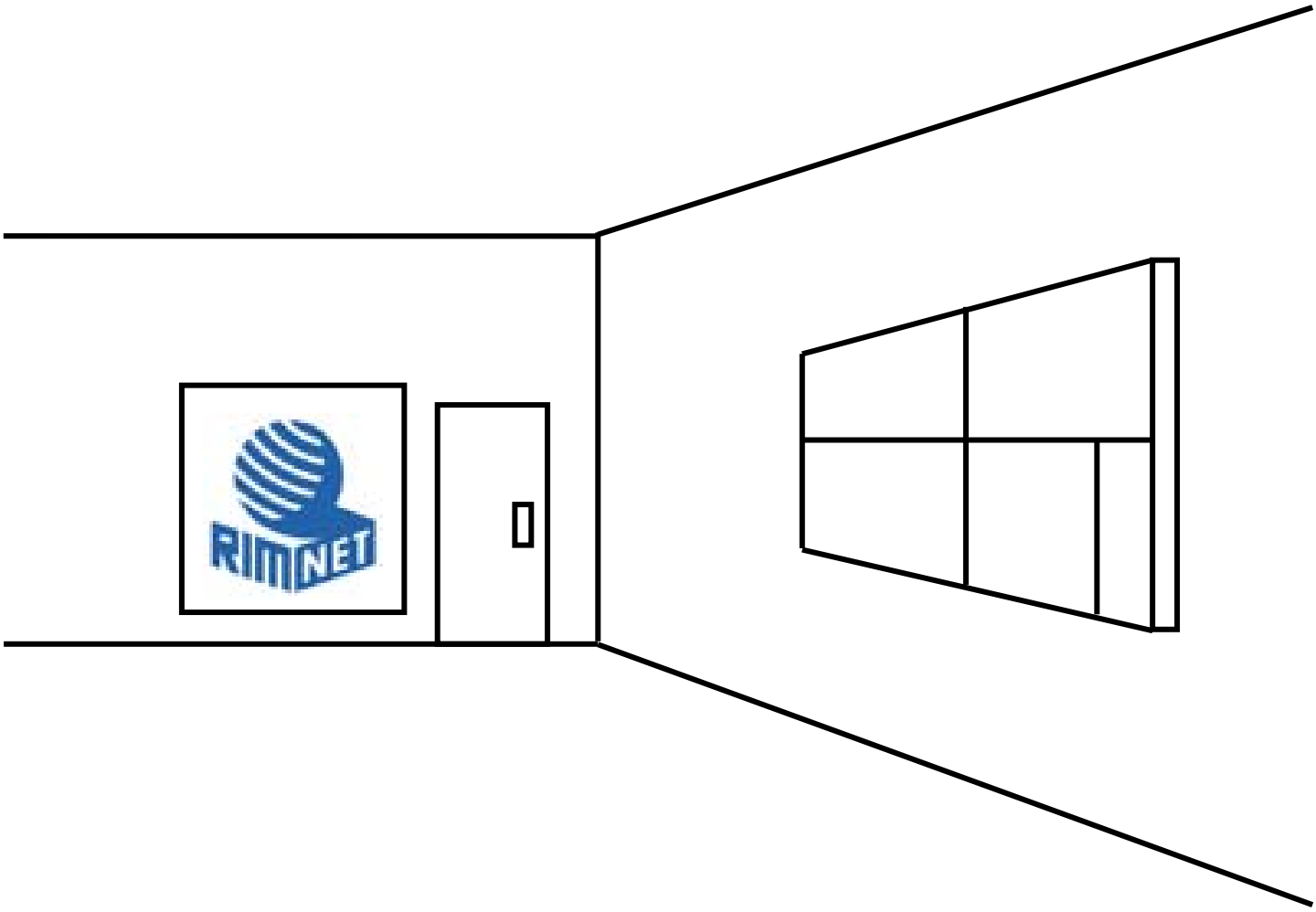


マイサーバーサービス 利用マニュアル
(グラフレポート / 自己監視 / ログ管理 / SNMP)
マイサーバーVPS compact

RIMNET http://www.rim.or.jp/support/

Members Guide Book **2010/07**

はじめに

本利用マニュアルでは、マイサーバーVPS compact の「グラフレポート」「自己監視」「ログ管理」
「SNMP エージェント」について解説します。

目次

１．グラフレポート

１－１．概要

HDE Controller にログインし、「グラフレポート」のアイコンをクリックします。
次項の項目に従って設定及び確認を実施してください。

１－２．グラフレポートの初期化

●グラフレポートの初期化
　自己監視の監視結果を時系列グラフとして表示できるようにします。

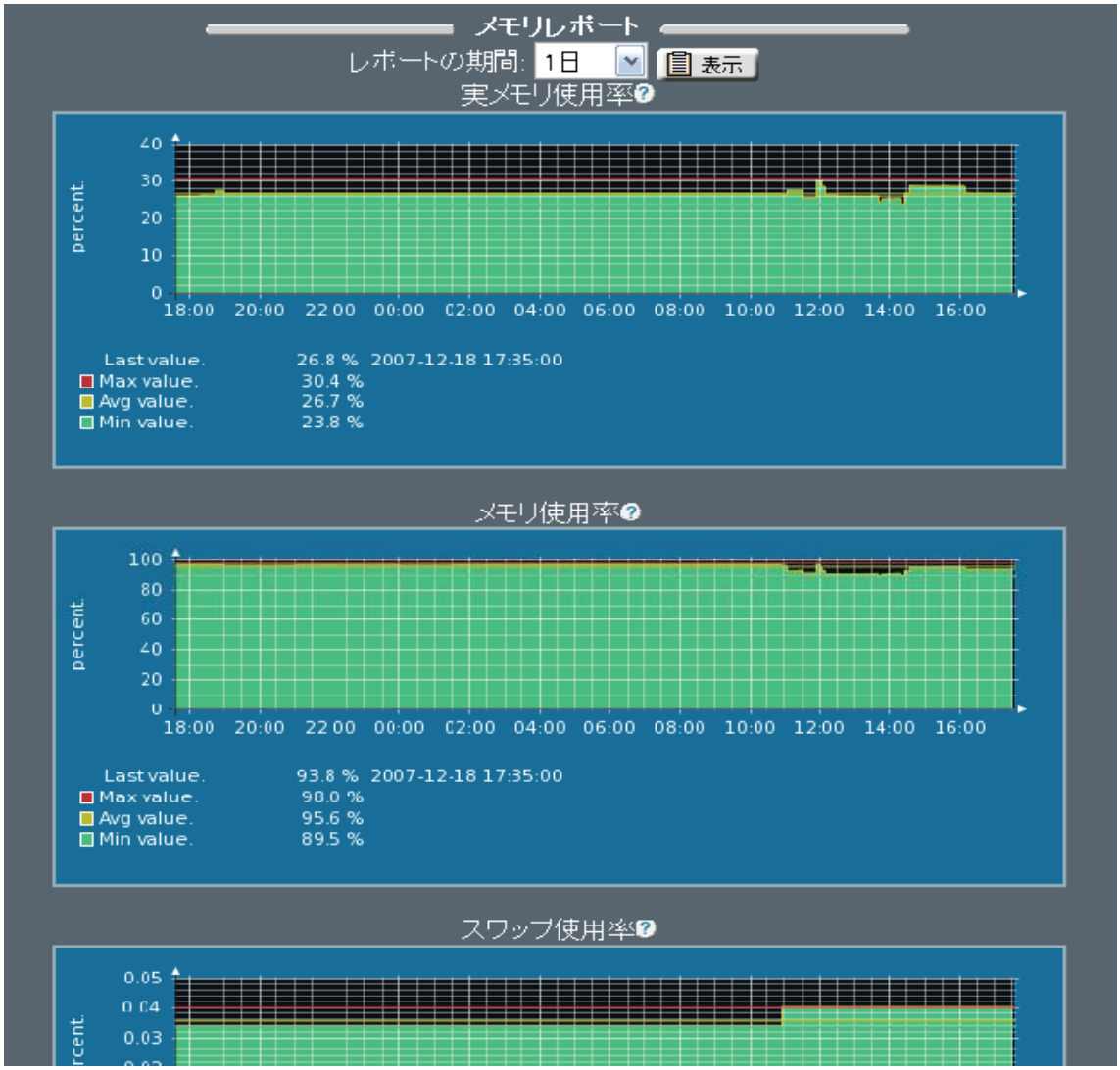
「グラフレポートの初期化」を選択します。
「設定する」をクリックします。
既に初期化されている場合はこの操作は必要ありません。

※サーバーのリソースやパフォーマンスなどの状況は　自己監視サービスが収集するので、　自己監視サービスを常時起動しておく必要があります。
　この時、監視間隔が「監視しない」以外に設定されている必要がありますが、　しきい値やアクションの設定は必須ではありません。

※サーバーの時刻が常に正確に設定されていないと監視結果が保存できなくなる場合があります。
　このため、リモート・NTP サーバーと時刻を同期させ常に正確な　時刻が設定させるよう「NTP サーバー」－「NTP サーバー設定」の設定を　行うことをお勧めします。

●しきい値の見直し
自己監視の監視結果を時系列グラフとして表示します。
時系列グラフを表示したい監視項目に対応するレポートを選択します。
時系列グラフの「レポートの期間」は１日(ディスク使用率は１ヶ月)ですが、１日、１週、１ヶ月、６ヶ月、１年に変更することもできます。
変更する場合、「レポートの期間」を変更し「表示」をクリックします。
なお、「レポートの期間」が複数ある場合は必要に応じてそれぞれ変更します。

「レポートの期間」が複数ある場合どの「表示」をクリックしてもかまいません。



Last value ・・・ 最新値、最終データ登録時刻です。

Max value ・・・ 最大値です。

Avg value ・・・ 平均値です。

Min value ・・・ 最小値です。

「レポートの期間」で指定した期間が長いと

グラフ中にデータ線が引かれず、

Last value(最新値)

Max value(最大値)

Avg value(平均値)

Min value(最小値)が

nan と表示される場合があります。

特にディスク使用率の「レポートの期間」の初期値は１ヶ月なのでしばらくの間このように表示されます。

このような場合は「レポートの期間」を短くしてください。
「レポートの期間」を 1 日に指定しても nan と表示される場合は、自己監視で設定した監視間隔に達してから再度表示してください

設定後
リソースレポート
パフォーマンスレポート
ログインレポート
プロセスレポート
任意のプロセスレポートが表示確認できます。

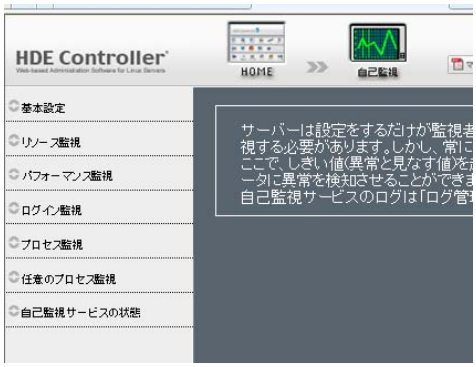
２．自己監視

２－１．概要

HDE Controller にログインし、「自己監視」のアイコンをクリックします。
次項の項目に従って設定及び確認を実施してください。

２－２．自己監視

●自己監視



●概要
サーバーの設定後、サーバーを安定稼動させるには、ディスクやメモリなどのハードウェアリソースやプロセスなどの監視が欠かせません。
サーバーの監視を行うことにより、サーバーが不安定になる前にパフォーマンス低下やリソース不足などの予兆を検知・対処することで、様々な障害を未然に防止できます。

しかし、システム管理者が常にサーバーを監視することは、多大な時間が必要であること、見逃しなど
人為的ミスが発生し易いので現実的ではありません。
「自己監視」を使用すれば、システム管理者の代わりにサーバーの状況を定期的に把握して異常時に
ログやメールで警告したり、あらかじめ設定しておいたスクリプトを実行させたりすることにより、
障害を自動復旧することもできます。

また、「グラフレポート」で表示する時系列グラフのデータとなるサーバーの状況を定期的に収集します。
「グラフレポート」を使用すれば、現在までのサーバーの状況を時系列グラフとして表示できます。
これを元に「自己監視」でしきい値(異常と見なす値)を超えた場合のアクション(メール送信やスクリプト実行)を
設定しておくと、コンピューターに異常を検知させることができます。

また、システム管理者は「サーバーステータス」を使用すれば、その瞬間のサーバーの状況を確認したり、
必要に応じてサービスを起動または停止したりすることもできます。

●サーバー監視の自動化
監視項目の選定としきい値の決定
自己監視で監視できる項目には、次のようなものがあります。
監視項目ごとに、それぞれの意味やしきい値の決め方について説明します。
これを参考に監視項目を選定し、しきい値を決めてください。

(1) ディスク使用率、iノード使用率
ファイルシステムによって適切な値は異なりますが、ディスク使用率やiノード使用率が100%になると
ディスクにメールなどのデータが保存できなくなります。
また、システムを続行できなくなることもありますので余裕を持った設定をお勧めします。

(2) 実メモリ使用率
バッファメモリ(buffersとcached)を含まないメモリ使用率です。
バッファメモリを含むメモリ使用率(物理メモリ使用率)より小さい値になります。
実メモリ使用率が高くなるとシステムが使用できるバッファメモリが少なくなりパフォーマンスの低下を招きます。

しきい値を設定する場合は、グラフレポートで通常使用されている実メモリ使用率を把握して多少大きめの値を
お勧めします。

(3) 物理メモリ使用率
この値が100%近くであっても特に問題ではありませんが、実メモリ使用率との差が小さい場合はパフォーマンスが
低下している可能性があります。

(4) swap使用率
性能を重視するサーバーであれば、swapを使用するようなら物理メモリの増設を検討することも必要となります。
あまり性能を重視しないサーバーであっても100%となった場合にはシステムが停止することもありますので

余裕を持った設定をお勧めします。

(5) システム負荷

システム負荷とは簡単にいうと、CPU の稼働率のことで 1.00 以下であれば滞りなくプロセスが実行されています。
1.00 以上であれば負荷が重くいくつかのプロセスの実行に遅延が生じていることを示します。

高負荷がかからない環境では 2.0 前後、データベースなどを使用し、高負荷がかかる環境では正常に処理が
行える範囲の目安を作り適切な値を設定してください。

(6) CPU 使用率

前回の監視時点からの CPU 使用率(idle を除く)の平均値です。
この値が 100%近くであ れば、監視間隔が 5 分なら 5 分間 CPU を 100%近く使用し続けていたということになります。
CPU の能力不足や動作しているプロセスに異常が発生してい る可能性が考えられます。
なお、プロセスによっては正常な動作として一定期間 CPU を 100%近く使用する場合がありますが、
監視間隔を長めに設定すれば このようなプロセスでアラートは上がりません。

(7) ログインユーザー数

ログインユーザーの増加に伴い、メモリや CPU などのシステムリソースが消費されます。
システムがサービスを提供する上で必要なシステムリソースまでも消費してしまい、システムが続行
できなくな ることもあります。
また、ログインを開放していないシステムであれば不正侵入などセキュリティ上の問題が考えられます。
telnet、ssh のログインを開放し、ユーザーのログインが行われていたり、管理を頻繁に行っていたりする
環境でない限り、管理に最低限必要なログイン数の設定をお勧めします。
各種ログインを許可している環境ではログインユーザーの使用状況により適切な値を設定してください。

(8) 全てのプロセス数

プロセスは、メモリや CPU などのシステムリソースを消費します。
プロセス数が多くなるほど、システムリソースの消費量も増加し、ついにはシステムが続行できなくなる
こともあります。
システムの状況により適切な値を決定し、設定してください。

(9) 実行中プロセス数

システムで実行中のプロセスの数です。特殊な場合を除き、この数を監視する必要はありません。

(10) スリープ中プロセス数

システムで実行待ちのプロセスの数です。特殊な場合を除き、この数を監視する必要はありません。

(11) 停止中プロセス数

ユーザーの指示などにより、実行を一時停止しているプロセスの数です。
実行を一時停止しているプロセスもメモリなどのシステムリソースを消費しています。
この数が多いとシステムリソースが有効に使用できず、システムリソース不足を招く要因になることもあります。
システムの状況により適切な値を決定し、設定してください。

(12) ゾンビプロセス数

ゾンビプロセスそのものは動作していませんが、システムリソースを無駄に消費している良くない状態です。
システムで新たなプロセスを起動することができなくなる要因になることもあります。
通常値は、1をお勧めしますが、システムの状況により適切な値を決定し、設定してください。

(13) 任意のプロセス数

プロセスには、crondのように１つだけ起動されるものもあれば、
httpdのようにある数の範囲内で起動されるものもあります。
１つだけ起動されるプロセスが二重起動されていたり、あるいは１つも起動されていない（サービスダウン）場合や
ある範囲の数で起動されるプロセスがこの範囲外で起動されている場合は、正常な運用ができなくなることが
あります。
プロセスごとの適切な下限数と上限数（どちらか１つでも可）を設定してください。

●設定の流れ

異常時にメールを送信したい

→ 「自己監視」－「基本設定」で送信先メールアドレスなどを設定します。

サーバーのリソース（メモリ、ディスク）を監視したい

→ 「自己監視」－「リソース監視」でしきい値や異常時に実行させるスクリプトを設定します。

サーバーの負荷を監視したい

→ 「自己監視」－「パフォーマンス監視」でしきい値や異常時に実行させるスクリプトを設定します。

ログインユーザー数を監視したい

→ 「自己監視」－「ログイン監視」でしきい値や異常時に実行させるスクリプトを設定します。

総プロセス数やゾンビプロセス数などを監視したい

→ 「自己監視」－「プロセス監視」でしきい値や異常時に実行させるスクリプトを設定します。

任意のプロセス数を監視したい

→ 「自己監視」－「任意のプロセス監視」で監視する
プロセス名、しきい値、異常時に実行させるスクリプトを設定します。

監視した結果を時系列グラフとして表示できるようにしたい

→ 「グラフレポート」－「初期化」で「設定する」をクリックして初期化します。
既に初期化されている場合はこの操作は必要ありません。

自己監視の設定をもとにサーバーの自動監視を開始したい

→ 「自己監視」－「自己監視サービスの状態」で自己監視サーバー、自己監視補助サーバーを起動します。

自己監視により検知されたアラートを確認したい

→ 「ログ管理」－「ログ閲覧」でログ監視のアラートログを選択し、「表示」をクリックします。

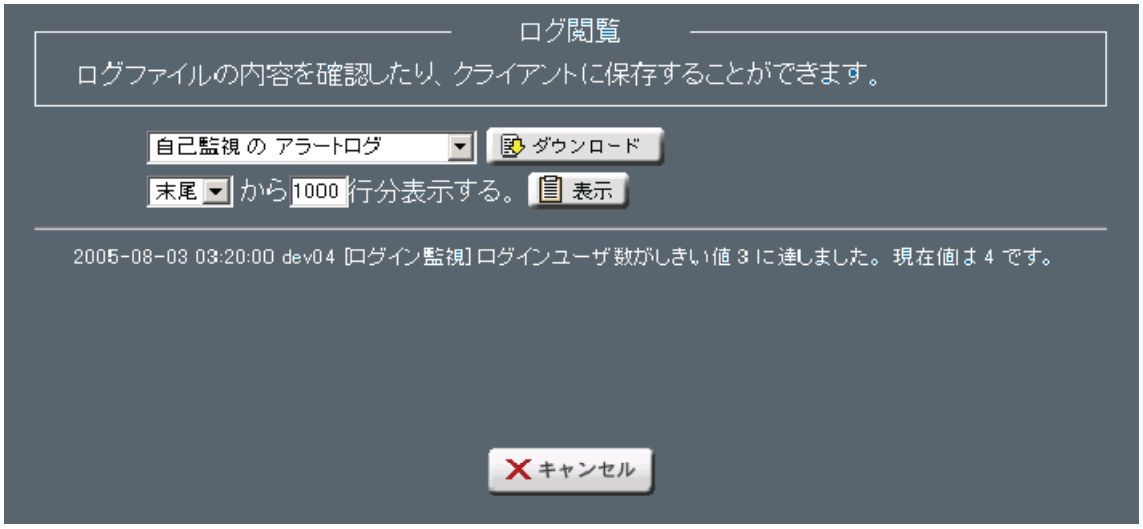
現在までのサーバーの状況を確認し、しきい値を見直したい
→ 「グラフレポート」で確認したい監視項目に該当するレポートをクリックします。

現在のサーバーの状況を確認したい
→ 後述のシステム管理者によるサーバー監視を参照してください。
必要に応じてしきい値や異常時に実行させるスクリプトを見直し、それぞれの設定画面で変更します。
なお、変更したしきい値などは次回の監視時刻から有効になります。

変更した値を有効にするために、自己監視デーモンや自己監視補助デーモンを再起動する必要はありません。

●アラートの確認
→しきい値を超えた場合、アラートログが出力されます。
このログを確認することにより、しきい値を超えた監視項目とその時の値などを知ることができます。
サーバーが不安定になる前にパフォーマンス低下やリソース不足などの予兆を検出・対処することでサーバーを安定稼動できます。

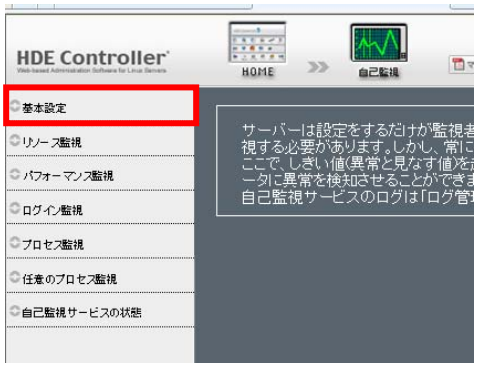
「ログ管理」－「ログ閲覧」を選択します。



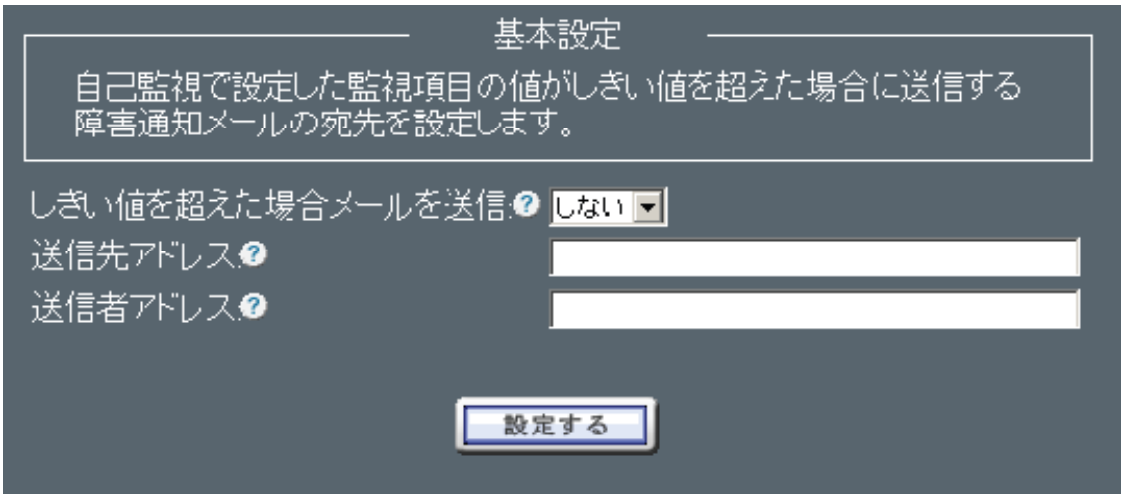
プルダウンメニューから、「自己監視のアラートログ」を選択して「表示」をクリックします。
自己監視のアラートログが表示されます。

※異常時に実行させるスクリプトはLinux上で実行可能である必要があります。

●基本設定



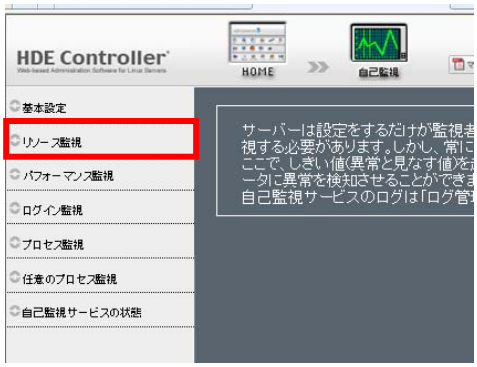
しきい値を超えた場合メールを送信する、または、送信しないよう設定します。
メールを送信すれば、携帯電話や PDA などでもサーバーの状況を把握できます。



しきい値を超えた場合メールを送信するか否か、「送信先アドレス」欄へ送信する場合は
送信先メールアドレスの入力
送信者メールアドレスを変更したい場合は「送信者アドレス」欄へ入力します。
（空欄の場合は root@localhost となります）

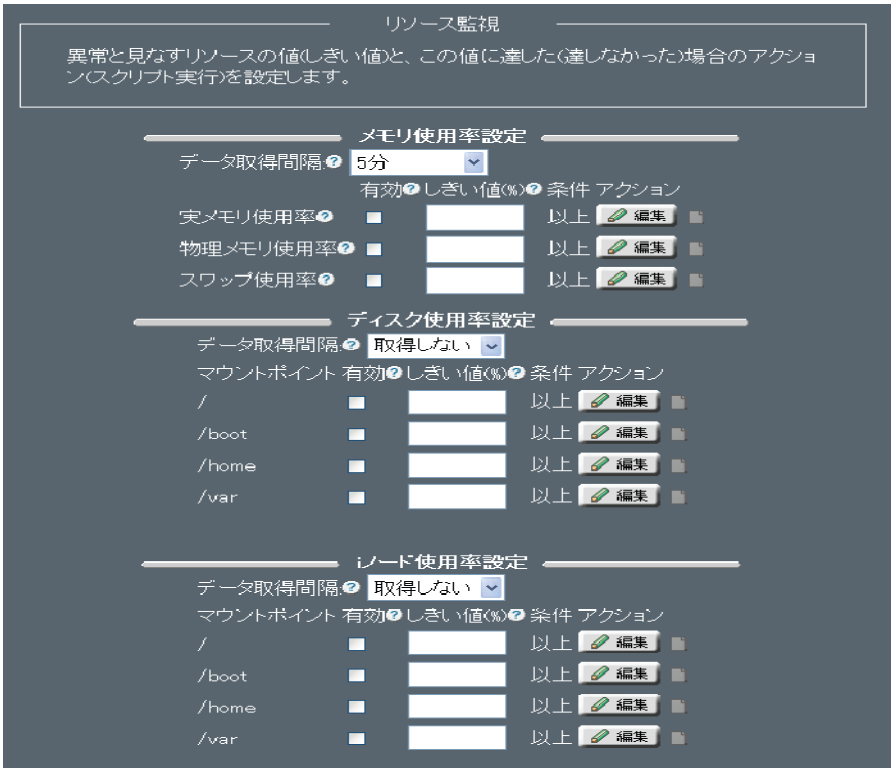
「設定する」をクリックします。
メールを送信する設定を行った場合、しきい値を超えるたびにメールを送信します。
このため、状況が変わらなければ大量にメールされることになりますのでご注意ください。

●リソース監視



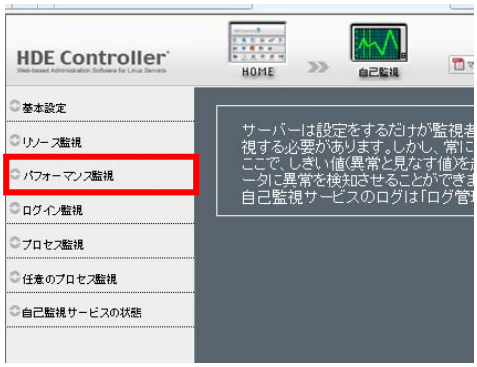
選定した監視項目などをもとに、以下のものについて、監視を有効にするか否か、
しきい値などを設定します。

- 実メモリ使用率
- 物理メモリ使用率
- swap 使用率
- ディスク使用率
- ｉノード使用率



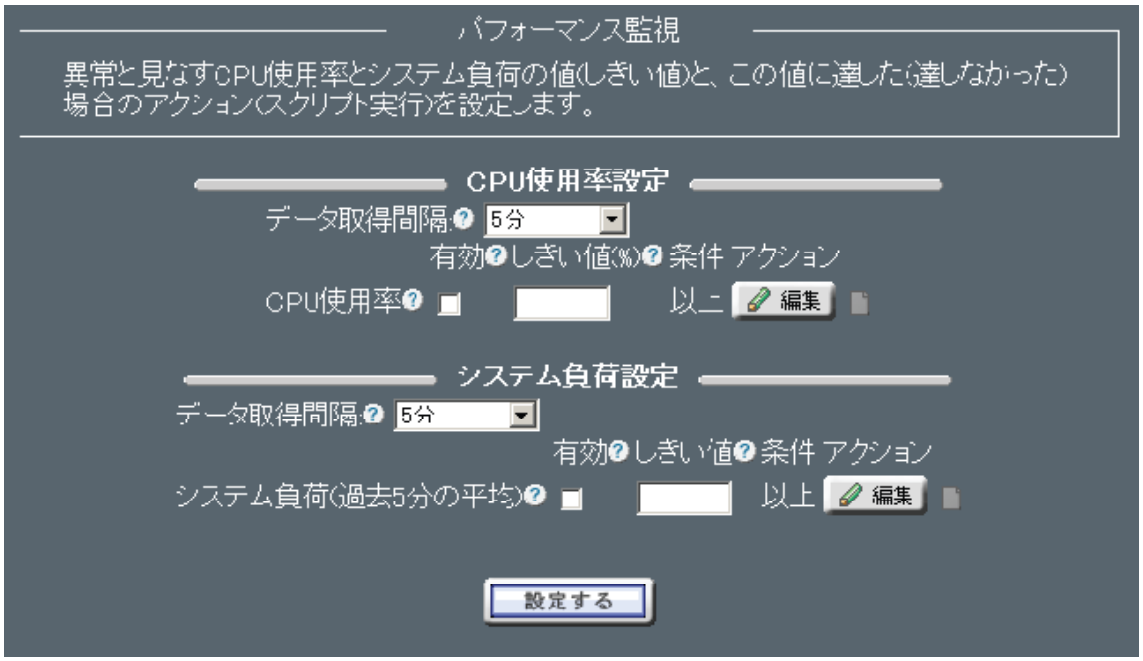
監視を有効にするか否か、しきい値を設定します。
更に、「編集」をクリックすると、しきい値を超えた場合の
アクション（スクリプト）を設定することもできます。
「設定する」をクリックします。

●パフォーマンス監視



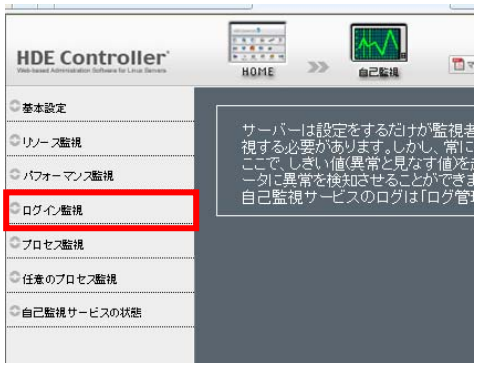
選定した監視項目などをもとに、以下のものについて、
監視を有効にするか否かや、しきい値などを設定します。

- CPU 使用率（データ取得間隔での平均値）
- システム負荷（過去５分間の平均値）

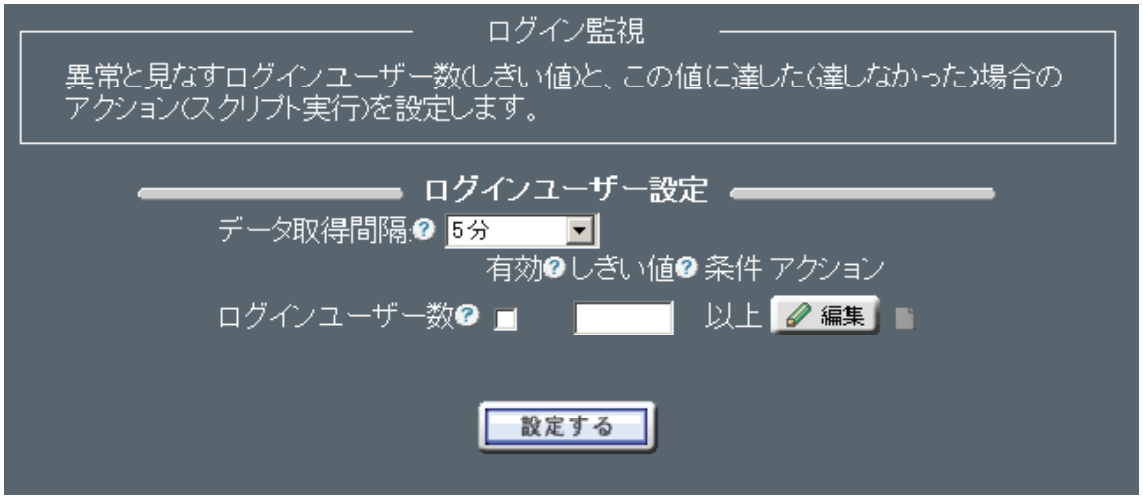


監視を有効にするか否か、しきい値を設定します。更に、「編集」をクリックすると、しきい値を超えた場合のアクション（スクリプト）を設定することもできます。
「設定する」をクリックします。

●ログイン監視

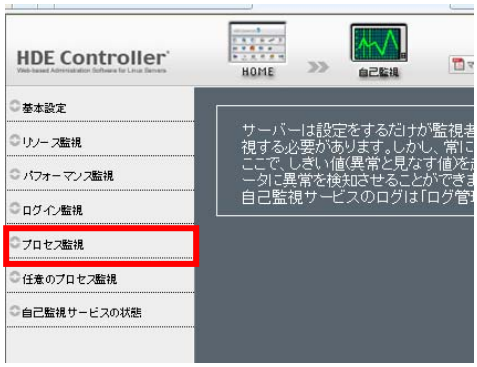


選定した監視項目などをもとに、ログインユーザー数について、
監視を有効にするか否かや、しきい値などを設定します。



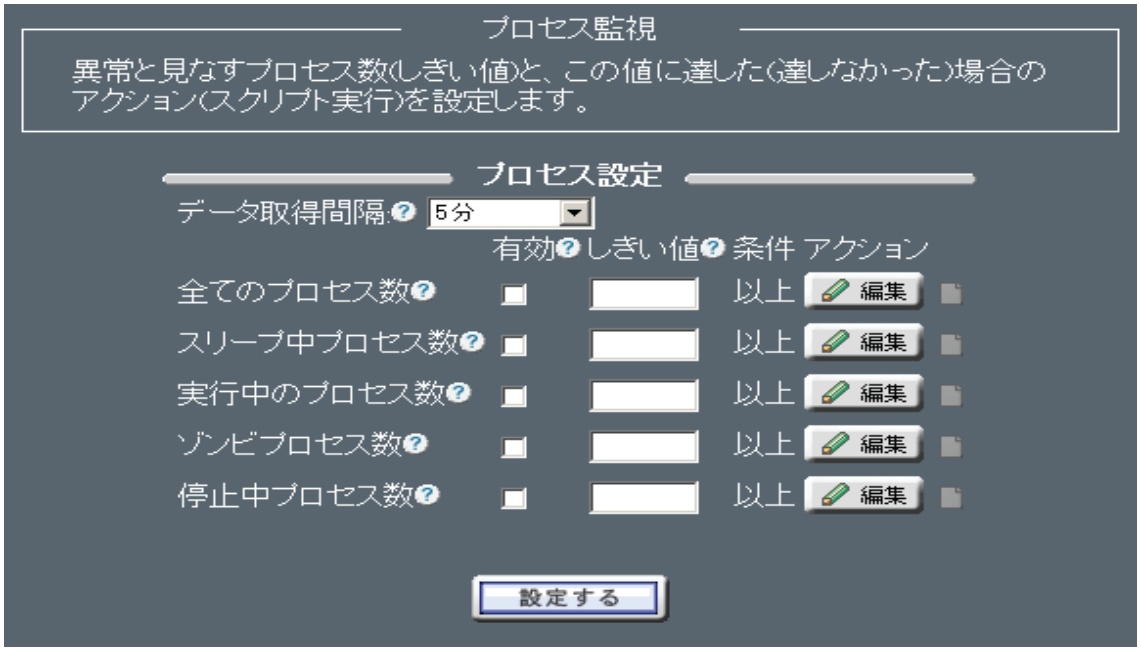
監視を有効にするか否か、しきい値を設定します。
更に、「編集」をクリックすると、しきい値を超えた場合のアクション（スクリプト）を設定することもできます。
「設定する」をクリックします。

●プロセス監視



選定した監視項目などをもとに、以下のものについて、監視を有効にするか否か、
しきい値などを設定します。

- 全てのプロセス数
- 実行中プロセス数
- スリープ中プロセス数
- 停止中プロセス数
- ゾンビプロセス数

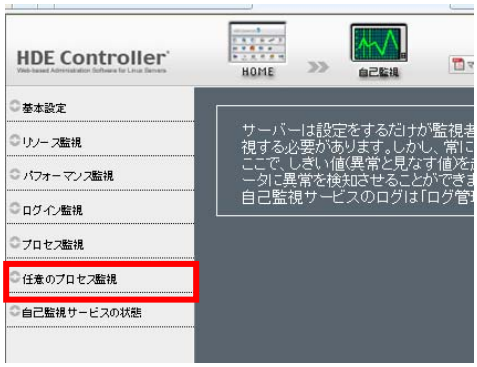


監視を有効にするか否か、しきい値を設定します。

さらに「編集」をクリックすると、しきい値を超えた場合の
アクション（スクリプト）を設定することもできます。

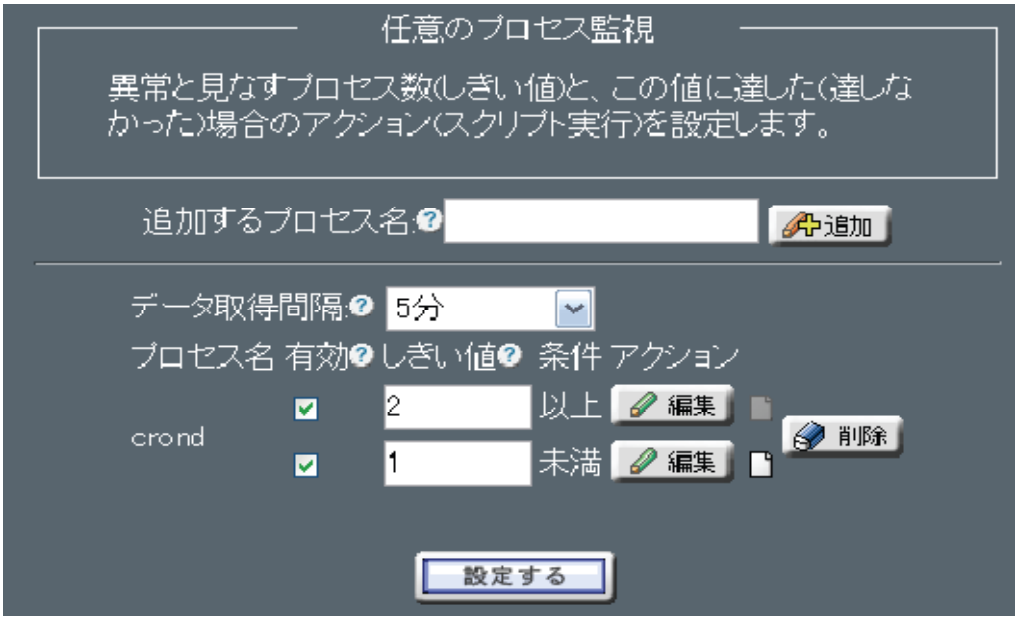
「設定する」をクリックします。

●任意のプロセス監視



選定した監視項目などをもとに、監視すべきプロセス名を追加し、
監視を有効にするか否か、しきい値などを設定します。

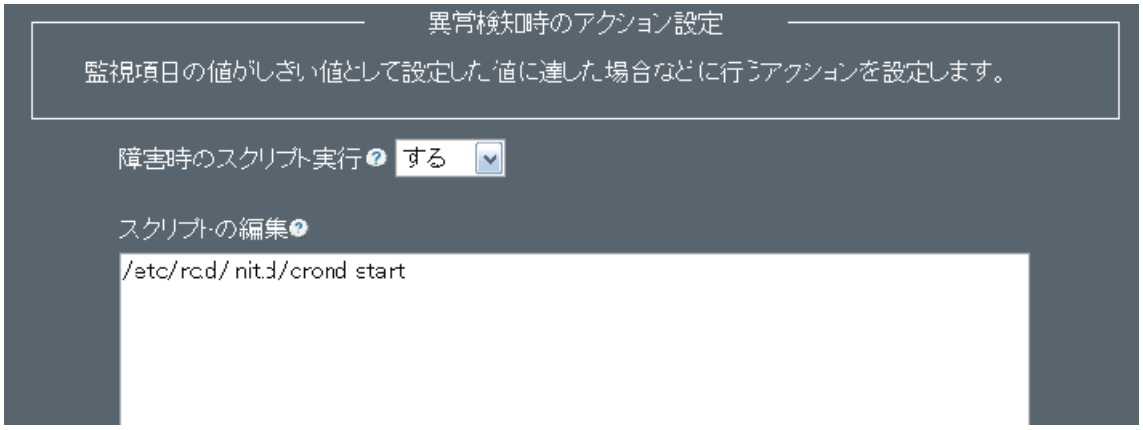
プロセスごとにプロセス数の上限と下限を設定できます。



例えば、crond のように 1 つだけ起動されるものについては、
上限に 2、下限に 1 を設定すれば、
該当プロセス数が 2 以上または 1 未満(0)になると異常とみなすことができます。

そして、1 未満(0)の場合に以下のようなスクリプトを設定しておくと、
crond を起動することもできます。

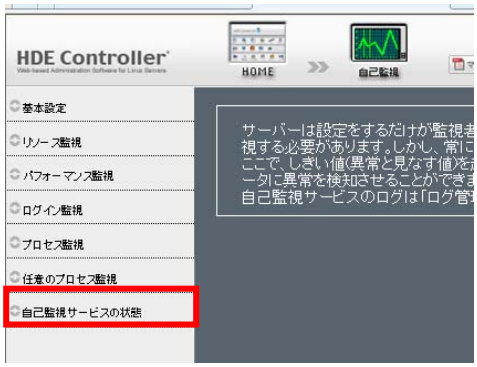
crond を起動するスクリプトの例
/etc/rc.d/init.d/crond start



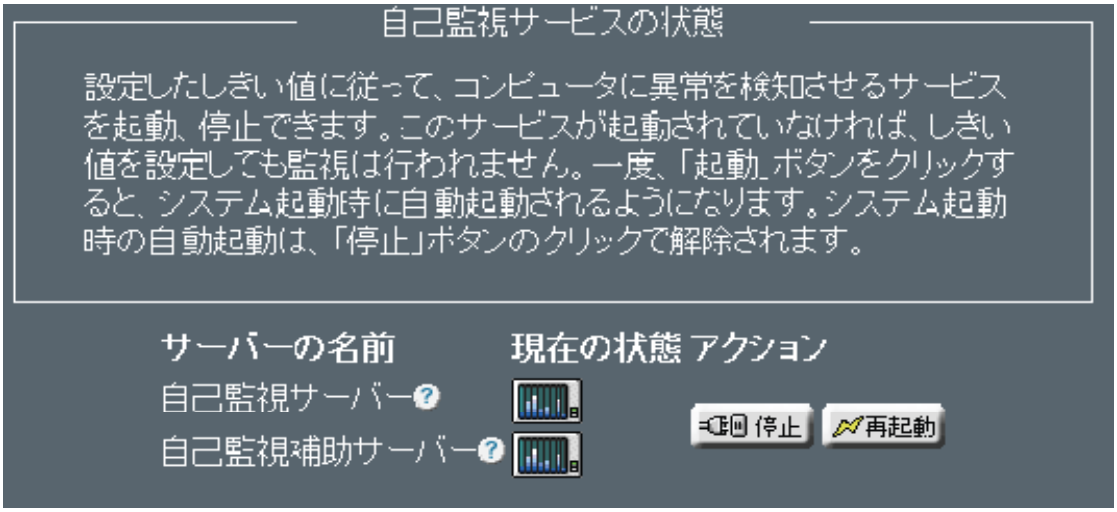
「自己監視」－「任意のプロセス監視」を選択します。
監視するプロセス名を「追加するプロセス名」に入力し、「追加」をクリックします

監視を有効にするか否か、しきい値を設定します。
さらに、「編集」をクリックすると、しきい値を超えた場合のアクション（スクリプトの実行など）を設定することもできます。
「設定する」をクリックします。

●自己監視サービスの状態



設定したしきい値に従って、コンピューターに異常を検知させるサービスを起動、停止します。
このサービスが起動されていなければ、しきい値を設定しても自己監視は行われません。
一度、「起動」をクリックすると、システム起動時に自動起動されるようになります。
システム起動時の自動起動は、「停止」のクリックで解除されます。



「起動」、「再起動」、または、「停止」をクリックします。

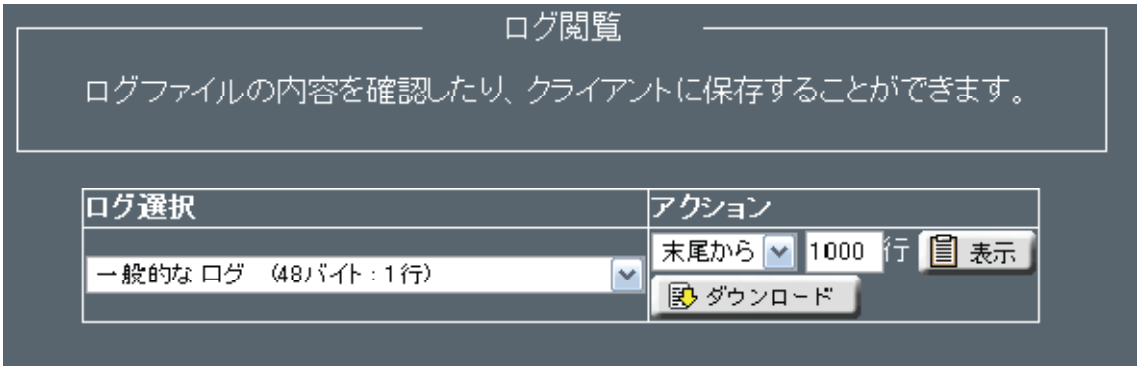
３．ログ管理

３－１．概要

HDE Controller にログインし、「ログ管理」のアイコンをクリックします。
次項の項目に従って設定及び確認を実施してください。

３－２．ログ閲覧

各サービスが記録したログファイルを管理します。
「ログ閲覧」のメニューをクリックすると、ログ閲覧画面が表示されます。



ログファイルの内容を表示します。
またクライアント側にダウンロードしてログを保存することができます。

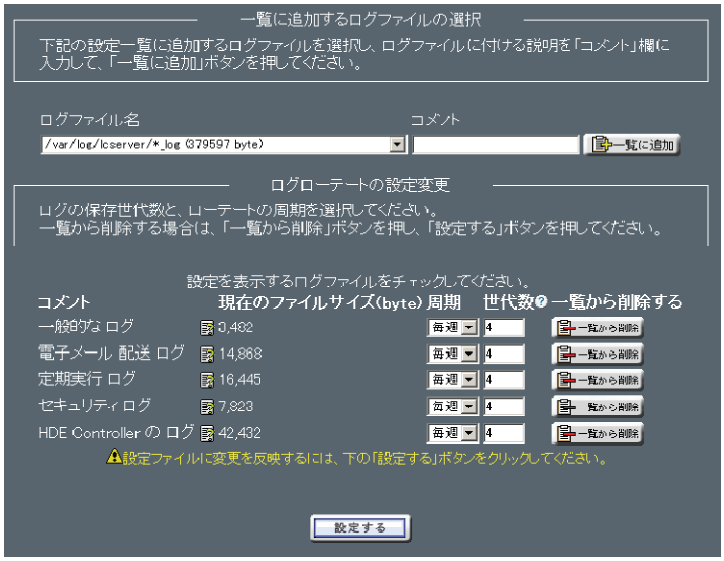
プルダウンメニューより閲覧したいログファイルを選択します。

次に、プルダウンメニューより「先頭」もしくは「末尾」からのログファイルの行数を指定します。

「ダウンロード」または「表示」を選択し、ログをダウンロードまたは閲覧します。

●ログローテート

「ログローテート」メニューをクリックすると「ログローテート」設定画面が表示されます。



ログの一覧に、新たにログファイルを追加する場合は、「ログファイル名」から追加するログを選択します。

ログの説明などを「コメント」に入力します。

「一覧に追加」をクリックして追加します。

ファイルの保存世代数と保存周期を変更する場合、各ログの「周期」から保存周期を選択し、「世代数」に保存するファイルの世代数を入力します。

コメントの右側に表示されている、ファイルのアイコンにマウスカーソルを重ねると、ログファイルの保存されているパスが表示され、確認することができます。

ログ一覧から、追加したログを削除する場合は「一覧から削除」をクリックします。

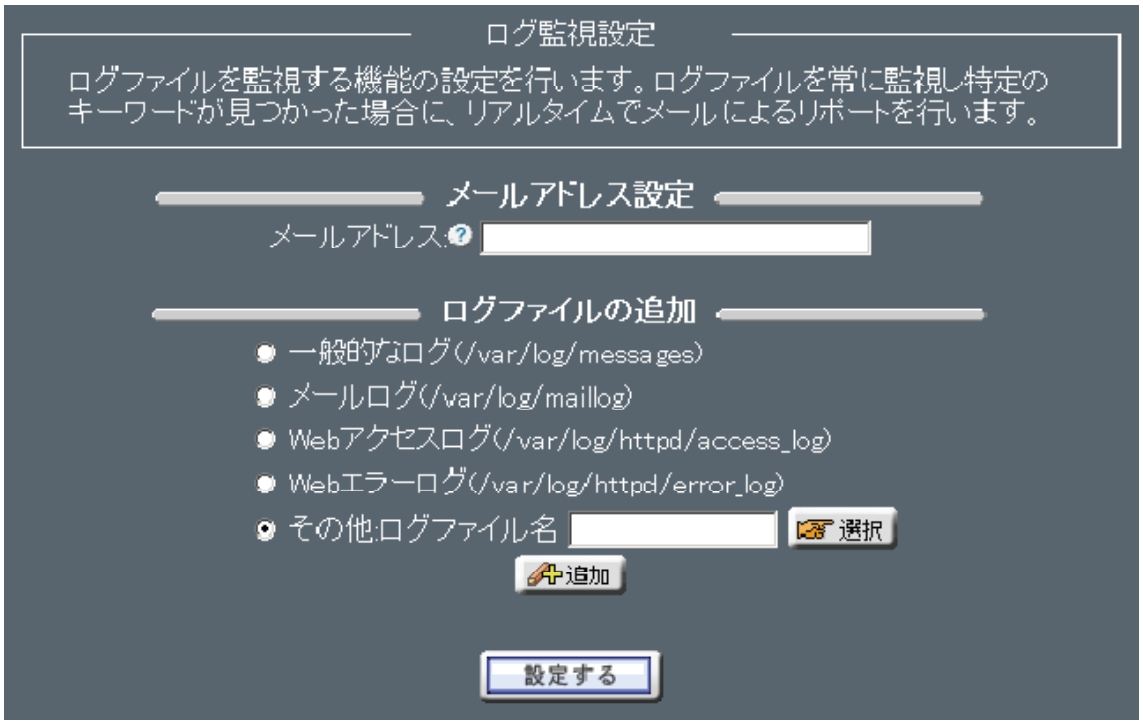
「設定する」をクリックして設定を終了します。

●ログ監視

Linux で Web サーバーなどを稼動させている場合
バックグラウンドで実行された結果はすべてログファイルに記録されます。

何か障害が起きた場合の原因究明や日々のサーバーの利用状況の調査、悪意のあるクラッカーからのアクセスの解明などログファイルの監視は様々な用途に応用でき、サーバーの運用管理には欠かせない機能となっています。

ログ監視設定では logsurfer を用いたログ監視の設定を行うことができます。
logsurfer は常にログの監視を行い、特定のキーワードを検出するとその結果をリアルタイムでメールによるレポートを行います。



●メールアドレス設定
「メールアドレス」にメールアドレスを指定します。
ここで登録されたメールアドレスに対してレポート結果がリアルタイムで送信されます。

●ログファイルの追加

監視する対象のログファイルの追加を行います。

既にいくつかの典型的なログファイルが選択肢にありますのでこの中から選ぶか、あるいはログファイル名を直接指定します。

「追加」をクリックしログファイルを追加してください。

ログファイルを追加するとルールの編集画面になります。

●ルールの設定

監視するログファイルに対するルールの追加・編集を行います。

ここで指定したルールが上から順に評価され、ルールにマッチするとアクションが実行されます。

一度ルールが評価されるとそれ以降のルールは評価されません。

ここで指定されたルールはログファイルの 1 行毎に評価されます。

ルールには「マッチする正規表現」「マッチしない正規表現」「アクション」の 3 つの要素があります。

それぞれの要素は以下のようになります。

●マッチする正規表現
マッチするための正規表現を指定します。
ここで指定した正規表現にマッチした行が見つかるとアクションが実行されます。

●マッチしない正規表現
マッチさせたくない正規表現を指定します。
「マッチする正規表現」でマッチしてもここで指定した正規表現がマッチした場合、
アクションは実行されません。
″-″（ハイフン）または空文字(何も入力しない)にすると何も指定しません。

●アクション
アクションには「無視」「メール送信」の 2 種類あります。

「無視」
何もしません。
以降のルールを適用させたくない場合に使用します。

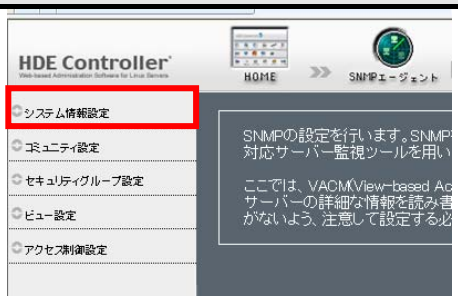
「メール送信」
メールを送信します。
マッチした行の内容が送信されます。

4. SNMP エージェント

４－１．システム情報設定

HDE Controller にログインし、「SNMP エージェント」のアイコンをクリックします。
次項の項目に従って設定及び確認を実施してください。

４－２．システム情報設定



SNMP(Simple Network Management Protocol)は、ネットワーク機器を管理するための規約で、多くのベンダーが SNMP に対応した機器を開発しています。

SNMP を用いたネットワーク管理は、管理する側(マネージャー)と管理される側(エージェント)で構成されます。

エージェントは、管理情報データベース(MIB)にエージェントの情報を保存します。
なお、MIB には様々なものがあり、機器によって管理する情報が異なるため、どの MIB をサポートしているかは
エージェントに依存します。

マネージャーは、エージェントと通信して MIB を取得し、グラフ表示するなどしてネットワーク機器を管理します。

HDE Controller は、サーバーを SNMP エージェントとして利用するための設定を行います。

SNMP エージェントとして、各ディストリビューションに含まれる net-snmp パッケージを利用します。

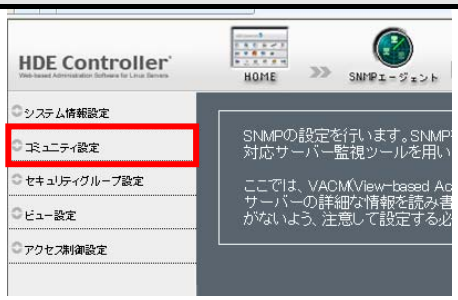
このため、SNMP エージェントがサポートする MIB については、各ディストリビューションの net-snmp パッケージを
ご確認ください。

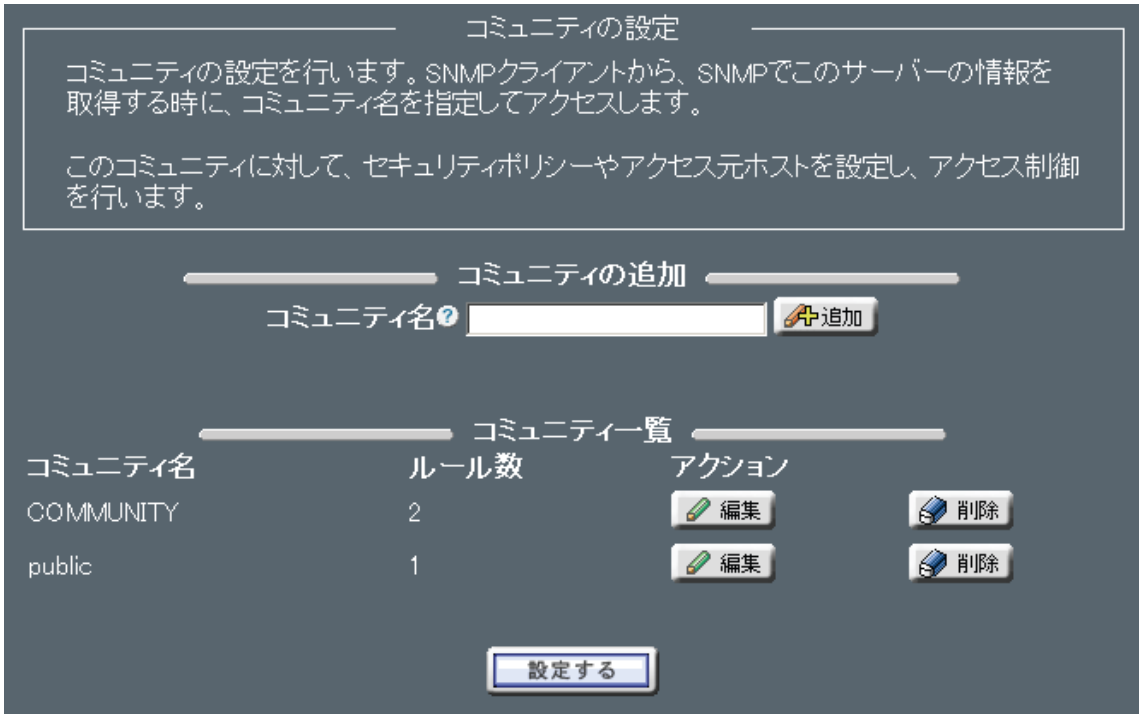
ここでは、システムの所在などを示すロケーション情報、システム管理者の名前やメールアドレスなどの
管理者情報を設定します。

システム情報設定
MIB をアクセスすることにより、ここで設定した内容を取得できます。
システムロケーション情報は.1.3.6.1.2.1.1.6.0、
　　管理者情報は.1.3.6.1.2.1.1.4.0 という MIB から取得できます。

ロケーション情報にシステムの所在などを、管理者情報にシステム管理者の名前やメールアドレスを指定し、
「設定する」をクリックします。

４－３．コミュニティ設定

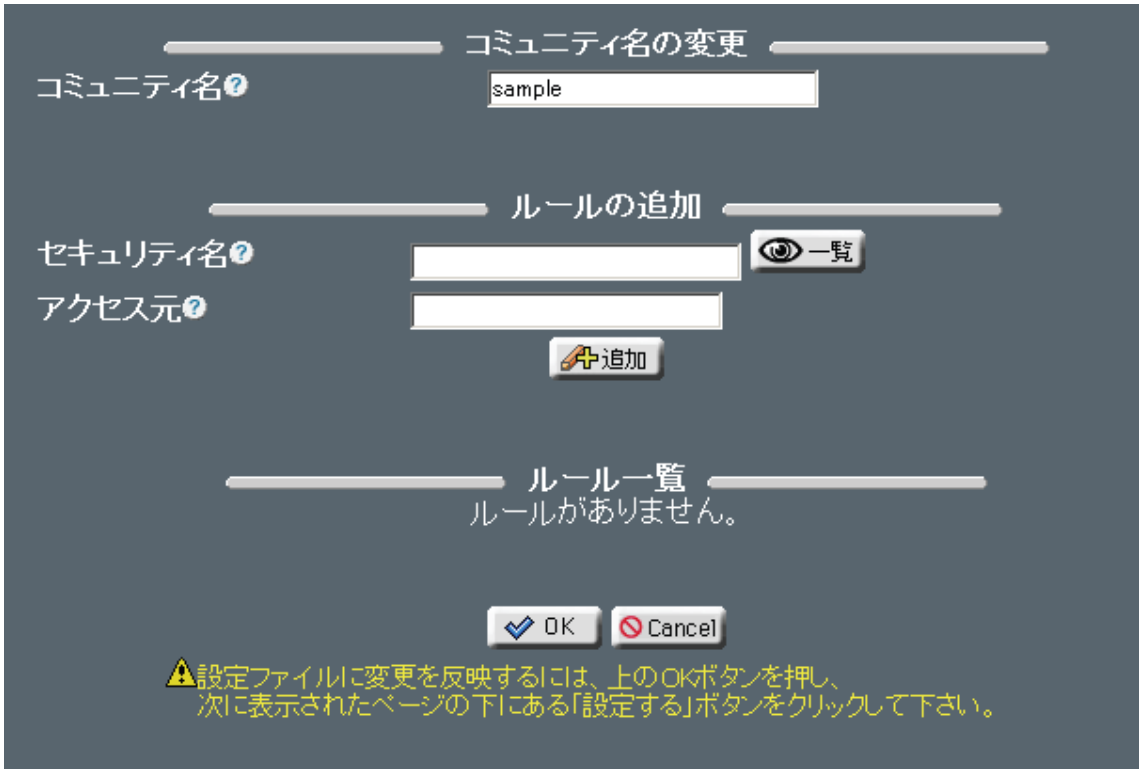




ここで設定したコミュニティ名は、

SNMP マネージャーから SNMP エージェントの MIB にアクセスする際に使用します。

コミュニティ名を入力し、「追加」をクリックします。

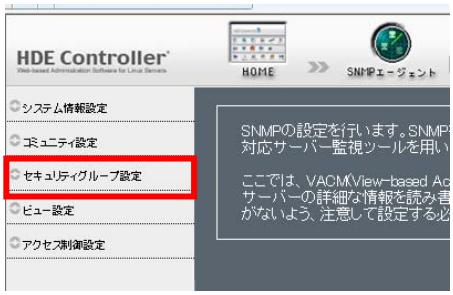


このコミュニティ名を許可するアクセス元をルールとして追加します。
ルールとして、「セキュリティ名」には任意の文字列を、「アクセス元」には SNMP マネージャーのアドレスを入力し、「追加」をクリックします。

ルールの有効がチェックされていることを確認してください。
また、不要なルールが設定されている場合は、有効のチェックを外してください。
確認したら「OK」をクリックします。

コミュニティ名の設定画面に切り替わったら、「設定する」をクリックします。

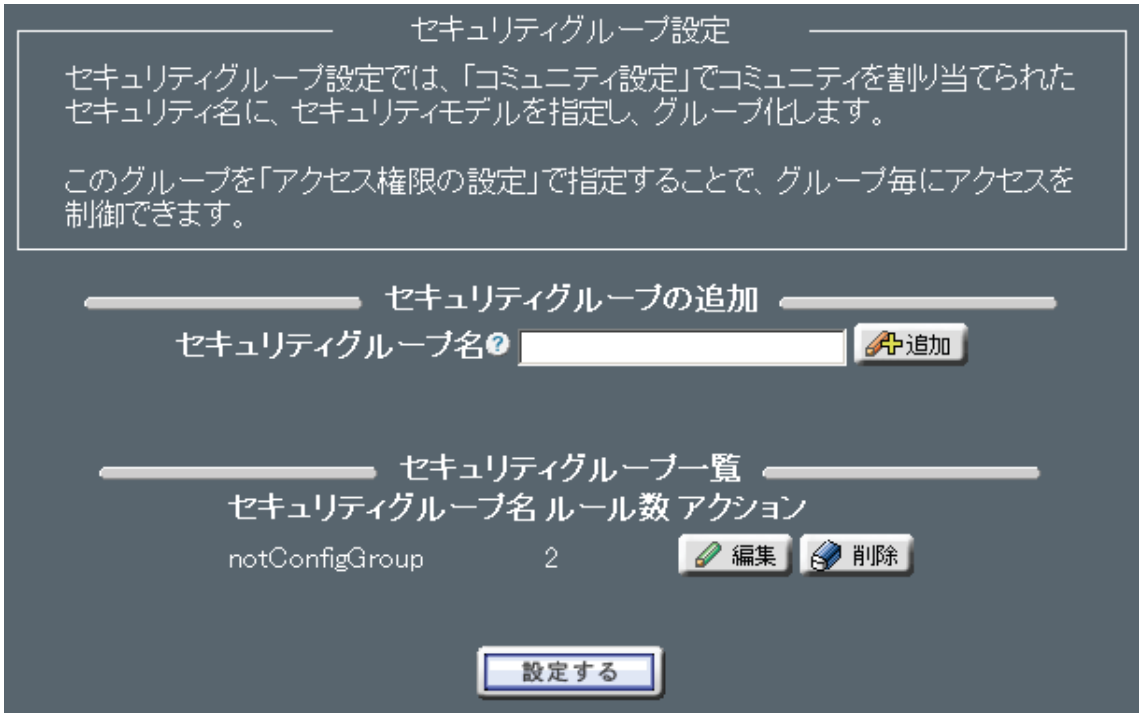
４－４．セキュリティグループ設定



ここでは、コミュニティ設定で割り当てたセキュリティ名と、SNMP マネージャーと通信する際のセキュリティモデル(v1,v2c など)を対応付けたルールを、セキュリティグループとして割り当てます。

※SNMP マネージャーがサポートするセキュリティモデルを指定していないと SNMP による監視は行えません。
　よく知られている SNMP マネージャーの多くは、v1、v2c のいずれか、または、両方をサポートします。

セキュリティグループ名を入力し、「追加」をクリックします。

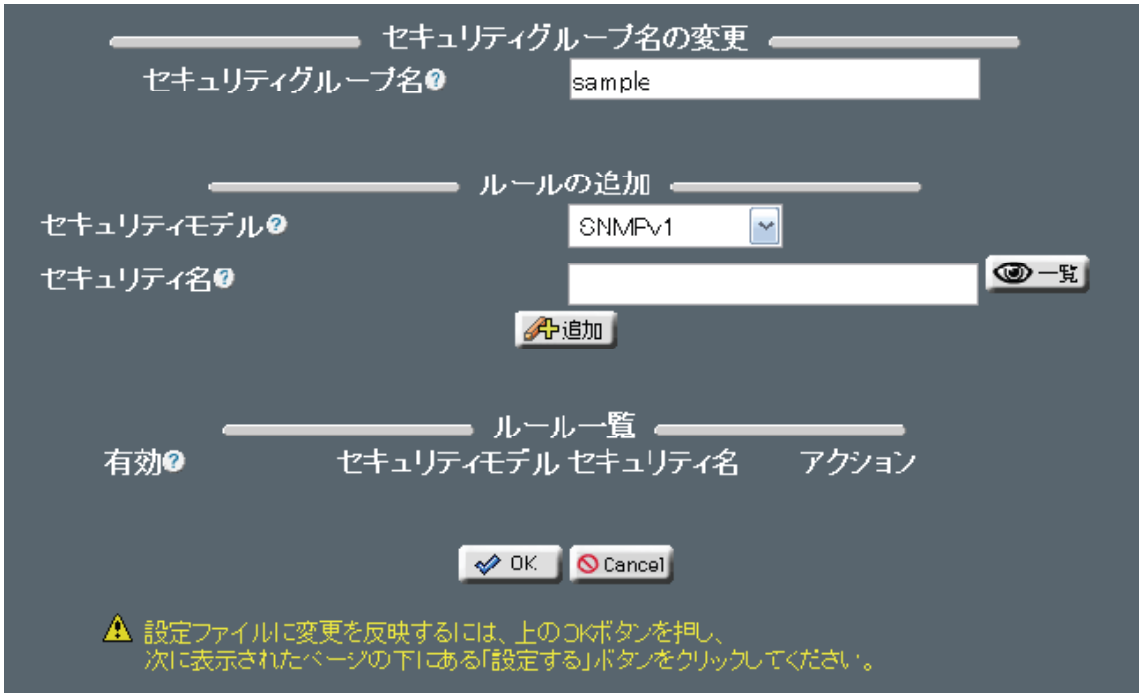


ルールの追加で、このセキュリティグループで利用できるセキュリティモデルをプルダウンメニューから選択、セキュリティ名を入力し、「追加」をクリックします。

セキュリティ名はコミュニティ設定で指定したものを入力します。
「一覧」をクリックすることにより、設定されているセキュリティ名を表示、選択することもできます。

設定したルールの「有効」がチェックされていることを確認してください。
また、不要なルールが設定されている場合は、「有効」のチェックを外してください。

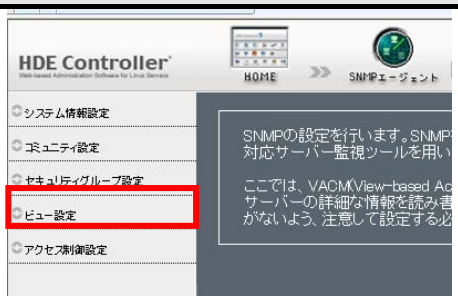
確認したら「OK」をクリックします。



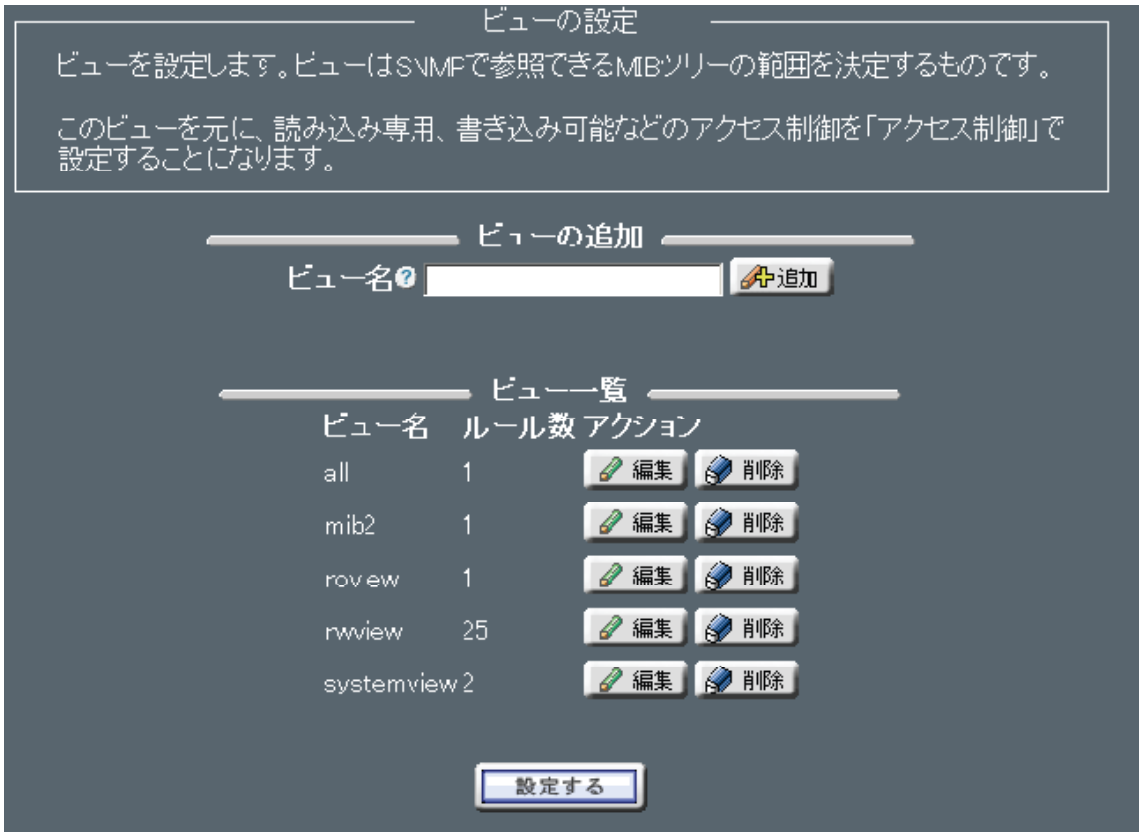
セキュリティグループ設定画面に切り替わったら、「設定する」をクリックします。

セキュリティグループの編集を行う場合は、該当するグループ名の
編集ボタンを押し、編集を行います。

４－５．ビュー設定



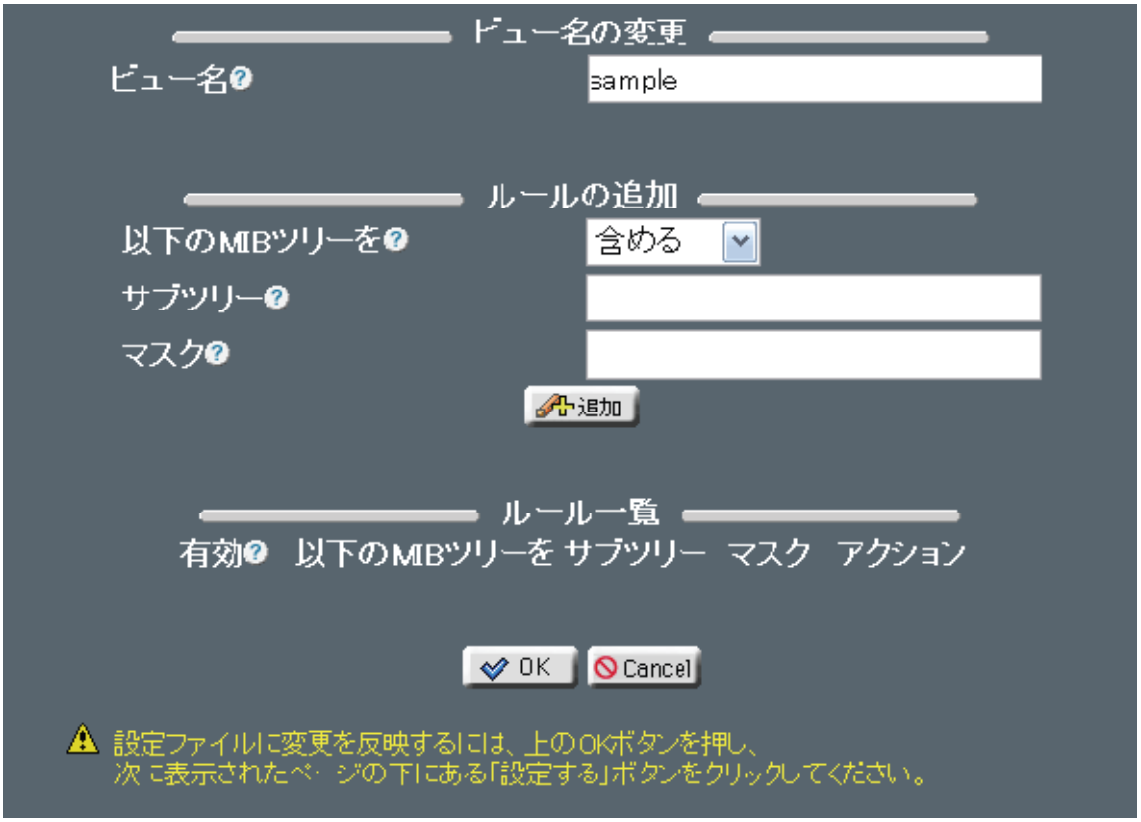
ここでは、SNMP マネージャーからアクセス可能な MIB の範囲をビュー名として設定します。



ビューの追加で、ビュー名を入力し、「追加」をクリックします。

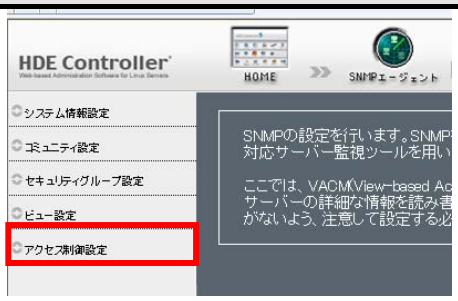
ルールの追加で、以下の MIB ツリーを含めるか、除外するをプルダウンメニュー
から選択し、サブツリーと必要に応じてマスクを入力し、「追加」をクリックします。
設定したルールの「有効」がチェックされていることを確認してください。
また、不要なルールが設定されている場合は、「有効」のチェックを外してください。

確認したら「OK」ボタンをクリックします。



ビューの設定画面に切り替わったら、「設定する」をクリックします。

４－６．アクセス制御設定



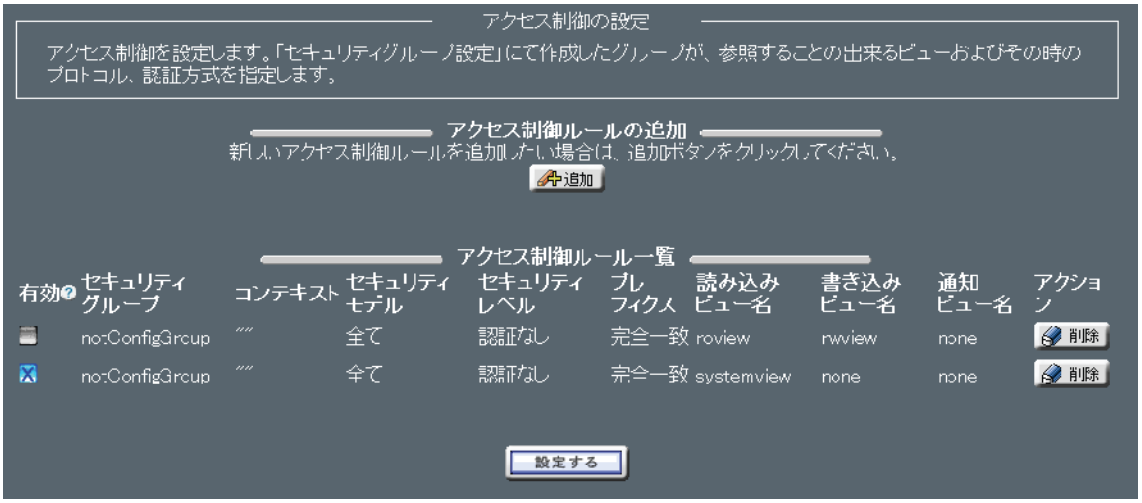
ここでは、

コミュニティ設定

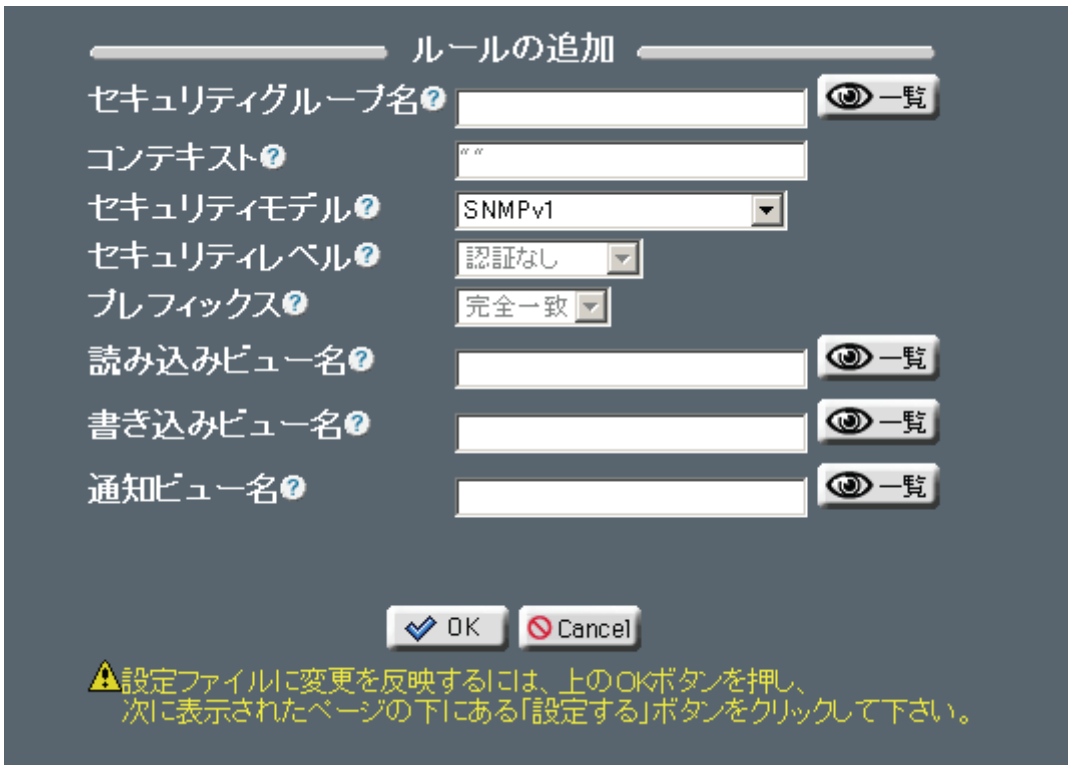
セキュリティグループ設定

ビュー設定

などで割り当てた内容を用いてセキュリティグループごとのアクセス制御を設定します。



アクセス制御ルールの追加で、「追加」をクリックします。



ルールの追加で、アクセス制御の設定対象となる「セキュリティグループ名」を入力します。

引き続き、
「セキュリティモデル」
「読み込みビュー名」
「書き込みビュー名」
「通知ビュー名」を指定します。

なお、SNMP マネージャーから全ての MIB を参照できる(書き込みや通知は不可)ようなアクセス制御を設定する場合は、書き込みビュー名と通知ビュー名は none を指定します。

セキュリティモデルに、SNMP マネージャーがサポートするものが指定されていないと SNMP による監視は行えません。

マイサーバーサービス 利用マニュアル
(グラフレポート / 自己監視 / ログ管理 / SNMP)
マイサーバーVPS compact

発行元：株式会社イージェーワークス
発効日：2010 年 7 月 9 日　rev1

リムネット カスタマーサポートセンターの連絡先

電 話 窓 口：0120-678-309
ファックス：045-472-2777
メ　ー　ル：support@rim.or.jp
受 付 時 間：24 時間 365 日