

## **ユーザーズガイド(Linux編)**

# **ESMPRO/ServerAgent for GuestOS Ver.1.5 他社機版ESMPRO/ServerAgent Ver.1.5**

- 1章 製品概要**
- 2章 監視機能**
- 3章 通報機能**
- 4章 追加機能**
- 5章 注意事項**
- 6章 よくあるご質問**

---

# 目 次

---

目 次 .....	2
本書で使う記号 .....	4
本文中の記号 .....	4
外来語のカタカナ表記 .....	4
商 標 .....	5
本書についての注意、補足 .....	6
最新版 .....	6
<b>1 章</b> 製品概要 .....	7
<b>2 章</b> 監視機能 .....	10
<b>1.</b> 監視設定 .....	11
<b>2.</b> 全般プロパティ .....	12
<b>3.</b> CPU 負荷監視 .....	14
<b>4.</b> Syslog 監視 .....	16
<b>5.</b> ファイルシステム監視 .....	18
<b>6.</b> ネットワーク(LAN)監視 .....	21
<b>7.</b> メモリ使用率監視 .....	23
<b>8.</b> ページフォルト監視 .....	25
<b>3 章</b> 通報機能 .....	27
<b>1.</b> 通報設定 .....	28
<b>2.</b> 基本設定 .....	30
<b>2.1</b> 通報手段の設定 .....	31
2.1.1 マネージャ通報(SNMP)の基本設定 .....	31
2.1.2 マネージャ通報(TCP_IP In-Band)の基本設定 .....	32
2.1.3 マネージャ通報(TCP_IP Out-of-Band)の基本設定 .....	33
<b>2.2</b> その他の設定 .....	34
<b>3.</b> 通報先リストの設定 .....	35
<b>3.1</b> 通報先 ID の設定変更 .....	36
3.1.1 通報手段がマネージャ通報(TCP_IP In-Band)の宛先設定 .....	37
3.1.2 通報手段がマネージャ通報(TCP_IP Out-of-Band)の宛先設定 .....	38
3.1.3 スケジュール設定 .....	40
<b>3.2</b> 通報先 ID の追加 .....	41
<b>4.</b> エージェントイベントの設定 .....	42
<b>4.1</b> 通報先の指定(エージェントイベント) .....	44
4.1.1 監視イベントごとに通報先を指定する方法 .....	44
4.1.2 ソースごとに通報先を一括指定する方法 .....	46
<b>5.</b> Syslog イベントの設定 .....	48
<b>5.1</b> 通報先の指定(Syslog イベント) .....	50
5.1.1 監視イベントごとに通報先を指定する方法 .....	50
5.1.2 ソースごとに通報先を一括指定する方法 .....	52

<b>5.2</b> Syslog イベントのソースの追加 .....	54
<b>5.3</b> Syslog イベントの追加 .....	57
<b>5.4</b> Syslog イベントのソースの削除 .....	58
<b>5.5</b> Syslog イベントの削除 .....	59
<b>5.6</b> Syslog イベントのテスト .....	60
<b>4 章</b> 追加機能 .....	63
<b>1.</b> コンフィグレーションツール .....	64
<b>1.1</b> esmamset コマンド .....	65
<b>1.2</b> esmsysrep コマンド .....	69
<b>2.</b> ツールについて .....	74
<b>2.1</b> 障害情報採取ツール(collectsa.sh) .....	74
<b>5 章</b> 注意事項 .....	77
<b>6 章</b> よくあるご質問 .....	86

---

## 本書で使う記号




---

---

### 本文中の記号

---

本書では 3 種類の記号を使用しています。これらの記号は、次のような意味があります。

	ソフトウェアの操作などにおいて、守らなければならないことについて示しています。
	ソフトウェアの操作などにおいて、確認しておかなければならないことについて示しています。
	知っておくと役に立つ情報、便利なことについて示しています。

---

### 外来語のカタカナ表記

---

本書では外来語の長音表記に関して、国語審議会の報告を基に告示された内閣告示に原則準拠しています。ただし、OS やアプリケーションソフトウェアなどの記述では準拠していないことがあります。誤記ではありません。

---

## 商 標

---

ESMPRO は日本電気株式会社の登録商標です。

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

Red Hat、Red Hat Enterprise Linux は、米国 Red Hat, Inc.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。

その他、記載の会社名および商品名は各社の商標または登録商標です。

なお、本文には登録商標や商標に(TM)、(R)マークは記載しておりません。

---

## 本書についての注意、補足

---

1. 本書の一部または全部を無断転載することを禁じます。
2. 本書に関しては将来予告なしに変更することがあります。
3. 弊社の許可なく複製、改変することを禁じます。
4. 本書について誤記、記載漏れなどお気づきの点があった場合、お買い求めの販売店までご連絡ください。
5. 運用した結果の影響については、4 項に関わらず弊社は一切責任を負いません。
6. 本書の説明で用いられているサンプル値は、すべて架空のものです。

この説明書は、必要なときすぐに参照できるよう、お手元に置いてください。

---

## 最新版

---

本書は作成日時点の情報をもとに作られており、画面イメージ、メッセージ、または手順などが**実際のも**  
**と異なる場合があります。**変更されているときは適宜読み替えてください。

また、ユーザズガイドをはじめとするドキュメントは、次のウェブサイトから最新版をダウンロードできます。

<https://jpn.nec.com/esmsm/download.html>

# ESMPRO/ServerAgent for GuestOS Ver.1.5 他社機版 ESMPRO/ServerAgent Ver.1.5

---

# 1

## 製品概要

ESMPRO/ServerAgent の製品概要について説明します。

## 製品概要

ESMPRO/ServerManager、ESMPRO/ServerAgent は、サーバーシステムの安定稼動と、効率的なサーバーシステム運用を目的としたサーバー管理ソフトウェアです。サーバーリソースの構成情報・稼動状況を管理し、サーバー障害を検出してシステム管理者へ通報することにより、サーバー障害の防止、障害に対する迅速な対処を可能にします。

## サーバー管理の重要性

分散化システムにおいては、サーバーの安定稼動は必要不可欠です。また、安定稼動を保証するためには、サーバー管理の負担を軽減する必要があります。

### サーバーの安定稼動

お客様の分散化システムの中核を担うサーバーの停止は、即、お客様の営業機会、利益の損失につながります。そのため、サーバーはつねに万全の状態稼動している必要があります。万が一サーバーで障害が発生した場合は、できるだけ早く障害の発生を知り、原因の究明、対処する必要があります。障害の発生から復旧までの時間が短ければ短いほど、利益(コスト)の損失を最小限にとどめることができます。

### サーバー管理の負担軽減

分散化システムにおけるサーバー管理は多くの労力を必要とします。とくに大規模な分散化システム、遠隔地にあるサーバーとなればなおさらです。サーバー管理の負担を軽減することは、すなわちコストダウン(お客様の利益)につながります。

## サーバー管理

では、サーバーをご利用のお客様がサーバー管理を行うには、どうすればよいのでしょうか？

このニーズに応えるため、サーバー管理ソフトウェア

「ESMPRO/ServerManager、ESMPRO/ServerAgent または

ESMPRO/ServerAgentService」

を Express5800 シリーズと NX7700x シリーズに標準(一部機種を除く)で添付しています。

※ESMPRO/ServerAgent の後継製品が ESMPRO/ServerAgentService となります。

ESMPRO/ServerManager、ESMPRO/ServerAgent をご利用いただくことにより、お客様のサーバーを管理できるようになります。

仮想マシン(ゲスト OS)を監視するためのサーバー管理ソフトウェア製品として、

「ESMPRO/ServerAgent for Guest OS (Windows/Linux)」

他社製サーバーを監視するためのサーバー管理ソフトウェア製品として、

「他社機版 ESMPRO/ServerAgent (Windows/Linux)」

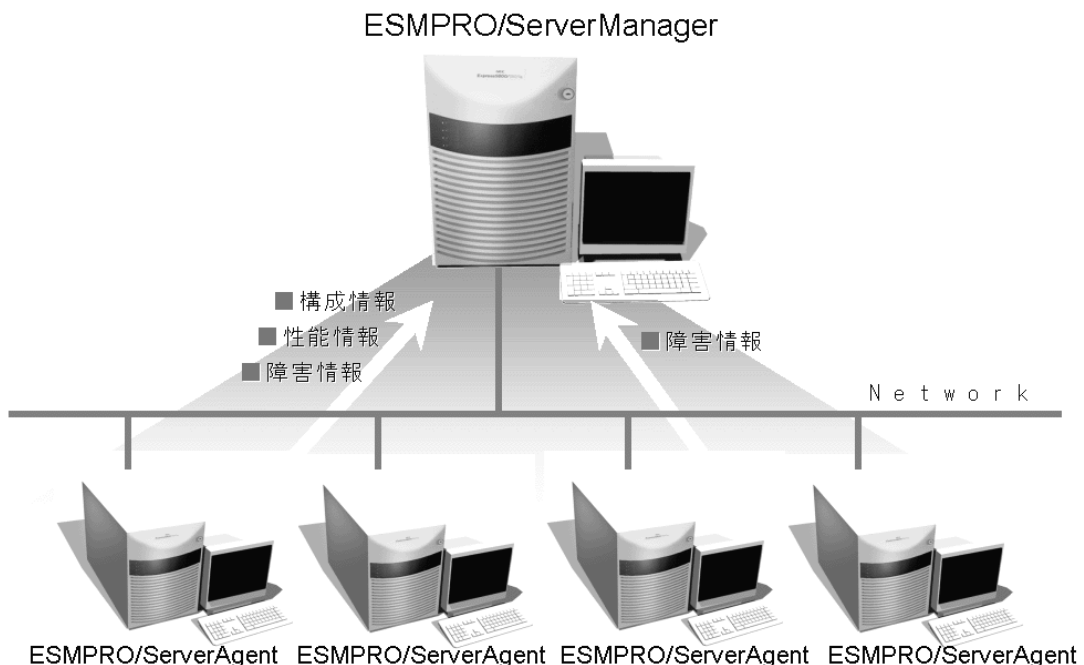
をご用意しておりますので、詳細は次のウェブサイトを参照してください。

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



## ESMPRO/ServerManager、ESMPRO/ServerAgent とは？

ESMPRO/ServerManager、ESMPRO/ServerAgent は、ネットワーク上のサーバーを管理・監視するサーバー管理ソフトウェアです。本製品を導入することにより、サーバーの構成情報・性能情報・障害情報をリアルタイムに取得・管理・監視できるほか、アラート通報機能により障害の発生を即座に知ることができます。



## ESMPRO/ServerManager、ESMPRO/ServerAgent の利用効果

ESMPRO/ServerManager、ESMPRO/ServerAgent は、多様化・複雑化するシステム環境におけるさまざまなニーズに対して十分な効果を発揮します。

### サーバー障害を検出

ESMPRO/ServerAgent は、サーバーのさまざまな障害情報を収集し、異常を判定します。サーバーで異常を検出したとき、ESMPRO/ServerManager へアラート通報します。

### サーバー障害を防止

ESMPRO/ServerAgent は、障害の予防対策として、事前に障害の発生を予測する予防保守機能をサポートしています。筐体内温度上昇や、ファイルシステムの空き容量、ハードディスクドライブ劣化などを事前に検出できます。

### サーバー稼動状況を管理

ESMPRO/ServerAgent は、サーバーの詳細なハードウェア構成情報、性能情報を取得できます。取得した情報は ESMPRO/ServerManager をととして参照できます。

### 分散したサーバーを一括管理

ESMPRO/ServerManager は、ネットワーク上に分散したサーバーを効率よく管理できる GUI インタフェースを提供します。

詳細は、次のウェブサイトからダウンロードできる ESMPRO サーバ管理ガイドを参照してください。

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

ダウンロード > ドキュメント

# ESMPRO/ServerAgent for GuestOS Ver.1.5 他社機版 ESMPRO/ServerAgent Ver.1.5

# 2

## 監視機能

ESMPRO/ServerAgent の監視機能について説明します。

1. 監視設定
2. 全般プロパティ
3. CPU 負荷監視
4. Syslog 監視
5. ファイルシステム監視
6. ネットワーク(LAN)監視
7. メモリ使用率監視
8. ページフォルト監視

# 1. 監視設定

本章では ESMPro/ServerAgent が提供する監視機能を説明します。各監視機能の設定は、コントロールパネル(ESMagntconf)で変更します。



テキストモード(runlevel 3)では、日本語が正しく表示できません。そのため、コントロールパネル(ESMagntconf)を日本語で表示させるためには、以下の手順を実行してください。

1. ネットワーク経由(ssh コマンド)で別の日本語端末からログインします。
2. root 権限がないときは、root ユーザーに昇格します。

```
# su -
```

3. LANG 環境変数を確認します。

```
# echo $LANG
```

4. LANG 環境変数が日本語(ja\_JP.~)ではない場合は、一時的に日本語に変更します。

```
# export LANG=ja_JP.UTF-8
```

5. コントロールパネルを起動します。

```
# cd /opt/nec/esmpro_sa/bin
```

```
# ./ESMagntconf
```

6. 作業終了後に、手順 2. で確認した LANG 環境変数に変更します。



コントロールパネルを複数のコンソールから起動しないでください。後から実行したコンソールからは起動できず、『レジストリの読み込みに失敗しました。』と表示します。

コントロールパネル(ESMagntconf)の起動方法は以下のとおりです。

1. root 権限のあるユーザーでログインします。
2. コントロールパネルが格納されているディレクトリに移動します。

```
# cd /opt/nec/esmpro_sa/bin
```
3. コントロールパネルを起動します。

```
# ./ESMagntconf
```



コントロールパネル(ESMagntconf)のメイン画面

## 2. 全般プロパティ

### 機 能

ESMPRO/ServerManager から SNMP を利用した設定やシャットダウン／リブート、使用するコミュニティ一名の設定、ラックマウント機種でのラック名の登録、筐体識別機能が使用できます。

### 設 定

コントロールパネル(ESMagntconf)の「全般」を選択して表示される[全般プロパティ]画面にて、設定ができます。

全般プロパティ

SNMP Setting

☒ マネージャからの SNMP での設定を許可する

☐ マネージャからのリモートシャットダウン/リブートを許可する

SNMP Community public

Rack Setting

Rack Name

Chassis Identify <Start> <Stop>

ok cancel

#### マネージャからの SNMP での設定を許可する

ESMPRO/ServerManager からの本機のしきい値変更等の動作設定の更新を許可するか、許可しないかを<スペース>キーで設定できます。許可するときは、チェックボックスをチェックします。

#### マネージャからのリモートシャットダウン/リブートを許可する

ESMPRO/ServerManager から本機をリモートシャットダウンまたはリモートリブートすることを許可するか、許可しないかを<スペース>キーで設定できます。許可するときは、チェックボックスをチェックします。「マネージャからの SNMP での設定を許可する」が許可されていないと「マネージャからのリモートシャットダウン/リブートを許可する」の許可はできません。

### **SNMP Community**

ESMPRO/ServerAgent がローカルマシンの情報を取得するときや SNMP トラップを送信するとき使用する SNMP コミュニティー名を選択します。リストに表示されるコミュニティ名は、SNMP 設定ファイル(snmpd.conf)に登録されているコミュニティ名です。localhost に対して「READ」または「READ WRITE」の権限を与えているコミュニティ名を<↑>か<↓>キーで選択してください。「READ」権限は、「マネージャからの SNMP での設定を許可する」を許可しない設定にした場合と同じ状態となり、ESMPRO/ServerManager から本機へのしきい値変更等ができません。

### **Rack Name**

本製品では未サポートです。

### **Chassis Identify(筐体識別)**

本製品では未サポートです。

### **[ok]ボタン**

設定した情報を登録し、この画面を閉じます。

### **[cancel]ボタン**

設定した情報を登録せずに、この画面を閉じます。

## 3. CPU 負荷監視

### 機 能

CPU 負荷監視機能は、CPU の高負荷状態を検出すると、syslog へ検出情報の記録と ESMPRO/ServerManager へ通報(アラート通報)します。ESMPRO/ServerManager を参照すると、異常や警告状態の CPU を確認できます。CPU の負荷状態は、“個々の CPU”と“CPU トータル”の 2 種類の単位で監視できます。そのため、個々の CPU にとらわれず、本機を 1 つのパッケージとして監視できます。

既定値では CPU の負荷率は、監視しません。CPU 負荷率を監視するときは設定を変更します。CPU 負荷率のしきい値は、基本的に変更する必要ありません。任意の値に設定を変更することもできますが、変更されたしきい値によっては頻繁に CPU 負荷に関するアラートが通報されることも考えられます。CPU 負荷率のしきい値を変更するとき、システムの負荷によってアラートが頻繁に通報されないように、しきい値を設定してください。

CPU 負荷率を監視するときの既定値は以下のとおりです。

監視間隔：10 秒

監視対象：1 分間の負荷率

監視間隔である 10 秒毎にその時点での使用率を取得し、監視対象である 1 分間の平均値[6(回)=60(対象秒)/10(間隔秒)]を「現在の使用率」として、しきい値と比較します。「現在の使用率」としきい値の比較は、ESMPRO/ServerAgent で設定した監視間隔である 10 秒毎に行い、状態(正常/警告/異常)に変化があったときは通報します。監視対象を“1 分間の負荷率”から“5 分間の負荷率”に変更した場合は、監視対象である 1 分間の平均値[30(回)=300(対象秒)/10(間隔秒)]を「現在の使用率」とし、しきい値と比較します。

### 設 定

コントロールパネル(ESMagntconf)の「CPU 負荷」を選択して表示される[CPU 負荷]画面にて、CPU 負荷監視機能の「監視間隔」と「監視対象」、「しきい値」が設定できます。

	しきい値	開放値
異常	100	97
警告	95	92

### 監視間隔

CPU 負荷率のデータを採取する間隔(秒)が設定できます。

1、2、3、4、5、6、10、12、15、20、30、60 のいずれかの監視間隔を<↑>か<↓>キーで選択できます。  
既定値は 10 秒です。

### 監視対象

監視の対象とする負荷率の種類が指定できます。

1 分間、5 分間、30 分間、1 時間、1 日間、1 週間の負荷率を<↑>か<↓>キーで選択できます。  
既定値は「1 分間の負荷率」です。

### CPU

監視設定の参照または設定する CPU を<↑>か<↓>キーで選択できます。

### 監視する

選択している CPU の負荷率監視の有効(チェックあり)と無効(チェックなし)を<スペース>キーで設定します。このチェックボックスをチェックしているときに「しきい値」と「開放値」を設定できます。  
既定値は「監視しない」です。

### しきい値 / 開放値

異常と警告の「しきい値」と「開放値」が設定できます。

0 から 100 の整数値で、次の大小関係を満たす必要があります。

$100 \geq \text{しきい値(異常)} > \text{開放値(異常回復)} > \text{しきい値(警告)} > \text{開放値(警告回復)} \geq 0$

既定値は次のとおりです。

監視項目名	しきい値(異常)	開放値(異常回復)	しきい値(警告)	開放値(警告回復)
CPU 負荷率(%)	100	97	95	92

### [ok]ボタン

設定した情報を登録し、この画面を閉じます。設定の変更は、次の監視間隔で有効になります。

### [cancel]ボタン

設定した情報を登録せずに、この画面を閉じます。

## 4. Syslog 監視

### 機 能

Syslog 監視機能は、Syslog イベントで設定されたキーワードが監視対象のファイルに記録されると、ESMPRO/ServerManager へ通報(アラート通報)します。Syslog イベントは、ESMPRO/ServerAgent インストール時にあらかじめ登録している Syslog イベント以外に、システム環境に応じた新たなソース、イベントを追加や削除できます。Syslog イベントの追加や削除方法は、本書の 3 章(5. Syslog イベントの設定)を参照してください。

### 既定監視対象

監視対象となる syslog は、"/var/log/messages"となり変更はできません。

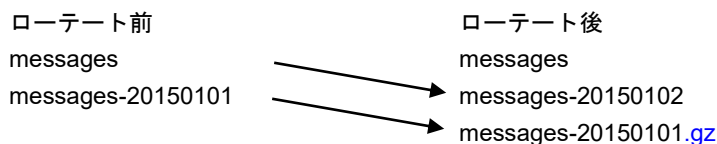
また、監視対象となる syslog ローテート後のファイル名は、/etc/logrotate.conf に"dateext"が定義されていない : /var/log/messages.n [n=1, 2, 3, ...]

定義されている : /var/log/messages-YYYYMMDD [YYYY=西暦年, MM=月, DD=日]

であり、他の命名規則となっているとき、Syslog 監視機能では監視できません。

また、/etc/logrotate.d/syslog に"compress"(圧縮する)が定義されているとき、ローテート後のファイルはテキストではないため、Syslog 監視機能では監視できません。

Red Hat Enterprise Linux 8 以降では、既定値で"dateext"が定義されています。"compress"は定義されていませんが、ローテートしたファイル(messages-YYYYMMDD)は gz 形式(messages-YYYYMMDD.gz)に圧縮されますので、Syslog 監視機能では監視できません。ただし、ESMPRO/ServerAgent が停止していない場合は gz 形式となる前に syslog を監視しているため、影響はありません。



### 追加監視対象

"/var/log/messages"の文字列を含まないファイルを監視対象として、1 つ追加できます。既定監視対象をチェックした後、追加監視対象のファイルをチェックするため、監視間隔のタイミングにより、時系列が逆転するときがあります。追加することのできる監視対象は、syslog と同じ以下のフォーマットで出力されるファイルのみとなり、監視対象ファイルの一行目は監視しません。

%b %d %H:%M:%S %HOSTNAME% %MESSAGE%

%b ロケールによる省略形の月の名前 (Jan~Dec), %d 日(月内通算日数 2 桁) (1~31)

%H 時 (00~23), %M 分 (00~59), %S 秒 (00~59)

%HOSTNAME% ホスト名, %MESSAGE% メッセージ (通報内容)

ログローテートするファイルを指定した場合は、ログローテート後のファイルは監視対象とはならないため、ログのファイル名の切り替わるタイミングで、追加監視対象ファイルの一部が監視できないときがあります。

### ファイル監視対象

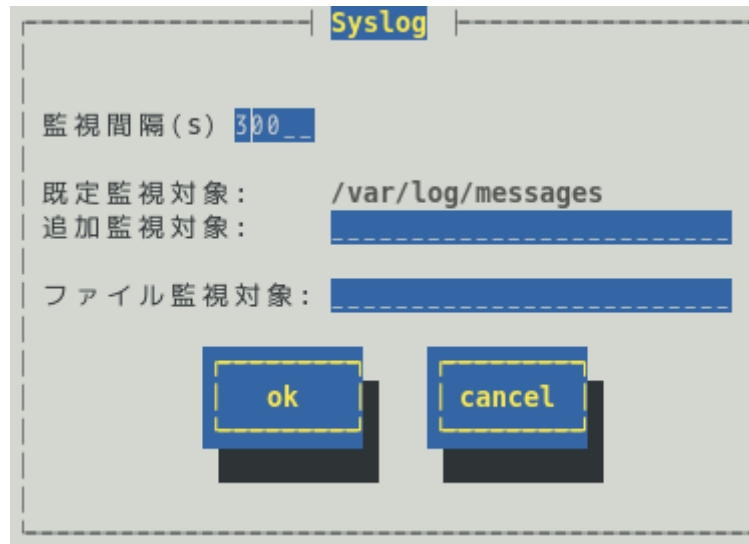
"/var/log/messages"の文字列を含まないファイルを監視対象として、1 つ追加できます。既定監視対象と追加監視対象をチェックした後、ファイル監視対象のファイルをチェックするため、監視間隔のタイミングにより、時系列が逆転するときがあります。追加することのできる監視対象のファイルフォーマットに指定はありません。

ログローテートするファイルを指定した場合は、ログローテート後のファイルは監視対象とはならないため、ファイル監視対象のファイルの一部が監視できないときがあります。



## 設 定

コントロールパネル(ESMagntconf)の「Syslog」を選択して表示される[Syslog]画面にて、Syslog 監視の「監視間隔」、「既定監視対象」、「追加監視対象」、「ファイル監視対象」が設定できます。「追加監視対象」と「ファイル監視対象」にて"/var/log/messages"の文字列を含まないファイルを監視対象に設定できます。

A screenshot of a Syslog configuration window. The window has a title bar with the text 'Syslog'. Inside, there are four input fields: '監視間隔 (s)' with a value of '300', '既定監視対象:' with a value of '/var/log/messages', '追加監視対象:' which is empty, and 'ファイル監視対象:' which is also empty. At the bottom of the window are two buttons labeled 'ok' and 'cancel'.

### 監視間隔(s)

Syslog 監視機能の監視する間隔(秒)が設定できます。  
既定値は 300 秒です。設定可能範囲は 10～3600 秒です。

### 既定監視対象

"/var/log/messages"からの変更、削除はできません。  
詳細は Syslog 監視の機能にある既定監視対象を参照してください。

### 追加監視対象

"/var/log/messages"の文字列を含まないファイルを監視対象として、パスの長さが 255 バイト以下となる絶対パスで設定できます。相対パスでの設定はできません。追加することのできる監視対象のファイルフォーマットは syslog と同じフォーマットです。詳細は Syslog 監視の機能にある追加監視対象を参照してください。既定値は空白で、追加監視対象は設定されていません。

### ファイル監視対象

"/var/log/messages"の文字列を含まないファイルを監視対象として、パスの長さが 255 バイト以下となる絶対パスで設定できます。相対パスでの設定はできません。追加することのできる監視対象のファイルフォーマットに指定はありません。詳細は Syslog 監視の機能にあるファイル監視対象を参照してください。既定値は空白で、ファイル監視対象は設定されていません。

### [ok]ボタン

設定した情報を登録し、この画面を閉じます。設定の変更は、次の監視間隔で有効になります。

### [cancel]ボタン

設定した情報を登録せずに、この画面を閉じます。

---

## 5. ファイルシステム監視

---

### 機 能

ファイルシステム監視機能は、OS にマウントされているファイルシステムの空き容量不足を検出すると、syslog へ検出情報の記録と ESMPRO/ServerManager へ通報(アラート通報)します。  
ESMPRO/ServerManager を参照すると、空き容量の不足したマウントポイントを確認できます。

ファイルシステム監視機能は、以下の条件をすべて満たすとき監視対象となります。

- ・ ファイルシステムのデバイスタイプ※1 が以下のとき

ide, rd, sd, sr, md, ramdisk, dac960, DAC960, device-mapper, dd, blkext, virtblk

※1 デバイスタイプは、マウントポイント(/etc/mntab)を確認し、ディスク I/O 情報(/proc/diskstats)と、ブロックデバイス(/proc/devices)から判断します。マウントポイントは、/etc/mntab の順番に準拠します。  
バインドマウントされた場合は、バインドマウントされた情報が優先されます。  
以下の例では、sda1 と sda2 のデバイスタイプは、"sd"です。sda3 の/home はバインドマウントされ、ファイルシステムのタイプが none となっており、監視対象外となります。

[/etc/mntab 抜粋]

```
/dev/sda1 /boot ext3 rw 0 0
/dev/sda2 / ext3 rw 0 0
/dev/sda3 /home ext3 rw 0 0
/home /home none rw,bind 0 0
```

[/proc/diskstats 抜粋]

```
8    1 sda1 127 984 13844 331 6 1 14 496 0 770 827
8    2 sda2 24361 15137 1112602 115034 10027 25261 282312 195758 ...
```

[/proc/devices 抜粋]

```
Block devices:
1 ramdisk
8 sd
```

- ・ ファイルシステムのタイプ(/etc/mntab 内に記載)が以下のとき

affs, BtrFS, coda, ext, ext2, ext3, ext4, hfs, hpfs, jfs, minix, msdos, ntfs, reiserfs, sysv, ufs, umsdos, vfat, xfs, xiafs

以下のファイルシステムの動作は検証済みです。

BtrFS, ext2, ext3, ext4, jfs, minix, msdos, ntfs, reiserfs, vfat, xfs

以下のファイルシステムの動作は未検証です。サポートしているカーネルが古いファイルシステムも含まれており、過去のバージョンでは動作を検証済みであるため、論理的には監視対象となります。

affs, coda, ext, hfs, hpfs, sysv, ufs, umsdos, xiafs

- ・ ファイルシステムの容量が 100MB 以上のとき

## 設 定

コントロールパネル(ESMagntconf)の「ファイルシステム」を選択して表示される[ファイルシステム]画面にて、ファイルシステム監視機能の「監視間隔」などの監視設定ができます。

ファイルシステム

監視間隔 (s) 60 (範囲: 1-3600 s) 既定値

ファイルシステム / 容量 20630MB

( ) 監視しない  
(\* ) 監視する

警告 2063 MB 既定値  
異常 206 MB

ok cancel

### 監視間隔(s)

監視する間隔(秒)が設定できます。  
既定値は 60 秒です。設定可能範囲は 1～3600 秒です。

### [既定値]ボタン

ボタンを押すと、監視間隔の既定値が設定されます。

### ファイルシステム

監視をするファイルシステムを<↑>か<↓>キーで選択できます。

### 監視しない

ファイルシステム監視をしないときは、<スペース>キーで選択してチェックします。  
既定値は“監視する”です。

### 監視する

ファイルシステム監視をするときは、<スペース>キーで選択してチェックします。  
このチェックボックスをチェックしている時のみ、警告と異常のしきい値を設定できます。  
既定値は“監視する”です。

### しきい値

「警告」と「異常」の「しきい値」が設定できます。  
単位は MB で、次の大小関係を満たす必要があります。  
全容量 > 警告 > 異常 > 0  
「警告」の既定値は全容量の約 10%、「異常」の既定値は全容量の約 1%です。

**[既定値]ボタン**

ボタンを押すと、しきい値の既定値が設定されます。

**[ok]ボタン**

設定した情報を登録し、この画面を閉じます。設定の変更は、次の監視間隔で有効になります。

**[cancel]ボタン**

設定した情報を登録せずに、この画面を閉じます。

## 6. ネットワーク(LAN)監視

### 機 能

ネットワーク(LAN)監視機能は、監視間隔中に発生した破棄パケットやエラーパケットが設定されたしきい値を超えたとき、syslog へ検出情報の記録と ESMPRO/ServerManager へ通報(アラート通報)します。異常を検出したあと、すぐに回復しているときは問題ありませんが、回復しなかったときや異常が頻繁に発生するときは、ネットワーク環境(ハードウェアも含め)の確認や、ネットワークの負荷を分散してください。

ネットワーク(LAN)監視機能は、監視間隔中に発生した送受信パケット数に対する割合で判断しているので、一時的なネットワーク負荷により検出する場合があります。

また、Red Hat Enterprise Linux 8 以降からプロトコル不明などのパケットがドロップした数も受信破棄パケット数として計上されることから、監視設定の既定値は無効としています。

■ネットワーク(LAN)監視を有効にするときは、ESMlan の設定を変更した後、ESMlan を起動します。

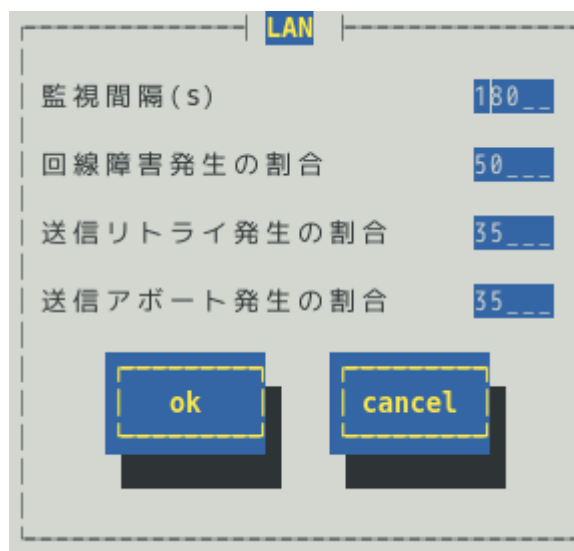
```
# systemctl enable ESMlan.service
# systemctl start ESMlan.service
```

■ネットワーク(LAN)監視設定を無効にするときは、ESMlan の設定を変更した後、ESMlan を停止します。

```
# systemctl disable ESMlan.service
# systemctl stop ESMlan.service
```

### 設 定

コントロールパネル(ESMagntconf)の「LAN」を選択して表示される[LAN]画面にて、ネットワーク(LAN)監視機能の「監視間隔」と「しきい値」が設定できます。



#### 監視間隔

監視する間隔(秒)が設定できます。

既定値は 180 秒です。

設定可能範囲は 1～3600 秒です。

#### 回線障害発生の割合

監視周期あたりの送受信パケット中の回線障害に繋がるエラーが発生した割合の「しきい値」が設定できます。エラーを検出した時、ただちに通報させたいときは、0 を指定してください。

既定値は 50%です。

設定可能範囲は 0～100%です。

回線障害は、ネットワークケーブルが外れているときや HUB の電源が入っていない時などに発生します。

各エラーは、以下のような原因で発生します。

エラー	原因
アライメントエラー	サイズがオクテット(8)単位でない受信パケット
FCS エラー	チェックサムでエラーが出た受信パケット
キャリアなし	パケット送信時の回線確認でエラー

#### 送信リトライ発生の割合

監視周期あたりの総送信パケット中のパケットの衝突、遅延で送信されたパケットの割合の「しきい値」が設定できます。送信リトライは、本機の送受信が高負荷状態の時などに発生します。

既定値は 35%です。

設定可能範囲は 10～50%です。

#### 送信アボート発生の割合

監視周期あたりの総送信パケット中の超過衝突等により、破棄されたパケットの割合の「しきい値」が設定できます。送信アボートは、本機の送受信が高負荷状態の時などに発生します。

既定値は 35%です。

設定可能範囲は 10～50%です。

#### [ok]ボタン

設定した情報を登録し、この画面を閉じます。設定の変更は、次の監視間隔で有効になります。

#### [cancel]ボタン

設定した情報を登録せずに、この画面を閉じます。

## 7. メモリ使用率監視

### 機 能

メモリ使用率監視機能は、メモリ使用量からメモリ使用率を算出し、警告・異常状態を検出すると、syslogへ検出情報の記録と ESMPRO/ServerManager へ通報(アラート通報)します。

既定値ではメモリ使用率は監視しません。メモリ使用率を監視するときは設定を変更します。メモリ使用率のしきい値は、基本的に変更する必要ありません。任意の値に設定を変更することもできますが、変更されたしきい値によっては頻繁にメモリ使用率に関するアラートが通報されることも考えられます。メモリ使用率のしきい値を変更するとき、メモリの使用状況によってアラートが頻繁に通報されないように、しきい値を設定してください。

監視間隔毎にメモリ使用量からメモリ使用率を算出します。しきい値と比較して、状態(正常/警告/異常)の変化がサンプリング回数に達したときは通報します。

以下の例は、サンプリング回数が6回(既定値)、異常しきい値は99%(既定値)、警告しきい値は95%(既定値)の設定で、メモリ使用率(下表では使用率の行)の変化にあわせ状態を判断します。

No.	1	2	3	4	5	6	7	8	9	10
使用率	40%	97%	97%	100%	100%	100%	100%	100%	100%	97%
異常				①	②	③	④	⑤	⑥	→
警告		①	②	③	④	⑤	⑥	→	↑	①
正常	①	→	→	→	→	→	↑			
状態	正常	正常	正常	正常	正常	正常	警告	警告	異常	異常

11	12	13	14	15	16	17	18	19	20
97%	97%	97%	40%	40%	40%	40%	40%	40%	40%
→	→	→	→	↓					
②	③	④	⑤	⑥	→	→	→	↓	
			①	②	③	④	⑤	⑥	→
異常	異常	異常	異常	警告	警告	警告	警告	正常	正常

#### 【正常状態から異常状態への変化】

- No.2：メモリ使用率は警告値(97%)ですが、サンプリング回数に達していないため、状態は変化しません。
- No.4：メモリ使用率は異常値(100%)ですが、サンプリング回数に達していないため、状態は変化しません。
- No.7：警告(より高い)状態が、サンプリング回数に達したため、警告状態に変化します。
- No.9：異常状態が、サンプリング回数に達したため、異常状態に変化します。

#### 【異常状態から正常状態への変化】

- No.10：メモリ使用率は警告値(97%)ですが、サンプリング回数に達していないため、状態は変化しません。
- No.14：メモリ使用率は正常値(40%)ですが、サンプリング回数に達していないため、状態は変化しません。
- No.15：警告(より低い)状態が、サンプリング回数に達したため、警告状態に変化します。
- No.19：正常状態が、サンプリング回数に達したため、正常状態に変化します。

## 設 定

コントロールパネル(ESMagntconf)の「メモリ」を選択して表示される[メモリ使用率]画面にて、メモリ使用率監視機能の「監視間隔」と「サンプリング回数」、「しきい値」が設定できます。

メモリ使用率

監視間隔(s) 150  
範囲:1-900 s

サンプリング回数 6  
範囲:1-10

[ ] 監視する

異常(%) 99 警告(%) 95

ok cancel

### 監視間隔

メモリ使用率を監視する間隔(秒)が設定できます。  
設定範囲は1～900 秒です。既定値は 150 秒です。

### サンプリング回数

状態が変化したことを検出に必要なサンプリング回数が設定できます。  
設定範囲は1～10 回です。既定値は 6 回です。

### 監視する

メモリ使用率監視の有効(チェックあり)と無効(チェックなし)を<スペース>キーで設定します。  
既定値は「監視しない」です。

### しきい値

「異常(%)」と「警告(%)」のしきい値が設定できます。  
単位は%で、次の大小関係を満たす必要があります。  
 $100 \geq \text{警告} > \text{異常} \geq 0$   
設定範囲は0～100%です。既定値は「異常(%)」が 99%、「警告(%)」が 95%です。

### [ok]ボタン

設定した情報を登録し、この画面を閉じます。設定の変更は、次の監視間隔で有効になります。

### [cancel]ボタン

設定した情報を登録せずに、この画面を閉じます。



## 8. ページフォルト監視

### 機 能

ページフォルト監視機能は、ページフォルトの警告・異常状態を検出すると、syslog へ検出情報の記録と ESM/PRO/ServerManager へ通報(アラート通報)します。

既定値ではページフォルトは監視しません。ページフォルトを監視するときは設定を変更します。任意の値に設定を変更することもできますが、変更されたしきい値によっては頻繁にページフォルトに関するアラートが通報されることも考えられます。ページフォルトのしきい値を変更するとき、システムの負荷などによってアラートが頻繁に通報されないように、しきい値を設定してください。

監視間隔毎にページフォルト数から 1 秒あたりのページフォルト数を算出します。しきい値と比較して、状態(正常/警告/異常)の変化がサンプリング回数に達したときは通報します。

以下の例は、サンプリング回数が 6 回(既定値は 10 回)、異常しきい値は 2000(既定値)、警告しきい値は 1600(既定値)の設定で、1 秒あたりのページフォルト数(下表ではフォルト数)の変化にあわせ状態を判断します。

No.	1	2	3	4	5	6	7	8	9	10
フォルト数	1400	1800	1800	2200	2200	2200	2200	2200	2200	1800
異常				①	②	③	④	⑤	⑥	→
警告		①	②	③	④	⑤	⑥	→	↑	①
正常	①	→	→	→	→	→	↑			
状態	正常	正常	正常	正常	正常	正常	警告	警告	異常	異常

11	12	13	14	15	16	17	18	19	20
1800	1800	1800	1400	1400	1400	1400	1400	1400	1400
→	→	→	→	↓					
②	③	④	⑤	⑥	→	→	→	↓	
			①	②	③	④	⑤	⑥	→
異常	異常	異常	異常	警告	警告	警告	警告	正常	正常

#### 【正常状態から異常状態への変化】

No.2 : ページフォルト数は警告値(1800)ですが、サンプリング回数に達していないため、状態は変化しません。

No.4 : ページフォルト数は異常値(2200)ですが、サンプリング回数に達していないため、状態は変化しません。

No.7 : 警告(より高い)状態が、サンプリング回数に達したため、警告状態に変化します。

No.9 : 異常状態が、サンプリング回数に達したため、異常状態に変化します。

#### 【異常状態から正常状態への変化】

No.10 : ページフォルト数は警告値(1800)ですが、サンプリング回数に達していないため、状態は変化しません。

No.14 : ページフォルト数は正常値(1400)ですが、サンプリング回数に達していないため、状態は変化しません。

No.15 : 警告(より低い)状態が、サンプリング回数に達したため、警告状態に変化します。

No.19 : 正常状態が、サンプリング回数に達したため、正常状態に変化します。

## 設 定

コントロールパネル(ESMagntconf)の「ページフォルト」を選択して表示される[ページフォルト]画面にて、ページフォルト監視機能の「監視間隔」と「サンプリング回数」、「しきい値」が設定できます。

ページフォルト

監視間隔 (s) 60  
範囲: 1-600 s

サンプリング回数 10  
範囲: 1-20

☐ 監視する

異常 (Pages/Sec) 2000 警告 (Pages/Sec) 1600

ok cancel

### 監視間隔

ページフォルトを監視する間隔(秒)が設定できます。  
設定範囲は 1～600 秒です。既定値は 60 秒です。

### サンプリング回数

状態が変化したことを検出に必要なサンプリング回数が設定できます。  
設定範囲は 1～20 回です。既定値は 10 回です。

### 監視する

ページフォルト監視の有効(チェックあり)と無効(チェックなし)を<スペース>キーで設定します。  
既定値は「監視しない」です。

### しきい値

「異常」と「警告」のしきい値が設定できます。  
単位は回(Pages/Sec)で、次の大小関係を満たす必要があります。  
 $20000 \geq \text{警告} > \text{異常} \geq 1$   
設定範囲は 1～20000 です。既定値は「異常」が 2000、「警告」が 1600 です。

### [ok]ボタン

設定した情報を登録し、この画面を閉じます。設定の変更は、次の監視間隔で有効になります。

### [cancel]ボタン

設定した情報を登録せずに、この画面を閉じます。

# ESMPRO/ServerAgent for GuestOS Ver.1.5 他社機版 ESMPRO/ServerAgent Ver.1.5

---

# 3

## 通報機能

ESMPRO/ServerAgent の通報機能について説明します。

1. 通報設定
2. 基本設定
3. 通報先リストの設定
4. エージェントイベントの設定
5. Syslog イベントの設定

# 1. 通報設定

本章では、どのようなイベントをどこに通報先にいつ通報するかといった通報設定の機能を説明しています。通報設定は、コントロールパネル(ESMamsadm)で設定します。

マネージャ通報には、次の3種類があります。

1. マネージャ通報(SNMP)

ESMPRO/ServerAgent 独自に SNMP Trap(UDP トラップ)を送信します。ESMPRO/ServerManager 以外の「SNMP Trap 受信をサポートしているマネージャー」にも通報できます。

2. マネージャ通報(TCP\_IP In-Band)

TCP/IP を利用して、ESMPRO/ServerManager に通報するため、信頼性の高い通報をする場合に使用します。

3. マネージャ通報(TCP\_IP Out-of-Band)

TCP\_IP In-Band と同様に TCP/IP を利用して、ESMPRO/ServerManager に通報しますが、PPP(Point to Point Protocol)を介して通報します。したがって、ESMPRO/ServerAgent と ESMPRO/ServerManager が遠隔地に存在し、公衆回線を通して、通報する場合(Wide Area Network 環境)に使用します。また、ダイヤルアップ接続となるため、ESMPRO/ServerAgent 側、ESMPRO/ServerManager 側のそれぞれにモデムと電話回線が必要となります。



チェック

テキストモード(runlevel 3)では、日本語が正しく表示できません。そのため、コントロールパネル(ESMamsadm)を日本語で表示させるためには、以下の手順を実行してください。

1. ネットワーク経由(ssh コマンドなど)で別の日本語端末からログインします。

2. root 権限がないときは、root ユーザーに昇格します。

```
# su -
```

3. LANG 環境変数を確認します。

```
# echo $LANG
```

4. LANG 環境変数が日本語(ja\_JP.~)ではない場合は、一時的に日本語に変更します。

```
# export LANG=ja_JP.UTF-8
```

5. コントロールパネルを起動します。

```
# cd /opt/nec/esmpo_sa/bin
```

```
# ./ESMagntconf
```

6. 作業終了後に、手順 2. で確認した LANG 環境変数に変更します。



ヒント

コントロールパネルを複数のコンソールから起動しないでください。後から実行したコンソールからは起動できず、『レジストリの読み込みに失敗しました。』と表示します。

コントロールパネル(ESMamsadm)の起動方法は以下のとおりです。

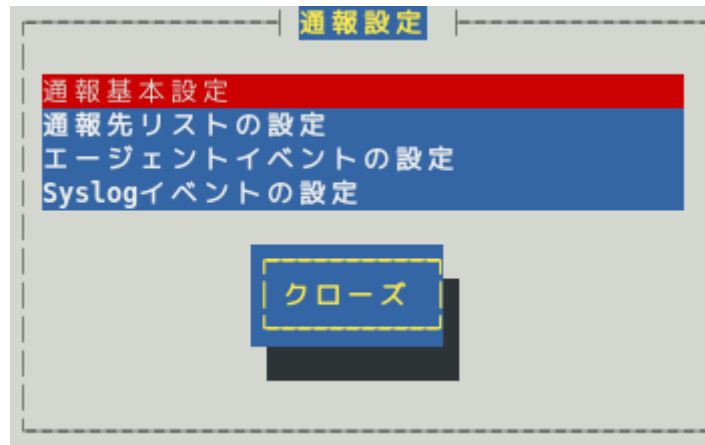
1. root 権限のあるユーザーでログインします。

2. コントロールパネルが格納されているディレクトリに移動します。

```
# cd /opt/nec/esmpo_sa/bin
```

3. コントロールパネルを起動します。

```
# ./ESMamsadm
```



コントロールパネル(ESMamsadm)のメイン画面

■ 通報手段として SNMP による通報をするとき

ESMPRO/ServerAgent のインストール時にあらかじめ、監視イベントに対して SNMP 通報手段による通報設定がひととおり設定済みとなっています。通報基本設定にて、通報先となる ESMPRO/ServerManager が導入されているマシンの IP アドレスを設定するだけで、通報準備が整います。SNMP による通報をするときの設定につきましては、本章(2.1.1. マネージャ通報(SNMP)の基本設定)を参照してください。

■ 通報手段として SNMP 以外による通報をするとき

以下の流れにしたがって設定してください。

1. 通報の基本設定をします。(通報基本設定)

TCP\_IP In-Band による通報をするときの基本設定は、本章(2.1.2. マネージャ通報(TCP\_IP In-Band)の基本設定)を参照してください。

TCP\_IP Out-of-Band による通報をするときの基本設定は、本章(2.1.3. マネージャ通報(TCP\_IP Out-of-Band)の基本設定)を参照してください。

2. 通報の宛先リストを設定します。(通報先リストの設定)

TCP\_IP In-Band による通報をするときの宛先設定は、本章(3.1.1. 通報手段がマネージャ通報(TCP\_IP In-Band)の宛先設定)を参照してください。

TCP\_IP Out-of-Band による通報をするときの宛先設定は、本章(3.1.2. 通報手段がマネージャ通報(TCP\_IP Out-of-Band)の宛先設定)を参照してください。

3. 監視イベントの設定、および、監視イベントへの通報先を結びつけます。

エージェントイベントとは、ESMPRO/ServerAgent が検出した故障の監視イベントを指します。

エージェントイベントの設定は、本章(4. エージェントイベントの設定)を参照してください。

Syslog イベントとは、Syslog 監視機能により検出した故障の監視イベントを指します。

Syslog イベントの設定は、本章(5. Syslog イベントの設定)を参照してください。

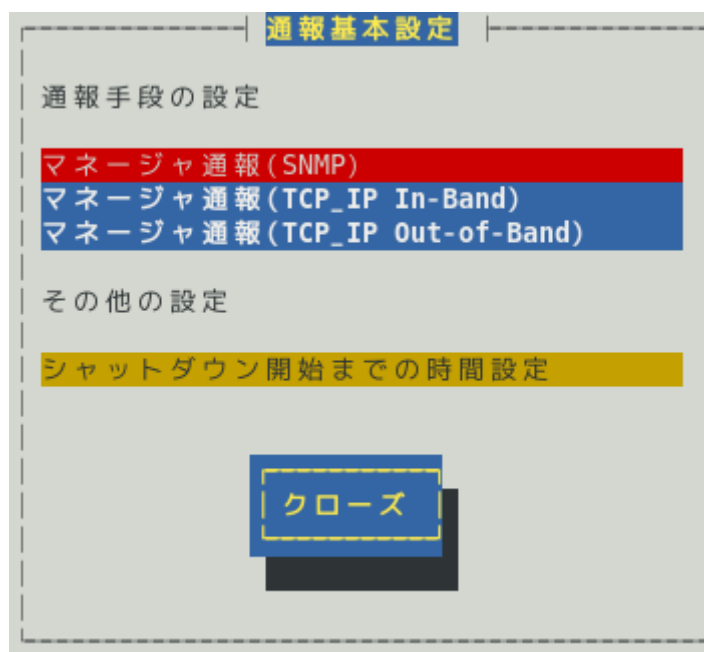
## 2. 基本設定

### 機 能

通報手段の有効/無効、マネージャ通報(SNMP)の Trap 送信先、エラー発生時のシャットダウン機能の有効/無効、シャットダウン開始までの時間を設定できます。通報手段を無効にすると、すべての監視イベントに設定されている当該通報手段による通報されなくなります。シャットダウンを無効にすると、ESMPRO/ServerManager からのリモートシャットダウン/リブートも無効となります。また、各監視イベントの通報後動作でシャットダウン/リブートが設定されているときも、通報発生後のシャットダウン/リブートが実行されなくなります。

### 設 定

コントロールパネル(ESMamsadm)の「通報基本設定」を選択して表示される[通報基本設定]画面にて、通報の基本設定ができます。



#### 通報手段一覧

通報手段が表示されます。

#### その他の設定

設定項目が表示されます。

#### [クローズ]ボタン

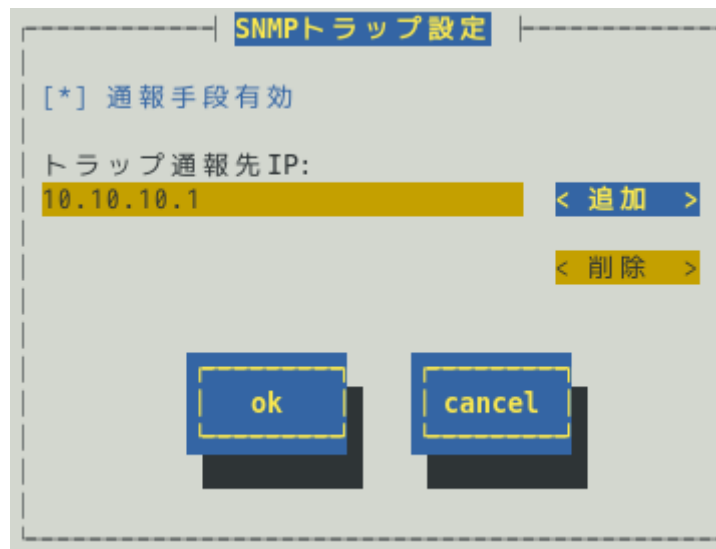
この画面を閉じます。

## 2.1 通報手段の設定

通報手段の有効/無効、マネージャ通報(SNMP)のトラップ通報先 IP が設定できます。

### 2.1.1 マネージャ通報(SNMP)の基本設定

[通報基本設定]画面の通報手段一覧から「マネージャ通報(SNMP)」を選択して表示される、[SNMP トラップ設定]画面にて、マネージャ通報(SNMP)の有効/無効、トラップ通報先 IP が設定できます。

The image shows a dialog box titled "SNMPトラップ設定" (SNMP Trap Setting). Inside the dialog, there is a section labeled "[\*] 通報手段有効" ([\*] Notification Method Enabled). Below this, there is a label "トラップ 通報先 IP:" (Trap Destination IP:). A text input field contains the IP address "10.10.10.1". To the right of the input field are two buttons: "< 追加 >" (Add) and "< 削除 >" (Delete). At the bottom of the dialog are two large buttons: "ok" and "cancel".

#### 通報手段有効

SNMP による通報手段の有効(チェックあり) と無効(チェックなし)が<スペース>キーで設定できます。既定値は"有効"です。

#### トラップ通報先 IP

通報先に設定している IP アドレスが一覧で表示されます。ESMPRO/ServerAgent から送信する Trap の宛先は、SNMP 設定ファイル(snmpd.conf)に設定される Trap Destination は使用しません。

トラップ通報先 IP は、最大で 128 個まで設定できます。

#### [追加...]ボタン

トラップ通報先 IP に新しい通報先の IP アドレスを追加できます。

#### [削除...]ボタン

トラップ通報先 IP から削除したい通報先の IP アドレスを削除できます。

#### [ok]ボタン

設定した情報を登録し、この画面を閉じます。

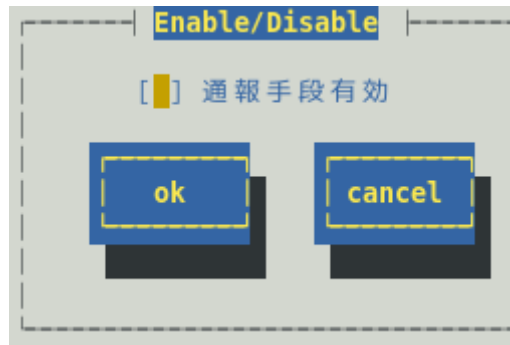
#### [cancel]ボタン

設定した情報を登録せずに、この画面を閉じます。

## 2.1.2 マネージャ通報(TCP\_IP In-Band)の基本設定

---

[通報基本設定]画面の通報手段一覧から「マネージャ通報(TCP\_IP In-Band)」を選択して表示される、[Enable/Disable]画面にて、マネージャ通報(TCP\_IP In-Band)の有効/無効が設定できます。



### 通報手段有効

TCP\_IP In-Band による通報手段の有効(チェックあり)と無効(チェックなし)が<スペース>キーで設定できます。

### [ok]ボタン

設定した情報を登録し、この画面を閉じます。

### [cancel]ボタン

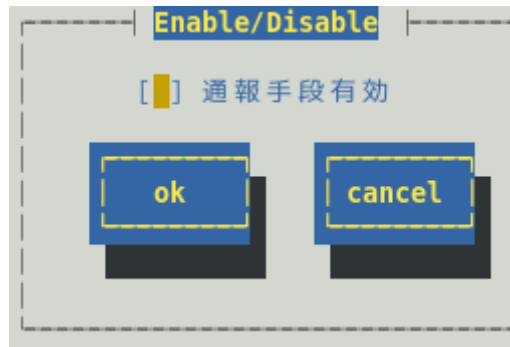
設定した情報を登録せずに、この画面を閉じます。



### 2.1.3 マネージャ通報(TCP\_IP Out-of-Band)の基本設定

---

[通報基本設定]画面の通報手段一覧から「マネージャ通報(TCP\_IP Out-of-Band)」を選択して表示される、[Enable/Disable]画面にて、マネージャ通報(TCP\_IP Out-of-Band)の有効/無効が設定できます。  
TCP/IP Out-of-Band 通報を有効にするときは、ESMPRO/ServerManager 側の RAS(Remote Access Service) 設定の暗号化の設定は、「クリアテキストを含む任意の認証を許可する」を必ず選択します。



#### 通報手段有効

TCP\_IP Out-of-Band による通報手段の有効(チェックあり)と無効(チェックなし)が<スペース>キーで設定できます。

#### [ok]ボタン

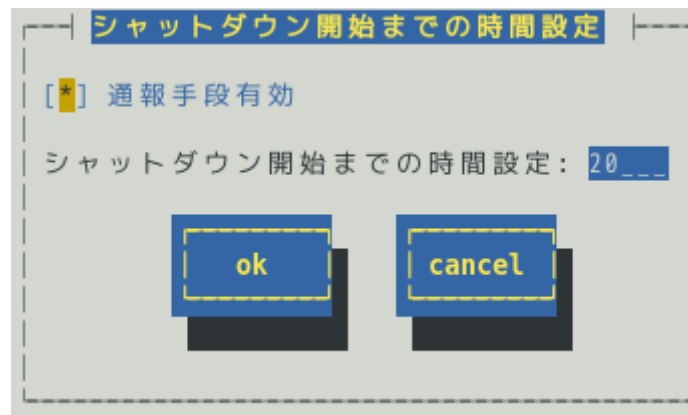
設定した情報を登録し、この画面を閉じます。

#### [cancel]ボタン

設定した情報を登録せずに、この画面を閉じます。

## 2.2 その他の設定

[通報基本設定]画面のその他の設定から「シャットダウン開始までの時間設定」を選択して表示される、[シャットダウン開始までの時間設定]画面にて、シャットダウン開始までの時間が設定できます。



### 通報手段有効

通報によるシャットダウン機能の有効(チェックあり)と無効(チェックなし)が<スペース>キーで設定できます。

既定値は"有効"です。

### シャットダウン開始までの時間設定

ESMPRO/ServerAgent が OS のシャットダウンを開始するまでの時間が設定できます。

既定値は 20 秒です。

設定可能範囲は 0～1800 秒です。

以下の場合において、ここで設定した時間が経過した後、OS のシャットダウンが開始します。

- ・ 通報後のアクションにシャットダウンを指定しているとき
- ・ ESMPRO/ServerManager からシャットダウン指示があったとき

### [ok]ボタン

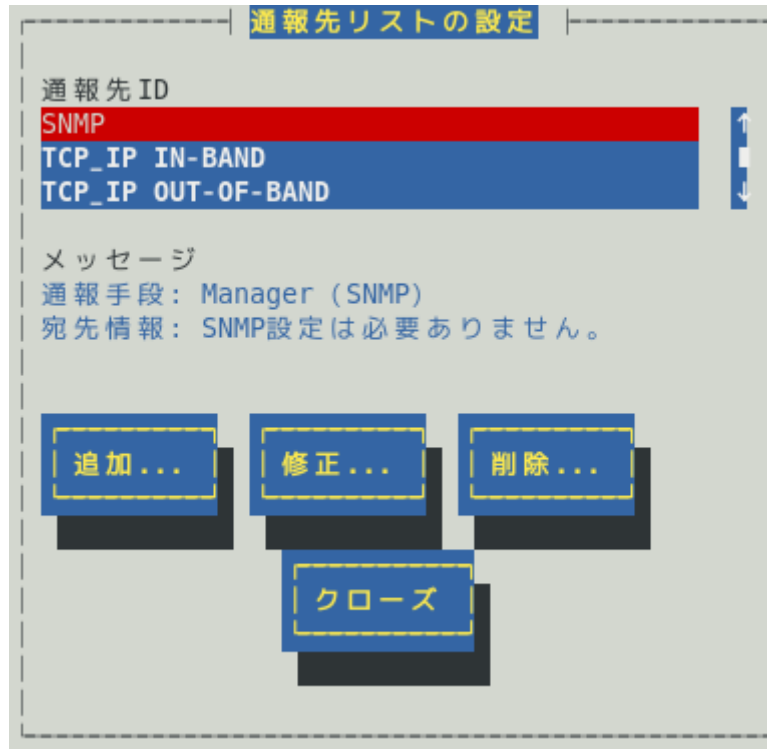
設定した情報を登録し、この画面を閉じます。

### [cancel]ボタン

設定した情報を登録せずに、この画面を閉じます。

## 3. 通報先リストの設定

コントロールパネル(ESMamsadm)の「通報先リストの設定」を選択して表示される[通報先リストの設定]画面にて、通報先 ID の設定変更、追加、削除および通報スケジュールが設定できます。



### 通報先 ID 一覧

通報先 ID のリストが表示されます。

### メッセージ

通報手段: 通報先 ID 一覧で選択された通報先 ID に設定されている通報手段が表示されます。

宛先情報: 通報先 ID 一覧で選択された通報先 ID に設定されている宛先情報が表示されます。

### [追加...]ボタン

通報先 ID を追加できます。[追加...]ボタンを押すと、[ID 設定]画面が表示されます。

同一通報手段で異なる通報先を持つ通報先 ID を登録しておくと、同一手段で複数の宛先に通報できます。

### [修正...]ボタン

通報先 ID 一覧で選択した通報先 ID に対して、通報先の設定が変更できます。

[修正...]ボタンを押すと、[ID 設定]画面が表示されます。

### [削除...]ボタン

通報先 ID 一覧で選択した通報先 ID を削除できます。

通報先 ID を削除すると、各監視イベントに設定されている通報先 ID も削除されます。また、既定で設定している"SNMP"と"TCP\_IP In-Band"、"TCP\_IP Out-of-Band"の 3 つの通報先 ID は、削除できません。

### [クローズ]ボタン

この画面を閉じます。

### 3.1 通報先 ID の設定変更

通報先リストに登録されている通報先 ID の設定変更ができます。[通報先リストの設定]画面の通報先 ID 一覧で変更したい通報先 ID を選択し、[修正]ボタンを押すと[ID 設定]画面が開きます。設定内容は、通報手段によって異なります。

ID: SNMP

通報手段: Manager (SNMP)

宛先情報:  
設定する必要はありません。

宛先設定...      スケジュール...      クローズ

#### ● 設定方法

必要に応じて[宛先設定...]ボタンおよび[スケジュール...]ボタンを押して、宛先と通報スケジュールを設定します。

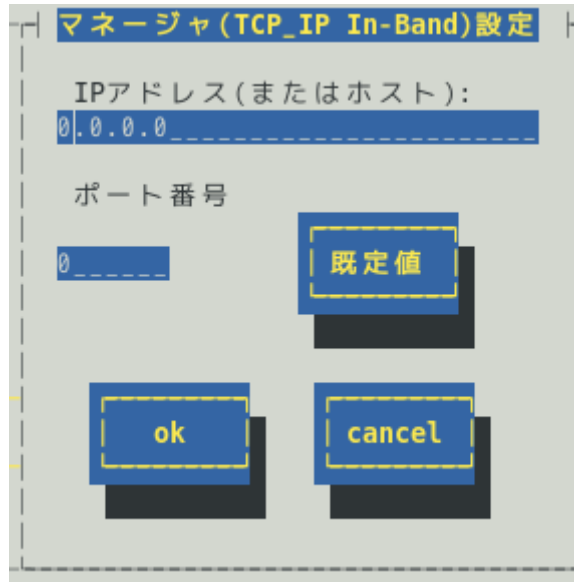
設定変更のとき、ID および通報手段の項目は、表示のみとなり、設定できません。

通報手段が「Manager(SNMP)」のときは、[宛先設定...]ボタンを押しても、ここでは設定する必要がないため、宛先設定画面は、表示されません。

### 3.1.1 通報手段がマネージャ通報(TCP\_IP In-Band)の宛先設定

通報手段がマネージャ通報(TCP\_IP In-Band)のとき、[ID 設定]画面で[宛先設定...]ボタンを押すと表示される[マネージャ(TCP\_IP In-Band)設定]画面にて、宛先が設定できます。

ESMPRO/ServerAgent は UDP のソケット通信を利用して、TRAP 送信元の IP アドレスを取得します。



マネージャ (TCP\_IP In-Band) 設定

IPアドレス(またはホスト):  
0.0.0.0

ポート番号  
0

既定値

ok cancel

#### IP アドレス(またはホスト)

通報先の ESMPRO/ServerManager が導入されたマシンの IP アドレス(またはホスト名)を指定します。  
省略することはできません。

#### ポート番号

ソケット間通信で使用するポート番号を設定できます。

このポート番号は、ESMPRO/ServerAgent と通報先の ESMPRO/ServerManager で同じ値を設定してください。既定値は 31134 です。既定値に問題がないかぎり、設定を変更しないでください。

既定値に問題があるとき、6001 から 65535 の範囲で番号を変更してください。番号を変更したとき、通報先の ESMPRO/ServerManager がインストールされているマシンで設定ツールを実行し、[通報基本設定]の[通報受信設定]-[エージェントからの受信(TCP/IP)]の設定を変更してください。



アクセス制御を設定している場合は、指定したポートのアクセスを許可してください。

#### [既定値]ボタン

ボタンを押すと、既定値が設定されます。

#### [ok]ボタン

設定した情報を登録し、この画面を閉じます。

#### [cancel]ボタン

設定した情報を登録せずに、この画面を閉じます。

### 3.1.2 通報手段がマネージャ通報(TCP\_IP Out-of-Band)の宛先設定

通報手段がマネージャ通報(TCP\_IP Out-of-Band)のとき、[ID 設定]画面で[宛先設定...]ボタンを押すと表示される[マネージャ(TCP\_IP Out-of-Band)設定]画面にて、宛先が設定できます。

ESMPRO/ServerAgent は UDP のソケット通信を利用して、TRAP 送信元の IP アドレスを取得します。

#### IP アドレス(またはホスト)

通報先の ESMPRO/ServerManager が導入されたマシンの IP アドレス(またはホスト名)を指定します。  
省略することはできません。

#### リモートアクセスサービスのエントリ選択

接続先の電話番号と、接続時に必要なユーザー名、パスワードを設定できます。

#### ポート番号

ソケット間通信で使用するポート番号を設定できます。  
このポート番号は、ESMPRO/ServerAgent と通報先の ESMPRO/ServerManager で同じ値を設定します。  
既定値は 31134 です。既定値に問題がないかぎり、設定を変更しないでください。

既定値に問題があるとき、6001 から 65535 の範囲で番号を変更してください。番号を変更したとき、通報先の ESMPRO/ServerManager がインストールされているマシンで設定ツールを実行し、[通報基本設定]の[通報受信設定]-[エージェントからの受信(TCP/IP)]の設定を変更してください。



アクセス制御を設定している場合は、指定したポートのアクセスを許可してください。

#### [既定値]ボタン

ボタンを押すと、既定値が設定されます。

**[ok]ボタン**

設定した情報を登録し、この画面を閉じます。

**[cancel]ボタン**

設定した情報を登録せずに、この画面を閉じます。

### 3.1.3 スケジュール設定

通報先 ID ごとに、通報スケジュールが設定できます。

スケジュール

リトライ間隔： 5 分

リトライ時間： 72 時間

通報時間帯

0-24,

例： 8-16,19-23

ok cancel

#### リトライ間隔

通報リトライをする間隔が設定できます。  
既定値は 5 分です。  
設定可能範囲は 1～30 分です。

#### リトライ時間

最大リトライ可能時間が設定できます。  
0 を設定したときは、通報リトライしません。  
既定値は 72 時間です。  
設定可能範囲は 0～240 時間です。

#### 通報時間帯

通報時間帯(24 時間表記の 1 時間単位)を指定してください。指定した時間帯に発生した故障のみを通報します。通報をしない時間帯に発生したイベントは通報されず、通報をする時間帯になると通報します。(それまでイベントの通報は保留されます。)  
既定値は 0-24 で、24 時間通報可能となっています。

#### [ok]ボタン

設定した情報を登録し、この画面を閉じます。

#### [cancel]ボタン

設定した情報を登録せずに、この画面を閉じます。



## 3.2 通報先 ID の追加

通報先 ID を追加します。設定内容は通報手段によって異なります。

The screenshot shows a dialog box titled "ID設定". It has three input fields: "ID:" with a blue text box, "通報手段:" with a yellow dropdown menu showing "MANAGER (SNMP)", and "宛先情報:" with a large empty text area. At the bottom, there are four buttons: "宛先設定...", "スケジュール...", "ok", and "cancel".

### < 設定手順 >

1. 通報先 ID を半角英数字または半角スペース、半角ハイフン(-)、半角アンダーバー(\_) を 31 文字以内で入力します。
2. 通報手段を<↑>か<↓>キーで選択します。
3. [宛先設定...]ボタンを押し、表示される画面にて宛先を設定します。
4. [スケジュール...]ボタンを押し、表示される画面で通報スケジュールを設定します。
5. [ok]ボタンを押します。

通報手段で「Manager(SNMP)」を選択したときは、[宛先設定...]ボタンを押しても、ここでは設定する必要がないため、宛先設定画面は表示されません。

## 4. エージェントイベントの設定

### 機 能

エージェントイベントの設定および通報先を結びつけます。監視対象のイベントが発生したとき、ここで結びつけた通報先に通報されます。

### 設 定

コントロールパネル(ESMamsadm)の「エージェントイベントの設定」を選択して表示される[エージェントイベント設定]画面にて、エージェントイベントの設定ができます。

#### ソース名

ソース名を<↑>か<↓>キーで選択します。

#### ソースに対する処理

ソースに対する処理を<スペース>キーで選択できます。

本選択はエージェントイベント設定内容ではなく、処理方法の選択です。

そのため、コントロールパネルの起動毎に「OFF」が選択されます。

以下の設定をするとき「OFF」を選択します。

- ・選択した「ソース名」のイベント ID に対して、通報先や監視イベントを設定するとき。

以下の設定をするとき「ON」を選択します。

- ・選択した「ソース名」のイベント ID すべてに対して、一括で通報先を設定するとき。  
ただし、監視イベントの設定はできません。

#### イベント ID

「ソースに対する処理」で「OFF」を選択しているとき、「ソース名」で選択されたイベント ID を<↑>か<↓>キーで選択し表示します。

「ソースに対する処理」で「ON」を選択しているとき、「イベント ID」は「すべて」と表示されます。

**Trap Name**

選択された「イベント ID」のトラップ名を表示します。

**[設定...]ボタン**

[設定...]ボタンを押すと、[監視イベント設定]画面が表示されます。

「ソースに対する処理」で「OFF」を選択しているとき、選択したソースのイベント ID に対して、設定できます。

「ソースに対する処理」で「ON」を選択しているとき、選択したソースのイベント ID すべてに対して一括で通報先を設定できます。

**[クローズ]ボタン**

この画面を閉じます。

---

## 4.1 通報先の指定(エージェントイベント)

---

通報先の指定方法には、以下の方法があります。

1. 監視イベントごとに通報先を指定する方法（「ソースに対する処理」で「OFF」を選択しているとき）
2. ソースごとに通報先を一括指定する方法（「ソースに対する処理」で「ON」を選択しているとき）

### 4.1.1 監視イベントごとに通報先を指定する方法

---

通報先の設定と通報後の動作、対処法の設定ができます。

#### < 設定手順 >

1. コントロールパネル(ESMamsadm)を起動し、「エージェントイベントの設定」を選択します。

[エージェントイベントの設定]画面が表示されます。

2. 「ソース名」でソースを<↑>か<↓>キーで選択します。
3. 「ソースに対する処理」で「OFF」に<スペース>キーでチェックします。
4. 「イベント ID」で設定したいイベント ID を<↑>か<↓>キーで選択します。
5. [設定...]ボタンを押します。  
[監視イベント設定]画面が表示されます。

**監視イベント設定**

ソース名: ESMCOMMONSERVICE

イベントID: 40000068

通報後動作: なし

対処法:

通報IDリスト: TCP\_IP IN-BAND  
TCP\_IP OUT-OF-BAND

< 追加 >  
< 削除 >

通報先: SNMP

ok      cancel

6. 「通報IDリスト」から通報したい通報IDを選択します。
7. [追加]ボタンを押します。  
通報IDが「通報先」から「通報IDリスト」に移動します。
8. 通報IDを通報対象から削除するには「通報先」から通報IDを選択して、[削除]ボタンを押します。  
通報IDが「通報先」から「通報IDリスト」に移動します。
9. [ok]ボタンを押します。

#### 通報後動作

通報後の動作を設定できます。通報後の動作とは、このイベントが発生した後の動作を指し、「シャットダウン」「リブート」「なし」の3つから<↑>か<↓>キーで選択します。

#### 対処法

通報する項目に対する対処法を設定できます。507バイト(半角文字で507文字、全角文字で253文字)以下で指定します。日本語は使用できます。

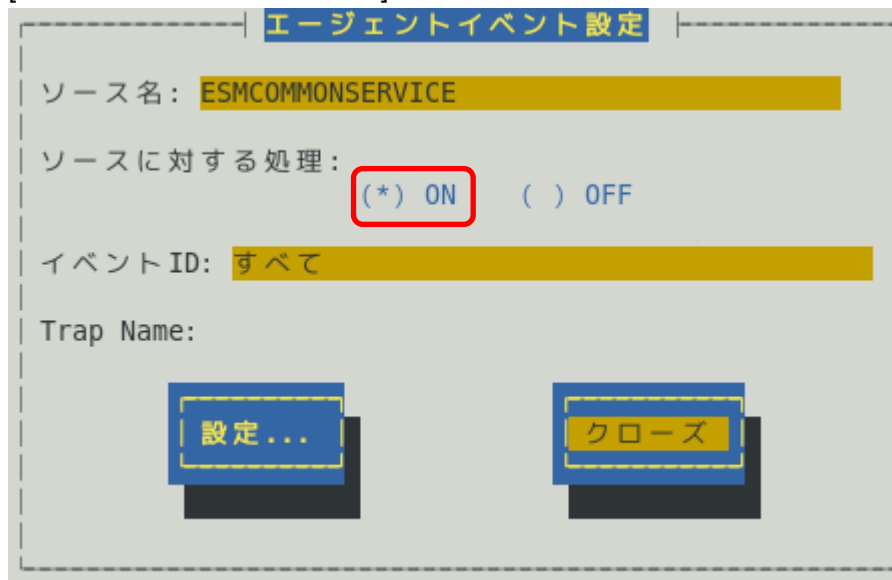
#### 4.1.2 ソースごとに通報先を一括指定する方法

ソースごとに通報先を一括で設定した後、再度、[監視イベント設定]画面を開いても、通報先一覧には何も表示されません。通報先の確認は「監視イベントごとに通報先を指定する方法」にて、個々のイベントを確認してください。

##### < 設定手順 >

1. コントロールパネル(ESMamsadm)を起動し、「エージェントイベントの設定」を選択します。

[エージェントイベントの設定]画面が表示されます。



エージェントイベント設定

ソース名: ESMCOMMONSERVICE

ソースに対する処理: (\*) ON ( ) OFF

イベントID: すべて

Trap Name:

設定... クローズ

2. 「ソース名」でソースを<↑>か<↓>キーで選択します。
3. 「ソースに対する処理」で「ON」に<スペース>キーでチェックします。
4. [設定...]ボタンを押します。  
[監視イベント設定]画面が表示されます。  
通報先は<none>で表示されます。



監視イベント設定

ソース名: ESMCOMMONSERVICE

イベントID: すべて

通報IDリスト: SNMP TCP\_IP IN-BAND TCP\_IP OUT-OF-BAND

通報先: <none>

< 追加 > < 削除 >

ok cancel

5. 「通報 ID リスト」から通報したい通報 ID を選択します。
6. [追加]ボタンを押します。  
通報 ID が「通報 ID リスト」から「通報先」に移動します。
7. 通報 ID を通報対象から削除するには「通報先」から通報 ID を選択して、[削除]ボタンを押します。  
通報 ID が「通報先」から「通報 ID リスト」に移動します。
8. [ok]ボタンを押します。

## 5. Syslog イベントの設定

### 機 能

Syslog イベントの設定および通報先を結びつけます。監視対象のイベントが発生したとき、ここで結びつけた通報先に通報されます。Syslog イベントは、あらかじめ登録されているイベント以外に、システム環境に応じて新たなソース、監視イベントを任意に追加や削除できます。Syslog 監視は既定値では 300 秒間隔で監視しています。Syslog 監視の監視間隔は変更できます。Syslog 監視の監視間隔の設定方法につきましては本書の 2 章(4. Syslog 監視)を参照してください。

### 設 定

コントロールパネル(ESMamsadm)の「Syslog イベントの設定」を選択して表示される[Syslog イベントの設定]画面にて、Syslog イベントの設定ができます。

#### ソース名

ソースを<↑>か<↓>キーで選択し表示します。

#### ソースに対する処理

ソースに対する処理を<スペース>キーで選択できます。

本選択は Syslog イベントの設定内容ではなく、処理方法の選択です。

そのため、コントロールパネルの起動毎に「OFF」が選択されます。

以下の設定をするとき「OFF」を選択します。

- ・選択した「ソース名」のイベント ID に対して、通報先や監視イベントを設定するとき。
- ・監視イベントの追加や削除をするとき。

以下の設定をするとき「ON」を選択します。



- ・ 選択した「ソース名」のイベント ID すべてに対して、一括で通報先を設定するとき。  
ただし、監視イベントの設定はできません。
- ・ ソースの追加や削除(すべての監視イベントを削除)をするとき。

#### イベント ID

「ソースに対する処理」で「OFF」を選択しているときは、「ソース名」で選択されたイベント ID を<↑>か<↓>キーで選択し表示します。  
「ソースに対する処理」で「ON」を選択しているときは、「イベント ID」に「すべて」と表示します。

#### Trap Name

選択されたイベント ID のトラップ名を表示します。

#### [クローズ]ボタン

[Syslog イベントの設定]画面を閉じます。  
[クローズ]ボタンを押すと、Syslog 監視の間隔はリセットされ、[クローズ]ボタンを押した時間から Syslog 監視間隔(既定値は 300 秒)までは、Syslog イベントを検知しません。

#### [追加...]ボタン

[追加...]ボタンを押すと、[Syslog イベントの追加]画面が表示されます。  
「ソースに対する処理」で「OFF」を選択しているときは、選択したソースの監視イベントを追加します。  
「ソースに対する処理」で「ON」を選択しているときは、ソースを含め監視イベントを追加します。

#### [削除...]ボタン

[削除...]ボタンを押すと、  
「ソースに対する処理」で「OFF」を選択しているときは、選択したソースの監視イベントを削除します。  
「ソースに対する処理」で「ON」を選択しているときは、ソースを含め監視イベントすべてを削除します。

#### [設定...]ボタン

[設定...]ボタンを押すと、[Syslog アプリケーション設定]画面が表示されます。  
「ソースに対する処理」で「OFF」を選択しているときは、選択したソースのイベント ID に対して、設定変更および通報先を設定できます。  
「ソースに対する処理」で「ON」を選択しているときは、選択したソースのイベント ID すべてに対して、一括で通報先を設定できます。

#### [テスト]ボタン

「ソースに対する処理」で「OFF」を選択しているときは、選択した Syslog イベントのキーワードを含む"ESMamsadm: [TEST - AlertManager] (キーワード)"文字列を syslog に記録することにより、テストイベントを発生させて、監視対象イベントに結び付けた宛先への通報を実際にシミュレートできます。通報のみならず「通報後動作」も動作します。そのため、設定によってはシャットダウンされることもありますので、テストする通報の選択にはご注意ください。  
「ソースに対する処理」で「ON」を選択しているときは、テストできません。

Syslog イベントの追加や削除、設定を変更したときは、Syslog イベントの情報を再読み込みさせる必要があります。[クローズ]ボタンを押して、[Syslog イベントの設定]画面を閉じ、[通報設定]画面から、再度「Syslog イベントの設定」を選択します。その後、[テスト]ボタンを押します。

## 5.1 通報先の指定(Syslog イベント)

通報先の指定方法には、以下の方法があります。

1. 監視イベントごとに通報先を指定する方法(「ソースに対する処理」で「OFF」を選択しているとき)
2. ソースごとに通報先を一括指定する方法(「ソースに対する処理」で「ON」を選択しているとき)

### 5.1.1 監視イベントごとに通報先を指定する方法

監視イベントごとに個別に通報先を指定するときの方法を説明します。  
通報先の設定と同時に、通報後の動作、対処法等の設定もできます。

#### < 設定手順 >

1. コントロールパネル(ESMamsadm)を起動し、「Syslog イベントの設定」を選択します。  
[Syslog イベントの設定]画面が表示されます。

2. 「ソース名」でソースを<↑>か<↓>キーで選択します。
3. 「ソースに対する処理」で「OFF」に<スペース>キーでチェックします。
4. 「イベント ID」で設定したいイベント ID を<↑>か<↓>キーで選択します。
5. [設定...]ボタンを押します。  
[Syslog アプリケーション設定]画面が表示されます。

**Syslogアプリケーション設定**

ソース名: ALERTMANAGER  
 イベントID: 80000001  
 キーワード1: AM FILE ERROR  
 キーワード2:  
 キーワード3:  
 通報後動作: なし  
 対処法: 保守員に連絡して下さい  
 レポートカウント: 1

[<Detail>](#)  
[<Detail>](#)  
[<Detail>](#)

通報IDリスト:  
 TCP\_IP IN-BAND  
 TCP\_IP OUT-OF-BAND

< 追加 >  
 < 削除 >

通報先: SNMP

監視時間帯  
0-24,

ok  
 cancel

6. 「通報 ID リスト」から通報したい通報 ID を選択します。
7. [追加]ボタンを押します。  
通報 ID が「通報 ID リスト」から「通報先」に移動します。
8. 通報 ID を通報対象から削除するには「通報先」から通報 ID を選択して、[削除]ボタンを押します。  
通報 ID が「通報先」から「通報 ID リスト」に移動します。
9. [ok]ボタンを押します。

#### 通報後動作

通報後のアクションを設定できます。[通報後のアクション]とは、このイベントが発生した後の動作を指し、「シャットダウン」「リブート」「なし」の3つから<↑>か<↓>キーで選択します。

#### 対処法

通報する項目に対する対処法を設定します。507 バイト(半角文字で 507 文字、全角文字で 253 文字)以下で指定します。日本語は使用できます。

#### レポートカウント

同一イベントを指定回数検出したときに通報をします。

#### 監視時間帯

監視時間帯を指定できます。指定した時間帯に発生したイベントのみを通報します。  
時間設定は 1 時間単位で指定できます。既定値では 24 時間通報可能となっています。

### 5.1.2 ソースごとに通報先を一括指定する方法

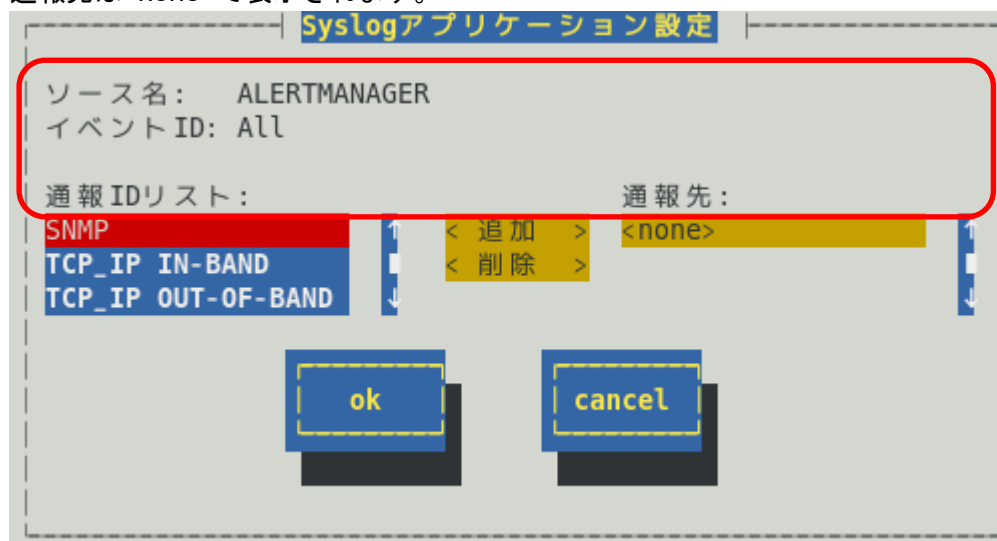
ソースごとに、ソース配下のすべての監視イベントに同じ通報先を一括して指定する方法を説明します。通報先を一括で設定した後、再度、[Syslog アプリケーション設定]画面を開いても、通報先一覧には何も表示されません。通報先の確認は「監視イベントごとに個別に通報先を指定する方法」にて、個々のイベントで確認します。

#### < 設定手順 >

1. コントロールパネル(ESMamsadm)を起動し、「Syslog イベントの設定」を選択します。  
[Syslog イベントの設定]画面が表示されます。



2. 「ソース名」でソースを<↑>か<↓>キーで選択します。
3. 「ソースに対する処理」で「ON」に<スペース>キーでチェックします。
4. [設定...]ボタンを押します。  
[Syslog アプリケーション設定]画面が表示されます。  
通報先は<none>で表示されます。



5. 「通報 ID リスト」から通報したい通報 ID を選択します。
6. [追加]ボタンを押します。  
通報 ID が「通報 ID リスト」から「通報先」に移動します。
7. 通報 ID を通報対象から削除するには「通報先」から通報 ID を選択して、[削除]ボタンを押します。  
通報 ID が「通報先」から「通報 ID リスト」に移動します。
8. [ok]ボタンを押します。

## 5.2 Syslog イベントのソースの追加

システム環境に応じて、新たな Syslog イベントのソースを任意に追加できます。ESMPRO/ServerAgent 以外のアプリケーションが登録するイベントを監視したいときに設定します。ソース登録と同時に、1 件目の監視イベントをあわせて登録します。本機に登録できるイベント数は、最大で 1024 個ですが、登録件数によりディスク使用量・メモリ使用量が増加しますので、設定には注意してください。

### < 設定手順 >

1. コントロールパネル(ESMamsadm)を起動し、「Syslog イベントの設定」を選択します。  
[Syslog イベントの設定]画面が表示されます。

Syslog イベントの設定

ソース名: ALERTMANAGER

ソースに対する処理: (\* ) ON ( ) OFF

イベント ID: すべて

テスト

Trap Name:

追加... 削除... 設定... クローズ

2. 「ソースに対する処理」で「ON」に<スペース>キーでチェックします。
3. [追加...]ボタンを押します。  
[Syslog イベントの追加]画面が表示されます。

**Syslogイベントの追加**

ソース名:

イベント ID:

キーワード 1:

キーワード 2:

キーワード 3:

Trap Name:

対処法:

4. 「ソース名」「イベント ID」「キーワード」「Trap Name」「対処法」を設定します。
5. [ok]ボタンを押します。  
このとき、「通報後動作：なし」「レポートカウント：1」が設定されます。

#### ソース名 (必須項目)

ソース名を 40 文字以下の半角英字で始まる半角英数字(大文字)で指定します。ソース名は大文字使用しますので、小文字を設定しても大文字に変換しますが、アラートビューアで表示する「タイプ」と「製品名」は設定した半角英数字のままとなります。小文字で設定したとき、「ソース」は大文字、「タイプ」と「製品名」は小文字となります。

ESMPRO/ServerManager のアラートビューアの「ソース」と「タイプ」、「製品名」欄に表示されます。

#### イベント ID (必須項目)

以下の命名規則にしたがって、半角英数字 8 文字(16 進数表記[0-9,A-F])で指定します。

<監視イベント ID 命名規則>

“x0000yyy”形式で指定します。(例：40000101、800002AB、C0000101)

“x”には、4,8,C の中から設定します。それぞれの意味は以下のとおりです。

4：情報系イベントを意味します。

ESMPRO/ServerManager のアラートビューアのアイコンが「緑色」で表示されます。

8：警告系イベントを意味します。

ESMPRO/ServerManager のアラートビューアのアイコンが「黄色」で表示されます。

C：異常系イベントを意味します。

ESMPRO/ServerManager のアラートビューアのアイコンが「赤色」で表示されます。

“yyy”には、0x001(1)~0xFFFF(4095)の範囲内で任意の 16 進数値を設定します。

#### キーワード 1 (必須項目)、キーワード 2、キーワード 3

syslog に記録されるメッセージを一意に特定できる文字列を、それぞれ 256 文字以下の半角英数字で指定します。すべてのキーワードを含むメッセージを syslog から検出(※)したときに、そのメッセージの全文を ESMPRO/ServerManager に通報します。

ESMPRO/ServerManager のアラートビューアの「詳細」欄に表示されます。

※1 行における検出範囲は、行頭から 1024Byte まで。

**Trap Name (必須項目)**

通報メッセージの概要を 79 バイト(半角文字で 79 文字、全角文字で 39 文字)以下で指定します。日本語は使用できます。

ESMPRO/ServerManager のアラートビューアの「概要」欄に表示されます。

**対処法**

通報メッセージを受けたときの対処法を 507 バイト(半角文字で 507 文字、全角文字で 253 文字)以下で指定します。日本語は使用できます。

ESMPRO/ServerManager のアラートビューアの「対処」欄に表示されます。



## 5.3 Syslog イベントの追加

すでに登録済みの Syslog イベントのソース配下に、システム環境に応じて新たな Syslog イベントを追加できます。

### < 設定手順 >

1. コントロールパネル(ESMamsadm)を起動し、「Syslog イベントの設定」を選択します。  
[Syslog イベントの設定]画面が表示されます。

2. 「ソース名」でソース名を<↑>か<↓>キーで選択します。
3. 「ソースに対する処理」で「OFF」に<スペース>キーでチェックします。
4. [追加...]ボタンを押します。  
[Syslog イベントの追加]画面が表示されます。
5. 「イベント ID」「キーワード」「Trap Name」「対処法」を設定します。  
各項目の設定内容は「5.2. Syslog イベントのソースの追加」に記載してある内容と同じです。
6. [ok]ボタンを押します。

## 5.4 Syslog イベントのソースの削除

Syslog イベント監視から、Syslog イベントのソースを削除できます。ソースを削除すると、その配下に登録されているすべての監視イベントも削除されます。また、ESMPRO/ServerAgent が登録している既定のソースを削除することはできません。

### < 設定手順 >

1. コントロールパネル(ESMamsadm)を起動し、「Syslog イベントの設定」を選択します。  
[Syslog イベントの設定]画面が表示されます。

2. 「ソース名」で削除したいソース名を<↑>か<↓>キーで選択します。
3. 「ソースに対する処理」で「ON」に<スペース>キーでチェックします。
4. [削除...]ボタンを押します。

## 5.5 Syslog イベントの削除

Syslog イベント監視から、Syslog イベントを削除できます。ESMPRO/ServerAgent が登録している既定の監視イベントを削除することはできません。

### < 設定手順 >

1. コントロールパネル(ESMamsadm)を起動し、「Syslog イベントの設定」を選択します。  
[Syslog イベントの設定]画面が表示されます。

2. 「ソース名」でソース名を<↑>か<↓>キーで選択します。
3. 「ソースに対する処理」で「OFF」に<スペース>キーでチェックします。
4. 「イベント ID」で削除したいイベント ID を<↑>か<↓>キーで選択します。
5. [削除...]ボタンを押します。

## 5.6 Syslog イベントのテスト

Syslog イベントのテストを実行して、SNMP 通報の送信テストができます。

### < テスト手順 >

1. コントロールパネル(ESMamsadm)を起動し、「Syslog イベントの設定」を選択します。  
[Syslog イベントの設定]画面が表示されます。

2. 「ソース名」で任意のソース名を<↑>か<↓>キーで選択します。
3. 「ソースに対する処理」で「OFF」に<スペース>キーでチェックします。
4. 「イベント ID」で任意のイベント ID を<↑>か<↓>キーで選択します。
5. [設定...]ボタンを押します。  
[Syslog アプリケーション設定]画面が表示されます。

**Syslogアプリケーション設定**

ソース名: ALERTMANAGER  
 イベントID: 80000001  
 キーワード1: AM FILE ERROR  
 キーワード2:  
 キーワード3:  
 通報後動作: なし  
 対処法: 保守員に連絡して下さい  
 レポートカウント: 1  
 通報IDリスト:  
 TCP\_IP IN-BAND  
 TCP\_IP OUT-OF-BAND  
 監視時間帯  
 0-24,  
 通報先: SNMP  
 <追加>  
 <削除>  
 ok cancel

6. 「通報後動作」が「なし」、「通報先」がSNMP となっていることを確認します。



「通報後動作」が「シャットダウン」や「リブート」の場合、テストであっても「通報後動作」が動作します。「通報先」がない場合、通報されません。

7. [ok]ボタンを押します。  
 [Syslog イベントの設定]画面が表示されます。

**Syslogイベントの設定**

ソース名: ALERTMANAGER  
 ソースに対する処理: ( ) ON (\*) OFF  
 イベントID: 80000001  
 Trap Name: AM FILE ERROR  
 テスト  
 追加... 削除... 設定... クローズ

8. [テスト]ボタンを押します。  
テストメッセージが syslog に記録されます。  
Syslog 監視の監視間隔(既定値 300 秒)を超えると、syslog に記録されたテストメッセージを検出し、SNMP 通報します。

# ESMPRO/ServerAgent for GuestOS Ver.1.5 他社機版 ESMPRO/ServerAgent Ver.1.5

---

# 4

## 追加機能

ESMPRO/ServerAgent の追加機能について説明します。

### 1. コンフィグレーションツール

---

# 1. コンフィグレーションツール

---

/opt/nec/esmpro\_sa/tools 配下にコンフィグレーションツール(以降、本ツールと表記)を提供しています。

1. 本ツールを使用するには、ESMPRO/ServerAgent が動作している必要があります。  
必ず、ESMPRO/ServerAgent をインストールして、動作させてください。
2. 本ツールを使用するには、root 権限が必要です。  
必ず、root 権限のあるユーザーでログインしてください。
3. 本ツールは複数同時に使用することはできません。  
また、ESMPRO/ServerAgent のコントロールパネル(ESMagntconf, ESMamsadm)も起動しないでください。
4. 本ツールの設定を ESMPRO/ServerAgent に反映するため、以下のどちらかを実行してください。
  - ・以下のコマンドを実行して、ESMPRO/ServerAgent のサービスを再起動します。  
# /opt/nec/esmpro\_sa/bin/ESMRestart
  - ・以下のコマンドを実行して、OS を再起動します。  
# reboot
5. 本ツールは、コマンドラインインタフェースを使用する特性により、シェルスクリプトから実行することも可能ですが、以下のような点に注意してください。
  - ・1 行目には「#!/bin/bash」を記述します。
  - ・ファイルの保存時には改行コードを Linux 改行コード (LF)とします。  
Windows 標準のテキストエディタ(メモ帳)では、ファイル保存時に改行コードを Windows 改行コード (CR+LF) に変換して保存します。
  - ・設定項目に日本語を使用する場合は、文字コードは OS に合わせ、euc や UTF-8 を使用します。

## esmamset コマンド

コマンドラインインタフェースを使用して、ESMPRO/ServerAgent が使用する通報の情報を設定します。  
esmamset コマンドでは、以下を設定できます。

1. ラック名の設定 (本製品では未サポートです)
2. SNMP コミュニティー名の設定
3. 通報手段(SNMP)の有効/無効設定
4. 通報手段(SNMP)の通報先 IP アドレスの追加または削除
5. 通報手段(TCP\_IP In-Band)の有効/無効設定
6. 通報手段(TCP\_IP In-Band)の IP アドレスの追加または削除
7. 通報手段(TCP\_IP In-Band)で使用するポート番号の設定
8. ESMPRO/ServerAgent からのシステムシャットダウン 有効/無効の設定
9. Syslog 監視の監視間隔の設定
10. Syslog 監視の追加監視対象の設定
11. Syslog 監視のファイル監視対象の設定

## esmsysrep コマンド

コマンドラインインタフェースを使用して、ESMPRO/ServerAgent が監視する Syslog 監視対象イベントを設定します。esmsysrep コマンドでは、以下を設定できます。

1. Syslog 監視対象イベントの追加
2. Syslog 監視対象イベントの変更
3. Syslog 監視対象イベントの削除



## 1.1 esmamset コマンド

### 機 能

コマンドラインインタフェースを使用して、ESMPRO/ServerAgent が使用する通報の情報を設定します。  
esmamset コマンドでは、以下を設定できます。

1. ラック名の設定 (本製品では未サポートです)
2. SNMP コミュニティ名の設定
3. 通報手段(SNMP)の有効/無効設定
4. 通報手段(SNMP)の通報先 IP アドレスの追加または削除
5. 通報手段(TCP\_IP In-Band)の有効/無効設定
6. 通報手段(TCP\_IP In-Band)の IP アドレスの追加または削除
7. 通報手段(TCP\_IP In-Band)で使用するポート番号の設定
8. ESMPRO/ServerAgent からのシステムシャットダウン 有効/無効の設定
9. Syslog 監視の監視間隔の設定
10. Syslog 監視の追加監視対象の設定
11. Syslog 監視のファイル監視対象の設定

### 設 定

esmamset コマンドの使用方法は以下のとおりです。

esmamset コマンドで実行した設定を動作中の ESMPRO/ServerAgent に反映するには、  
ESMPRO/ServerAgent の再起動(ESMRestart)が必要です。

```
# cd /opt/nec/esmpro_sa/tools
# ./esmamset [OPTION]
:
# /opt/nec/esmpro_sa/bin/ESMRestart
```

```
Usage:
esmamset [-r <rackname>] [-c <community>]
        [--mi <second>] [--cmo <filename>] [--fmo <filename>]
        [-s ON|OFF] [-d <delip|ALLIP ...>] [-a <addip ...>]
        [-t ON|OFF] [-i <ip>] [-p <port>]
        [-o ON|OFF]
        [-f <filename>]
        [-P]
        [-h]
```



ESMPRO/ServerAgent は、日本語(2 バイト)文字を EUC コードで管理しています。  
そのため、日本語文字の入力や表示をさせる場合は、ネットワーク経由(ssh コマンドなど)  
で別の日本語端末からログインし、一時的に LANG 環境変数を日本語環境に変更してくだ  
さい。

- 1)現在の LANG 環境変数を確認します。

```
# echo $LANG
```

- 2)LANG 環境変数を ja\_jp.eucJP に変更します。

```
# export LANG=ja_jp.eucJP
```

- 3)esmamset または esmsysrep コマンドを実行します。

```
# cd /opt/nec/esmpro_sa/tools/

# ./esmamset [OPTION]

# ./esmsysrep [OPTION]

:

# /opt/nec/esmpro_sa/bin/ESMRestart
4)LANG 環境変数を 1) の値に戻します。

# export LANG=xxxxxxx
```

## [OPTION] 指定

[OPTION] には以下のオプションを指定します。複数のオプションを同時に指定することもできます。設定する値にスペースが含まれるときは、前後に" (ダブルクォーテーション) を付加してください。

オプション	説明
-r <rackname>	本製品では未サポートです。
-c <community>	コミュニティ名を設定します。最大で 33 バイトまで指定できます。snmpd.conf に設定されていないコミュニティ名を指定したときは、設定は変更されませんので、先に snmpd.conf を修正してください。
--mi <second>	Syslog 監視の監視間隔(秒)を設定します。設定範囲は 10~3600(秒)です。
--cmo <filename>	/var/log/messages を含まない syslog と同じフォーマットの追加で監視対象とするファイルをフルパスで指定します。最大で 255 バイトまで指定できます。
--fmo <filename>	/var/log/messages を含まないファイル監視対象とするファイルをフルパスで指定します。最大で 255 バイトまで指定できます。
-s ON OFF	通報手段(SNMP)の有効/無効を設定します。 ON :有効 / OFF :無効
-d <delip ...>	通報手段(SNMP)に指定されている通報先 IP アドレスを削除します。半角スペースを空格、2 つ以上の IP アドレスを同時に削除することもできます。
-d <ALLIP>	通報手段(SNMP)に指定されている通報先 IP アドレスをすべて削除します。
-a <addip ...>	通報手段(SNMP)に指定されている通報先 IP アドレスを追加します。半角スペースを空格、2 つ以上の IP アドレスを同時に追加することもできます。最大で 255 個の IP アドレスを指定できます。
-t ON OFF	通報手段(TCP_IP In-Band)の有効/無効を設定します。 ON :有効 / OFF :無効
-i <ip>	通報手段(TCP_IP In-Band)の通報先 IP アドレスを指定します。
-p <port>	通報手段(TCP_IP In-Band)で使用するポート番号を指定します。ファイアウォールを設定している場合は指定したポートを開放してください。
-o ON OFF	ESMPRO/ServerAgent からのシステムシャットダウンの有効/無効を設定します。 ON :有効 / OFF :無効
-f <filename>	配置ファイルを指定して読み込み、ファイルに記載の内容にしたがって、各種設定をします。配置ファイルは後述します。 配置ファイルを読み込んだ時点で、成功と判断するため、配置ファイル内で指定されたオプションが不正であっても戻り値は 0 (成功) を返却します。
-P	設定内容を一覧で表示します。esmamset コマンドで実行した設定を動作中の ESMPRO/ServerAgent に反映するには、ESMPRO/ServerAgent の再起動 (ESMRestart) が必要です。
-h	ヘルプ (Usage:) を表示します。

## 配置ファイル

[OPTION]で指定する内容が記載されたテキストファイルのことを指します。配置ファイルを -f オプションで指定して読み込むことで、[OPTION]を指定したときと同じことができます。

配置ファイルは

```
keyname "value"
```

の形式で記載します。keyname と ダブルクォート(")の間には空白(スペースかタブ)を入れてください。また、改行コードが Linux 改行コード(LF)となるように注意してください。Windows 改行コード(CR+LF)で保存されたテキストファイルのときは、配置ファイルの内容を正しく読み込むことができません。

keyname の説明は下表を参照してください。

keyname(大文字)	説明
RACKNAME	本製品では未サポートです。
COMMUNITY	-c オプションで指定する内容と同じです。
SYSLOG-MONITOR-INTERVAL	--mi オプションで指定する内容と同じです。
CUSTOM-MONITORING-OBJECT	--cmo オプションで指定する内容と同じです。
FILE-MONITORING-OBJECT	--fmo オプションで指定する内容と同じです。
SNMP	-s オプションで指定する内容と同じです。
DELIP	-d オプションで指定する内容と同じです。
ADDIP	-a オプションで指定する内容と同じです。
IN-BAND	-t オプションで指定する内容と同じです。
IN-BANDIP	-i オプションで指定する内容と同じです。
IN-BANDPORT	-p オプションで指定する内容と同じです。
SHUTDOWN	-o オプションで指定する内容と同じです。

## 戻り値

esmamset コマンドの戻り値は以下のとおりです。

戻り値	説明
0	設定に成功しました。
1	設定に失敗しました。指定されているオプションの内容を確認してください。
2	設定に失敗しました。ESMPRO/ServerAgent をインストールしてください。
4	設定に失敗しました。ログインしているユーザーにコマンドの実行権限がありません。

## エラーメッセージ

エラーメッセージは以下のとおりです。

メッセージ	説明	戻り値
Usage:	HELP 情報を表示します。	0
%s: Setting succeed!	指定された項目が設定成功、%s は項目名です。	0
%s: Setting failed!	指定された項目が設定失敗、%s は項目名です。	1
System Error!	システムエラーが発生しました。	1
Usage:	オプションが存在しません。	1
Please input a valid rackname after "-r" option (length<=63).	"-r"(rackname)のパラメーターが取得できません。または、rackname が最大長(63 バイト)を超えています。	1
Please input a valid community after "-c" option (length<=33).	"-c"(community)のパラメーターが取得できません。または、community が最大長(33 バイト)を超えています。	1
[%s] was not found in snmpd.conf file! The community [%s] must be set in snmpd.conf file.	インプットされた community は snmpd.conf には存在しない。%s はインプットした community です。	1

メッセージ	説明	戻り値
Please input number range from 10 to 3600 after "--mi" option (Monitor Interval).	"--mi"(監視間隔)のパラメーターが取得できません。または、指定された値が無効(「10~3600」の数値)です。	1
Please input a readable file's name after "--cmo" option with full path (length<=255). And cannot be set "/var/log/messages".	"--cmo"(追加監視対象)のパラメーターが取得できません。追加監視対象のフルパスが必要で、読み込み権限が必要です。または、filename が最大長(255 バイト)を超えます。そして、「/var/log/messages」は設定できません。	1
Please input a readable file's name after "--fmo" option with full path (length<=255). And cannot be set "/var/log/messages".	"--fmo"(ファイル監視)のパラメーターが取得できません。ファイル監視のフルパスが必要で、読み込み権限が必要です。または、filename が最大長(255 バイト)を超えます。そして、「/var/log/messages」は設定できません。	1
The filenames of "File Monitoring Object (--fmo) and "Custom Monitoring Object (--cmo) must be different.	追加監視対象(--cmo)とファイル監視(--fmo)は、異なるファイルを指定する必要があります。	1
Please input ON or OFF after "-s" option (SNMP).	"-s"(SNMP)のパラメーターが取得できません。または、ON/OFF 以外の値が設定されています。	1
Please input valid IP address after "-d" option (SNMP).	削除したい IP が指定されない。"-d"のパラメーターが取得失敗しました。	1
Please input valid IP address after "-a" option (SNMP).	追加したい IP が指定されない。"-a"のパラメーターが取得失敗しました。	1
Please input ON or OFF after "-t" option (TCP_IP In-Band).	"-t"(TCP_IP In-Band)のパラメーターが取得できません。または、ON/OFF 以外の値が設定されています。	1
Please input valid IP address after "-i" option (TCP_IP In-Band).	"-i"(TCP_IP In-Band)のパラメーターが取得できません。または、IP アドレスが正しくありません。	1
Please input a port number range from 6001 to 65535 after "-p" option (TCP_IP In-Band).	"-p"(TCP_IP In-Band)のパラメーターが取得できません。または、指定されたポート番号が設定可能な範囲(6001~65535)と異なります。	1
Please input ON or OFF after "-o" option (Shutdown Delay).	シャットダウン開始"-o"(Shutdown Delay)のパラメーターが取得できません。または、ON/OFF 以外の値が設定されています。	1
Please input a config file after "-f" option.	設定ファイルを指定されていません。"-f" のパラメーターが取得できません。	1
Access %s failed!	ファイルのアクセスできません。%s は設定ファイル名です。	1
Skip the line in setting file, lineno=%d.	設定ファイルには問題があります。%d は設定ファイルの行番号です。	1
Please install ESMPro/ServerAgent.	ESMPro/ServerAgent がインストールされていません。	2
Please change to root user.	このツールを実行しているのは、root ユーザーではありません。	4

---

## 1.2 esmsysrep コマンド

---

### 機 能

コマンドラインインタフェースを使用して、ESMPRO/ServerAgent が監視する Syslog 監視対象イベントを設定します。esmsysrep コマンドでは、以下を設定できます。

1. Syslog 監視対象イベントの追加
2. Syslog 監視対象イベントの変更
3. Syslog 監視対象イベントの削除

---

### 設 定

esmsysrep コマンドの使用方法は以下のとおりです。

esmsysrep コマンドで実行した設定を動作中の ESMPRO/ServerAgent に反映するには、ESMPRO/ServerAgent の再起動(ESMRestart)が必要です。

```
# cd /opt/nec/esmpro_sa/tools
# ./esmsysrep [ACTION] [SOURCE] [EVENT] [OPTION]
:
# /opt/nec/esmpro_sa/bin/ESMRestart
```

#### Usage:

```
esmsysrep --add -S <sourcename> -E <eventid> -K <keyword1> [OPTION]...
esmsysrep --mod -S <sourcename> -E <eventid> [-K <keyword1>] [OPTION]...
esmsysrep --del -S <sourcename> -E <eventid>
esmsysrep --list
esmsysrep --help
```

#### Action-selection option and specification:

```
--help    Show this help message
--list    List all event id's information
--add     Add an event id
--mod     Change the configuration of event id
--del     Delete an event id
```

#### Common option and specification:

```
-S <sourcename>    Specify the source name
-E <eventid>       Specify the event id
-K, -1 <keyword1> Specify the first keyword, and the argument of
                  -K will be used if -1 and -K are both specified.
                  It can't be omitted when --add is specified.
```

Other options(defaults in [ ] will be used if the options are not specified in --add):

```
-2 <keyword2>      Specify the second keyword. ["" ]
-3 <keyword3>      Specify the third keyword. ["" ]
-s <ON|OFF>         Set ON/OFF of the SNMP report method. [ON]
-i <ON|OFF>         Set ON/OFF of the TCP/IP IN-BAND report method. [OFF]
-o <ON|OFF>         Set ON/OFF of the TCP/IP OUT-OF-BAND report method. [OFF]
-t <trapname>       Set the trap name. ["" ]
-d <dealmethod>     Set the deal method. ["" ]
```

```
-w <watchtime>      Set the watch time. ["0-24"]
-c <reportcount>     Set the report count. [1]
-r <NONE|SHUTDOWN|REBOOT> Set the action after a report. [NONE]
```



ESMPRO/ServerAgent は、日本語(2 バイト)文字を EUC コードで管理しています。そのため、日本語文字の入力や表示をさせる場合は、ネットワーク経由(ssh コマンドなど)で別の日本語端末からログインし、一時的に LANG 環境変数を日本語環境に変更してください。

1)現在の LANG 環境変数を確認します。

```
# echo $LANG
```

2)LANG 環境変数を ja\_jp.eucJP に変更します。

```
# export LANG=ja_jp.eucJP
```

3)esmamset または esmsysrep コマンドを実行します。

```
# cd /opt/nec/esmpro_sa/tools/
```

```
# ./esmamset [OPTION]
```

```
# ./esmsysrep [OPTION]
```

```
:
```

```
# /opt/nec/esmpro_sa/bin/ESMRestart
```

4)LANG 環境変数を 1) の値に戻します。

```
# export LANG=xxxxxxx
```

## コマンド使用例

```
# ./esmsysrep --add -S TESTSOURCE -E 80001234 -K "test1234" -t "test trap"
# /opt/nec/esmpro_sa/bin/ESMRestart
```

上記の例では、

- ・ソース名"TESTSOURCE"に、"80001234"のイベント ID を新規追加します。
- ・ESMPRO/ServerAgent のサービスを再起動した後、syslog(/var/log/messages)に、文字列"test1234"が記録されると、Syslog 監視機能にて検出し、イベント ID:80001234 を SNMP で通報します。
- ・アラートビューアで表示するトラップ名は"test trap"となります。

## [ACTION] 指定

[ACTION] には以下のオプションを指定します。省略することはできません。

また、複数のオプションを同時に指定することはできません。

オプション	説明
--add	Syslog イベントを追加します。
--mod	既存の Syslog イベントを変更します。
--del	Syslog イベントを削除します。
--list	Syslog イベントの一覧を CSV 形式(コンマ区切り)で出力します。 "Source","EventID","KeyWord1","KeyWord2","KeyWord3","Manager","ALIVE(ALIVELevel)","TrapName","DealMethod","WatchTime","ReportCount","AfterReport"
Source	アラートビューアで表示するソースを表示します。
EventID	アラートビューアで表示するイベント ID を表示します。
KeyWord1	Syslog 監視の通報対象文字列であるキーワード 1 を表示します。
KeyWord2	Syslog 監視の通報対象文字列であるキーワード 2 を表示します。

オプション	説明
KeyWord3	Syslog 監視の通報対象文字列であるキーワード 3 を表示します。
Manager	通報手段(SNMP)の有効または無効を表示します。 ON : 有効 / OFF : 無効
ALIVE (ALIVELevel)	本製品では未サポートです。
TrapName	アラートビューアで表示するトラップ名を表示します。
DealMethod	アラートビューアで表示する対処を表示します。
WatchTime	監視時間帯を表示します。
ReportCount	監視時間帯における、通報に必要な該当イベントの発生回数を 1~65535 の数字で表示します。
AfterReport	通報後の動作を表示します。 NONE : 何もしない SHUTDOWN: シャットダウン REBOOT : 再起動
--help	ヘルプ (Usage:)を表示します。

## [SOURCE] 指定

[SOURCE] には以下のオプションを指定します。省略することはできません。

オプション	説明
-S <sourcename>	[ACTION]の対象となるソース名を半角英数字の大文字で指定します。

## [EVENT] 指定

[EVENT] には以下のオプションを指定します。省略することはできません。

オプション	説明
-E <eventid>	<p>Syslog イベントを追加する場合、以下の命名規則にしたがって、[ACTION] の対象となるイベント ID を 16 進数(半角英数字 0~F)の 8 桁で指定します。</p> <p>&lt;監視イベント ID 命名規則&gt;</p> <p>“x0000yyy”形式で指定します。(例: 40000101、800002AB、C0000101)</p> <p>“x” には、4,8,C の中から設定します。それぞれの意味は以下のとおりです。</p> <ul style="list-style-type: none"> <li>4 : 情報系イベントを意味します。 ESMPRO/ServerManager のアラートビューアのアイコンが「緑色」で表示されます。</li> <li>8 : 警告系イベントを意味します。 ESMPRO/ServerManager のアラートビューアのアイコンが「黄色」で表示されます。</li> <li>C : 異常系イベントを意味します。 ESMPRO/ServerManager のアラートビューアのアイコンが「赤色」で表示されます。</li> </ul> <p>“yyy” には、0x001(1)~0xFFFF(4095)の範囲内で任意の 16 進数値を設定します。</p> <p>Syslog イベントを変更・削除する場合、該当するイベント ID を指定します。</p>

## [OPTION] 指定

[OPTION] には以下のオプションを指定します。複数のオプションを同時に指定することもできます。  
設定する値にスペースが含まれるときは、前後に”(ダブルクォーテーション)を付加してください。

オプション	説明
-------	----

オプション	説明
-K <keyword1> -1 <keyword1>	keyword1 を設定します。256 バイト以内の 1 バイト文字を使用します。-K と -1 を同時に指定したときは、-K の内容が設定されます。 [ACTION]が--add のときは省略することができません。
-2 <keyword2>	keyword2 を設定します。256 バイト以内の 1 バイト文字を使用します。 [ACTION]が--add のときの既定値は、""(空白)です。
-3 <keyword3>	keyword3 を設定します。256 バイト以内の 1 バイト文字を使用します。 [ACTION]が--add のときの既定値は、""(空白)です。
-s ON OFF	通報手段(SNMP)の有効または無効を設定します。 ON : 有効 / OFF : 無効 [ACTION]が--add のときの既定値は、"ON"です。
-i ON OFF	通報手段(TCP_IP In-Band)の有効または無効を設定します。 ON : 有効 / OFF : 無効 [ACTION]が--add のときの既定値は、"OFF"です。
-o ON OFF	通報手段(TCP_IP Out-of-Band)の有効または無効を設定します。 ON : 有効 / OFF : 無効 [ACTION]が--add のときの既定値は、"OFF"です。
-t <trapname>	アラートビューアで表示するトラップ名を設定します。79 バイト以内の文字列で、1 バイトまたは 2 バイト文字が使用できます。日本語も使用できます。 [ACTION]が--add のときの既定値は、""(空白)です。
-d <dealmethod>	アラートビューアで表示する対処を設定します。507 バイト以内の文字列で、1 バイトまたは 2 バイト文字が使用できます。日本語も使用できます。 [ACTION]が--add のときの既定値は、""(空白)です。
-w <watchtime>	監視時間帯を設定します。複数の時間帯を指定するときは、コンマ(,)区切りで設定します。 [ACTION]が--add のときの既定値は、"0-24"です。
-c <reportcount>	監視時間帯における、通報に必要な該当イベントの発生回数を 1~65535 の数字で設定します。 [ACTION]が--add のときの既定値は、"1"です。
-r <NONE   SHUTDOWN   REBOOT>	通報後の動作を設定します。<action>は以下のいずれかを設定します。 NONE : 何もしない SHUTDOWN: シャットダウン REBOOT : 再起動 [ACTION]が--add のときの既定値は、"NONE"です。

## 戻り値

esmsysrep コマンドの戻り値は以下のとおりです。

戻り値が 0 以外の場合は、コンソールにエラーメッセージを表示します。

戻り値	説明
0	設定に成功しました。
0 以外	設定に失敗しました。詳細はエラーメッセージを参照してください。

## エラーメッセージ

エラーメッセージは以下のとおりです。

メッセージ	説明	戻り値
Only root can execute the tool.	ログインしているユーザーに実行権限がありません。	1
プログラム名: error while loading	ESMPRO/ServerAgent がインストールされてい	127



メッセージ	説明	戻り値
shared libraries: ライブラリーのパス: cannot open shared object file: No such file or directory	ません。	
parameter error : "オプション名" is not specified.	省略不可の"オプション名"が指定されていません。	1
parameter error : argument of "オプション名" is too long.	"オプション名"に指定したパラメーターの文字列長が長すぎます。	1
parameter error : argument of "オプション名" is too short.	"オプション名"に指定したパラメーターの文字列長が短すぎます。	1
parameter error : argument of "オプション名" is invalid.	"オプション名"に指定したパラメーターは無効です。	1
parameter error : option "オプション名" requires an argument.	"オプション名"にパラメーターが指定されていません。	1
parameter error : invalid option "オプション名".	"オプション名"に指定したオプションは無効です。	1
parameter error : "オプション名".	"オプション名"に指定したオプションが不正です。	1
Can't make all of the keywords empty.	--mod の設定を反映すると、キーワード(1~3)が、すべて""(空白)となります。	1
Can't access "<sourcename>", which isn't the object source of this tool.	本コマンドで設定できないソース名が指定されました。	1
ESMntserver service is not started.	ESMntserver が起動していません。	1
Other program is accessing the syslog events setting.	他のプログラム(ESMamsadm など)が syslog 設定にアクセスしているため、アクセスできません。	1
"<sourcename>/<eventid>" already exists.	--add で指定したソース名/イベント ID は、すでに存在しています。	1
"<sourcename>/<eventid>" doesn't exist.	--mod または --del で指定したソース名/イベント ID は存在しません。	1
Access the "<sourcename>/<eventid>" failed.	[ACTION]に失敗しました。	1

---

## 2. ツールについて

---

ツールを使用するには、root ユーザーでログインしてください。

---

### 2.1 障害情報採取ツール(collectsa.sh)

---

#### 機 能

本機または ESMPRO/ServerAgent で発生した問題を調査するため、本機情報を収集します。  
障害情報採取ツールで収集する情報は以下を参照してください。

<https://www.support.nec.co.jp/View.aspx?id=3170102037>

collectsa.sh 採取情報一覧

#### 使 用 方 法

障害情報採取ツールの使用方法是以下のとおりです。

- 1) root ユーザーでログインします。



SELinux が無効以外に設定されている場合、障害情報採取ツールを実行時の syslog に setroubleshoot 関連のメッセージが記録される場合があります。

syslog へのメッセージの記録を抑止するには以下のウェブサイトを参照し、setroubleshootd プロセスを一時的に無効化してください。

<https://access.redhat.com/ja/solutions/3220471>

- 2) 任意のディレクトリに移動します。
- 3) 障害情報採取ツールを実行します。

```
# /opt/nec/esmpro_sa/tools/collectsa.sh
```

カレントディレクトリに collectsa.tgz が作成されます。

- 4) NEC カスタマーサポートセンター経由でお問い合わせください。

NEC カスタマーサポートセンターの案内にしたがって、collectsa.tgz の提供をお願いします。



障害情報採取ツールで収集する情報で、以下のディレクトリやファイルの数が多い場合、またはファイルのサイズが大きい場合、情報の収集に数時間掛かることがあります。

- /sys/ ディレクトリ配下

- /var/log/sa ディレクトリ配下

→システムの動作統計情報(SAR)の格納先



障害情報採取ツールを実行するカレントディレクトリの空き容量が少ない場合、収集処理が正常に動作せず意図しないディレクトリに格納される場合があります。

障害情報採取ツールは空き容量に余裕のあるカレントディレクトリで実行してください。



障害情報採取ツールでパーティションの情報を採取しますが、ご使用の構成により、CPU が高負荷となる場合があります。必要に応じて、“-nas” フラグで採取してください。

```
# /opt/nec/esmpro_sa/tools/collectsa.sh -nas
```



SELinux が無効以外に設定されている場合、情報を採取するためのコピーなどの処理で、以下のメッセージが大量に記録される場合があります。この場合は collectsa.tgz をご提供ください。

以下は setroubleshoot 関連メッセージの一例となります。

「XXXXX」は英数字で、状況により異なります。

```
setroubleshoot[XXXXX]: SELinux により、/usr/bin/cp による create アクセスが、ディレクトリー fd で拒否されました。完全な SELinux メッセージを見るには、sealert -l XXXXX を実行します
setroubleshoot[XXXXX]: SELinux により、/usr/bin/cp による create アクセスが、ディレクトリー fd で拒否されました。#012#012***** プラグイン catchall (100. 信頼性) による示唆 *****#012#012cp に、fd directory の create アクセスがデフォルトで許可されるべきと考える場合。#012 このようにします: バグとして報告してください。#012 ローカルのポリシーモジュールを生成すると、#012 このアクセスを許可することができます。#012 そして、以下を実行します: #012 以下を実行して、このアクセスを許可します:#012# ausearch -c 'cp' --raw | audit2allow -M my-cp#012# semodule -X 300 -i my-cp.pp#012
...
setroubleshoot[XXXXX]: SELinux により、/usr/bin/cp による create アクセスが、ディレクトリー attr で拒否されました。完全な SELinux メッセージを見るには、sealert -l XXXXX を実行します
setroubleshoot[XXXXX]: SELinux により、/usr/bin/cp による create アクセスが、ディレクトリー attr で拒否されました。#012#012***** プラグイン catchall (100. 信頼性) による示唆 *****#012#012cp に、attr directory の create アクセスがデフォルトで許可されるべきと考える場合。#012 このようにします: バグとして報告してください。 #012 ローカルのポリシーモジュールを生成すると、#012 このアクセスを許可することができます。#012 そして、以下を実行します: #012 以下を実行して、このアクセスを許可します:#012# ausearch -c 'cp' --raw | audit2allow -M my-cp#012# semodule -X 300 -i my-cp.pp#012
```

## 障害情報採取ツールの動作に問題が発生した場合

障害情報採取ツールが正しく動作しない(終了しない等)場合は、採取済みの情報を採取の上、NEC カスタマーサポートセンター経由でお問い合わせください。

- 1) 障害情報採取ツールを終了させます。

- 1-1) 障害情報採取ツールを実行しているターミナルで、<Ctrl>+<C>キーを押します。

- 1-2) 障害情報採取ツールが終了したことを確認します。

```
# ps aux | grep collectsa.sh |grep -v grep
```

たとえば下記のように表示された場合、collectsa.sh はバックグラウンドで実行されています。

```
root 11313 0.0 0.4 4196 1124 pts/0 T 14:46 0:00 /bin/bash ./collectsa.sh
```

- 1-3) バックグラウンドで実行されていた場合は、プロセスを終了させます。

```
# kill -9 {pid}
```

(例) # kill -9 11313

- 2) カレントディレクトリに作成された collectsa ディレクトリを tgz 形式で圧縮します。  
# tar czvf collectsa\_dir.tgz collectsa/
- 3) NEC カスタマーサポートセンター経由でお問い合わせください。  
NEC カスタマーサポートセンターの案内にしたがって、collectsa\_dir.tgz の提供をお願いします。

# ESMPRO/ServerAgent for GuestOS Ver.1.5 他社機版 ESMPRO/ServerAgent Ver.1.5

# 5

## 注意事項

ESMPRO/ServerAgent の注意事項について説明します。

Linux サポート情報リストに、各ディストリビューションの注意・制限事項を公開しておりますので、こちら  
も参照してください。

■Linux サポート情報リスト【Linux サービスセットご契約のお客様限定】

<https://www.support.nec.co.jp/View.aspx?id=3140001278>

## ESMPRO/ServerAgentの仕様

---

### OSまたはサービス起動時に、ESMamvmainでsegfaultが発生するときがある

---

対象：ESMPRO/ServerAgent 全バージョン

詳細：Syslog イベントは 1024 個まで使用できますが、他製品の通報テーブルを取り込んだ際に ESMamvmain サービスが起動時に segfault が発生します。PID やアドレスを示す値は、状況により異なります。

```
kernel: ESMamvmain[0000]: segfault at 0000000000000000 ip 0000000000000000  
sp 0000000000000000 error 4 in amvmmnev.dll[0000000000000000+000000]
```

対処：以下に格納されているファイルを移動し、Syslog イベント数を減らします。

```
/opt/nec/report/inf  
/opt/nec/report/table
```

---

### ESMamvmainが高負荷となるときがある

---

対象：すべての ESMPRO/ServerAgent バージョン

詳細：Esmamvmain サービスは Syslog 監視機能を提供しています。syslog(/var/log/messages)などの監視対象となっているファイルに書き込みが多い場合は、ESMamvmain サービスも高負荷となります。

対処：監視対象となっているファイルの書き込みを抑止してください。

---

### アンマウントした時に、ファイルシステムの空き容量を誤検出するときがある

---

対象：Linux OS

詳細：ファイルシステム監視機能は、監視間隔毎にマウントポイントを確認し、OS の関数である statfs()関数を利用して、ファイルシステム情報を取得しています。

- 1) マウントポイントを確認する。
- 2) マウントポイントを元に statfs()関数を利用して、情報を取得する。

上記の 1)と 2)の間にマウントポイントがアンマウントされたとき、statfs()関数からはエラーではなく、上位にあるマウントポイントのファイルシステム情報が返却される事を確認しました。

- 1) マウントポイントを確認(/hoge)する。  
→/hoge がアンマウントされる。
- 2) マウントポイント(/hoge)を元に statfs()関数を利用して、情報を取得する。  
空き容量/全容量は、上位である / の情報が返却される。

また、/etc/mntab に新たなマウントポイントが追加された場合、監視対象とするため、stat()関数によりマウント状況を確認します。マウントされている場合、statfs()関数により全容量を取得します。

しかし、stat()関数の処理時点ではマウントされていたが、statfs()関数の処理時点でアンマウントされていた場合は、全容量は固定値(4294967295MB)で認識します。

異常しきい値・警告しきい値の既定値は全容量を元に計算するため、次回監視時に異常イベントを検知します。

CLUSTERPRO を導入されているとき、クラスター構成システムでのクラスター停止時・フェールオーバー発生時に本現象が発生する可能性があります。

対処：以下の 2 点の対処により回避してください。

ファイルシステム監視機能が新しいマウントポイントを検出したとき、既定値として、監視しないように変更することで、誤検出を防止します。コントロールパネルから監視する設定に変更できます。

<手順>

- 1) root 権限のあるユーザーでログインします。
- 2) 以下のコマンドでファイルシステム監視サービスを一時的に停止します。  
# systemctl stop ESMfilesys.service
- 3) /opt/nec/esmpro\_sa/data/ディレクトリに移動します。  
# cd /opt/nec/esmpro\_sa/data

- 4) 念のため、ファイルシステム監視の設定ファイルをバックアップします。  
# cp esmfs.inf esmfs.org
- 5) テキストエディタを使用して、esmfs.inf の 4 行目にある ThSwitchDef を以下のように変更します。

[変更前]	[変更後]
ThSwitchDef=1	ThSwitchDef=0

- 6) 以下のコマンドでファイルシステム監視サービスを再開します。

```
# systemctl start ESMfilesys.service
```

※コントロールパネル(ESMagntconf)からファイルシステム監視の設定を変更すると、既定値が監視するに戻ります。上記の手順で、もう一度、"ThSwitchDef=0"に変更してください。

アンマウント時に一時的にファイルシステム監視を停止します。

<手順>

- 1) root 権限のあるユーザーでログインします。
- 2) 以下のコマンドでファイルシステム監視サービスを一時的に停止します。  
# systemctl stop ESMfilesys.service
- 3) ファイルシステムのアンマウントを実行します。
- 4) 以下のコマンドでファイルシステム監視サービスを再開します。  
# systemctl start ESMfilesys.service

---

#### OSまたはサービスを再起動するとファイルシステム監視のしきい値が既定値となる

対象：ESMPRO/ServerAgent 全バージョン

詳細：ファイルシステム監視サービスが起動したときにマウントされていないマウントポイントは監視対象から外れるため、監視対象の設定を削除します。その後、マウントされて、マウントポイントを検出したときに新規マウントポイントと認識するため、監視対象の設定が既定値となります。

<システム起動後の動作例>

```
↓(オート)マウント[ポイント A] → システム起動前の設定を使用
↓ファイルシステム監視サービスの起動(マウントポイント確認)
  マウント[ポイント A]を検出、設定は継続使用
  マウント[ポイント B]は未検出、設定は削除(監視対象外とする)
↓(オート)マウント[ポイント B]
↓ファイルシステム監視サービスの監視間隔(マウントポイント確認)
  マウント[ポイント B]を検出、設定は既定値(新規マウントポイントと認識)
```

回避：[前準備]

ファイルシステム監視サービス(ESMfilesys)を自動起動しない設定にします。

```
# systemctl disable ESMfilesys.service
```

システムが起動して、すべてマウントした後にファイルシステム監視サービスを起動します。

```
# systemctl start ESMfilesys.service
```

---

#### rpcbindとnetworkサービスに関する注意事項

対象：Linux OS

詳細：ESMPRO/ServerAgent では、rpcbind と network サービスの機能を利用しています。

ESMPRO/ServerAgent 運用中に rpcbind と network サービスの停止や再起動をされたとき、ESMPRO/ServerAgent は正常に動作できません。

対処：以下のコマンドを実行して、ESMPRO/ServerAgent のサービスを再起動します。

```
# /opt/nec/esmpro_sa/bin/ESMRestart
```

---

#### OSまたはサービス停止時に、syslogにメッセージが記録されるときがある

対象：ESMPRO/ServerAgent 全バージョン

詳細：OS またはサービス停止時、syslog に以下のメッセージが記録されるときがあります。「XXXXXX」は英数字で、状況により異なります。

###ERR###RPC###: RPC XXXXX

対処: OS またはサービス停止時のみに発生する現象であり、次回の OS またはサービス起動時の動作に影響はありません。

---

#### OSまたはサービス停止時に、ESMamvmainでsegfaultが発生するときがある

対象: 64 ビット Linux OS 上で動作している ESMPRO/ServerAgent 全バージョン

詳細: ESMamvmain サービスが停止時にファイルをクローズしていますが、タイミングにより、その関数 (dlclose)内で、segfault が発生します。また、syslog には、general protection も記録される場合があります。PID やアドレスを示す値は、状況により異なります。

```
kernel: ESMamvmain[0000] general protection rip:000000000000 rsp:000000000
error:0
kernel: ESMamvmain[0000]: segfault at 0000000000000000 rip 0000000000000000
rsp 0000000000000000 error 0
```

対処: OS またはサービス停止時に呼び出している dlclose 関数内で発生する現象であり、次回の OS またはサービス起動時の動作に影響はありません。

---

#### システム高負荷時のsyslogにpidofのメッセージが記録されるときがある

対象: 64 ビット Linux OS 上で動作している ESMPRO/ServerAgent 全バージョン

詳細: ESMPRO/ServerAgent では、pidof コマンドを使用する処理があり、システム高負荷時の syslog に以下のメッセージが記録されるときがあります。PID は、状況により異なります。

```
pidof[0000]: can't read sid for pid 0000
```

対処: OS の動作、ESMPRO/ServerAgent の動作に影響はありません。

---

#### SNMP通報の遅延もしくはSNMP通報漏れが発生するときがある

対象: ESMPRO/ServerAgent 全バージョン

詳細: ESMPRO/ServerManager を起動した状態で、かつサーバ状態/構成情報の更新間隔をデフォルト設定 (60 秒)より短く設定したとき、通報の遅延もしくは通報漏れが発生する事があります。

対処: サーバ状態/構成情報の更新間隔はデフォルト設定の 60 秒以上で運用するようにしてください。またはマネージャ通報(TCP/IP)を使用するように運用してください。

---

#### OS起動時のSNMP通報遅延が発生するときがある

対象: ESMPRO/ServerAgent 全バージョン

詳細: OS 起動時に通報の準備ができていない時に通報対象の現象が発生したとき、リトライ処理をします。通報対象の現象が発生するタイミングにより、OS 起動時に通報されるときとリトライ(5分)後に通報されるときがあります。

対処: OS が起動してから 5 分以上経過後に、アラートビューアへ表示されるメッセージを確認してください。

---

#### SNMP通報の通報手段が有効でないときにもSNMP通報が送信されるときがある

対象: Linux OS

詳細: OS 起動時に通報の準備ができていない時に通報対象の現象が発生したとき、リトライ処理をします。リトライ処理は、SNMP の通報手段(ON/OFF)に関係なく通報を処理するため、リトライ処理をするタイミングでトラップ通報先 IP が設定されたとき、SNMP 通報の通報手段が OFF のときでも通報します。

対処: 通報させたくないとき、OS 起動後 5 分以上経ってから設定してください。

---

#### 障害情報採取ツールを実行中にコンソールの表示またはsyslogにメッセージが記録されるときがある

詳細: 障害情報採取ツール(collectsa.sh)を実行中、コンソールの表示または syslog に以下のメッセージが記録されるときがあります。



```
BUG: scheduling while atomic: kipmi0
```

collectsa.sh では ipmitool を使用して情報を採取する処理があり、ipmi ドライバーの既知問題が発生した場合にメッセージが記録されます。ipmi ドライバーの排他制御方法に問題があるため、システムの動作状況や、現象発生タイミングによっては、運用中にカーネルパニックなどの致命的な問題が発生する可能性があります。この不具合は、kernel-2.6.32-504.el6 以降のカーネルで修正されておりますので、カーネルアップデートをご検討ください。

■System logs include a message similar to "kernel: BUG: scheduling while atomic: kipmi0"

<https://access.redhat.com/solutions/691403>

■BUG: scheduling while atomic in acpi\_ipmi

<https://access.redhat.com/solutions/656603>

```
kernel: process 'sysctl' is using deprecated sysctl (syscall)
net.ipv6.neigh.vswif0.base_reachable_time; Use
net.ipv6.neigh.vswif0.base_reachable_time_ms instead.
kernel: process 'cp' is using deprecated sysctl (syscall)
net.ipv6.neigh.vswif0.base_reachable_time; Use
net.ipv6.neigh.vswif0.base_reachable_time_ms instead.
kernel: process 'cp' is using deprecated sysctl (syscall)
net.ipv6.neigh.default.retrans_time; Use
net.ipv6.neigh.default.retrans_time_ms instead.
```

カーネルパラメータの名称が変更されることを示す警告です。旧名称のカーネルパラメータにアクセスしたことを示すメッセージです。システムのエラーを示すものではなく、システムへの影響はありません。

```
kernel: ACPI Error: No handler for Region [OEM2] (ffff88105999d780) [IPMI]
(20090903/evregion-319)
kernel: ACPI Error: Region IPMI(7) has no handler (20090903/exfldio-295)
kernel: ACPI Error (psparse-0537): Method parse/execution failed
[_SB_.PMI0._PMM] (Node ffff88105999f470), AE_NOT_EXIST
```

「/sys/bus/acpi/devices/ACPI000D:00/power1\_average」などを含む、/sys/bus 配下の全ファイル(サブディレクトリ含む)をコピーしていることが原因です。ACPI テーブルの IPMI 領域を介した電源管理機能が利用できないことを示すメッセージです。システムのエラーを示すものではなく、システムへの影響はありません。

```
kernel: netlink: 12 bytes leftover after parsing attributes.
```

snmpd からカーネルに渡されたデータが規定より 12byte 長いことを示すメッセージです。システムのエラーを示すものではなく、システムへの影響はありません。

```
kernel: CPUFREQ: ondemand sampling_rate_max sysfs file is deprecated - used
by: cp
kernel: CPUFREQ: Per core ondemand sysfs interface is deprecated -
sampling_rate_max
kernel: CPUFREQ: Per core ondemand sysfs interface is deprecated -
sampling_rate_min
kernel: CPUFREQ: Per core ondemand sysfs interface is deprecated -
sampling_rate
kernel: CPUFREQ: Per core ondemand sysfs interface is deprecated - up_threshold
kernel: CPUFREQ: Per core ondemand sysfs interface is deprecated -
ignore_nice_load
kernel: CPUFREQ: Per core ondemand sysfs interface is deprecated -
powersave_bias
```

sys/devices/system/cpu/cpu0/cpufreq/ondemand/配下の将来廃止される予定のファイルにアクセスしたことを示すメッセージです。システムのエラーを示すものではなく、システムへの影響はありません。

```
kernel: mbox_read: Bad State
kernel: mbox_read: Bad State
```

lpfc ドライバーが作成した/sys/class/scsi\_host/hostX 配下のファイルにアクセスしたことを示すメッセージです。システムのエラーを示すものではなく、システムへの影響はありません。

```
警告: command substitution: ignored null byte in input
```

collectsa.sh の処理の中で終端の文字列である'¥0'が変数に含まれると警告メッセージが表示されます。メッセージの表示のみでシステムのエラーを示すものではなく、システムへの影響はなく、collectsa.sh の収集機能にも影響はありません。

## WebSAM AlertManagerとの通報連携するためには、レジストリーを登録する

対象：ESMPRO/ServerAgent 全バージョン

詳細：Syslog イベントの設定で追加したイベントを WebSAM AlertManager で通報連携するとき、ESMPRO/ServerManager をインストールしたマシンに、以下のレジストリーを登録してください。

対処：レジストリーに以下のキー、名前、データを設定してください。

xxxx が新しく設定するアラートタイプの名前です。

アラートタイプ(xxxx)には以下を設定してください。

- ・ Syslog 監視で設定した通報ソース名  
Syslog 監視では、通報ソース名がアラートタイプに変換されるため。
- ・ 以下のアラートタイプ  
AM  
bootmsglogger  
DS450

※64bit OS では、以下の記述の

HKEY\_LOCAL\_MACHINE¥SOFTWARE¥NEC

を

HKEY\_LOCAL\_MACHINE¥SOFTWARE¥Wow6432Node¥NEC

に読み替えてください。

```
[HKEY_LOCAL_MACHINE¥SOFTWARE¥NEC¥NVBASE¥AlertViewer¥AlertType¥xxxx]
"WavDefault"="Server.wav"
"AniDefault"="Default.bmp"
"Image"="Default.bmp"
"SmallImage"="Default.bmp"
```

=の左辺が名前、右辺がデータです。

データはいずれも文字列型です。

Windows XP(Home Edition は除く), 2000/2003, Vista では追加したアラートタイプのキー(¥AlertType¥xxxx) に対して、以下のアクセス権を設定してください。

Administrators	フルコントロール
Everyone	読み取り
SYSTEM	フルコントロール

## ESMPRO ユーザーグループ (\*) フルコントロール

(\*) ESMPRO ユーザーグループ は、ESMPRO/ServerManager インストール時に指定した、ESMPRO を使用するユーザーを管理するためのグループ名です。

これはインストール時にユーザーが指定するグループ名ですが、以下のレジストリーにも格納されています。

[HKEY\_LOCAL\_MACHINE\SOFTWARE\NEC\NVBASE]

名前 : LocalGroup

以下の製品ページ FAQ もご参考にしてください。

<https://jpn.nec.com/websam/alertmanager/faq.html>

Q43.アラートタイプの追加手順を教えてください。

## Linux OSに含まれるパッケージの仕様

### ESMPRO/ServerAgentのメモリ使用量が増加するときがある

対象 : Red Hat Enterprise Linux

詳細 : dlopen 関数が動的ライブラリーを二重ロードし、かつ失敗した場合に(32+ファイル名)バイトメモリリークが発生します。二重ロードがともに成功した場合、または一重ロードで失敗した場合はいずれもメモリリークは発生しません。

弊社の評価で、net-snmp-libs パッケージに含まれる libsnmp.so ライブラリーの snmp\_sess\_init 関数が確保したメモリを開放しないためにメモリが増加することを確認しています。

snmp\_sess\_init 関数は通報する際に使用しており、使用しているプロセスと 1 回と 10 回、100 回の測定結果(単位は KB)は、次のとおりです。

プロセス名	1 回 (KB)	増加量 (KB)	10 回 (KB)	増加量 (KB)	50 回 (KB)	増加量 (KB)	100 回 (KB)
ntagent	3636	876	4512	12	4524	16	4540
ESMamvmain	3320	212	3532	0	3532	4	3536
ESMcmn	5940	0	5940	0	5940	20	5960

この結果から 10 回までに、数十パーセントの増加は見られますが、それ以降は僅かな増加となっており、メモリ使用量が同じサイズで増加し続ける現象ではないことを確認しています。しかし、プロセスのメモリ使用量が大きくなった場合は、回避策でメモリの開放をお願いします。

回避 : メモリを開放するために、ESMPRO/ServerAgent のサービスを再起動します。

```
# /opt/nec/esmpro_sa/bin/ESMRestart
```

### SELinuxが有効の時、障害情報採取ツール(collectsa.sh)を実行すると、syslogにメッセージが記録される

対象 : Red Hat Enterprise Linux

詳細 : 障害情報採取ツールでは、/proc 配下のファイルを収集しております。SELinux が有効の時、/proc 配下へのアクセスが制限され、syslog に複数のメッセージが記録されます。

```
SELinux is preventing cp ...
```

対処 : 障害情報採取ツールで、アクセス制限されたファイルが収集されませんが、OS の動作には影響ありません。

## ESMPRO/ServerManagerの表示

DVDコンボドライブを搭載した機種で、[構成情報]-[ストレージ]-[CD-ROM]を複数表示するときがある

対象：DVD コンボドライブを搭載した機種の 2.4 系カーネル以降

詳細：2.4 系カーネルでは、IDE 接続の書き込み可能な光ドライブの書き込み機能を使用するとき、ide-scsi エミュレーションが必要となります。このとき、光ドライブは IDE 接続と SCSI 接続の両方から認識されるため、本現象が発生します。

対処：表示のみの影響のみであり、ESMPRO/ServerAgent の機能に影響はありません。

---

### ネットワークの転送スピードが正しく表示されないときがある

対象：Linux OS

詳細：ハードウェアの仕様、および、ドライバーの仕様により、[構成情報]-[ネットワーク]において、ネットワークの転送スピードが正しく表示されないときがあります。

対処：表示のみの影響であり、ESMPRO/ServerAgent の機能に影響はありません。

---

### サポートしているネットワークのインタフェースタイプ

対象：Linux OS

詳細：ESMPRO/ServerManager がサポートしているネットワークのインタフェースタイプはイーサネット、ループバックのみとなります。それ以外のタイプのときは、ネットワークのタイプが正しく表示されないときがあります。

---

### 物理メモリ使用量の表示

対象：ESMPRO/ServerAgent 全バージョン

詳細：[構成情報]-[システム]-[メモリ]で表示している物理メモリ使用量は、/proc/meminfo の情報を元に以下の計算式で、メモリ使用量を算出しています。

メモリ使用量 = MemTotal-MemFree

また、物理メモリ使用率は以下の計算式となります。

物理メモリ使用率 = (MemTotal-MemFree) \* 100 / MemTotal

上記値は、Buffers と Cached を含んだ値となるため、OS の状況によっては、高い値が表示されるときがあります。

---

### シリアルポートのコネクタ形状が不明と表示されるときがある

対象：SMBIOS Type8 Port Connector Information が未サポートの装置

詳細：[構成情報]-[I/O デバイス]で表示しているシリアルポートのコネクタ形状は、SMBIOS Type8 Port Connector Information の情報を元に表示しております。SMBIOS Type8 Port Connector Information が未サポートの装置において、シリアルポートのコネクタ形状は、不明と表示します。SMBIOS Type8 のサポート有無は、dmidecode コマンドの実行結果に以下の情報(type 8)が表示されるかを確認してください。

Handle 0x000C, DMI type 8, 9 bytes

Port Connector Information

対処：表示のみの影響であり、ESMPRO/ServerAgent の機能に影響はありません。

---

### マウス情報が表示されない

対象：Linux OS

詳細：[構成情報]-[I/O デバイス]で表示しているマウス情報は、/etc/sysconfig/mouse ファイルの内容を情報元としています。そのため、/etc/sysconfig/mouse ファイルが存在しないとき、マウス情報は表示されません。

対処：表示のみの影響であり、ESMPRO/ServerAgent の監視機能に影響はありません。

---

### ハードディスクドライブ情報の表示

対象：Linux OS

詳細：[構成情報]-[ストレージ]で表示しているハードディスクドライブ情報は、/proc/scsi/scsi の情報を元にしており、実際のハードウェアと異なる情報が表示されるときがあります。一例として、SCSI ディス

クや RAID 環境のときはデバイスから取得した値(INQUIRY)がそのまま Vendor に設定されますが、SATA ディスクのとき、T10 SCSI/ATA translation の仕様に従い、'ATA 'という文字列が入ります。

----

```
Host: scsi0 Channel: 00 Id: 00 Lun: 00
Vendor: ATA      Model: SSDSA2SH064G1GC Rev: 445C
Type:   Direct-Access          ANSI SCSI revision: 05
```

## OS環境により、UUID/GUIDが異なるときがある

---

対象 : Linux OS

詳細 : [サーバ状態]で表示している GUID は、dmidecode コマンドより、[構成情報]-[ハードウェア]-[装置情報]-[システムマネージメント]の UUID/GUID は、SMBIOS から情報を取得しています。dmidecode のバージョンが 2.10 以降のときは、SMBIOS のバージョンを判断しています。SMBIOS のバージョンが 2.6 以降のときは UUID をバイトオーダーへ入れ替える処理があります。その影響により、UUID/GUID が異なる場合があります。

例)SMBIOS Ver.2.6 の値

12345678 ABCD EFGH IJKL MNOPQRSTUVWXYZ

波下線の部分が 4byte 2byte 2byte 単位でバイト交換される。

78563412 CDAB GHEF IJKL MNOPQRSTUVWXYZ

対処 : ESMPPRO/ServerManager Ver.5.28 以降を使用すれば、マネージメントコントローラ管理と SNMP 管理の両方が有効の場合は、別々のサーバーとして登録される問題が修正されています。

**ESMPRO/ServerAgent for GuestOS Ver.1.5**  
**他社機版 ESMPRO/ServerAgent Ver.1.5**

---

6

## よくあるご質問

ESMPRO/ServerAgent のよくあるご質問について説明します。

## ESMPRO/ServerManagerから自動発見に失敗する

---

### アクセス制限の設定を確認してください

ESMPRO/ServerManager から監視するとき、以下のポートを利用しています。お使いの環境でアクセス制限の設定をされているとき、以下のポートに対してアクセスを許可する設定か確認してください。

```
snmp          161/udp
snmp-trap     162/udp
```

---

### snmpdが起動していることを確認してください

以下のコマンドを実行して、snmpd が起動していることを確認してください。

```
# ps ax | grep snmpd
- 起動しているときは、何もする必要はありません。
- 起動していないときは、snmpd の設定を変更した後、snmpd を起動します。
# systemctl enable snmpd.service
# systemctl start snmpd.service
```

---

### snmpdで使用するコミュニティ名の設定内容を確認してください

snmpd.conf に設定したコミュニティ名と ESMPRO/ServerAgent で設定しているコミュニティ名が一致しているか確認してください。設定方法の詳細につきましては本書の2章(2. 全般プロパティ)を参照してください。

---

### snmpd.confの設定内容を確認してください

ESMPRO/ServerManager から監視するときは、ESMPRO MIB 配下に対して、コミュニティの権利を「READ WRITE」以上に設定する必要があります。既定値では、権限が不足していますので、SNMP 環境設定ファイルを変更してください。

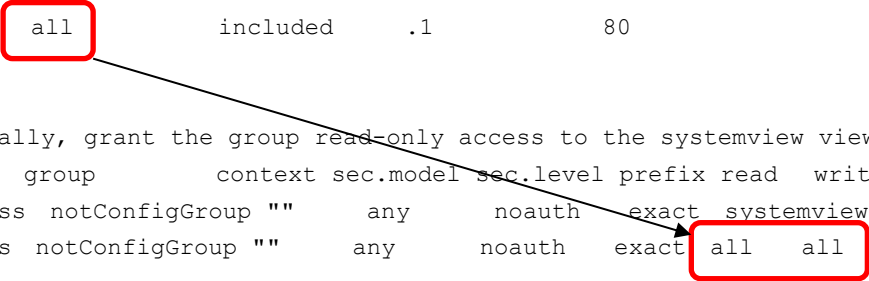
```
ESMPRO MIB : .1.3.6.1.4.1.119.2.2.4.4
Ethernet Like MIB : .1.3.6.1.2.1.10.7
```

SNMP 環境設定ファイルは、/etc/snmp/snmpd.conf を使用することが多いですが、他のパッケージや OS の仕様により異なる場合があります。以下の記述例は、既定値のコミュニティ(public)のすべての MIB に対して、「READ WRITE」権限を与えます。

記載例)

```
####
# Third, create a view for us to let the group have rights to:
#      name          incl/excl    subtree      mask(optional)
#view   systemview   included     .1.3.6.1.2.1.1
#view   systemview   included     .1.3.6.1.2.1.25.1.1
view    all          included     .1          80

####
# Finally, grant the group read-only access to the systemview view.
#      group          context sec.model sec.level prefix read  write notif
#access notConfigGroup ""      any      noauth   exact  systemview none none
access notConfigGroup ""      any      noauth   exact  all    all    none
```



各設定内容の詳細については、snmpd.conf のヘルプを参照してください。

snmpd.conf のヘルプは、man コマンドを実行します。

```
# man snmpd.conf
```

---

### snmpd.confの設定内容を確認してください

snmpd.conf に以下の設定があるか確認してください。

```
dlmod ntpass /opt/nec/esmpro_sa/lib/ntpass.so
ntpass .1.3.6.1.4.1.119.2.2.4.4
ntpass .1.3.6.1.2.1.10.7
```

上記の設定は ESMPRO/ServerAgent がインストール時に ESMPRO MIB と Ethernet Like MIB の SNMP 要求に対応するため、snmpd.conf に書き込む設定情報です。これらの設定が存在しないとき、上記の設定を追記後に snmpd を再起動してください。設定が存在しない原因は、ESMPRO/ServerAgent インストール後に snmpd の再インストールやアップグレードをしたことが考えられます。

### 登録済みの設定内容を確認してください

ESMPRO/ServerManager に登録されているサーバー名、IP アドレスを確認してください。登録されているサーバーの「マシン名」または「IP アドレス」が登録しようとするサーバーの「マシン名」「IP アドレス」と重なっていないか確認してください。重なっていると登録できません。

### /etc/hosts.deny、/etc/hosts.allow の設定内容を確認してください

/etc/hosts.deny と /etc/hosts.allow ファイルの設定を確認してください。/etc/hosts.deny で原則禁止の設定をしているときは、/etc/hosts.allow ファイルで snmpd や rpcbind のアクセスの許可を設定してください。

本件に関する設定は、次のウェブサイトを参照してください。

Linux サービスセット : /etc/hosts.deny、/etc/hosts.allow を使ったアクセス制限(TCP wrappers)の方法を教えてください。【Linux サービスセットご契約のお客様限定】

<https://www.support.nec.co.jp/View.aspx?id=3150005102>

#### <過去事例>

/etc/hosts.deny に "ALL : ALL" が記述されており、/etc/hosts.allow に rpcbind が 127.0.0.1(localhost) を許可する記述がありませんでした。

#### <過去事例の対処>

/etc/hosts.allow に "rpcbind : 127.0.0.1" と記述し、rpcbind のローカルアクセスを許可します。

または、"ALL : 127.0.0.1" と記述し、すべてのローカルアクセスを許可します。

その後、ESMRestart コマンドで ESMPRO/ServerAgent を再起動します。

```
# /opt/nec/esmpro_sa/bin/ESMRestart
```

### SELinux機能の設定状況を確認してください

SELinux の設定は、以下のとおりです。



SELinux の設定を「無効(Disabled)」以外に設定されている場合は、SELinux のポリシー設定ファイルで適切なセキュリティコンテキストの設定をしてください。設定を行わないと、利用するソフトウェアでセキュリティ違反の警告またはエラーが発生し、正常に動作しない可能性があります。

「無効」以外を使用する場合は、SELinux のセキュリティコンテキストについて十分ご理解の上、設定を変更してください。

- 1) root ユーザーでログインします。
- 2) SELinux のカレント設定を確認します。
  - ・カレント設定が「無効」の場合は、次のように表示されます。

```
# getenforce
Disabled
```
  - ・カレント設定が「有効」の場合は、次のように表示されます。



```
# getenforce
Enforcing
# getenforce
Permissive
```

- ・カレント設定が「警告のみ」の場合は、次のように表示されます。

- 3) /etc/sysconfig/selinux をエディターで開き、以下の行を探します。

```
SELINUX=<カレント設定>
```

- 4) 上記の行を編集し、ファイルを保存します。

- ・「無効」にする場合、以下に変更します。  
SELINUX=disabled
- ・「有効」にする場合、以下に変更します。  
SELINUX=enforcing
- ・「警告のみ」にする場合、以下に変更します。  
SELINUX=permissive

- 5) 「有効」にした場合、以下のコマンドを実行し、snmpd\_t を permissive にします。

```
# semanage permissive -a snmpd_t
```



semanage コマンドが見つからない場合は、policycoreutils-python-utils パッケージをインストールしてください。



audit パッケージをインストールがインストールされている場合は、SELinux に拒否されるアクションを表示できます。

```
# ausearch -m AVC,USER_AVC,SELINUX_ERR,USER_SELINUX_ERR -ts today
```

setroubleshoot-server パッケージがインストールされている場合は、以下のコマンドを実行し、syslog から確認できます。

```
# grep "SELinux is preventing" /var/log/messages
```

- 6) システムを再起動します。

```
# reboot
```



SELinux が「有効」の場合、setroubleshoot プロセスにより、snmpd に関するログが syslog に記録されます。以下の対処を実施してください。

```
# ausearch -c 'snmpd' --raw | audit2allow -M my-snmpd
# semodule -X 300 -i my-snmpd.pp
```

ausearch コマンドが見つからない場合は、audit パッケージをインストールしてください。semodule コマンドが見つからない場合は、policycoreutils パッケージをインストールしてください。

## ESMPRO/ServerManagerからの設定に失敗(しきい値の設定に失敗しました)

snmpd.confの設定内容を確認してください

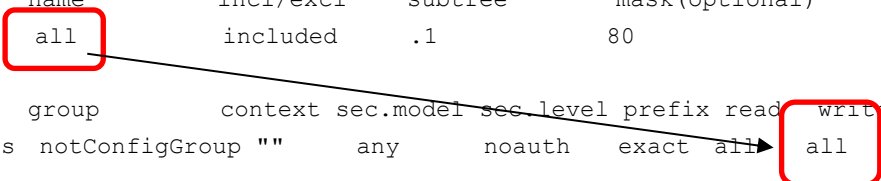
ESMPRO/ServerManager から設定するとき、SNMP の書き込み権限が必要です。snmpd.conf の定義に write

権限が付与されているか確認してください。

#### 記載例

```
#      name      incl/excl  subtree      mask(optional)
view  all        included    .1           80

#      group      context  sec.model  sec_level  prefix read  write  notif
access notConfigGroup ""      any       noauth    exact all  all  none
```



## ESMntserverのメッセージがsyslogへ記録され、OSの起動に時間が掛かる

下記メッセージが表示される原因として考えられるのは、rpcbind が起動されていない可能性や ESMPRO/ServerAgent が使用するポートが開放されていない可能性が考えられます。

```
###ERR### Please check /opt/nec/esmpro_sa/work/ESMntserver.ready or fopen is
failed(errno:2)
```

以下を確認してください。

- ・ rpcbind が起動していることを確認してください。
- ・ /etc/sysconfig/iptables の内容を確認してください。  
システム内のプログラム間通信で使用されるループバック・インタフェースへの通信を許可する設定があるか確認してください。ファイアウォールを利用していないときは問題ありません。  
例) `-A INPUT -i lo -j ACCEPT`
- ・ /etc/hosts.deny と /etc/hosts.allow の内容を確認してください。  
/etc/hosts.allow に対し、ループバックアドレスを許可する設定があるか確認してください。  
例) `ALL : 127.0.0.1`

## コントロールパネル(ESMagntconf, ESMamsadm)に関する質問

### コントロールパネルが起動できない

syslog に以下のメッセージが記録されている場合、rpcbind に対する 127.0.0.1(localhost)からの要求が拒否されています。コントロールパネルは rpcbind の機能を使用していますので、/etc/hosts.deny と /etc/hosts.allow の内容を見直してください。

```
rpcbind: connect from 127.0.0.1 to <アクション>: request from unauthorized host
<プロセス名>: ###ERR###RPC###: RPC: ポートマッパーの失敗です - RPC: 認証エラー
```

#### <過去事例>

/etc/hosts.deny に "ALL : ALL" が記述されており、/etc/hosts.allow に rpcbind が 127.0.0.1(localhost) を許可する記述がありませんでした。

#### <過去事例の対処>

/etc/hosts.allow に "rpcbind : 127.0.0.1" と記述し、rpcbind のローカルアクセスを許可します。または、"ALL : 127.0.0.1" と記述し、すべてのローカルアクセスを許可します。

その後、ESMRestart コマンドで ESMPRO/ServerAgent を再起動します。

```
# /opt/nec/esmpro_sa/bin/ESMRestart
```

### コントロールパネルが起動できない

コントロールパネルの起動には、root ユーザーで実行する必要があります。ログインしているユーザーの実行権限を確認してください。

```
例) [root@localhost bin]# コントロールパネルは起動できます。
[admin@localhost bin]$ コントロールパネルは起動できません。
```

## コントロールパネルが起動できない

ディストリビューションやバージョンにより、必須パッケージは異なります。ESMPRO/ServerAgent 必須パッケージを確認していただき、ESMPRO/ServerAgent が動作に必要なパッケージがインストールされているか確認してください。ESMPRO/ServerAgent 必須パッケージは ESMPRO/ServerAgent ドキュメントに公開しています。

### ■ESMPRO/ServerAgent ドキュメント

<https://www.support.nec.co.jp/View.aspx?id=3170102037>

必須パッケージ一覧 > ESMPRO/ServerAgent (Linux 版) 必須パッケージ一覧

※本製品は OpenIPMI を使用しておりませんので、OpenIPMI 関連パッケージのインストールは不要です。

## コントロールパネルで日本語の表示、および入力ができない

コントロールパネル(ESMagntconf, ESMamsadm)を日本語で表示させるためには、以下の手順を実行してください。

1. ネットワーク経由(ssh コマンド)で別の日本語端末からログインします。
2. root 権限がないときは、root ユーザーに昇格します。  
# su -
3. LANG 環境変数を確認します。  
# echo \$LANG
4. LANG 環境変数が日本語(ja\_JP.~)ではない場合は、一時的に日本語に変更します。  
# export LANG=ja\_JP.UTF-8 または ja\_JP.eucJP
5. コントロールパネルを起動します。  
# cd /opt/nec/esmpro\_sa/bin  
# ./ESMagntconf
6. 作業終了後に、手順 3.で確認した LANG 環境変数に変更します。

## コントロールパネルで日本語の入力に切り替えできない

ESMPRO/ServerAgent のコントロールパネルは、newt パッケージの機能を利用しています。newt パッケージのバージョンにより、切り替え方法が異なります。<Space>キーまたは<Ctrl>+<Space>キーを押して、入力の切り替えできるか確認してください。

## ESMPRO/ServerAgentのサービスに関する質問

### ESMPRO/ServerAgentのサービスの起動に失敗する

syslog に以下のメッセージが記録されている場合、rpcbind に対する 127.0.0.1 (localhost)からの要求が拒否されています。ESMPRO/ServerAgent のサービスは rpcbind の機能を使用していますので、/etc/hosts.deny と/etc/hosts.allow の内容を見直してください。

```
rpcbind: connect from 127.0.0.1 to <アクション>: request from unauthorized host
<プロセス名>: ###ERR###RPC###: RPC: ポートマッパーの失敗です - RPC: 認証エラー
```

#### <過去事例>

/etc/hosts.deny に"ALL : ALL"が記述されており、/etc/hosts.allow に rpcbind が 127.0.0.1(localhost)を許可する記述がありませんでした。

#### <過去事例の対処>

/etc/hosts.allow に"rpcbind : 127.0.0.1"と記述し、rpcbind のローカルアクセスを許可します。または、"ALL : 127.0.0.1"と記述し、すべてのローカルアクセスを許可します。

その後、ESMRestart コマンドで ESMPRO/ServerAgent を再起動します。

```
# /opt/nec/esmpro_sa/bin/ESMRestart
```

### ESMPRO/ServerAgentのサービスを一括で停止や起動させたい

root 権限のあるユーザーでログインし、ESMRestart コマンドを実行します。

#### 【停止させるとき】

引数に"stop"を指定して、ESMRestart コマンドを実行します。

```
# /opt/nec/esmpro_sa/bin/ESMRestart stop
```

#### 【起動させるとき】

引数に"start"を指定して、ESMRestart コマンドを実行します。

```
# /opt/nec/esmpro_sa/bin/ESMRestart start
```

#### 【再起動させるとき】

引数を指定せず、ESMRestart コマンドを実行します。

```
# /opt/nec/esmpro_sa/bin/ESMRestart
```

## ESMPRO/ServerAgentの機能や仕様に関する情報を教えてください

### ウィルスチェックの除外対象ファイルはありますか

ESMPRO/ServerAgent のバージョンは問わず、インストールディレクトリ(/opt/nec/esmpro\_sa)配下と Syslog 監視対象ファイルをスキャン対象外としてください。

インストールディレクトリ(/opt/nec/esmpro\_sa)配下：

過去のお問い合わせで、ウィルス対策ソフトのスキャンにより、ESMPRO/ServerAgent のファイルが圧縮ファイル爆弾(zip bomb)として検出された事例がありました。検出の原因は、インストールディレクトリ配下にあるファイルの解凍後のフォルダーやファイル数が多いためであり、問題ありません。

また、ウィルス対策ソフトでオンアクセススキャンを実施している場合、ファイルアクセスが遅くなり、データ取得に時間がかかり、サーバアクセス不能と検知される場合があります。

Syslog 監視対象ファイル：

ウィルス対策ソフトが利用している fsnotify\_mark プロセスのステータスが、D (割り込み不可能なスリープ状態)となる場合があります。

--ps -axlw 実行例-----

F	UID	PID	PPID	PRI	NI	VSZ	RSS	WCHAN	STAT	TTY	TIME	COMMAND
1	0	231	2	-	-	0	0	-	-	?	0:00	[fsnotify_mark]
1	0	-	-	20	0	-	-	synchr	D	-	0:00	-

この影響で、Syslog 監視対象ファイルにアクセスできなくなる事例がありました。

原因はカーネル側(fsnotify)にあり、3.10.0-327.29.1.el7 で修正されています。

### ESMPRO/ServerAgentがsyslogへ記録するロケールは変更できますか

ESMPRO/ServerAgent は、ロケールのデフォルト以外での動作をサポートしておりません。そのため、ロケールのデフォルト以外に変更する事もできません。ロケールのデフォルトは以下のとおりです。

UTF-8

### OSの時刻を変更(進める、または遅らせる)した場合、ESMPRO/ServerAgentに与える影響について教えてください

OSの時刻を変更(進める、または遅らせる)した場合でも、ESMPRO/ServerAgent は、特に影響はございません。

### ESMPRO/ServerAgentが使用するポート番号を教えてください

ESMPRO/ServerManager(以降、ESMPRO/SM と表記)から ESMPRO/ServerAgent(以降、ESMPRO/SA と表記)がインストールされた装置を監視するとき、以下のポートを利用しています。

お使いの環境でファイアウォールの設定をされるときは、これらへのアクセスを許可する設定にしてください。

表中「自動割当」のか所は、OS により使用可能なポートを一定の範囲内で割り振られます。そのため固定することはできません。ポートの範囲は以下のファイルを参照してください。

/proc/sys/net/ipv4/ip\_local\_port\_range

#### ■ESMPRO/SA ↔ ESMPRO/SM

機能	ESMPRO/SA	方向	ESMPRO/SM	備考
自動登録 サーバー監視(SNMP)	161/udp	← →	161/udp	Snmp
マネージャ通報(SNMP)	自動割当/udp	→	162/udp	
マネージャ通報 (TCP/IP in Band, TCP/IP Out-of-Band)	自動割当/tcp	→ ←	31134/tcp	

※方向が双方向のか所は、上段の矢印は通信を開始した方向を示し、下段は折り返しの通信を示します。

※SNMP 以外で使用するポート番号は、通報の設定画面より設定します。

※iptables または firewalld を使用したポートの開放例は以下のとおりです。

使用しないサービス(iptables または firewalld)は停止してください。

・iptables を利用したポートの開放例は以下のとおりです。

事前に iptables または iptables-services のインストールが必要です。

```
# iptables -I INPUT -p udp --dport 161 -s <ESMPRO/SM の IP アドレス> -j ACCEPT
# iptables -I OUTPUT -p udp --dport 161 -j ACCEPT
# iptables -I OUTPUT -p udp --dport 162 -j ACCEPT
# iptables -I OUTPUT -p tcp --dport 31134 -j ACCEPT
# service iptables save
```

・firewalld を使用したポートの開放例は以下のウェブサイトを参照して、使用するポートを解放してください。

Linux サービスセット : firewalld (ファイアウォール機能) の基本的な使用方法について教えてください。

<https://www.support.nec.co.jp/View.aspx?id=3150110809>

※TCP Wrappers を使ったアクセス制御をするときは以下のウェブサイトを参照して、使用するポートを解放してください。

Linux サービスセット : /etc/hosts.deny、/etc/hosts.allow を使ったアクセス制限(TCP wrappers)の方法を教えてください。

<https://www.support.nec.co.jp/View.aspx?id=3150005102>

ESMPRO/ServerAgent は以下の内部ポートを使用しています。

iptables を使ったパケットフィルタリング設定をするときは、これらへのアクセスを許可する設定にしてください。

#### ■ESMPRO/SA ↔ ESMPRO/SA

機能	ポート番号
rpcbind	111/tcp
	111/udp
ESMPRO/ServerAgent	自動割当/tcp

※iptables を利用したポートの開放例は以下のとおりです。

使用しない場合、サービス(iptables)は停止してください。

事前に iptables または iptables-services のインストールが必要です。

```
# iptables -A INPUT -i lo -j ACCEPT
# service iptables save
```

※TCP Wrappers を使ったアクセス制御をするときは以下のウェブサイトを参照して、使用するポートを解放してください。

Linux サービスセット : /etc/hosts.deny、/etc/hosts.allow を使ったアクセス制限(TCP wrappers)の方法を教えてください。

---

### ESMPRO/ServerAgentの監視機能を教えてください

ESMPRO/ServerAgent の監視機能は、ESMPRO/ServerAgent 監視項目一覧の機能概要を参照してください。  
ESMPRO/ServerAgent 監視項目一覧は ESMPRO/ServerAgent ドキュメントに公開しています。

■ESMPRO/ServerAgent ドキュメント

<https://www.support.nec.co.jp/View.aspx?id=3170102037>

機能一覧 > ESMPRO/ServerAgent (Linux 版) 機能一覧

---

### ESMPRO/ServerAgentのサービス(プロセス)の機能を教えてください

ESMPRO/ServerAgent のサービス(プロセス)の機能は、ESMPRO/ServerAgent プロセス情報資料のプロセスの機能概要を参照してください。

ESMPRO/ServerAgent プロセス情報資料は ESMPRO/ServerAgent ドキュメントに公開しています。

■ESMPRO/ServerAgent ドキュメント

<https://www.support.nec.co.jp/View.aspx?id=3170102037>

プロセス情報 > ESMPRO/ServerAgent (Linux 版) サービスプロセス

Esmpro-common パッケージに含まれるプロセスを確認してください。

---

### ESMPRO/ServerAgentが出力するログについて教えてください

ESMPRO/ServerAgent が出力するログは、ESMPRO/ServerAgent 内部ログ情報資料を参照してください。

ESMPRO/ServerAgent 内部ログ情報資料は ESMPRO/ServerAgent ドキュメントに公開しています。

■ESMPRO/ServerAgent ドキュメント

<https://www.support.nec.co.jp/View.aspx?id=3170102037>

内部ログ情報 > ESMPRO/ServerAgent (Linux 版) 内部ログ情報

プロセス情報の Esmpro-common パッケージに含まれるプロセスの内部ログ情報を確認してください。

---

### NICのLink Up/Downが通報されない

ESMPRO/ServerAgent のネットワーク(LAN)監視はトラフィックを監視しているため、NIC の Link Up/Down は検出できません。NIC の Link Up/Down 時に、システムから syslog(/var/log/messages)に記録されるメッセージがあるとき、Syslog イベントを追加することで通報できます。ただし、Link Down のときは、ネットワークが使用できない状態のため、通報されない可能性があります。

---

### MIB定義ファイルは、どこに格納されていますか？

ESMPRO/ServerAgent が拡張している ESMPRO MIB(1.3.6.1.4.1.119.2.2.4.4)の定義ファイルは、OS 種別 (Windows、Linux)を問わず本製品のインストール媒体に格納しております。

(CD) : win/SA46\_J/MIBS

---

### ESMPRO/ServerAgentの通報に関する情報を教えてください

---

#### ESMPRO/ServerAgentが通報するSNMPトラップ内容を教えてください

ESMPRO/ServerAgent が通報する SNMP トラップ内容は以下に公開しているアラート一覧を参照してください。

■ダウンロード - ESMPRO/ServerAgent for GuestOS、他社機版 ESMPRO/ServerAgent - ドキュメント

[https://jpn.nec.com/esmsm/download.html#sa\\_ver4\\_guest](https://jpn.nec.com/esmsm/download.html#sa_ver4_guest)

アラート一覧(Linux)

---

#### ESMPRO/ServerAgentが送信するSNMPトラップ内の文字コード

ESMPRO/ServerAgent が送信する SNMP トラップ内の日本語文字コードは、OS で使用している日本語文字コードに影響されず S-JIS に変換して送信しています。ESMPRO/ServerManager のアラートビューアは問題ありませんが、SNMP トラップを受信するソフトウェアの仕様によっては、S-JIS が表示できず文字化けす

る可能性があります。

### **ESMPRO/ServerManagerのアラートビューアで受信した通報が部分的に英語表記となる**

#### **ESMPRO/ServerAgentがsyslogに記録するメッセージが部分的に英語表記となる**

ESMPRO/ServerAgent のサービスは、各サービス起動時の LANG 環境変数の値を元に動作する言語(日本語と英語)を判断しております。OS の設定言語に関わらず、サービス起動時の LANG 環境変数は、英語環境(en\_US.UTF-8)となります。通報内容を日本語で通知させるには、ESMPRO/ServerAgent 日本語設定ツール(esmset.sh)を実行してください。ツールを実行すると、ESMPRO/ServerAgent のサービスのみ、LANG 環境変数を日本語環境(ja\_JP.UTF-8)で動作するように設定します。

ESMPRO/ServerAgent が送信する通報には、ESMPRO/ServerAgent 側から、すべてのメッセージを送信する Generic Trap と、ESMPRO/ServerAgent 側から、メッセージの作成に必要な情報のみを送信して、ESMPRO/ServerManager 側でメッセージを作成する predefine Trap があります。そのため、ESMPRO/ServerManager のアラートビューアで受信するメッセージは日本語で表記される情報があります。

### **ESMPRO/ServerManagerのアラートビューアで受信した通報が「不明なサーバ」またはトラップの送信元とは異なるサーバが表示される**

ESMPRO/ServerAgent は、以下の処理で取得した IP アドレスを SNMP Trap の AgentAddress フィールドに埋め込み送信します。

- 1)システムコールの gethostname()関数から、ホスト名を取得します。
- 2)システムコールの gethostbyname()関数から、1)で取得したホスト名を検索し、最初に一致するホスト名の IP アドレスを取得します。  
gethostbyname()関数の取得データは、/etc/hosts の定義と関連しています。  
もし/etc/hosts に1)で取得したホスト名が存在しない場合、または、取得した IP アドレスがローカルホスト(127.0.0.1)の場合は、UDP のソケット通信を利用して通信に使用する IP アドレスを取得し、TRAP 送信元の IP アドレスとして埋め込みます。

ESMPRO/ServerManager のアラートビューアは、AgentAddress フィールドに埋め込まれている IP アドレスを元に、登録されているサーバの情報(IP アドレス)を検索し、最初に合致するホスト名を表示します。そのため、検索に合致しない場合は「不明なサーバ」、別サーバの情報に合致した場合は別サーバのホスト名が表示されます。

上記 1)のホスト名が "server1" の場合に、/etc/hosts の内容によってどのような IP アドレスを取得し、トラップの送信元 IP アドレスとして埋め込むかの例を記載します。

(/etc/hosts の設定例 1) 通信に使用する IP アドレスを埋め込みます。

```
127.0.0.1 server1 localhost.localdomain localhost
10.1.2.1 server1
10.1.2.2 server2
```

(/etc/hosts の設定例 2) 10.1.2.1 となります。

```
10.1.2.1 server1
127.0.0.1 server1 localhost.localdomain localhost
10.1.2.2 server2
```

(/etc/hosts の設定例 3) 10.1.2.1 となります。

```
127.0.0.1 localhost.localdomain localhost
10.1.2.1 server1
10.1.2.2 server2
```



(/etc/hosts の設定例 4) 通信に使用する IP アドレスを埋め込みます。

```
127.0.0.1 localhost.localdomain localhost
10.1.2.2 server2
```

## ESMPRO/ServerAgentがsyslogに記録するメッセージを教えてください

ESMPRO/ServerAgentがsyslogに記録するメッセージはESMPRO/ServerAgent アラート一覧の通報メッセージを参照してください。

<例>

```
Sep 13 07:46:26 test-host ESMamvmain: SRC: ESMCpuPerf, ID:C0000064, MSG:CPU Total
の負荷が異常に高くなっています。
```

上記メッセージとアラート一覧の対応としては、以下のとおりです。

SRC: ESMCpuPerf	= アラート一覧の通報ソース名
ID: C0000064	= アラート一覧の通報 ID
MSG: CPU Total の負荷	= アラート一覧の通報メッセージ

が....

ESMPRO/ServerAgent アラート一覧はESMPRO/ServerAgent ドキュメントに公開しています。

■ダウンロード - ESMPRO/ServerAgent for GuestOS、他社機版 ESMPRO/ServerAgent - ドキュメント

[https://jpn.nec.com/esmsm/download.html#sa\\_ver4\\_guest](https://jpn.nec.com/esmsm/download.html#sa_ver4_guest)

アラート一覧(Linux)

## ESMPRO/ServerAgentがsyslogに記録するメッセージのファシリティとプライオリティを教えてください

ESMPRO/ServerAgentがsyslogに記録するメッセージのファシリティとプライオリティは以下のとおりです。

情報	ファシリティ	: user	プライオリティ	: info
警告	ファシリティ	: user	プライオリティ	: warning
異常	ファシリティ	: user	プライオリティ	: err

## 任意のメールアドレスへの通知やパトロールランプを鳴動させる方法を教えてください

任意のメールアドレスへの通知やパトロールランプを鳴動させる方法はありません。

ESMPRO/ServerManager(Windows)をインストールしている管理PC(Windows)にWebSAM AlertManagerを導入することにより、運用環境に合わせた通報手段を提供しています。

【WebSAM AlertManager - 特長・機能の抜粋】

- ・システム管理者がどこからでも障害状況の確認ができる mail 通報
- ・サーバーの異常をサーバーのオペレーターに通知するポップアップ通報
- ・サーバーの異常情報をリモートプリンターにも印刷可能なプリンター書き出し
- ・サーバーの異常を検出した場合に、業務アプリケーションと連携して障害回避、障害復旧処理をする事を可能とするアプリケーションの実行
- ・サーバーの異常を検出した場合に、パトロールランプを鳴動させるパトロールランプ通報
- ・サーバーの異常情報履歴をファイル保存するファイル出力

■WebSAM AlertManager - 特長・機能

<https://jpn.nec.com/websam/alertmanager/kinou.html>

## ESMPRO/ServerAgentがサポートしているsnmpバージョンを教えてください

ESMPRO/ServerAgentがサポートしているsnmpバージョンは、SNMPv1のみです。snmpd.confの設定では、以下の波線が該当します。SNMPv2やSNMPv3をサポートする予定はありません。

【snmpd.confの抜粋】

```
#      groupName      securityModel securityName
group  notConfigGroup.v1.....notConfigUser
```



## 設定を変更したときに再設定する必要がある項目を教えてください

---

### root権限のあるユーザーのパスワードを変更されるとき

---

- ・ ESMPRO/ServerAgent 側の設定を変更する項目  
設定を変更する項目はありません。
- ・ ESMPRO/ServerManager 側の設定を変更する項目  
設定を変更する項目はありません。

---

### ESMPRO/ServerAgentマシン側のIPアドレスを変更されるとき

---

- ・ ESMPRO/ServerAgent 側の設定を変更する項目  
設定を変更する項目はありません。
- ・ ESMPRO/ServerManager 側の設定を変更する項目  
ESMPRO/ServerManager に登録されている ESMPRO/ServerAgent アイコンの IP アドレスを変更してください。

---

### ESMPRO/ServerAgentマシン側のホスト名を変更されるとき

---

- ・ ESMPRO/ServerAgent 側の設定を変更する項目  
設定を変更する項目はありません。
- ・ ESMPRO/ServerManager 側の設定を変更する項目  
ESMPRO/ServerManager に登録されている ESMPRO/ServerAgent アイコンのホスト名を変更してください。統計情報自動収集を設定しているときは、ホスト名を変更すると、それまでの収集データを参照することができなくなります。  
そのときは、  
¥Program Files¥ESMPRO¥NVWORK¥esmpro 配下にある  
元のホスト名.dat  
元のホスト名.bak  
というファイルのファイル名を、変更後のホスト名に合わせて変更してください。

---

### ESMPRO/ServerManagerマシン側のユーザーのパスワードを変更されるとき

---

- ・ ESMPRO/ServerAgent 側の設定を変更する項目  
マネージャ通報(TCP\_IP Out-of-Band)を使用している環境で、「リモートアクセスサービスのエントリ選択」の宛先設定に使用している ESMPRO/ServerManager 側のユーザ名およびパスワードが変更になった場合は、3 章の以下を参照して、設定を変更してください。  
3.1.2 通報手段がマネージャ通報(TCP\_IP Out-of-Band)の宛先設定

---

### ESMPRO/ServerManagerマシン側のIPアドレスを変更されるとき

---

- ・ ESMPRO/ServerAgent 側の設定を変更する項目  
マネージャ通報(SNMP/TCP\_IP)に ESMPRO/ServerManager マシンの IP アドレスを指定しているときは、3 章の以下を参照して、コントロールパネル(ESMamsadm)から通報先の設定を変更してください。  
2.1.1. マネージャ通報(SNMP)の基本設定  
3.1.1. 通報手段がマネージャ通報(TCP\_IP In-Band)の宛先設定  
3.1.2. 通報手段がマネージャ通報(TCP\_IP Out-of-Band)の宛先設定  
また、snmpd に対して IP アドレスによるアクセスを制限しているときは、設定を変更してください。  
/etc/snmp/snmpd.conf  
/etc/hosts.allow  
/etc/hosts.deny
- ・ ESMPRO/ServerManager 側の設定を変更する項目  
ESMPRO/ServerManager のサービスを再起動してください。手順については、ESMPRO/ServerManager

インストールガイドの4章(3. サービス一覧)に記載の「サービス開始/停止順序」を参照してください。

サービスの再起動の代わりに ESMPRO/ServerManager がインストールされている装置を再起動していただくことで対応可能です。

---

### ESMPRO/ServerManagerマシン側のホスト名を変更されるとき

- ・ ESMPRO/ServerAgent 側の設定を変更する項目

マネージャ通報(TCP\_IP)に ESMPRO/ServerManager マシンのホスト名を指定しているときは、3章の以下を参照して、コントロールパネル(ESMamsadm)から通報先の設定を変更してください。

3.1.1. 通報手段がマネージャ通報(TCP\_IP In-Band)の宛先設定

3.1.2. 通報手段がマネージャ通報(TCP\_IP Out-of-Band)の宛先設定

また、snmpd に対してホスト名によるアクセスを制限しているときは、設定を変更してください。

/etc/snmp/snmpd.conf

/etc/hosts.allow

/etc/hosts.deny

- ・ ESMPRO/ServerManager 側の設定を変更する項目

<ESMPRO/ServerManager インストールフォルダー>

¥ESMWEB¥wbserver¥webapps¥esmpro¥WEB-INF¥service¥options.txt 中の "SM\_NAME=xxxx" と記載されている行を削除してください。

その後、以下の手順で ESMPRO/ServerManager のサービスを再起動してください。

サービスの再起動後、管理対象サーバーの接続チェックを実行してください。

サービスの再起動の代わりに ESMPRO/ServerManager がインストールされている装置を再起動していただくことで対応可能です。

ESMPRO/ServerManager に付属の以下のマニュアルを参照して、必ずここに記載どおりの順序でサービス一式の停止・開始をお願いいたします。

- ・ ESMPRO/ServerManager インストールガイド (Windows 編)

→4章 付録

→3. サービス一覧

→● サービス開始/停止順序

---

### ドメインを変更されるとき

- ・ ESMPRO/ServerAgent 側の設定を変更する項目

設定を変更する項目はありません。

- ・ ESMPRO/ServerManager 側の設定を変更する項目

ESMPRO ユーザーグループをグローバルグループとして登録しているときは、ドメインを変更することで ESMPRO ユーザーグループ へアクセスできない状態になると、ESMPRO/ServerManager が正常に動作しなくなりますので、ご注意ください。

---

### MACアドレスを変更されるとき(ネットワークボードの交換など)

- ・ ESMPRO/ServerAgent 側の設定を変更する項目

設定を変更する項目はありません。

- ・ ESMPRO/ServerManager 側の設定を変更する項目

ESMPRO/ServerManager の Remote Wake Up 機能をご利用になられているとき、ツリービュー上の対象サーバーのアイコンのプロパティ画面を開いて、[機能]タブの「RWU 機能 MAC アドレス」に新しい MAC アドレスを設定してください。

---

### SNMPのコミュニティ名を変更されるとき

- ・ ESMPRO/ServerAgent 側の設定を変更する手順

1) SNMP 設定ファイル(snmpd.conf)を編集して、コミュニティ名を変更する。

2) コントロールパネル(ESMagntconf)の「全般プロパティ」の「SNMP Community」にて、コミュニテ

- イー名を変更する。
- 3) snmpd サービスと ESMPRO/ServerAgent または OS を再起動する。
- ・ ESMPRO/ServerManager 側の設定を変更する手順
  - 1) 管理対象サーバーの SNMP コミュニティー名に関する登録情報を変更する。
  - 2) 管理対象サーバーの [接続設定]-[編集]にて、SNMP コミュニティー名(取得用)と SNMP コミュニティー名(設定用)を変更する。

## 障害情報採取ツール(collectsa.sh) に関する質問

---

### ESMPRO/ServerAgentの動作に問題が発生した場合

---

ESMPRO/ServerAgent の動作に問題が発生した場合は、障害情報採取ツール(collectsa.sh)で情報を採取の上、NEC カスタマーサポートセンター経由でお問い合わせください。

- ・ 障害情報採取ツールの使用手順
  - 5) root ユーザーでログインします。
  - 6) 任意のディレクトリに移動します。
  - 7) 障害情報採取ツールを実行します。

```
# /opt/nec/esmpro_sa/tools/collectsa.sh
```

カレントディレクトリに collectsa.tgz が作成されます。
  - 8) NEC カスタマーサポートセンター経由でお問い合わせください。  
NEC カスタマーサポートセンターの案内にしたがって、collectsa.tgz の提供をお願いします。

---

### 障害情報採取ツール(collectsa.sh)の動作に問題が発生した場合

---

障害情報採取ツール(collectsa.sh)が正しく動作しない(終了しない等)場合は、採取済みの情報を採取の上、NEC カスタマーサポートセンター経由でお問い合わせください。

- 4) 障害情報採取ツールを終了させます。
  - 1-1) 障害情報採取ツールを実行しているターミナルで、<Ctrl>+<C>キーを押します。
  - 1-2) 障害情報採取ツールが終了したことを確認します。

```
# ps aux | grep collectsa.sh |grep -v grep
```

たとえば下記のように表示された場合、collectsa.sh はバックグラウンドで実行されています。

```
#root 11313 0.0 0.4 4196 1124 pts/0 T 14:46 0:00 /bin/bash ./collectsa.sh
```
  - 1-3) バックグラウンドで実行されていた場合は、プロセスを終了させます。

```
# kill -9 {pid}
```

(例) # kill -9 11313
- 5) カレントディレクトリに作成された collectsa ディレクトリを tgz 形式で圧縮します。

```
# tar czvf collect_dir.tgz collectsa/
```
- 6) NEC カスタマーサポートセンター経由でお問い合わせください。  
NEC カスタマーサポートセンターの案内にしたがって、collect\_dir.tgz の提供をお願いします。

ESMPRO/ServerAgent for GuestOS Ver.1.5  
他社機版 ESMPRO/ServerAgent Ver.1.5  
ユーザーズガイド(Linux 編)

日 本 電 気 株 式 会 社  
東京都港区芝五丁目 7 番 1 号  
TEL (03) 3454-1111 (大代表)