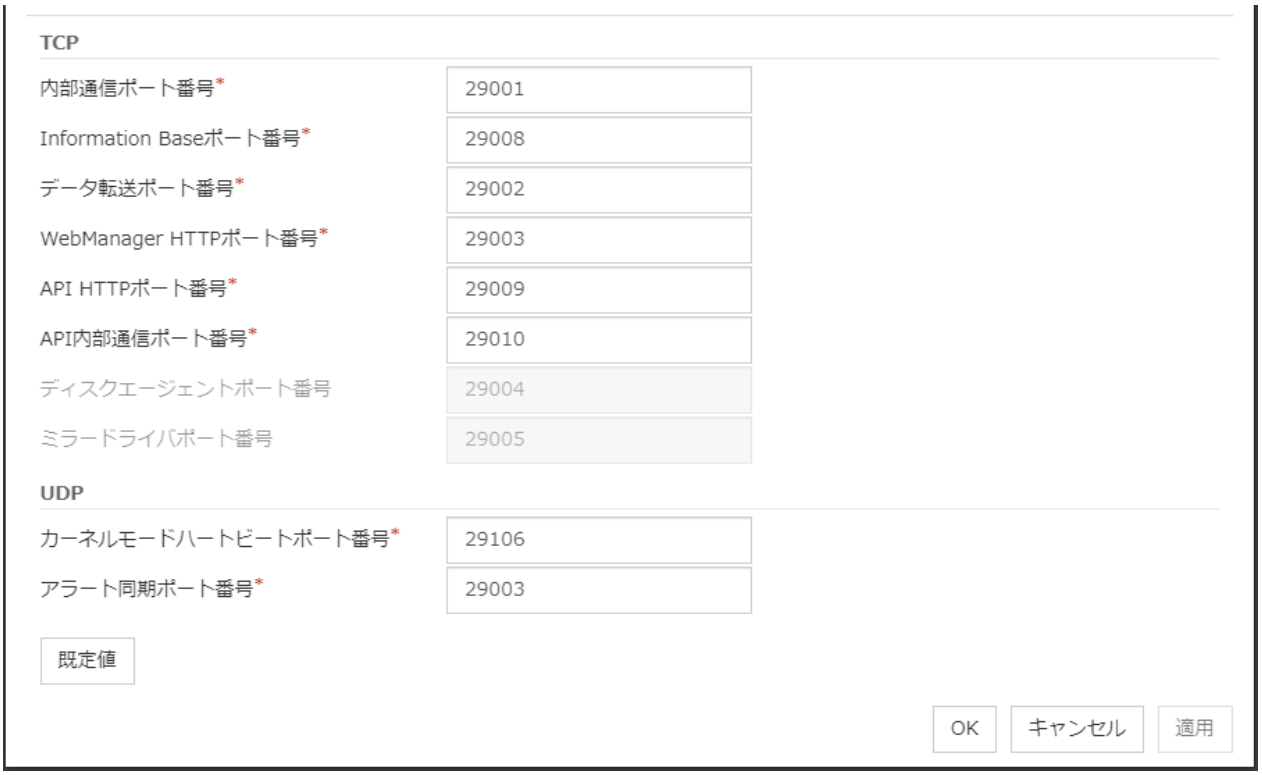
内部通信タイムアウトを極端に大きな値に設定すると、ハートビートが途絶した場合に clpstat コマンドの実行や Cluster WebUI の表示に要する時間に大きく影響します。
既定値を設定することを推奨します。

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。

6.1.5 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。
- ディスクエージェントポート番号 (1〜65535[*3])
  使用しません。
- ミラードライバポート番号 (1〜65535[*3])
  使用しません。

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])
  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。

[*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。

6.1.6 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動作を指定します。

- 緊急シャットダウン

  サーバをシャットダウンします。

  注釈: ユーザ空間監視リソースを設定している場合、シャットダウン処理中にハートビートタイムアウトが経過すると、ユーザ空間監視リソースのタイムアウト発生時動作が実行される場合があります。

- 意図的なストップエラーの発生

  意図的にストップエラー (Panic) を発生させてサーバを再起動します。

- HW リセット

  HW リセットによりサーバを再起動します。

注釈: CLUSTERPRO Server サービス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。

  - 何もしない
  - 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、システム監視リソースやプロセスリソース監視リソース、JVM 監視リソース、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。

- 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。
- 意図的なストップエラーの発生

  ストールが発生したサーバに対し意図的にストップエラー (Panic) を発生させます。
- 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 ： 意図的なストップエラーの発生

最終動作に「クラスタサービス停止と OS シャットダウン」または「クラスタサービス停止と OS 再起動」を指定した場合は、クラスタサービス停止に時間がかかります。

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:

- 外部連携監視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
  - 意図的なストップエラーの発生

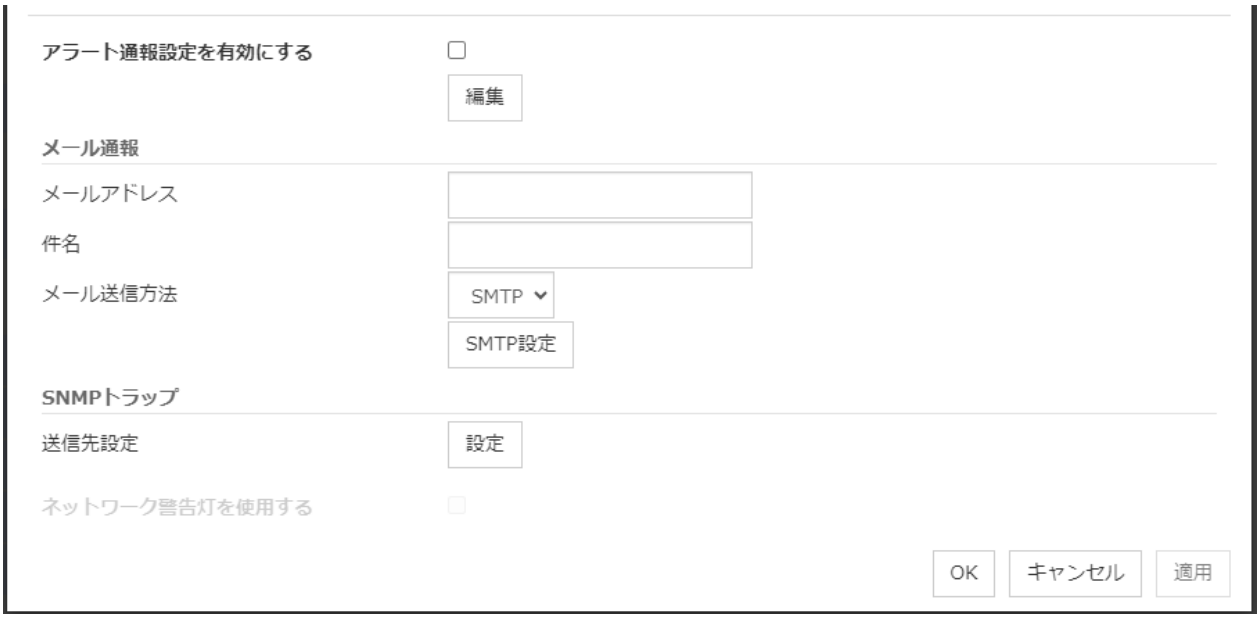
両系活性検出時のシャットダウンを抑制する。

使用しません。

6.1.7 アラートサービスタブ

アラート通報とネットワーク警告灯の設定を行います。

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 Windows 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「イベントログ、アラートメッセージ」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。現在は SMTP のみ選択可能です。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。

- SMTP

  SMTP サーバと直接通信をしてメール通報をします。

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。

ネットワーク警告灯を使用する

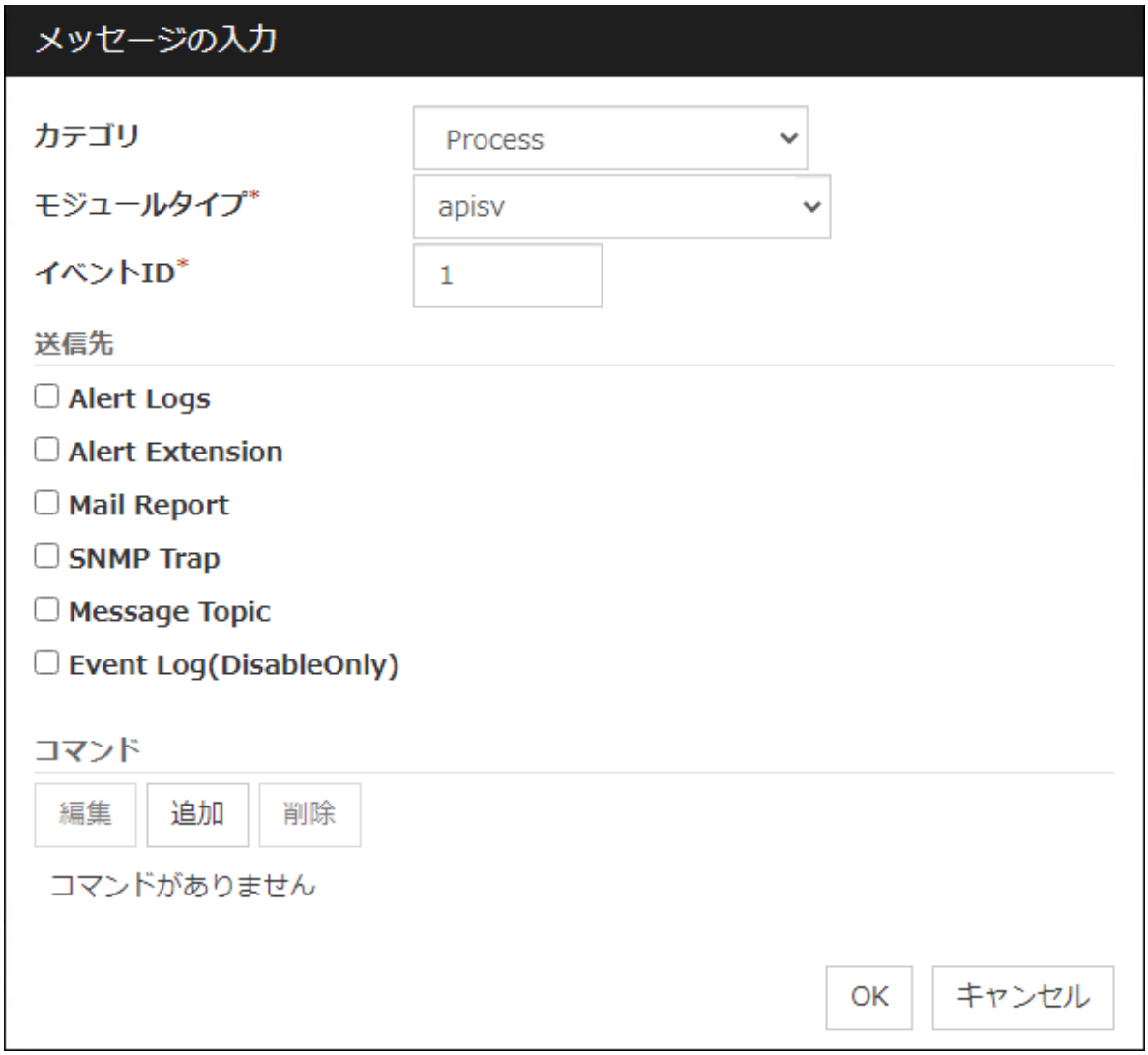
使用しません。

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アラート 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メッセージ ID を入力します。メッセージ ID は『操作ガイド』の「エラーメッセージ一覧」の「イベントログ、アラートメッセージ」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。

- Alert Logs

アラートログにメッセージを表示します。

- 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)。

- 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

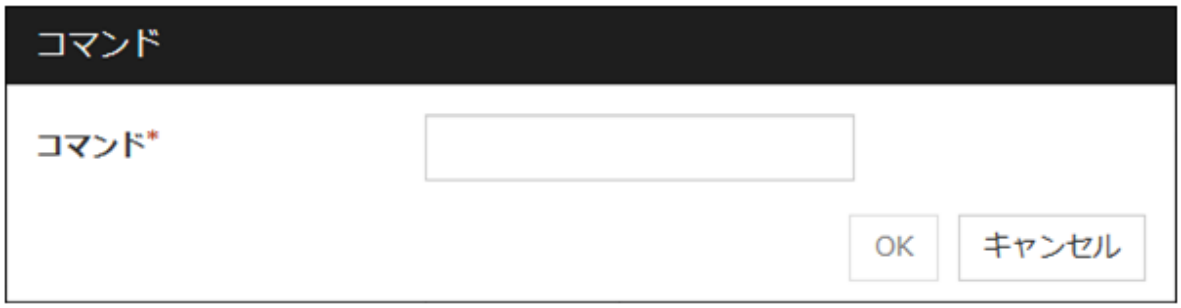
  Amazon SNS へ送信します。

- Event Log(DisableOnly)

  チェックを外すことにより、OS の EventLog への記録を行わないようにすることができます。
  (EventLog に出力しないメッセージを出力する様に変更する事は出来ません)。

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 (511 バイト以内)

任意のコマンドを入力します。

- キーワードについて

  %%MSG%% を指定すると、該当の 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。

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] ボタンを選択してください。

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] ボタンを選択してください。

SMTP の設定

[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 サーバの一覧

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 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」 - 「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。

SNMP の設定

SNMP トラップの [設定] をクリックする SNMP トラップで使用する [送信先設定] ダイアログボックスが表示されます。

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

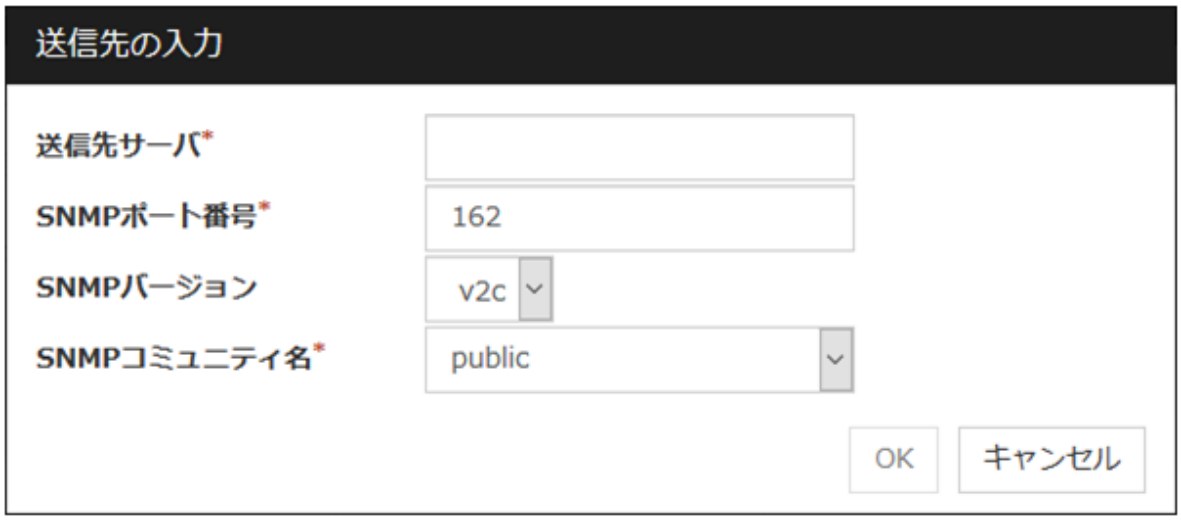
SNMP トラップ送信先を追加します。[追加] をクリックすると 送信先の入力ダイアログが表示されます。

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。

6.1.8 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。

- 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。

- サーバがワークグループに所属している場合

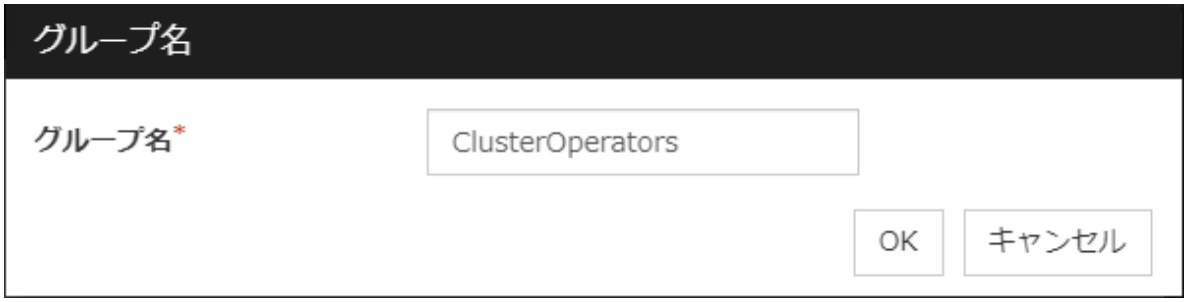
  サーバにユーザ、グループを登録します。

- 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

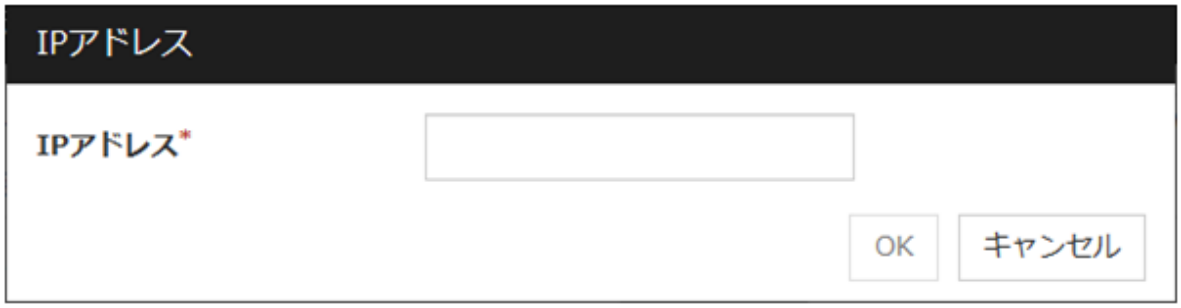
  [追加]、[削除]、[編集] ボタンが表示されます。

- 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] ボタンを選択すると 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] ボタンを選択してください。

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] ボタンを選択します。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。

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] ボタンを選択すると統合 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。サーバの IP アドレスは、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] ボタンを選択すると [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。

6.1.9 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

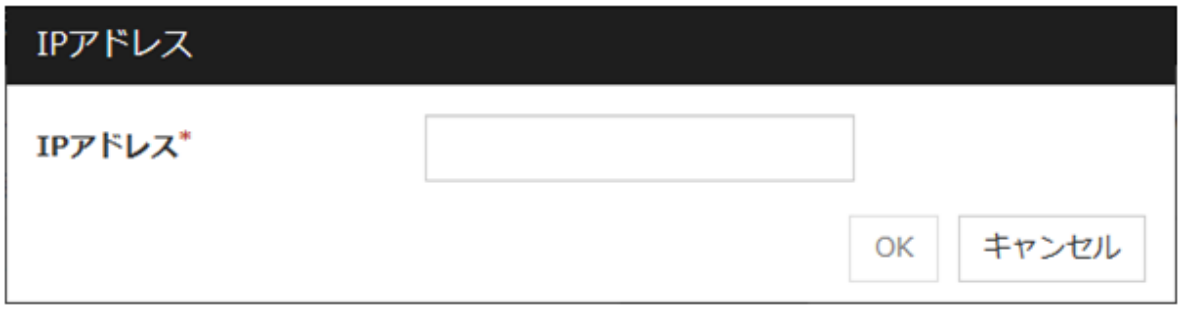
  [追加]、[削除]、[編集] が表示されます。

- 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
  クライアント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
  クライアントはクラスタの状態表示のみ行えます。

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

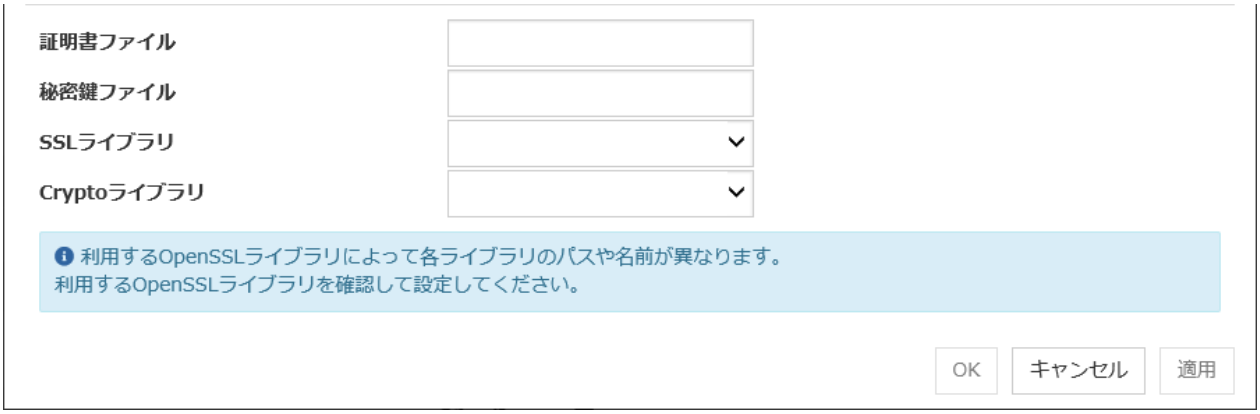
  API サービスが HTTP サーバの起動に失敗した時から次の起動をリトライするまでの間隔を設定します。

- 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。

6.1.10 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。

6.1.11 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 CLUSTERPRO Web Alert 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

  CLUSTERPRO Web Alert サービスを有効にします。

- チェックボックスがオフ

  CLUSTERPRO Web Alert 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 CLUSTERPRO Web Alert 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)

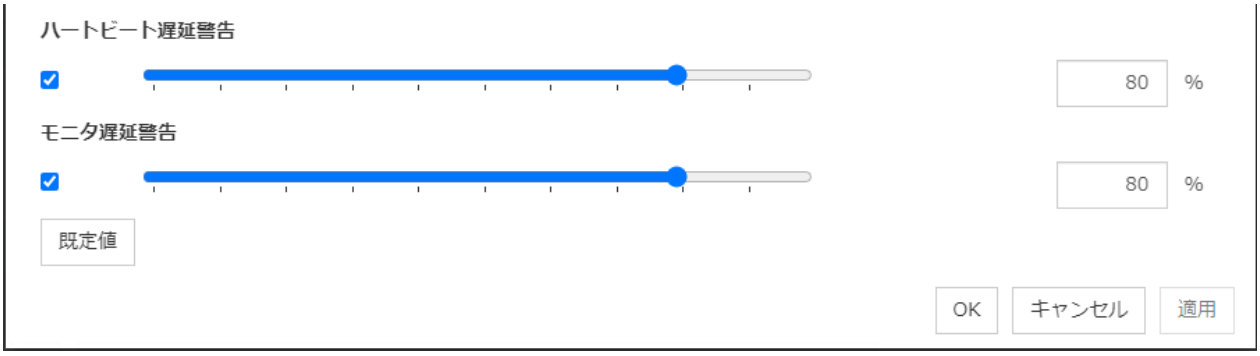
使用しません。

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。

6.1.12 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「監視動作の詳細」の「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 (1～99)

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。

モニタ遅延警告 (1～99)

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。

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。

6.1.13 ディスクタブ

使用しません。

6.1.14 ミラーディスクタブ

使用しません。

6.1.15 アカウントタブ

クラスタシステムが実行するスクリプト等で使用するユーザアカウントの登録/削除を行います。ユーザアカウントは、最大 16 まで設定できます。

追加

[アカウント一覧] にユーザアカウントを追加する場合に使用します。[追加] をクリックすると [アカウントの入力] ダイアログボックスが表示されます。

- ユーザ名

  登録するユーザアカウント名を入力します。ドメインのアカウントを指定する場合は、「**ドメイン名\アカウント名**」のように入力してください。

- パスワード

  登録するユーザアカウントのパスワードを入力します。

削除

[アカウント一覧] からユーザアカウントを削除する場合に使用します。[アカウント一覧] から 削除したいユーザアカウントを選択して、[削除] をクリックしてください。

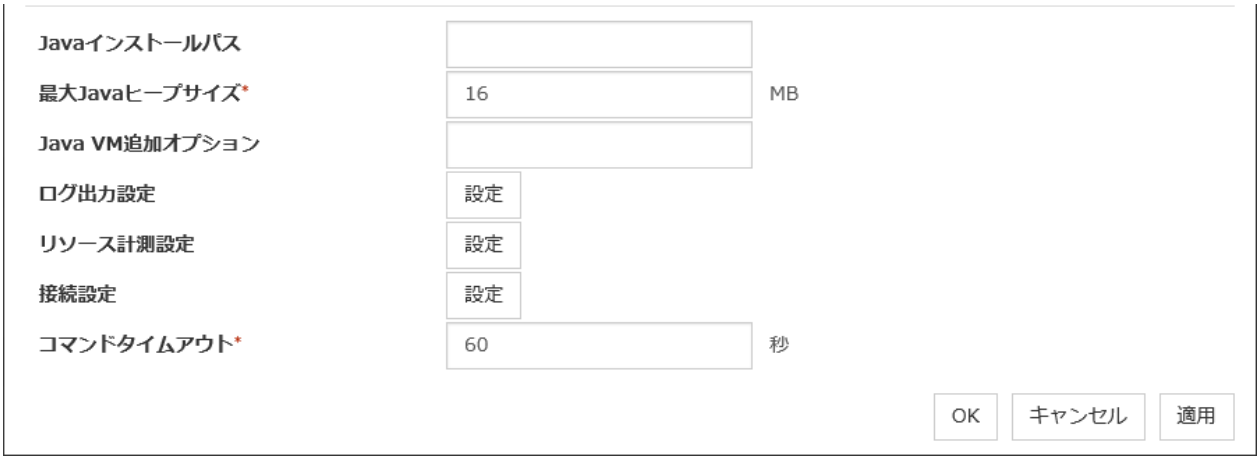
編集

ユーザアカウントを編集する場合に使用します。[アカウント一覧] から編集したいユーザアカウントを選択して、[編集] をクリックします。選択されたユーザアカウントが入力されている [アカウントの入力] ダイアログボックスが表示されます。

6.1.16 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 の設定モードで 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：`C:\Program Files\Java\jdk1.8.0_102`

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した [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、「5. 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、「5. 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)

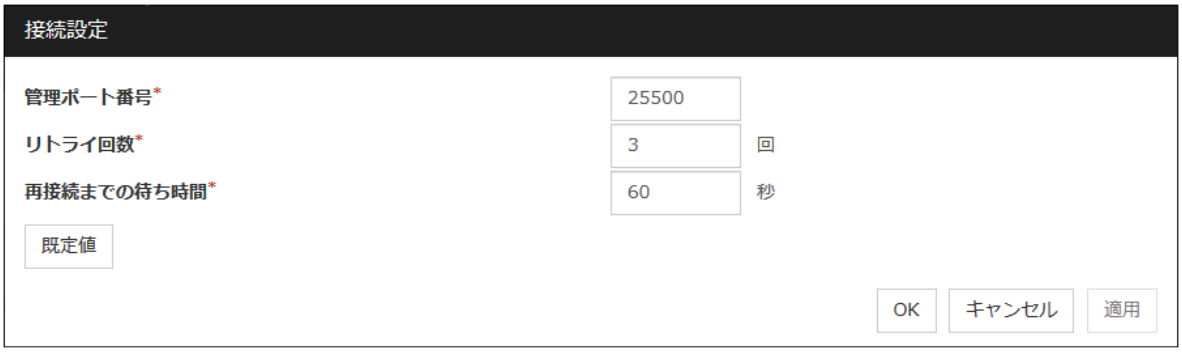
JVM 監視が WebLogic 監視におけるワークマネージャおよびスレッドプールのリクエスト数平均値を計測するインターバルを設定します。インターバル リクエスト数で設定されている整数倍の値を設定してください。

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 監視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。42424～61000 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。

6.1.17 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「イベントログ、アラートメッセージ」の [8] 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。

6.1.18 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。

システムリソース統計情報

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

  クラスタ動作中に 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。ログ収集の詳細については、『操作ガイド』の「CLUSTERPRO X SingleServerSafe コマンドリファレンス」の「ログを収集する (clplogcc コマンド)」または、オンラインマニュアルを参照してください。

  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

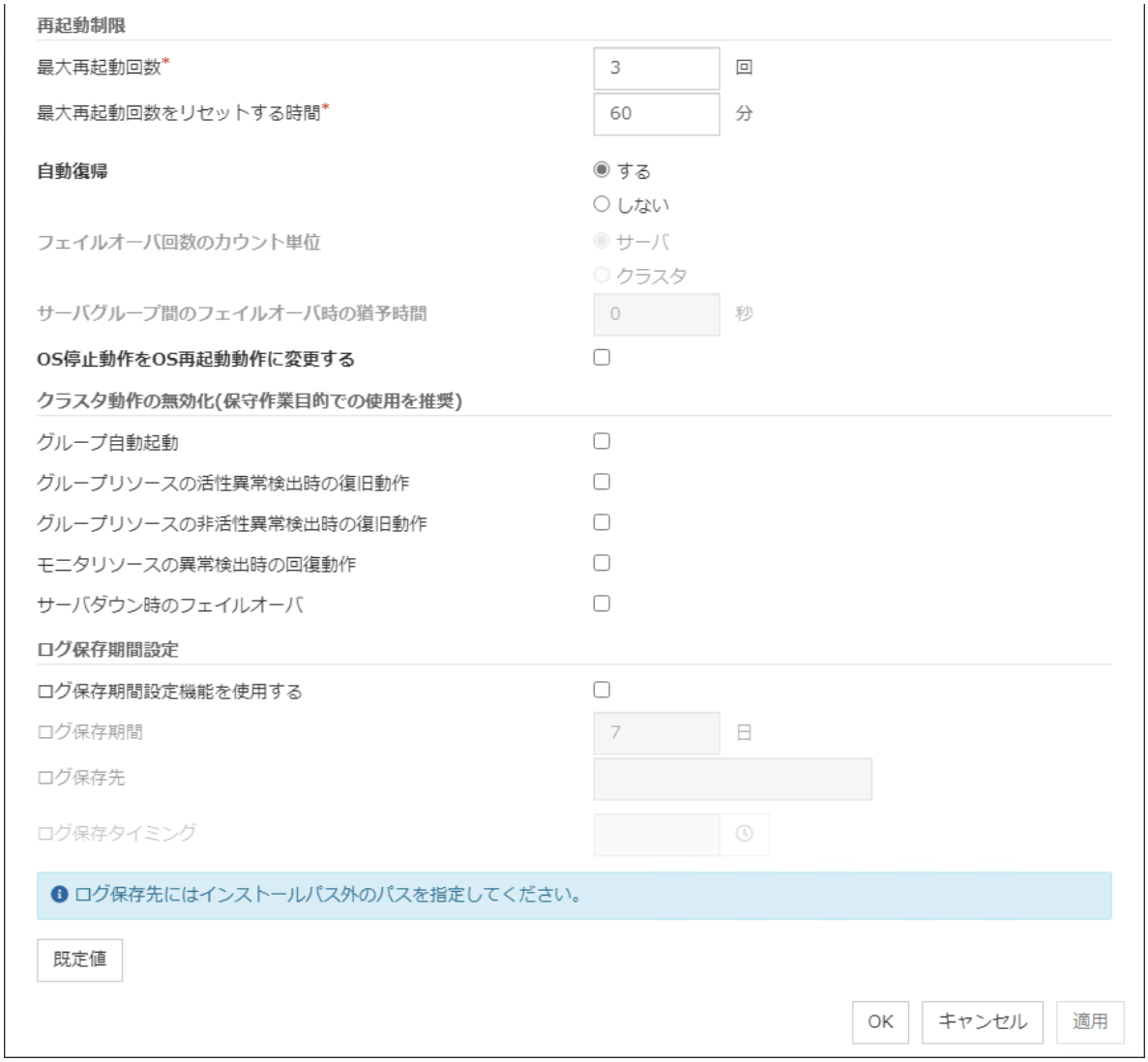
  システムリソース情報を収集しません。

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。

6.1.19 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には、それぞれ異常検出時の最終動作として [OS 再起動] や [OS シャットダウン] が設定できます。これらを設定している場合、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] が 1 以上に設定されている場合は、[最大再起動回数をリセットする時間] は 1 以上に設定してください。[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、再起動回数制限が無効となり、最大再起動回数の設定によらず、異常検出時に毎回シャットダウン/再起動を行います。

自動復帰

- する
  自動復帰を行います。
- しない
  自動復帰を行いません。

フェイルオーバ回数のカウント単位

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。

- クラスタサービスのプロセス異常時動作
  - 「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。
- グループリソース活性/非活性ストール発生時動作
  - 「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。
- 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。
- 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。

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。

- 外部連携監視リソース
- ユーザ空間監視リソース

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:

以下の動作は、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。
・ディスク RW 監視リソースのストール異常検出時動作
・ユーザ空間監視リソースのタイムアウト発生時動作
・外部連携監視リソースの回復動作

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 (ファイル名末尾が 0.log, 1.log, pre のいずれか) 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.zip」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。

6.2 サーバプロパティ

「サーバのプロパティ」では、サーバにおいて利用するインタフェース (IP アドレスやデバイス) の追加、削除および編集を行います。ネットワーク環境に関する注意事項として、IP アドレスには、以下の規則があります。

- 1 サーバ内に同一ネットワークアドレスに属する IP アドレスが複数存在してはいけません。また、以下のように包含関係にあってもいけません。
  - IP アドレス：10.1.1.10、サブネットマスク：255.255.0.0
  - IP アドレス：10.1.2.10、サブネットマスク：255.255.255.0

6.2.1 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。

6.2.2 警告灯タブ

使用しません。

6.2.3 BMC タブ

使用しません。

6.2.4 HBA タブ

使用しません。

6.2.5 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。

6.3 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	512
モニタリソース	4.0.0-1 以降	384

第 7 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。

- 7.1. 常時監視と活性時監視について
- 7.2. モニタリソースの擬似障害 発生/解除
- 7.3. モニタリソースの監視インターバルのしくみ
- 7.4. モニタリソースによる異常検出時の動作
- 7.5. 監視異常からの復帰 (正常)
- 7.6. 回復動作時の回復対象活性/非活性異常
- 7.7. 回復スクリプト、回復動作前スクリプトについて
- 7.8. モニタリソースの遅延警告
- 7.9. モニタリソースの監視開始待ち
- 7.10. モニタリソース異常検出時の再起動回数制限

7.1 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、指定されたリソースが活性してから、そのリソースが非活性 (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

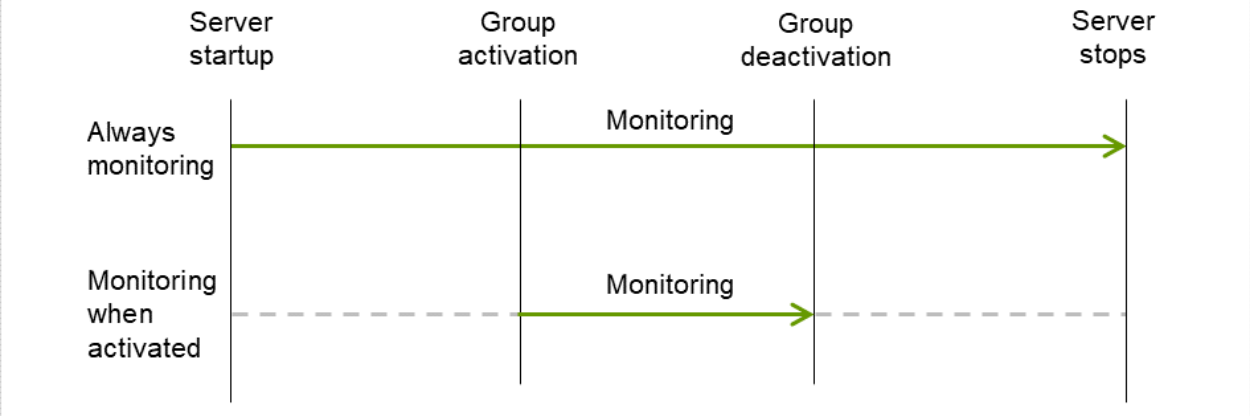


図 7.1　モニタリソースの常時監視と活性時監視

7.2 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

7.3 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

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

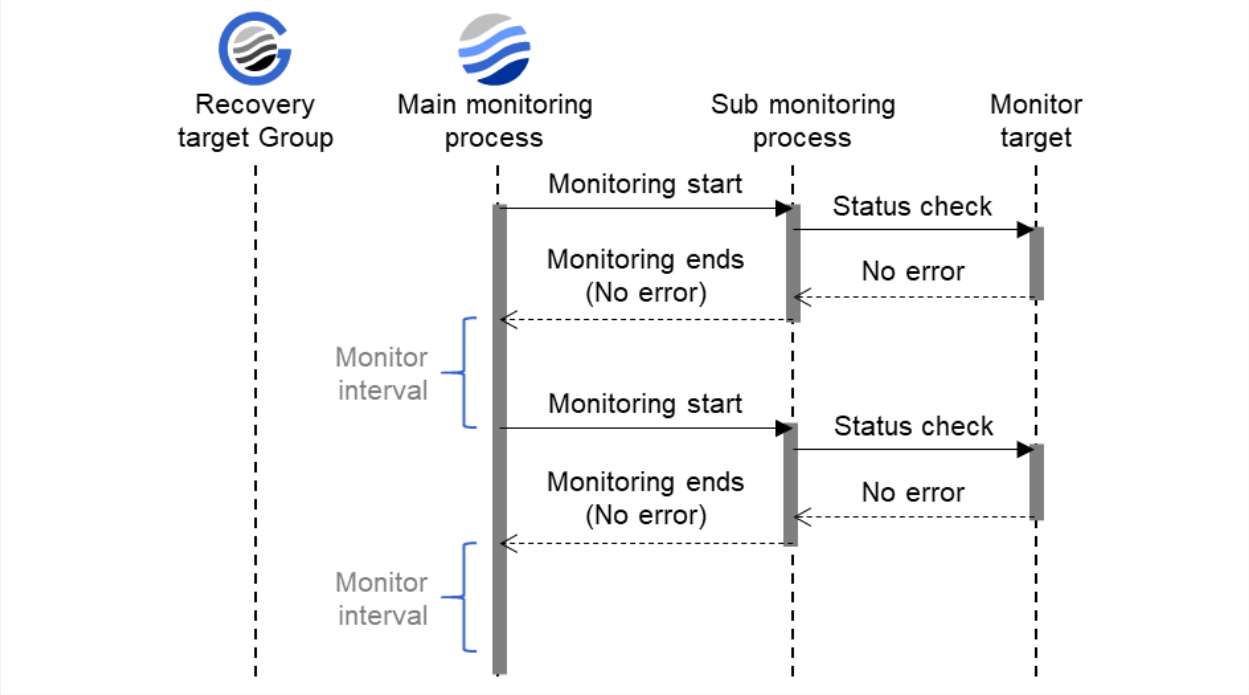


図 7.2　監視インターバル（監視正常検出時）

監視異常検出時 (監視リトライ設定なし)

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

最大再活性回数 0 回

最終動作 何もしない

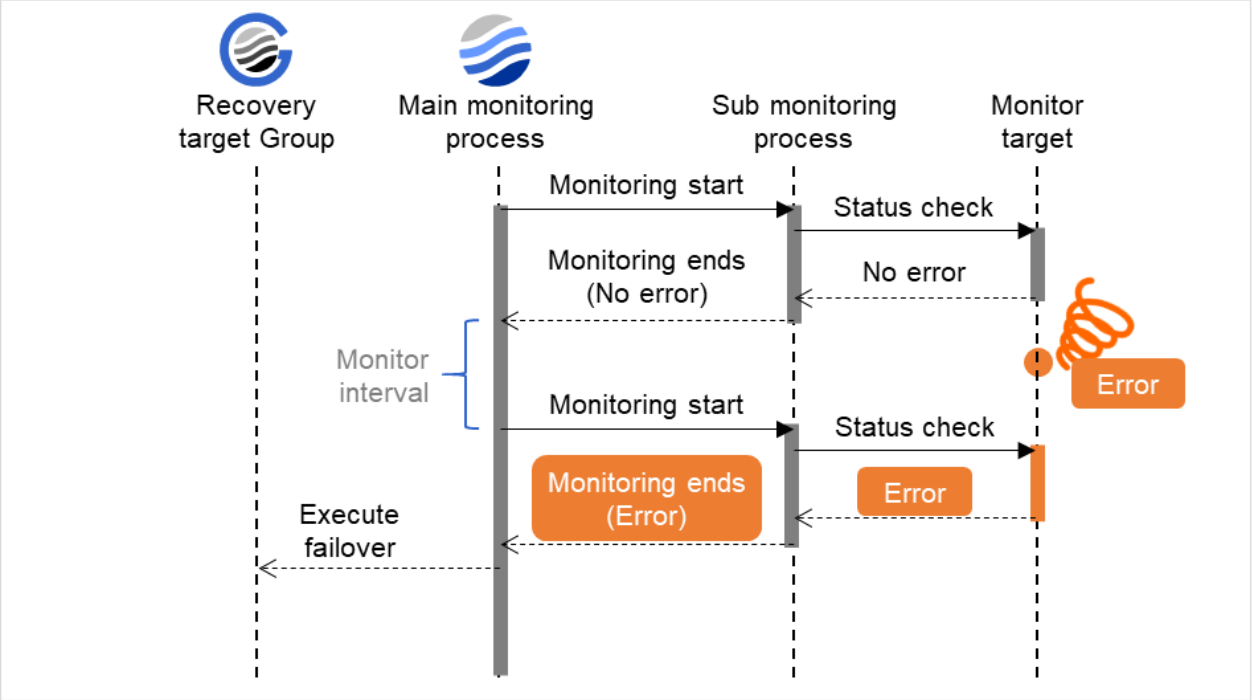


図 7.3　監視インターバル（監視異常検出時 ・監視リトライ設定なし）

監視異常検出時 (監視リトライ設定あり)

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

最大再活性回数 0 回

最終動作 何もしない

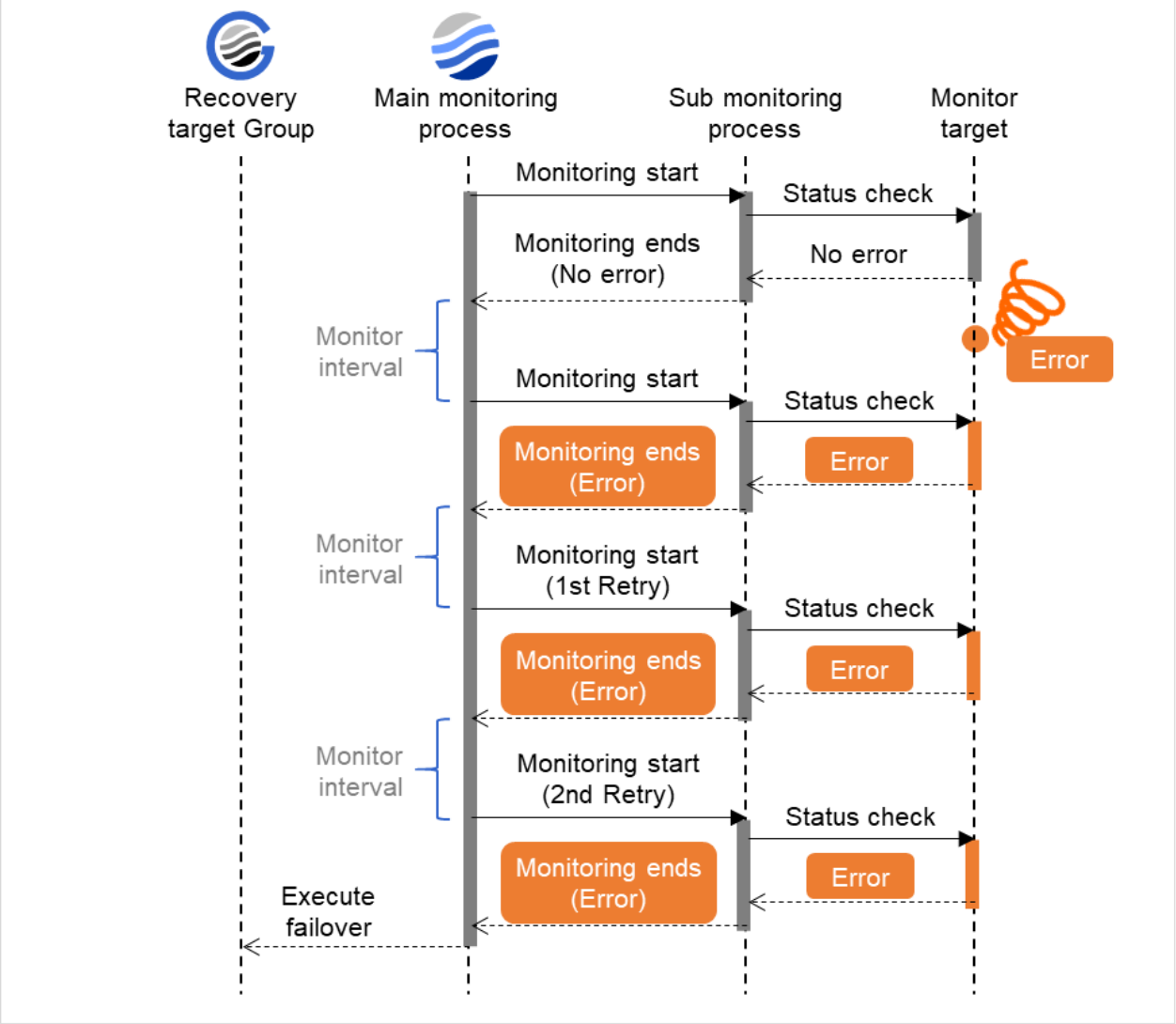


図 7.4　監視インターバル（監視異常検出時 ・監視リトライ設定あり）

監視タイムアウト検出時 (監視リトライ設定なし)

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

最大再活性回数 0 回

最終動作 何もしない

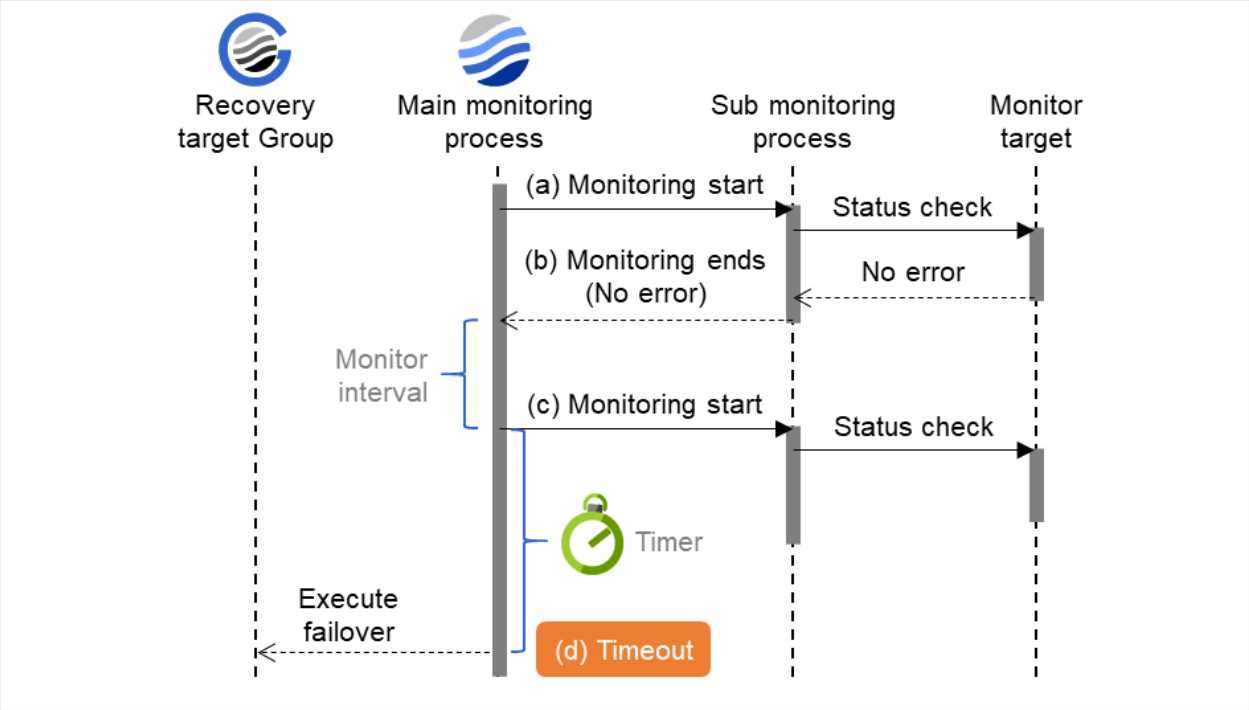


図 7.5　監視インターバル（監視タイムアウト検出時 ・監視リトライ設定なし）

監視タイムアウト検出時 (監視リトライ設定あり)

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

最大再活性回数 0 回

最終動作 何もしない

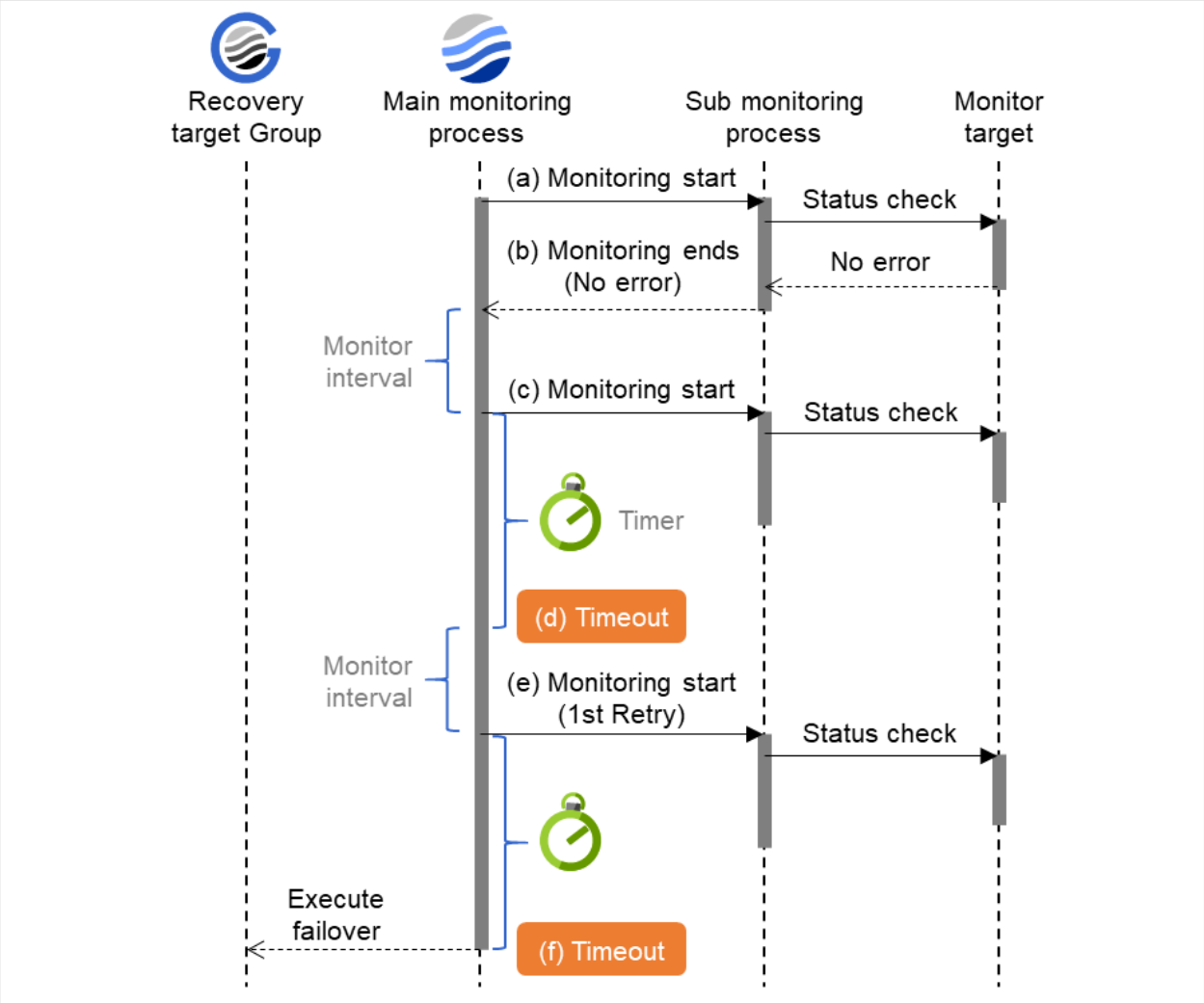


図 7.6　監視インターバル（監視タイムアウト検出時 ・監視リトライ設定あり）

7.4 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. 262, *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: サービスリソース、アプリケーションリソース) 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。

- クラスタの停止 / 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。

7.5 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再活性化しきい値に対する回数カウンタ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。

最終動作については、実行要否がリセット (実行要に) されます。

7.6 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。

7.7 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） 13.31
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）13
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）`C:\Program Files\CLUSTERPRO`

次のページに続く

表 7.2 – 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）Windows Server 2016 Standard
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）6.2.0.0.274.3
CLP_ACTION …回復動作種別	RECOVERY RESTART FAILOVER FINALACTION	回復スクリプトとして実行された場合。 再起動前に実行された場合。 使用しません。 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。
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

```
rem ************************************************************
rem *                      preaction.bat                       *
rem ************************************************************

echo START

IF "%CLP_ACTION%"=="" GOTO NO_CLP

IF "%CLP_ACTION%"=="RECOVERY" GOTO RECOVERY
IF "%CLP_ACTION%"=="RESTART" GOTO RESTART
IF "%CLP_ACTION%"=="FINALACTION" GOTO FINALACTION
GOTO NO_CLP


:RECOVERY
echo RECOVERY COUNT: %CLP_RECOVERYCOUNT%

rem ここに回復処理を記述する。
rem この処理は以下のタイミングで実行される。
rem
rem  回復動作：回復スクリプト

GOTO EXIT


:RESTART
echo RESTART COUNT: %CLP_RESTARTCOUNT%

rem ここに再活性化前処理を記述する。
rem この処理は以下のタイミングで実行される。
rem
rem  回復動作：再活性化

GOTO EXIT


:FINALACTION
echo FINALACTION
```

(次のページに続く)

(前のページからの続き)

```
rem ここに回復処理を記述する。
rem この処理は以下のタイミングで実行される。
rem
rem  回復動作：最終動作

GOTO EXIT

:NO_CLP

:EXIT
echo EXIT
exit
```

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。

回復スクリプト、回復動作前スクリプト 注意事項

- 特にありません。

7.8 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。

図は監視タイムアウトに 60 秒、遅延警告割合には既定値の 80%（48 秒） を指定した場合です。矢印は監視のポーリング時間を表しています。

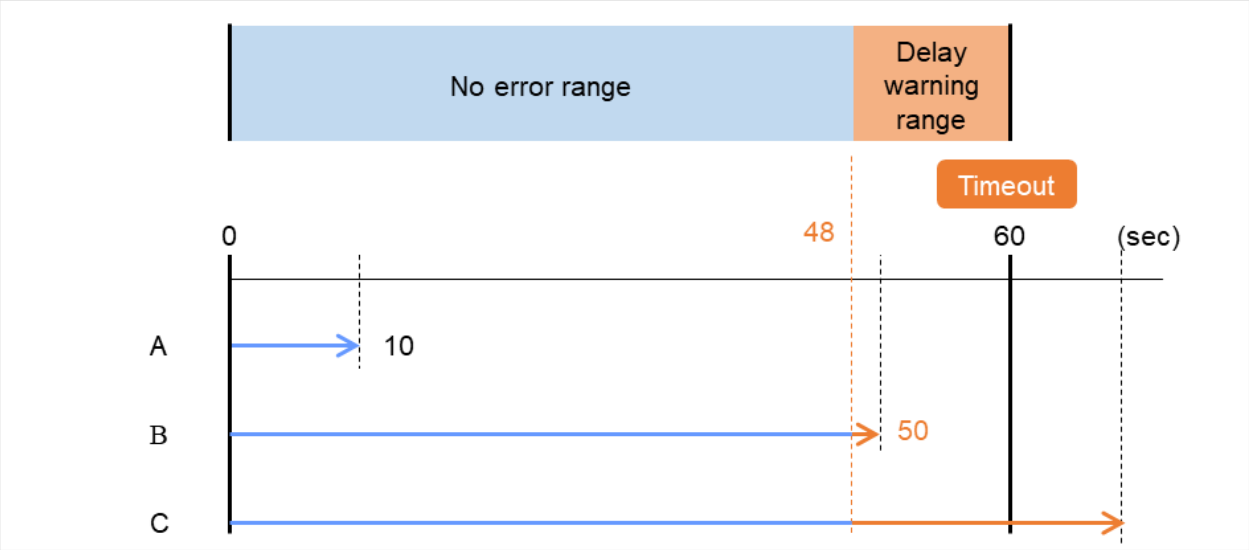


図 7.7　監視ポーリング時間と遅延警告

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。

参考:

モニタリソースの遅延警告は [クラスタプロパティ] → [遅延警告] タブの [モニタ遅延警告] で設定します。

7.9 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。

[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

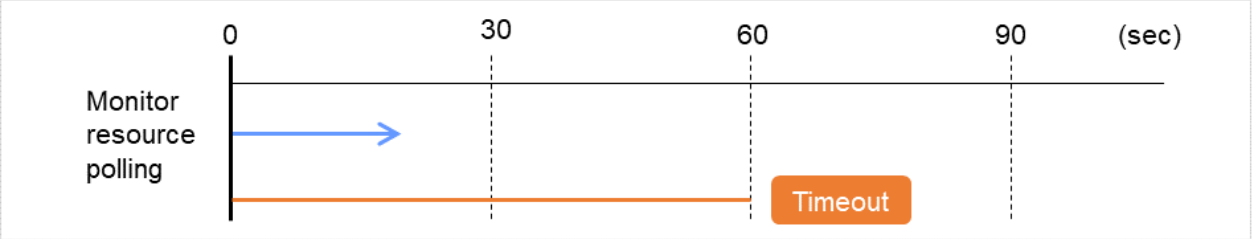


図 7.8　モニタリソースの監視開始待ち（監視開始待ち時間 0 秒）

[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

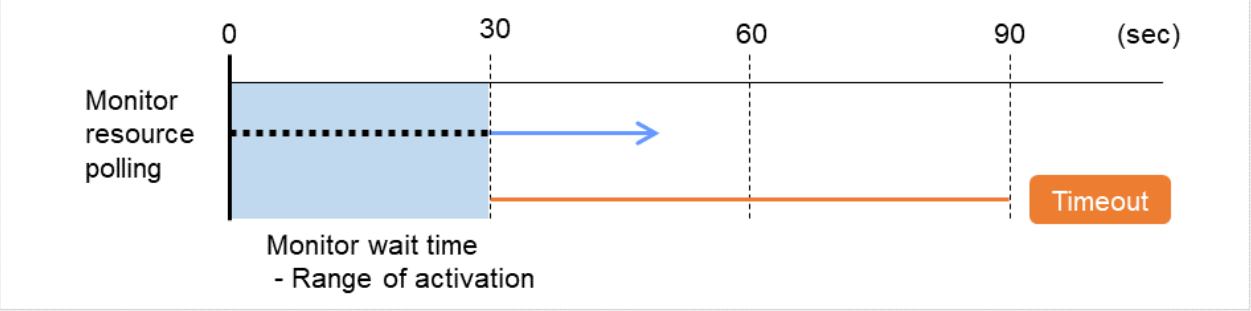


図 7.9　モニタリソースの監視開始待ち（監視開始待ち時間 30 秒）

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、アプリケーション監視リソースが監視するアプリケーション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。

[アプリケーション監視リソース構成]

<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 (既定値)

<異常検出>
回復動作 以下のターゲットを再起動
回復対象 appli1
最終動作 グループ停止

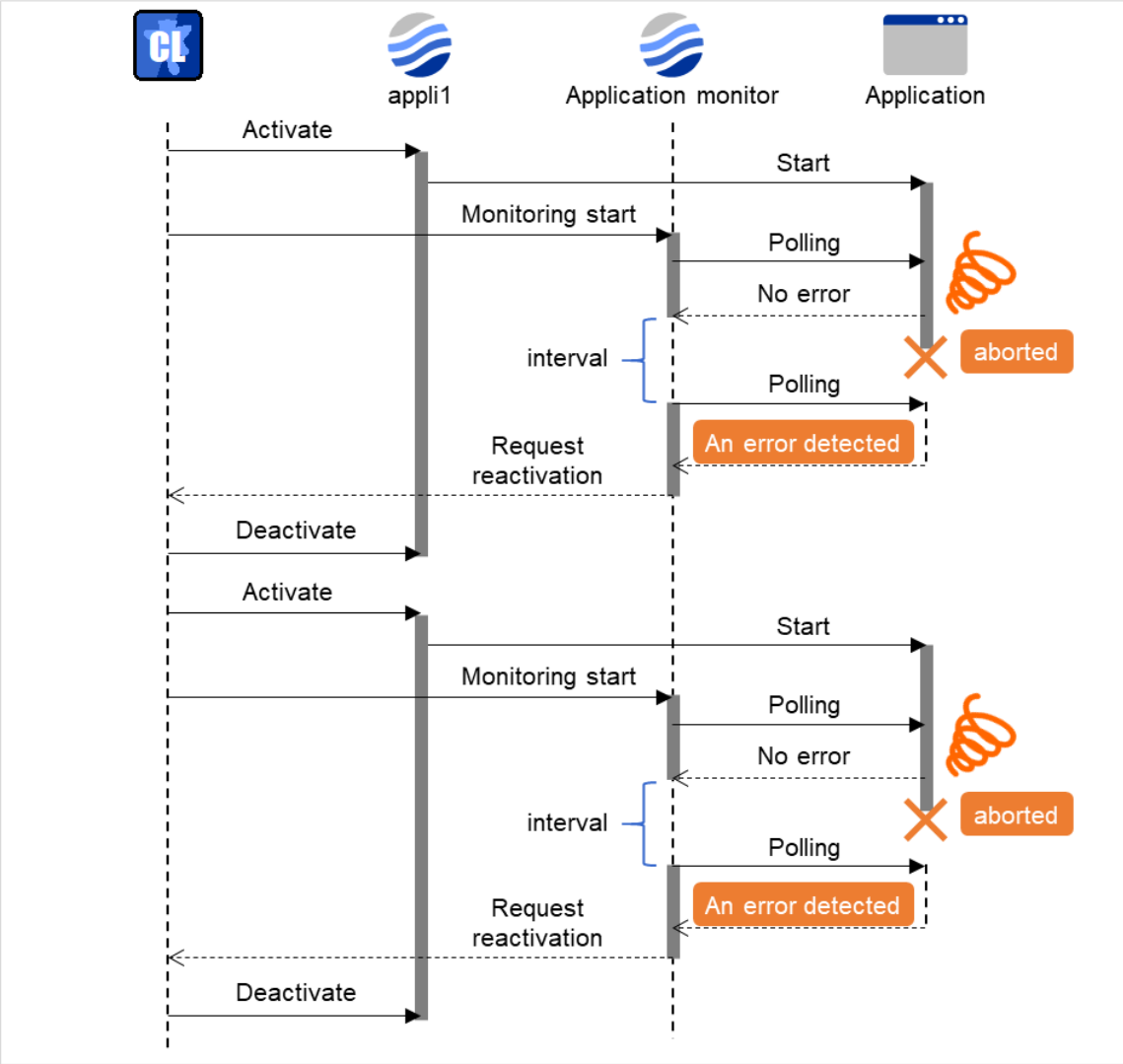


図 7.10　モニタリソースの監視開始待ち（監視開始待ち時間 0 秒）

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。

[アプリケーション監視リソース構成]

<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 以下のターゲットを再起動

回復対象 appli1

最終動作 グループ停止

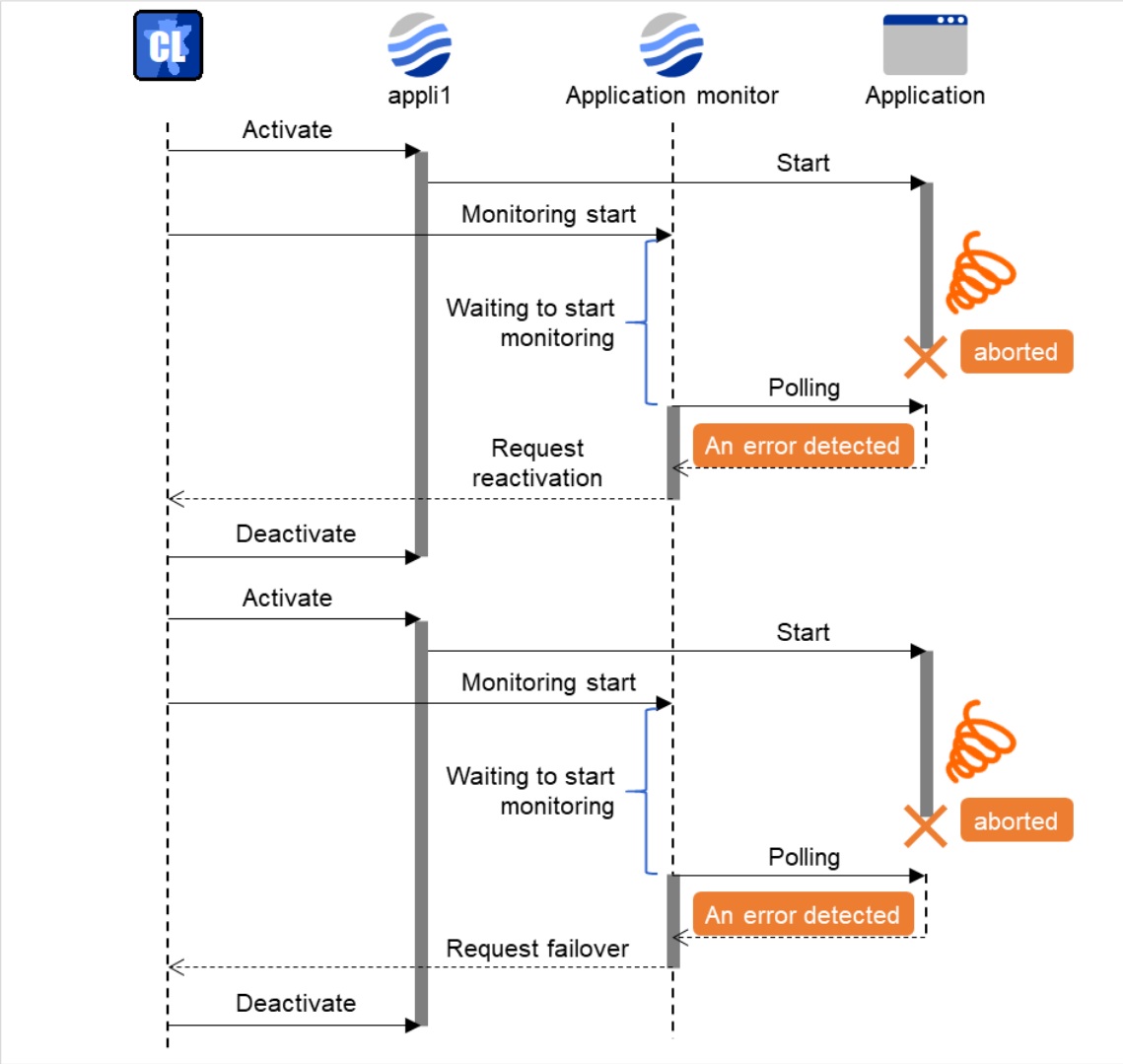


図 7.11　モニタリソースの監視開始待ち（監視開始待ち時間 60 秒）

7.10 モニタリソース異常検出時の再起動回数制限

モニタリソース異常検出時の最終動作として [クラスタサービス停止と OS シャットダウン] 、または [クラスタサービス停止と OS 再起動] を設定している場合に、モニタリソース異常の検出による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。

再起動回数をリセットするには、clpregctrl コマンドを使用します。clpregctrl コマンドについての詳細は『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。

注釈:

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。

第 8 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。

- 8.1. **システム構成検討時**
- 8.2. *CLUSTERPRO X SingleServerSafe* **の構成情報作成時**
- 8.3. *CLUSTERPRO X SingleServerSafe* **の構成変更時**

8.1 システム構成検討時

HW の手配、システム構成時に留意すべき事項について説明します。

8.1.1 CLUSTERPRO X Alert Service について

CLUSTERPRO X Alert Service のライセンスで、メール通報の機能は使用できますが、パトランプ通報の機能は使用できません。

8.1.2 JVM 監視リソースについて

- 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 監視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 監視リソースが監視できる Java VM は、JVM 監視リソースが動作中のサーバと同じサーバ内のみです。
- 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 監視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。

8.1.3 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。

8.2 CLUSTERPRO X SingleServerSafe の構成情報作成時

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。

8.2.1 インストールパス配下のフォルダやファイルについて

インストールパス配下にあるフォルダやファイルは、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 以外からフォルダ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。

8.2.2 グループリソースの非活性異常時の最終動作

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。

実際に業務で使用する際には、「何もしない」は設定しないように注意してください。

8.2.3 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。

8.2.4 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、Windows 環境で編集されたスクリプトは Shift-JIS、Linux 環境で編集されたスクリプトは EUC 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。

8.2.5 JVM 監視の設定について

- 監視対象が WebLogic の場合、JVM 監視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]
- Java Resource Agent を使用するには、『インストールガイド』 -「CLUSTERPRO X SingleServerSafe について」 -「CLUSTERPRO X SingleServerSafe の動作環境を確認する」 -「JVM 監視の動作環境」に記載している JRE(Java Runtime Environment) もしくは JDK(Java Development Kit) 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 や JDK 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。1 つのサーバに JRE と JDK の両方をインストールしている場合、どちら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。

8.2.6 システム監視の設定について

- 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 (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。

8.2.7 Windows Server 2012 以降のシステムにおけるサービス失敗時の回復操作について

Windows Server 2012 以降のシステムにおいて、サービスが失敗 (異常終了) した時に行われる回復操作として [コンピューターを再起動する] が設定されている場合、実際にサービスが失敗した際の動作が従来 (Windows Server 2008 以前) の OS 再起動からストップエラーを伴う OS 再起動へ変更されています。

回復操作として既定で [コンピューターを再起動する] が設定されている CLUSTERPRO のサービスは下記です。

- CLUSTERPRO Disk Agent サービス
- CLUSTERPRO Server サービス

- CLUSTERPRO Transaction サービス

8.2.8 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。

8.2.9 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。

8.2.10 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。

<システムドライブ>\Users\Administrator\.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* **の構成情報作成時**」 - 「*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。

8.3 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。

8.3.1 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。

8.3.2 外部連携監視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監視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。外部連携監視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。

8.3.3 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 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『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 コマンド)」を参照してください。

第 9 章

免責・法的通知

9.1 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。
- 本書に記載されている内容の著作権は、日本電気株式会社に帰属します。本書の内容の一部または全部を日本電気株式会社の許諾なしに複製、改変、および翻訳することは禁止されています。

9.2 商標情報

- CLUSTERPRO ® は、日本電気株式会社の登録商標です。
- Microsoft、Windows、Windows Server、Internet Explorer、Azure、Hyper-V は、米国 Microsoft Corporation の米国およびその他の国における登録商標です。
- 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。
- 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。
- WebOTX は、日本電気株式会社の登録商標です。
- 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。
- Apache Tomcat、Tomcat、Apache は、Apache Software Foundation 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。
- 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。
- 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。
- 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。
- PowerGres は、株式会社 SRA の商標または登録商標です。
- 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 10 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	内部バージョン 13.31 に対応
3	2026/01/30	誤記修正等
4	2026/07/13	誤記修正等

© Copyright NEC Corporation 2025. All rights reserved.