NEC

SigmaSystemCenter 3.7
UPS 連携機能 構築ガイド

SSC0307-doc-0010

利用条件・免責事項

本書の利用条件や免責事項などについては、次のページを参照してください。

http://jpn.nec.com/site/termsofuse.html

目次

はじめに

この文書では、「VMware vSphere」と管理ツールの「WebSAM SigmaSystemCenter 3.7」及び「ESMPRO/AutomaticRunningController」の UPS 監視機能を利用して、停電障害時に影響を受けるマシンを自動的に一括して停止やメンテナンスモード設定を行う機能(UPS 連携機能)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 3.7 UPS 連携機能 構築ガイド」は、SigmaSystemCenter により UPS 連携機能を実現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、SigmaSystemCenter の他のドキュメントをお読みください。

  また、UPS の管理製品である「ESMPRO/AutomaticRunningController」のインストール及び設定が完了していることを前提に説明しています。

1. お使いになる前に

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、「ESMPRO/AutomaticRunningController」の UPS 監視機能と連携して、停電障害時に影響を受けるマシンを自動的に一括して停止やメンテナンスモード設定を行う機能の実現を目標としています。

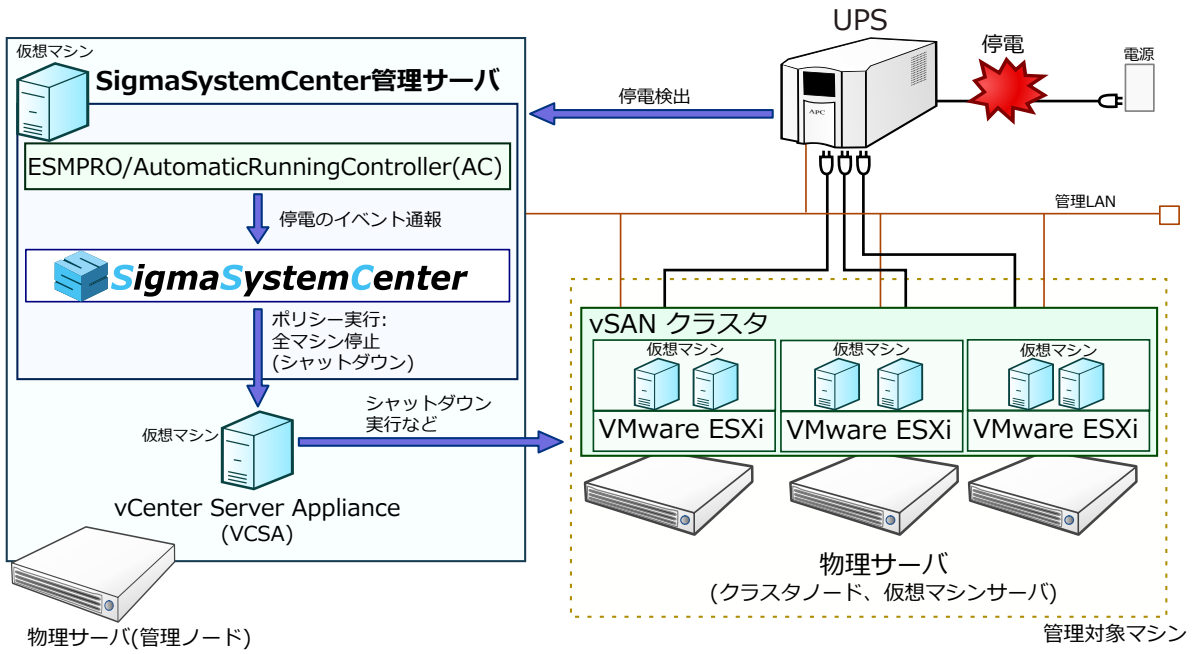
本連携機能の使用条件は次の通りです。

- ESMPRO/AutomaticRunningController: Ver5.31 以上
  - オプションパッケージ製品の ESMPRO/AC Enterprise も必要です。
- 対象 UPS: ESMPRO/AutomaticRunningController の対応 UPS
- その他： N+1 リカバリ機能を使用する環境では利用できません。

  ※ESMPRO/AutomaticRunningController は N+1 リカバリ機能に対応していないため、N+1 リカバリ機能を利用する場合は本連携機能を利用できません。

注

本連携は VMware 環境でのみ利用可能です。他の環境の場合は、ESMPRO/AutomaticRunningController 側の本連携用の設定を有効にしないでください。ESMPRO/AutomaticRunningController が正常に動作しない可能性があります。



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。

- 2.インストール前の準備
  - 2.1. 管理サーバの準備
  - 2.2. 管理対象（物理サーバと仮想マシン）の準備
- 3.SSC のインストール
- 4.SSC の初期設定
  - 4.1. ユーザの作成
  - 4.2. ライセンスの登録
  - 4.3. 通報に必要な環境設定
- 5.管理対象マシンの登録
  - 5.1.仮想化基盤(vCenter Server / ESXi)の登録
  - 5.2.BMC の登録
- 6.UPS の登録
  - 6.1.UPS オブジェクトの作成
  - 6.2.UPS とマシンの関連設定
  - 6.3.UPS 用ポリシーの UPS への割り当て
- 7.動作テスト

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
  - 物理サーバ（3 台）
    - VMware ESXi(Virtual SAN)
    - ホスト名：IP アドレス(管理用ネットワーク)
      - 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(管理用ネットワーク)
      - 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 2016 Standard
        * ホスト名：IP アドレス(VM 管理用ネットワーク)
            + 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
        * ※サービス用ネットワークについては説明を省略します。業務の必要に応じて設定してください。
- 管理サーバ（1 台）
    - Windows Server 2016 Standard
    - SigmaSystemCenter
    - ESMPRO/ServerManager
    - ESMPRO/AutomaticRunningController
    - ホスト名：IP アドレス
        * SSCmanager：172.16.0.1 (管理用ネットワーク)
- vCenter Server Appliance：172.16.0.2

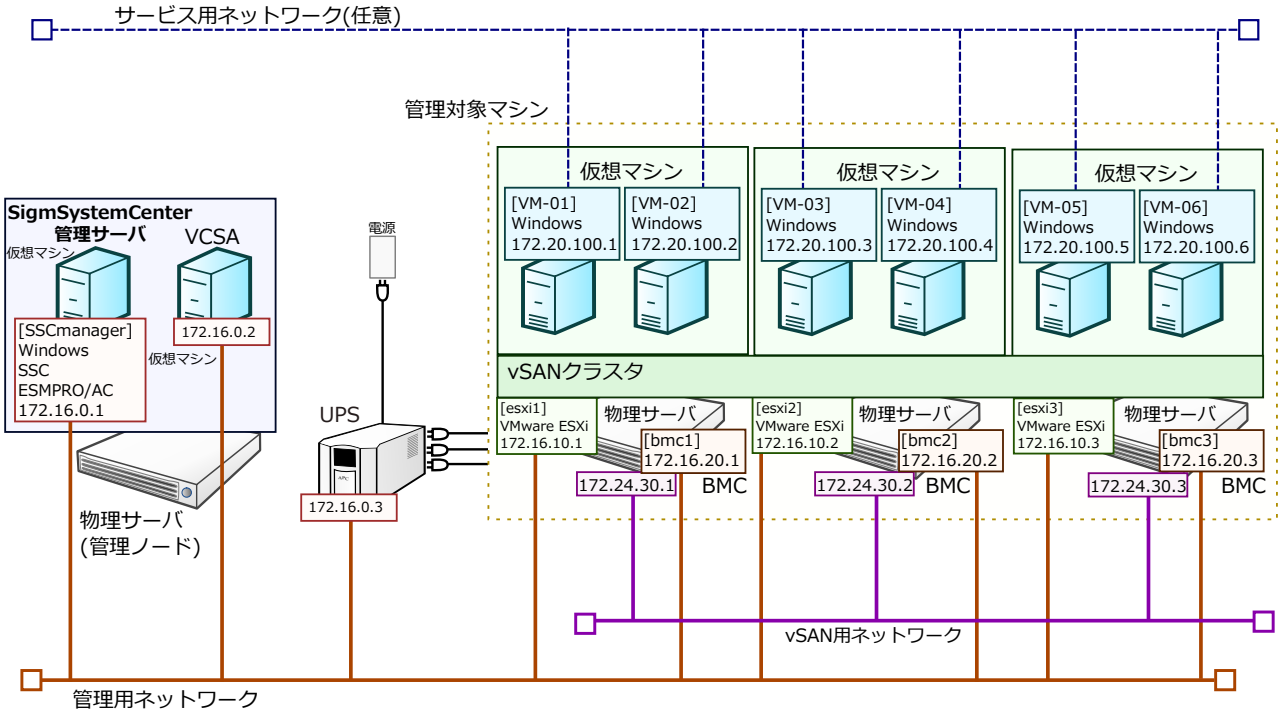


図　今回構築するシステムの構成

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。

- Windows Server
- vCenter Server

管理サーバの Windows Server については、本書では、Windows Server 2016 を使用した場合の例を中心に説明を行います。

SigmaSystemCenter を動作させるために、以下の Windows のコンポーネント・機能が必要です。

- .NET Framework 4.6.2 (※)
- Web サーバー (IIS)

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ください。

≪管理サーバが Windows Server 2012、Winsows Server 2012 R2、Winsows Server 2016 の場合≫

- 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
    - Windows Server 2012、Winsows Server 2012 R2 の場合は、ASP.NET 4.5 を選択
    - Windows Server 2016 の場合は、ASP.NET 4.6 を選択
  - IIS 管理コンソール
  - IIS 6 メタベース互換

Windows Server 2012、Winsows Server 2012 R2 の場合、既定の.NET Framework のバージョンは 4.5 ですが、.NET Framework 4.6.2 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。

Windows Server 2016 は、.NET Framework 4.6.2 は、既定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。

(※).NET Framework 4.7 も利用可能です。必要に応じて、.NET Framework 4.6.2 からアップデートして利用してください。

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。

3. SSC のインストール

SSC のインストールについて説明します。

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]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。

なお、ESMPRO/ServerManager は管理サーバに添付のものをあらかじめインストールしておくことでも利用できますが、SSC に添付の ESMPRO/ServerManager のバージョン(6.20)以上の ESMPRO/ServerManager をインストールしてください。

※物理サーバの機種が Express5800/D120h の場合は ESMPRO/ServerManager のバージョンは 6.22 以上が必要です。ESMPRO の下記製品サイトより、ESMPRO/ServerManager の最新のインストールモジュールを入手してインストールしてください。

http://jpn.nec.com/esmsm/index.html

[ダウンロード]→[インストールモジュール]の一覧表より、「ESMPRO/ServerManager Ver.6」の項目から入手することができます。

4. SSC の初期設定

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://172.16.0.1:80/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]をクリックしてログインします。

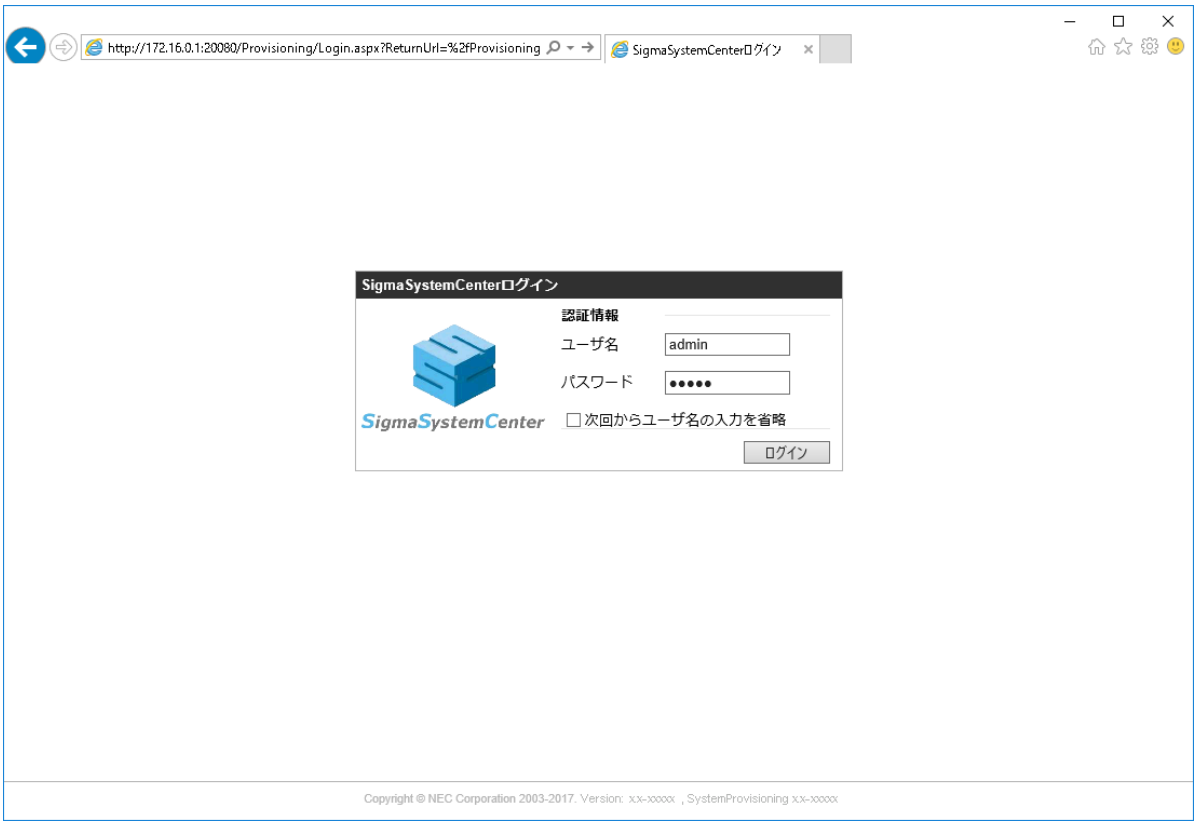


図 「SigmaSystemCenter ログイン」画面

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。

画面の右上にある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。

画面左側のツリービューにある[ユーザ]をクリックし、「ユーザ一覧」、「ロール一覧」の画面を表示されたら「ユーザ一覧」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]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 「ユーザ追加」画面

[OK]を押すと「ユーザ一覧」、「ロール一覧」の画面に遷移し、「ユーザ一覧」に[sysadmin]が追加されていることが確認できます。

注

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一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 「ユーザ一覧」、「ロール一覧」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。画面右上の[管理]をクリックし、[管理]ビューに移動します。画面左側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]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]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　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[スタート]メニューから[Windows 管理ツール]→[サービス」で[PVMService]を再起動してください。

4.3　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（画面右上の[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。

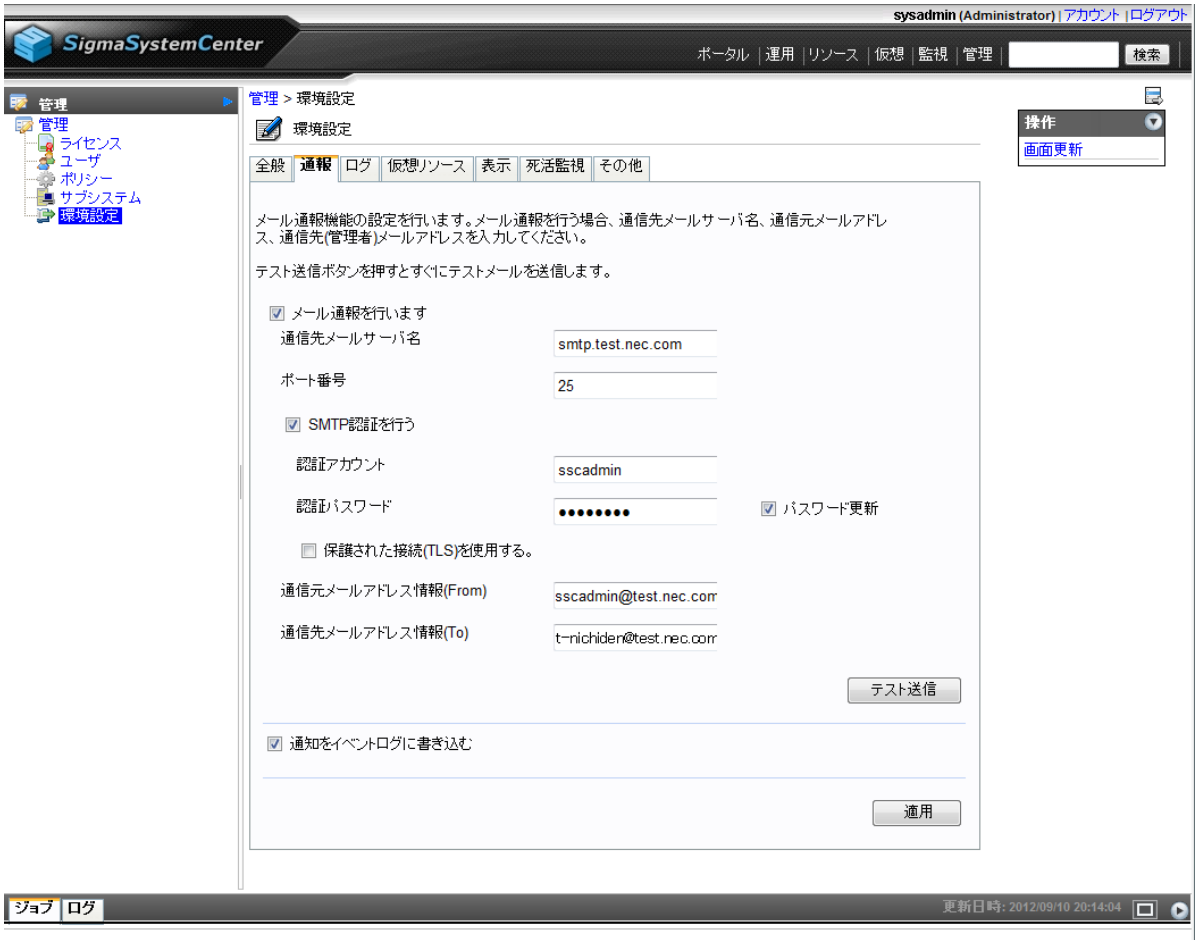


図 「環境設定」画面（[通報]タブ）

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 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	―
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	-
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	―

設定項目	説明	入力例
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]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]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. 管理対象マシンの登録

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 仮想化基盤(vCenter Server / ESXi)の登録

SSC の[管理]ビューを開き（画面右上の[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
- **[マシンを運用グループへ自動登録する]のチェックをオン**

上記の項目を入力したら[OK]をクリックしてください。

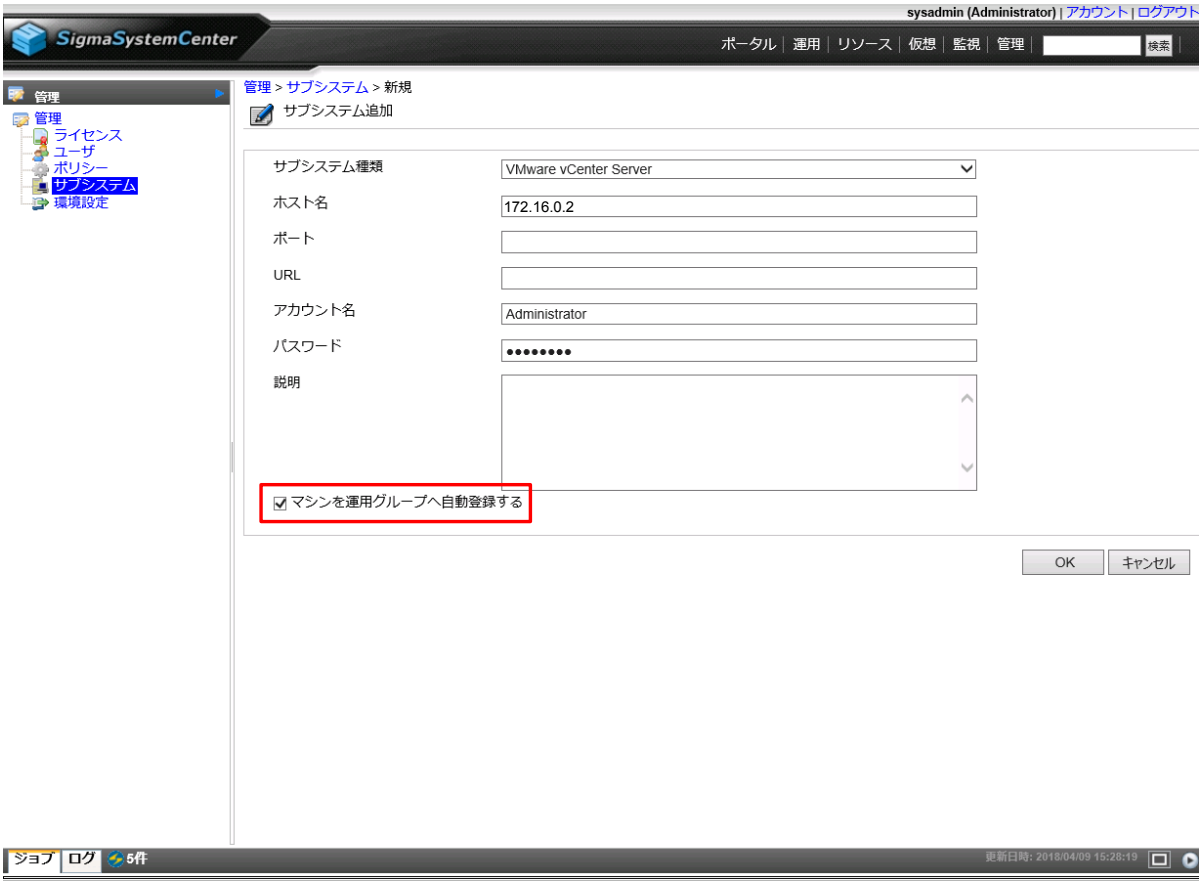


図　vCenter Server の登録

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）。

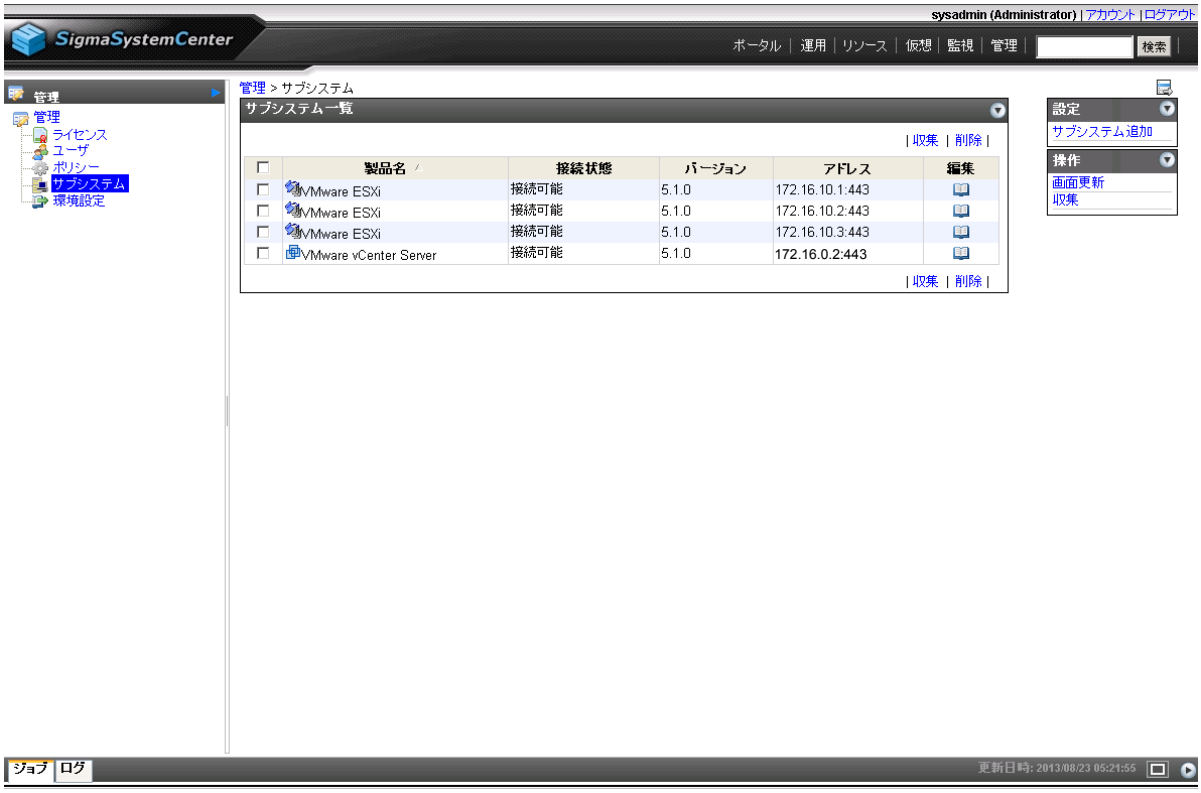


図　サブシステム一覧

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。「環境設定」の「仮想リソース」で、VMware ESXi 仮想マシンサーバの root パスワードの既定値を設定します。

なお、個別にパスワードを設定したい場合(ESXi のパスワードがそれぞれ違う場合など)、

に関しては、「付録 B. VMware ESXi サーバの個別パスワード設定（37 ページ）」を参照してください

画面右上の[リソース]をクリックして[リソース]ビューを開いた後、ツリービューの[マシン]をクリックして「マシン一覧」画面に移動して、登録内容を確認してみましょう。

vCenter Server に登録されている物理サーバ[172.16.10.1](esxi1)、[172.16.10.2](esxi2)、[172.16.10.3](esxi3)、業務用仮想マシン[VM-01]、[VM-02]、[VM-03]、[VM-04]、[VM-05]、[VM-06]が次のように登録されています。

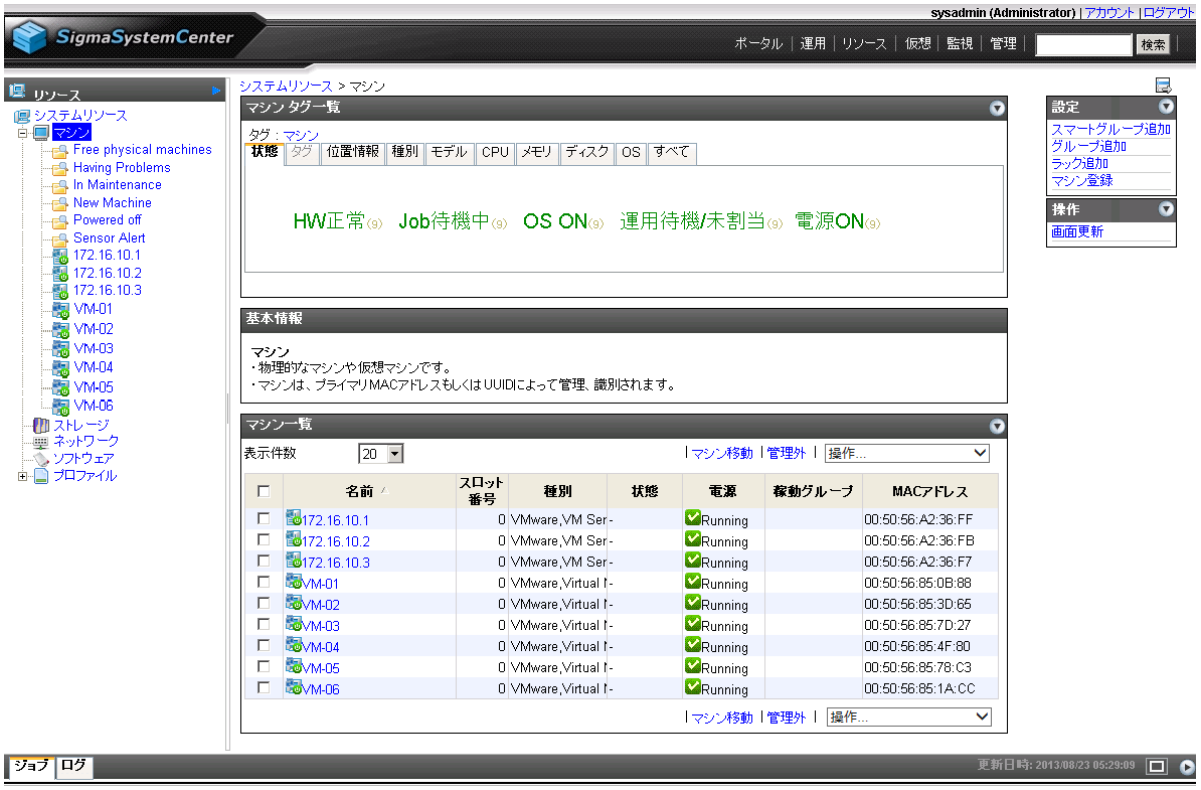


図　マシン登録後の[マシン一覧]

なお、サブシステムの登録の後に vCenter Server への物理サーバの登録や業務用仮想マシンの作成を行った場合は SSC に自動的に登録されませんので、注意してください。

この場合は、次のように、収集の操作で SSC に登録を行う作業が必要です。

画面右上の[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[システムリソース]をクリックして「システムリソース」画面に移動します。

次に[操作]メニュー下の[収集]をクリックします。

収集の処理が完了した後、前述と同様に「マシン一覧」画面に移動して、登録内容を確認してください。

図　収集の操作

以上でマシン登録の確認は終了です。

5.2　BMC の登録

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[172.16.10.2](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、物理サーバの BMC(EXPRESSSCOPE エンジンや iLO など)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 BMC の設定
2. SSC 上で、管理対象の OOB アカウント設定

1.に関しては機種別に設定方法が異なります。「付録 A.　物理サーバの BMC の設定（26 ページ）」を参照してください。

以下より、 2. SSC 上で、管理対象の OOB アカウント設定に関して記載します。

SSC では、物理サーバの BMC(EXPRESSSCOPE エンジンや iLO など)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。

まず画面右上の[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]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　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： 物理サーバの BMC(※)のユーザ名を入力（今回は、ssc）
- パスワード：物理サーバの BMC(※)のパスワードを入力（今回は、sscadmin）
- 接続先：物理サーバの BMC(※)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

※BMC の設定については、機種に応じて、「A.1 EXPRESSSCOPE エンジン（BMC）の設定（26 ページ）」/「A.2 iLO（BMC）の設定（27 ページ）」/「A.3 Express5800/D120h などの BMC/CMC の設定（31 ページ）」を参照してください。

図　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]を押します。

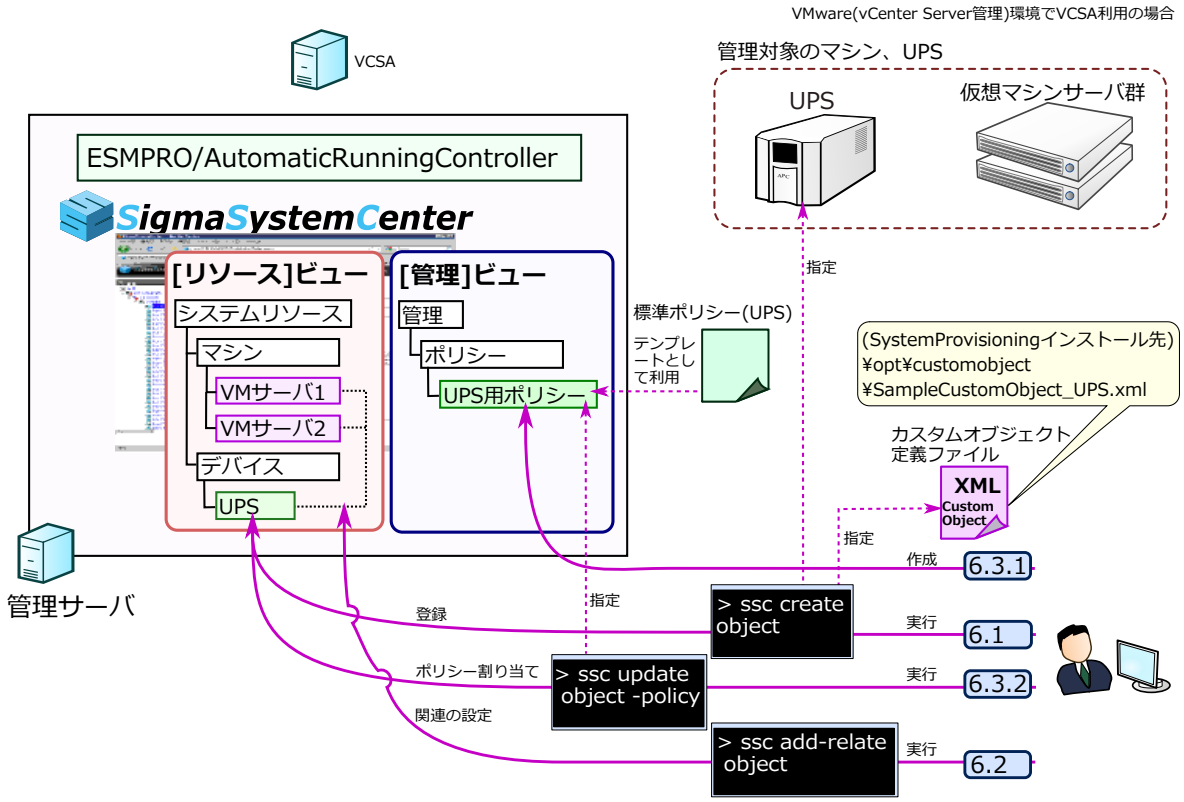
OOB アカウント追加後の[アカウント情報]タブです。[アカウント一覧]の枠に[OOB]が追加され、[接続状態]が[接続可能]となっていれば SSC が管理対象の物理サーバの BMC にログインできたことを示しています。

図　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. UPS の登録

SigmaSystemCenter 上で、UPS の登録を以下の手順で実施します。



6.1 UPS オブジェクトの作成

ssc create object コマンドで UPS オブジェクトを作成します。

UPS01 という名前で IP アドレスが[172.16.0.3]の場合、以下のコマンドを実施してください。

```
ssc create object "C:¥Program Files (x86)¥NEC¥PVM¥opt¥customobject¥SampleCus
tomObject_UPS.xml" -name UPS01 -id 172.16.0.3
```

コマンド実施後、リソース/デバイスビューにて、作成した UPS が表示されることを確認してください。

なお、ssc delete object コマンドで UPS オブジェクトの削除ができます。

6.2 UPS とマシンの関連設定

ssc add-relate object コマンドで UPS に接続しているマシンとの関連付けを実施します。

カスタムオブジェクト名が UPS01 という名前でマシン名が[172.16.10.1], [172.16.10.2], [172.16.10.3]の場合、以下 3 つのコマンドをマシンごとに実施してください。

```
ssc add-relate object UPS01 -dest 172.16.10.1 machine -dir forward
ssc add-relate object UPS01 -dest 172.16.10.2 machine -dir forward
ssc add-relate object UPS01 -dest 172.16.10.3 machine -dir forward
```

注

-dir オプションにより、影響範囲の方向を設定します。-dir オプションを付与し忘れないように注意してください。

コマンド実施後、リソース/デバイス/UPS にて、マシンの関連が設定されていることを確認してください。

なお、ssc delete-relate object コマンドで関連設定の削除ができます。

6.3 UPS 用ポリシーの UPS への割り当て

6.3.1 UPS 用ポリシーの作成

UPS 用のポリシーを作成します。

「管理」/「ポリシー」ビューにてポリシーの追加を押します。

テンプレートより「標準ポリシー(UPS)」を選択し、名前に"UPSPolicy"と入力して「OK」ボタンを押します。

6.3.2 UPS 用ポリシーの割り当て

ssc update object コマンドを用いて、作成した UPS ポリシーを UPS に割り当てます。

UPS オブジェクト名が UPS01 及びポリシー名が「UPSPolicy」の場合、以下のコマンドを実施してください。

```
ssc update object UPS01 -policy UPSPolicy
```

以上で 6.UPS の登録は完了です。

7. 動作テスト

UPS 停電時にポリシーが起動して、サーバ及び仮想マシンが安全にシャットダウンされるか動作テストをします。

今回は UPS の IP アドレスが 172.16.0.3 ですので、

C:¥Program Files¥AUTORC 配下にある ac_pvm.exe を用いて、以下のコマンドを実施してください。

(80000583 は UPS の停電時のイベント番号です。)

```
ac_pvm.exe -e 172.16.0.3 80000583 "UPS 停電イベントテスト送信"
```

上記コマンドにより、UPS 停電時のイベントが送信され、ポリシーを介して、UPS に接続しているサーバ及び仮想マシンのシャットダウンが実行されます。

リソースビューより、UPS に接続されているサーバ及び仮想マシンがシャットダウンされていることを確認してください。

注

ac_pvm.exe を利用するためには事前設定が必要です。

設定詳細は ESMPRO/AC Enterprise セットアップカード「3.3 WebSAM SigmaSystemCenter 連携機能の設定」を

参照してください。

付録 A.　物理サーバの BMC の設定

A.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 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 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　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]→[通報]→[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。

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　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。

A.2　iLO（BMC）の設定

◇**管理 LAN の設定**

まず、[172.16.10.1](esxi1)となるサーバの iLO（BMC）の管理 LAN の設定を行います。手順については、「iLO 5 ユーザーズガイド」の「2. iLO セットアップ」を参照して、管理 LAN を設定してください。

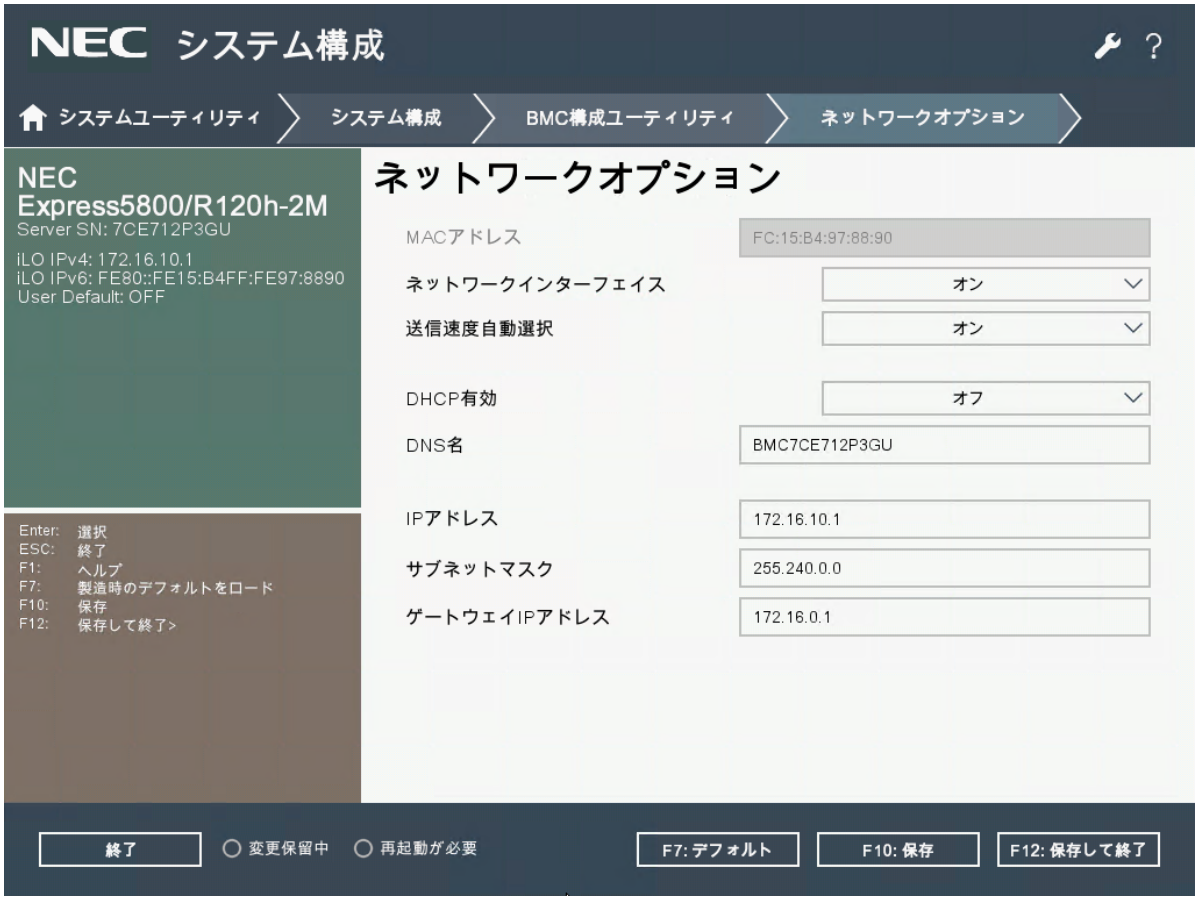


図　iLO 5 の管理 LAN の設定

◇ローカルユーザアカウントの作成

次に、[172.16.10.1](esxi1)となるサーバの iLO（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、「iLO 5 ユーザーズガイド」の「2. iLO セットアップ」を参照して、ローカルユーザ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。


NEC システム構成
More Forms
BMC構成ユーティリティ
ユーザー管理
ユーザーの追加
NEC Express5800/R120h-2M
Server SN: 7CE712P3GU
iLO IPv4: 172.16.10.1
iLO IPv6: FE80::FE15:B4FF:FE97:8890
User Default: OFF
ユーザーの追加
新しいユーザーのBMCの権限:
ユーザーアカウント管理 はい
リモートコンソールアクセス はい
仮想電源およびリセット はい
仮想メディア はい
設定の構成 はい
ホストBIOS はい
ホストNIC はい
ホストストレージ はい
新しいユーザー情報:
新しいユーザー名 ssc
ログイン名 ssc
Enter: 選択
ESC: 終了
F1: ヘルプ
F7: 製造時のデフォルトをロード
F10: 保存
F12: 保存して終了>
終了
変更保留中
再起動が必要
F7: デフォルト
F10: 保存
F12: 保存して終了


NEC システム構成
More Forms
BMC構成ユーティリティ
ユーザー管理
ユーザーの追加
NEC Express5800/R120h-2M
Server SN: 7CE712P3GU
iLO IPv4: 172.16.10.1
iLO IPv6: FE80::FE15:B4FF:FE97:8890
User Default: OFF
新しいユーザーのBMCの権限:
ユーザーアカウント管理 はい
リモートコンソールアクセス はい
新しいパスワードを入力します。
****
新しいユーザー情報:
新しいユーザー名 ssc
ログイン名 ssc
パスワード
入力するにはEnterキーを押してください
Enter: 選択
ESC: 終了
F1: ヘルプ
F7: 製造時のデフォルトをロード
F10: 保存
F12: 保存して終了>
終了
変更保留中
再起動が必要
F7: デフォルト
F10: 保存
F12: 保存して終了

図　iLO 5 のローカルユーザアカウントの作成

◇IPMI 通信の有効化

次に、[172.16.10.1](esxi1)となるサーバの iLO（BMC）で IPMI 通信を有効にします。手順については、「iLO 5 ユーザーズガイド」の「14. iLO のセキュリティ機能の使用」を参照して、IPMI/DCMI アクセスオプションを[有効]に設定し、[適用]をクリックします。

図　iLO 5 の IPMI 通信の有効化

◇SNMP の設定

続いて、iLO（BMC）で、管理サーバである SSCmanager(172.16.0.1)へ SNMP アラートを行うための設定をします。手順については、「iLO 5 ユーザーズガイド」の「15. iLO マネージメント設定の構成」を参照して、SNMP の設定をします。

1. 以下の設定を行います。

項目名	設定値
読み取りコミュニティ	public
トラップコミュニティ	public
SNMP アラートの送信先	172.16.0.1

2. [適用]をクリックします。

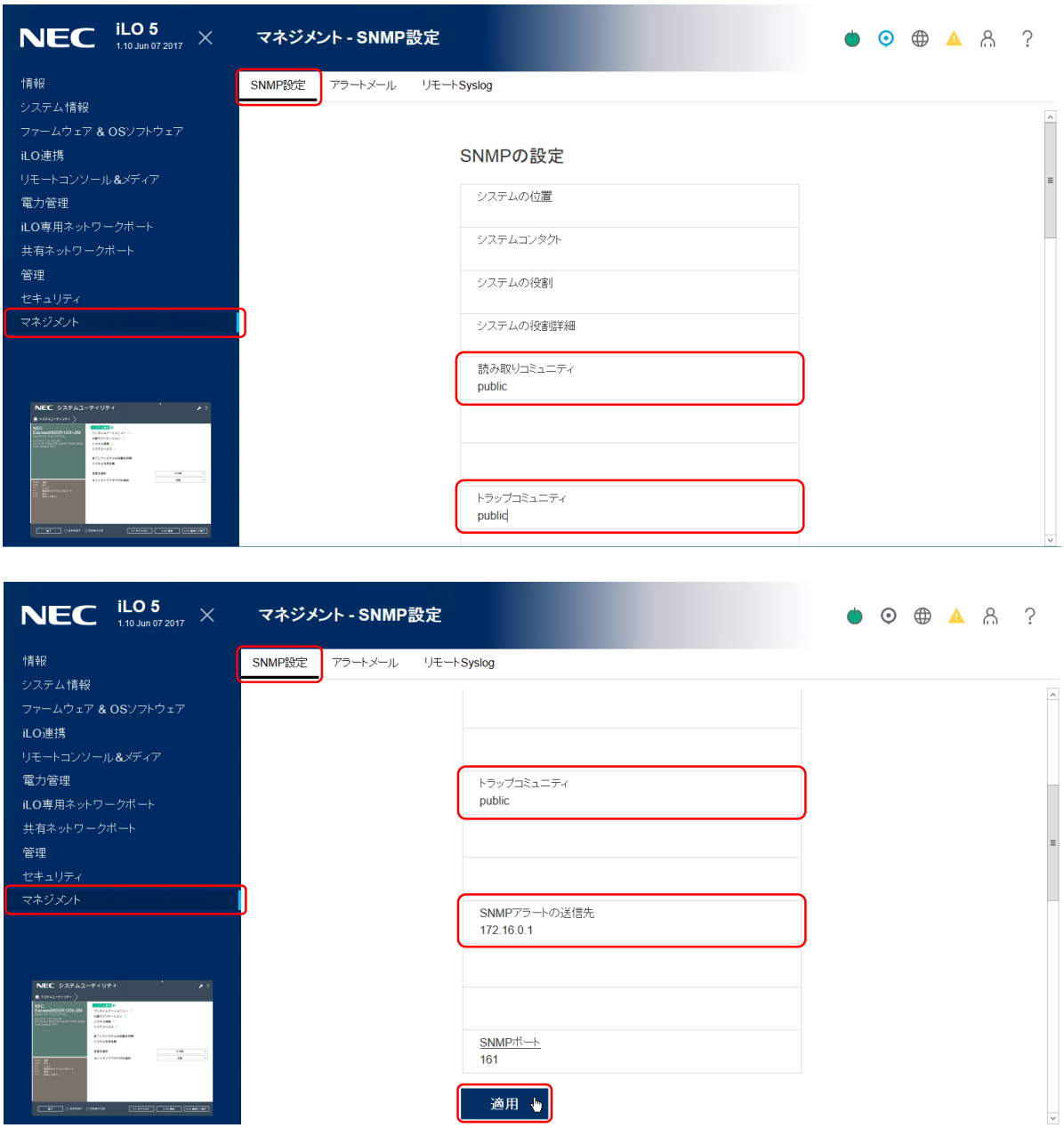


図　iLO 5 の SNMP の設定

[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。

A.3　Express5800/D120h などの BMC/CMC の設定

◇**管理 LAN の設定**

まず、[172.16.10.1](esxi1)となるサーバの BMC の管理 LAN の設定を行います。手順については、「BMC/CMC 管理コンソール ユーザーズガイド」の「2. サーバ側の設定」を参照して、マネージメント LAN 設定を行ってください。

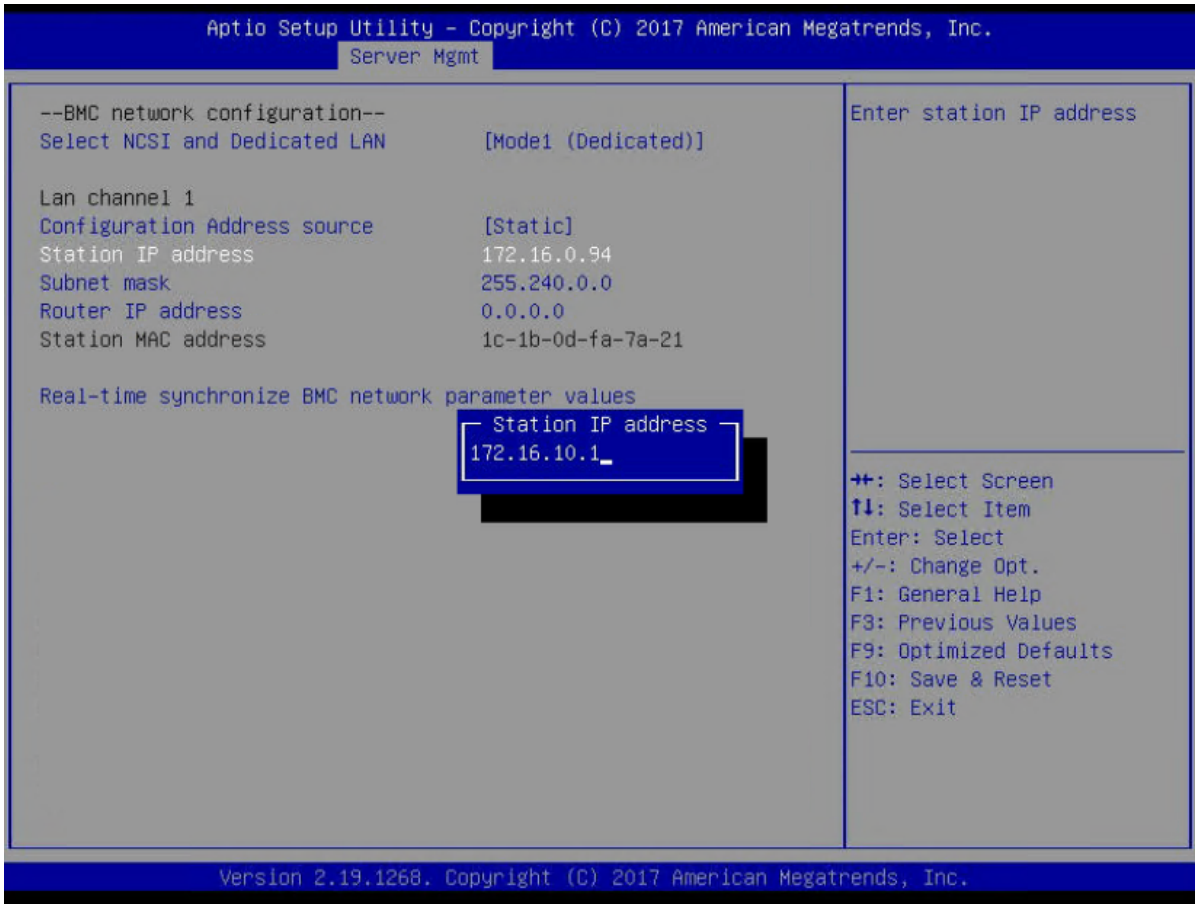


図　マネージメント LAN 設定

◇管理者権限のあるユーザーの作成

次に、[172.16.10.1](esxi1)となるサーバの BMC のリモートマネジメントで管理者権限のあるユーザーを作成します。手順については、「BMC/CMC 管理コンソール ユーザーズガイド」の「5. リモートマネジメントの使い方」を参照して、ユーザー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。

1. 左ペインのメニューから[EMS]→[設定]→[ユーザー]をクリックします。
2. メインペインのユーザーリストで任意の[ユーザー ID]をクリックします。

図　ユーザーの選択

3. メインペインの一般セクションで以下の設定を行います。

項目名	設定値
ユーザーを有効にする	チェック
ユーザー名	ssc
パスワードを変更する	チェック
新しいパスワード	sscadmin
パスワードの確認	sscadmin

4. メインペインのユーザー権限セクションで以下の設定を行います。

項目名	設定値
ユーザーロール	アドミニストレータ
IPMI LAN 権限	アドミニストレータ
IPMI Serial 権限	アドミニストレータ
Serial Over LAN を有効にする	チェック

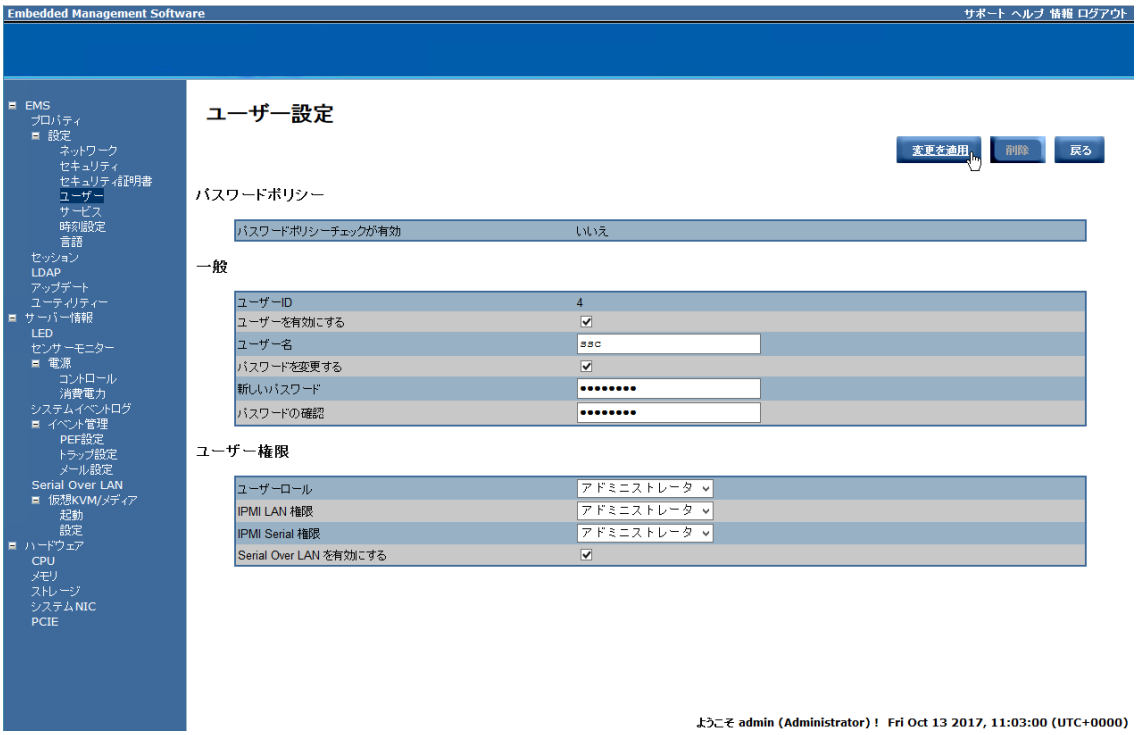


図　ユーザーの追加

◇<u>トラップ設定</u>

続いて、BMC のリモートマネジメントで、管理サーバである SSCmanager(172.16.0.1)へ SNMP アラートを行うための設定をします。手順については、「BMC/CMC 管理コンソール ユーザーズガイド」の「5. リモートマネジメントの使い方」を参照します。今回は、IP 通報先リストの IP 通報先 1 を使うことにします。

1. 左ペインのメニューから[サーバー情報]→[イベント管理]→[トラップ設定]をクリックします。
2. メインペインの IP 通報先リストセクションで以下の設定を行います。

項目名	設定値
有効	チェック
IPv4/IPv6	該当する IP を選択
IP アドレス	172.16.0.1

3. メインペインのコミュニティ名セクションで以下の設定を行います。

項目名	設定値
コミュニティ名	public

4. メインペイン右上の[変更を適用]をクリックします。

図　トラップ設定

◇PEF 設定

続いて、BMC のリモートマネジメントで、プラットフォームイベントフィルタの設定をします。手順については、「BMC/CMC 管理コンソール ユーザーズガイド」の「5. リモートマネジメントの使い方」を参照します。ハードウェアに関連するすべてのイベントが届くように、全てのフィルタで[PET の生成]にチェックを入れます。

1. 左ペインのメニューから[サーバー情報]→[イベント管理]→[PEF 設定]をクリックします。
2. メインペインのプラットフォームイベントフィルタ (PEF) アクショングローバル制御リストで以下の設定を行います。

項目名	設定値
アクション名	[PET の生成]をチェック

3. メインペインのプラットフォームイベントフィルタ (PEF) リストセクションで以下の設定を行います。

項目名	設定値
通報有効	チェック
フィルタ名	全てのフィルタについて、[PET の生成]をチェック

4. メインペイン右上の[変更を適用]をクリックします。

図　PEF 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。

付録 B.　VMware ESXi サーバの個別パスワード設定

[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]をクリックします。

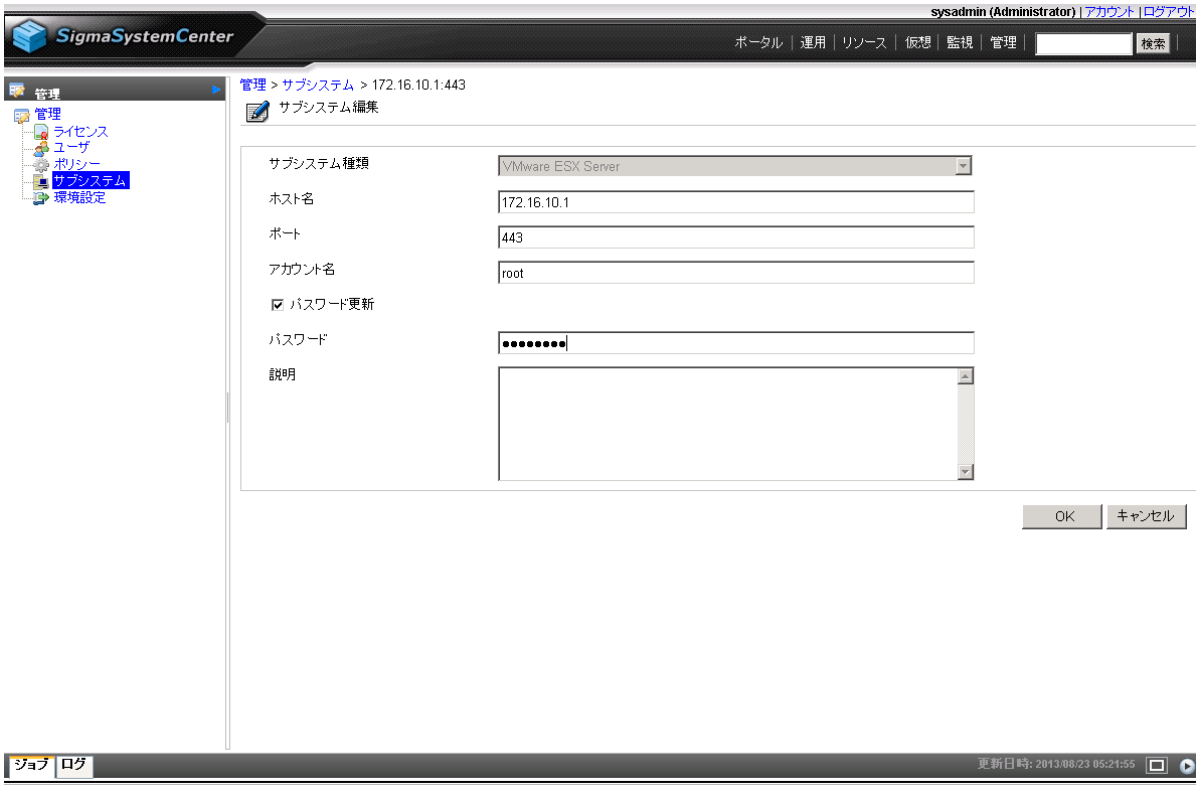


図　ESXi の追加設定

なお、サブシステムにおいてパスワードを設定していない場合には、環境設定のパスワードが使用されます。

SigmaSystemCenter 3.7
UPS 連携機能 構築ガイド

SSC0307-doc-0010

2018 年 5 月 1 版 発行