BOM Linux オプション Ver.7.0
ユーザーズ マニュアル

2021 年 4 月 1 日

免責事項

本書に記載された情報は、予告無しに変更される場合があります。セイ・テクノロジーズ株式会社は、本書に関していかなる種類の保証（商用性および特定の目的への適合性の黙示の保証を含みますが、これに限定されません）もいたしません。

セイ・テクノロジーズ株式会社は、本書に含まれた誤謬に関しての責任や、本書の提供、履行および使用に関して偶発的または間接的に起こる損害に対して、責任を負わないものとします。

著作権

■ 目次

本ユーザーズマニュアルについて

製品表記

本ユーザーズマニュアルでは、以下の製品について略称を使用しております。

正式名称	本マニュアルでの呼称（略称）
BOM Linux オプション Ver.7.0 SR4	Linux オプション
BOM for Windows Ver.7.0 SR4	BOM 7.0
Amazon Web Services	AWS
Amazon Simple Storage Service	Amazon S3

使用方法

本ユーザーズマニュアルには、Linux オプションを使用する際に必要となる詳細な情報と手順が記載されています。

本ユーザーズマニュアルを使用するには Linux 及び、Microsoft Windows オペレーティングシステムについての実際的な知識と、BOM 7.0 の基本的な知識が必要です。

表記規則

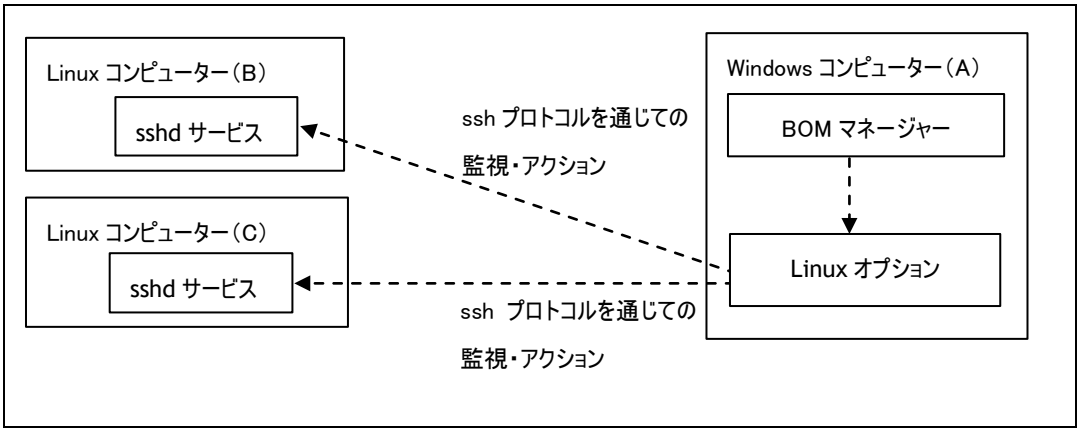
本ユーザーズマニュアルでは、以下の表記規則を使用しています。

表記	**説明**
‘参照先’	シングルクォート内（‘と’）は本マニュアル内、あるいは別のマニュアルの参照を示します
[ボタン]	角括弧内（[と]）はボタン名を示します
<キー>	山括弧（不等号記号）内（<と>）はキーボード入力を示します

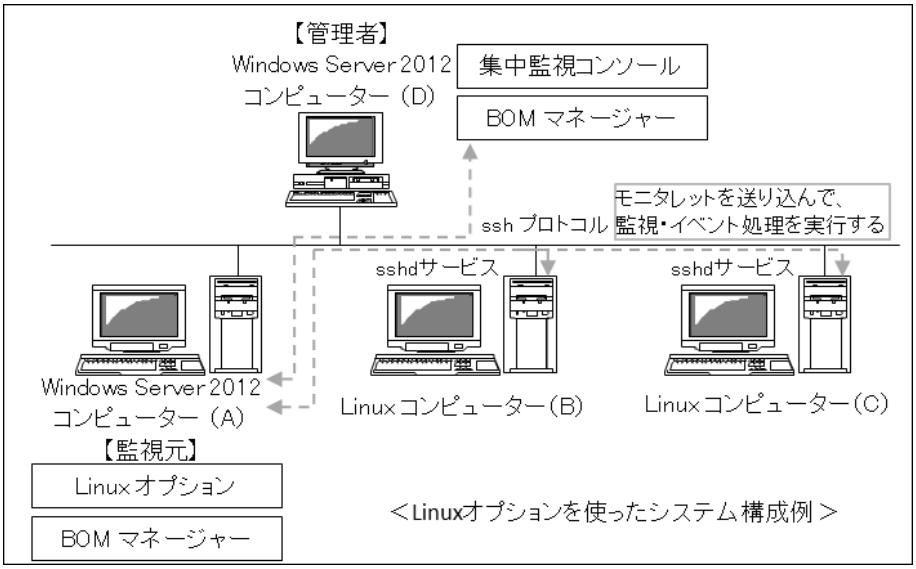
第1章 システム構成

Linux オプションは、BOM 7.0 が導入済みの Windows コンピューターから Linux コンピューターを監視するためのオプション製品です。

- Linux オプションは、BOM 7.0 を導入したコンピューターにインストールして使用します。
- Windows コンピューター上から、Linux コンピューターの監視設定及び Linux コンピューター上でのアクションを設定できます。
- Windows コンピューター上で、監視結果の表示やステータス表示、ログ表示などを行うことができます。



Linux オプションは、SSH（Secure Shell Protocol）を使用して、リモートの Windows コンピューター（A）から Linux コンピューター（B）、（C）の各種リソースの監視、Linux 上でのアクションを実行します。監視対象の Linux コンピューターには、各ディストリビューションに標準で付属する SSH サーバー（OpenSSH）のインストールその他の簡単な設定が必要になりますが、Linux 上に BOM の監視サービスをインストールする必要はありません。 Linux オプションを追加購入することで 1 台の Windows コンピューターから複数の Linux コンピューターを監視することが可能になります。



※ 「モニタレット」（monitorlet）とは

“Linux サーバー上で実行可能なスクリプトまたはプログラム”です。Linux サーバー上で実行されると監視を行い、その結果値が監視元 Windows コンピューターに戻されます。

第2章 インストール

2.1 動作環境

A. 監視対象コンピューター（Linux）の動作環境

Linux オプションは、以下のバージョンの Linux ディストリビューションの動作環境に対応しています。

Linux ディストリビューション	バージョン
Red Hat Enterprise Linux ※1	6.0 以降（ 32bit / 64bit ）
	7.1 以降（ 64bit ）
	8.0 以降（ 64bit ）

※1 Red Hat Enterprise Linux 7.0 はサポート対象外です

B. 監視対象コンピューター（Linux）の設定要件

- OpenSSH Ver2.3.0 以上（最新のバージョンを推奨）
- Perl Ver5.8.0 以上がインストールされていること
- IPv6 環境下では perl-Socket6 パッケージがインストールされていること
- bash が使用できること
- perl-Net-Ping モジュールがインストールされていること
- perl-Encode-Locale モジュールがインストールされていること

BOM Report オプション Ver.7.0 を使用して、Linux を対象としたハードウェア情報のレポートを出力する場合、以下の要件を満たす必要があります。

- Red Hat Enterprise Linux 6.x:
  「haldaemon」を起動する、もしくは「lshw」および「perl-JSON」のパッケージを導入すること。
- Red Hat Enterprise Linux 7.x:
  「OpenLMI」、もしくは「lshw」および「perl-JSON」のパッケージを導入すること。
- Red Hat Enterprise Linux 8.x:
  「lshw」および「perl-JSON」のパッケージを導入すること。

C. 監視元コンピューター（BOM）の動作環境

Linux オプションを導入する監視元コンピューターは、Windows Server ベースのコンピューターで動作いたします。
監視元コンピューターについては、‘BOM for Windows Ver.7.0 インストールマニュアル’の‘1 .2 BOM のシステム要件’をご確認ください。

※ SSH サーバーは、SSH プロトコル Ver2 方式でアクセス可能で、パスワード認証方式または公開鍵認証方式が許可されていなくてはなりません。またチャレンジレスポンス認証が無効化されている必要があります

※ 1 台の Windows コンピューターで正常に監視可能な Linux コンピューターの台数は、Windows コンピューター、Linux コンピューター双方のハードウエアスペック、通常の運用における負荷状況、ネットワークの状況、監視設定の数、設定の内容などにより異なります

※ Windows クライアント OS 上では動作いたしません

※ 公開鍵認証方式では PuTTY 形式（.ppk）かつ RSA（SSH-2）または DSA の鍵ファイルのみ使用できます。
また、鍵のパスフレーズには改行コードおよび、UTF-16 の文字を使用できません。

※ 公開鍵認証方式を使用する場合、監視対象の Linux コンピューターに接続する監視元となる Windows コンピューターには、BOM for Windows Ver.7.0 SR1 以降が導入されている必要があります

Linux オプションは BOM 7.0 が既にインストールされており、正常に動作していることを稼動前提としています。BOM がインストールされていない場合は、まず BOM 7.0 のインストールおよび正常動作の確認後、このマニュアルに従って Linux オプションをインストールして下さい。

◆ BOM Linux オプションを導入・運用するエンジニアは、BOM 7.0 、使用している Windows オペレーティングシステム、ネットワーク環境および監視対象 Linux ディストリビューションについての充分な知識と情報を持っている必要があります。

2.2 事前の準備

2.2.1 監視対象 Linux コンピューター

Linux オプションの監視対象となる Linux コンピューターにはあらかじめいくつかの設定が必要です。
以下はディストリビューションごとに共通する内容ですが、詳細は各ディストリビューションのマニュアルを参照してください。

監視対象 Linux コンピューターにインストールされている必要のあるソフトウェア

OpenSSH（Ver.2.3.0 以上） ※ OpenSSH はセキュリティ上、最新のバージョンを導入することを推奨します
Perl（v5.8.0 以上）

上記がインストールされているかどうかの確認手順は以下の通り（Red Hat の例）です。

1. Linux コンピューターに root でログインします。
2. OpenSSH のサービスがインストールされているかを確認する場合、「/usr/sbin/ntsysv」または、
   「/sbin/chkconfig --list」コマンド等を使用し[sshd]が一覧に表示されるかどうかで確認できます。
   Red hat Enterprise Linux 7.1 以降の環境では、「yum list installed | grep ssh」コマンド等を使用し確認できます。
3. Perl がインストールされているかを確認するには、「perl −v」コマンドを実行します。Perl が正常に動作している環境でこのコマンド実行すると、動作している Perl のバージョンが表示されます。

※ 上記のパッケージがインストールされていない場合、各ディストリビューションのマニュアル等を参照してインストールしてください

2.2.2 監視・アクション用 Linux ログインユーザーアカウントの権限

SSH プロトコルを使って監視用 Windows コンピューターから監視対象 Linux コンピューターにログインするためのユーザーアカウントを、監視対象 Linux コンピューターに登録しておく必要があります。(root でログインの上、useradd 等使用)。監視項目またはイベント処理アクションの種類によって、Linux ログインユーザーアカウントには以下の権限が必要です。

※ Linux オプションでパスワード認証を使用する場合、Linux ログインユーザーアカウントには必ずパスワードを設定してください。(passwd コマンド等使用)

監視の種類	監視に必要な権限
Linux ディスク容量監視	アカウントによる制限なし ※1
Linux ディレクトリ・ファイル監視	監視ディレクトリ以下の全ディレクトリの参照権限 ※2
Linux サービスポート監視	アカウントによる制限なし ※3
Linux プロセッサ監視	アカウントによる制限なし ※1
Linux メモリ監視	アカウントによる制限なし ※1
Linux ディスクアクセス監視	アカウントによる制限なし ※1
Linux ネットワーク インターフェイス監視	アカウントによる制限なし ※1
Linux プロセス監視	アカウントによる制限なし ※1
Linux プロセス数監視	アカウントによる制限なし ※1
Linux テキストログ監視	監視するテキストファイルの read 権限
Linux スクリプト監視	スクリプトの処理内容に依存

イベント処理の種類	イベント処理に必要な権限
Linux SYSLOG 書き込み	アカウントによる制限なし ※4
Linux プロセスコントロール	root であること
Linux シャットダウン	root であること
Linux スクリプト実行	スクリプトの処理内容に依存

※ 1 /proc ファイルシステムが存在し、参照できることが前提です

※ 2 一部のディレクトリしか権限がない場合、権限のない部分の値は取得できません

※ 3 ポートに対するアクセス制限がされていないこと、UDP の場合は「root」であることが前提です

※ 4 logger コマンドによる書き込みが可能なことが前提です

2.2.3 監視対象 Linux コンピューターのシェル環境

監視・イベント処理アクション用 Linux ログインユーザーアカウントのシェル環境は、下記表を参照し異なる場合には変更してください。

シェル（$SHELL）:	/bin/bash
プロンプト（$PS1）:	[root@hostname root]# または [username@hostname username]$
ヒアプロンプト（$PS2）:	>

※　プロンプトの後には 1 半角スペースが必ず必要です

2.2.4 SSH サーバーの設定（Linux）

SSH サーバーは sshd というサービスで実装されています。監視対象 Linux コンピューターを、SSH で接続可能なサーバーとして使用するためには、sshd の設定を行う必要があります。sshd の設定ファイルは、通常、/etc/ssh/sshd_config という名前でインストールされています。

root でログインし、/etc/ssh/sshd_config ファイルの設定を確認してください。設定ファイルは、デフォルトのものを使用することを推奨します。（記、デフォルトの値はディストリビューションやインストール時の設定によって違う場合があります）。

	デフォルト	・Linux オプションを使用する場合の要件
Port	22	SSH のポート番号を指定 変更可能
Protocol	2,1	SSH のプロトコルバージョン 必ず“2”が含まれるようにしてください
PermitRootLogin	yes	root ログインの許容 監視・イベント処理用アカウントに root を使用する場合は必ず“yes”にして下さい
PubkeyAuthentication	yes でコメントアウト	公開鍵認証の設定 公開鍵認証を使用する場合は必ず行頭の“#”を削除して“yes”（使用する）にしてください。
AuthorizedKeysFile	.ssh/authorized_keys	公開鍵認証に使用する公開鍵ファイルの保存場所とファイル名の設定
PasswordAuthentication	yes	パスワード認証の設定 必ず yes にしてください
PermitEmptyPasswords	no	パスワードがない場合のログイン許容の可否 必ず“no”にしてください
ChallengeResponseAuthentication	no	チャレンジレスポンス認証の設定 必ず“no”にしてください

また、/etc/hosts.allow、/etc/hosts.deny で監視元 Windows コンピューターから sshd へのアクセスが許可されていることを確認して下さい。

▼ sshd サービスの制御（6 系）

```
#   /sbin/service sshd start（Enter）
#   /sbin/service sshd stop（Enter）
```

・・・・・・・・・ sshd サービスの開始
・・・・・・・・・ sshd サービスの停止

▼ sshd が自動起動するか確認（6 系）

```
#   /sbin/chkconfig --list sshd   （Enter）
sshd              0:オフ    1:オフ    2:オン    3:オン    4:オン    5:オン    6:オフ
#
```

・・・・・・・・・ この場合、2,3,4,5 のランレベルで自動起動するように設定されている

▼ sshd サービスの制御（7 系）

```
#   systemctl start sshd.service（Enter）
#   systemctl stop sshd.service（Enter）
```

・・・・・・・・・ sshd サービスの開始
・・・・・・・・・ sshd サービスの停止

▼ sshd が自動起動するか確認（7 系）

```
# systemctl is-enabled sshd（Enter）
```

・・・・・・・・・ sshd サービスの自動起動確認

コマンド結果が enabled と表示されていれば自動起動設定になっています。

2 .2 .5 公開鍵認証を使用する際の Linux コンピューターの準備

- “sshd_config”の“PubkeyAuthentication”での設定で、公開鍵認証が許可されている必要があります。
- “sshd_config”の“AuthorizedKeysFile”で指定した場所に、指定したファイル名で公開鍵（監視元の Windows コンピューターに保存された秘密鍵に対応したもの）が保存されている必要があります。

2 .2 .6 監視用 Windows コンピューター

- Linux オプションが未インストールのコンピューターでは、‘2 .3 インストール手順’に従って Linux オプションをインストールします。
- ローカルコンピューターの管理者権限をもつユーザーでコンピューターにログインしてください。
- ローカルコンピューターで起動しているすべての BOM のコンソールプログラムを閉じてください。
- 鍵認証を使用する場合は、SSH 接続に使用する秘密鍵ファイル（PuTTY 形式かつ、RSA（SSH-2）または DSA のもの）が Windows コンピューター上に保存されている必要があります。
  OpenSSH 形式や Amazon EC2 のプライベートキー形式（.pem）の秘密鍵ファイルを PuTTY 形式に変換する場合は、‘第 5 章 BOM 7.0 PuTTYgen について’を参照してください。
  ※ 鍵のパスフレーズには改行コードおよび、UTF-16 の文字を使用できません。

2.3 インストール手順

監視元コンピューターに、BOM 7.0 と Linux オプションをインストールする手順を以下でご案内します。

BOM 7.0 、Linux オプション、および関連ソフトウェアのインストールについて、以下の手順に沿って作業してください。

なお、インストール作業は管理者権限が必要となりますので、管理者権限を持つアカウントにてログオンの上、作業を行ってください。

※ 以降の手順は必要な作業項目の概要のみを抽出した概略手順となります。

BOM 7.0 の詳細な導入手順については、'BOM for Windows Ver.7.0 インストール マニュアル' をご参照ください。

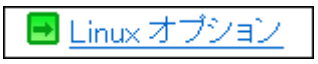
2.3.1 Linux オプションのインストール

Linux を監視するため、Linux オプションのインストールは、以下の手順にて実施します。

A. Linux オプションの新規インストール

BOM 7.0 のコンポーネントを一切入れていないコンピューターに Linux オプションをインストールする手順の概要を示します。

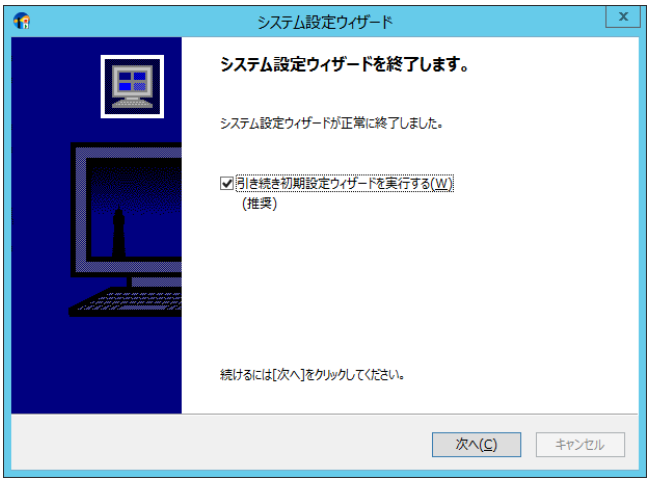
1. BOM 7.0 の媒体をコンピューターに挿入し、インストールランチャーを起動します。
2. メニューから"Linux オプション"をクリックし、セットアップウィザードを起動します。



3. "セットアップタイプ"画面まで進め、"標準"または"カスタム"を選択して[次へ]ボタンをクリックします。
"カスタム"を選択した場合は、"監視サービス"ツリー以下の"Linux オプション"がインストール対象となっている(ハードディスクアイコンになっている)ことを確認し、必要に応じて他の機能の追加やインストール先の変更をおこなって、[次へ]ボタンをクリックします。
4. 以降はセットアップウィザードに従い、Linux オプションのセットアップを完了させます。
その際、"続けてシステム設定ウィザードを起動する"チェックボックスにはチェックを入れて、[完了]ボタンをクリックします。

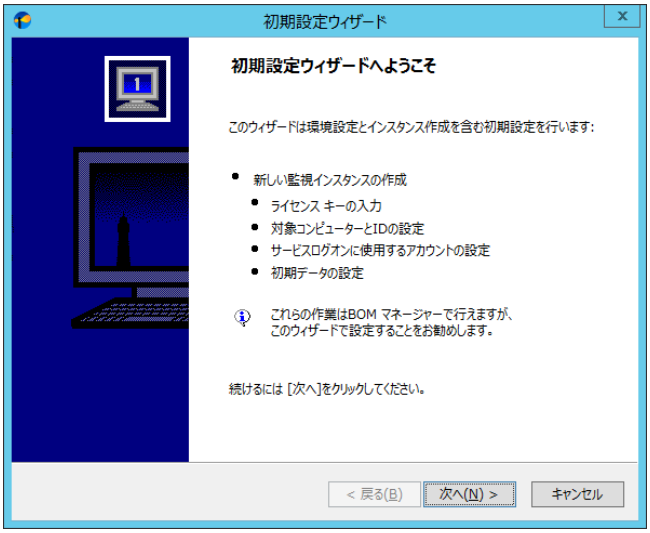
5. 続くシステム設定ウィザードも、ウィザードに従い設定を完了させます。

   その際、“引き続き初期設定ウィザードを実行する”チェックボックスはチェックを入れておきます。

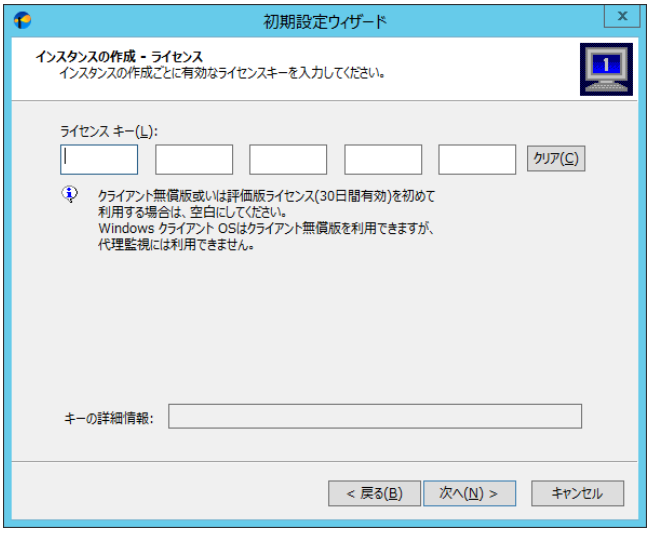


6. 初期設定ウィザードが起動します。

   [次へ]ボタンをクリックし、“ライセンス”画面を表示します。

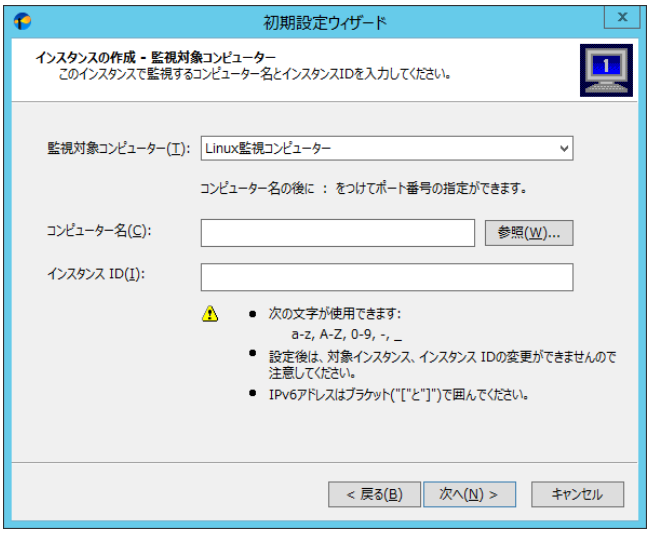


7. Linux オプションのライセンスキーを入力し、[次へ]ボタンをクリックします。



8. “コンピューター名”欄に Linux のコンピューター名または IP アドレスを入力します。

“インスタンス ID”欄に Linux が識別可能な名称を設定します。

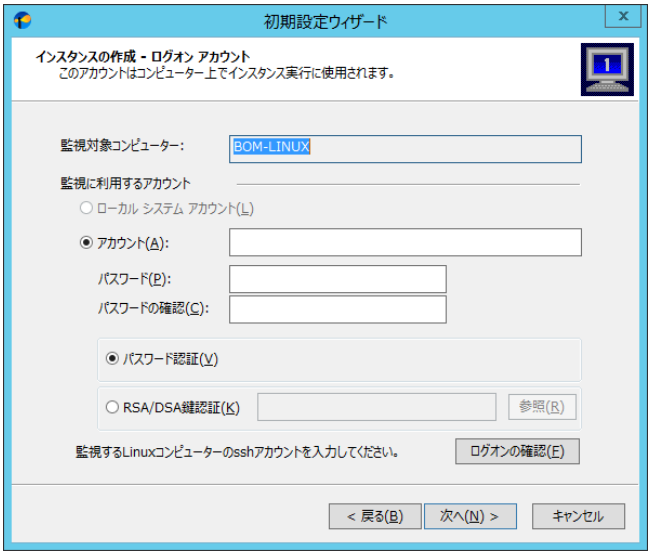


※　ホスト名は名前解決可能環境でのみ指定できます

※　SSH のポート番号はデフォルトで 22 番が設定されます

デフォルト値でない場合にはコンピューター名の後に半角英字の「:」(コロン)を入力しポート番号を半角数字で入力します

9. Linux に接続するためのアカウントの設定を行います。



● パスワード認証を使用する場合

“パスワード認証”にチェックを入れ、以下の情報を入力します。

“アカウント” … ssh ログインユーザー名を入力します。

“パスワード”、“パスワードの確認” … 指定したアカウントに対するパスワードを入力します。(必須入力)

● 鍵認証を使用する場合

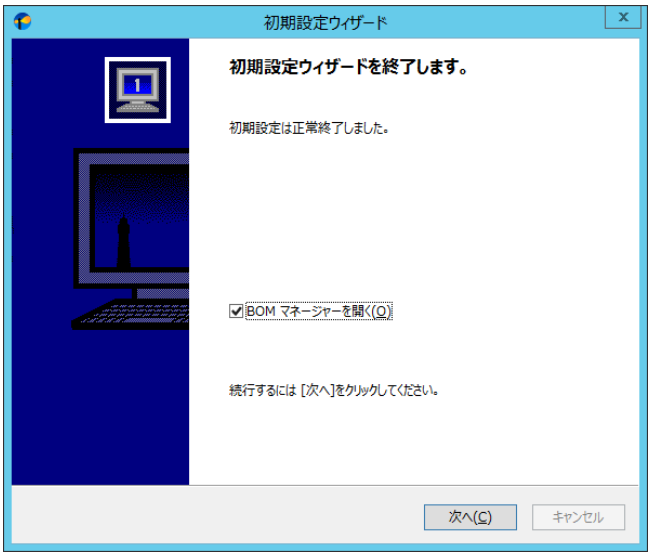
“RSA/DSA 鍵認証”にチェックを入れ、以下の情報を入力します。

“RSA/DSA 鍵認証” … 使用する秘密鍵ファイルを指定します。

“アカウント” … ssh ログインユーザー名を入力します。

“パスワード”、“パスワードの確認” … 鍵に対するパスフレーズを入力します。(省略可)

10. [ログオンの確認]ボタンをクリックし、Linux に接続可能なことを確認した後に[次へ]ボタンをクリックします。
11. 初期設定ウィザードに従い、Linux オプションのインストールを完了させます。

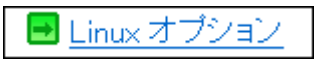


B. Linux オプションの追加インストール

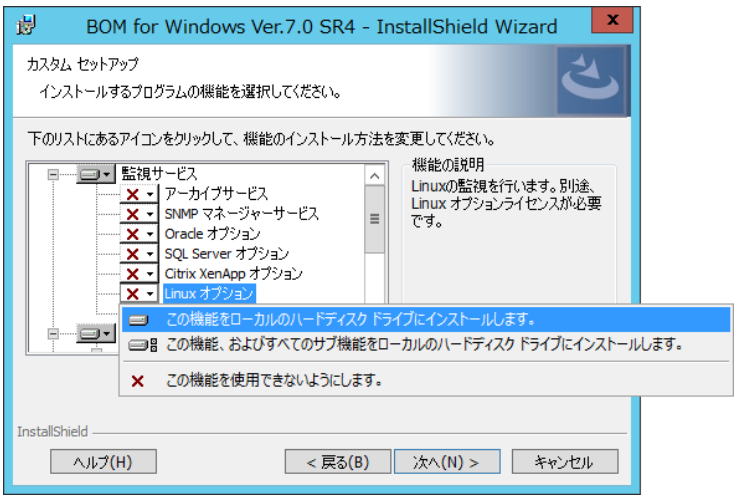
監視元コンピューターに“BOM 7.0 監視サービス”などの Linux オプション以外の BOM 7.0 コンポーネントを既に入れている場合、追加インストール方式にて Linux オプションを導入します。

以下に Linux オプションの追加インストール手順の概要を示します。

1. BOM 7.0 の媒体をコンピューターに挿入し、インストールランチャーを起動します。
2. メニューから“Linux オプション”をクリックし、セットアップウィザードを起動します。



3. “プログラムの保守”画面まで進め、“変更”ラジオボタンが有効になっていることを確認して[次へ]ボタンをクリックします。
4. “カスタムセットアップ”画面で“Linux オプション”のアイコンをクリックし、“この機能をローカルのハードディスク ドライブにインストールします。”を選択して、[次へ]ボタンをクリックします。



5. 以降はセットアップウィザードに従い、“Linux オプション”のセットアップを完了させます。

C. Linux 用監視インスタンスの追加作成

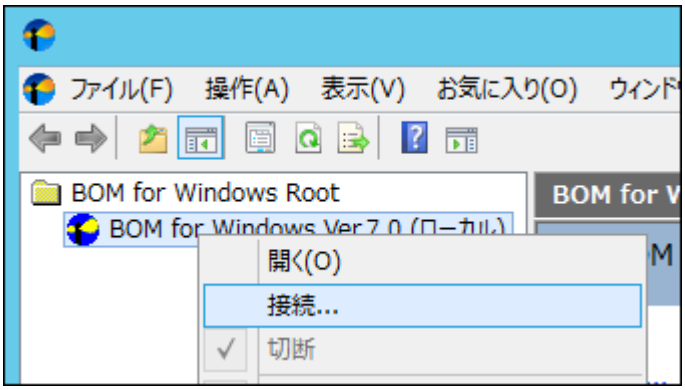
Linux を監視するには、Linux 用の監視インスタンスを作成する必要があります。

以下に Linux 監視インスタンスの作成手順の概要を示します。

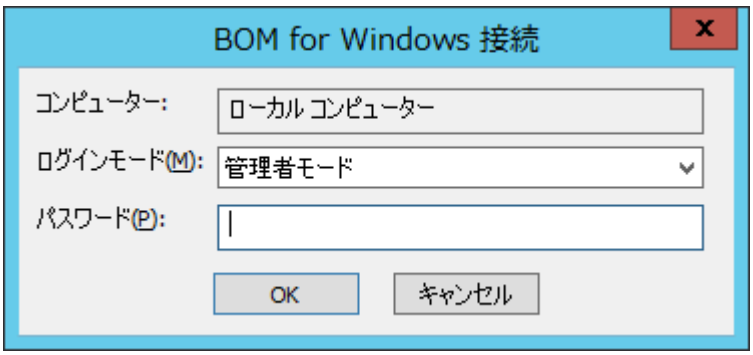
1. スタートメニューから“BOM 7.0 マネージャー”を選択します。

2. BOM 7.0 マネージャーが起動します。

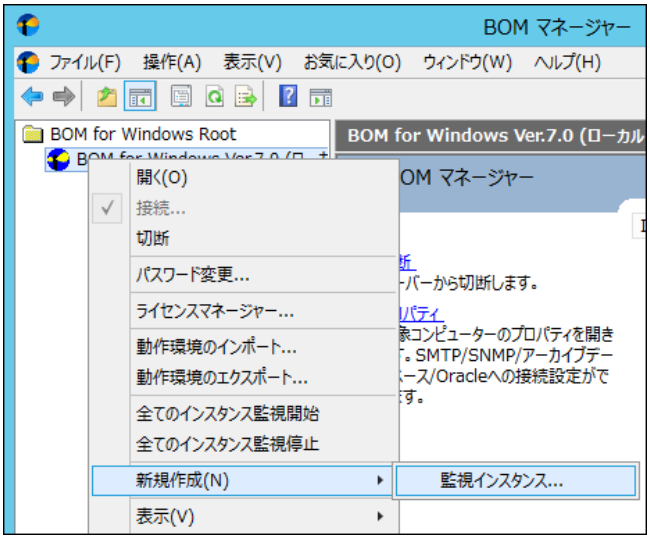
   スナップイン“BOM for Windows Ver.7.0（ローカル）”の右クリックメニューから“接続”を選択します。



3. “パスワード”に接続パスワード（既定では“bom”）を入力し、[OK]ボタンをクリックします。

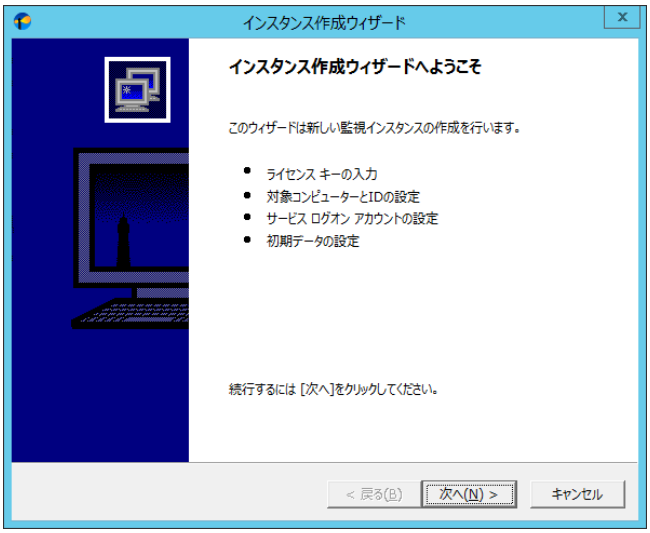


4. スナップイン“BOM for Windows Ver.7.0（ローカル）”の右クリックメニューから、“新規作成”→“監視インスタンス”を選択します。

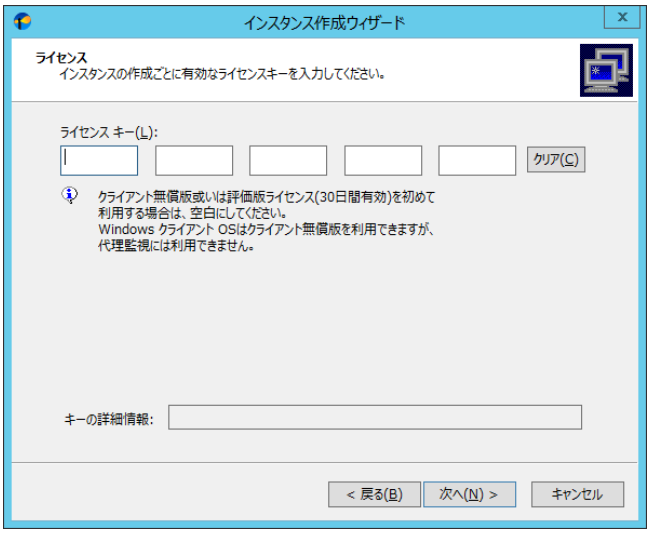


5. インスタンス作成ウィザードが起動します。

[次へ]ボタンをクリックし、“ライセンス”画面を表示します。

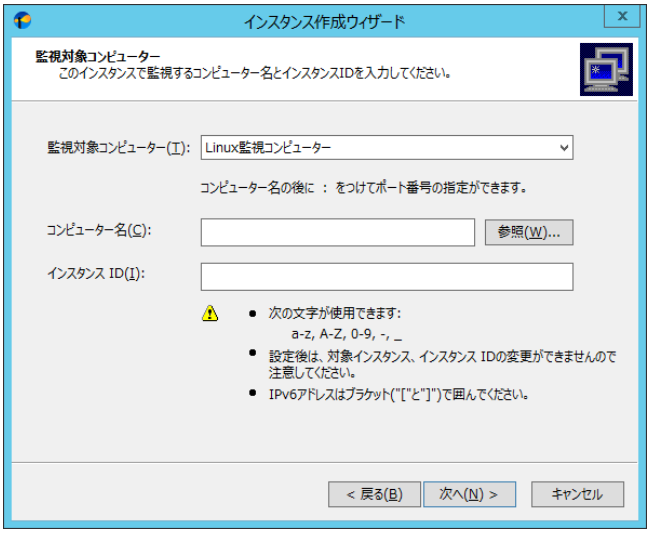


6. Linux オプションのライセンスキーを入力し、[次へ]ボタンをクリックします。



7. “コンピューター名”欄に Linux のコンピューター名または IP アドレスを入力します。

“インスタンス ID”欄に Linux が識別可能な名称を設定します。

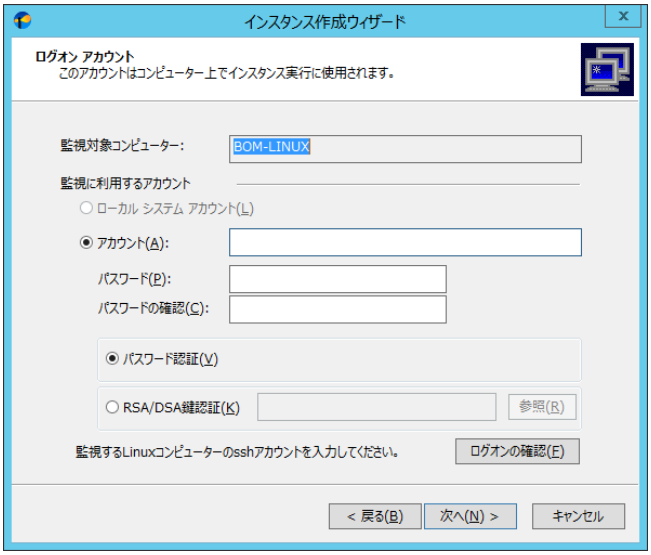


※　ホスト名は名前解決可能環境でのみ指定できます

※　SSH のポート番号はデフォルトで 22 番が設定されます

デフォルト値でない場合には、コンピューター名の後に半角英字の「:」(コロン)を入力しポート番号を半角数字で入力します

8. Linux に接続するためのアカウントの設定を行います。



● パスワード認証を使用する場合

“パスワード認証”にチェックを入れ、以下の情報を入力します。

“アカウント” … ssh ログインユーザー名を入力します。

“パスワード”、“パスワードの確認” … 指定したアカウントに対するパスワードを入力します。(必須入力)

● 鍵認証を使用する場合

“RSA/DSA 鍵認証”にチェックを入れ、以下の情報を入力します。

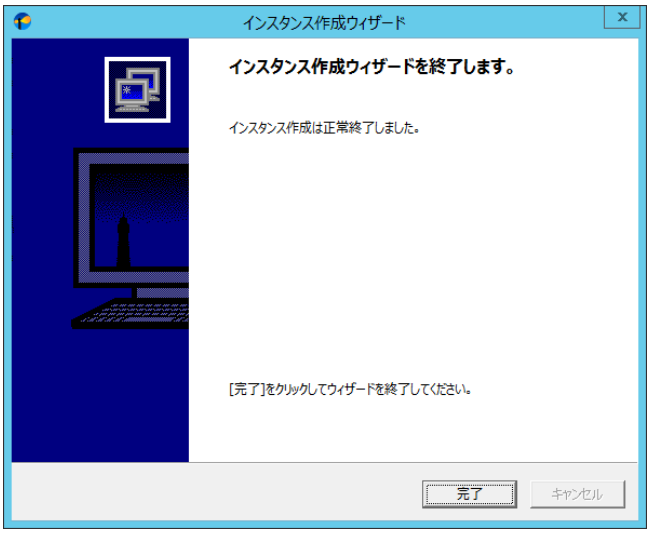
“RSA/DSA 鍵認証” … 使用する秘密鍵ファイルを指定します。

“アカウント” … ssh ログインユーザー名を入力します。

“パスワード”、“パスワードの確認” … 鍵に対するパスフレーズを入力します。(省略可)

9. [ログオンの確認]ボタンをクリックし、Linux に接続可能なことを確認した後に[次へ]ボタンをクリックします。

10. インスタンス作成ウィザードに従い、インスタンスの作成を完了させます。



2.4 アンインストール方法

Linux オプションと関連ソフトウェアのアンインストールについて、以下の手順に沿って作業してください。

アンインストール作業は管理者権限が必要となりますので、管理者権限を持つアカウントにてログオンの上、作業を行ってください。

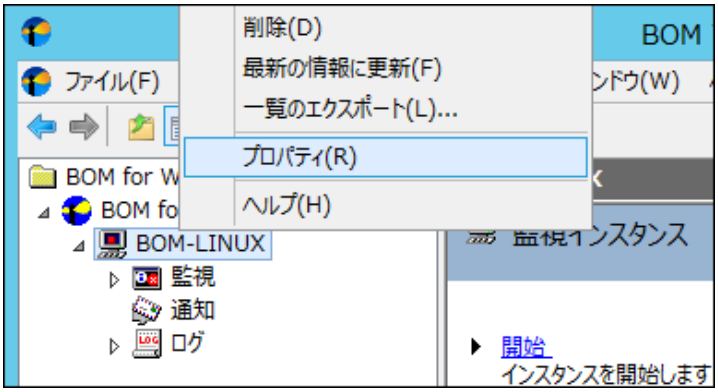
※　以降の手順は必要な作業項目の概要のみを抽出した概略手順となります。

BOM 7.0 の詳細なアンインストール手順については、'BOM for Windows Ver.7.0 インストール マニュアル' をご参照ください。

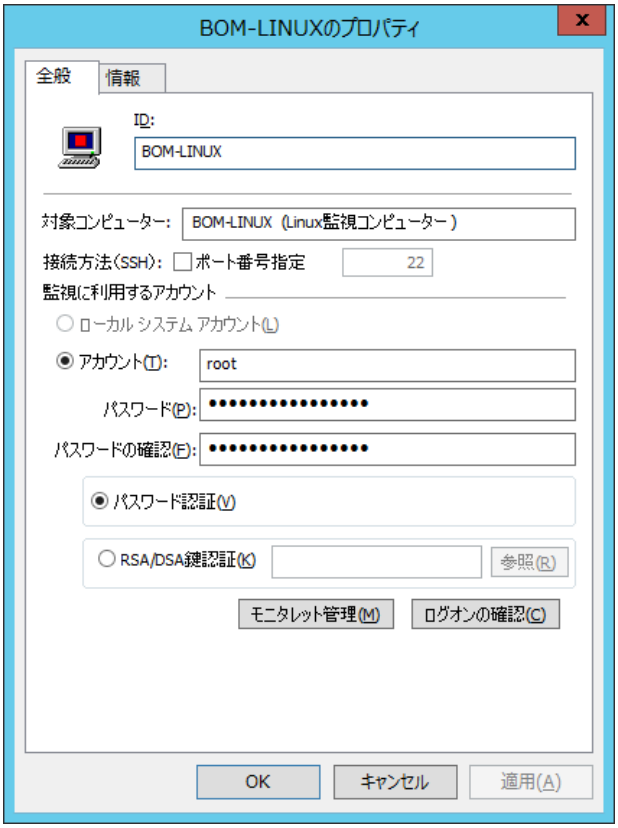
Linux オプションのアンインストール時には、モニタレットの削除を実行後、Linux オプションのアンインストールを行います。

2.4.1 モニタレットの削除

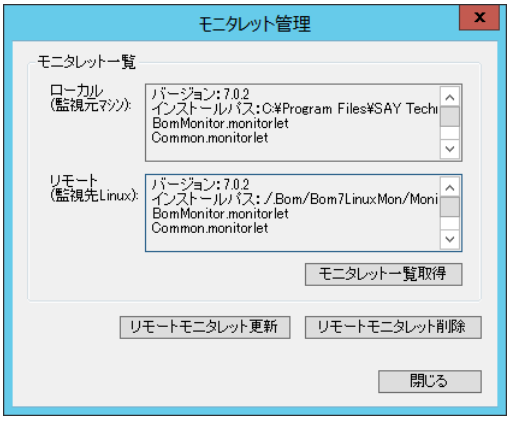
1. Linux コンピューターのインスタンスの"プロパティ"を開きます。



2. 「全般」タブの[モニタレット管理]ボタンをクリックします。



3. [リモートモニタレット削除]ボタンをクリックします。

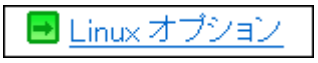


2.4.2 Linux オプションのアンインストール

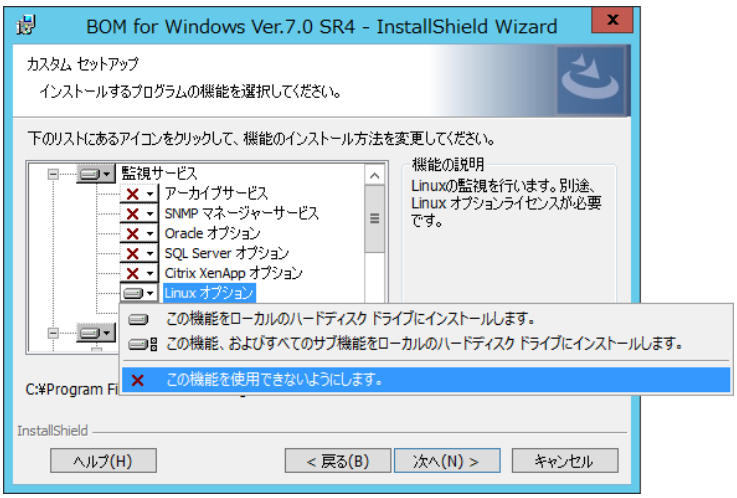
監視元コンピューターから Linux オプションをアンインストールする手順を以下に示します。

A. BOM 7.0 の Linux オプションのみをアンインストールする

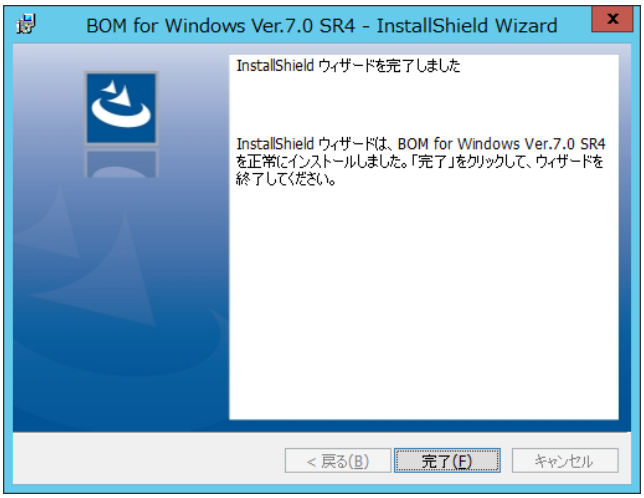
1. BOM 7.0 の媒体をコンピューターに挿入し、インストールランチャーを起動します。
2. メニューから“Linux オプション”をクリックし、セットアップウィザードを起動します。



3. “プログラムの保守”画面まで進め、“変更”ラジオボタンが有効になっていることを確認して[次へ]ボタンをクリックします。
4. “カスタムセットアップ”画面で“Linux オプション”の左のハードディスクアイコンをクリックし、“この機能を使用できないようにします。”を選択して[次へ]ボタンをクリックします。



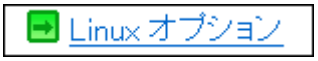
5. 以降はセットアップウィザードに従い、Linux オプションのアンインストールを完了させます。



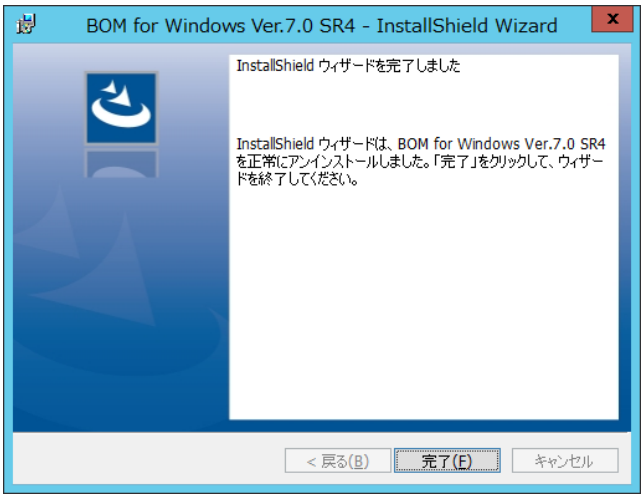
B. BOM 全体をアンインストールする

コンピューターから BOM 7.0 のすべてのコンポーネントをアンインストールするには、以下の作業を実施してください。

1. BOM 7.0 の媒体をコンピューターに挿入し、インストールランチャーを起動します。
2. メニューから“Linux オプション”をクリックし、セットアップウィザードを起動します。



3. “プログラムの保守”画面まで進め、“削除”ラジオボタンが有効になっていることを確認して[次へ]ボタンをクリックします。
4. 以降はセットアップウィザードに従い、Linux オプションを含む BOM 全体のアンインストールを完了させます。



第3章 BOM 7.0 の基本操作

Linux オプションの監視設定には、BOM 7.0 マネージャーを使用します。

以下に、BOM 7.0 の基本的な操作方法をご案内いたします。

ただし、以降の手順は Linux オプションを使用する上で必要な作業項目の概要のみを抽出した概略手順となります。

BOM 7.0 マネージャーや BOM 7.0 集中監視コンソールの詳細な利用方法については、'BOM for Windows Ver.7.0 ユーザーズ マニュアル' をご参照ください。

3.1 BOM 7.0 マネージャーの基本操作

以下に、BOM 7.0 マネージャーの基本的な操作方法をご案内いたします。

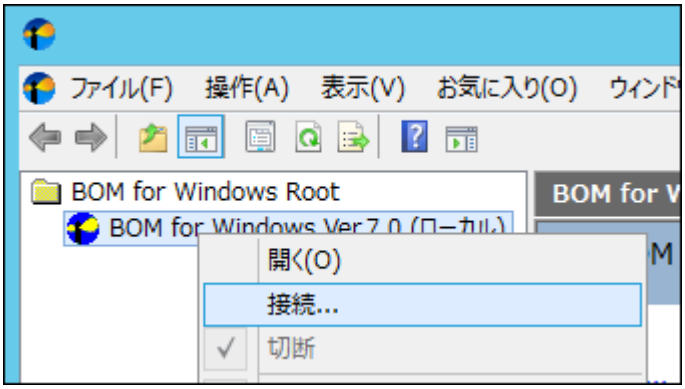
なお、以降の作業は管理者権限が必要となりますので、管理者権限を持つアカウントにてログオンの上、作業を行ってください。

3.1.1 BOM 7.0 マネージャーの起動と接続

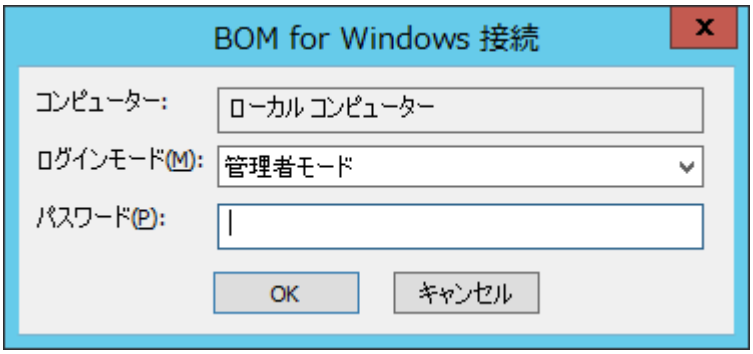
1. "スタートメニュー"を表示し"BOM 7.0 マネージャー"をクリックします。

2. BOM 7.0 マネージャーが起動します。

スナップイン"BOM for Windows Ver.7.0(ローカル)"の右クリックメニューから"接続"を選択します



3. “パスワード”欄に接続パスワード（既定では“bom”）を入力し、[OK]ボタンをクリックします。



以上の手順にて、BOM への接続が完了し、操作できる状態になります。

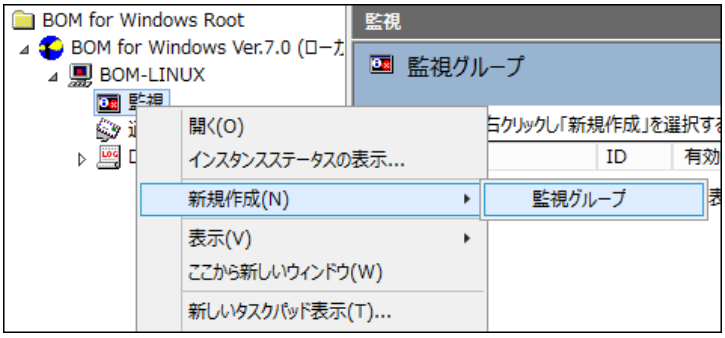
3.1.2 監視グループの作成/削除と設定変更

A. 監視グループの作成

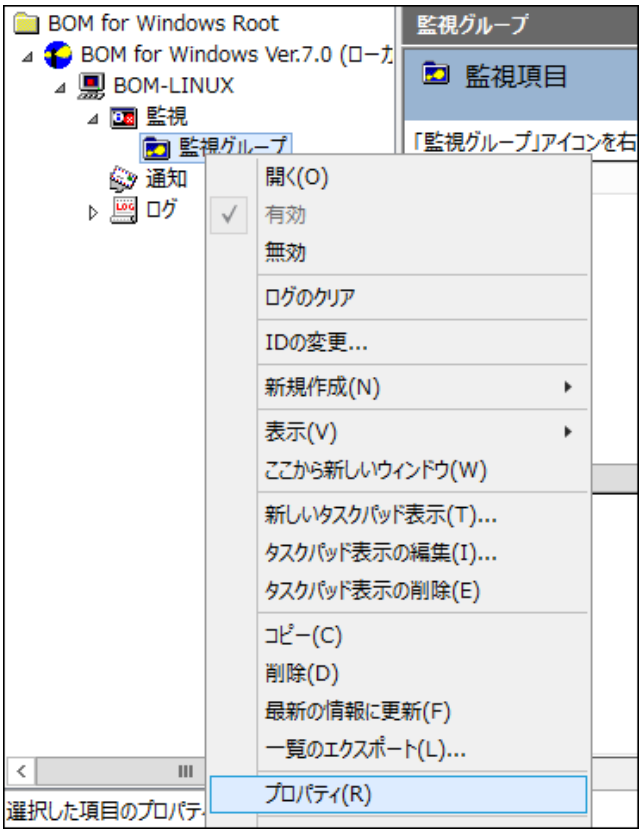
以下に、監視を行うための土台となる“監視グループ”の作成手順を示します。

1. スコープペインより“BOM for Windows Ver.7.0（ローカル）”→“（監視インスタンス名）”→“監視”を選択します。

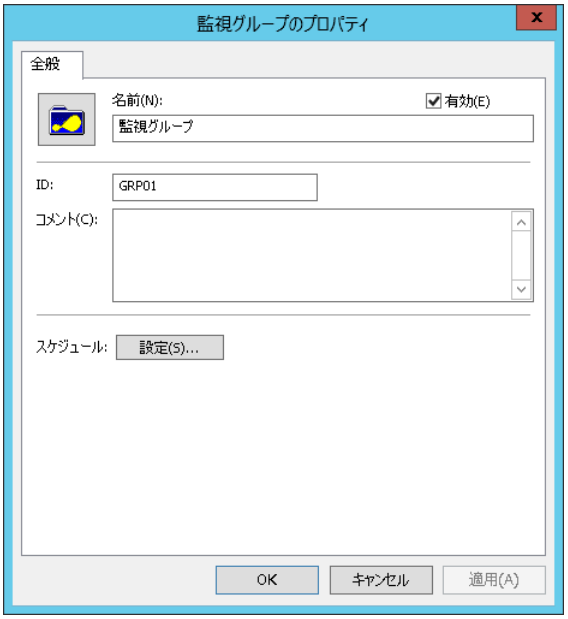
2. 右クリックメニューから“新規作成”→“監視グループ”を選択し、監視グループを作成します。



3. 作成した監視グループをいずれかのペインで選択し、右クリックメニューから“プロパティ”を選択します。



4. 監視グループ名、監視の有効/無効など各種設定を必要に応じて変更します。 [OK]ボタンをクリックし設定を保存します。



B. 監視グループの削除

以下に、“監視グループ”の削除手順を示します。

1. “監視”ノードを展開し、監視グループを表示します。
2. 削除対象の監視グループを右クリックし、“削除”を選択します。

3.1.3 監視項目の作成/削除と設定変更

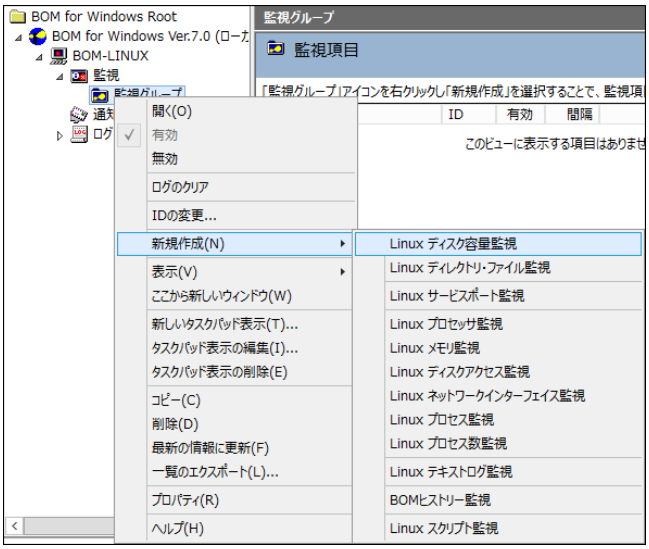
A. 監視項目の作成

監視項目は“新規作成”と“テンプレートのインポート”のいずれかの方法で作成します。以下に、それぞれの手順を示します。

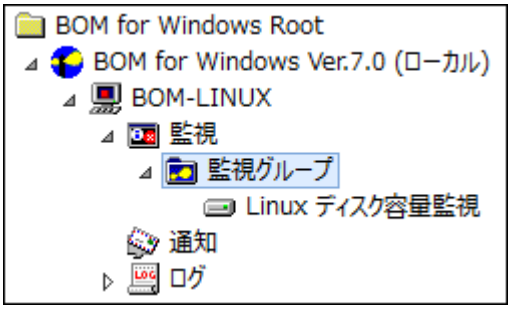
①「新規作成」による作成

1. 登録先のインスタンスを停止します。
2. スコープペインより“BOM for Windows Ver.7.0(ローカル)”→“(監視インスタンス)”→“監視”→“監視グループ”を選択します。

3. 右クリックメニューから“新規作成”→“（任意の監視項目）”を選択し、任意の監視項目を作成します。

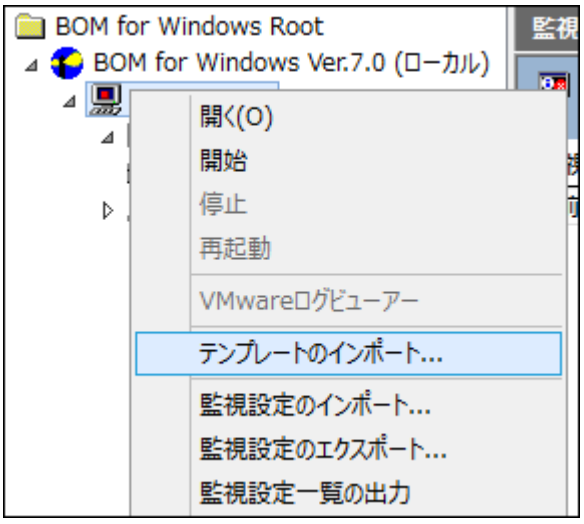


4. 監視グループ内に監視項目が作成されます。

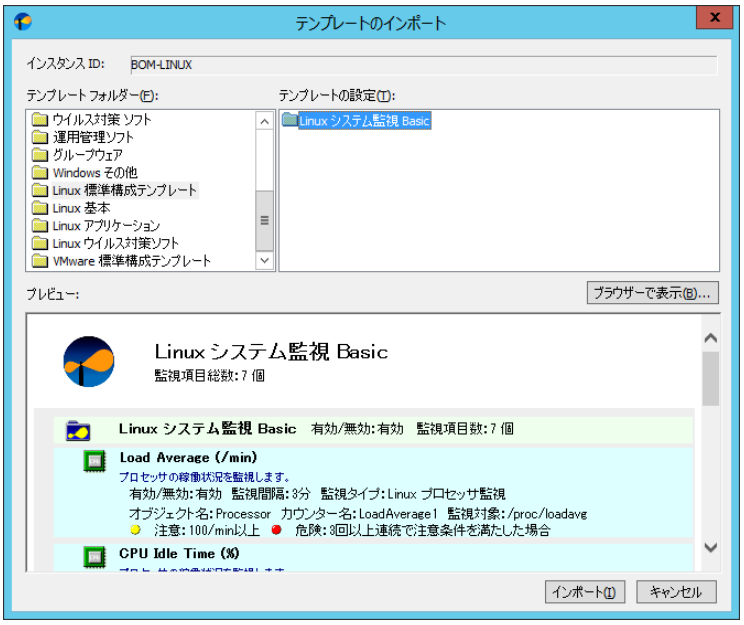


② テンプレートのインポートによる作成

1. 登録先の監視インスタンスを停止します。
2. 登録先のインスタンスを右クリックし“テンプレートのインポート”を選択します。

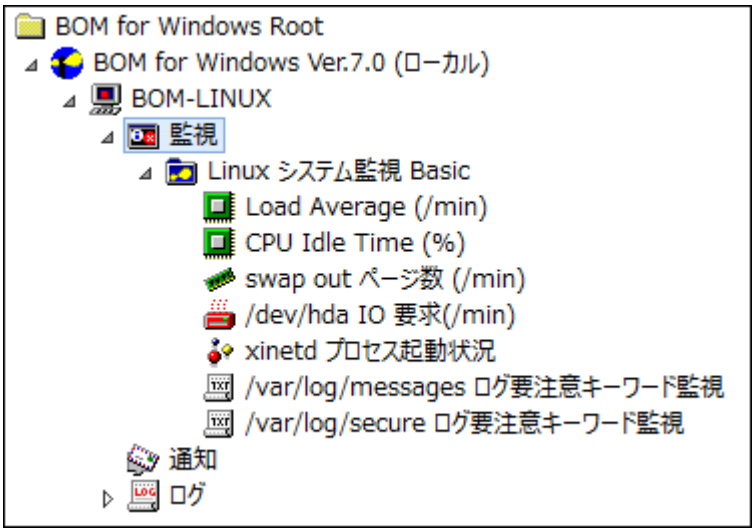


3. “テンプレートのインポート”ウインドウで、監視対象 Linux に適合したバージョン用のテンプレートを選択します。



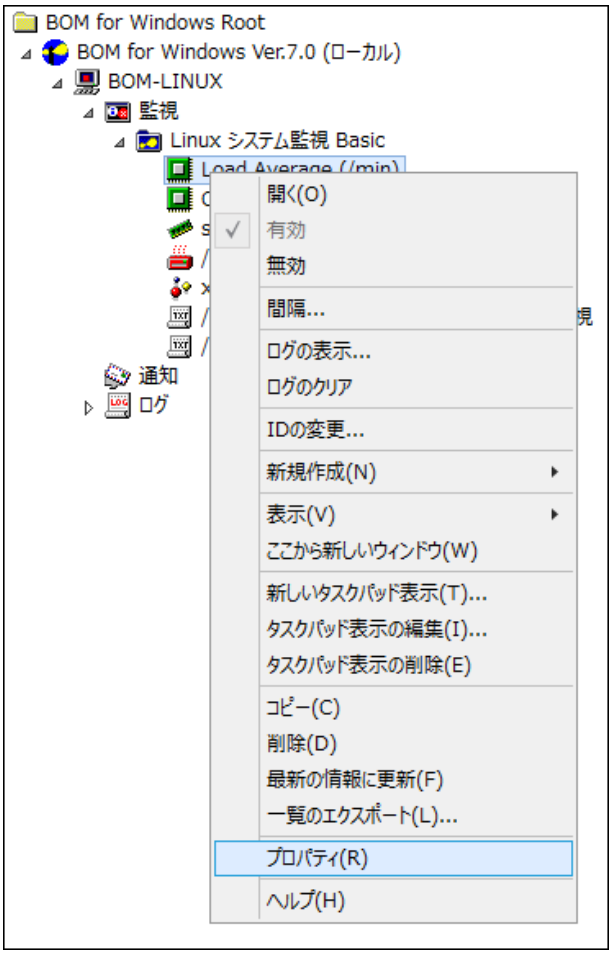
4. [インポート]ボタンをクリックし、インポートを実行します。

インポート先監視インスタンスの“監視”ノードに、“Linux xx 監視”グループが追加されたことを確認します。

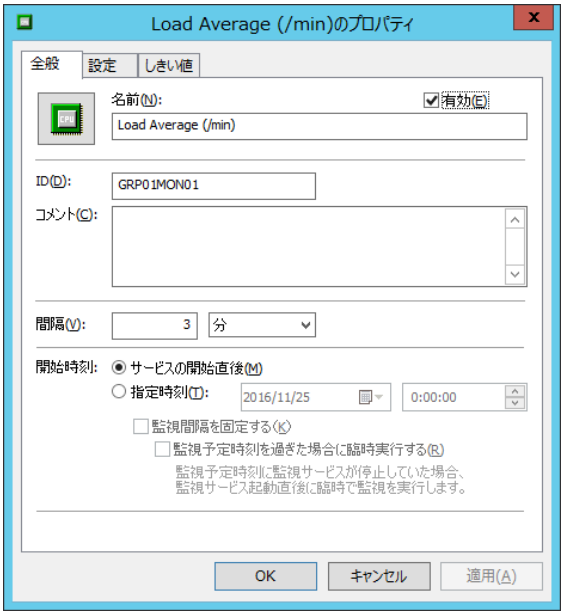


B. 監視項目の設定変更

1. 作成した監視項目をいずれかのペインで選択し、右クリックメニューから“プロパティ”を選択します。

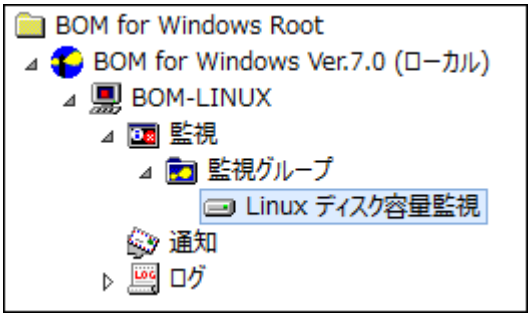


2. 監視項目名、監視の有効/無効など、各種設定を必要に応じて変更します。
3. [OK]ボタンをクリックし、設定を保存します。

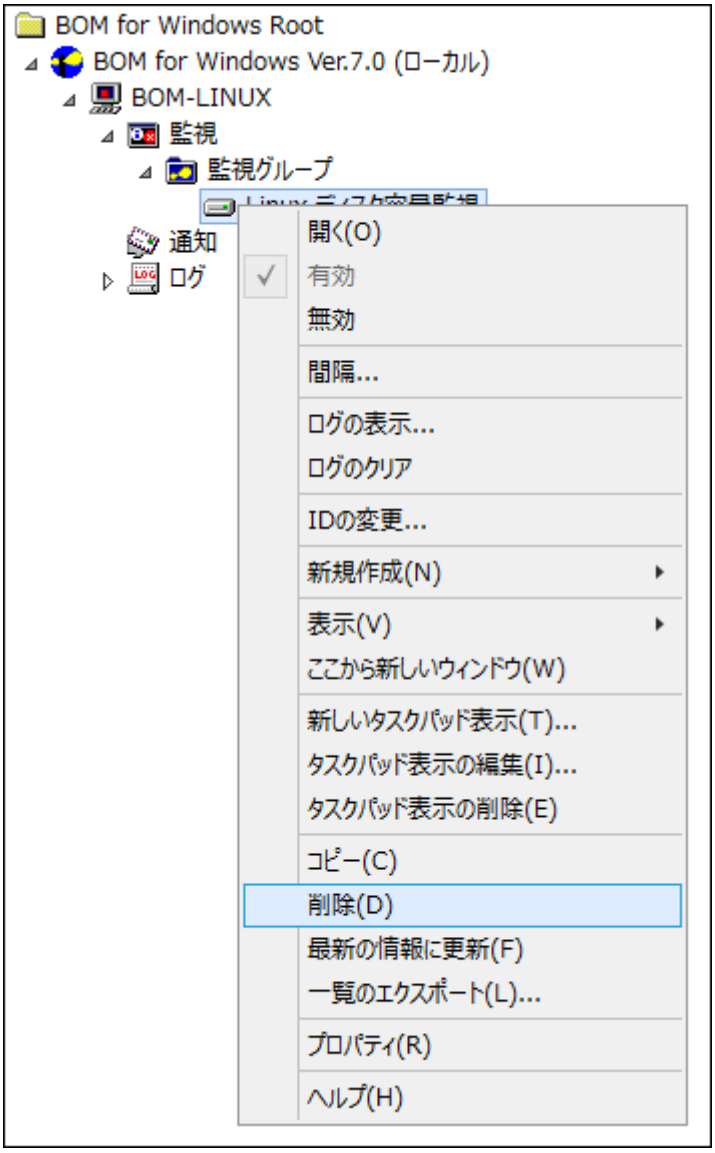


C. 監視項目の削除

1. “監視”ノードを展開し、更に削除対象の監視項目を含む監視グループを展開します。



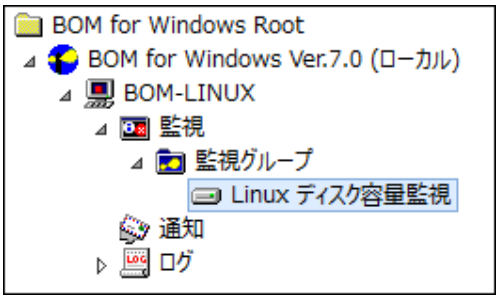
2. 削除したい監視項目を右クリックし、“削除”を選択します。



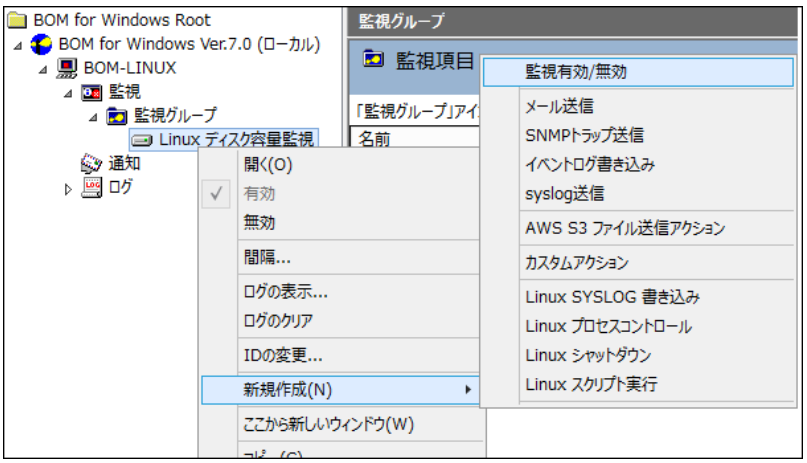
3.1.4 アクション項目の作成と設定変更

以下に、実際に監視結果（ステータス）を元に処理を行う“アクション項目”の作成手順を示します。

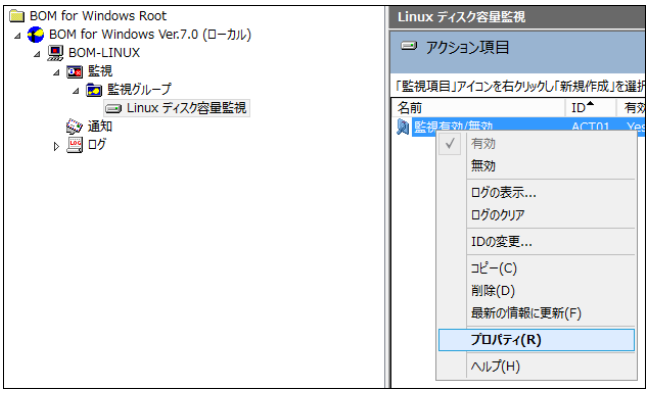
1. スコープペインより“BOM for Windows Ver.7.0（ローカル）”→“（監視インスタンス名）”→“監視”→“（任意の監視グループ）”→“（任意の監視項目）”を選択します。



2. 右クリックメニューから“新規作成”→“（任意のアクション項目）”を選択し、任意のアクション項目を作成します。

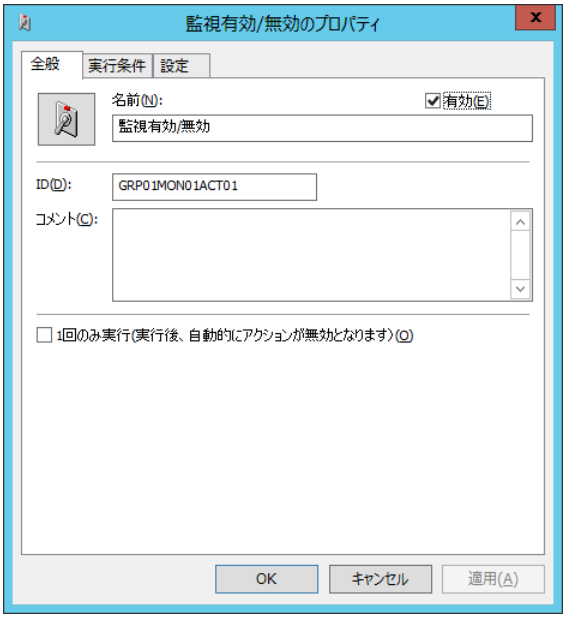


3. 作成したアクション項目をリザルトペインで選択し、右クリックメニューから“プロパティ”を選択します。



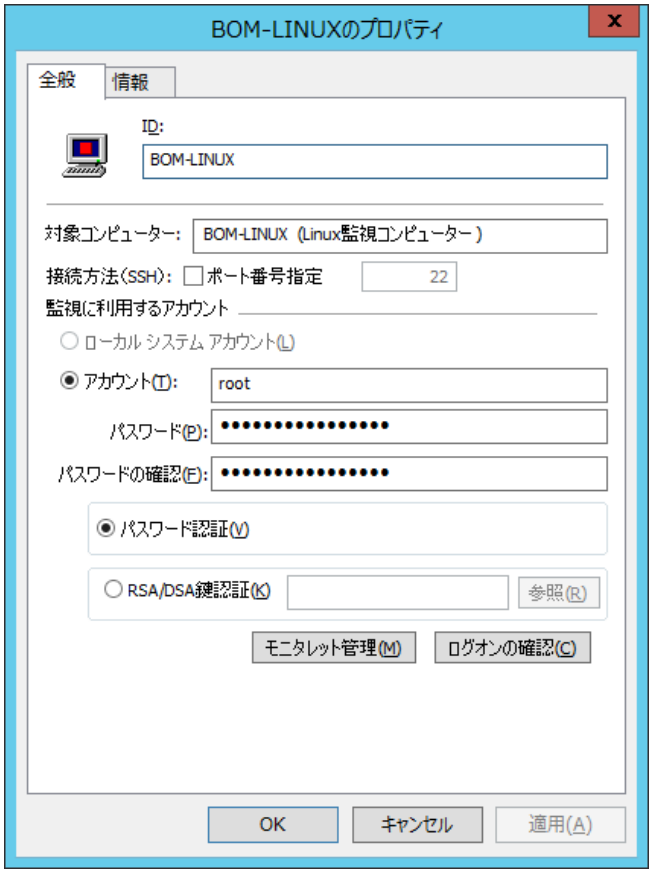
4. アクション項目名、アクションの有効/無効など、各種設定を必要に応じて変更します。

   [OK]ボタンをクリックし、設定を保存します。

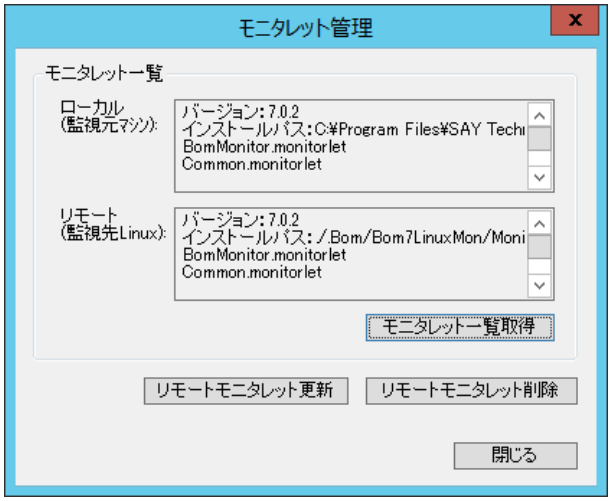


3 .2 Linux インスタンスのプロパティ

Linux コンピューターのインスタンスのプロパティは Windows の標準インスタンスのプロパティとは異なります。インスタンス作成後、SSH のポート番号が変更、あるいは監視用アカウント変更（パスワードを含む）する場合にはこのプロパティで変更します。監視用アカウントを変更した場合には、必ずモニタレットの更新が必要になります。



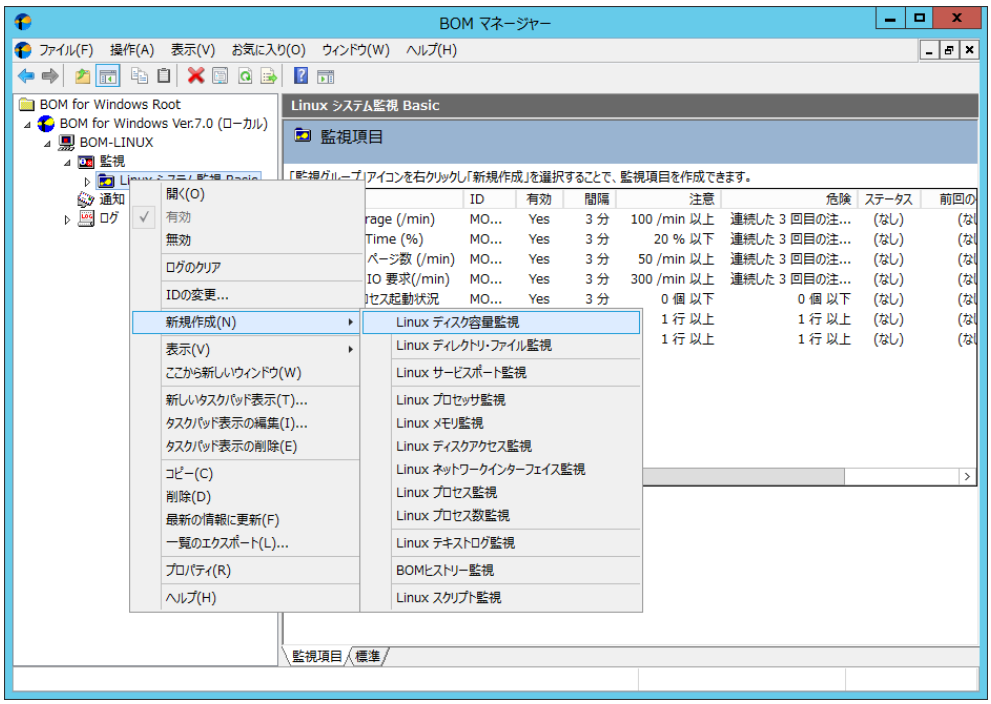
ID	監視対象コンピューターのインスタンス ID が表示されます
対象コンピューター	監視対象コンピューターの対象コンピューター名＋（Linux 監視コンピューター）と表示されます
接続方法(SSH)	ポート番号の指定を行います。デフォルト値は 22 ですが Linux コンピューターの SSH のポート番号がデフォルト値以外に設定されている場合には“ポート番号指定”をチェックし番号を指定して下さい
アカウント	インスタンス作成時に設定したアカウントが表示されます アカウントを変更する場合にはここで指定します
パスワード、パスワードの確認	設定アカウントのパスワード（パスワード認証の場合）または、鍵ファイルのキーフレーズ（RSA/DSA 鍵認証の場合）を指定します
パスワード認証	パスワード認証を使用する場合はこちらにチェックを入れます。
RSA/DSA 鍵認証	鍵認証を使用する場合はこちらにチェックを入れ、使用する秘密鍵ファイルを指定します。
モニタレット管理	監視用のモニタレットのバージョン確認・更新・削除を行います
ログオンの確認	指定したアカウントとパスワードで監視対象コンピューターにログオンできるか確認します



モニタレット一覧取得	監視対象コンピューターにインストールされたモニタレットのバージョンを表示します これから更新しようとするモニタレットのバージョンが“ローカル”に表示され 既にインストールされたモニタレットのバージョンが“リモート”に表示されます
リモートモニタレット更新	Linux コンピューター上のモニタレットを更新します
リモートモニタレット削除	Linux コンピューター上のモニタレットを削除します

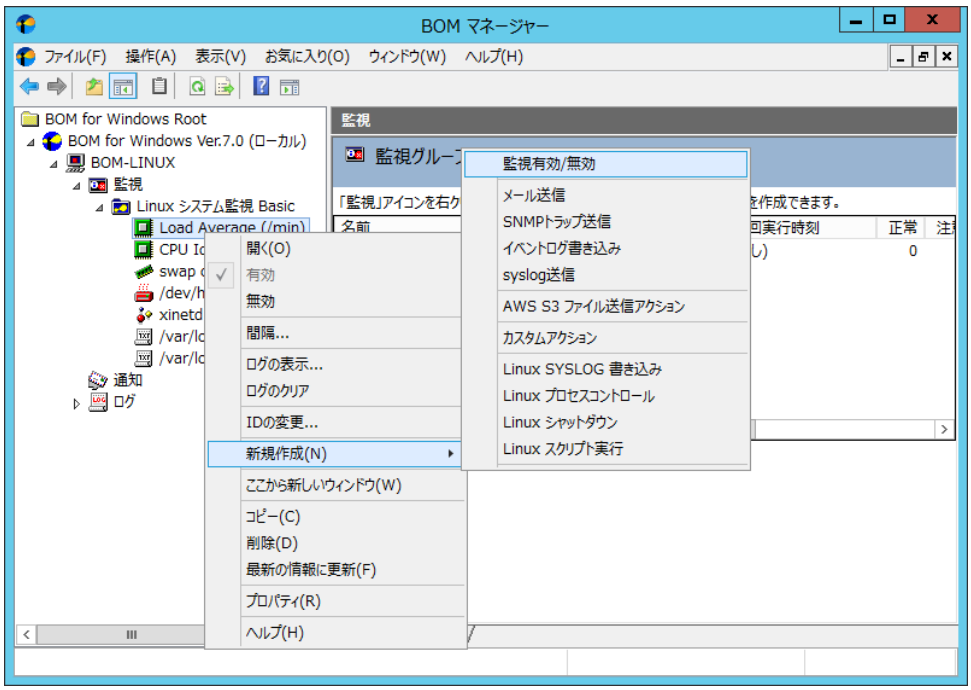
3 .3 Linux 監視メニュー

BOM 7.0 マネージャーの Linux コンピューターのインスタンスノード下の“監視”ノードの任意の監視グループを右クリックし、新規作成を選択すると、Linux オプションの監視項目メニューが現れます。



3 .4 アクションメニュー

各監視項目を右クリックし新規作成を選択すると、Linux オプションで追加されたアクションメニューが表示されます。



第4章 Linux オプションによる監視

4.1 Linux オプション概要

Linux オプションでは、監視コンピューター（BOM）から監視対象コンピューター（Linux）に接続し、各種情報を取得して監視いたします。

本章では、Linux を監視するための情報をご案内いたします。

なお、Linux の監視にあたりましては、Linux 用の監視インスタンス（Linux 監視インスタンス）が必要になります。

Linux 監視インスタンスを作成していない場合には、‘2.3 インストール手順’をご参照ください。

4.2 監視項目設定

Linux 監視インスタンスにて使用できる監視項目について、使用方法を解説いたします。

Linux 監視インスタンスにて使用できる監視項目は、以下の 12 種類です。

アイコン	監視項目名	説明
	Linux ディスク容量監視	Linux のディスク容量を監視
	Linux ディレクトリ・ファイル監視	Linux のディレクトリ/ファイルを監視
	Linux サービスポート監視	Linux のサービスポートを監視
	Linux プロセッサ監視	Linux のプロセッサを監視
	Linux メモリ監視	Linux のメモリを監視
	Linux ディスクアクセス監視	Linux のディスクアクセス状況を監視
	Linux ネットワークインターフェイス監視	Linux のネットワーク インターフェイスを監視
	Linux プロセス監視	Linux 上で動作しているプロセスを監視
	Linux プロセス数監視	Linux 上で動作しているプロセス数を監視
	Linux テキストログ監視	Linux のテキストログを監視
	Linux スクリプト監視	任意のプログラムを Linux 上で実行し、実行結果を監視
	BOM ヒストリー監視	BOM のヒストリーを監視

以降は、それぞれの監視項目の使用方法と設定方法についてご案内いたします。

4.2.1 各監視項目共通の設定

監視項目は、作成しただけでは意図した監視が行えません。監視項目は、作成した後に設定を行います。

監視項目をいずれかのペインで選択し、右クリックメニューから“プロパティ”を選択すると、プロパティシートが表示されます。

監視項目の設定は、このプロパティシートにて行います。

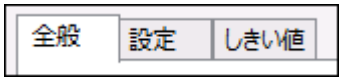
※　監視項目の概念は BOM 7.0 と同一であるため以降では設定に必要な説明のみご案内いたします

詳細については‘BOM for Windows Ver.7.0 ユーザーズ マニュアル’をご参照ください

A. 基本操作

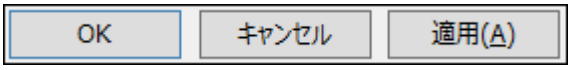
1. タブ

プロパティシートは、「全般」、「設定」などのタブで構成されています。それぞれのタブをクリックすることで、該当するタブが表示され、設定を変更できます。



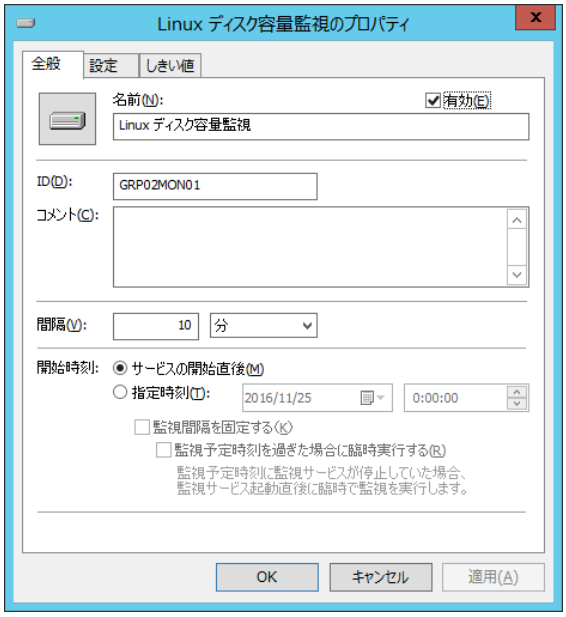
2. 変更した設定の反映と破棄

変更した設定は、[OK]ボタン、または[適用]ボタンをクリックすることで BOM 7.0 に反映することができます。変更した設定を破棄したい場合には[キャンセル]ボタンをクリックします。



B.「全般」タブ

「全般」タブは、“アイコン”、“ID”、“名前”、“間隔”に設定されている値を除き、すべての監視項目で共通です。

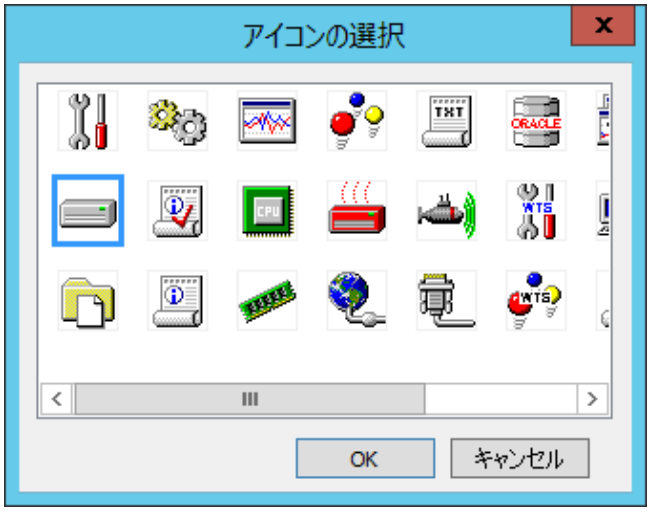


1. [アイコン]ボタン

[アイコン]ボタンは監視項目で設定されているアイコンが表示されています。

既定では、監視項目の種類に合わせたアイコンが設定されています。

[アイコン]ボタンをクリックすることで、アイコンを変更するためのダイアログを表示することができます。



アイコンを変更する場合には、ダイアログにて変更したいアイコンをクリックし、[OK]ボタンをクリックします。

2. “有効”チェックボックス

“有効”チェックボックスはチェックを入れることで監視が有効になります。既定ではチェックボックスにチェックが入っています。監視を行いたくない場合にはチェックボックスからチェックを外してください。

3. “名前”欄

“名前”欄には、監視項目名を入力します。既定値として監視項目の種類と同じ名称が入力されています。必要に応じて、分かりやすい名称に変更してください。

4. “ID”欄

“ID”欄には、監視項目 ID が表示されます。監視項目 ID は、インスタンス内で監視項目ごとに一意になるように、BOM が自動的に設定します。

5. “コメント”欄

“コメント”欄には、監視項目の補足情報を入力します。既定では空白です。必要に応じて入力してください。

6. “間隔”欄

“間隔”欄には、監視項目の監視間隔を入力します。既定値として監視項目の種類ごとに定められた推奨値が入力されています。

入力欄には、1 から 9999 までの整数を入力できます。単位は“秒”、“分”、“時”、または“日”から選択できます。

7. 開始時刻

開始時刻には、監視項目を開始する日時を指定します。既定ではラジオボタン“サービスの開始直後”が選択されています。ラジオボタン“サービスの開始直後”を選択した場合には BOM 監視サービスの起動時に、ラジオボタン“指定時刻”を選択した場合には指定の日時に、初回の監視を実行します。

なお、初回以降の監視は、指定した監視間隔ごとに行われます。

8. “監視間隔を固定する”チェックボックス

“監視間隔を固定する”チェックボックスは、チェックを入れることで指定時間を基準日時として監視間隔を固定します。ラジオボタン“指定時刻”を選択した場合のみ利用できる機能で、既定ではチェックボックスのチェックは外れています。

チェックボックスのチェックが外れている場合、BOM 監視サービスを再起動すると、前回の監視時刻を無視して監視を即時実行します。監視サービス再起動によって監視間隔が変動することを防止したい場合には、チェックボックスにチェックを入れてください。

9. “監視予定時刻を過ぎた場合に臨時実行する”チェックボックス

“監視予定時刻を過ぎた場合に臨時実行する”チェックボックスは、チェックボックスのチェックを入れることで監視サービス再起動などによって前回の監視から監視間隔以上を経過していた場合、臨時で監視を行います。

“監視間隔を固定する”チェックボックスにチェックを入れた場合のみ利用できる機能で、既定ではチェックボックスのチェックは外れています。

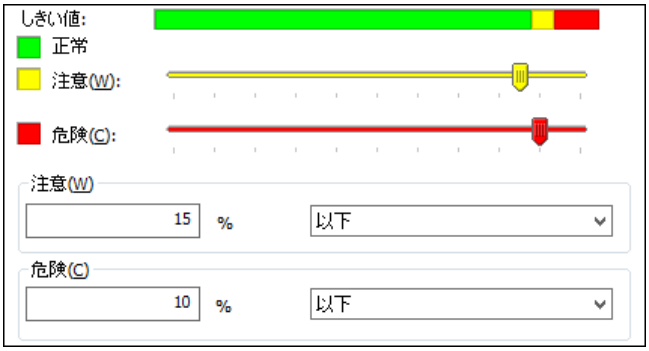
例えば、毎日 10:00 に監視するように設定した上で、当日の 10:00 に監視サービスが起動していなかった場合に、10:20 に監視サービスを起動すると、チェックボックスにチェックを入れた場合は、当日は 10:20 に臨時で監視を行い、翌日以降は 10:00 に監視します。

チェックボックスのチェックを外した場合には、当日は監視が行われず、翌日以降は 10:00 に監視します。

C. しきい値

すべての監視項目では、しきい値を設定する必要があります。しきい値に設定した条件に合致することで、監視ステータスが“注意”や“危険”に変化します。しきい値に設定した条件に合致しない場合には監視ステータスが“正常”になります。

しきい値の設定方法は監視項目の種類によって異なります。



4.2.2 Linux ディスク容量監視

Linux ディスク容量監視では、Linux で使用しているディスクの空き容量を監視します。

※ df コマンドで出力されるもので かつ/dev から始まるものが対象になります

※ ローカルファイルシステムのみ監視可能です

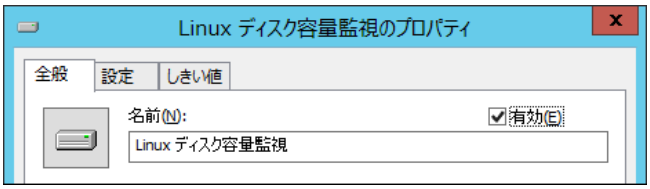
※ サイズが 0 の特殊マウントデバイスは表示されません

A.「全般」タブ

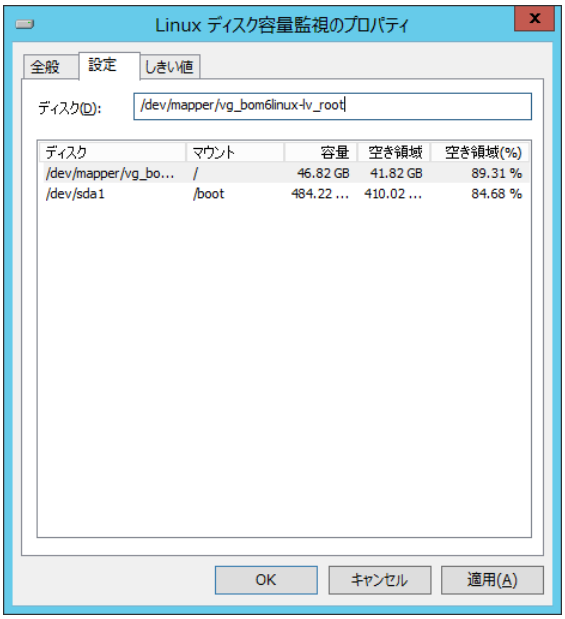
「全般」タブは、“アイコン”、“ID”、“名前”、“間隔”に設定されている値を除き、すべての監視項目で共通です。

Linux ディスク容量監視では、監視間隔の既定値は 10 分に指定されています。

「全般」タブの詳細については‘4.2.1 各監視項目共通の設定’の項目‘B.「全般」タブ’をご参照ください。



B.「設定」タブ



1. “ディスク”欄

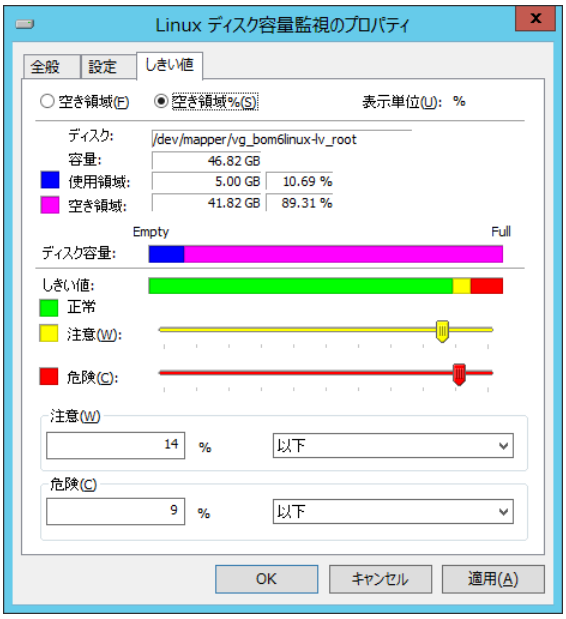
   監視するディスクをリストビューより選択して設定します。

   デフォルト(まだ設定されていない場合)は、先頭のディスクが自動的に設定されます。

   入力は 260 文字までです。

C.「しきい値」タブ

「しきい値」タブでは、監視項目のしきい値を指定します。



1. 空き領域

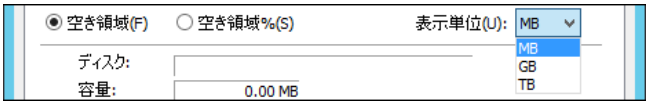
空き領域では、空き領域の取得方法を選択します。既定ではラジオボタン“空き領域%”が選択されています。

ラジオボタン“空き領域”を選択した場合には、空き領域をバイト単位で監視します。

ラジオボタン“空き領域%”を選択した場合には、空き領域を全容量からの割合で監視します。

2. 表示単位

表示単位は、しきい値を指定する際の単位です。ラジオボタン“空き領域%”を選択した場合には、表示単位は“%”固定です。ラジオボタン“空き領域”を選択した場合には、“MB”、“GB”、または“TB”から選択できます。

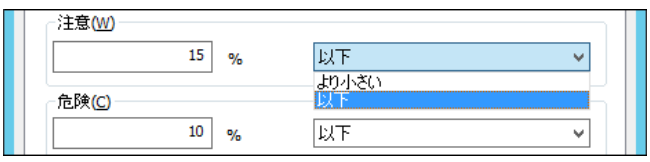


3. しきい値

しきい値では、“注意”および“危険”のしきい値条件を指定します。

既定では“注意”しきい値が 15 % 以下、“危険”しきい値が 10 % 以下に設定されています。

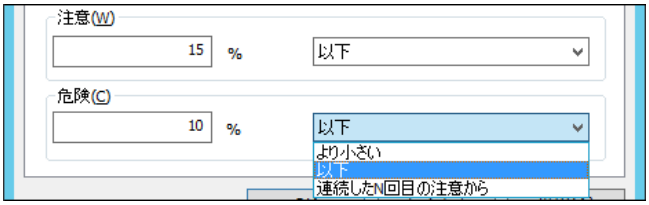
“注意”しきい値は、全容量よりも小さい 0 以上 100 以下の整数を指定します。容量はスライドバーで指定することもできます。



また、“注意”しきい値の条件指定は、“より小さい”、“以下”から選択できます。

“危険”しきい値は、“注意”しきい値と同様に設定できます。それに加え、条件指定では“注意”しきい値の条件を連続して満たすことを条件にする“連続した N 回目の注意から”を選択できます。

“連続した N 回目の注意から”を使用する場合には、入力欄には 1 から 99 までの整数を入力できます。



4 .2 .3 Linux ディレクトリ・ファイル監視

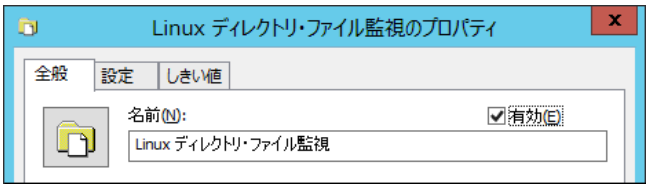
Linux ディレクトリ・ファイル監視では、Linux のディレクトリ・ファイルサイズや数を監視します。

A.「全般」タブ

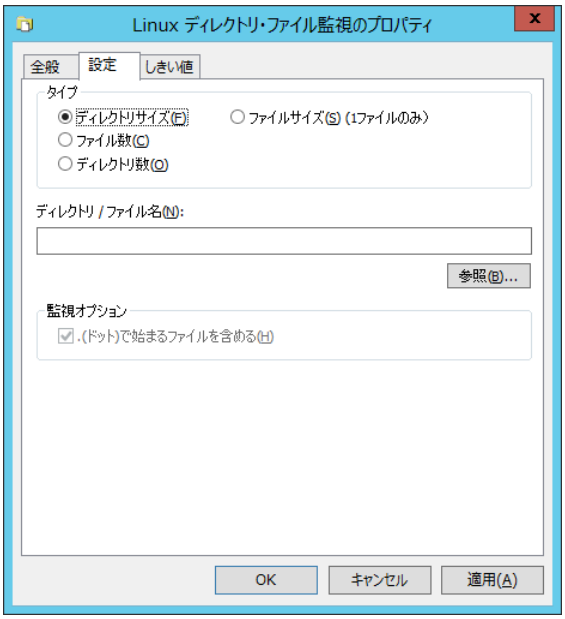
「全般」タブは、“アイコン”、“ID”、“名前”、“間隔”に設定されている値を除き、すべての監視項目で共通です。

Linux ディレクトリ・ファイル監視では、監視間隔の既定値は 10 分に指定されています。

「全般」タブの詳細については ‘4 .2 .1 各監視項目共通の設定’ の項目 ‘B.「全般」タブ’ をご参照ください。



B.「設定」タブ



1. タイプ

次の 4 つのうち 1 つを選択します。デフォルトはディレクトリサイズです。

ディレクトリサイズ	ディレクトリを指定します ディレクトリの使用サイズを監視します
ファイル数	ディレクトリを指定します ディレクトリ内のファイル数を監視します
ディレクトリ数	ディレクトリを指定します ディレクトリ内のディレクトリ数を監視します
ファイルサイズ	ファイルを指定します 指定したファイルのサイズを取得します

2. ディレクトリ/ファイル名

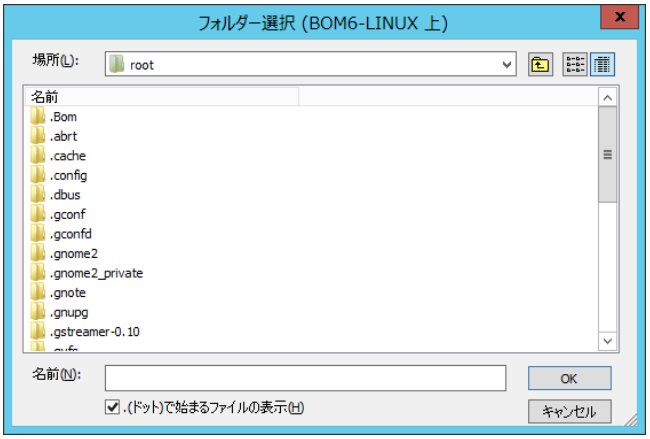
“タイプ”欄の選択に従い、監視する対象のパスを指定します。

デフォルトでは空欄ですが、指定しないと監視を行うことができません。

※260 文字まで入力することができます

3. 参照

ディレクトリ/ファイルを選択します。



ファイルサイズの場合にはファイル選択の画面になります。ファイルサイズ以外の場合にディレクトリ選択の画面になります。

ドットで始まるファイルの表示をチェックすると、隠しエントリとしてのドットファイル/ディレクトリが一覧に表示されます。初期状態はチェック状態です。結果はディレクトリ/ファイル名にセットされます。

※260 文字までのファイル名/ディレクトリ名が指定できます

※ファイル・ディレクトリのシンボリックリンクは“実ファイル”・“ディレクトリ”と同様の扱いです

※アカウントに参照権限がない場合ファイルダイアログに一覧表示されません　また監視時はエラーになります

※ファイル・ディレクトリ名に ASCII 文字以外が含まれる場合ファイルダイアログの表示や監視が正しくできません

※ボリュームの大きなディレクトリの監視で処理に 10 分以上かかる場合はタイムアウトして“エラー”となります

（後続の監視値も“エラー”になる場合があります）大きなボリュームにはディスク監視を使用されることを推奨します

4. 監視オプション

“B”で選択した内容が、“ファイル数”・“ディレクトリ数”の場合にのみ有効になります。

“.(ドット)で始まるファイルの表示”はデフォルトは有効になっています。隠しファイルとしてのドットファイルを検索に含めない場合にはチェックを外して下さい。

C.「しきい値」タブ

1. ディレクトリ/ファイル名

設定タブで入力したディレクトリ/ファイル名がそのまま表示されます。

2. 現在値の取得

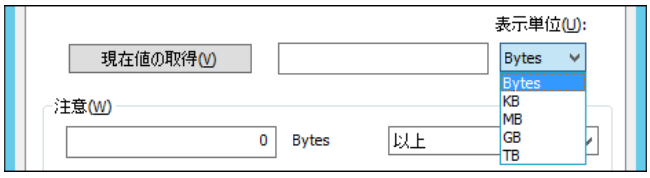
設定タブで指定したタイプの現在の値を取得します。

3. 表示単位

表示単位は、しきい値を指定する際の単位です。

「設定」タブのタイプ欄で、“ファイル数”、“ディレクトリ数”を選択した場合、表示単位はグレーアウトして選択できません。

“ディレクトリサイズ”、“ファイルサイズ”を選択した場合は、“Bytes”、“KB”、“MB”、“GB”、または“TB”から選択できます。

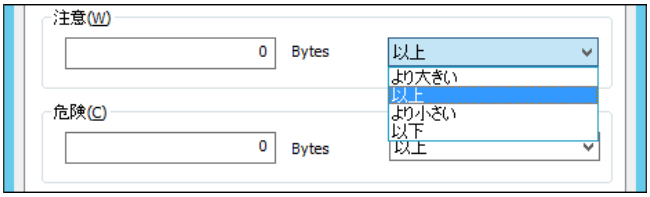


4. しきい値

しきい値では、“注意”および“危険”のしきい値条件を指定します。

既定では“注意”しきい値が 0 Bytes、“危険”しきい値が 0 Bytes 以上に設定されています。

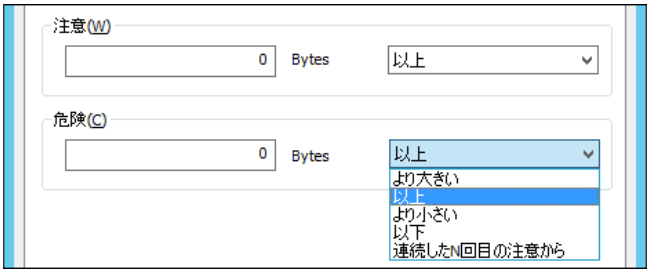
しきい値の設定範囲（上限下限）は 0～999999999 です。



また、“注意”しきい値の条件指定は、“より大きい”、“以上”、“より小さい”、“以下”から選択できます。

“危険”しきい値は、“注意”しきい値と同様に設定できます。それに加え、条件指定では“注意”しきい値の条件を連続して満たすことを条件にする“連続した N 回目の注意から”を選択できます。

“連続した N 回目の注意から”を使用する場合には、入力欄には 1 から 99 までの整数を入力できます。



4.2.4 Linux サービスポート監視

Linux サービスポート監視では、Linux のポート(TCP/UDP)稼働状況を監視します。

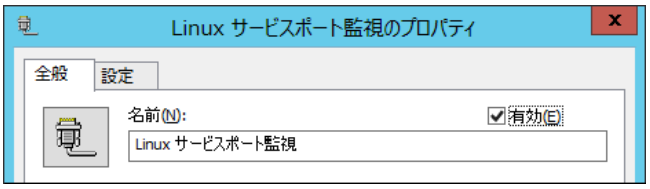
※ Linux サービスポート監視を実行する場合、Linux インスタンスの“プロパティ”の「全般」タブに設定する“監視に利用するアカウント”を、root にしてください。
それ以外の一般ユーザーに設定すると、監視に失敗しステータスとして“失敗”を表示します。

A.「全般」タブ

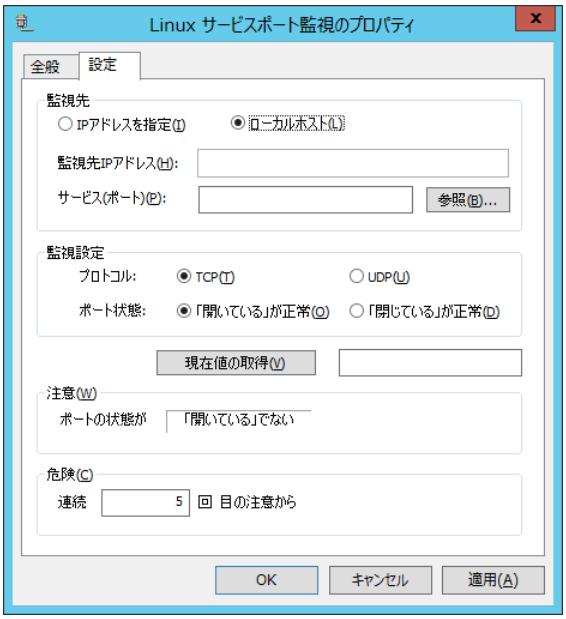
「全般」タブは、“アイコン”、“ID”、“名前”、“間隔”に設定されている値を除き、すべての監視項目で共通です。

Linux サービスポート監視では、監視間隔の既定値は 3 分に指定されています。

「全般」タブの詳細については‘4.2.1 各監視項目共通の設定’の項目‘B.「全般」タブ’をご参照ください。



B.「設定」タブ



1. 監視先

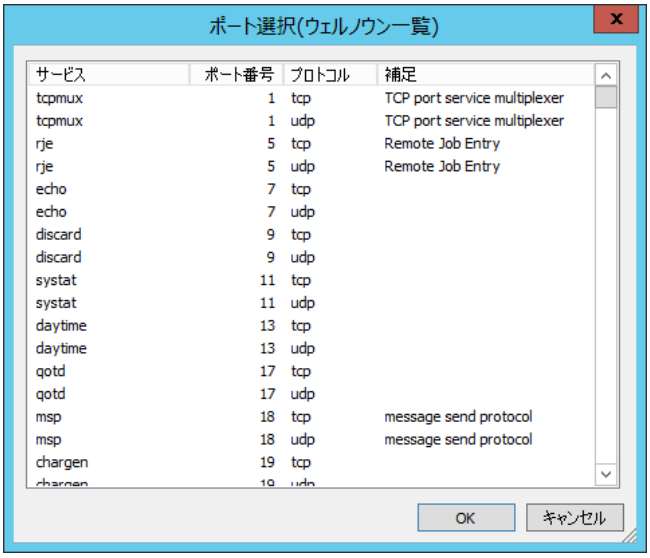
“IP アドレスを指定”“ローカルホスト”どちらかを選択します。既定では、“ローカルホスト”が選択されています。

“監視先 IP アドレス”は“IP アドレスを指定”を選択した場合のみ入力できます。

リモートポートが監視対象の場合、必須項目です。

“サービス(ポート)”ではサービス名または、ポート番号を設定します。必須項目です。

[参照]ボタンをクリックするとポート選択ダイアログを表示します。[参照]ボタンは指定した監視先 IP アドレスのポートを参照するのではなく、ローカルホストのポートを参照します。選択した結果はサービス(ポート)にセットされます。



※　Linux コンピューターの/etc/services に定義された一覧を表示しています。

※　ここに表示されたサービス名であれば、ポート番号の替わりに設定できます。

※　IPv6 アドレスの監視を行う場合は perl-socket6 パッケージが必須です

2. 監視設定

プロトコルでは、 “TCP” 、“UDP”どちらかを選択します。既定では“TCP”が選択されています。

ポート状態では、“「開いている」が正常”、“「閉じている」が正常”どちらかを選択します。既定では“「開いている」が正常”が選択されています。

※　UDP ポート監視時の注意点

UDP パケットを送信したのち、下記の判断を順次行いポートの状態を決定しております。

● ICMP 到達不能メッセージ(type-3)を受信した場合

ポート“閉”状態

● 受信タイムアウトした場合

Ping(echo request)を行い、Ping 応答(echo reply)があった場合、ポート“開”状態

Ping(echo request)を行い、Ping 応答(echo reply)がない(タイムアウト)の場合、ポート“閉”状態

3. 現在値の取得

[現在値の取得]ボタンをクリックした場合、指定した監視先のポートの“開”または“閉”を取得します。

4. しきい値

注意しきい値は“ポート状態”に反する場合（“「閉じている」が正常”の場合、“開”の状態がセットされます。規定値では“「閉じている」でない”になります。

危険しきい値は“注意状態の連続回数”を指定します。規定値では“連続「5」回目の注意から”になります。入力欄には1~99 までの整数を入力できます。

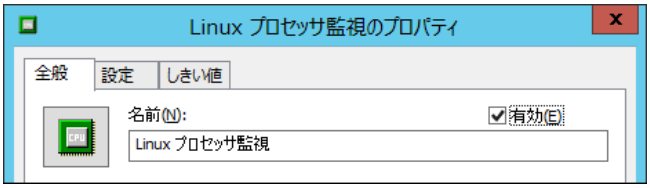
4.2.5 Linux プロセッサ監視

A.「全般」タブ

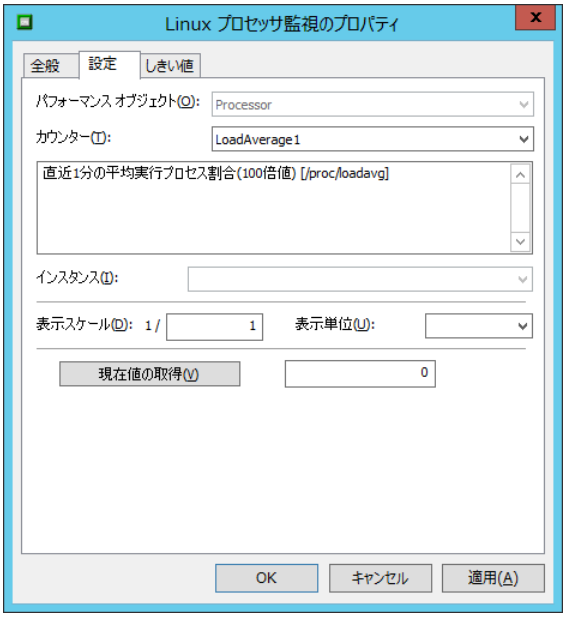
「全般」タブは、“アイコン”、“ID”、“名前”、“間隔”に設定されている値を除き、すべての監視項目で共通です。

Linux プロセッサ監視では、監視間隔の既定値は 10 分に指定されています。

「全般」タブの詳細については‘4.2.1 各監視項目共通の設定’の項目‘B.「全般」タブ’をご参照ください。



B.「設定」タブ



1. パフォーマンスオブジェクト

   パフォーマンスオブジェクトは“Processor”が固定値です。

2. カウンター

   プルダウンリストから1つを選択します。

   各カウンターについては説明文が表示されます。

3. インスタンス

   カウンターによってインスタンスの指定が必要な場合に指定します。

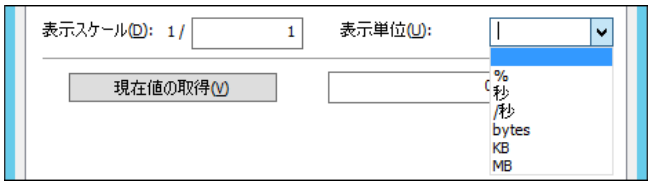
   必要のないカウンターについては、無効化されます。

4. 表示スケール

取得した値を単位変換(小さくする)場合に使用します。

表示単位で“KB”を指定した場合は 1024 に、“MB”を指定した場合は 1048576 が自動的に表示スケールに設定されます。入力欄には 1～999999999 の整数を入力できます。

表示単位は“(空欄)、%、秒、/秒、bytes、KB、MB”から選択します。



※ システムカウンターの詳細については、巻末の‘システムカウンター一覧’をご参照ください。

5. 現在値の取得

選択したカウンターの現在の値を取得してきます。

C.「しきい値」タブ

1. “前回からの増分を監視値とする”チェックボックス

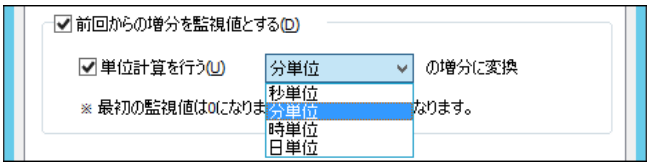
チェックボックスにチェックを入れると初回をのぞき、前回からの増分を監視値とします。

初回(監視サービス開始後 1 回目)の監視値と減少した場合の監視値は 0 となります。

“単位計算を行う”チェックボックスにチェックを入れると、前回からの増分を監視値とした場合、

“前回からの増分値/(秒、分、時、日)単位”を増分値とします。

チェックボックスからチェックを外した場合は、前回取得した値からの単純な増分値となります。

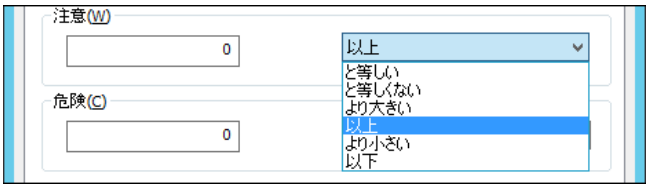


2. しきい値

しきい値では、“注意”および“危険”のしきい値条件を指定します。

既定では“注意”しきい値が 0 以上、“危険”しきい値が 0 以上に設定されています。

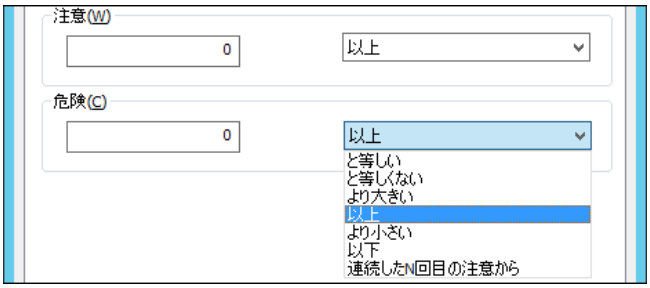
しきい値の設定範囲(上限下限)は 0～999999999 です。



また、“注意”しきい値の条件指定は、“と等しい”、“と等しくない”、“より大きい”、“以上”、“より小さい”、“以下”から選択できます。

“危険”しきい値は、“注意”しきい値と同様に設定できます。それに加え、条件指定では“注意”しきい値の条件を連続して満たすことを条件にする“連続した N 回目の注意から”を選択できます。

“連続した N 回目の注意から”を使用する場合には、入力欄には 1 から 99 までの整数を入力できます。



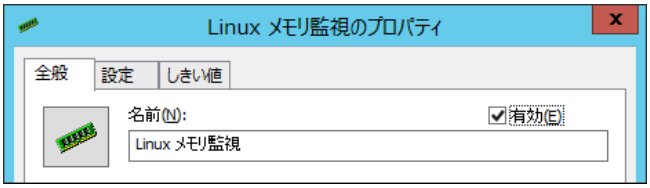
4.2.6 Linux メモリ監視

A.「全般」タブ

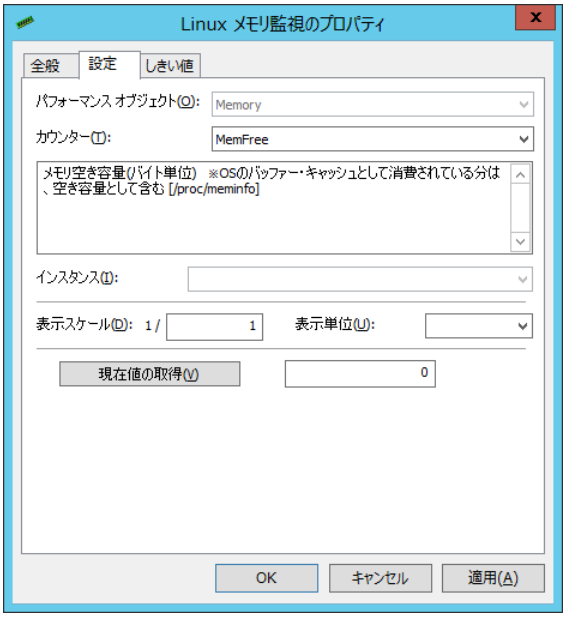
「全般」タブは、“アイコン”、“ID”、“名前”、“間隔”に設定されている値を除き、すべての監視項目で共通です。

Linux メモリ監視では、監視間隔の既定値は 3 分に指定されています。

「全般」タブの詳細については‘4.2.1 各監視項目共通の設定’の項目‘B.「全般」タブ’をご参照ください。



B.「設定」タブ



1. パフォーマンスオブジェクト

   パフォーマンスオブジェクトは“Memory”が固定値です。

2. カウンター

   プルダウンリストから1つを選択します。

   各カウンターについては説明文が表示されます。

3. インスタンス

   カウンターによってインスタンスの指定が必要な場合に指定します。

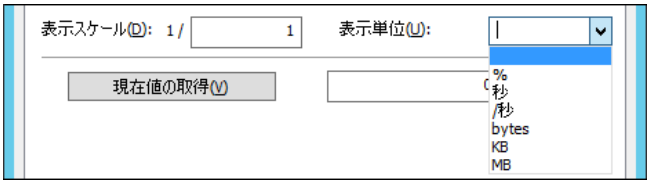
   必要のないカウンターについては、無効化されます。

4. 表示スケール

   取得した値を単位変換(小さくする)場合に使用します。

表示単位で“KB”を指定した場合は 1024 に、“MB”を指定した場合は 1048576 が自動的に表示スケールに設定されます。入力欄には 1～999999999 の整数を入力できます。

表示単位は“(空欄)、%、秒、/秒、bytes、KB、MB”から選択します。



※ システムカウンターの詳細については、巻末の‘システムカウンター一覧’をご参照ください。

※ Linux カーネル 2.6 の場合、カウンター“shared”は指定できません。指定すると監視結果が“失敗”になります。また、[現在値の取得]ボタンをクリックすると、エラーが発生します。

5. 現在値の取得

選択したカウンターの現在の値を取得してきます。

C.「しきい値」タブ

1. “前回からの増分を監視値とする”チェックボックス

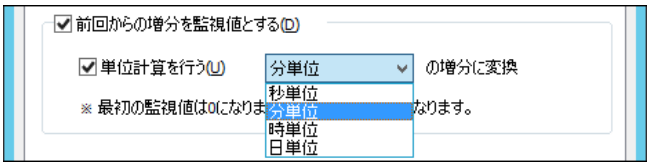
チェックボックスにチェックを入れると、初回を除き前回からの増分を監視値とします。

初回(監視サービス開始後 1 回目)の監視値と減少した場合の監視値は 0 となります。

“単位計算を行う”チェックボックスにチェックを入れると、前回からの増分を監視値とした場合、

“前回からの増分値/(秒、分、時、日)単位”を増分値とします。

チェックボックスからチェックを外した場合は、前回取得した値からの単純な増分値となります。

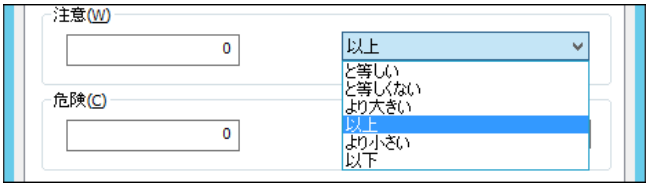


2. しきい値

しきい値では、“注意”および“危険”のしきい値条件を指定します。

既定では“注意”しきい値が 0 以上、“危険”しきい値が 0 以上に設定されています。

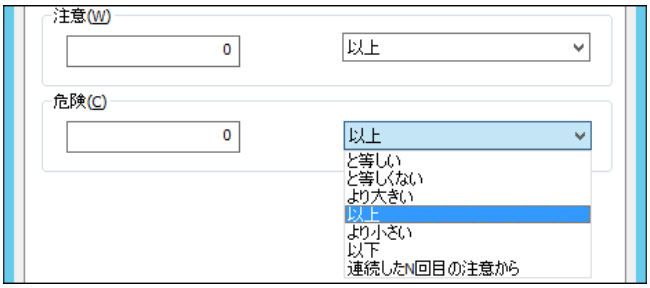
しきい値の設定範囲(上限下限)は 0～999999999 です。



また、“注意”しきい値の条件指定は、“と等しい”、“と等しくない”、“より大きい”、“以上”、“より小さい”、“以下”から選択できます。

“危険”しきい値は、“注意”しきい値と同様に設定できます。それに加え、条件指定では“注意”しきい値の条件を連続して満たすことを条件にする“連続した N 回目の注意から”を選択できます。

“連続した N 回目の注意から”を使用する場合には、入力欄には 1 から 99 までの整数を入力できます。



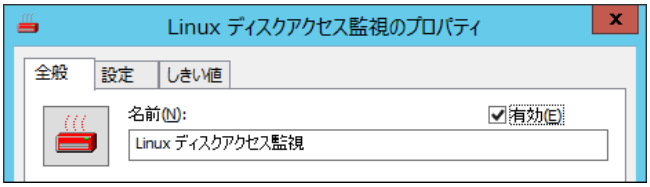
4.2.7 Linux ディスクアクセス監視

A.「全般」タブ

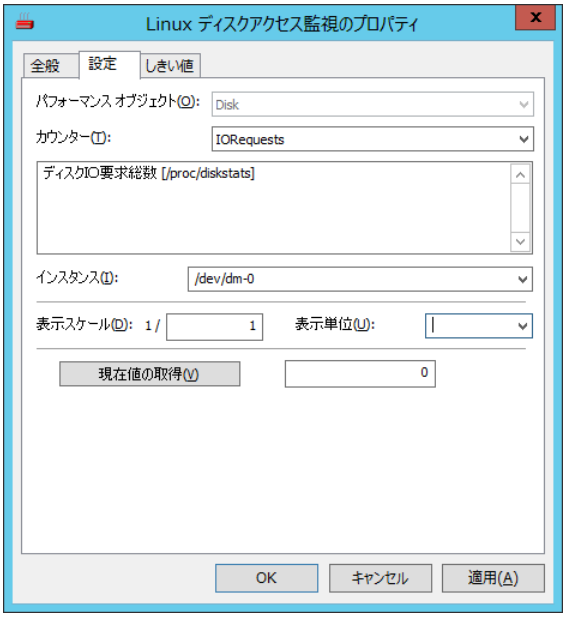
「全般」タブは、“アイコン”、“ID”、“名前”、“間隔”に設定されている値を除き、すべての監視項目で共通です。

Linux ディスクアクセス監視では、監視間隔の既定値は 3 分に指定されています。

「全般」タブの詳細については‘4.2.1 各監視項目共通の設定’の項目‘B.「全般」タブ’をご参照ください。



B.「設定」タブ



1. パフォーマンスオブジェクト

   パフォーマンスオブジェクトは“Disk”が固定値です。

2. カウンター

   プルダウンリストから1つを選択します。

   各カウンターについては説明文が表示されます。

3. インスタンス

   カウンターによってインスタンスの指定が必要な場合に指定します。

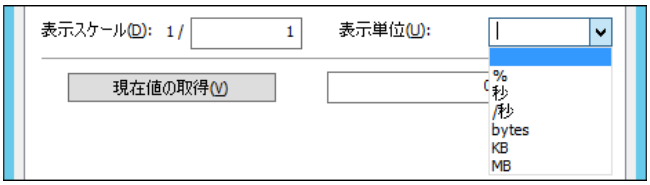
   必要のないカウンターについては、無効化されます。

4. 表示スケール

取得した値を単位変換(小さくする)場合に使用します。

表示単位で“KB”を指定した場合は 1024 に、“MB”を指定した場合は 1048576 が自動的に表示スケールに設定されます。入力は 1～999999999 の整数が可能です。

表示単位は“(空欄)、%、秒、/秒、bytes、KB、MB”から選択します。



※ システムカウンターの詳細については、巻末の‘システムカウンター一覧’をご参照ください。

5. 現在値の取得

選択したカウンターの現在の値を取得してきます。

C.「しきい値」タブ

1. “前回からの増分を監視値とする”チェックボックス

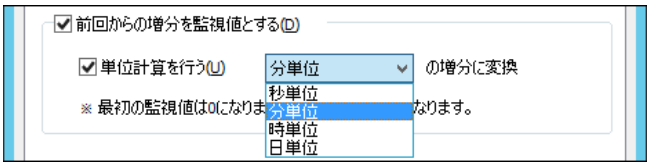
チェックボックスにチェックを入れると、初回をのぞき前回からの増分を監視値とします。

初回(監視サービス開始後 1 回目)の監視値と減少した場合の監視値は 0 となります。

“単位計算を行う”チェックボックスにチェックを入れると、前回からの増分を監視値とした場合、

“前回からの増分値/(秒、分、時、日)単位”を増分値とします。

チェックボックスからチェックを外した場合は、前回取得した値からの単純な増分値となります。

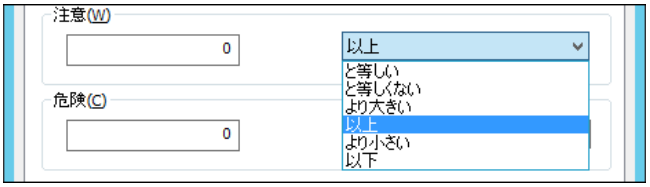


2. しきい値

しきい値では、“注意”および“危険”のしきい値条件を指定します。

既定では“注意”しきい値が 0 以上、“危険”しきい値が 0 以上に設定されています。

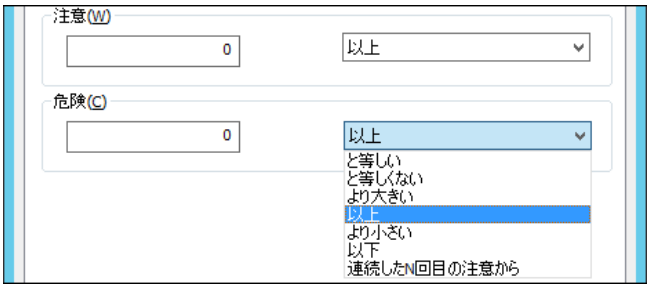
しきい値の設定範囲(上限下限)は 0～999999999 です。



また、“注意”しきい値の条件指定は、“と等しい”、“と等しくない”、“より大きい”、“以上”、“より小さい”、“以下”から選択できます。

“危険”しきい値は、“注意”しきい値と同様に設定できます。それに加え、条件指定では“注意”しきい値の条件を連続して満たすことを条件にする“連続した N 回目の注意から”を選択できます。

“連続した N 回目の注意から”を使用する場合には、入力欄には 1 から 99 までの整数を入力できます。



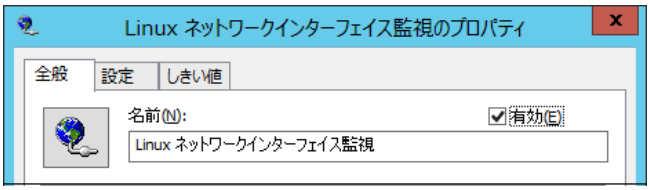
4.2.8 Linux ネットワークインターフェイス監視

A.「全般」タブ

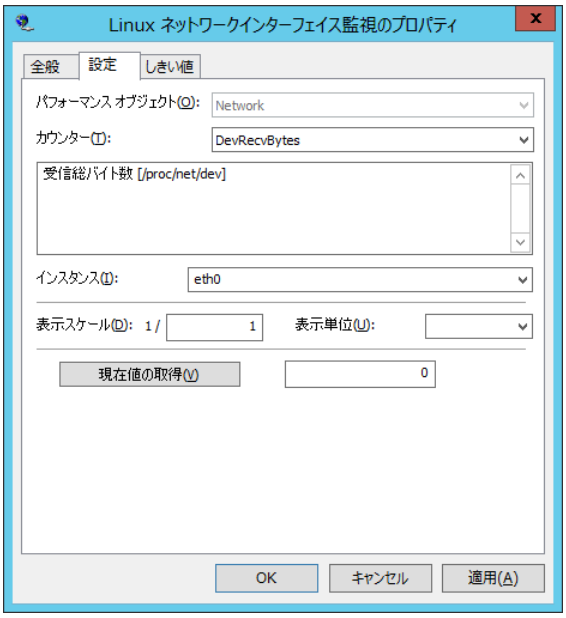
「全般」タブは、“アイコン”、“ID”、“名前”、“間隔”に設定されている値を除き、すべての監視項目で共通です。

Linux ネットワークインターフェイス監視では、監視間隔の既定値は 3 分に指定されています。

「全般」タブの詳細については‘4.2.1 各監視項目共通の設定’の項目‘B.「全般」タブ’をご参照ください。



B.「設定」タブ



1. パフォーマンスオブジェクト

   パフォーマンスオブジェクトは“Network”が固定値です。

2. カウンター

   プルダウンリストから1つを選択します。

   各カウンターについては説明文が表示されます。

3. インスタンス

   カウンターによってインスタンスの指定が必要な場合に指定します。

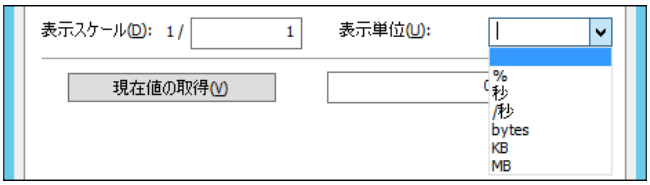
   必要のないカウンターについては、無効化されます。

4. 表示スケール

取得した値を単位変換(小さくする)場合に使用します。

表示単位で“KB”を指定した場合は 1024 に、“MB”を指定した場合は 1048576 が自動的に表示スケールに設定されます。入力は 0～999999999 の整数が可能です。

表示単位は“(空欄)、%、秒、/秒、bytes、KB、MB”から選択します。



※ システムカウンターの詳細については、巻末の‘システムカウンター一覧’をご参照ください

※ 注意事項

Linux オプションにおいて、Linux ネットワークインターフェイス監視のカウンター“TCPMaxConn”監視した場合、以下のエラーが発生します。

【現在値取得】

分類:ヘルパー

ソース:MxLinuxMon.CoLinuxEnumPerfInfo.1

種類:エラー

エラーコード:-2147023269

説明:

[6308] ネットワーク情報の取得に失敗しました。 (Perivale)

【監視】

監視 'TCPMaxConn' はコード 0x8007065B で失敗しました。

ID: GRPxxMONxx

オブジェクト名: ¥Network¥TCPMaxConn

値名: Value

オプション引数:

実行時間: yyyy/mm/dd hh:mm:ss +0900

メッセージ: 関数は実行中に失敗しました。

ソース: MxLinuxMon.CoLinuxPerfMonitor.1

説明:

[6308] ネットワーク情報の取得に失敗しました。 (PerfMonitor)

【原因】

監視対象のファイル(/proc/net/snmp)のカウンター(MaxConn)はデフォルト値が"-1"となっています。

BOM は負の値を監視できないため、本エラーが発生してしまいます。

これは Linux の仕様である為、正常に監視を行う事が出来ません。

5. 現在値の取得

選択したカウンターの現在の値を取得してきます。

C.「しきい値」タブ

1. “前回からの増分を監視値とする”チェックボックス

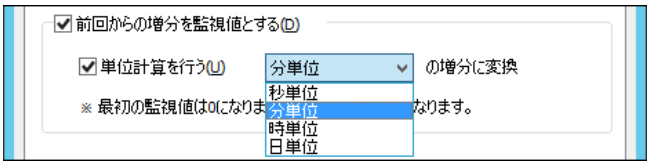
チェックボックスを有効にすると初回をのぞき、前回からの増分を監視値とします。

初回(監視サービス開始後 1 回目)の監視値と減少した場合の監視値は 0 となります。

“単位計算を行う”チェックボックスを有効にすると、前回からの増分を監視値とした場合、

“前回からの増分値/(秒、分、時、日)単位”を増分値とします。

指定しない場合は、前回取得した値からの単純な増分値となります。

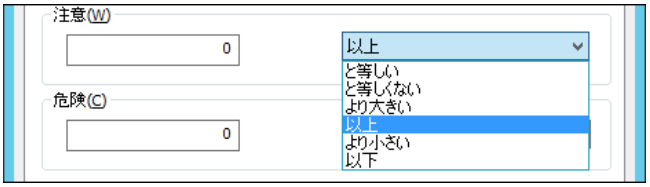


2. しきい値

しきい値では、“注意”および“危険”のしきい値条件を指定します。

既定では“注意”しきい値が 0　以上、“危険”しきい値が 0　以上に設定されています。

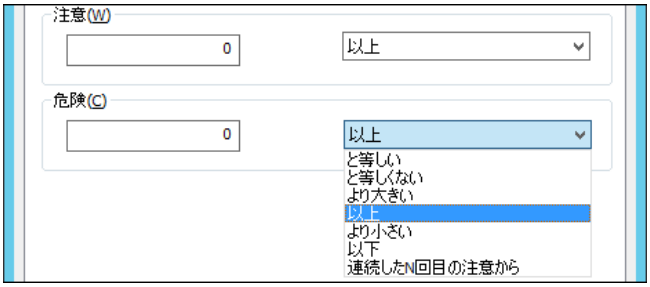
しきい値の設定範囲(上限下限)は 0～999999999 です。



また、“注意”しきい値の条件指定は、“と等しい”、“と等しくない”、“より大きい”、“以上”、“より小さい”、“以下”から選択できます。

“危険”しきい値は、“注意”しきい値と同様に設定できます。それに加え、条件指定では“注意”しきい値の条件を連続して満たすことを条件にする“連続した N 回目の注意から”を選択できます。

“連続した N 回目の注意から”を使用する場合には、入力欄には 1 から 99 までの整数を入力できます。



4.2.9 Linux プロセス監視

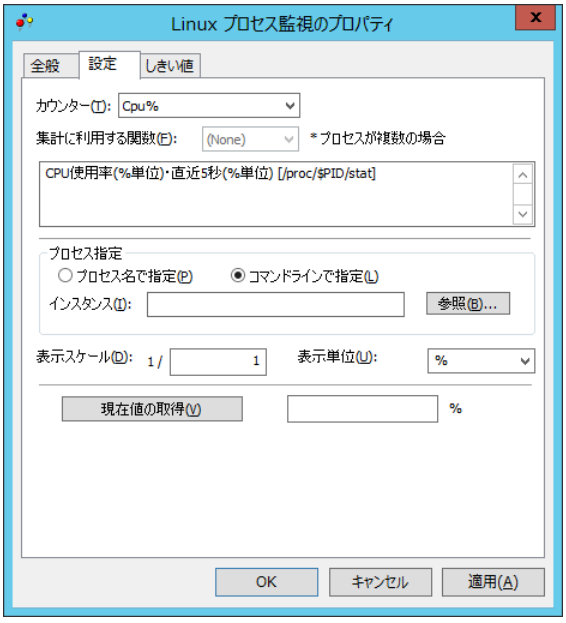
A.「全般」タブ

「全般」タブは、“アイコン”、“ID”、“名前”、“間隔”に設定されている値を除き、すべての監視項目で共通です。

Linux プロセス監視では、監視間隔の既定値は 10 分に指定されています。

「全般」タブの詳細については‘4.2.1 各監視項目共通の設定’の項目‘B.「全般」タブ’をご参照ください。

B.「設定」タブ



1. カウンター

   プロセスのパフォーマンスオブジェクトとしてリストで表示されたものから1つ選択します。

2. 集計に利用する関数

   “(None)”、“Sum”、“Min”、“Max”、“Avg”より選択します。規定値は“(None)”です。

   カウンターによって適合するプロセスが複数となる場合に適用されます。

   該当するプロセスが複数にならないカウンターについては、無効化されます。

集計関数は以下の 4 つです。

Sum	値の合計
Min	値の最小値
Max	値の最大値
Avg	値の平均

RunningProcesses などすべてのプロセスの合計値を取得するタイプのカウンターには使用できません。

結果が%となるカウンターは Sum のみ使用可能です。Memory%の場合、同名のプロセスすべてを合計した Memory の使用割合を返します。Cpu%の場合、同名のプロセスすべてを合計した直近 5 秒間の CPU 使用割合を返します。

3. プロセス指定

“プロセス名で指定”はプロセスをプロセス名で指定し、文字列完全一致で適合したプロセスが監視対象になります。

“コマンドラインで指定”は本設定の既定値となっており、プロセスコマンドラインによってプロセスを指定します。こちらも文字列完全一致で適合したプロセスが監視対象になります。

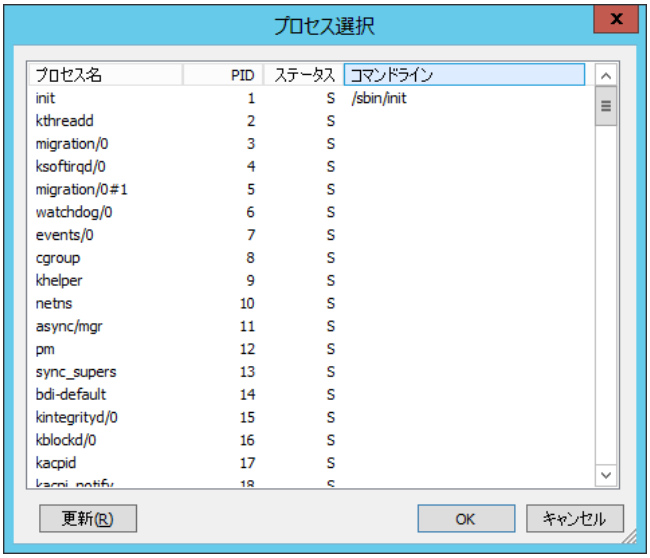
※ 「*」(アスタリスク)も文字として認識します。

“インスタンス”はプロセス指定が有効な場合、“プロセス名で指定”か“コマンドラインで指定”かのどちらかで、プロセスを指定する必要があります。

※ 260 文字まで入力できます

4. 参照

プロセス選択ダイアログを表示します。



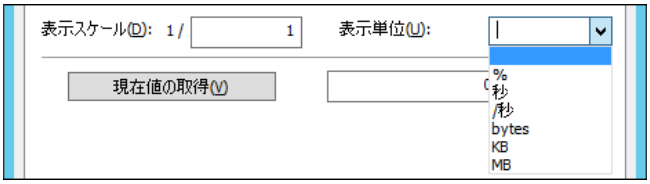
Linux のプロセス一覧コマンド(ps)の実行の結果を出力します。選択すると、プロセス名またはコマンドラインの内容がインスタンスに設定されます。

5. 表示スケール

取得した値を単位変換(小さくする)場合に使用します。

表示単位で“KB”を指定した場合は 1024 に、“MB”を指定した場合は 1048576 が自動的に表示スケールに設定されます。入力は 1～999999999 の整数が可能です。

表示単位は“(空欄)、%、秒、/秒、bytes、KB、MB”から選択します。



※システムカウンターの詳細については、巻末の「システムカウンター一覧」をご参照ください

※Linux スレッドはプロセスと同様の扱いになります

※プロセス関連で取得する一覧や値は、/proc より取得しています

※プロセス監視の場合、インスタンスに、BomMonitor.monitorlet というプロセスが現れますが、これは BOM マネージャーで何らかの処理（実行確認など）がある間だけ存在します。それ以外の時には存在しないプロセスであるため、監視を行ってもほとんどの場合“失敗”となります

6. 現在値の取得

選択したカウンターの現在の値を取得してきます。

C.「しきい値」タブ

1. “前回からの増分を監視値とする”チェックボックス

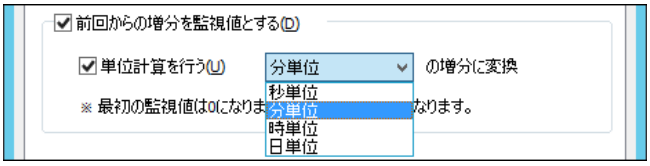
チェックボックスを有効にすると初回をのぞき、前回からの増分を監視値とします。

初回(監視サービス開始後 1 回目)の監視値と減少した場合の監視値は 0 となります。

“単位計算を行う”チェックボックスを有効にすると、前回からの増分を監視値とした場合、

“前回からの増分値/（秒、分、時、日）単位”を増分値とします。

指定しない場合は、前回取得した値からの単純な増分値となります。

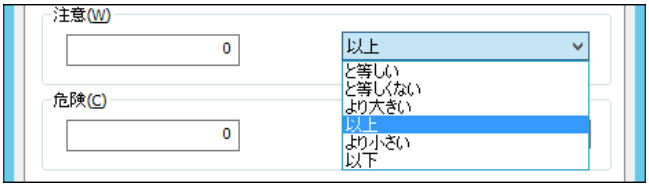


2. しきい値

しきい値では、“注意”および“危険”のしきい値条件を指定します。

既定では“注意”しきい値が 0%　以上、“危険”しきい値が 0%　以上に設定されています。

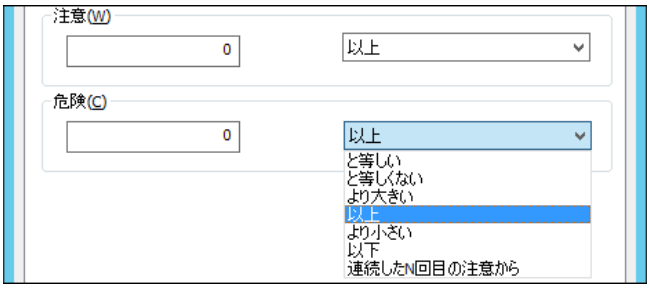
しきい値の設定範囲（上限下限）は 0～999999999 です。



また、“注意”しきい値の条件指定は、“と等しい”、“と等しくない”、“より大きい”、“以上”、“より小さい”、“以下”から選択できます。

“危険”しきい値は、“注意”しきい値と同様に設定できます。それに加え、条件指定では“注意”しきい値の条件を連続して満たすことを条件にする“連続した N 回目の注意から”を選択できます。

“連続した N 回目の注意から”を使用する場合には、入力欄には 1 から 99 までの整数を入力できます。



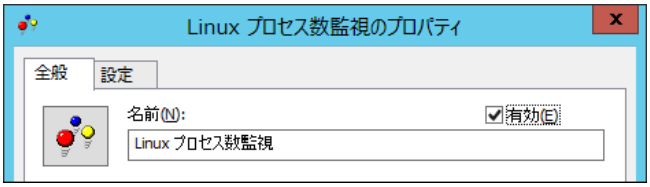
4 .2 .10 Linux プロセス数監視

A.「全般」タブ

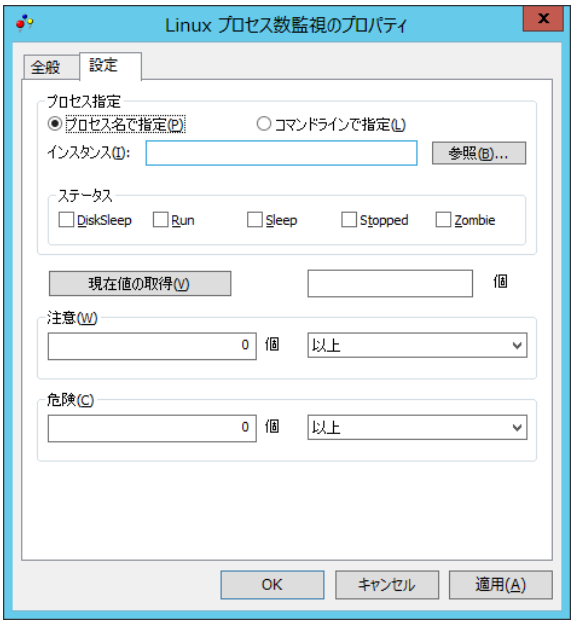
「全般」タブは、“アイコン”、“ID”、“名前”、“間隔”に設定されている値を除き、すべての監視項目で共通です。

Linux プロセス数監視では、監視間隔の既定値は 3 分に指定されています。

「全般」タブの詳細については‘4 .2 .1 各監視項目共通の設定’の項目‘B.「全般」タブ’をご参照ください。



B.「設定」タブ



1. プロセス指定

“プロセス名で指定”はプロセスをプロセス名で指定します。前方一致で適合したプロセスが監視対象になります。

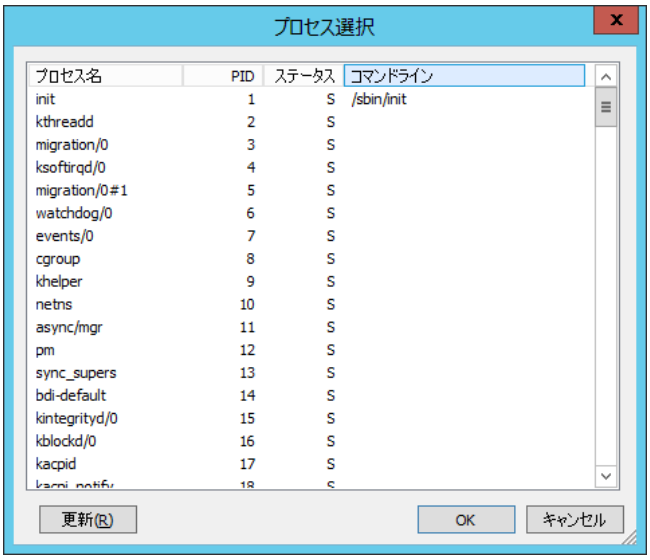
“コマンドラインで指定”はプロセスコマンドラインによってプロセスを指定します。規定値はこの設定になります。前方一致で適合したプロセスが監視対象になります。

“インスタンス”はプロセス指定が有効な場合、“プロセス名で指定”か“コマンドラインで指定”かのどちらかで、プロセスを指定する必要があります。

※ 260 文字まで入力できます

2. 参照

プロセス選択ダイアログを表示します。



Linux のプロセス一覧コマンド(ps)の実行の結果を出力します。選択すると、プロセス名またはコマンドラインの内容がインスタンスに設定されます。

3. ステータス

“DiskSleep”、 “Run”、“Sleep”、“Stopped”、“Zombie”のうち、監視対象とするステータスをチェックします。

（複数選択可）

※ 選択したインスタンスのステータスが自動的にチェックされます

※ 指定なしの場合は全てのステータスが対象となります

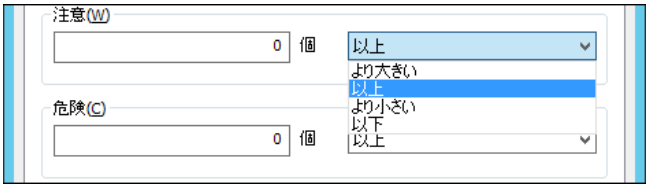
DiskSleep	割り込み不可能なスリープ状態 (通常 IO 中)
Run	実行可能状態 (実行キューにある)
Sleep	スリープ状態
Stopped	トレース中または停止中
Zombie	消滅した (ゾンビ) プロセス

4. しきい値

しきい値では、“注意”および“危険”のしきい値条件を指定します。

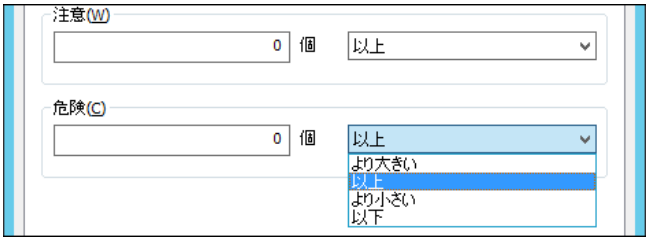
既定では“注意”しきい値が 0 個以上、“危険”しきい値が 0 個以上に設定されています。

しきい値の設定範囲（上限下限）は 0～999999999 です。



また、“注意”しきい値の条件指定は、“より大きい”、“以上”、“より小さい”、“以下”から選択できます。

“危険”しきい値は、“注意”しきい値と同様に設定できます。



4.2.11 Linux テキストログ監視

テキストログの出力内容を監視します。

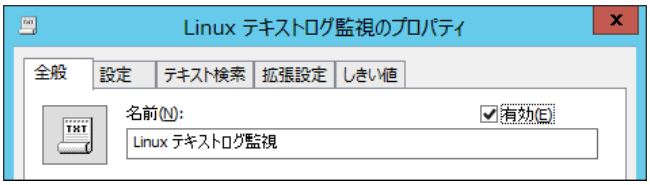
- 前回監視から増えた行を対象として、文字列を検索し行数をカウントします。(前回監視の際の位置を記憶しています)
- バイナリ形式のログファイルは監視できません
- 監視対象のログファイルを 1 行毎に読み込みますが、1 行の上限は 10KB(10,000Bytes)です。10KB を超えると次行頭まで以降の内容を無視し検索対象としません
- 特定コード 0x0D/0x0A(改行)、0x09(TAB)はテキストとみなします
- 特定コード 0x00(NULL)、0x1A(EOF)の場合は当該文字の前の文字までを検索対象とします。ただし、先頭にこれらの特定コードがあった場合には無視されます
- 上記以外の ASCII 制御コードの場合、当該文字の次の文字以降～行末までを検索対象とします

A.「全般」タブ

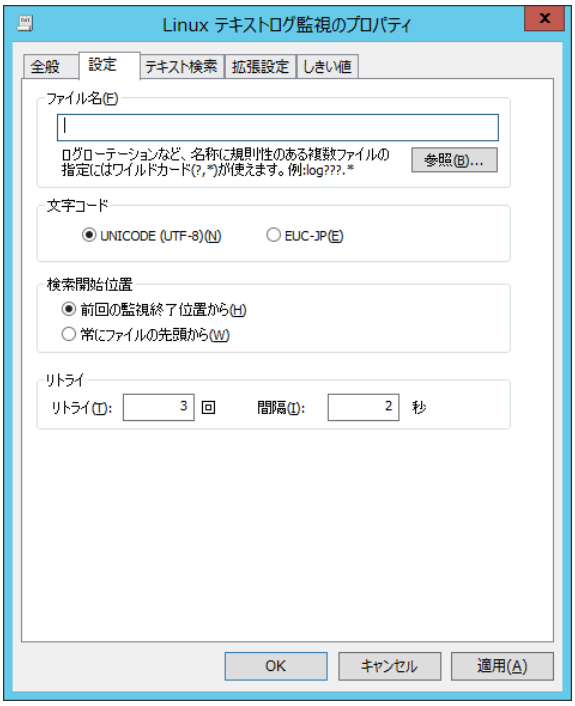
「全般」タブは、“アイコン”、“ID”、“名前”、“間隔”に設定されている値を除き、すべての監視項目で共通です。

Linux テキストログ監視では、監視間隔の既定値は 5 分に指定されています。

「全般」タブの詳細については ‘4.2.1 各監視項目共通の設定’ の項目 ‘B.「全般」タブ’ をご参照ください。



B.「設定」タブ



1. ファイル名

   必須項目です。監視対象のテキストファイルをフルパスで指定します。以下のワイルドカードによる複数ファイルの指定が可能です。260 文字まで設定できます。

   ※*:0 文字以上の文字列。ただし最初の一文字は.(ドット)を除く

   ※?: 任意の 1 文字。ただし最初の一文字は.(ドット)を除く

   【ワイルドカードを使用する際のご注意】

   Linux テキストログ監視を実行した際、BOM 7.0 は監視の終端位置（次回監視の開始位置）を、テキストログに記録された文字列末尾の情報を基に生成した値で保持します。そのため、ワイルドカードで指定された対象のファイルが監視実行時点で 0 バイト（1 文字も記録されていないファイル）だった場合、正しい終端位置が保持されず、次回の監視実行の際にすでに監視済みの過去のログファイルが監視対象となって誤検知が発生する場合があります。

   ワイルドカードに合致するファイルが複数存在し、なおかつ 0 バイトのファイルが監視対象となる可能性がある環境では、「Linux テキストログ監視」にワイルドカードを使用することはできません。

2. 文字コード

   テキストログの文字コードを指定します。デフォルトは UNICODE です。

3. 検索開始位置

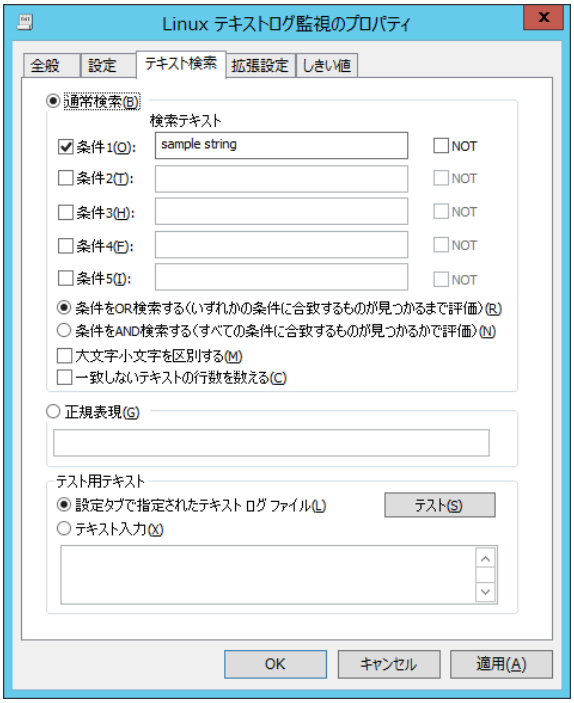
   検索開始位置の指定を行います。デフォルトは、“前回の監視終了位置から”です。

4. リトライ

   テキストログ監視中にデータの変更を検出した場合のリトライと時間間隔を指定します。

   デフォルトは、リトライ 3 回、間隔 2 秒です。リトライは 1～9 の整数値、間隔は 1～30 の整数値が設定できます。

C.「テキスト検索」タブ



“通常検索”か“正規表現”いずれかを指定します。規定値は“通常検索”です。

1. 通常検索

   “検索テキスト” 検索文字列を指定します。部分一致で適合した 1 行単位のテキストが監視対象になります。1024 文字まで検索文字列を設定できます。

   “条件 1～5” 条件 1～5 に複数の文字列を指定できます。条件毎に“NOT”を選択すると除外指定ができます。

   “条件を OR 検索する” 条件 1～5 の条件のうちどれかが合致する行を検索します。デフォルト設定は OR 検索するになっています。

   “条件を AND 検索する” 条件 1～5 がすべて適合した行を検索します。

   “大文字小文字を区別する” チェックの場合、半角英文字の大小を区別します。

   “一致しないテキストの行数を数える” 結果を反転させます。

2. 正規表現

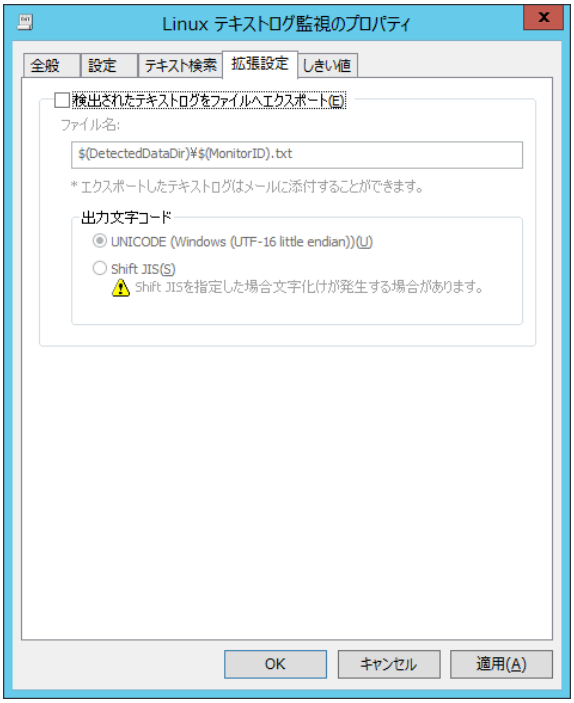
   Perl5 形式の正規表現を指定します。

   ※入力制限：1024 文字以下です。

3. テスト

   テキストログファイルもしくは指定テキストでの検索テストを実行します。入力制限は 2000 文字です。

D.「拡張設定」タブ



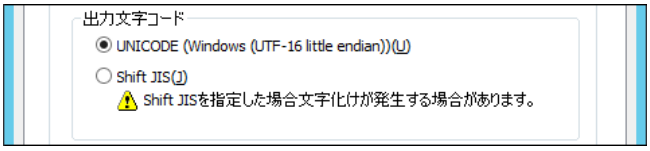
1. 検出ログをファイルへエクスポート

   チェックをすると既定のテキストファイルに検出行を出力します。1 行以上検出のたびに上書き出力されます。

2. 出力する際の文字コードを指定できます。

   UNICODE

   Shift JIS



※Shift JIS を選択した場合、文字化けが発生する場合があります

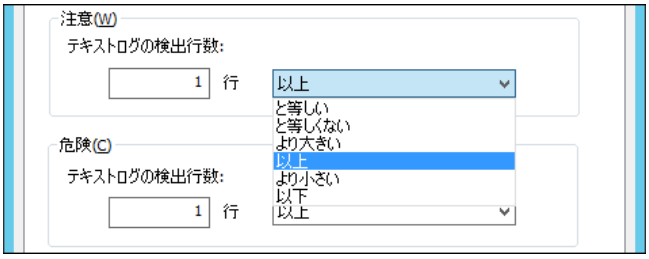
E.「しきい値」タブ

1. しきい値

   しきい値では、“注意”および“危険”のしきい値条件を指定します。

   既定では“注意”しきい値が 1 行以上、“危険”しきい値が 1 行以上に設定されています。

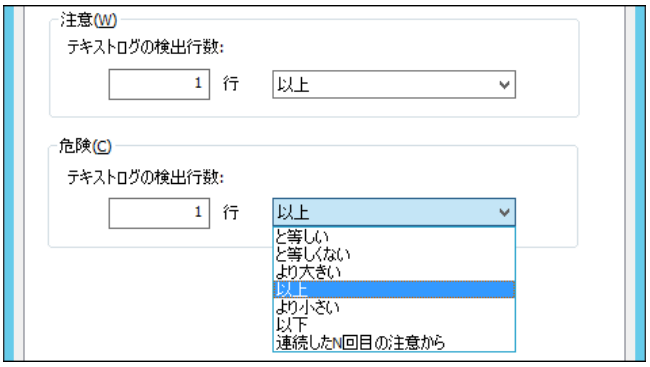
   しきい値の設定範囲（上限下限）は 0～99999 です。



また、“注意”しきい値の条件指定は、“と等しい”、“と等しくない”、“より大きい”、“以上”、“より小さい”、“以下”から選択できます。

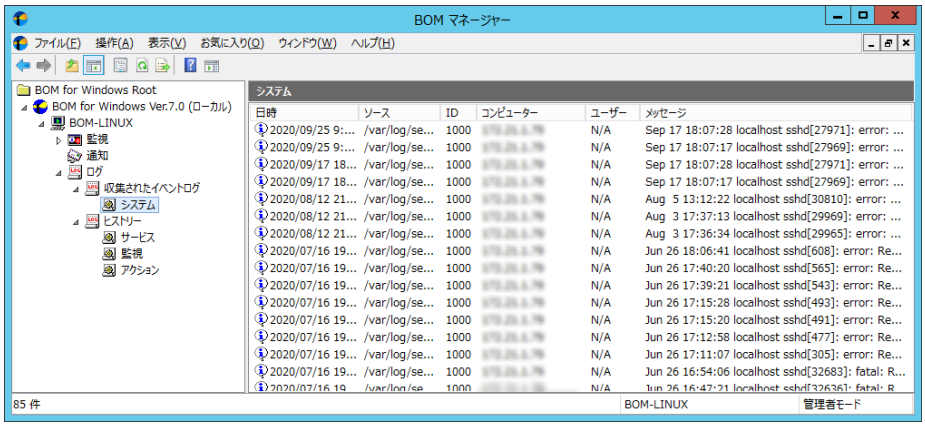
“危険”しきい値は、“注意”しきい値と同様に設定できます。それに加え、条件指定では“注意”しきい値の条件を連続して満たすことを条件にする“連続した N 回目の注意から”を選択できます。

“連続した N 回目の注意から”を使用する場合には、入力欄には 1 から 99 までの整数を入力できます。



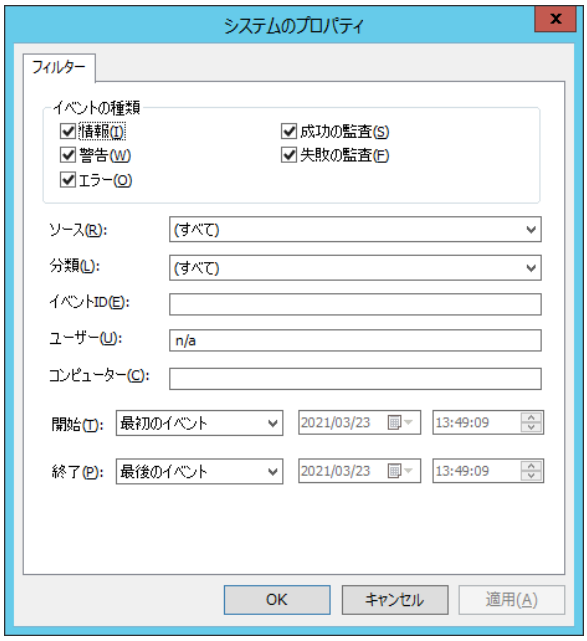
F. ログノード

Linux テキストログ監視の結果、該当するログ内容は“ログ”ノードの“収集されたイベントログ”下の“システム”に保存されます。



● ログのフィルタリング

収集されたログは、フィルタリングして表示することも可能です。“ログ”ノードの“収集されたイベントログ”下の“システム”で右クリックし、コンテキストメニューの“プロパティ”をクリックしてください。



1. イベントの種類、分類、イベント ID、ユーザー、コンピューター

   Linux テキストログ監視の場合、フィルタリング条件には使用できません。

   イベントの種類は“情報”、分類は“なし”、イベント ID は“1000”、ユーザーは“N/A”、コンピューターは対象の IP アドレスまたはコンピューター名が固定値となります。

2. ソース

   対象のログファイルを選択します。

3. 開始・終了

   ログの収集日時をしているすることで、ログを絞り込めます。

● ログのプロパティ表示

ログの詳細情報は、各項目のプロパティを見ることで参照できます。

プロパティの表示は、リザルトペインで対象のログを右クリックし、コンテキストメニューで“プロパティ”を選択してください。

※　イベントの種類は“情報”、分類は“なし”、イベント ID は“1000”、ユーザーは“N/A”、コンピューターは対象の IP アドレスまたはコンピューター名が固定値となります。

● テキストログ監視で収集されたログのローテーション

テキストログ監視で収集されたログは、10000 件まで各テキストログ監視で収集されたログに保存されるよう設定されています。10000 件を超えると古いものから消え、新しいものに上書きされます。

※　“イベントログ監視で収集されたログ”ノードをクリックした場合、リザルトペインに表示される件数は、最大で最新の 1000 件分となります。すべてのログを表示する場合は“ログ”ノードの“収集されたイベントログ”下の“システム”で右クリックし、コンテキストメニューで“すべてのレコードを表示”を選択してください。

テキストログ監視で収集されたログの最大件数の変更

テキストログ監視で収集されたログではデフォルト 10000 件までのログを保存できますが、以下の ini ファイルを書き換えることで最大件数を変更できます。

<BOM のインストールディレクトリ>¥BOMW7¥Environment¥Config¥BomLnxTxtlogMon.ini

[LOG_ROTATION_SETTINGS]

DEFAULT=10000

BOM_LOG_System=10000

上記の DEFAULT の数字を変更します。ただし、既に該当のログが保存されている状態で ini ファイルを書き換える場合は、一度収集されたイベントログをクリアしなければ、その後の監視結果が全て N/A となり、テキストログも収集されません。必ず、以下のログの削除を行ってから ini ファイルを変更してください。

テキストログ監視で収集されたログの削除

テキストログ監視で収集されたログの削除を行う場合、“ログ”ノードの“収集されたイベントログ”で右クリックし、コンテキストメニューで“ログのクリア”を選択します。

4.2.12 Linux スクリプト監視

任意のスクリプトを動作させた結果の値を監視します。

※　ユーザー作成されるスクリプトの仕様は以下の条件を満たす必要があります。

● スクリプトの返却値(監視値)は標準出力してください。

数値を返却する場合

監視値:0 以上の整数

※　上記出力後、改行させてください。例) print “1001¥n”;

文字列を返却することはできません。

● 時間のかかる処理は行わないでください。(スクリプトの処理中、監視サービスは処理が終了するのを待ちます。10 分以内で処理が完了しないとタイムアウトになります)

● 返却値以外の出力はエラーメッセージも含め出さないようにしてください。

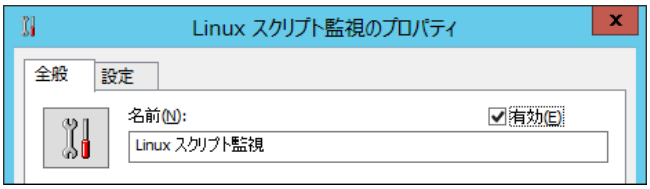
※　スクリプトの内容によっては正しく実行できない場合があります。スクリプトの内容および作成方法に関しては製品サポート対象外です。

A.「全般」タブ

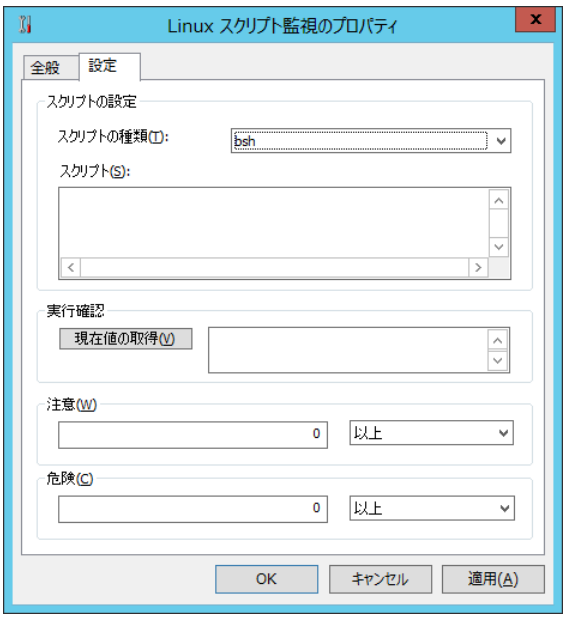
「全般」タブは、“アイコン”、“ID”、“名前”、“間隔”に設定されている値を除き、すべての監視項目で共通です。

Linux スクリプト監視では、監視間隔の既定値は 3 分に指定されています。

「全般」タブの詳細については ‘4.2.1 各監視項目共通の設定’ の項目 ‘B.「全般」タブ’ をご参照ください。



B.「設定」タブ



1. スクリプトの種類

“bsh”、 “csh”、“bash”、“perl”よりいずれかを指定します。規定値は bsh が選択されています。

2. スクリプト

スクリプト種別に対応するスクリプトを記述します。入力文字数は 2000 文字までです。

スクリプトの実行結果は、数値でリターンします。1 行目に数値と改行の出力を実行します。

(perl の場合の例)

print “12345¥n”;

→12345 として値を取得。

※1 行目に数値をリターンしない場合、戻り値は 0 となります。

スクリプト実行は以下のコマンドライン処理を行った場合と等価です。

1.ヒアドキュメントスクリプト読み込み

/bin/sh<<'EOT'または

/bin/csh<<'EOT'または

/bin/bash<<'EOT'または

perl<<'EOT'

2.スクリプトの送信

3.EOT 送信

4.実行結果取得

3. 現在値の取得

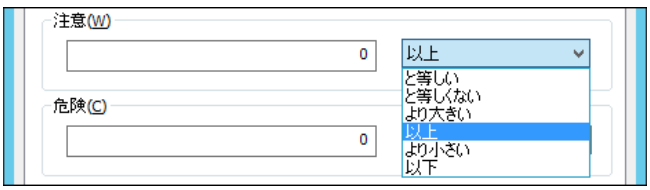
スクリプトの実行結果を表示します。

4. しきい値

しきい値では、“注意”および“危険”のしきい値条件を指定します。

既定では“注意”しきい値が 0 以上、“危険”しきい値が 0 以上に設定されています。

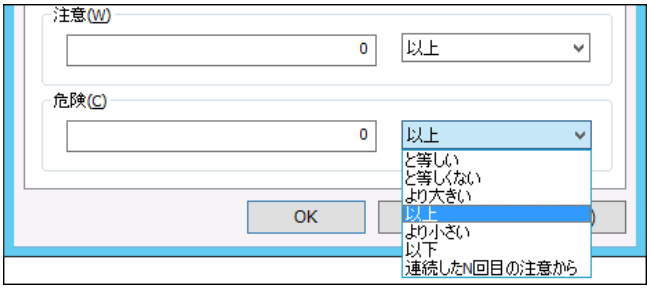
しきい値の設定範囲（上限下限）は 0～999999999 です。



また、“注意”しきい値の条件指定は、“と等しい”、“と等しくない”、“より大きい”、“以上”、“より小さい”、“以下”から選択できます。

“危険”しきい値は、“注意”しきい値と同様に設定できます。それに加え、条件指定では“注意”しきい値の条件を連続して満たすことを条件にする“連続した N 回目の注意から”を選択できます。

“連続した N 回目の注意から”を使用する場合には、入力欄には 1 から 99 までの整数を入力できます。



4.2.13 BOM ヒストリー監視

Linux インスタンス上でも Windows インスタンスと同様に、BOM が出力するヒストリーログの監視が可能です。

設定方法の詳細につきましては、‘BOM for Windows Ver.7.0 ユーザーズ マニュアル’の‘ 5.10.15 BOM ヒストリー監視’をご参照ください。

4.3 アクション項目の種類

Linux 監視インスタンスにて使用できるアクション項目について、使用方法を解説いたします。

Linux 監視インスタンスにて使用できるアクション項目は以下の 9 種類です。

アイコン	アクション項目名	説明
	監視有効/無効	監視グループ/監視項目の有効化/無効化制御
	メール送信	SMTP 形式のメール通知
	SNMP トラップ送信	SNMP（v1/v2c/v3）形式のトラップ送信による通知
	イベントログ書き込み	Windows イベントログへの書き込みによる通知
	syslog 送信	syslog サーバーへ監視結果を送信
	AWS S3 ファイル送信アクション	Amazon S3 および、Amazon S3 互換ストレージ（※）へ、任意のファイルを送信
	カスタムアクション	外部アプリケーションを利用した制御/通知
	Linux SYSLOG 書き込み	Linux の SYSLOG に BOM イベント情報を書き込みます
	Linux プロセスコントロール	Linux のプロセスをコントロールします
	Linux シャットダウン	Linux を再起動・シャットダウンします
	Linux スクリプト実行	Linux 上でスクリプトを実行します

※ Amazon S3 互換ストレージについて、API 準拠をうたう全てのストレージでの動作を保証するものではありません。
弊社では、クラウディアン株式会社の CLOUDIAN HYPERSTORE について動作確認を取っており、今後の対応確認情報は弊社ウェブサイト（www.say-tech.co.jp）で随時公開いたします。

アクション項目“Linux SYSLOG 書き込み”“Linux プロセスコントロール”“Linux シャットダウン”“ Linux スクリプト実行”以外は、BOM 7.0 の標準アクションです。
そのため、以降は“Linux SYSLOG 書き込み”“Linux プロセスコントロール”“Linux シャットダウン”“ Linux スクリプト実行”の使用方法と設定方法についてのみご案内いたします。
BOM 7.0 の標準アクション項目については、‘BOM for Windows Ver.7.0 ユーザーズ マニュアル’をご参照ください。

4.3.1 Linux アクション項目の共通部分

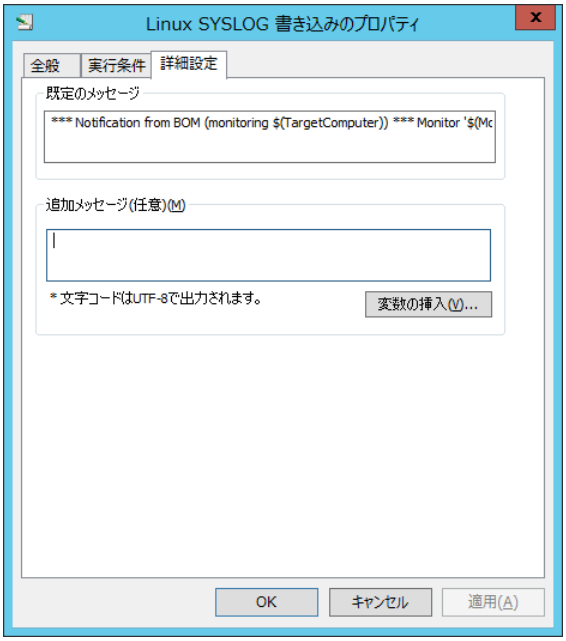
Linux オプションで設定するアクション項目設定の、「全般」タブ「実行条件」タブの画面は、BOM 標準アクション項目共通ですが、デフォルト値がアクション項目によって違います。
「全般」タブ、「実行条件」タブの詳細については ‘BOM for Windows Ver.7.0 ユーザーズ マニュアル’ を参照下さい。

4.3.2 Linux SYSLOG 書き込み

Linux コンピューターの SYSLOG(/var/log/messages)に BOM イベント情報を書き込みます。

※ 実行条件タブは“監視するステータス”が“注意”、“危険”、“失敗”に、“実行頻度”は“毎回”がデフォルト時チェックされています。

A. 詳細設定タブ



1. 既定のメッセージ

   1 行の以下のメッセージが SYSLOG に書き込まれます。メッセージは変更できません。

*** Notification from BOM (monitoring $(TargetComputer)) *** Monitor '$(MonitorID)' has detected a status $(StatusCode) (0:Normal1:Warning2:Critical4:Failure). SendTime: $(CurrentTime) InstanceID: $(InstanceID) MonitorID: $(MonitorID) RunTime: $(RunTime) Duration: $(Duration) Code: $(ResultCode) Value: $(Value)

2. 追加メッセージ

   既定のメッセージの後に追加して SYSLOG に書きこむ内容を指定します。1 行(改行なし)で指定します。

   日本語入力可能(UTF-8 で書き込まれます)です。文字数制限はありません。

   改行を指定した場合は、行ごとに別個の SYSLOG メッセージとして書き込まれます。

3. 変数の挿入

追加メッセージ内に既定の変数を指定します。[変数の挿入]ボタンを選択すると書き込まれる際に該当する変数が変換されてメッセージに書き込まれます。

出力例）

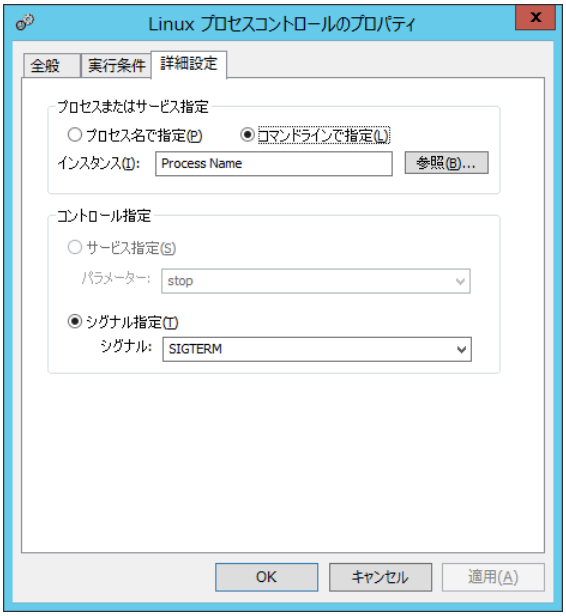
Jun 5 14:22:06 localhost logger: *** Notification from BOM (monitoring 192.168.1.1) *** Monitor 'GRP01MON01' has detected a status 4 (0:Normal,1:Warning,2:Critical,4:Failure). SendTime: 2016/06/05 14:59:40 +0900 InstanceID: 19216811 MonitorID: GRP01MON01 RunTime: 2016/06/05 14:59:40 +0900 Duration: 0.110 Code: 0x80070057 Value: (N/A)

4.3.3 Linux プロセスコントロール

Linux コンピューターのプロセスを制御します。

※ “監視するステータス”は“注意”、“危険”に“実行頻度”は“毎回”にデフォルト時チェックされています。

A. 詳細設定タブ



1. プロセスまたはサービス指定

   “プロセス名で指定”はプロセスをプロセス名で指定します。前方一致で適合したプロセスが監視対象になります。

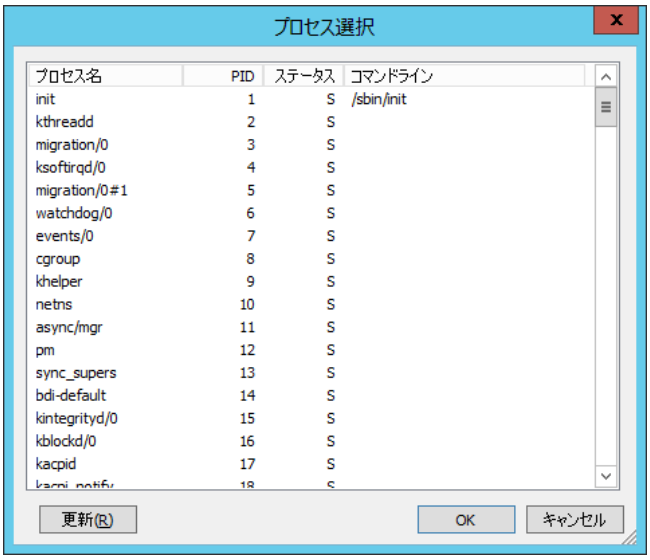
   “コマンドラインで指定”はプロセスコマンドラインによってプロセスを指定します。規定値はこの設定になります。前方一致で適合したプロセスが監視対象になります。

   “インスタンス”はプロセス指定が有効な場合、“プロセス名で指定”か“コマンドラインで指定”かのどちらかで、プロセスを指定する必要があります。

   ※ 260 文字まで入力できます

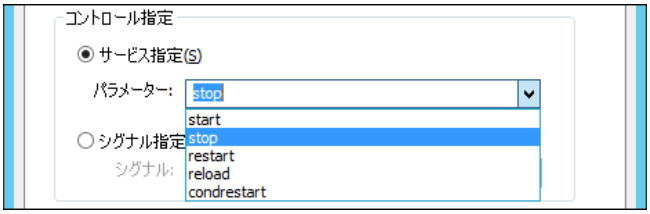
2. 参照

プロセス選択ダイアログを表示します。



Linux のプロセス一覧コマンド(ps)の実行の結果を表示します。選択すると、プロセス名またはコマンドラインの内容がインスタンスに設定されます。プロセス名(コマンドライン名)とサービス名が異なる場合、[参照]ボタンは使用しないでください。

3. サービス指定



インスタンスに対して指定のサービスコマンドを実行します。ポップアップメニューからの選択の他、260 文字まで手入力可能です。デフォルトは“stop”です。

※ Linux の service コマンドを使用しています。

start：サービス開始

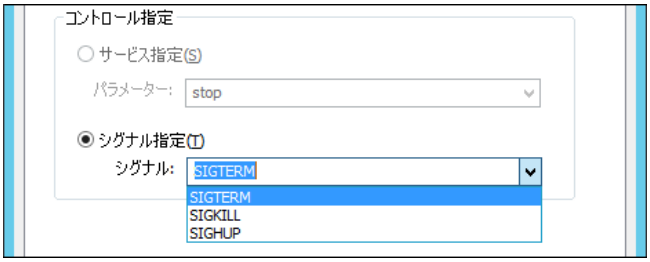
stop：サービス停止

restart:サービス停止後開始

reload：設定ファイル再読込

condrestart：該当サービス稼働確認後停止し開始

4. シグナル指定



インスタンスに対して指定のシグナルを送信します。ポップアップメニューからの選択の他、260 文字まで手入力可能です。デフォルトは“SIGTERM”です。

※ SIGTERM: 安全に終了 SIGKILL: 強制終了 SIGHUP: 変更の反映

※ 対象の Linux コンピューターへの監視・アクション用ログインユーザーアカウントが root であることが必要です

※ この処理は指定したプロセスに対する“停止シグナルを送信する処理”を行いますが対象のプロセスによっては実際に停止しない場合があります

※ 手入力の場合は前方一致でプロセス名やコマンドラインを入力する必要があります

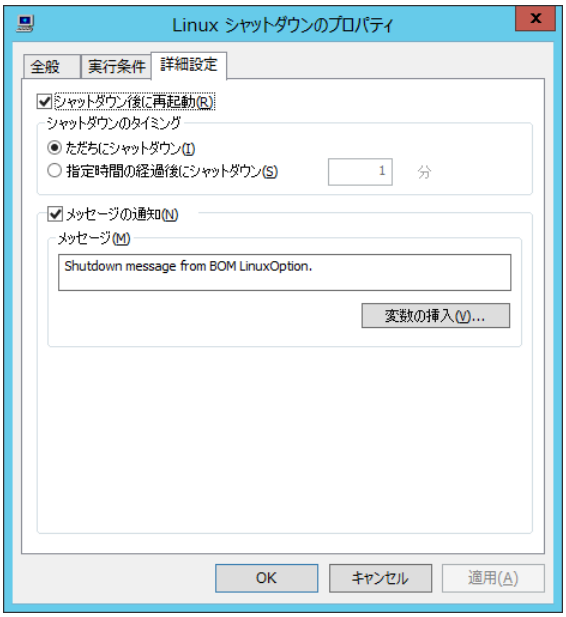
4.3.4 Linux シャットダウン

Linux コンピューターをシャットダウン／再起動します。

※ 「全般」タブは“1 回のみ実行”チェックボックスにデフォルト時チェックされています

※ 「実行条件」タブは“監視するステータス”が“危険”に“実行頻度”は“毎回”にデフォルト時チェックされています

A. 詳細設定タブ



1. シャットダウン後に再起動

   再起動します。デフォルトで設定されています。

2. シャットダウンのタイミング

   “ただちにシャットダウン”は処理を直ちに開始します。規定値で選択されています。

   “指定時間後にシャットダウン” は指定の分数経過後にシャットダウンを開始します。1～999 の整数のみ指定できます。

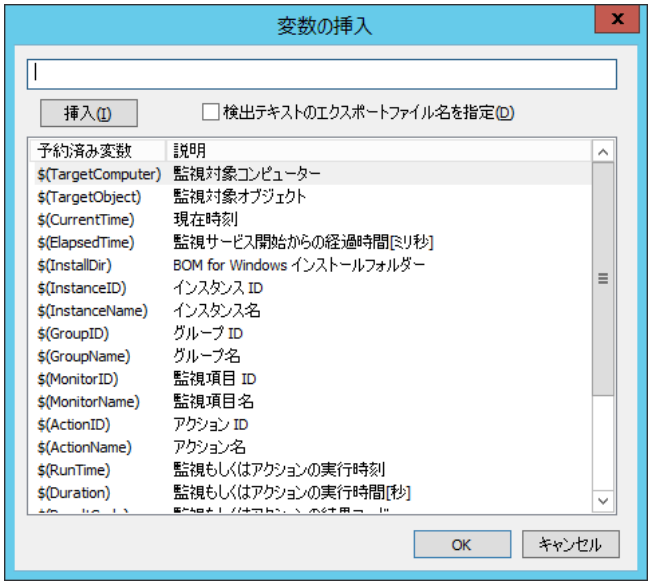
3. メッセージの通知

   シャットダウン時にログインコンソールに指定メッセージを追加します。デフォルトで設定されています。デフォルトのメッセージは以下の通りです。英数字(半角)100 文字まで手入力できます。

   [Shutdown message from BOM7 LinuxOption.]

4. 変数の挿入

追加メッセージ内に既定の変数を指定します。[変数の挿入]ボタンを選択すると書き込まれる際に該当する変数が変換されてメッセージに書き込まれます。



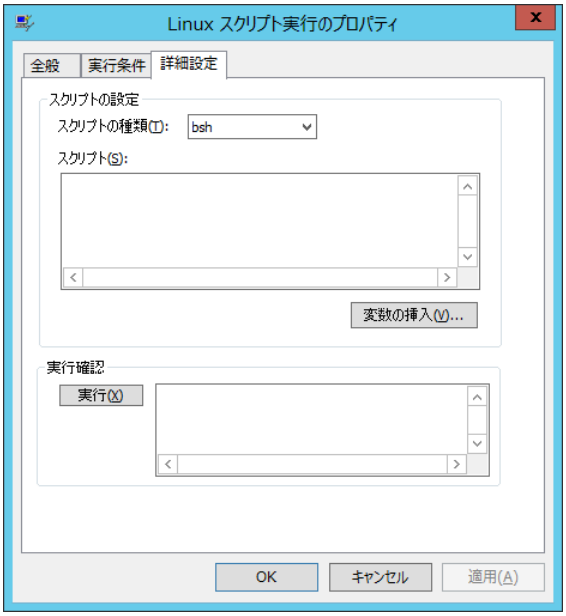
※アクション項目対象 Linux コンピューターへの監視・アクション項目用ログインユーザーアカウントが root でなくてはなりません

4.3.5 Linux スクリプト実行

Linux コンピューター上で任意のスクリプトを実行します。

※ 「実行条件」タブは“監視するステータス”が“注意”、“危険”に“実行頻度”は“毎回”にデフォルト時チェックされています。

A. 詳細設定 タブ



1. スクリプトの種類

   “bsh”、 “csh”、 “bash”、 “perl”よりいずれかを指定します。規定値は bsh が選択されています。

2. スクリプト

   スクリプト種別に対応するスクリプトを 2000 文字以内で記述します。

   例：スクリプトの実行結果をエラーとする場合 1 行目に“error”と改行の出力を実行する。

   (perl の場合の例)

   print “error¥n”;

   →実行エラー。

3. 変数の挿入

   追加メッセージ内に既定の変数を指定します。[変数の挿入]ボタンを選択すると書き込まれる際に該当する変数が変換されてメッセージに書き込まれます。

4. 実行確認

[実行] ボタンはスクリプトを実行し、アクションが実際に実行されるか結果を表示します。

スクリプト実行は以下のコマンドライン処理を行った場合と等価

1.ヒアドキュメントスクリプト読み込み

/bin/sh<<'EOT'または

/bin/csh<<'EOT'または

/bin/bash<<'EOT'または

perl<<'EOT'

2.スクリプトの送信

3.EOT 送信

4.実行結果取得

※ スクリプトの内容によっては正しく実行できない場合があります

※ またスクリプトの内容に関しては製品サポート対象外です

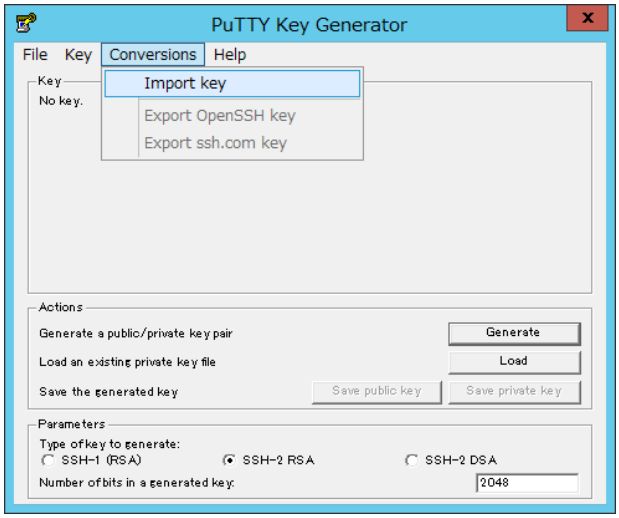
第5章 BOM 7.0 PuTTYgen について

ここでは BOM Linux オプションのインストールで同時にインストールされる、“BOM 7.0 PuTTYgen”について記載します。
“BOM 7.0 PuTTYgen”を使用することで、OpenSSH 形式や Amazon EC2 のプライベートキー形式（.pem）の秘密鍵ファイルを Linux オプションの公開鍵認証方式で利用可能な PuTTY 形式（.ppk）の秘密鍵ファイルに変換できます。

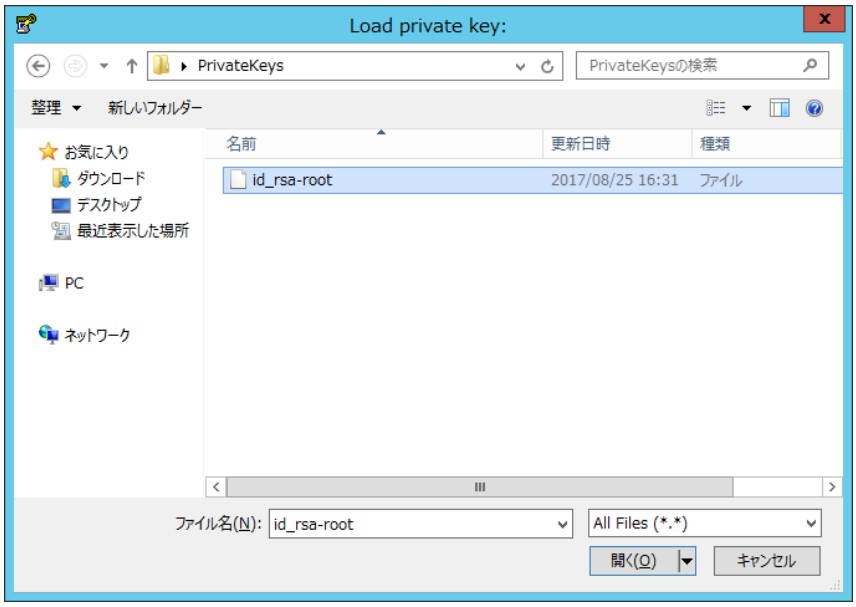
鍵ファイルの変換手順は以下の通りです。

1. スタートメニューから“BOM 7.0 PuTTYgen”を選択します。

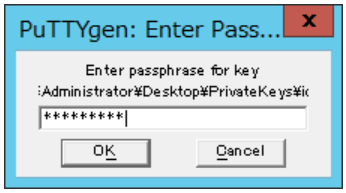
2. PuTTY Key Generator が起動します。
   メニューバーから“Conversions”→“Import key”を選択します。



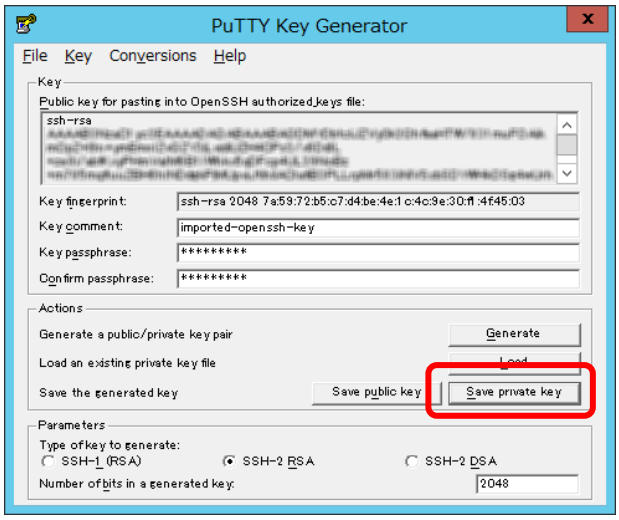
3. 変換したい秘密鍵ファイルを選択し、[開く]をクリックします。



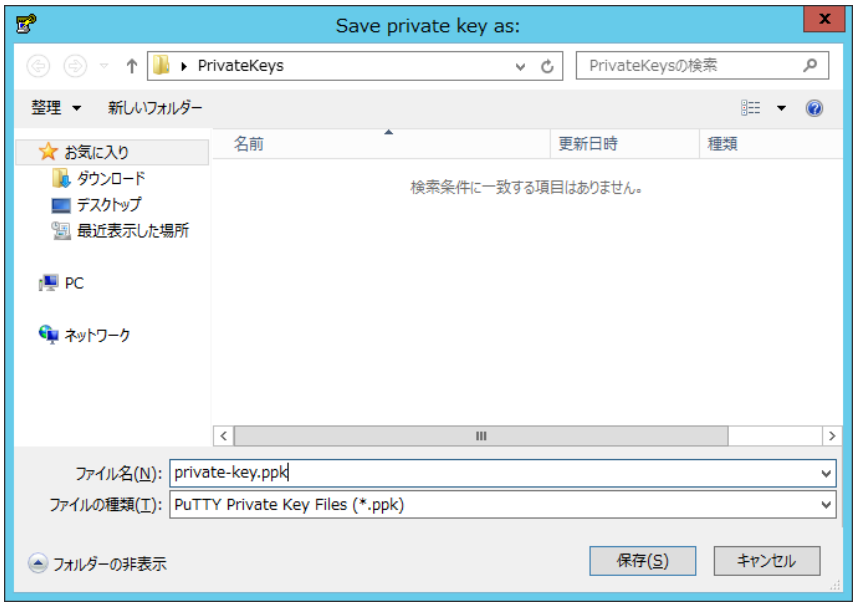
4. 選択した鍵ファイルにパスフレーズを設定している場合は、パスフレーズ入力画面が表示されます。
入力して[OK]ボタンをクリックしてください。



5. PuTTY Key Generator の Key フィールドに鍵の情報が読み込まれたことを確認し、“Actions”の“Save private key”ボタンをクリックします。



6. 鍵ファイルの出力先を指定し、任意のファイル名を入力して[保存]ボタンをクリックします。



（参考情報）

Amazon EC2 のプライベートキー形式（.pem）の秘密鍵ファイルを変換する方法については、以下の参考情報もご参照ください。

Amazon Elastic Compute Cloud Linux インスタンス用ユーザーガイド

PuTTYgen を使用した秘密キーの変換

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/putty.html?icmpid=docs_ec2_console#putty-private-key （2021 年 3 月 22 日現在）

※ 上記 URL はアマゾン ウェブ サービスのウェブサイトです。

本アプリケーションのその他の機能（秘密鍵/公開鍵の作成、その他の鍵形式の変換など）の詳細な使用方法につきましては、以下のウェブサイトで公開されているドキュメントをご参照ください。

PuTTY Documentation Page

https://www.chiark.greenend.org.uk/~sgtatham/putty/docs.html （2021 年 3 月 22 日現在）

※ 上記 URL は“PuTTYgen”開発元のウェブサイトです。

第6章 エラーメッセージ

≪ Linux オプションのエラー ≫

エラー番号	内容	説明
0x80070057	パラメーターが間違っています	監視モジュールに対するパラメーターが不正な場合
0x8000FFFF	致命的なエラーです	想定外のシステムエラーが発生した場合
0x8007065b	関数は実行中に失敗しました	モニタレット実行中にモニタレット内部でエラーが発生した場合 (詳細メッセージ部に、モニタレットエラー一覧で記載したエラーがセットされます)
0x800705B4	タイムアウト期間が経過したため、この操作は終了しました	Linux のコマンド実行で、タイムアウトが発生した場合
0x800700E9	パイプの他端にプロセスがありません	Linux のコマンド実行で、何らかの理由で接続が切れた場合
0x80070035	ネットワーク パスが見つかりません	Linux のコマンド実行で、ホストのアドレスに接続できない場合
0x8007003A	指定されたサーバーは、要求された操作を実行できません	Linux のコマンド実行で、ssh サービスに接続できない場合
0x80070043	ネットワーク名が見つかりません	Linux のコマンド実行で、名前解決ができない場合
0x8007052E	ログオン失敗: ユーザー名を認識できないか、またはパスワードが間違っています	Linux のコマンド実行で、ユーザーまたはパスワードが間違っている場合
0x800704D3	要求は中断されました	Linux のコマンド実行で、スケジュール後、監視終了等の理由で実行が行われなかった場合
0x800703EB	この関数を完了できません	Linux のコマンド実行で、想定外の実行時エラーが発生した場合
0x80040150	レジストリのキーを読み取れませんでした	レジストリキーが読み取れない場合
0x80004003	ポインタが無効です	想定外のシステムエラーが発生した場合(ポインタ不正)
0x80004005	エラーを特定できません	想定外のシステムエラーが発生した場合(原因が不明な場合)
0x8007000E	この操作を完了するのに十分な記憶域がありません	メモリエラーが発生した場合
0x80004001	実装されていません	想定外の機能呼び出しが行われた場合

[モニタレットエラー一覧](以下のエラーは上記 0x8007065b エラーの詳細メッセージに記述されます)

≪ モニタレット全般のエラー ≫

エラー番号	内容	説明
1001	モニタレットの関数が未定義です	定義されていない Method を入力した

≪ ディスク監視 ≫

エラー番号	内容	説明
2101	df コマンドの実行に失敗しました	df コマンドに失敗、df コマンドが無い、または Linux のエラー
2201	不明な監視タイプです	監視タイプが'MBFree'または'PercentFree'以外
2102	df コマンドの実行に失敗しました	df コマンドに失敗、df コマンドが無い、または Linux のエラー
2301	デバイスが見つかりません	df コマンドの実行結果、ディスクデバイスが見つからなかった

≪ ディレクトリ・ファイルサイズ監視 ≫

エラー番号	内容	説明
3101～3102	検索パスが見つかりません	指定されたパスが見つからなかった場合
3104～3105	指定パスはディレクトリではありません	指定パスがディレクトリでない
3103	指定パスはファイルではありません	指定パスがファイルでない
3106	ディレクトリのオープンに失敗しました	指定されたディレクトリを権限不足などで開くことが出来ない
3107	ディレクトリの読み込みに失敗しました	オープンされたディレクトリの内容の読み込みに失敗
3201	du コマンドの実行に失敗しました	du コマンドに失敗、du コマンドが無い、または Linux のエラー
3301	不明な監視タイプです	監視タイプが'FileCount','DirectoryCount','FileSize','DirectorySize'以外

≪ サービスポート監視 ≫

エラー番号	内容	説明
4101	ファイルのオープンに失敗しました	/etc/services のオープンに失敗
4201	不明な監視タイプです	監視タイプが'CurrentState'以外
4202	不明なプロトコルです	プロトコル名が'tcp'または'udp'以外
4203	不明なサービス名です	サービス名からポート番号を検索できない
4301	TCP ソケットの生成に失敗しました	ソケットオープンに失敗、ソケットが無い、またはシステムコールのエラー等
4302	UDP ソケットの生成に失敗しました	ソケットオープンに失敗、ソケットが無い、またはシステムコールのエラー等
4303	RAW ソケットの生成に失敗しました	ソケットオープンに失敗、ソケットが無い、またはシステムコールのエラー等
4304	ソケットの BIND に失敗しました	ソケットへ IP アドレスとポートの割り当てに失敗 localhost のアドレスが無いなど
4305	ICMP パケットの長さが異常です	ICMP パケットの長さが 57Byte ではない
4306	ICMP パケットの内容が不正です	パケットの内容が壊れている Type と Code が3では無いなど

≪ テキストログ監視 ≫

エラー番号	内容	説明
5101	不明な監視タイプです	監視タイプが'MonitorCount'以外
5102	検索条件が指定されていません	通常検索時、検索条件が指定されていない
5103	正規表現が指定されていません	正規表現検索時、正規表現文字列が指定されていない
5104	正規表現構文が不正です	正規表現構文が間違っている、または perl では解析できない構文
5201	ファイルが見つかりません	指定されたファイルが存在しない
5202～5203	ファイルのオープンに失敗しました	ファイルのオープンに失敗
5301	リトライ回数に達しました	指定リトライ回数以内に正常に検索処理を行えなかった
5401	データがありません	テストデータが無い
5402	データのオープンに失敗しました	テストデータの読み込みに失敗、perl のバージョンが古いなど

≪ システムカウンター関連のエラー ≫

エラー番号	内容	説明
6101	オブジェクトタイプが指定されていません	オブジェクトタイプが未指定
6106	不明なオブジェクトタイプです	オブジェクトタイプが不明、'PerfObjectList'で取得した値でない
6102	オブジェクトタイプが指定されていません	オブジェクトタイプが未指定
6110	カウンタータイプが指定されていません	カウンタータイプが未指定
6201～6205	ファイルのオープンに失敗しました	ファイルのオープンに失敗
6103	オブジェクトタイプが指定されていません	オブジェクトタイプが未指定
6111	カウンタータイプが指定されていません	カウンタータイプが未指定
6107	不明なオブジェクトタイプです	オブジェクトタイプが不明、'PerfObjectList'で取得した値でない
6114	不明なカウンタータイプです	カウンタータイプが不明、'PerfCounterList'で取得した値でない
6104	オブジェクトタイプが指定されていません	オブジェクトタイプが未指定
6112	カウンタータイプが指定されていません	カウンタータイプが未指定
6108	不明なオブジェクトタイプです	オブジェクトタイプが不明、'PerfObjectList'で取得した値でない
6115	不明なカウンタータイプです	カウンタータイプが不明、'PerfCounterList'で取得した値でない
6206～6215	ファイルのオープンに失敗しました	ファイルのオープンに失敗
6301	プロセッサ情報の取得に失敗しました	オブジェクトが'Processor'時、/proc 下のファイル仕様が変わっている等
6302～6304	プロセス情報の取得に失敗しました	オブジェクトが'Processor'時、/proc 下のファイル仕様が変わっている等
6305	メモリ情報の取得に失敗しました	オブジェクトが'Processor'時、/proc 下のファイル仕様が変わっている等
6306	ディスク情報の取得に失敗しました	オブジェクトが'Disk'時 -Instance で指定されたディスク情報が取得できなかった
6307	ネットワーク情報の取得に失敗しました	オブジェクトが'Disk'時/proc 下のファイルの仕様が変わっているなど
6401	プロセスが見つかりませんでした	-Instance'で指定されたプロセスが見つからなかった
7201	ディレクトリのオープンに失敗しました	/proc ディレクトリを権限不足などで開くことが出来ない
7202	ディレクトリの読み込みに失敗しました	オープンされた/proc ディレクトリの内容の読み込みに失敗

≪ プロセス監視 ≫

エラー番号	内容	説明
7201	ディレクトリのオープンに失敗しました	/proc ディレクトリを権限不足などで開くことが出来ない
7202	ディレクトリの読み込みに失敗しました	オープンされた/proc ディレクトリの内容の読み込みに失敗
7201	ディレクトリのオープンに失敗しました	/proc ディレクトリを権限不足などで開くことが出来ない
7202	ディレクトリの読み込みに失敗しました	オープンされた/proc ディレクトリの内容の読み込みに失敗
7101	監視タイプが指定されていません	監視タイプが未指定
7102	不明な監視タイプです	監視タイプが Process のカウンター値以外
7104	プロセス名が指定されていません	プロセス名が未指定
7106	オプションが指定されていません	オプションに'-Process'または'-CommandLine'が指定されていない
6401	プロセスが見つかりませんでした	-Instance'で指定されたプロセスが見つからなかった
7108	不明な集計関数です。	集計関数が'Sum','Min','Max','Avg'以外。
6302～6304	プロセス情報の取得に失敗しました。	/proc 下のファイルの仕様が変わっているなど。

≪ プロセス数監視 ≫

エラー番号	内容	説明
7103	不明な監視タイプです	監視タイプが'MonitorCount'以外
7105	プロセス名が指定されていません	プロセス名が未指定
7107	オプションが指定されていません	オプションに'-Process'または'-CommandLine'が指定されていない
7201	ディレクトリのオープンに失敗しました	/proc ディレクトリを権限不足などで開くことが出来ない
7202	ディレクトリの読み込みに失敗しました	オープンされた/proc ディレクトリの内容の読み込みに失敗

第7章 制限および注意事項

1. Linux オプションを使用するのに事前に必要な Linux コンピューターの設定、操作は、製品サポート対象外です。Linux の使い方、設定方法、トラブルなどについてのご質問については承っておりません

2. Linux オプションは BOM 7.0 コントロールパネルの「設定ユーティリティ」タブの“BOM 7.0 設定一括配布ツール”に対応していません。Linux インスタンスを含むコンピューターからの設定一括配布及び Linux インスタンスを含むコンピューターへの設定一括配布はできません

3. Linux インスタンスのプロパティの“アカウント”を変更する場合は、「全般」タブで、アカウントとパスワードを変更した後、[モニタレット管理]ボタンから[リモートモニタレット更新]ボタンを使用し更新を行ってください

4. アクション項目の追加メッセージで指定できる[変数の挿入(V)]ボタンにおいて、“アクション終了コード”と“アクション実行結果”は指定しないでください。これらの変数は通知項目のみで使用できます。

5. Linux オプションとアーカイブサービスがインストールされている環境で、Linux を監視する場合、アーカイブサービス開始直後とその 24 時間毎に一定時間監視が行われないことがあります。これは監視とは別の必要な情報を Linux コンピューターより取得しているからです。監視が行われない間には、スキップメッセージがログに書かれます。なお、Windows のインスタンスでは発生しません

第8章 FAQ

Q インストール時にファイアウォールの向こうにある Linux へ監視を設定したいのですが。

A BOM の監視サービスと、監視する Linux コンピューターは標準的な SSH プロトコルで接続されているので、SSH（通常は 22 番）を通過させる設定をしてください。

Q ファイアウォール越しに Linux を監視したいのですが。

A BOM の監視サービスと、監視する Linux コンピューターは標準的な SSH プロトコルで接続されているので、SSH（通常は 22 番）を通過させる設定をしてください。

Q 監視で使用する Linux のアカウントのパスワードはどこに保存されているのですか。

A 暗号化されて監視サービスのある Windows コンピューターのファイル内に保存されます。なお、パスワードがそのままネットワーク上を流れることはありません。

Q ディレクトリ監視に時間がかかる（タイムアウトでNGになる）のですが。

A du コマンドと同様の処理となるため、特に初回監視時に非常に時間がかかることがあります（キャッシュされていないため）。処理に 10 分以上かかる場合は、エラーとなります。（後続の監視値もエラーになる場合があります）。大きなボリュームにはディスク監視を使用するようにしてください。

Q ディレクトリ監視の取得サイズが小さすぎるのですが。

A 監視するディレクトリ以下に存在する全てのディレクトリに対する参照権限がない場合、権限がないディレクトリの分の容量が除かれてしまいます。

Q プロセスコントロールとシャットダウンは root でなければならないのでしょうか。

A はい。同処理を行う場合は、監視・アクション用アカウントを root にしてください。

Q システムログに監視処理のための SSH の認証関連のログが出力されているのですが。

A 監視処理・アクションを実行するために、必要のある都度、login/logoff を繰り返すため、そのタイミングで/var/log/messages 等にログが残ることがあります。

Q サービスポート監視で監視しているアプリケーションのエラーログが出ているのですが。

A 監視ポートに対して実際に接続を試みるため、そのスキャン処理がアプリケーション側でエラーとみなされアプリケーションのエラーログ等として残る場合があります。例えば、sshd（22 番ポート）の場合は、「/var/log/secure」等に「Did not receive identification string from 127.0.0.1」というログが出ることがあります。

Q Linux コンピューターに何かインストールされたり勝手に設定が変えられたりするのでしょうか。

A 監視・アクション用のアカウントのホームディレクトリに.Bom というディレクトリが作成され、内部にファイルが配置される以外のことは行われません。

Q たまに監視の値がエラーになっているようですが。

A ネットワークの異常など（IP のコンフリクト）がある場合は、監視はエラーになります。監視の処理が実行されている途中で ssh のコネクションが落ちてしまうような場合は、タイミングによってはエラーになることもあります。監視が行われていない、監視と監視の間で ssh のコネクションが落ちてしまっても、監視時に復旧していれば再度ログインを試みるので監視は正常に行えます。

第9章 システムカウンター一覧

オブジェクト	カウンター	インスタンス	情報取得先ファイル	詳細説明
Processor	LoadAverage1	-	/proc/loadavg	直近 1 分間の平均プロセス実行割合を 100 倍した値
	LoadAverage5	-	/proc/loadavg	直近 5 分間の平均プロセス実行割合を 100 倍した値
	LoadAverage15	-	/proc/loadavg	直近 15 分間の平均プロセス実行割合を 100 倍した値
	Uptime	-	/proc/uptime	システム起動時からの経過時間を 1/100 秒単位で取得
	UserTime	cpu または_Total	/proc/stat	ユーザーモードでの CPU 実行時間を 1/100 秒単位で取得
	NiceTime	cpu または_Total	/proc/stat	低優先度のユーザーモードでのCPU実行時間を1/100秒単位で取得
	SystemTime	cpu または_Total	/proc/stat	システムモードでの CPU 実行時間を 1/100 秒単位で取得
	IdleTime	cpu または_Total	/proc/stat	タスク待ちでの CPU 実行時間を 1/100 秒単位で取得
	TotalTime	cpu または_Total	/proc/stat	ユーザー･低優先度のユーザー･システムモードでの合計 CPU 実行時間を 1/100 秒単位で取得
	UserTime%	cpu または_Total	/proc/stat	直近 1 秒間のユーザーモードでの CPU 実行時間比率を%単位で取得
	NiceTime%	cpu または_Total	/proc/stat	直近 1 秒間の低優先度のユーザーモードでの CPU 実行時間比率を%単位で取得
	SystemTime%	cpu または_Total	/proc/stat	直近 1 秒間のシステムモードでの CPU 実行時間比率を%単位で取得
	IdleTime%	cpu または_Total	/proc/stat	直近 1 秒間のタスク待ちでの CPU 実行時間比率を%単位で取得
	TotalTime%	cpu または_Total	/proc/stat	直近 1 秒間のユーザー･低優先度のユーザー･システムモードでの合計 CPU 実行時間比率を%単位で取得
	ContextCount	-	/proc/stat	システム起動時からのコンテキストスイッチの延べ回数
	ForkCount	-	/proc/stat	システム起動時からの Fork の延べ回数

オブジェクト	カウンター	インスタンス	情報取得先ファイル	詳細説明
Process	RunningProcesses	-	/proc/$PID/stat	実行中のプロセス数
	TotalProcesses	-	/proc/$PID/stat	総プロセス数
	ZombieProcesses	-	/proc/$PID/stat	ゾンビプロセス数
	SleepingProcesses	-	/proc/$PID/stat	休止中プロセス数 割り込み不可能な休止プロセスも含む
	StoppedProcesses	-	/proc/$PID/stat	停止中プロセス数
	VirtualSize	プロセス名	/proc/$PID/statm	プログラムサイズのバイト単位の総計
	ResidentSetSize	プロセス名	/proc/$PID/stat	常駐しているプログラムサイズのバイト単位の総計
	Memory%	プロセス名	/proc/$PID/stat	物理メモリ使用率を%単位で取得
	Cpu%	プロセス名	/proc/$PID/stat	直近 5 秒間の CPU 使用率を%単位で取得
	MinorFaults	プロセス名	/proc/$PID/stat	ディスクからメモリページへのロードを必要としないフォールトの回数
	MinorFaultsC	プロセス名	/proc/$PID/stat	子プロセスを含めたディスクからメモリページへのロードを必要としないフォールトの回数
	MajorFaults	プロセス名	/proc/$PID/stat	ディスクから メモリページへのロードを必要とするフォールトの回数
	MajorFaultsC	プロセス名	/proc/$PID/stat	子プロセスを含めたディスクから メモリページへのロードを必要とするフォールトの回数
	UserTime	プロセス名	/proc/$PID/stat	ユーザーモードでの CPU 実行時間を 1/100 秒単位で取得
	UserTimeC	プロセス名	/proc/$PID/stat	子プロセスを含めたユーザーモードでの CPU 実行時間を 1/100 秒単位で取得
	SystemTime	プロセス名	/proc/$PID/stat	システムモードでの CPU 実行時間を 1/100 秒単位で取得
	SystemTimeC	プロセス名	/proc/$PID/stat	子プロセスを含めたシステムモードでの CPU 実行時間を 1/100 秒単位で取得

※2.4 2.6 はカーネルバージョンです

オブジェクト	カウンター	インスタンス	情報取得先ファイル	詳細説明
Memory	MemUsed	-	/proc/meminfo	OS のバッファ・キャッシュとして消費されている分を除いたメモリ使用量をバイト単位で取得
	MemUsed%	-	/proc/meminfo	OS のバッファ・キャッシュとして消費されている分を除いたメモリ使用割合を%単位で取得
	MemFree	-	/proc/meminfo	OS のバッファ・キャッシュとして消費されている分を含むメモリ空き容量をバイト単位で取得
	SwapUsed	-	/proc/meminfo	スワップメモリの使用量をバイト単位で取得
	SwapUsed%	-	/proc/meminfo	スワップメモリの使用割合を%単位で取得
	SwapFree	-	/proc/meminfo	スワップメモリの空き容量をバイト単位で取得
	Buffers	-	/proc/meminfo	バッファメモリ使用量をバイト単位で取得
	Cached	-	/proc/meminfo	キャッシュメモリの使用量をバイト単位で取得
	Shared	-	/proc/meminfo	共有メモリの使用量をバイト単位で取得
	SwapIn	-	2.4:/proc/stat 2.6:/proc/vmstat	仮想メモリの総スワップインページ数
	SwapOut	-	2.4:/proc/stat 2.6:/proc/ vmstat	仮想メモリの総スワップアウトページ数
	PageIn	-	2.4:/proc/stat 2.6:/proc/ vmstat	仮想メモリの総ページイン数
	PageOut	-	2.4:/proc/stat 2.6:/proc/ vmstat	仮想メモリの総ページアウト数
Disk	IORequests	ディスクデバイス名	2.4:/proc/stat 2.6:/proc/diskstats	ディスクIO要求総数
	ReadRequests	ディスクデバイス名	2.4:/proc/stat 2.6:/proc/diskstats	ディスク読み出し要求総数
	ReadBlocks	ディスクデバイス名	2.4:/proc/stat 2.6:/proc/diskstats	ディスク読み出しブロック総数
	WriteRequests	ディスクデバイス名	2.4:/proc/stat 2.6:/proc/diskstats	ディスク書き込み要求総数
	WriteBlocks	ディスクデバイス名	2.4:/proc/stat 2.6:/proc/diskstats	ディスク書き込みブロック総数

オブジェクト	カウンター	インスタンス	情報取得先ファイル	詳細説明
Network	DevRecvBytes	インターフェイス名	/proc/net/dev	受信総バイト数
	DevRecvPackets	インターフェイス名	/proc/net/dev	受信パケット総数
	DevRecvErrs	インターフェイス名	/proc/net/dev	受信エラー総数
	DevRecvDrop	インターフェイス名	/proc/net/dev	受信破棄総数
	DevTransBytes	インターフェイス名	/proc/net/dev	送信総バイト数
	DevTransPackets	インターフェイス名	/proc/net/dev	送信パケット総数
	DevTransErrs	インターフェイス名	/proc/net/dev	送信エラー総数
	DevTransDrop	インターフェイス名	/proc/net/dev	送信破棄総数
	DevTransColls	インターフェイス名	/proc/net/dev	送信衝突総数
	IPInReceives	-	/proc/net/snmp	受信 IP データグラムの総数
	IPInHdrErrors	-	/proc/net/snmp	IP ヘッダ内のエラーにより破棄した IP データグラムの総数
	IPInAddrErrors	-	/proc/net/snmp	IP ヘッダ内の宛先アドレスが無効なために破棄された IP データグラムの総数
	IPForwDatagrams	-	/proc/net/snmp	転送された IP データグラムの総数
	IPInUnknownProtos	-	/proc/net/snmp	プロトコルが不明なために破棄した IP データグラムの総数
	IPInDiscards	-	/proc/net/snmp	バッファ不足などエラー以外の理由で破棄した IP データグラム総数
	IPInDelivers	-	/proc/net/snmp	正常処理された IP データグラムの総数
	IPOutRequests	-	/proc/net/snmp	送信要求された IP データグラムの総数
	IPOutDiscards	-	/proc/net/snmp	バッファ不足などで送信できなかった IP データグラム総数
	IPOutNoRoutes	-	/proc/net/snmp	送信先への経路が不明なため破棄された IP データグラム総数
	IPReasmReqds	-	/proc/net/snmp	再構成が必要だった IP データグラムの総数
	IPReasmOKs	-	/proc/net/snmp	再構成された IP データグラムの総数
	IPReasmFails	-	/proc/net/snmp	再構成できなかった IP データグラムの総数
	IPReasmTimeout	-	/proc/net/snmp	フラグメントが再構成された IP データグラムを保持しておく最大秒数
	IPFragOKs	-	/proc/net/snmp	フラグメントされた IP データグラムの総数
	IPFragFails	-	/proc/net/snmp	フラグメントに失敗した IP データグラムの総数
	IPFragCreates	-	/proc/net/snmp	作成されたフラグメント IP データグラムの総数
	IPDefaultTTL	-	/proc/net/snmp	IP データグラムを保持する時間のデフォルト値
	IPForwarding	-	/proc/net/snmp	IP データグラムが転送されゲートウェイとして動作しているかを示すフラグ
	TCPActiveOpens	-	/proc/net/snmp	TCP 接続がクライアントとして能動的にオープンされた回数
	TCPPassiveOpens	-	/proc/net/snmp	TCP 接続がサーバーとして受動的にオープンされた回数
	TCPAttemptFails	-	/proc/net/snmp	TCP 接続に失敗した回数
	TCPEstabResets	-	/proc/net/snmp	TCP 接続がリセットされた回数
	TCPCurrEstab	-	/proc/net/snmp	現在の TCP 接続数
	TCPInSegs	-	/proc/net/snmp	受信 TCP セグメント数
	TCPOutSegs	-	/proc/net/snmp	送信 TCP セグメント数
	TCPRetransSegs	-	/proc/net/snmp	再送信した TCP セグメント数
	TCPInErrs	-	/proc/net/snmp	エラーのあった受信 TCP セグメント数
	TCPOutRsts	-	/proc/net/snmp	RST フラグを含む送信 TCP セグメント数
	TCPRtoMax	-	/proc/net/snmp	最大再送信タイムアウト時間を 1/1000 秒単位で取得
	TCPRtoMin	-	/proc/net/snmp	最小再送信タイムアウト時間を 1/1000 秒単位で取得
	TCPRtoAlgorithm	-	/proc/net/snmp	現在の再送信タイムアウトアルゴリズムを示すフラグ

オブジェクト	カウンター	インスタンス	情報取得先ファイル	詳細説明
	TCPMaxConn	-	/proc/net/snmp	最大接続可能数
	UDPInDatagrams	-	/proc/net/snmp	受信した UDP データグラムの総数
	UDPNoPorts	-	/proc/net/snmp	ポート指定が無効なため破棄した UDP データグラム総数
	UDPInErrors	-	/proc/net/snmp	受信したエラーUDP データグラムの総数
	UDPOutDatagrams	-	/proc/net/snmp	送信した UDP データグラムの総数
	ICMPInAddrMasks	-	/proc/net/snmp	受信したアドレスマスクのリクエストの総数
	ICMPInAddrMaskReps	-	/proc/net/snmp	受信したアドレスマスクのレスポンスの総数
	ICMPInDestUnreachs	-	/proc/net/snmp	受信した宛先到達不可能メッセージ数
	ICMPInEchos	-	/proc/net/snmp	受信したエコーリクエストの総数
	ICMPInEchoReps	-	/proc/net/snmp	受信したエコーレスポンスの総数
	ICMPInErrors	-	/proc/net/snmp	受信した ICMP エラーメッセージの総数
	ICMPInMsgs	-	/proc/net/snmp	受信した ICMP メッセージの総数
	ICMPInParmProbs	-	/proc/net/snmp	受信したパラメーター異常メッセージの総数
	ICMPInRedirects	-	/proc/net/snmp	受信した経路変更要求メッセージの総数
	ICMPInSrcQuenchs	-	/proc/net/snmp	受信した送信抑制要求メッセージの総数
	ICMPInTimeExcds	-	/proc/net/snmp	受信したデータグラム生存時間超過メッセージの総数
	ICMPInTimestamps	-	/proc/net/snmp	受信したタイムスタンプリクエストの総数
	ICMPInTimestampReps	-	/proc/net/snmp	受信したタイムスタンプレスポンスの総数
	ICMPOutAddrMasks	-	/proc/net/snmp	送信したアドレスマスクリクエストの総数
	ICMPOutAddrMaskReps	-	/proc/net/snmp	送信したアドレスマスクレスポンスの総数
	ICMPOutDestUnreachs	-	/proc/net/snmp	送信した宛先到達不可能メッセージの総数
	ICMPOutEchos	-	/proc/net/snmp	送信したエコーリクエストの総数
	ICMPOutEchoReps	-	/proc/net/snmp	送信したエコーレスポンスの総数
	ICMPOutErrors	-	/proc/net/snmp	送信した ICMP エラーメッセージの総数
	ICMPOutMsgs	-	/proc/net/snmp	送信した ICMP メッセージの総数
	ICMPOutParmProbs	-	/proc/net/snmp	送信したパラメーター異常メッセージの総数
	ICMPOutRedirects	-	/proc/net/snmp	送信した経路変更要求メッセージの総数
	ICMPOutSrcQuenchs	-	/proc/net/snmp	送信した送信抑制メッセージの総数
	ICMPOutTimeExcds	-	/proc/net/snmp	送信したデータグラム生存時間超過メッセージの総数
	ICMPOutTimestamps	-	/proc/net/snmp	送信したタイムスタンプリクエストの総数
	ICMPOutTimestampReps	-	/proc/net/snmp	送信したタイムスタンプレスポンスの総数

BOM Linux オプション Ver.7.0

ユーザーズ マニュアル

2017 年 1 月 1 日　初版
2021 年 4 月 1 日　改訂版

著者　　セイ・テクノロジーズ株式会社
発行者　セイ・テクノロジーズ株式会社
発行　　セイ・テクノロジーズ株式会社
バージョン　Ver.7.0.40.0