WebSAM SigmaSystemCenter 3.5
簡易構築ガイド

~ VMware 編 ~

ー第１版ー

免責事項

商標

目次

はじめに

エンタープライズコンピューティングの分野において、この数年間で最も大きな変化の1つが「仮想化」です。メインフレームなどの大規模コンピュータでは以前から仮想化技術が使われていましたが、ハードウェアの高性能化により現在では一般的なPCサーバでも仮想化技術が使えるようになりました。仮想化はコンピュータリソースを“プール”として抽象化するために必須の技術となりつつあり、これをうまく導入することで企業は自社のリソースを効率よく分配することが可能になります。

一方、システム管理者にとって仮想化技術の導入は、管理レイヤの増加も意味します。管理レイヤが増えて管理の手間が増えるようでは、仮想化の導入メリットも半減してしまいます。

この文書では、「VMware vSphere」と管理ツールの「WebSAM SigmaSystemCenter 3.5」（SSC）を用いて、仮想マシンシステムを構築する手順を紹介します。SigmaSystemCenterは仮想化に対応した統合管理プラットフォームであり、物理的なサーバで動作するホストと仮想マシンを単一のコンソールから統一的に管理することが可能です。

対象読者と目的

「WebSAM SigmaSystemCenter 3.5 簡易構築ガイド」は、SigmaSystemCenter により仮想化サーバと仮想マシンを管理するシステムの構築、運用するために必要な最低限の知識と手順に限って説明しています。よって、本書では SigmaSystemCenter の全ての機能、役割について説明しておらず、本書で説明する以外の機能の利用、応用については、「付録 B SigmaSystemCenter マニュアル体系」で紹介のドキュメントをお読みください。

本書の表記規則

本書では以下の表記法を使用します。

表記	使用方法	例
[ ] 角かっこ	画面に表示される項目 (テキストボックス、チェックボックス、タブなど) の前後	[マシン名] テキストボックスにマシン名を入力します。 [すべて] チェックボックス
「」 かぎかっこ	画面名 (ダイアログボックス、ウィンドウなど)、他のマニュアル名の前後	「設定」ウィンドウ 「インストレーションガイド」
コマンドライン中の [ ] 角かっこ	かっこ内の値の指定が省略可能であることを示します。	`add [/a] Gr1`
モノスペースフォント (courier new)	コマンドライン、システムからの出力 (メッセージ、プロンプトなど)	以下のコマンドを実行してください。 `replace Gr1`
モノスペースフォント斜体 (*courier new*)	ユーザが有効な値に置き換えて入力する項目 値の中にスペースが含まれる場合は "" (二重引用符) で値を囲んでください。	`add` *`GroupName`* `InstallPath=”`*`Install Path`*`”`

1. お使いになる前に

[重要] トラブルを避けるため、SSCをお使いになる前に、「付録 A 運用に関する重要な情報」をよくお読みください。

1.1. 本ガイドで実現するシステム

本書で構築するシステムでは、以下の機能を実現することを目標とします。

- 障害監視をする。
  以下の対象の障害を監視します。
  - 業務用仮想マシン
  - 物理サーバ（ESXi）

- 負荷監視をする。
  以下の対象の負荷を監視します。
  - 業務用仮想マシン
  - 物理サーバ（ESXi）

- 予兆障害を契機にvMotionをする。
  物理サーバ（ESXi）の障害予兆を検出し、その上で動作する以下の仮想マシンをvMotionで別の物理サーバへ移動します。
  - 業務用仮想マシン

1.2. 構築の流れ

本書では、以下の流れでSSCの構築を行います。図の各作業の冒頭にある数字は本書の章番号になります。

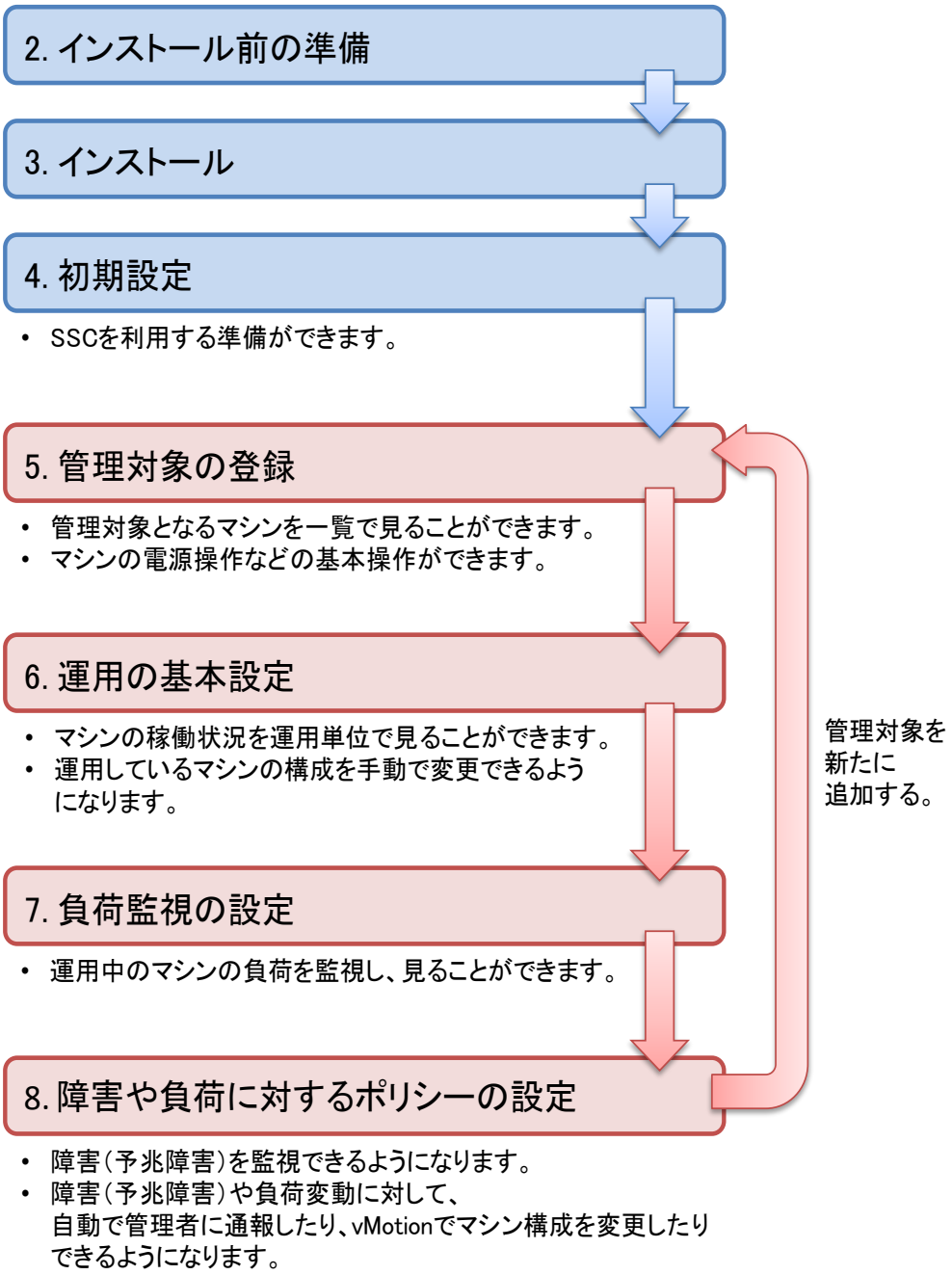

図 1 本ガイドでの構築の流れ

1.3. システム構成と使用機材

今回構築するシステムの構成は以下のとおりです。

- 管理対象サーバ
  - 物理サーバ(3台)
    - VMware ESXi
    - ホスト名:IPアドレス
      - esxi1:172.16.10.1
      - esxi2:172.16.10.2
      - esxi3:172.16.10.3
    - EXPRESSSCOPEエンジンのホスト名:IPアドレス
      - bmc1:172.16.20.1
      - bmc2:172.16.20.2
      - bmc3:172.16.20.3
  - 業務用仮想マシン(6台)
    - Windows Server 2008 R2 Standard Edtion
    - ホスト名:IPアドレス
      - VM-01:172.20.100.1
      - VM-02:172.20.100.2
      - VM-03:172.20.100.3
      - VM-04:172.20.100.4
      - VM-05:172.20.100.5
      - VM-06:172.20.100.6
- 管理サーバ(1台)
  - Windows Server 2008 R2 Standard Edtion
  - SigmaSystemCenter
  - vCenter Server
  - vSphere Client
  - ESMPRO/ServerManager
  - ホスト名:IPアドレス
    - SSCmanager:172.16.0.1

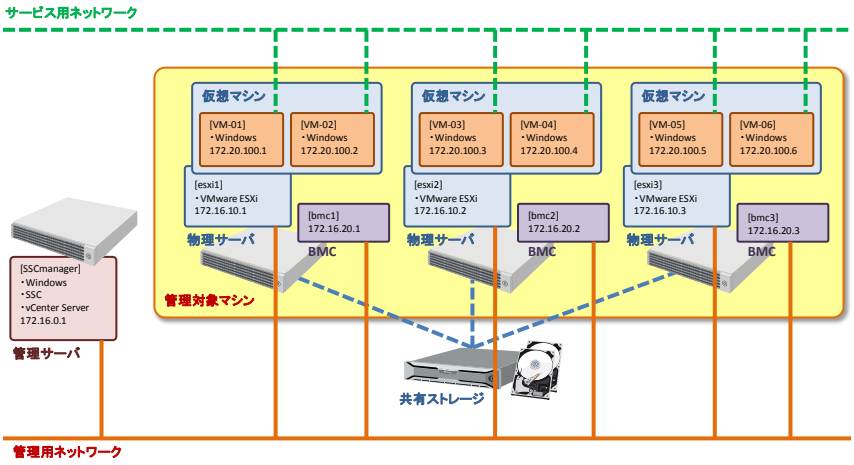

図 2 今回構築するシステムの構成

上記のように、3台のラックサーバ上で6台の業務用の仮想マシンを運用します。仮想マシンは7台でも8台でもかまいませんが、仮想マシンの必要とするリソースが物理サーバのキャパシティを超えないようにサイジングには十分注意する必要があります。

2. インストール前の準備

SSCをインストールする前に行う準備を説明します。SSCをインストールする前の準備には、大きく分けて「管理サーバの準備」、「管理対象（物理サーバと仮想マシン）の準備」の二種類の準備があります。

また、本ガイドでは、仮想マシンのシステムバックアップ、仮想マシンへのソフトウェア配布といったDeploymentManager(DPM)の機能の利用を想定していないため、DPMを利用するための説明は省略しています。DPMを利用する予定がある場合は、管理サーバと同一のネットワーク内にDHCPサーバを用意し、仮想マシンにDPMクライアントをインストールするなど、必要な設定を別途実施してください。

2.1. 管理サーバの準備

管理サーバには、あらかじめ以下のソフトウェアをインストールしておきます。

- vSphere Client
- vCenter Server
- ESMPRO/ServerManager

サーバに添付のESMPRO/ServerManagerのバージョンが“**6.10より前**”のバージョンの場合、 SSCに添付のESMPRO/ServerManagerをインストールしてください。

管理サーバには、以下のソフトウェアが必要です。

- .NET Framework 4.5.2
- Webサーバー (IIS)
- ASP.NET v4.0、または ASP.NET 4.5

≪管理サーバが Windows Server 2008 R2 の場合≫
管理サーバのWindows Server 2008 R2 には、事前にWindowsの[サーバー マネージャー]を使って以下の役割と機能を追加しておきます。

- Windowsに追加する役割
  Webサーバー（IIS）

  Webサーバー（IIS）にインストールする役割サービス
  ✧ **静的なコンテンツ**
  ✧ **ASP.NET**
  ✧ **IIS 管理コンソール**
  ✧ **IIS 6 メタベース互換**

管理サーバがWindows Server 2008 R2の場合、.NET Framework 4.5.2 は、SSCのインストーラからインストールされるため、別途インストールは不要です。
また、ASP.NET v4.0 は、IIS がインストールされている環境に.NET Framework 4.5.2 をインストールした際に自動でインストールされるため、別途インストールは不要です。

≪管理サーバが Windows Server 2012、Winsows Server 2012 R2 の場合≫
管理サーバのWindows Server 2012、Winsows Server 2012 R2 には、事前にWindowsの[サーバー マネージャー]を使って以下の役割と機能を追加しておきます。

- Windowsに追加する役割
  Webサーバー（IIS）

  Webサーバー（IIS）にインストールする役割サービス
  ✧ **静的なコンテンツ**

- ✧ **ASP.NET 4.5**
- ✧ **IIS 管理コンソール**
- ✧ **IIS 6 メタベース互換**

- Windowsに追加する機能
  .NET Framework 3.5 Features

管理サーバがWindows Server 2012、Winsows Server 2012 R2の場合、.NET Framework 4.5.2 は、SSCのインストーラからインストールされるため、別途インストールは不要です。
また、.NET Framework 3.5 Features の機能を追加する際には、Windows OSのインストールメディアのサイドバイサイドストア（SxS）フォルダを代替ソールパスとして指定する必要があります。

2.2. 管理対象（物理サーバと仮想マシン）の準備

管理対象のラックサーバには、最初に以下の仮想化基盤ソフトウェアをインストールしておきます。

- ESXi

次に、業務で利用する仮想マシンの作成とゲストOSのインストールを済ませておいてください。今回はマイグレーション（vMotion）を利用する関係上、仮想マシンの構成ファイル群を共有ストレージ上に配置する必要があります。

3. インストール

ここでは、SSCのインストールとそれに伴う管理サーバの設定について説明します。

3.1. SSC のインストール

管理サーバにSSCのインストールメディアをセットし、インストーラ（ManagerSetup.exe）をダブルクリックして起動します。
すべてのコンポーネントをチェックして、[実行]ボタンをクリックしてください。あとはインストールウィザードにしたがって作業を進めます。

3.2. 管理サーバの設定

3.2.1. IIS の設定

IISのhttpのポート(80)を変更します。
vCenter Serverは、デフォルトの設定でインストールした場合はポート(80)を使用します。一方、SSCが利用するIISのWebサービスも、httpのポート(80)を使用する設定がデフォルトなので競合しないようにIISのhttpのポートを変更します。
もし、vCenter Serverのインストールでポート(80)を使わない設定にした場合は、この変更作業は必要ありません。

今回は、IIS7.0のhttpポートを80から**20080**に変更することにします。
Windowsの[スタート]メニューから[管理ツール]→[インターネット インフォメーション サービス (IIS) マネージャー]をクリックします。
[インターネット インフォメーション サービス (IIS) マネージャー]画面が表示されたら、[接続]ツリービュー上で、管理サーバ名（ここでは、[***SSCmanager***]）→[サイト]→Web サイト名（ここでは、[Default Web Site]）を右クリックします。メニューから[バインドの編集]をクリックします。
[サイト バインド]ダイアログが開いたら、種類の[**http**]を選択した状態で、[編集]ボタンをクリックします。[サイト バインドの編集]ダイアログが開いたら、[ポート]に[***20080***]を入力し[OK]ボタンを押せば変更が完了します。

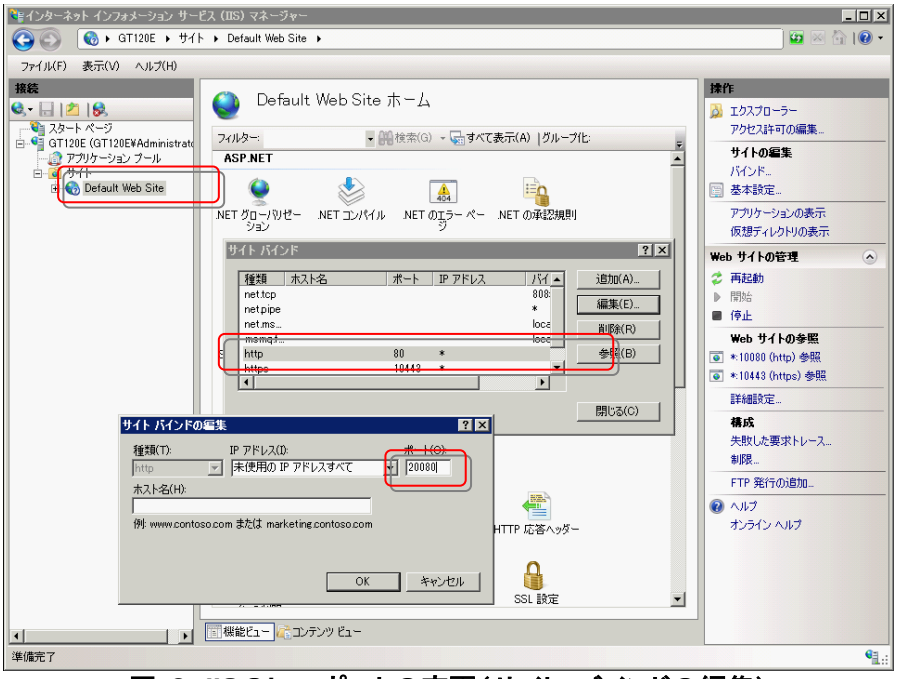

図 3 IISのhttpポートの変更（サイト バインドの編集）

3.2.2. SNMP Trap サービスの設定

SSCで管理対象の物理サーバのイベント（PET）を受け取るために、管理サーバでSNMP Trapの受信設定を確認します。

まず、ESMPRO/ServerManagerのSNMPTrapの受信方法がWindowsのSNMP Trapサービスを使用するようになっているかを確認します。
SSC管理サーバのデスクトップ上のショートカット[ESMPRO ServerManager]をクリックします。ESMPROのWebコンソールが起動しますので、[アラートビューア]をクリックします。アラートビューアが起動しますので、メニューから[アラート受信設定]をクリックします。
デフォルトでは、次の図のように[アラート受信設定]ダイアログの[SNMPトラップ受信設定]の枠の[**SNMPトラップサービスを使用する**]が選択されています。もし、選択されていない場合は[**SNMPトラップサービスを使用する**]のラジオボタンをクリックし、[OK]ボタンをクリックします。

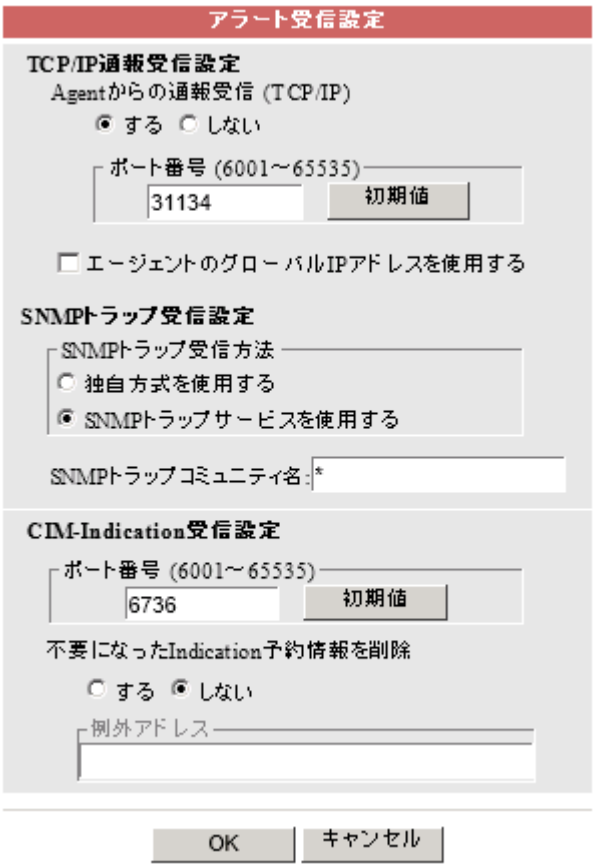

図 4 ESMPRO/ServerManagerのアラートビューア（[アラート受信設定]ダイアログ）

次に、OS起動時にWindowsのSNMP Trapサービスが自動的に起動するように設定します。
Windowsの[スタート]メニューから[管理ツール]→[サービス]をクリックします。[サービス]が開いたら、[SNMP Trap]サービスの[スタートアップの種類]を[**自動**]に設定します。

3.2.3. Windows ファイアウォールの設定

SSCが管理対象と通信できるように、Windows ファイアウォールに接続を許可する設定を行います。SSCのインストーラでは、Windows ファイアウォールに最低限の接続許可設定を行いますが、管理内容によっては設定を追加しておく必要があります。
今回、物理サーバからの障害通報の受信と仮想マシンの死活監視のために、Windows ファイアウォール

の設定を追加します。

まず、障害通報の受信のためにSNMP Trapを受信できるようにします。
Windowsの[スタート]メニューから[管理ツール]→[セキュリティが強化された Windows ファイアウォール]をクリックします。[セキュリティが強化された Windows ファイアウォール]が開いたら、[受信の規則]をクリックして規則の一覧を表示します。

デフォルトでは、一覧の中にはプロファイルの異なる二つの[SNMP トラップ サービス (UDP 受信)]があります。管理用ネットワークに適したプロファイルの[SNMP トラップ サービス (UDP 受信)]を選択し、[操作]メニューから[**規則の有効化**]をクリックします。どちらのプロファイルの規則もデフォルトでは[接続が許可する]ようになるので、これでSNMP Trapを受信できるようになります。今回は、[**プライベート，パブリック**]を選択します。

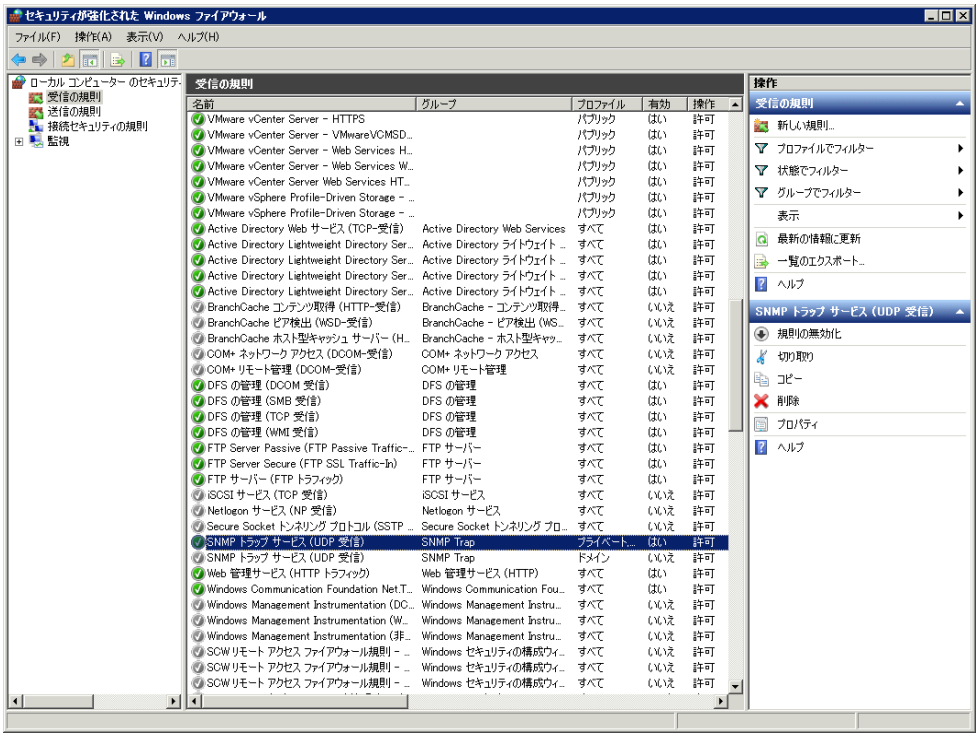

図 5 セキュリティが強化された Windows ファイアウォール
（SNMP トラップ サービス (UDP 受信)）

次に、死活監視（Ping 監視）のためにICMP Echo Replyを受信できるようにします。
[セキュリティが強化された Windows ファイアウォール]の[受信の規則]をクリックして規則の一覧を表示します。[操作]メニューから[**新しい規則**]をクリックします。
[新規の受信の規則ウィザード]ダイアログが開いたら、各ステップで次のように規則を作成します。

- 規則の種類
  - [カスタム]ラジオボタンを選択

- プログラム
  - [このプログラムのパス]を選択
  - パス入力欄に[***%ProgramFiles% (x86)¥NEC¥PVM¥bin¥PVMServiceProc.exe***]を入力

- プロトコルおよびポート
  - [プロトコルの種類]で[**ICMPv4**]を選択

- スコープ
  - [この規則を適用するローカルIPアドレスを選択してください。]で、[**任意のIPアドレス**]を選択（デフォルト）
  - [この規則を適用するリモートIPアドレスを選択してください。]で、[**任意のIPアドレス**]を選択（デフォルト）

- 操作
  - [**接続を許可する**]を選択（デフォルト）

- プロファイル
  - 管理用ネットワークに適したプロファイルを選択します。今回は[**プライベート**]を選択します。

- 名前
  - 任意の名前を入力します。今回は[**SystemProvisioning(ICMPv4)**]と入力します。

[受信の規則]の一覧に[名前]が[**SystemProvisioning(ICMPv4)**]で、[プロトコル]が[**ICMPv4**]の規則が追加されたことを確認します。

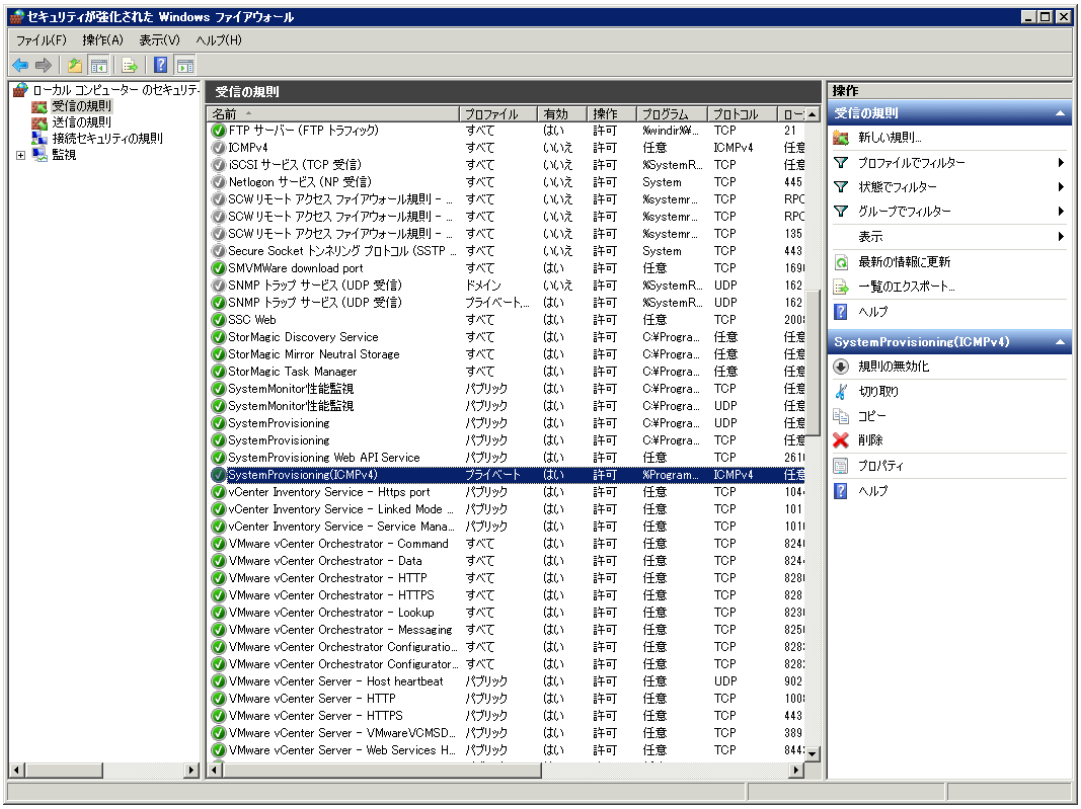

図 6 セキュリティが強化された Windows ファイアウォール（SystemProvisioning(ICMPv4)）

以上の設定が完了したら、管理サーバを再起動してください。

4. 初期設定

SSCのWebコンソールにアクセスします。
Webブラウザを起動し、
[**http://*管理サーバのホスト名またはIPアドレス*:*ポート番号*/Provisioning/Default.aspx**]
にアクセスしてください。今回の場合は、[http://172.16.0.1:20080/Provisioning/Default.aspx] にアクセスします。
初期アカウントとして設定されているユーザ名[**admin**]、パスワード[**admin**]を入力し、[ログイン]ボタンをクリックしてログインします。

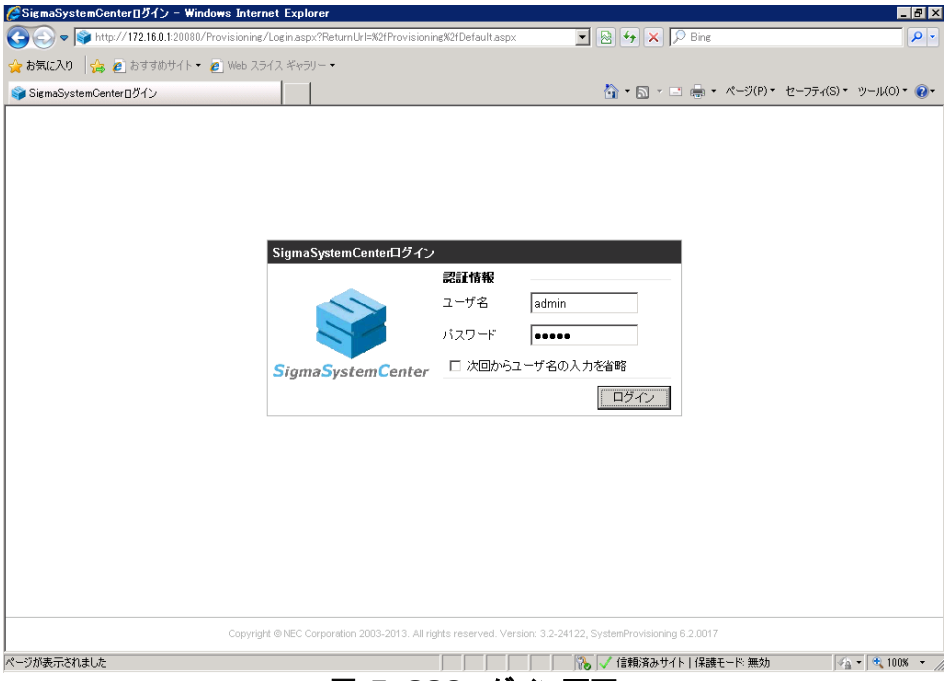

図 7 SSCログイン画面

4.1. ユーザの作成

Webコンソールが表示されたら、普段の管理で使うためのユーザを作成します。
画面の上にあるタイトルバーのビュー切り替えリンクの中から[管理]をクリックし、管理ビューに移動します。
左ペインのツリービューにある[ユーザ]をクリックし、ユーザー覧、ロール一覧画面を表示されたら[ユーザー覧]の枠の右上の[追加]をクリックし[ユーザ追加]画面を表示します。

[ユーザ名]、[パスワード]、[認証種別]、[ロール]を設定し[OK]ボタンを押せば、ユーザが作成されます。今回は、[ユーザ名]を[***sysadmin***]とし、[ロール]には[***システム管理者***]を選択しました。今回、作成するユーザは、LDAPを利用した認証を行わないので、[認証種別]には、[***Local***]を選択します。[パスワード]には任意の文字列を設定してください。

図 8 ユーザ追加画面

[OK]ボタンを押すとユーザー覧、ロールー覧画面に遷移し、[ユーザー覧]に[sysadmin]が追加されていることが確認できます。
ちなみに、デフォルトの[**admin**]ユーザは正規のシステム管理者ユーザを追加するまでの仮のユーザであるためユーザー覧には表示されません。また、正規のシステム管理者ユーザを追加した後、デフォルトの[**admin**]ユーザは無効になりログインできなくなります。

図 9 ユーザー覧、ロールー覧画面（sysadmin追加後）

ユーザが作成できたら、作成したユーザでログインしなおしてください。ログアウトするためには、画面右上の[ログアウト]をクリックします。

4.2. ライセンスの登録

ライセンス登録を行います。画面の上にあるタイトルバーのビュー切り替えリンクの中から[管理]をクリックし、管理ビューに移動します。左ペインのツリービューにある[ライセンス]をクリックし、遷移した画面の一番下にある[ライセンス追加]の枠の[ライセンスキー]ラジオボタンを選択します。[ライセンスキー]のテキストボックスにライセンスキーを入力して[追加]ボタンをクリックしてください。

「PVM サービスを再起動し、ライセンスを有効化してください。」というメッセージが表示されたら、[OK]ボタンをクリックしてください。[ライセンス個別情報]に追加したライセンスキーが表示されます。

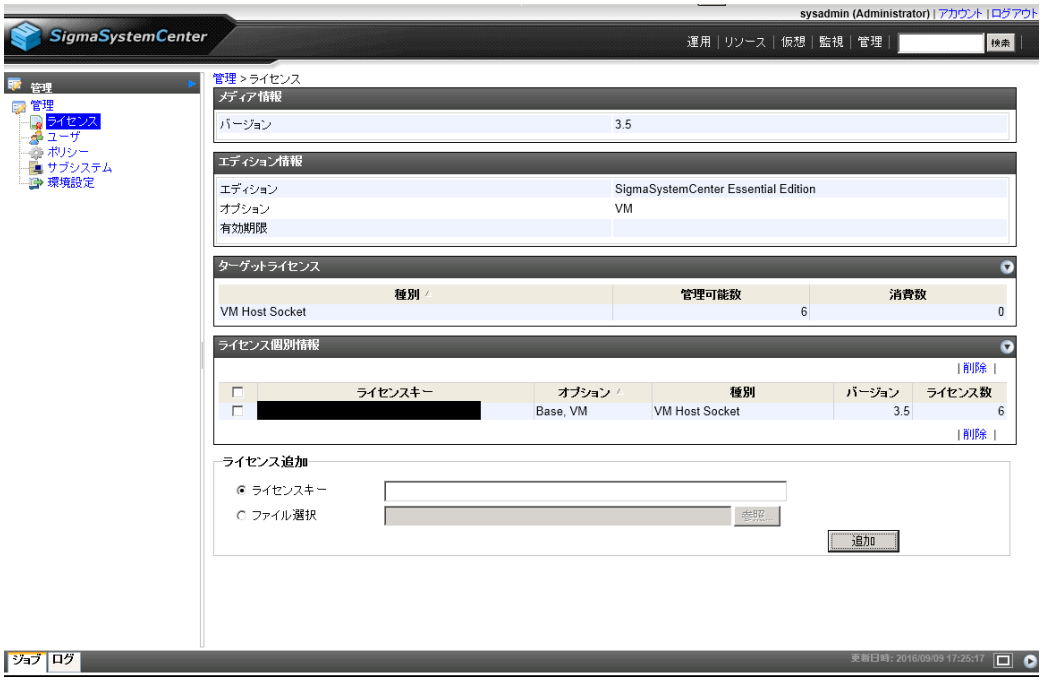

図 10 ライセンス登録

すべてのライセンスの登録が完了したら、Windowsの「管理ツール」の「サービス」で[**PVMService**]を再起動してください。

4.3. 死活監視の基本設定

SSCで死活監視を行う場合は、全体としてどの死活監視を有効にするのか、どういった間隔で実行するのかの基本の設定をしておきます。その上でそれぞれの管理対象ではどの死活監視を利用するのかだけを別に設定します。
基本設定を行うために管理ビュー（タイトルバーの[管理]をクリック）を開きます。管理ビューが開いたらツリービューにある[環境設定]をクリックして環境設定画面を開き、[死活監視]タブをクリックします。
今回は仮想マシンも死活監視の対象とするので、[監視対象モデル種別]の枠の[VM]チェックボックスをチェックし、右下の[適用]ボタンを押してください。

図 11 環境設定画面（死活監視タブ）

他の設定項目については、死活監視により機能停止イベントなどを過剰に検出する場合など、ネットワークや、サーバの性能に応じて調整します。

今回はそのままの値で使用し、問題がある場合のみ調整してください。

4.4. 通報に必要な環境設定

次に、障害や負荷といった事象が発生した際に通報を行うための設定を行っておきます。
通報には、メール通報とイベントログ出力の二種類があります。デフォルトではイベントログ出力のみが有効なので、メール通報は実行されません。今回はメール通報も行うように設定します。

メール通報の環境設定は管理ビュー（タイトルバーの[管理]をクリック）で行います。管理ビューを開いたらツリービューにある[環境設定]をクリックし環境設定画面を開き、[通報]タブをクリックします。

図 12 環境設定画面（通報タブ）

まず、[**メール通報を行います**]のチェックボックスをチェックし、入力欄を有効にします。その後、メールを送信するためのメールサーバ（SMTP）、通報先メールアドレス、送信元メールアドレスを設定します。
各項目は次のように設定します。

表 1 メール通報の設定（入力例）

設定項目	説明	入力例
メール通報を行います	メール通報を有効にする場合はチェック	ー
通信先メールサーバ名	通報メールを送信するためのメールサーバ(SMTP)	smtp.test.nec.com
ポート番号	「通信先メールサーバ」が使用しているポート番号	25（デフォルト）
SMTP認証を行う	「通信先メールサーバ」がSMTP認証を行っている場合はチェック	ー
認証アカウント	SMTP認証で使用するアカウント名	sscadmin
認証パスワード	SMTP認証で使用するパスワード(「パスワード更新」をチェックして入力)	表示されません
保護された接続(TLS)を使用する。	「通信先メールサーバ」に暗号化(TLS)接続する場合はチェック	ー
通信元メールアドレス(From)	通報メールの送信元となるメールアドレス(必須)	sscadmin@test.nec.com
通信先メールアドレス(To)	通報メールの送信先となるメールアドレス(必須)	t-nichiden@test.nec.com

メール通報に必要な項目を入力したら、実際に送信できるかのテストを行います。右下の[**テスト送信**]ボタンを押すと通信先メールアドレスへテストメールが送信されます。テストメールを受信して問題がないことを確認します。

テストで問題がないことを確認したら、右下の[**適用**]ボタンを押して、設定内容を保存します。

なお、[通報]タブの下の[通知をイベントログに書き込む]チェックボックスは、管理サーバのWindowsのイベントログへの出力を有効にします。デフォルトではチェック(有効)になっており、今回も出力することとします。

5. 管理対象の登録

管理対象となるマシンを登録します。SSCでは管理機能がコンポーネント化（サブシステム化）されているので、管理対象に対応するサブシステムをSSC本体に先に登録しておく必要があります。
今回は管理対象がVMware ESXiですので、サブシステムとしてVMware vCenter Serverを先に登録しておきます。

5.1. サブシステムの登録

SSCの管理ビューを開き（タイトルバーの[管理]をクリック）、左ペインのツリービューにある[サブシステム]をクリックします。右サイドバーの[設定]メニューにある[サブシステム追加]をクリックすると下の画面が表示されるので、[サブシステム種類]ドロップダウンリストで[**VMware vCenter Server**]を選択します。残りの項目は以下のように設定します。

- **ホスト名**: vCenter Serverがインストールしてあるサーバのホスト名もしくはIPアドレス
- **ポート**: vCenter Serverに接続するためのHTTPSポート
  （入力を省略した場合、デフォルトの**443**になります）
- **URL**: 何も入力しないでください。
- **アカウント名**: vCenter Serverの管理アカウント名
- **パスワード**: vCenter Serverの管理アカウントのパスワード

上記の項目を入力したら[OK]をクリックしてください。

図 13 vCenter Serverの登録

さて、SSCのサブシステムにはVMware用の「VMware vCenter Server」のほかに「VMware ESXi」があります。ただし、こちらはvCenter Serverを登録するとそのvCenter Serverで管理しているESXiが自動的に検出/登録されるので、手動で登録する必要はありません。vCenter Server登録後に[サブシステム一覧]画面の[操作]メニューで[画面更新]をクリックすると、ESXiがサブシステム一覧に表示されます（表示されていない場合は少し時間を置いて画面を更新してみてください）。

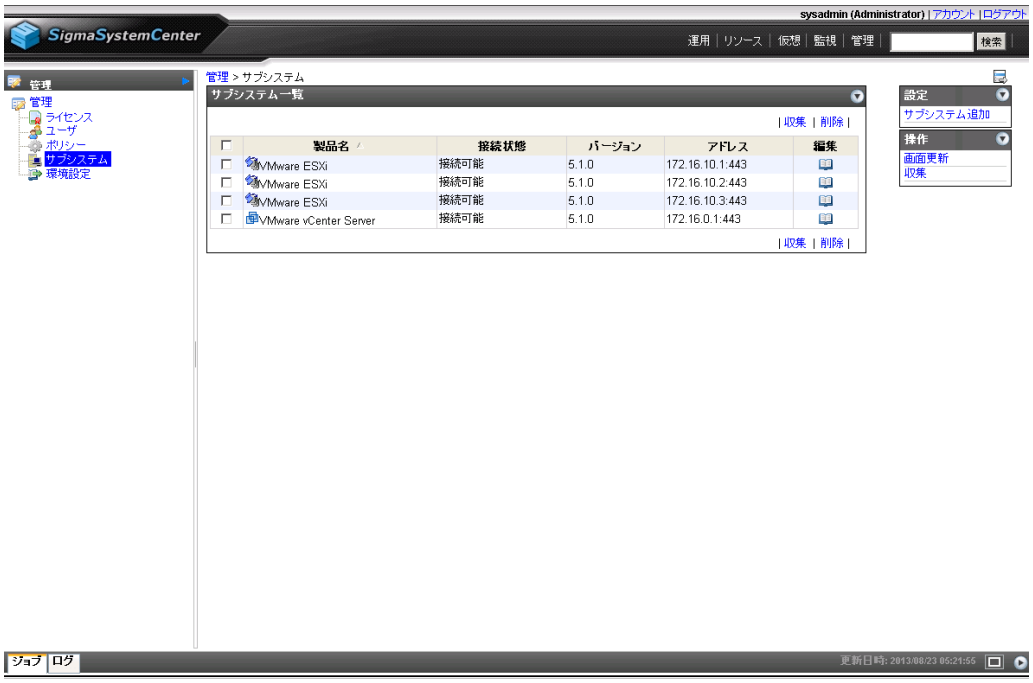

図 14 サブシステム一覧

もっとも、ESXiが検出されただけでは、Failover、VM作成/再作成などの操作をSSCから実行することができません。そこで追加の設定を行います。[サブシステム一覧]のVMware ESXiの右端にある[編集]アイコンをクリックして下の画面を開いてください。[ホスト名]および[ポート]には自動検出された値が設定されているので、[アカウント名]に管理者アカウントの[**root**]を入力し、[パスワード更新]をチェックして[パスワード]にrootのパスワードを入力して[OK]ボタンをクリックします。今回は物理サーバが3台なので、3台それぞれで追加の設定を行います。

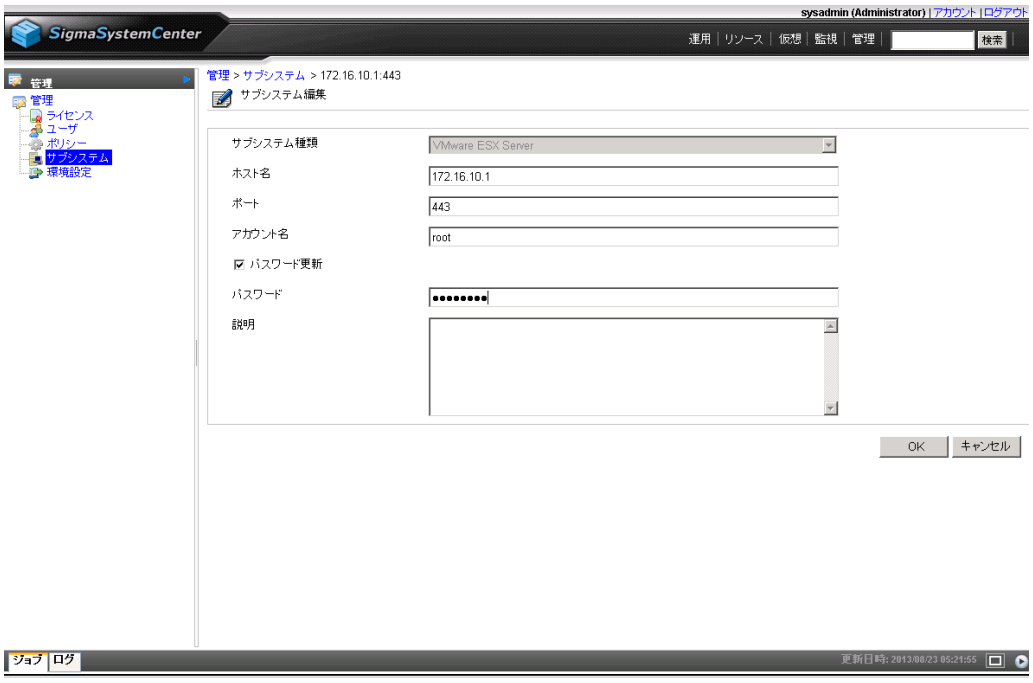

図 15 ESXiの追加設定

5.2. リソースの登録

サブシステムの登録が終わったら、次に管理対象となるマシンをSSCに登録します。マシン登録の基本的な手順は次のようになります。

1. グループの作成
2. グループにマシンを登録

まず、グループを作成しましょう。タイトルバーの[リソース]をクリックしてリソースビューを開き、ツリービューの[マシン]をクリックして[マシン一覧]画面に移動します。

図 16 リソースビュー「マシン一覧」

グループを作成するには[設定]メニューの[グループ追加]をクリックします。すると、下の画面が開くので、[名前]に分かりやすいグループ名を付けて[OK]ボタンをクリックします。今回は物理サーバのグループ[**ESXi**]と業務用仮想マシンのグループ[**業務用VM**]を作成しました。

図 17 グループの作成

下はグループ作成後の[マシン一覧]画面です。ツリービューの[マシン]の下に作成したグループが追加されているのが分かります。

図 18 グループ作成後の「マシン一覧」

次に、グループにマシンを登録します。[設定]メニューの[マシン登録]をクリックしてください。すると、下の[管理外のマシン一覧]画面になります。ここでは登録するマシンにチェックを入れ、下の[親のリソース]から所属グループを選択して[OK]をクリックします。まず物理サーバである[**172.16.10.1**](esxi1)と[**172.16.10.2**](esxi2)、[**172.16.10.3**](esxi3)をチェックして[親のリソース]で[**ESXi**]を選択して[OK]をクリックします。
次に、業務用仮想マシンを登録します。再度、[管理外のマシン一覧]画面を開いて、[**VM-01**]、[**VM-02**]、[**VM-03**]、[**VM-04**]、[**VM-05**]、[**VM-06**]にチェックを入れ、[親のリソース]で[**業務用VM**]を選択して[OK]をクリックします。

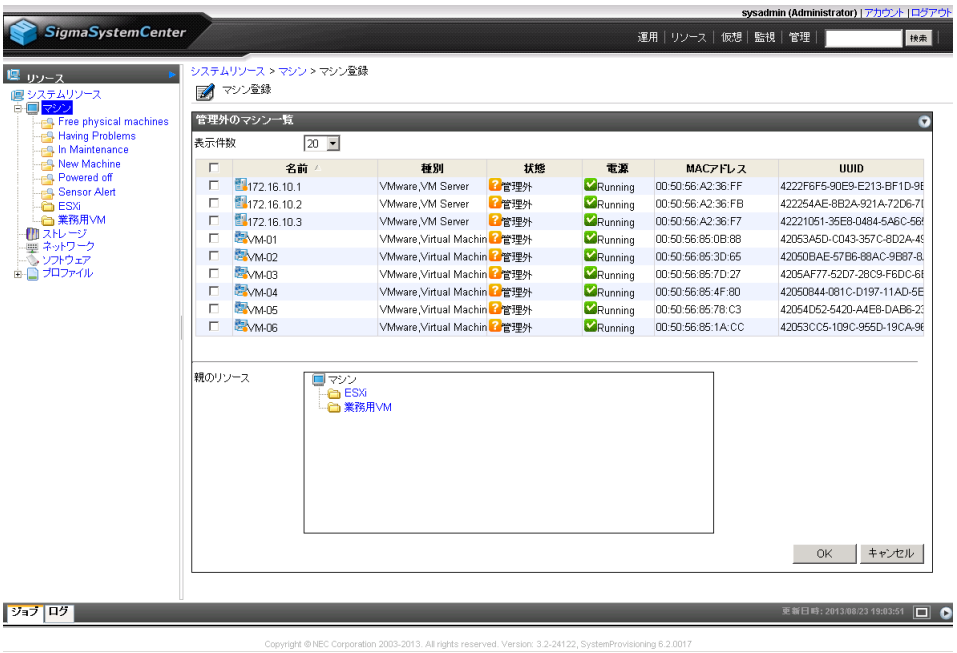

図 19 管理外のマシン一覧

マシン登録後の[マシン一覧]画面です。

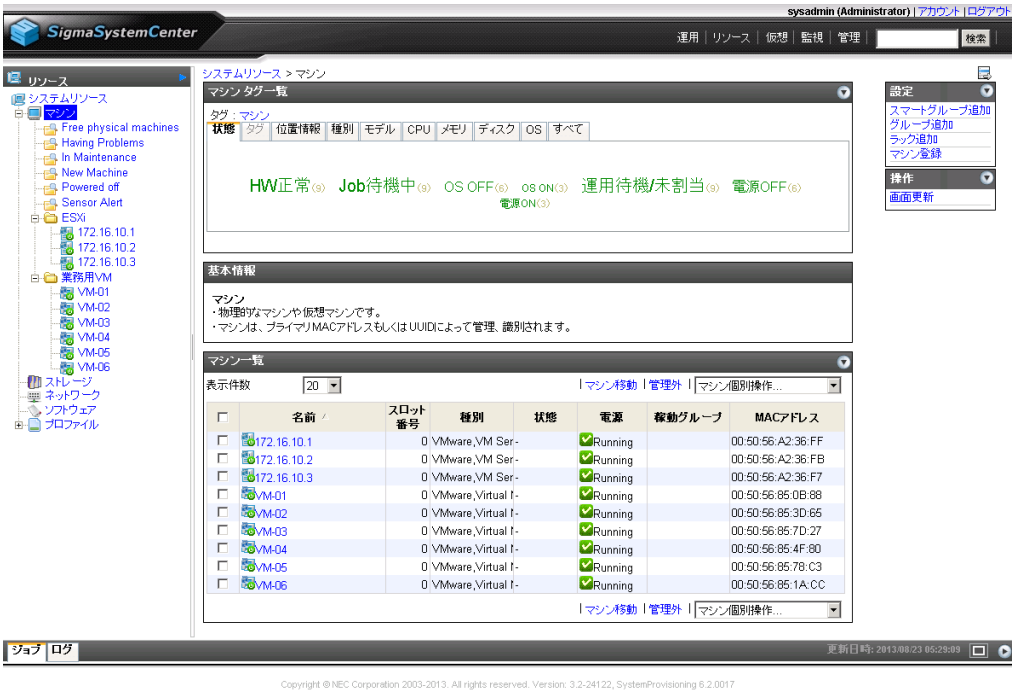

図 20 マシン登録後の[マシン一覧]

以上でマシン登録は終了です。

5.3. 物理サーバの設定

ここまでの作業で、管理対象リソースをSSCに登録することができました。次に、物理サーバである「172.16.10.1」(esxi1)と「172.16.10.3」(esxi2)、「172.16.10.3」(esxi3)の電源制御やセンサ情報の取得を可能にするための設定を行います。
SSCが「Out-of-Band（OOB）Managementを利用するための設定」として、EXPRESSSCOPEエンジン（BMC）にリモートログインするための以下の設定を行います。

1. 管理対象の物理サーバのEXPRESSSCOPEエンジン（BMC）の設定を行う。
2. SSC上で、管理対象のOOBアカウント設定を行う。

5.3.1. EXPRESSSCOPE エンジン（BMC）の設定

✧ 管理LANの設定

まず、「172.16.10.1」(esxi1)となるサーバのEXPRESSSCOPEエンジン（BMC）の管理用LANの設定を行います。手順については、「EXPRESSSCOPEエンジン 3 ユーザーズガイド」の「2. 本体装置側の設定」を参照して、管理用LANを設定してください。

✧ 管理者権限のあるユーザの作成

次に、「172.16.10.1」(esxi1)となるサーバのEXPRESSSCOPEエンジン（BMC）で管理者権限のあるユーザを作成します。手順については、「EXPRESSSCOPEエンジン 3 ユーザーズガイド」の「5. リモートマネージメントの使い方」を参照して、ユーザ管理画面でアカウントを作成してください。
ここでは、仮に[ユーザ名]を[**ssc**]、[パスワード]を[**sscadmin**]に設定したとします。

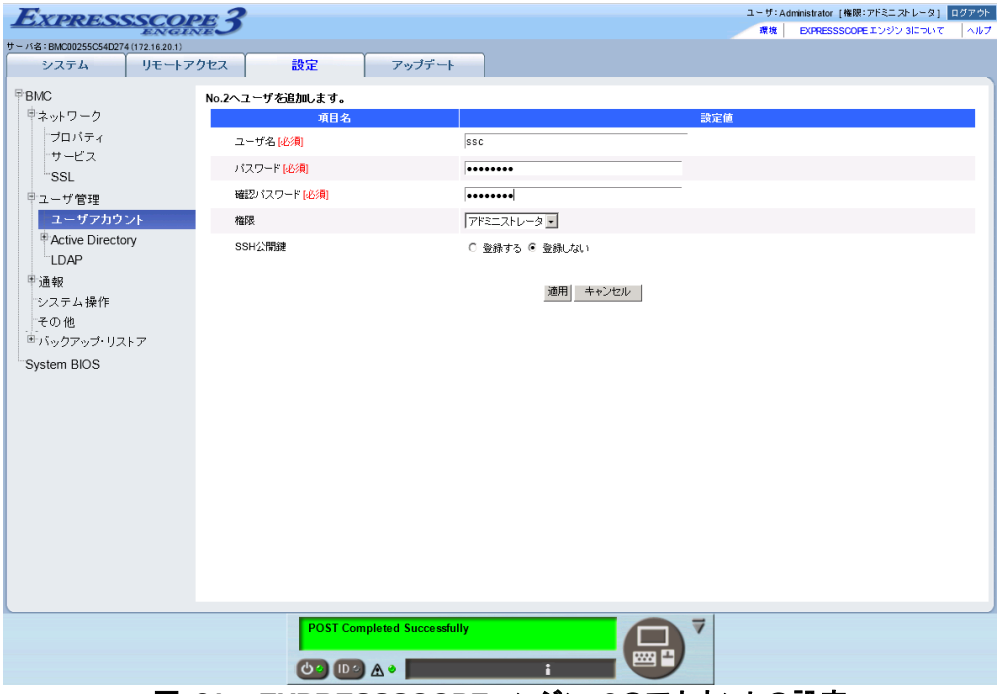

図 21 EXPRESSSCOPEエンジン 3のアカウントの設定

✧ PET通報の設定

続いて、EXPRESSSCOPEエンジン（BMC）で、管理サーバであるSSCmanager(172.16.0.1)へPET通報を行うための設定をします。今回は、通報先の設定枠の1次通報先を使うことにします。

1 [設定] タブをクリックします。
2 左のメニューツリーから[BMC] ー [通報] ー [SNMP 通報] をクリックします。

3　中央メインペイン下の[編集] をクリックして、以下の設定を行います。

表 2 PET通報の設定（入力例）

項目名	設定値
通報	有効
コンピュータ名	esxi1
コミュニティ名	public
通報手順	全ての通報先
通報応答確認	無効
1次通報先－通報先IPアドレス	チェックの上、172.16.0.1
2次通報先－通報先IPアドレス	他のアプリケーションに合わせて任意
3次通報先－通報先IPアドレス	他のアプリケーションに合わせて任意
通報レベル	異常、警告、情報

4　メインペイン下の[適用]をクリックします。

図 22　EXPRESSSCOPEエンジン 3のSNMP(PET)通報の設定

[172.16.10.2」(esxi2)と[172.16.10.3」(esxi3)となるサーバについても、同様に設定します。

5.3.2.　SSC での OOB のアカウント設定

SSCでは、物理サーバのEXPRESSSCOPEエンジン（BMC）にログインするために、リソースビューで「172.16.10.1」(esxi1)と「172.16.10.2」(esxi2)、[172.16.10.3」(esxi3)のそれぞれのOOBアカウントを設定します。

まずタイトルバーの[リソース]をクリックしてリソースビューを開きます。ツリービューから設定対象の物理サーバである[172.16.10.1](esxi1)（ここでは、[マシン]→**[ESXi]**グループの配下）をクリックすると、下の画面のようにマシンの詳細情報が表示されます。

図 23 マシンの詳細

リソースの設定を編集するには、[設定]メニューにある[プロパティ]をクリックしてマシンのプロパティ設定画面を開きます。

マシンの設定項目は、複数のタブに分類されています。OOBアカウントを設定するには、[アカウント情報]タブをクリックします。[アカウント一覧]の枠の右上の[追加]をクリックすると、[アカウント追加]画面が表示されます。
さらに、[アカウント追加]画面の[プロトコル一覧]の枠の右上の[追加]をクリックすると、下の画面のように[プロトコル]追加の枠が表示されます。
各項目は、以下のように入力します。

- アカウントタイプ: **OOB**
- ユーザ名: EXPRESSSCOPEエンジンのユーザ名を入力（今回は、***ssc***）
- パスワード: EXPRESSSCOPEエンジンのパスワードを入力（今回は、***sscadmin***）
- 接続先: EXPRESSSCOPEエンジンの管理LANのホスト名、または、IPアドレス（今回は、***172.16.20.1***）
- オフラインマシンのアカウントでも登録する。: **チェックしない**
- [プロトコル追加]の枠のIPMI: **チェックする**
- [プロトコル追加]の枠の[監視を有効にする]: **チェックする**

図 24 OOBアカウントの追加

上記を全て入力した状態で[プロトコル追加]の枠の左下の[OK]をクリックすると、[プロトコル一覧]の枠に[IPMI]が追加されます。続いて、右下の[OK]ボタンを押します。

OOBアカウント追加後の[アカウント情報]タブです。[アカウント一覧]の枠に[OOB]が追加され、[接続状態]が[接続可能]となっていればSSCがEXPRESSSCOPEエンジンにログインできたことを示しています。

図 25 OOBアカウント追加後のマシンプロパティ設定(「アカウント情報」タブ)

以上で物理サーバの「172.16.10.1」(esxi1)のOOBアカウントが設定できました。同様の手順を繰り返して、「172.16.10.2」(esxi2)と「172.16.10.3」(esxi3)も設定してください。

6. 運用の基本設定

ここからは、登録したリソースをどのような用途でどのように利用するのかといった運用に関する設定を行います。このような設定は運用ビュー（タイトルバーの[運用]をクリック）で行います。

6.1. 運用グループの作成

運用ビューで最初に行う作業は“グループ”の追加です。
グループはシステムを構成するサーバの種類ごとに作成します。また、後で設定する障害監視のポリシーや負荷監視はこのグループ単位に設定することになるので、障害監視や負荷監視の内容に応じてグループを分けて作るようにします。
今回のシステムでは、次の表のように同じ考え方や要素で管理するサーバをひとかたまりのグループとしており、物理サーバのグループ「ESXi」と業務用仮想マシンのグループ「業務用VM」を作成することにします。同じ仮想マシン（VM）でもOSや業務が違う場合は、障害監視と負荷監視の内容を別にするためにもグループを分けるようにします。

表 3 グループの設計例

サーバ	グループを設計する際の考え方				グループ
	物理サーバか？仮想サーバか？	OSは何か？	障害発生時にどのように対応するか？	負荷を監視するか？	
172.16.10.1 (esxi1)	物理（VMサーバ）	ESXi	障害（予兆）対応	監視する	ESXi
172.16.10.2 (esxi2)	物理（VMサーバ）	ESXi	障害（予兆）対応	監視する	
172.16.10.3 (esxi3)	物理（VMサーバ）	ESXi	障害（予兆）対応	監視する	
VM-01	仮想（VM）	Windows Server	障害対応（通報）	監視する	業務用VM
VM-02	仮想（VM）	Windows Server	障害対応（通報）	監視する	
VM-03	仮想（VM）	Windows Server	障害対応（通報）	監視する	
VM-04	仮想（VM）	Windows Server	障害対応（通報）	監視する	
VM-05	仮想（VM）	Windows Server	障害対応（通報）	監視する	
VM-06	仮想（VM）	Windows Server	障害対応（通報）	監視する	

運用ビューの[設定]メニューにある[グループ追加]をクリックし、下の画面を開きます。[名前]にグループ名を入力し、[マシン種別]のドロップダウンリストから当該グループで稼動させるマシンのマシン種別を選び、[OS種別]のドロップダウンリストから当該グループで利用するOSを選んで[OK]をクリックします。ESXiのマシン種別はVMサーバなので、[ESXi]グループの[マシン種別]は[**VMサーバ**]を選び、ESXiはLinuxベースなので、[ESXi]グループの[OS種別]は[**Linux**]を選びます。
業務用仮想マシンのマシン種別はVMなので、[業務用VM]グループの[マシン種別]は[**VM**]を選び、業務用仮想マシンはWindows Server 2008 R2なので、[業務用VM]グループの[OS種別]は[**Windows Server**]にします。

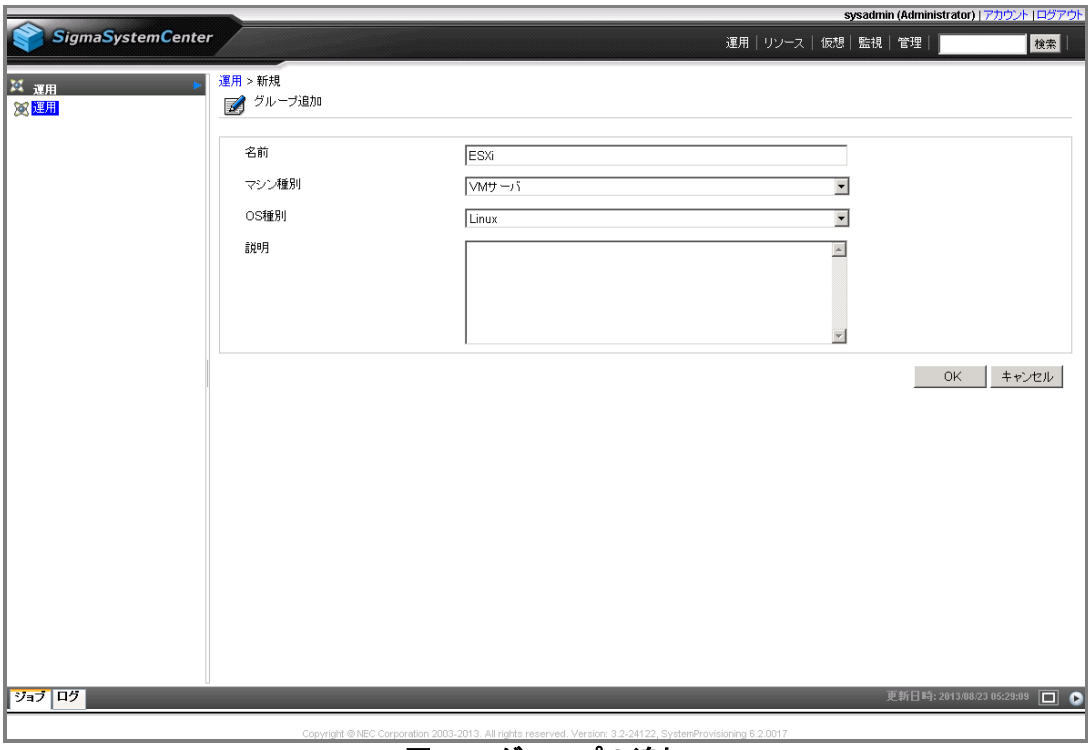

図 26 グループの追加

グループ追加後の運用ビュー（テナント/カテゴリ/グループ一覧）です。

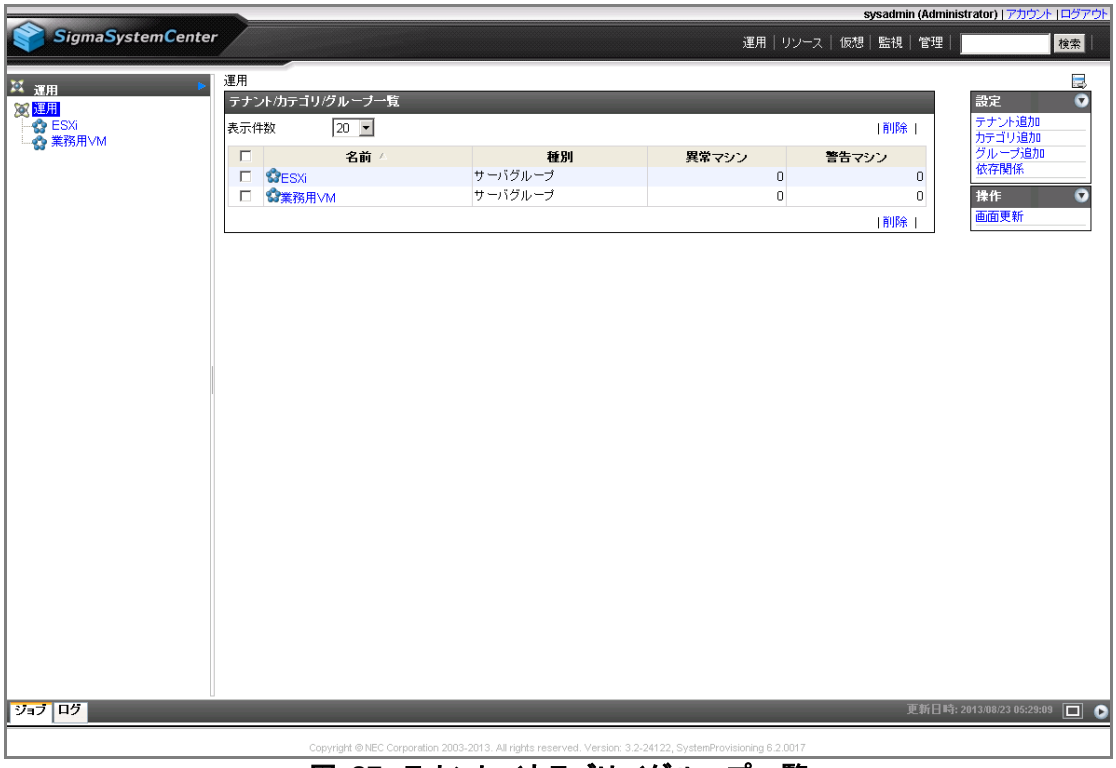

図 27 テナント／カテゴリ／グループ一覧

6.1.1. 物理サーバグループへのホストの追加

次に、“ホスト”の追加を行います。
“ホスト”は、実体のマシンに対してSSCでどのような運用・管理を行うかの定義の枠になります。
ホストを追加するには、ツリービューにあるグループ名（ここでは[ESXi]）をクリックし、下の画面のようにグループの詳細情報画面を開きます。

図 28 グループの詳細情報

中央の[ホスト一覧]枠内メニューの[ホスト追加]をクリックし、[ホスト追加]画面を開きます。ここでは物理サーバのホスト「**172.16.10.1**」(esxi1)について設定します。IPアドレスには、管理用LANに接続する際のIPアドレスを入力してください。

- 複数ホストを作成する: チェックしない
- ホスト名: ***esxi1***
- タグ: 設定しない
- ネットワークを設定: **チェックする**
- IPアドレス: ***172.16.10.1***
- サブネットマスク: ***255.255.0.0***
- デフォルトゲートウェイ: ***172.16.0.254***
- 管理用IPアドレスにする: **チェックする**

下の画面のように、[ホスト追加]画面へ入力したら、[OK]をクリックします。

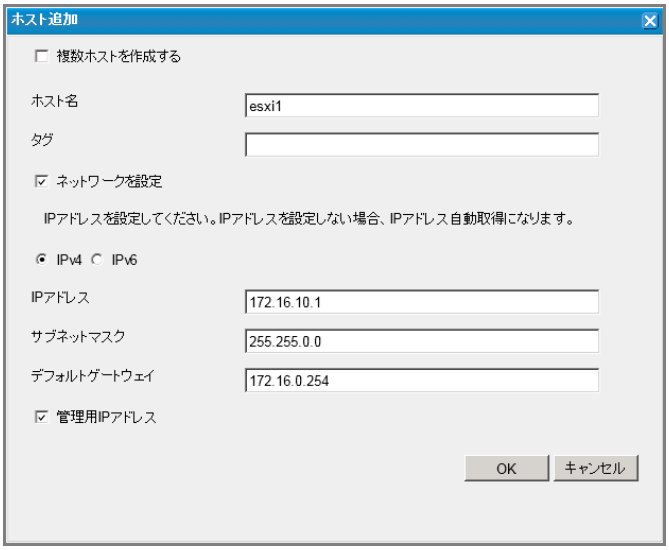

図 29 ホスト追加

図 30 ESXiグループのホスト一覧（esxi1追加後）

ホスト追加後の[ESXi]グループの詳細情報の画面です。[ホスト一覧]に追加したホスト[esxi1]が表示されています。この時点では、まだ実体となる物理サーバを割り当てていないので、状態には[定義のみ]と表示されます。

以上で物理サーバのホスト「esxi1」が設定できました。同様の手順を繰り返して、「**esxi2**」と「**esxi3**」も設定してください。下はesxi2とesxi3設定後のホスト一覧です。

図 31 ESXiグループのホスト一覧

6.1.2. 仮想マシングループへのホストの追加

続けて仮想マシンのグループ「業務用VM」にもホストを追加します。手順は物理サーバグループ「ESXi」のときと同様に、「ホスト追加」を実施します。ホスト追加とIPアドレス設定の方法は物理サーバのときとまったく同じです。下は業務用VMの6台の仮想マシン[VM-01]、[VM-02]、[VM-03]、[VM-04]、[VM-05]、[VM-06]にそれぞれIPアドレスを設定した状態のホスト一覧です。

図 32 VMグループのホスト一覧

6.1.3. マスタマシンの登録

ここまでの作業で、システムを構成するサーバの定義をSigmaSystemCenter（SSC）に追加することができました。次はこのサーバの定義にリソースを割り当てます。まずはESXiグループのホストにリソースを割り当ててみましょう。運用ビューのツリービューでESXiグループをクリックすると、グループの情報が表示されます。[ホスト一覧]の枠のリソースを割り当てるホスト（ここでは「**esxi1**」）のチェックボックスをチェックし、枠内メニューの[マスタ登録]をクリックしてください。

図 33 マスタマシン登録

すると、割り当てるマシンが属しているプールを選択する画面が表示されます。今回は、[**共通プールから選択**]のラジオボタンをチェックして[次へ]をクリックします。

図 34 プールの選択

次に、割り当てるマシンを選択する画面が表示されます。ここには登録済みのリソースの中から、運用グループで選択しているマシン種別に適合するものだけがリストアップされます。割り当てるマシンのラジオボタンをチェックして「次へ」をクリックします。

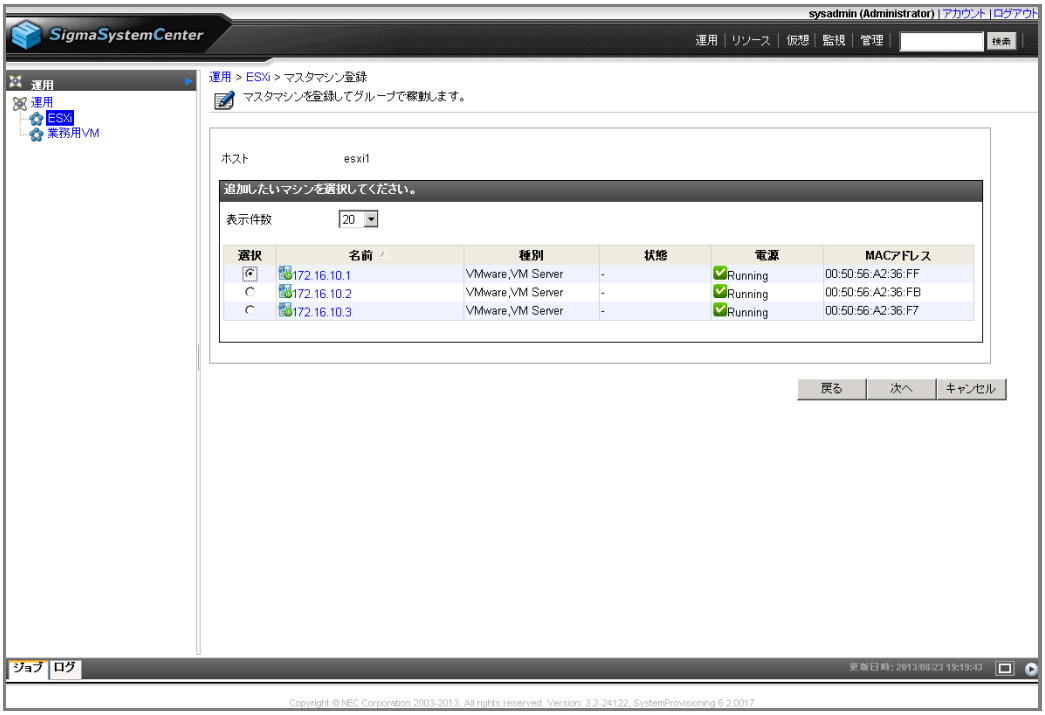

図 35 割り当てマシンの選択

マスタマシン登録の確認画面が表示されるので、間違ったマシンを選択していないことを確認してから「完了」をクリックしてください。

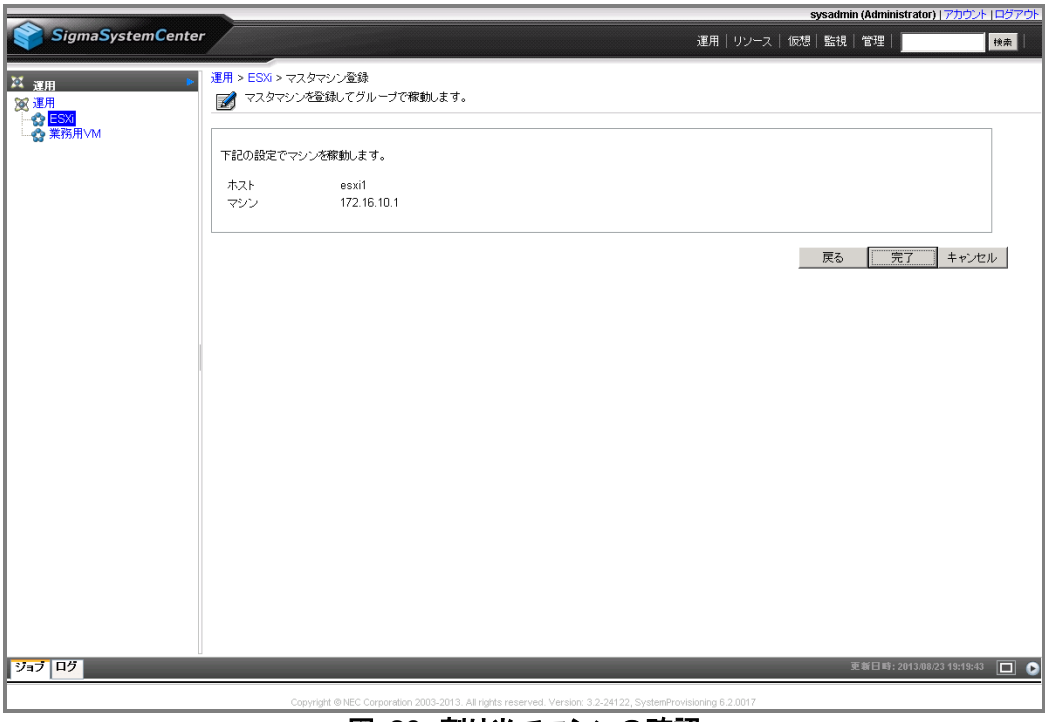

図 36 割り当てマシンの確認

グループの情報画面に戻るので、同じ手順で2台目の物理サーバホスト「**esxi2**」と「**esxi3**」にもマスタマシンを登録します。下は、3台の物理サーバにマスタマシンを登録した状態です。

図 37 マスタマシン登録後のグループ情報（ESXi）

業務用仮想マシンのホスト定義にも物理サーバと同じようにしてマスタマシンを登録します。下は、6台の仮想マシンにマスタマシンを登録した状態です。

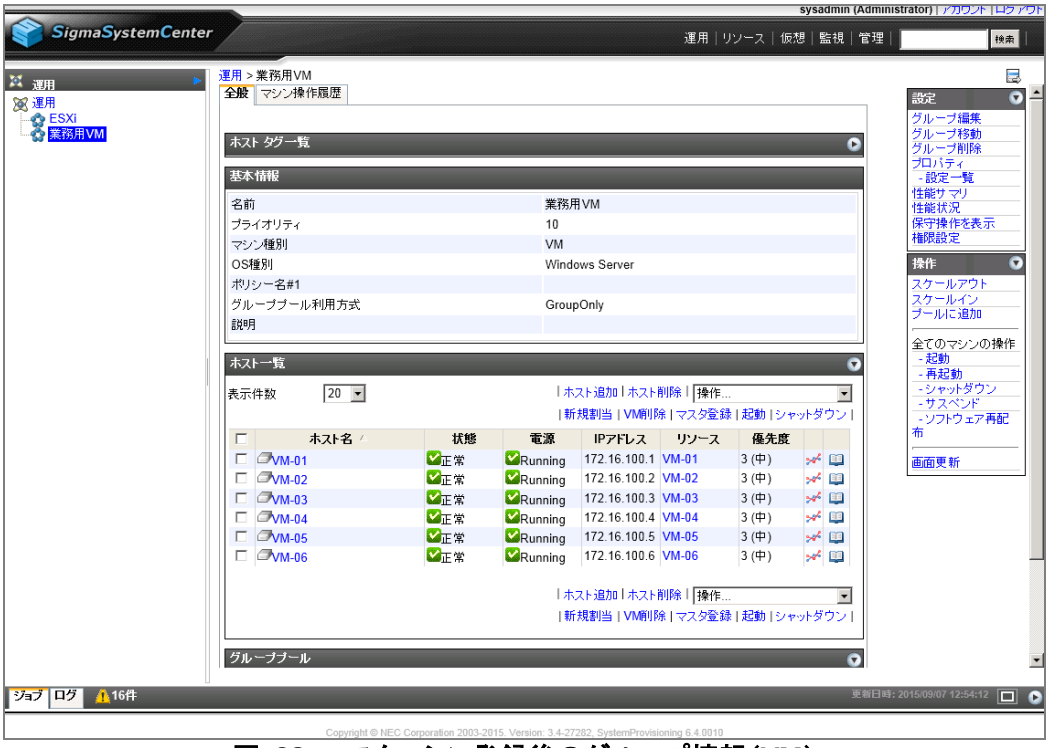

図 38 マスタマシン登録後のグループ情報（VM）

6.2. 手動でのマイグレーション（vMotion）

以上の作業により、システム構成定義と管理対象サーバ（リソース）の対応関係がSSCに設定されました。目標の自律運用を実現するには運用ポリシーを作成して適用する必要がありますが、この段階でも手動での制御はSSC上から行えます。そこで、テストを兼ねて手動での“マイグレーション”（VMwareの用語では「vMotion」）を行ってみることにしましょう。“マイグレーション”は、仮想マシンを稼働させたままの状態で物理サーバ間の移動を行うことを指します。

SSCでは、仮想マシンの状態確認や手動での制御は仮想ビューから行います（タイトルバーの[仮想]をクリック）。ツリービューを確認すると、物理サーバ[172.16.10.1](esxi1)上で仮想マシン[VM-01]、[VM-02]が動作しており、物理サーバ[172.16.10.1](esxi2)上で仮想マシン[VM-03]、[VM-04]が動作していることが分かります。
ここでは[VM-02]を172.16.10.1(esxi1)から172.16.10.2(esxi2)に移動してみます。ちなみに仮想マシンの制御は運用ビューから行うこともできますが、仮想ビューのほうが仮想マシンの配置状況が把握しやすいのでオペレーションミスの発生を防ぎやすいでしょう。

図 39 仮想ビュー

仮想マシンを移動させるには、まずツリービュー上で当該仮想マシンが使用している物理サーバ[172.16.10.1](esxi1)をクリックして選択します。表示された画面を中ほどまでスクロールすると[稼働中VM一覧]という枠があるので、移動させる仮想マシン[**VM-02**]をチェックして、右上のアクションメニューの[VM移動]をクリックしてください。

図 40 移動する仮想マシンの選択

[VM移動]をクリックすると、移動先の物理サーバと移動方法を選択する画面が表示されます。[移動先データセンタ名]ではドロップダウンリストから移動先となる「172.16.10.2」(esxi2)がvCenter上で属しているデータセンタを選択します。次に、移動先となる[**172.16.10.2**](esxi2)のラジオボタンをチェックします。

一方、移動方法としては以下の3つが用意されています。

- **Migration**: 稼働状態を保持したまま仮想マシンを移動します。VMwareのvMotionを利用します。
  特に、[サスペンド後に移動(Quick Migration)]をチェックした場合は、移動するVMをサスペンドしてから移動を行い、異動後にVMをレジュームします。

- **Storage Migration**: 稼働状態を保持したまま仮想マシンと仮想ストレージを移動します。VMwareのStorage vMotionを利用するため、適切なVMwareのライセンスを用意してください。
  特に、[停止後に移動(Move)]をチェックした場合には、移動するVMを停止してから仮想マシンと仮想ストレージを移動します。この場合、VMwareのStorage vMotionは利用しません。さらに、移動後にVMを起動したい場合には[VM移動後の状態]の枠の[自動起動]をチェックします。

- **Failover**: 仮想マシンを障害が発生した物理サーバから正常稼働中の物理サーバに移動します。仮想マシンの稼働状態は保持されず、コールドブートします(再起動したイメージになります)。

これらの移動方法のStorage Migrationの[停止後に移動(Move)]を除いては、移動元のESXiと移動先のESXiで共有するストレージが必要になります。Storage Migrationの[停止後に移動(Move)]のみ、ローカルディスクなど共有していないストレージでも移動が可能です。

今回、共有ストレージを利用できるので、仮想マシンを稼働させたまま移動する[**Migration**]をチェックします。

移動先と移動方法を選択したら[OK]をクリックします。

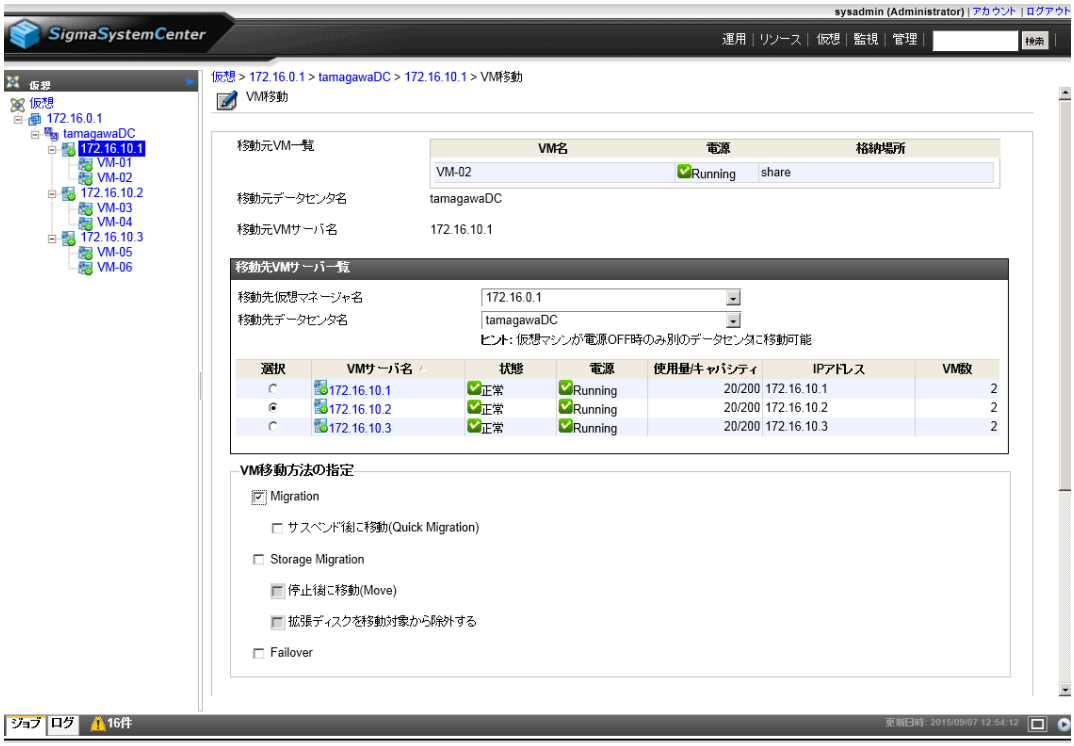

図 41 移動先と移動方法の選択

下は仮想マシンを移動させたあとの仮想ビューです。ツリービューを見ると、[VM-02]が[172.16.10.2](esxi2)に移動していることが分かります。なお、仮想マシンの移動がツリービューに反映されていない場合は[操作]メニューの[画面更新]をクリックしてみてください。

図 42 仮想マシン移動後の仮想ビュー

7. 負荷監視の設定

ここからは管理対象マシンの負荷状況を監視するために必要な設定を行います。SSCは管理対象マシンの負荷状況を時系列のグラフとしてコンソール上に表示し、閾値によって監視することができます。本章では、管理対象マシン（ESXi、仮想マシン）の負荷状況を取得し、SSCのコンソール上で確認するための手順について説明します。

7.1. 監視プロファイルの設定

監視プロファイルは、性能情報の監視項目、監視間隔、閾値などの設定を含む、性能監視設定のセットです。管理対象マシンの負荷監視を実施する場合、監視プロファイルを準備して、運用グループに割り当てることで、負荷監視が可能となります。

SSCでは、一般的な監視項目が既に設定済みの監視プロファイルをあらかじめ用意しています。今回は、デフォルトで用意されている監視プロファイル **Standard Monitoring Profile (1min)** をベースにして新規の監視プロファイル **Standard Monitoring Profile for Small Scale Pack** を作成する手順について説明します。

Standard Monitoring Profile (1min) は、4つの性能情報について、1分間隔で性能データを収集する監視プロファイルです。今回利用する監視プロファイル **Standard Monitoring Profile for Small Scale Pack** は、**Standard Monitoring Profile (1min)** をベースに、監視する項目として メモリの空き容量割合を追加して、CPU使用率とメモリの空き容量割合の閾値監視を有効にしたものです。

表 4 監視プロファイル比較

性能情報	説明	Standard Monitoring Profile		Standard Monitoring Profile for Small Scale Pack	
		データ収集	閾値監視	データ収集	閾値監視
CPU Usage (%)	CPU使用率です。プロセッサの処理状況を示すために、ビジー時間を指定収集間隔内の平均割合としてパーセントで取得します。	有効	無効	有効	**有効**
Disk Space (MB)	ディスク空き容量です。ディスクドライブ上の利用可能な空き領域をメガバイト数で取得します。	有効	無効	有効	無効
Disk Transger Rate (Bytes/sec)	ディスク転送速度です。書き込みまたは読み取り操作中にディスク間でバイトが転送される速度を取得します。	有効	無効	有効	無効
Physical Memory Space (MB)	メモリ空き容量です。割り当て可能な物理メモリのサイズをメガバイト数で取得します。	有効	無効	有効	無効
Physical Memory Space Ratio (%)	物理メモリの合計サイズに対する、割り当て可能なサイズの割合をパーセントで取得します。Physical Memory Space (MB) /メモリの合計サイズ×100 によって、計算する数値です。	無効	ー	**有効**	**有効**

監視プロファイルの設定はリソースビュー（タイトルバーの[リソース]をクリック）で行います。リソースビューを開いたら、ツリービューから[監視プロファイル]を選択します。用意されている監視プロファイルの一覧が表示されます。

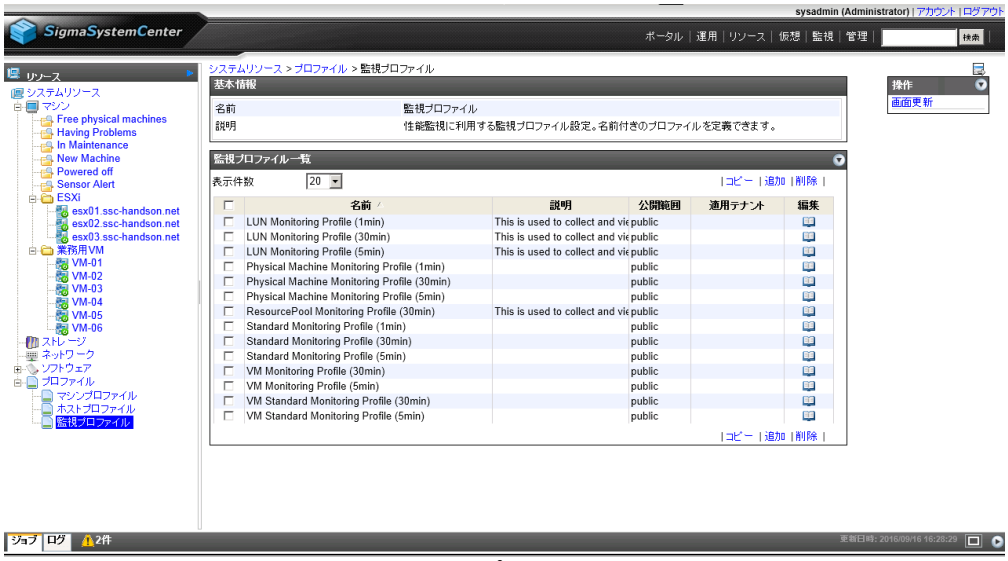

図 43 監視プロファイル一覧

Standard Monitoring Profile (1min) をチェックして、[コピー]をクリックします。コピー完了後、**Standard Monitoring Profile (1min)[2]** という名前の監視プロファイルが新たに追加されます。

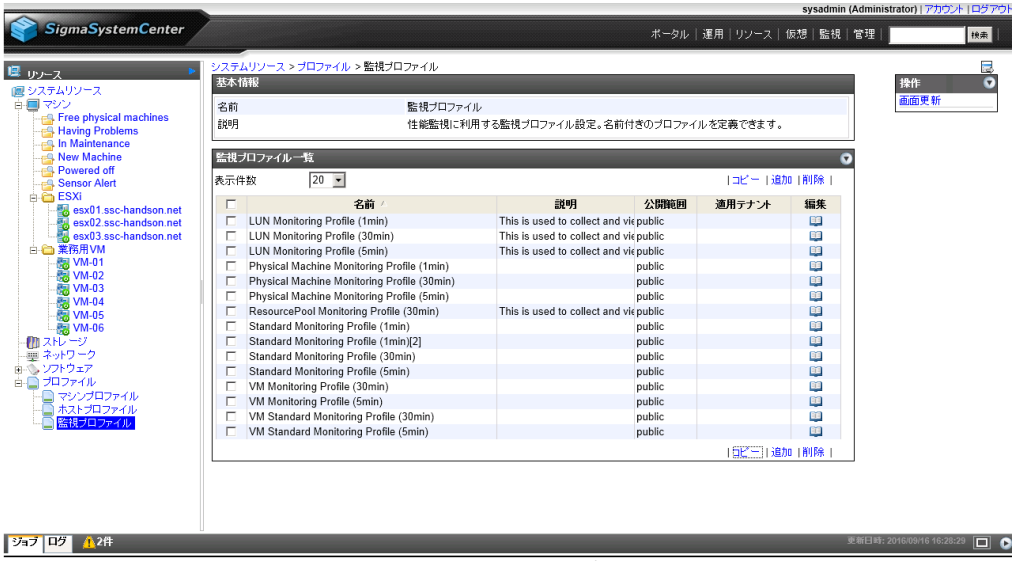

図 44 コピー実施後の監視プロファイル一覧

コピーした監視プロファイルを編集します。**Standard Monitoring Profile (1min)[2]** の[編集]をクリックすると、監視プロファイル編集画面が表示されますので、プロファイル名として [**Standard Monitoring Profile for Small Scale Pack**] と入力します。

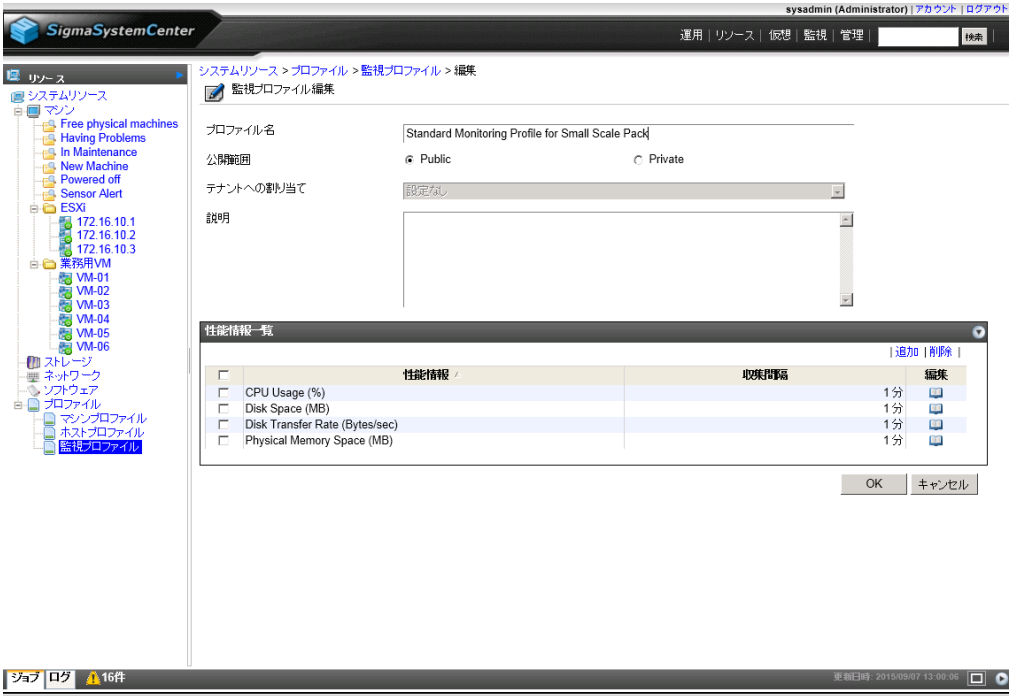

図 45 監視プロファイル編集

ここからは、個々の性能情報の設定を行います。

まず、CPU使用率が閾値に達した際に通報するための設定を行います。CPU使用率を表す **CPU Usage (%)** についての設定を変更するために、**CPU Usage (%)** の[編集]をクリックして、設定画面を表示します。

図 46 CPU Usage (%) 性能情報設定

CPU Usage (%) の閾値監視の設定を追加するので、閾値監視情報一覧画面の[追加]をクリックします。クリックすると、閾値監視設定画面が開きます。**CPU Usage (%)** が80%に達する状況が、10分間続いた場

合に通報する場合は、以下のように設定します。

有効にする:	**チェックする**（変更しません）
性能情報:	CPU Usage (%)
監視種類:	**上限異常値監視**（変更しません）
監視対象種類:	**マシン**（変更しません）
統計計算方法:	**平均値**（変更しません）
閾値:	**80**
超過通報:	**上限異常超過**
回復通報:	**上限異常回復**
超過時間:	**10**（分）
再通報する:	**チェックする**（変更しません）

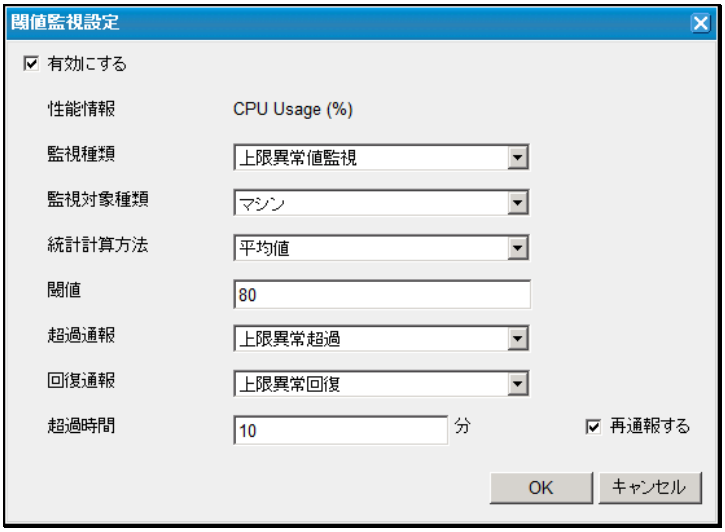

図 47　CPU Usage (%) 性能監視設定

[OK]をクリックすると、閾値監視情報一覧に設定が追加されます。

図 48　性能監視情報一覧

[OK]をクリックすると、性能情報設定が閉じます。

次に、メモリの空き容量割合について、データを収集し、閾値に達した際に通報するための設定を実施します。メモリの空き容量割合を表す **Physical Memory Space Ratio (%)** は、監視プロファイル **Standard Monitoring Profile** に含まれていないため、新たに追加する必要があります。性能情報一覧画面で[追加]をクリックして、表示された性能情報設定画面に、以下のような設定を行います。

リソース:	**Memory**
性能情報:	**Physical Memory Space Ratio (%)**
収集間隔:	1分（変更しません）

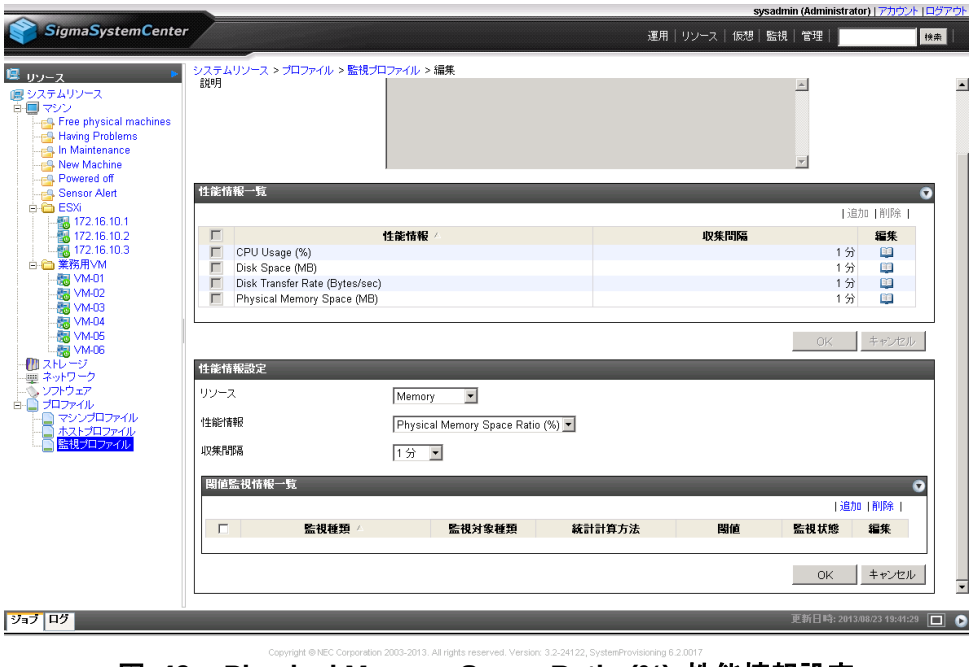

図 49 Physical Memory Space Ratio (%) 性能情報設定

Physical Memory Space Ratio (%) の閾値監視の設定を追加するので、閾値監視情報一覧画面の[追加]をクリックします。クリックすると、閾値監視設定画面が開きます。メモリの空き容量割合が10%に達する状況が、30分間続いた場合に通報する場合は、以下のように設定します。

有効にする:	**チェックする**（変更しません）
性能情報:	Physical Memory Space Ratio (%)
監視種類:	**下限異常値監視**
監視対象種類:	**マシン**（変更しません）
統計計算方法:	**平均値**（変更しません）
閾値:	**10**
超過通報:	**下限異常超過**
回復通報:	**下限異常回復**
超過時間:	**30**（分）
再通報する:	**チェックする**（変更しません）

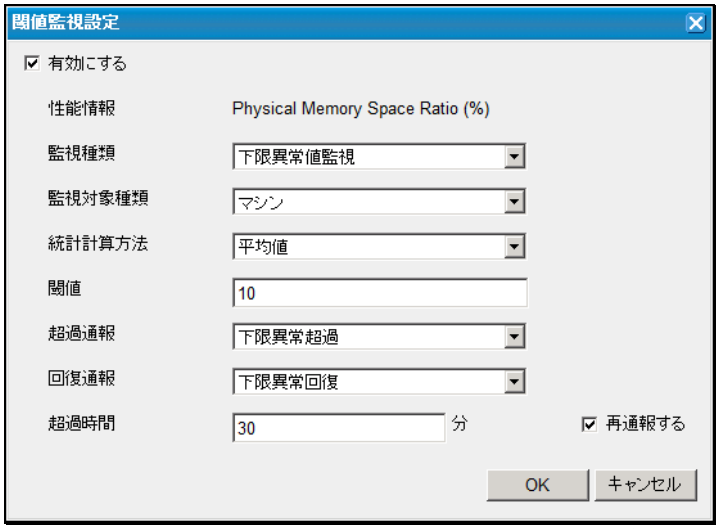

図 50　Physical Memory Space Ratio (%) 性能監視設定

[OK]をクリックすると、CPU Usage (%) の設定時と同様、閾値監視情報一覧に設定が追加されます。
性能情報設定の[OK]をクリックすると、性能情報一覧に設定が追加されます。

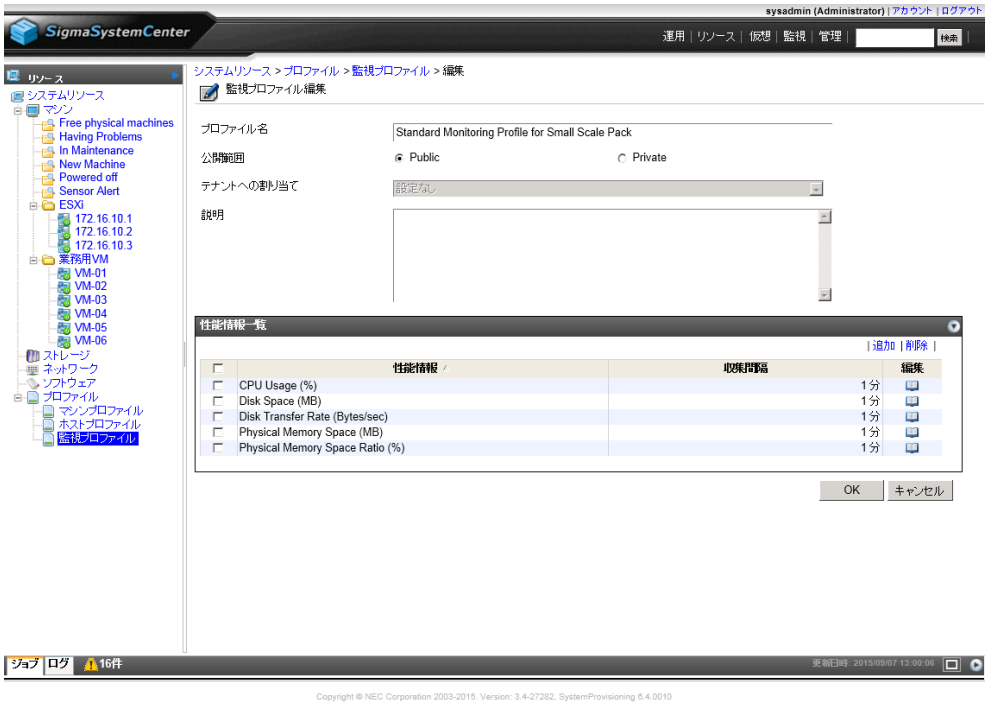

図 51　性能情報一覧

[OK]をクリックすると、監視プロファイル一覧が表示されます。監視プロファイルの名前が **Standard Monitoring Profile for Small Scale Pack** に更新されていることを確認します。

図 52 監視プロファイル一覧

これで、監視プロファイルの準備は完了です。

7.2. 物理サーバの負荷監視の設定

物理サーバ(ESXi)の負荷監視に必要な設定について説明します。

7.2.1. 物理サーバ上の設定

SSCでは、ESXiの負荷状況を取得するために、ESXiに直接アクセスして情報を取得します。ESXiにアクセスするには、十分な権限を持ったアカウントがESXi上に準備されている必要があります。負荷状況を取得するためのアカウントとしてrootを利用できますので、ESXiに対して追加の設定は不要です。

7.2.2. ESXi 用運用グループの設定

SSCがESXiの負荷状況を取得するための設定を運用ビュー(タイトルバーの[運用]をクリック)で行います。運用ビューを開いたら、ツリービューから設定対象の運用グループである[ESXi]をクリックします。ESXiの性能監視設定を行うには、[設定]メニューにある[プロパティ]をクリックしてグループのプロパティ設定画面を開き、[性能監視]タブに移動します。[性能監視]タブの各項目は、以下のように入力し、[適用]をクリックします。

性能データ収集設定:	**チェックする**
プロファイル名:	**Standard Monitoring Profile for Small Scale Pack**
IPアドレス:	**127.0.0.1**(変更しません)
ポート番号:	**26200**(変更しません)
アカウント:	**root**
パスワード更新:	**チェックする**
パスワード:	ESXiのrootのパスワード

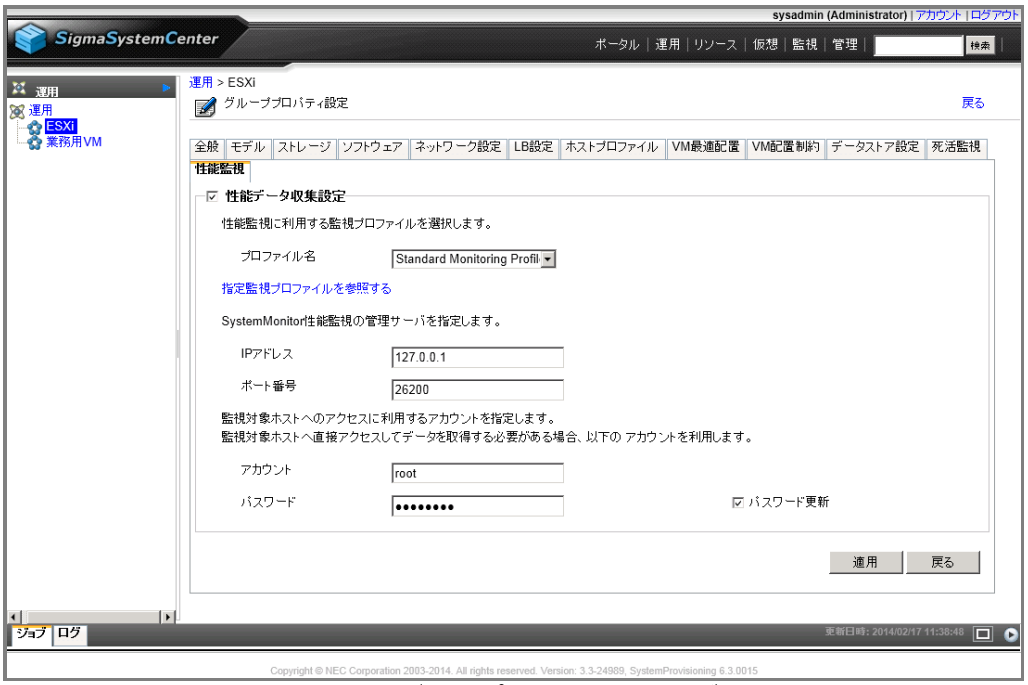

図 53 グループの「性能監視」タブ

7.3. 業務用 VM の負荷監視の設定

業務用VMの負荷監視に必要な設定について説明します。

7.3.1. 仮想マシン上の設定

SSCでは、ゲストOS（Windows Server 2008 R2）の負荷状況を取得するために、ゲストOSに直接アクセスして情報を取得します。仮想マシン上で動作しているゲストOSにアクセスするには、十分な権限を持ったアカウントがゲストOS上に準備されている必要があります。Windowsサーバから負荷状況を取得するためのアカウントとしてAdministratorを利用できますので、Administratorアカウントが有効であればWindowsサーバに対してアカウントの追加は不要です。（デフォルトではAdministratorアカウントは有効です。）

負荷状況を取得するための管理サーバからゲストOSへの通信を確保するために、ゲストOS上のWindowsファイアウォールの設定を変更する必要があります。[VM-01]に管理者権限を持つアカウントでログオンしてください。Windowsの[スタート]メニューから[管理ツール]→[セキュリティが強化された Windows ファイアウォール]をクリックします。左のツリーで[受信の規則]を選択し、以下の規則について、接続を許可します。

- ファイルとプリンターの共有（NB セッション受信）
- ファイルとプリンターの共有（NB 名受信）
- ファイルとプリンターの共有（SMB 受信）

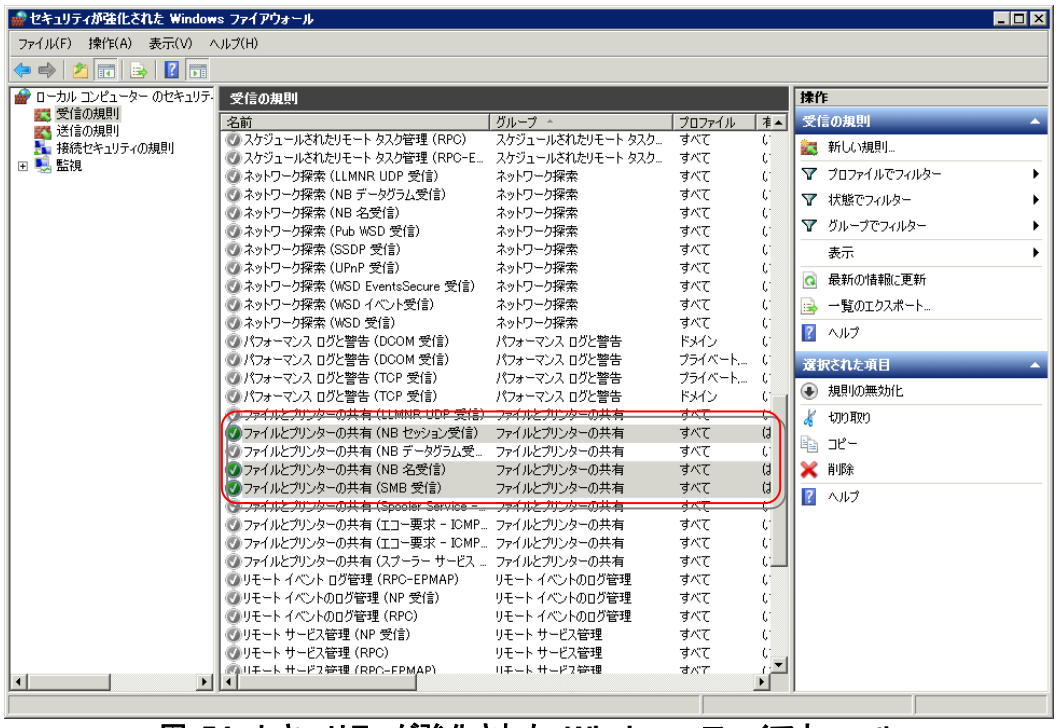

図 54 セキュリティが強化された Windows ファイアウォール

[VM-02]、[VM-03]、[VM-04]、[VM-05]、[VM-06]についても同様の設定を行います。

7.3.2. VM 用運用グループの設定

SSCがWindowsサーバの負荷状況を取得するための設定を運用ビュー（タイトルバーの[運用]をクリック）で行います。運用ビューを開いたら、ツリービューから設定対象の運用グループである[業務用VM]をクリックします。業務用VMの性能監視設定を行うには、[設定]メニューにある[プロパティ]をクリックしてグループのプ

ロパティ設定画面を開き、[性能監視]タブに移動します。[性能監視]タブの各項目は、以下のように入力し、[適用]をクリックします。

性能データ収集設定:	**チェックする**
プロファイル名:	**Standard Monitoring Profile for Small Scale Pack**
IPアドレス:	**127.0.0.1**（変更しません）
ポート番号:	**26200**（変更しません）
アカウント:	**Administrator**
パスワード更新:	**チェックする**
パスワード:	WindowsサーバのAdministratorのパスワード

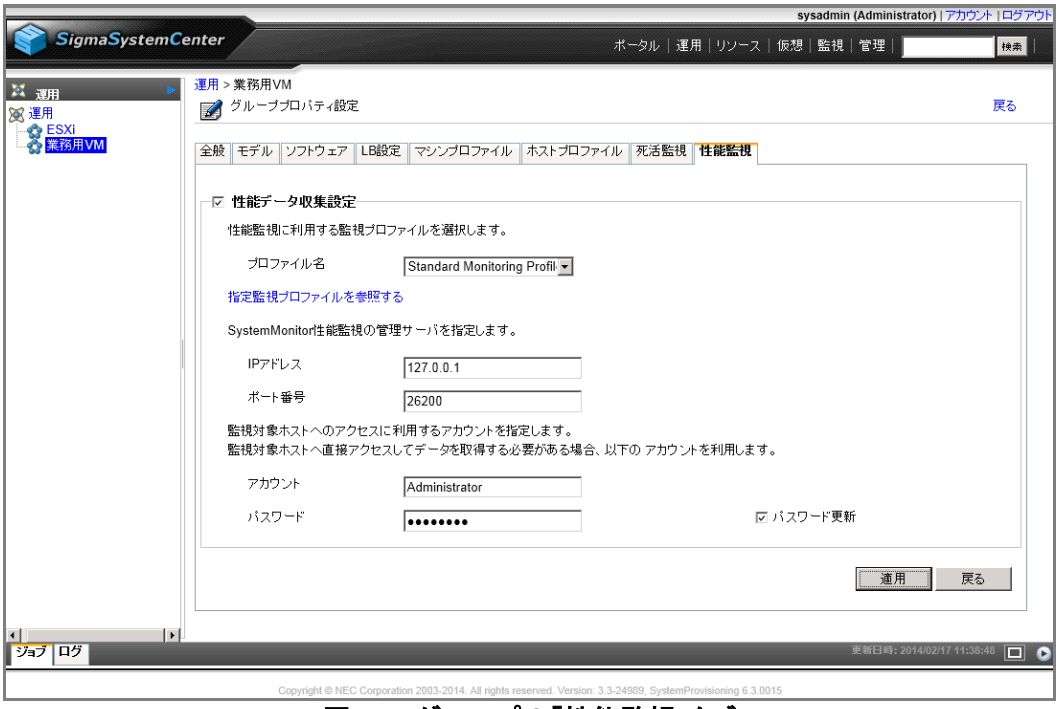

図 55 グループの「性能監視」タブ

7.4. 動作テスト

では実際に、管理対象マシン（ESXi、仮想マシン）の負荷状況をSSCのコンソール上で確認してみましょう。

※注意事項
負荷監視設定が有効化されるには、既述の設定を行ってから、デフォルトで最大10分程度必要となります。

まずは、物理サーバの負荷状況を確認します。

SSCのコンソールで負荷状況を確認するには、運用ビュー（タイトルバーの[運用]をクリック）を利用します。運用ビューを開いたら、ツリービューから設定対象の運用グループである[ESXi]をクリックします。負荷状況を確認したい物理サーバを[ホスト一覧]から確認し、グラフ表示のアイコンをクリックします。

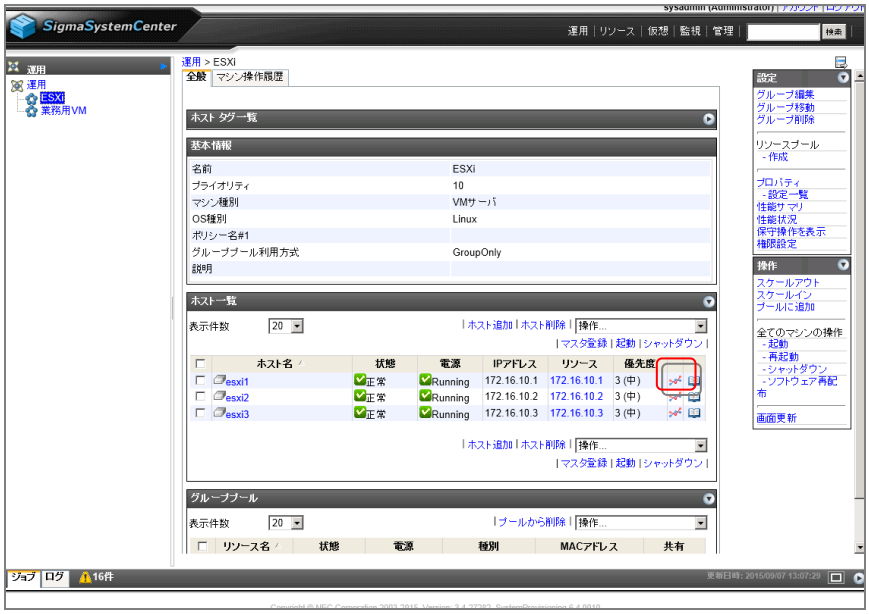

図 56 ホスト一覧

[グラフ設定]が開きますので、近々の負荷状況を確認するために、以下のように入力します。

表示期間: **1時間**

図 57 グラフ設定

[表示]ボタンをクリックすると、以下のように負荷状況がグラフ表示されます。[保存]ボタンをクリックすると、そのホストごとのグラフ設定を保存することもできます。

図 58 負荷状況

業務用VMの負荷状況についても、同様の手順で負荷状況を確認できます。

8.　障害や負荷に対するポリシーの設定

ここからは障害発生時や負荷変動に応じて仮想マシンを制御するためのポリシーの設定を行います。このポリシーは「あるイベントが発生した際にどのようなアクションを実行するか」というルールの集まりです。
例えば、「障害を示すイベントが発生した場合は、対象のサーバに故障マークを設定し通報を行う。」といった動作もポリシーで設定します。
ポリシーの設定は管理ビュー（タイトルバーの[管理]をクリック）で行います。管理ビューを開いたらツリービューにある[ポリシー]をクリックし、[ポリシー一覧]を表示させます。

図 59 ポリシー一覧

ご覧のように、ポリシー一覧にはあらかじめ4種類のポリシーが用意されています。これらの標準ポリシーはそのまま使うこともできますが、システムに合わせてテンプレートから作成したものを使うこともできます。
また、あらかじめシステムに合わせて作られたポリシーをインポートして利用することもできます。

本ガイドで想定するシステム向けには、Webサイトに仮想マシン用のポリシーと物理サーバ用のポリシーが用意されているので、今回はこれらをインポートして利用します。

8.1.　ポリシーのインポート

Webサイトから以下のファイルをダウンロードし、管理サーバの適当なフォルダに保存します。今回は、<***C:¥temp***> に保存したとします。

- vm_policy.xml　：仮想マシン用ポリシー
- esxi_policy.xml ：物理サーバ（仮想マシンサーバ）用ポリシー

まず、仮想マシン用のポリシーファイルである[**vm_policy.xml**]をインポートします。

Windowsの[スタート]メニューから[すべてのプログラム]→[アクセサリ]→[コマンド プロンプト]をクリックします。「コマンド プロンプト]が起動したら、次のようにsscコマンドを実行してください。

```
> ssc import policy "C:¥temp¥vm_policy.xml"
```

実行後に[実行終了　　コード:0]が表示されれば、インポートが完了しています。
同様に、物理サーバ用の[**esxi_policy.xml**]もインポートしてください。

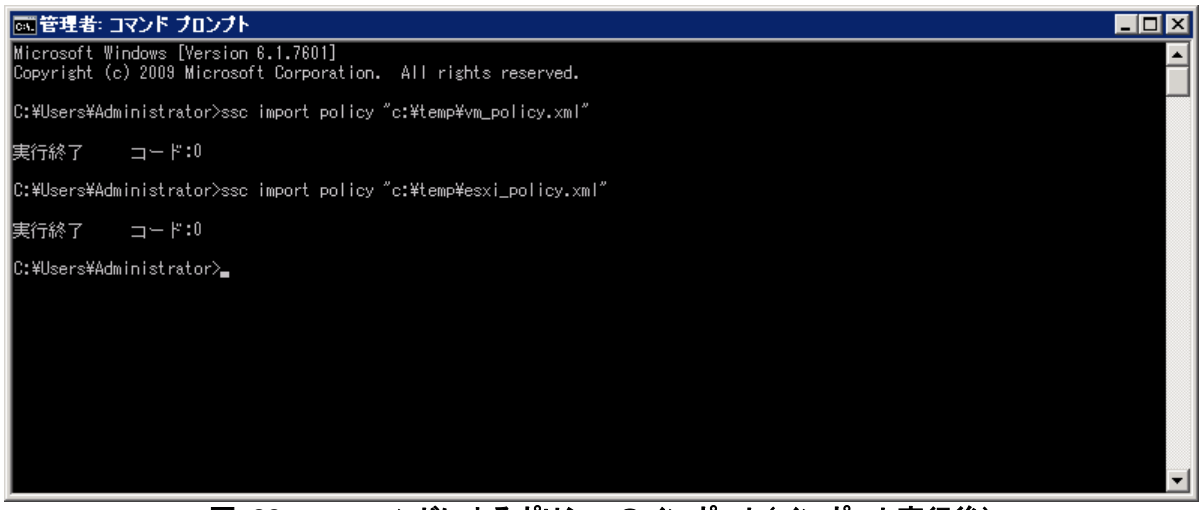

図 60　sscコマンドによるポリシーのインポート（インポート実行後）

二つのポリシーのインポートが完了したらSSCのWebコンソールに戻り、[ポリシー一覧]画面の[操作]メニューの[画面更新]をクリックしてください。

図 61　ポリシー一覧（インポート後）

ポリシー一覧に「仮想マシンサーバ用ポリシー」と「仮想マシン用ポリシー」が表示されます。

8.2. 仮想マシン用ポリシーの確認と適用

「6 運用の基本設定」で設計したように仮想マシン用のグループ（業務用VMグループ）に、先ほどインポートした仮想マシン用のポリシーを適用することにします。

8.2.1. 仮想マシン用のポリシーの確認

ポリシーを適用する前にどのようなルールが定義されているのかを確認しておきましょう。管理ビューを開いたらツリービューにある[ポリシー]をクリックし、[ポリシー一覧]を表示させます。

仮想マシン用にインポートしたポリシーは、[仮想マシン用ポリシー]です。[仮想マシン用ポリシー]の[プロパティ]アイコンをクリックしてポリシープロパティ設定画面を開き[ポリシー規則]タブをクリックします。
[ポリシー規則一覧]の枠の[状態]が[有効]になっているイベントに注目します。
[仮想マシン用ポリシー]では大まかに次の考えに基づいた設定がデフォルトとなっています。

- 仮想マシンが停止している可能性がある場合
  対処として、故障マーク設定と通報、イベントログ出力を行います。
  「ターゲットアクセス不可」、「マシン停止」が該当します。

- 仮想マシンの負荷が設定したしきい値を上回った（下回った）場合
  対処として、通報、イベントログ出力を行います。
  「CPU使用率（%）異常（回復）」、「メモリ空き容量割合（%）異常（回復）」が該当します。

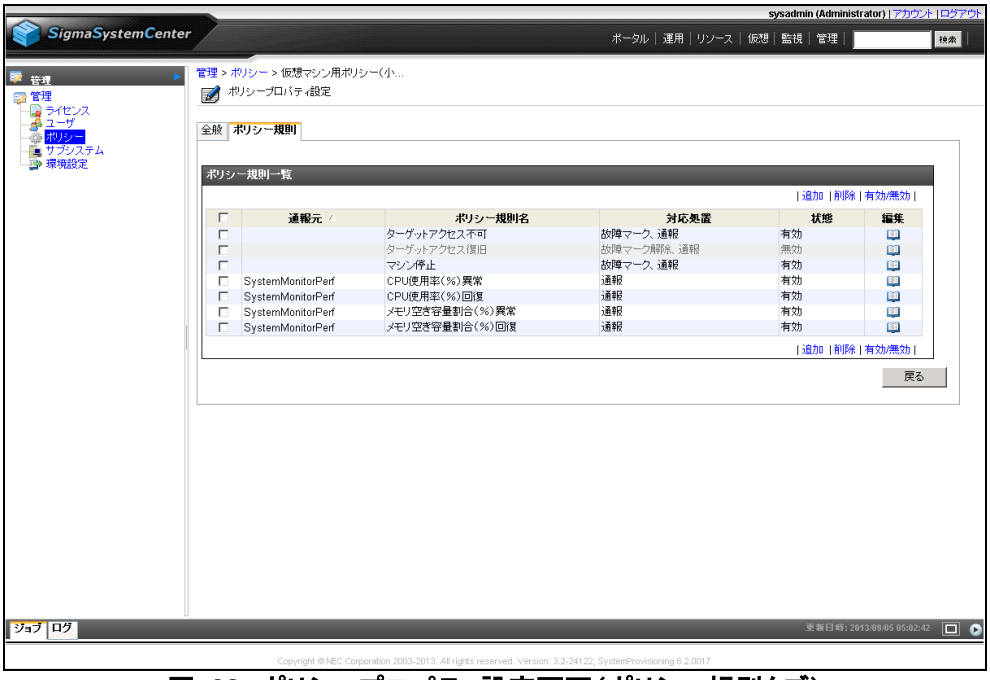

図 62 ポリシープロパティ設定画面（ポリシー規則タブ）

次に、イベントが発生した際に実行する対応処置の詳細を確認します。
「ターゲットアクセス不可」ではPing監視とポート監視によって仮想マシンの死活監視を行っています。「**ターゲットアクセス不可**」イベントの列の[編集]アイコンをクリックすると、[ポリシー規則設定（編集）]画面が表示されます。
この画面（ポリシー規則設定（編集））では、監視するイベントの情報とそのイベントが発生した際に実行する処理（アクション）を確認、設定することができます。

画面上ではイベントを定義し、そのイベントに対し、画面下にある[イベントに対するアクション]の枠内で実行するアクションを設定します。
デフォルトでは、1番目のアクションとして[通報/ E-mail通報、イベントログ出力]、2番目のアクションとして[マシン設定/ ステータス設定　故障]が設定されていることが確認できます。

仮想マシンがPing監視、ポート監視で反応がない場合には、通報/ E-mail通報、イベントログ出力を行い、故障マークを設定する。という動作を行うことが分かります。

今回はデフォルト設定を利用するので、何も変更せずに画面下の[戻る]ボタンをクリックします。

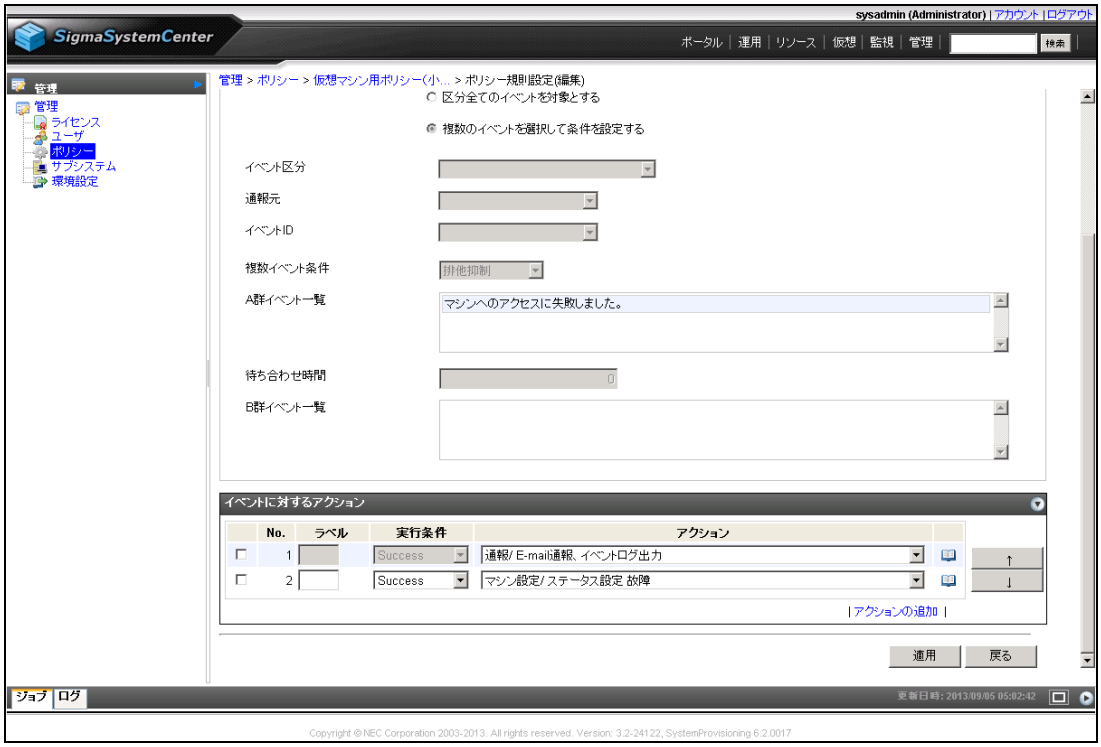

図　63　対応処置詳細設定（編集）

8.2.2.　仮想マシン用のポリシーの適用

運用ビューで作成したグループ単位にポリシーを適用するため、運用ビューのグループプロパティ設定画面で適用作業を行います。
まず、[VM-01]、[VM-02]、[VM-03]、[VM-04]、[VM-05]、[VM-06]にポリシーを適用するために、[業務用VM]グループに先ほどインポートした[**仮想マシン用ポリシー**]を適用することにします。手順は以下のとおりです。

- タイトルバーの[運用]をクリック
- ツリービューで対象グループ（ここでは[**業務用VM**]）をクリック
- [設定]メニューの[プロパティ]をクリック
- [全般]タブをクリック
- [ポリシー名#1]のドロップダウンリストで適用するポリシー（ここでは[**仮想マシン用ポリシー**]）を選択
- 右下の[適用]ボタンをクリック後、[戻る]ボタンをクリック

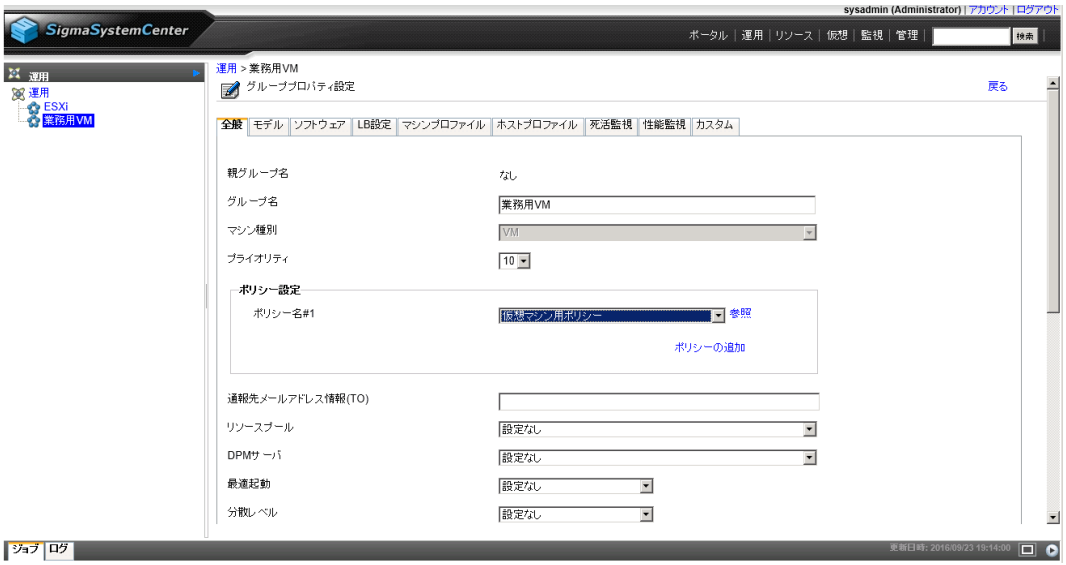

図 64 仮想マシン用ポリシーの適用

以上で仮想マシンへのポリシー適用は終了です。

8.3. 物理サーバ用ポリシーの確認と適用

仮想マシンの次は、物理サーバであるESXi用のポリシーを用意します。物理サーバのグループ（ESXiグループ）にも仮想マシン用ポリシーと同様に、先ほどインポートしたポリシーを適用します。

8.3.1. 物理サーバ用のポリシーの確認

仮想マシン用と同様に、ポリシーを適用する前にどのようなルールが定義されているのかを確認します。管理ビューを開いたらツリービューにある[ポリシー]をクリックし、[ポリシー一覧]を表示させます。

物理サーバであるESXi用にインポートしたポリシーは、[仮想マシンサーバ用ポリシー]です。[仮想マシンサーバ用ポリシー]の[プロパティ]アイコンをクリックしてポリシープロパティ設定画面を開き[ポリシー規則]タブをクリックします。
[ポリシー規則一覧]の枠の[状態]が[有効]になっているイベントに注目します。
[仮想マシンサーバ用ポリシー]では大まかに次の考えに基づいた設定がデフォルトとなっています。

- イベント発生時点、ESXiが機能停止している可能性が高い障害
  対処として、故障マーク設定、通報、イベントログ出力を行った上で、他のESXiへVMを移動し、再起動（Failover）を行います。
  「CPU温度異常」、「VMSアクセス不可」が該当します。
  ※ vCenter上でvSphere HAを利用する設定をしているESXiに対しては、SSCの再起動（Failover）アクションが動作しないようにしてください。障害発生時に双方の復旧処理が競合し、意図しない動作となる可能性があります。
  SSCの再起動（Failover）アクションを動作させないためには、次の3つのいずれかの方法があります。
  1. 運用ビューのグループのプロパティのポリシー設定で再起動（Failover）アクションを含むポリシーを設定しない。
  2. ポリシー規則一覧で再起動（Failover）アクションを含むポリシー規則を無効に設定する。
  3. ポリシー規則の設定のイベントに対するアクションから再起動（Failover）アクションを削除する。

- イベント発生時点、ESXiは稼働しているが、即時に停止させたほうがよい障害
  対処として、故障マーク設定、通報、イベントログ出力を行った上で、ESXiとVMをシャットダウン（できない場合は強制停止）します。その後、別のESXiでVMの再起動（Failover）を行います。
  「ファン/冷却装置異常(復旧不能)」、「電圧異常(復旧不能)」、「筐体温度異常(復旧不能)」が該当します。

- イベント発生時点、ESXiは稼働しているが、その後、致命的な障害に陥る可能性がある障害
  対処として、故障マーク設定、通報、イベントログ出力を行った上で、他のESXiへVMの移動を行います。まず、マイグレーション（vMotion）によりVMを稼働させたままの移動を試し、マイグレーションできない場合には続けて再起動（Failover）を試します。
  その後、障害イベントが発生したESXiを停止させます。
  「予兆：〇〇」が該当します。

- イベント発生時点、ストレージに異常がある場合
  対処として、故障マーク設定、通報、イベントログ出力を行った上で、他のESXiへVMの移動を行います。まず、マイグレーション（vMotion）によりVMを稼働させたままの移動を試し、マイグレーションできない場合には、ESXiとVMをシャットダウン（できない場合は強制停止）し、VMの再起動（Failover）を行います。

「ハードディスク障害」が該当します。

- イベント発生時点、ストレージパスに異常がある場合
  対処として、故障マーク設定、通報、イベントログ出力を行った上で、他のESXiへVMの移動を行います。まず、マイグレーション（vMotion）によりVMを稼働させたままの移動を試し、マイグレーションできない場合には続けて再起動（Failover）を試します。「ストレージパス冗長性喪失」、「ストレージパス冗長性低下」が該当します。

- イベント発生時点、ハードウェア自身の機能により縮退動作している場合
  対処として、故障マークを設定、通報、イベントログ出力を行います。
  「CPU障害」、「メモリ縮退障害」が該当します。

- イベント発生時点、経過を観察する判断になる障害、効果的な対応処置がない障害
  対処として、故障マークを設定、通報、イベントログ出力を行います。
  「メモリ障害」が該当します。

- ESXiの負荷が設定したしきい値を上回った（下回った）場合
  対処として、通報、イベントログ出力を行います。
  「CPU使用率（%）異常（回復）」、「メモリ空き容量割合（%）異常（回復）」が該当します。

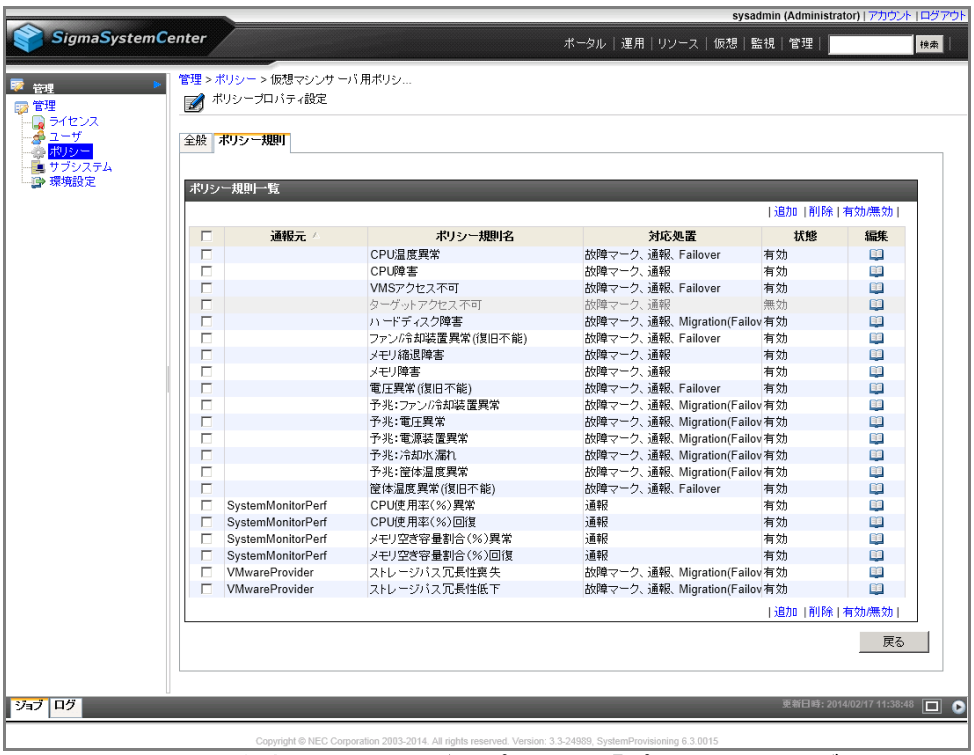

図 65　仮想マシンサーバ用ポリシーの「ポリシー規則」タブ

8.3.2. 故障状態の物理サーバの制約と故障状態の解除

先ほどのポリシーで故障マークを設定した物理サーバであるESXiは、下の図のように[ハードウェアステータス]に[故障]と表示されます。

図 66 障害発生後の物理サーバの詳細情報(リソースビュー)

故障状態になったESXiでは、仮想マシンを新たに起動できないようにSSCの動作が制限されます。故障状態になったESXiをマイグレーション(vMotion)やFailoverによる仮想マシンの移動先とすることもできません。
まず、ESXiで発生した障害を解消することは当然のことですが、さらに、故障状態を解除することでESXiを通常の運用で利用できるようにする必要があります。
SSCで故障状態を解除するためには、次の操作をおこないます。

- タイトルバーの[リソース]をクリック
- リソースビューが表示されたら、ツリービューで、故障マークがついているESXiをクリック
- ESXiの詳細画面が表示されたら、中央の[マシンステータス情報]の枠の[ハードウェアステータス]の[(状態詳細)]をクリック
- 状態詳細画面が表示されたら、[状態一覧]の枠の[状態]が**[正常]以外**のステータス名のチェックボックスをチェックし、右上の[リセット(正常)]をクリック
- 再び、ツリービューで、故障マークがついているESXiをクリック
- 左側の[操作]メニューの[故障状態の解除]をクリック

SSCでは自動的に故障状態を解除するポリシーを設定することもできますが、管理者がESXiに問題ないことを実際に確認した上で、手動で故障状態を解除することをお勧めします。

8.3.3. 物理サーバ用のポリシーの適用

監視イベントを確認したところで、仮想マシンと同様に運用ビューのグループプロパティ設定画面でポリシーの適用作業を行います。
[esxi1]、[esxi2]にポリシーを適用するために、[ESXi]グループに先ほどインポートした[**仮想マシンサーバ用ポリシー**]を適用することにします。手順は以下のとおりです。

- タイトルバーの[運用]をクリック
- ツリービューで対象グループ（ここでは[**ESXi**]）をクリック
- [設定]メニューの[プロパティ]をクリック
- [全般]タブをクリック
- [ポリシー名#1]のドロップダウンリストで適用するポリシー、ここでは[**仮想マシンサーバ用ポリシー**]を選択
- [適用]ボタンをクリック後、[戻る]ボタンをクリック

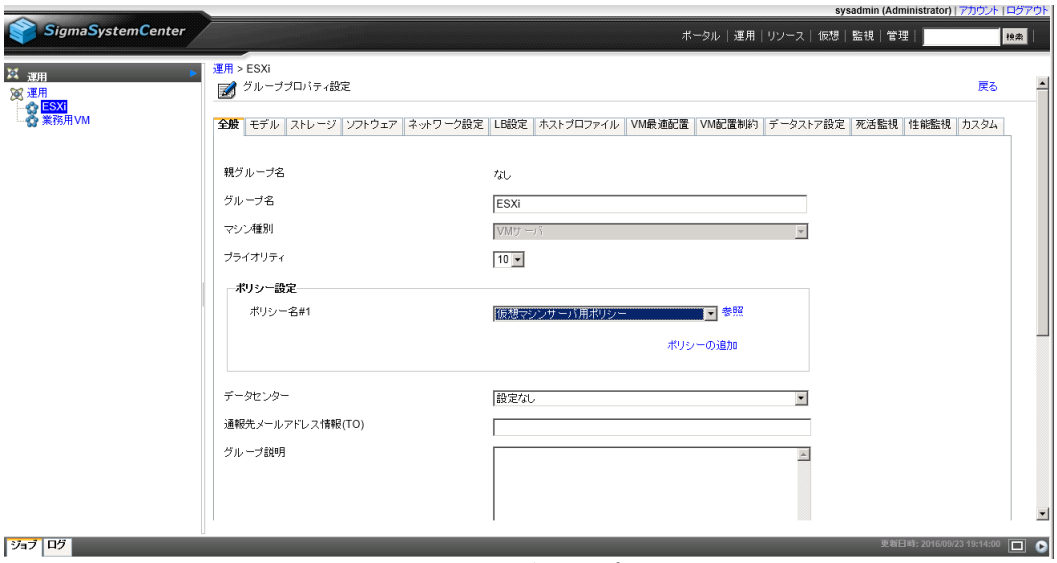

図 67 物理サーバへのポリシー適用

8.4. 死活監視の設定

死活監視を行うには、「4.3 死活監視の基本設定」で説明した共通の基本設定を行った上で、それぞれのグループ、または、ホストへの設定を行います。
今回は、「6.1 運用グループの作成」で作成したグループの単位で死活監視の設定を行います。

8.4.1. グループ単位の死活監視の設定

グループ単位の死活監視の設定を行うには、運用ビュー（タイトルバーの[運用]をクリック）を開きます。

まずは、[業務用VM]グループの設定を行うことにします。業務用VMに先ほど適用した[**仮想マシン用ポリシー**]では、Ping監視、ポート監視のイベント（ターゲットアクセス不可）に対処するようになっています。

今回、業務用VMグループの仮想マシンではWebサーバが動作しているものとして、Port監視では**80**を監視します。次の手順で、Ping監視、ポート監視を行うように設定します。

- ツリービューにある[**業務用VM**]グループをクリック
- [設定]メニューの[プロパティ]をクリック
- グループプロパティ画面が開いたら[死活監視]タブをクリック
- [死活監視機能を有効にする]チェックボックスをチェック
- [Ping監視]チェックボックスをチェック
- [Port監視]チェックボックスをチェックし、[監視ポート]に[***80***]を入力
- 右下の[適用]ボタンを押す

図 68 グループプロパティ設定画面（死活監視タブ）、Ping監視、Port監視の設定

ESXiグループの物理マシンに先ほど適用した[**仮想マシンサーバ用ポリシー**]では、vCenter Serverを利用した死活監視のイベント（VMSアクセス不可）に対処するようになっています。
ESXiグループの物理マシンについては、ESMPROによる死活監視を行わないので、次の手順でESMPRO

による監視を無効にします。

- ツリービューにある[**ESXi**]グループをクリック
- [設定]メニューの[プロパティ]をクリック
- グループプロパティ画面が開いたら[死活監視]タブをクリック
- [ESMPRO/SMに登録する]チェックボックスのチェックを外す
- 右下の[適用]ボタンを押す

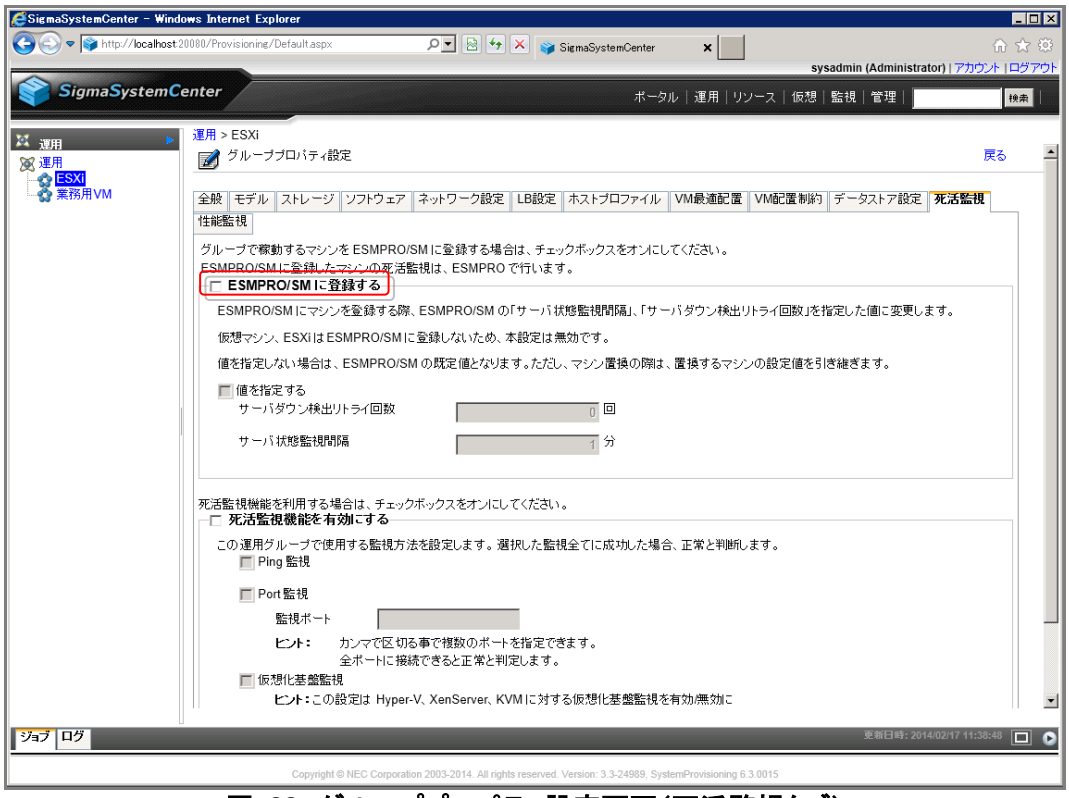

図 69 グループプロパティ設定画面（死活監視タブ）

8.5. 動作テスト

ポリシーを適用したところで、ひとまず動作テストを行ってみます。今回は物理サーバ[esxi1]に擬似的なストレージ障害を発生させることで、[仮想マシンサーバ用ポリシー]の[ストレージパス冗長性喪失]イベントへの対応処置をテストします。
「8.3.1　物理サーバ用のポリシーの確認」で説明したとおり、[ストレージパス冗長性喪失]イベントの対応処置は、故障マーク設定、通報、イベントログ出力、そして、VMの他のESXiへの移動です。テストでは、SSCのGUIで擬似障害を発生させた物理サーバ[esxi1]に故障マークが付き、[esxi1]上の仮想マシンが他のESXiに移動されることを確認します。

まず、Webサイトから[***擬似イベント発生ツール***]の圧縮ファイルをダウンロードし、管理サーバの適当なフォルダに解凍・保存します。今回は、<***C:¥temp***>に保存したとします。

Windowsの[スタート]メニューから[すべてのプログラム]→[アクセサリ]→[コマンド プロンプト]をクリックします。「コマンド プロンプト]が起動したら、次のようにカレントディレクトリを<***C:¥temp***>に移動します。

```
> cd ¥temp
```

次に、<***C:¥temp***>内に保存した[***擬似イベント発生ツール(sendevent.exe)***]を次のように実行します。

```
> sendevent localhost VMwareProvider "Storage path redundancy on VMS
  is lost" test ESXi esxi1
```

障害がどのように見えるか確認しましょう。
まず、タイトルバーの[運用]をクリックし、運用ビューを開きます。ツリービューの[ESXi]グループに故障マーク(赤い×アイコン)が付いているのが確認できるので、[**ESXi**]グループをクリックします。
[全般]タブの[ホスト一覧]の枠を見ると、[esxi1]が[故障]状態であることが分かります。

図 70 障害発生時の運用ビュー

[ホスト一覧]の枠の[esxi1]のリソース[**172.16.10.1**]をクリックし、リソースの状態を確認してみます。
下の図のように[リソース]ビューでリソース[172.16.10.1]の状態が表示されます。[マシンステータス情報]の枠を見ると、やはり[故障]であることが分かります。

図 71 障害発生時のリソースビュー

さらに、[運用情報]の枠の[仮想パス]の[**virtual:/172.16.0.1/新規データセンター/172.16.10.1**]をクリックし、仮想ビューを確認してみます。
下の図のように、仮想ビューのツリービュー上でも[172.16.10.1]に故障マークが表示され、故障状態にある

ことが分かります。さらに、各ESXiのツリーを展開すると、[172.16.10.1]の配下にあった[VM-01]が別のESXiの配下に移動していることが分かります。
ちなみに、擬似障害の投入直後のVMの移動が完了していない場合、[172.16.10.1]の配下に[VM-01]が残っていることがあります。その場合は、しばらく時間をおいてから右側[操作]メニューの[画面更新]をクリックし、VMが移動したことを確認してください。
また、各ESXiで稼働しているVMの一覧は、中央の[稼働中VM一覧]の枠でも見ることができます。

図 72 障害発生時の仮想ビュー

次に、[172.16.10.1]の[運用情報]の枠の[ハードウェアステータス]の[**(状態詳細)**]をクリックしてみます。
[172.16.10.1]の[状態詳細]が表示され、[状態一覧]の枠の[**ストレージ接続性**]の状態が[**一部故障**]となっていることが分かります。

図 73 [172.16.10.1]の状態一覧画面

最後に、テストの確認が終わったら、仮想ビューで故障状態を解除し、[172.16.10.1]の配下に[VM-01]と

[VM-02]を移動しておきます。

ツリービューの[172.16.10.1]をクリックし、[172.16.10.1]を選択状態にします。左の[操作]メニューから[**故障状態の解除**]をクリックすると、故障状態がクリアされ、ステータスが[正常]に変わります。

[172.16.10.1]の配下へのVMの移動は、次のように行います。

- [172.16.10.2](esxi2)、または、[172.16.10.3](esxi3)の[稼働中VM一覧]の枠に表示されている[VM-01]と[VM-02]のチェックボックスをチェック
- [稼働中VM一覧]の枠の右上のアクションメニューの[VM移動]をクリック
- VM移動画面が表示されたら、[移動先データセンタ名]のドロップダウンリストから移動先となる「172.16.10.1」(esxi1)がvCenter上で属しているデータセンタを選択
- [172.16.10.1](esxi1)のラジオボタンをチェック
- [VM移動方法の指定]では[Migration]のチェックボックスをチェック
- [OK]をクリック

VMが移動する時間をしばらく待ち、ツリービューなどで[172.16.10.1](esxi1)に[VM-01]と[VM-02]が移動したことを確認します。仮想マシンの移動がツリービューに反映されていない場合は[操作]メニューの[画面更新]をクリックしてみてください。

付録

付録 A　　運用に関する重要な情報

仮想マシンサーバと仮想マシンの操作

以下のような仮想マシンサーバと仮想マシンについての操作は SSC で実施し、vCenter Server やオペレーティングシステムから直接実施しないでください。

- 電源の On/Off
- ハイパーバイザーやオペレーティングシステムのシャットダウン

上記の操作を行うことで、仮想マシンサーバや仮想マシンの実際の状態と SSC の収集した状態との間にずれが生じることがあるためです。
さらに、SSC からこの状態のずれが生じている仮想マシンサーバや仮想マシンの操作を行った場合、その操作が失敗することもあります。

実際のマシンの状態と SSC の収集した状態との間にずれが生じた場合や、ずれが原因で操作が失敗した場合は、「**マシンの状態のずれを解消する**」の対処を行ってください。

マシンの状態のずれを解消する

仮想マシンサーバや仮想マシンの実際の状態と SSC の収集した状態との間にずれを解消するには、以下のように**仮想ビュー**で仮想マシンサーバの状態の**収集**を行います。
タイトルバーの[仮想]をクリック
ツリービューで、ずれが生じている仮想マシンサーバ（ESXi）、または、ずれが生じている仮想マシンが稼働している仮想マシンサーバ（ESXi）を選択
[操作]メニューの[**収集**]をクリック

マシンの状態のずれが原因で SSC の操作が失敗していた場合は、マシンの状態の収集を行った後でもう一度失敗した操作を行います。

付録 B　SigmaSystemCenter マニュアル体系

SigmaSystemCenter のマニュアルは、各製品、およびコンポーネントごとに以下のように構成されています。
また、本書内では、各マニュアルは「本書での呼び方」の名称で記載します。

製品 / コンポーネント名	マニュアル名		本書での呼び方
WebSAM SigmaSystemCenter 3.5	WebSAM SigmaSystemCenter 3.5 ファーストステップガイド		SigmaSystemCenter ファーストステップガイド
	WebSAM SigmaSystemCenter 3.5 インストレーションガイド		SigmaSystemCenter インストレーションガイド
	WebSAM SigmaSystemCenter 3.5 コンフィグレーションガイド		SigmaSystemCenter コンフィグレーションガイド
	WebSAM SigmaSystemCenter 3.5 リファレンスガイド	概要編	SigmaSystemCenter リファレンスガイド 概要編
		データ編	SigmaSystemCenter リファレンスガイド データ編
		注意事項、トラブルシューティング編	SigmaSystemCenter リファレンスガイド 注意事項、トラブルシューティング編
		Webコンソール編	SigmaSystemCenter リファレンスガイド Webコンソール編
SystemMonitor性能監視 5.7	SystemMonitor性能監視 5.7 ユーザーズガイド		SystemMonitor性能監視 ユーザーズガイド

関連情報: SigmaSystemCenter のすべての最新のマニュアルは、以下の URL から入手できます。
http://jpn.nec.com/websam/sigmasystemcenter/index.html
→「ダウンロード」

SigmaSystemCenterの製品概要、インストール、設定、運用、保守に関する情報は、以下の４つのマニュアルに含みます。各マニュアルの役割を以下に示します。

「SigmaSystemCenter ファーストステップガイド」
SigmaSystemCenter を使用するユーザを対象読者とし、製品概要、システム設計方法、動作環境などについて記載します。

「SigmaSystemCenter インストレーションガイド」
SigmaSystemCenterのインストール、アップグレードインストール、およびアンインストールを行うシステム管理者を対象読者とし、それぞれの方法について説明します。

「SigmaSystemCenter コンフィグレーションガイド」
インストール後の設定全般を行うシステム管理者と、その後の運用・保守を行うシステム管理者を対象読者とし、インストール後の設定から運用に関する操作手順を実際の流れに則して説明します。また、保守の操作についても説明します。

「SigmaSystemCenter リファレンスガイド」
SigmaSystemCenterの管理者を対象読者とし、「SigmaSystemCenter インストレーションガイド」、および「SigmaSystemCenter コンフィグレーションガイド」を補完する役割を持ちます。
SigmaSystemCenter リファレンスガイドは、以下の 4 冊で構成されています。

「SigmaSystemCenter リファレンスガイド データ編」
SigmaSystemCenter のメンテナンス関連情報などを記載します。

「SigmaSystemCenter リファレンスガイド 注意事項、トラブルシューティング編」
SigmaSystemCenter の注意事項、およびトラブルシューティング情報などを記載します。

「SigmaSystemCenter リファレンスガイド 概要編」
SigmaSystemCenter の機能説明などを記載します。

「SigmaSystemCenter リファレンスガイド Web コンソール編」
SigmaSystemCenter の操作画面一覧、および操作方法などを記載します。

付録 C　　用語集

英数字

BMC

"Baseboard Management Controller (ベースボードマネージメントコントローラ)" の略です。

DHCP サーバ

DHCPとは、"Dynamic Host Configuration Protocol" の略です。DHCPサーバとは、ネットワークにおいて、コンピュータに動的にIPアドレスを割り当てるための機能を実装したサーバです。DHCPクライアントからの要求により、あらかじめ用意したIPアドレス、サブネットマスク、ドメイン名などの情報を割り当てます。

DPM

"DeploymentManager" の略です。SystemProvisioningからの指示により、管理対象マシンへOS、アプリケーション、パッチなどのソフトウェアの配布、更新やマシンの起動、停止を行います。

ESMPRO/ServerManager
ESMPRO/ServerAgent

Express5800シリーズに標準添付のマシン管理ソフトウェアです。SigmaSystemCenterは、管理対象マシンが物理マシンの場合にESMPRO/ServerManagerを介してマシンを監視します。

ESXi

スタンドアロン環境で仮想マシンを実現できるVMware社の製品です。

vCenter Serverを介して管理することも、SystemProvisioningから直接管理することもできます。SystemProvisioningから直接管理されるESXiを "スタンドアロンESXi" と呼びます。また、ESXiの管理・運用形態について、vCenter Serverを使用した運用を "vCenter Server環境での運用"、SystemProvisioningから直接管理する運用を "スタンドアロン環境での運用" と呼びます。

IIS

"Internet Information Services" の略で、Microsoft社が提供するインターネットサーバ用ソフトウェアです。

IPMI

"Intelligent Platform Management Interface (インテリジェントプラットフォームマネージメントインターフェース)" の略です。装置に対して、センサ情報の取得、電源操作、装置のログを取得するインターフェースを提供します。

Migration

Migrationは、共有ディスク上に存在する仮想マシンを別の仮想マシンサーバに移動します。仮想マシンの電源がオンの場合、稼動状態のままライブマイグレーションします (Hot Migration)。仮想マシンの電源がオフの場合は、電源オフの状態のまま移動します (Cold Migration)。電源オンの状態の仮想マシンをサスペンド状態にして移動させる方法は、Quick Migrationと呼びます。

OOB	"Out-of-Band (アウトオブバンド)" の略です。ハードウェア上で動作しているソフトウェアとの通信ではなく、直接ハードウェアに対して管理、操作を行う管理方法です。
PET	"Platform Event Trap" の略です。 BIOSやハードウェアで発生したイベントを、SNMPトラップを利用してBMCなどから直接通報するものです。
RMCP/RMCP+	"Remote Management Control Protocol (リモートマネージメントコントロールプロトコル)" の略です。IPMIの命令をリモートからネットワークを介して実行するプロトコルです。UDPを使います。
SNMP Trap (SNMP トラップ)	SNMP (Simple Network Management Protocol、簡易ネットワーク管理プロトコル) における通信で、SNMPエージェントがイベントをマネージャに通知することです。
SQL Server	Microsoft社が提供している、リレーショナルデータベースを構築・運用するための管理ソフトウェアです。SigmaSystemCenterは、システムの構成情報を格納するデータベースとしてSQL Serverを使用します。
SystemMonitor 性能監視	マシンリソースの使用状況などを監視するSigmaSystemCenterのコンポーネントです。性能障害発生時にはSystemProvisioningに通報することも可能です。
SystemProvisioning	SigmaSystemCenterの中核となるコンポーネントです。管理対象マシンの構築、構成情報の管理、構成変更、マシン障害時の自律復旧などを行います。
vCenter Server	複数のESX、およびその上に構成された仮想マシンを統合管理するためのVMware社の製品です。
vSphere Client	仮想マシン、および仮想マシンのリソースとホストの作成、管理、監視を行うユーザインターフェースを備えたVMware社の製品です。
VM	"Virtual Machine" の略です。仮想マシンと同じです。「仮想マシン」の項を参照してください。
VMS	"Virtual Machine Server" の略です。仮想マシンサーバと同じです。「仮想マシンサーバ」の項を参照してください。
VM サーバ	仮想マシンサーバを指します。

Web コンソール

Webコンソールには、SigmaSystemCenterのWebコンソールとDPMのWebコンソールの2種類があります。本書で、Webコンソールと記載している場合、SigmaSystemCenterのWebコンソールを指します。SigmaSystemCenterのWebコンソールは、ブラウザからSigmaSystemCenterの設定や運用を行うものです。DPMのWebコンソールは、ブラウザからDPMサーバを操作するものです。

か

SSC 小規模仮想化運用パック

VMware vSphere Essentials Plusを導入している仮想化環境を管理対象としたSigmaSystemCenterと専用のマニュアル、ポリシーのパック製品です。

仮想マシン

仮想マシンサーバ上に仮想的に実現されたマシンを指します。

仮想マシンサーバ

仮想マシンを実現するためのサーバを指します。

SystemProvisioningでは、VMware ESX、ESXi、Citrix XenServer、Microsoft Hyper-V、Red Hat KVMを管理対象とすることができます。

稼動

SigmaSystemCenterでホストにマシンを割り当て、グループに登録した状態を指します。

監視対象マシン

SystemMonitor性能監視により監視されているマシンです。

管理サーバ

SystemProvisioningがインストールされたサーバです。

管理対象マシン

SystemProvisioningで管理対象とするマシンです。

共有ディスク

複数のマシンで共有できるディスクボリュームを指します。

グループ

SystemProvisioningは、運用時にマシンをグループ単位で管理します。グループ管理により、マシン管理の負担を軽減し、運用コストを削減することができます。このような同じ用途で使用するマシンの集合を運用グループと呼びます。SystemProvisioningで、"グループ" という場合、"運用グループ" を指します。

また、SystemProvisioningでは、管理対象マシンをリソースとして管理します。Webコンソールの [リソース] ビューでは、管理対象マシンを分類表示するためのグループを作成することができます。こちらは、"リソースグループ" と呼びます。

さ

閾値

SigmaSystemCenterに含まれるESMPROやSystemMonitor性能監視などの監視製品は、管理対象のデータと閾値を比較して、異常 / 正常状態を判断しています。

スタンドアロン ESXi

VMware vCenter Serverを使用しないで、SystemProvisioningから直接管理されるESXiを指します。

スマートグループ

管理対象マシンの検索条件を保持する論理的なグループです。検索条件に合致する管理対象マシンが検索できます。

また、電源状態など、逐次変化するステータス情報を検索条件として設定することもできます。

た

タグクラウド

管理対象マシンの様々な情報を "タグ" として分類・集計し、管理対象マシン全体の情報を "タグの集合" として視覚的に表示する機能です。

また、"タグ" を選択することで、そのタグに分類されたマシンのみを絞り込むことができます。

データセンタ

仮想マシンサーバを束ねる役割を持ちます。

vCenter Server環境を管理する場合には、vCenter Serverのデータセンタと対応しています。vCenter Serverのクラスタは、SigmaSystemCenterではデータセンタと同等に扱います。

は

復旧処理設定

イベントが発生した際に行う復旧処理を定めた設定です。

SystemProvisioningでは、ポリシーと呼びます。

配布ソフトウェア

SigmaSystemCenterでは、マシン稼動や置換などの構成変更の際に使用する設定を配布ソフトウェアと呼びます。以下の3種類があります。

・ シナリオ

・ テンプレート

・ ローカルスクリプト

パワーサイクル

いったん、マシンの電源をオフにした後、再度、オンにする操作です。

物理マシン

実体を持つハードウェアマシンの総称です。

物理マシンは、一般マシン、および仮想マシンサーバを含みます。

プライマリ NIC

SystemProvisioning管理対象マシンの管理に使用するネットワークに接続するNICです。WakeOnLANにより起動する設定を行ったNICです。

ポリシー

"マシンで障害が発生した場合、どのような処理を自動実行するのか" といった障害時の復旧処理設定を指します。SystemProvisioningでは、ESMPRO/ServerManager、vCenter Serverなどの仮想マシン基盤、Out-of-Band Management管理機能、およびSystemMonitor性能監視が検出したマシンの障害に対し、復旧処理を設定できます。

ま

マシン

SigmaSystemCenterで管理できる物理マシン / 仮想マシンの総称です。

マスタマシン

作成元とするマシン1台を構築し、そのマシンのイメージを他のマシンにクローニング (複製) することにより、複数のマシンを同じ構成で作成することができます。この作成元となるマシンをマスタマシンと呼びます。

マスタ VM

仮想マシンを作成するためのテンプレートの作成元とする仮想マシンです。

メンテナンスモード

マシンのメンテナンス作業中など、障害通報を無視したいときに使用するモードです。メンテナンスモードに設定したマシンで障害が発生しても、ポリシーによる復旧処理は行いません。

ら

ローカルスクリプト機能

.bat形式の実行可能ファイル (ローカルスクリプトと呼びます。) をSigmaSystemCenter管理サーバ上で実行する機能です。管理対象マシンの追加や用途変更、置換などを行う際に、システム構成や環境に依存した特定の処理を管理サーバ上で行いたい場合に使用します。

論理マシン

SigmaSystemCenterは、ハードウェアの機能によってMACアドレスやWWN、UUIDなどを仮想化したマシンを論理マシンとして扱います。論理マシンは、もともと装置に設定されたIDを持つ物理マシンと関連付けて管理します。

付録 D　　改版履歴

版数	年月	改版内容
第1版	2016.09	・新規作成

付録 E　　ライセンス情報

本製品には、一部、オープンソースソフトウェアが含まれています。当該ソフトウェアのライセンス条件の詳細につきましては、以下に同梱されているファイルを参照してください。また、GPL / LGPLに基づきソースコードを開示しています。当該オープンソースソフトウェアの複製、改変、頒布を希望される方は、お問い合わせください。

<SigmaSystemCenterインストールDVD>¥doc¥OSS

▪ PXE Software Copyright (C) 1997 - 2000 Intel Corporation.

▪本製品には、Microsoft Corporationが無償で配布しているMicrosoft SQL Server Expressを含んでいます。使用許諾に同意したうえで利用してください。著作権、所有権の詳細につきましては、以下のLICENSEファイルを参照してください。
<Microsoft SQL Server Expressをインストールしたフォルダ>¥License Terms

▪ Some icons used in this program are based on Silk Icons released by Mark James under a Creative Commons Attribution 2.5 License. Visit http://www.famfamfam.com/lab/icons/silk/ for more details.

▪ This product includes software developed by Routrek Networks, Inc.

▪ This product includes NM Library from NetApp, Inc. Copyright 2005 - 2010 NetApp, Inc. All rights reserved.