SSC 連携設定マニュアル

(PowerChute Network Shutdown)

2026.04.17

第 1 版

改版履歴

版数	改版日付	内 容
1	2026/04/17	新規作成

免責事項

本書の内容は、予告なしに変更されることがあります。
日本電気株式会社は、本書の技術的もしくは編集上の間違い、欠落について、一切責任をおいません。
また、お客様が期待される効果を得るために、本書に従った導入、使用および使用効果につきましては、お客様の責任とさせていただきます。

商標情報

ESMPRO、WebSAM は日本電気株式会社の登録商標です。
Microsoft、Windows、Windows Server、Hyper-V は、米国 Microsoft Corporation の米国およびその他の国における登録商標です。
Red Hat は米国およびその他の国で Red Hat, Inc. の登録商標または商標です。
Smart-UPS、PowerChute、APC は、Schneider Electric Industries SAS またはその関連会社の登録商標または商標です。
VMware is a registered trademark or trademark of Broadcom in the United States and other countries. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.
本書に記載されたその他の製品名および標語は、各社の商標または登録商標です。
その他のシステム名、社名、製品名等はそれぞれの会社の商標または登録商標です。

目次

第 1 章　SSC 連携設定機能とは 6
1.1. 機能概要 6
1.2. PCNS、SSC 連携動作の概略 7
1.3. SSC 連携設定用ファイルのダウンロード 8

第 2 章　SSC 管理サーバの連携設定手順 9
2.1. SSC 連携用のコマンド実行環境の準備 9
2.2. SSH 実行環境の設定 11

第 3 章　PCNS で電源管理を行うサーバの連携設定手順 15
3.1. Windows 環境の連携設定 15
3.2. Linux 環境の連携設定 27
3.3. VMware ESX/ESXi 環境(デプロイした PCNS 環境より制御)の連携設定 32
3.4. VMware ESX/ESXi 環境(SSC 管理サーバ上の PCNS(Windows)環境より制御)の連携設定 35

はじめに

対象読者

PowerChute Network Shutdown(以降 PCNS)および WebSAM SigmaSystemCenter(以降 SSC)を使用したサーバの電源管理を行うシステムエンジニアと、システム導入後の保守・運用を行うシステム管理者が対象読者となります。「SSC 導入した管理サーバ」より「PCNS を導入したサーバ」を連携して管理するための設定手順を説明していきます。

対象システム

・PCNS(v5.2 以降)を導入したサーバ
・SSC を導入した管理サーバ

本書の構成

第1章 「SSC 連携対応機能とは」
SSC 連携設定機能の動作の概要を説明します。

第2章 「SSC 管理サーバの連携設定手順」
SSC 管理サーバで SSC 連携対応スクリプトを動作させるための設定手順を説明します。

第3章 「PCNS で電源管理を行うサーバの連携設定手順」
PCNS で電源管理を行うサーバの SCC 連携対応スクリプトの設定手順を説明します。

最新情報の入手先

最新の製品情報については、以下の Web サイトを参照してください。
https://jpn.nec.com/esmpro_ac/
→PowerChute Network Shutdown

第1章 SSC 連携設定機能とは

1.1. 機能概要

PCNS において「サーバのシャットダウンおよび起動の状態」を SSC の管理サーバに SSH 経由で通知する SSC 連携対応スクリプトを設定することを、SSC 連携設定機能と呼びます。

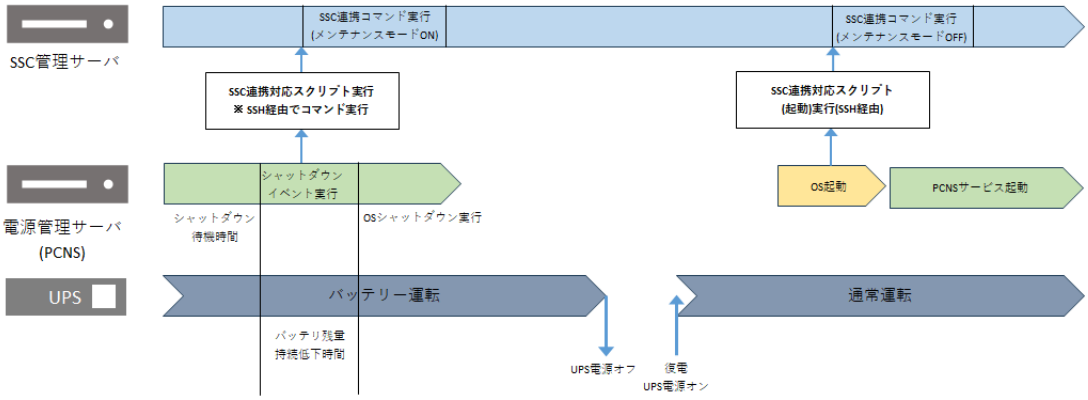
SSC 連携対応スクリプトを設定することで、PCNS と SSC 機能を連携動作させることができます。

1.2. PCNS、SSC連携動作の概略

- 電源管理サーバ内の PCNS の OS シャットダウンイベントに「SSC 連携対応スクリプト」を登録することで、停電発生後、シャットダウン待機時間が経過し PCNS より OS シャットダウンイベントが発生すると、SSC 連携対応スクリプト内より SSH 経由で、SSC 管理サーバ内の SSC 連携コマンド(ac_pvm.exe)を実行することで、電源管理サーバをメンテナンスモードに設定にした後、電源管理サーバをシャットダウンします。

- 電源管理サーバ内の OS 起動サービス内に「SSC 連携対応スクリプト」を登録することで、復電後、OS 起動サービスが動作すると、SSC 連携対応スクリプト内より SSH 経由で、SSC 管理サーバ内の SSC 連携コマンド(ac_pvm.exe)を実行することで、電源管理サーバをメンテナンスモード解除に設定します。

※下図は SSC 連携対応スクリプトの実行時のイメージ図です。



1.3. SSC連携設定用ファイルのダウンロード

（1） SSC 連携設定用ファイル「pcns_ssc_file.zip」を以下よりダウンロードします。
https://jpn.nec.com/esmpro_ac/pcns_download.html
→各種資料
→SSC 連携設定用ファイル

（2） 解凍後のファイルは以降の設定手順で利用します。

ファイル名	概要説明
ac_pvm.exe.config	SSC連携コマンド(ac_pvm.exe)実行用のファイル
ac_pvm.exe.manifest	SSC連携コマンド(ac_pvm.exe)実行用のファイル
ac_pvm_registry.bat	SSC連携コマンド(ac_pvm.exe)のレジストリ設定ファイル
ac_pvm_on.bat	Windows用SSC連携対応スクリプト(シャットダウン用)
ac_pvm_off.bat	Windows用SSC連携対応スクリプト(起動用)
ac_pvm_on_sv.bat	SSC管理サーバにPCNSがインストールされている場合の Windows用SSC連携対応スクリプト(シャットダウン用)
ac_pvm_on_sv.csv	SSC管理サーバにPCNSがインストールされている場合の Windows用SSC連携対応スクリプト(シャットダウン用)
ac_pvm_on.sh	Linux用SSC連携対応スクリプト(シャットダウン用)
ac_pvm_off.sh	Linux用SSC連携対応スクリプト(起動用)

第2章 SSC 管理サーバの連携設定手順

2.1. SSC連携用のコマンド実行環境の準備

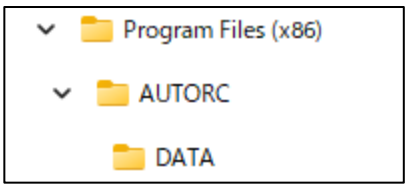
SSC 連携用のコマンド(ac_pvm.exe)の実行環境を SSC 管理サーバ上に準備します。

（１）連携コマンド実行用ディレクリの作成

エクスプローラー等で以下のディレクトリを作成します

・C:¥Program Files (x86)¥AUTORC

・C:¥Program Files (x86)¥AUTORC¥DATA



（２）連携コマンド実行ファイルのコピー

SSC インストール環境より以下のファイルをリネームしてコピーします。

例）SSC が C:¥Program Files (x86)¥NEC 配下にインストールされている場合

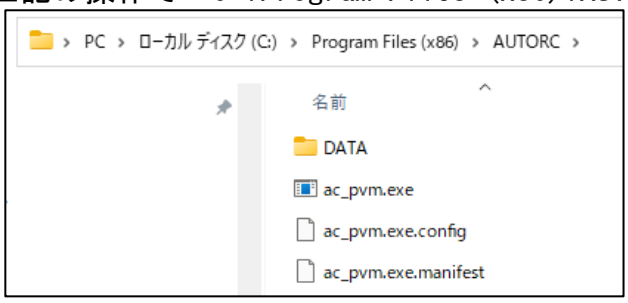
C:¥Program Files (x86)¥NEC¥PVM¥opt¥esmproac¥ac_pvm_u3.exe
↓コピー
C:¥Program Files (x86)¥AUTORC¥ac_pvm.exe

（３）連携コマンド関連ファイルのコピー

SSC 連携設定用ファイル「pcns_ssc_file.zip」を C:¥WORK ディレクトリに解凍した場合を説明します。以下の 2 つの連携コマンド関連ファイルを「C:¥Program Files (x86)¥AUTORC」にコピーしてください。

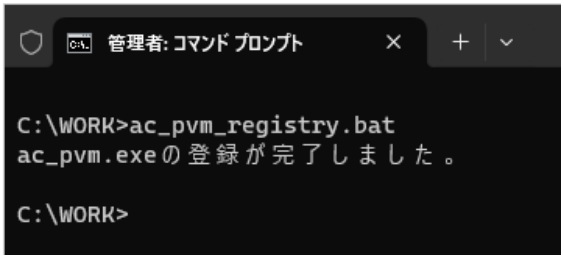
・C:¥WORK¥ac_pvm.exe.config
・C:¥WORK¥ac_pvm.exe.manifest

上記の操作で「C:¥Program Files (x86)¥AUTORC」は以下のようになります



（４）連携コマンド用のレジストリ登録

C:¥WORK ディレクトリ中の「ac_pvm_registry.bat」をコマンドプロンプトより実行し、「ac_pvm.exe の登録が完了しました。」が表示されることを確認してください。



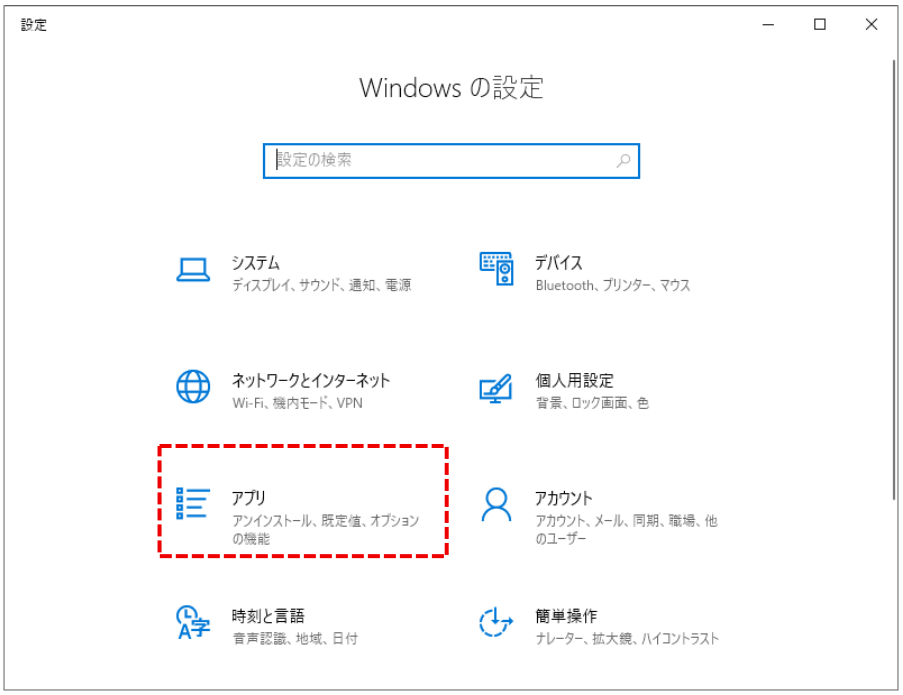
以上で「SSC 連携用のコマンド(ac_pvm.exe)の実行環境」の準備は完了です。

2.2. SSH実行環境の設定

「SSC 連携対応スクリプト」は OpenSSH を利用しています。OpenSSH を利用できるよう設定します。

（１）SSC 管理サーバ(Windows)に「OpenSSH SSH Server」サービスを導入します。

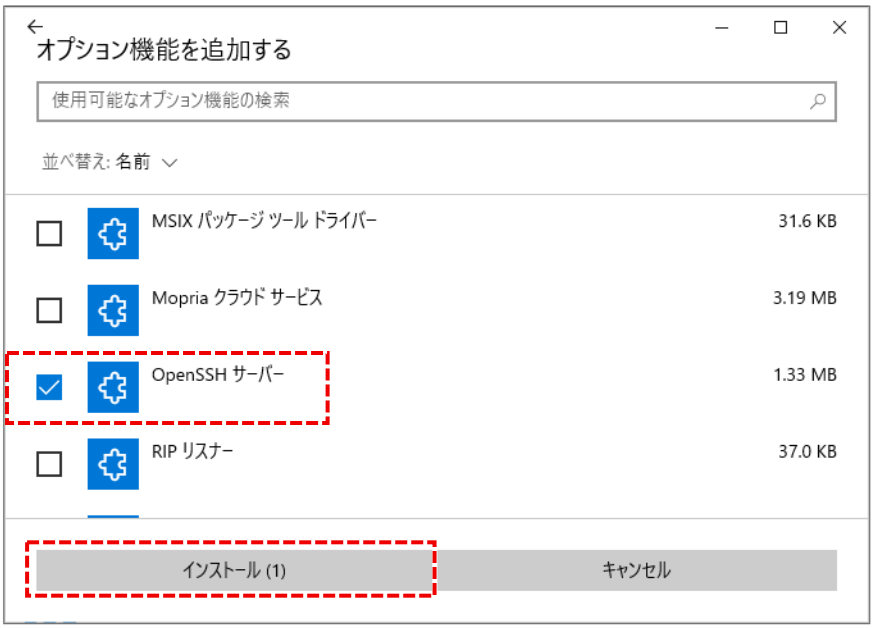
「設定」を開き「アプリ」を選択します。



「オプション機能」を選択

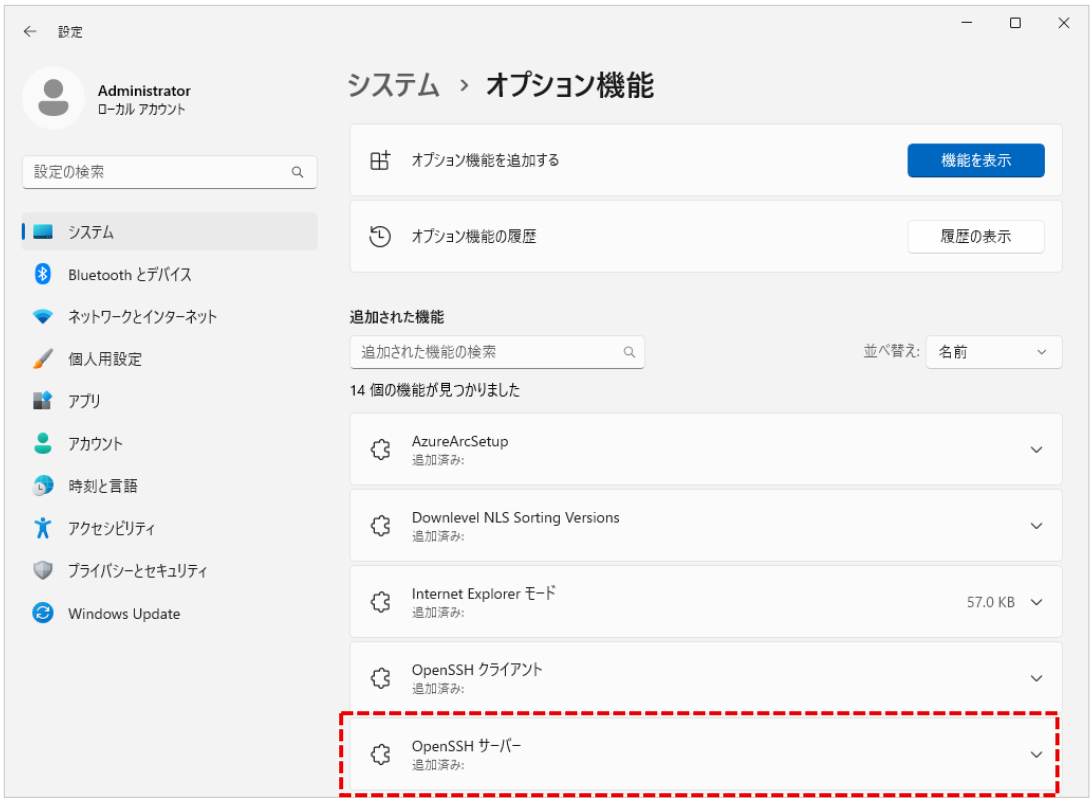
「機能の追加」「＋」を選択する

「Open SSH サーバ」をチェックし「インストール」を選択

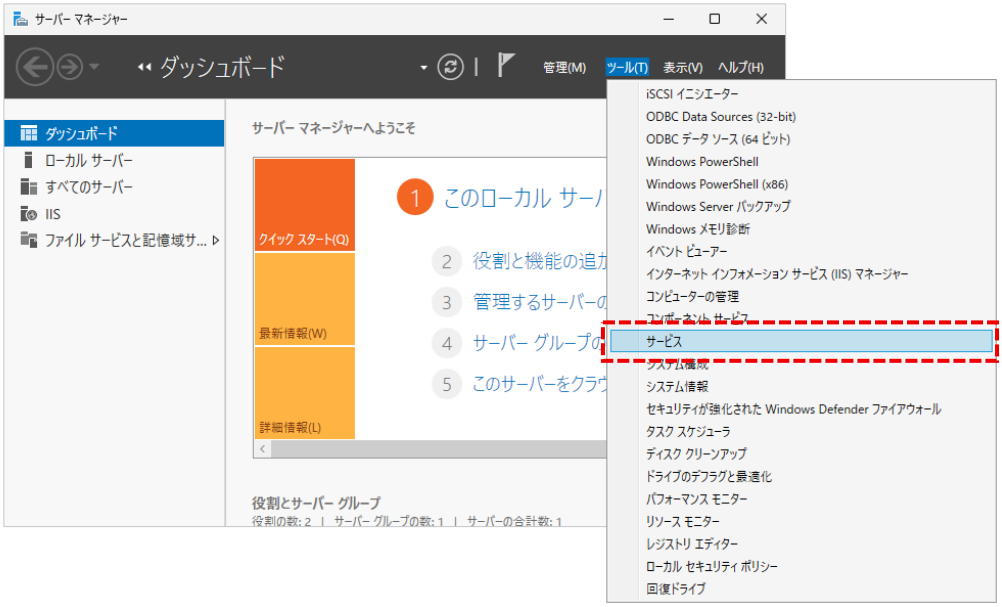


※Windows の標準機能で Open SSH サーバを導入できない場合は、OepnSSH のダウンロードならびにインストールが必要です。Microsoft による GitHub の OepnSSH フォークリポジトリに OepsnSSH が公開されております。ダウンロードならびにインストールは下記 URL を参照ください。
https://github.com/powershell/Win32-OpenSSH/releases

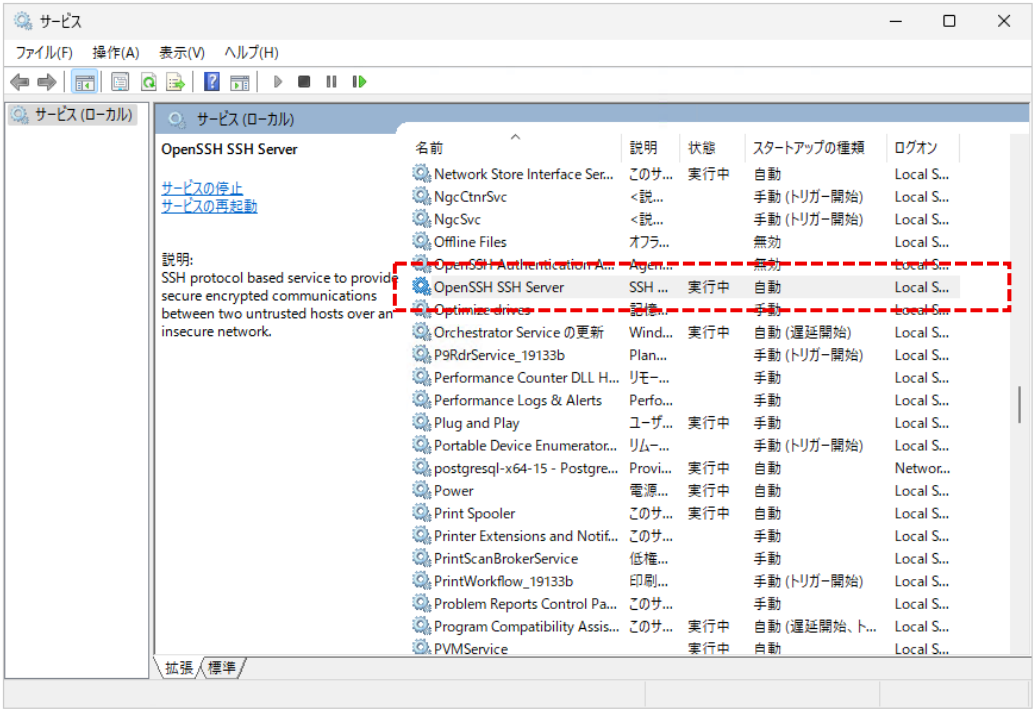
※Windows Server 2025 は「アプリ」「システム」「オプション機能」で
「OpenSSH サーバ」が追加済みであることを確認



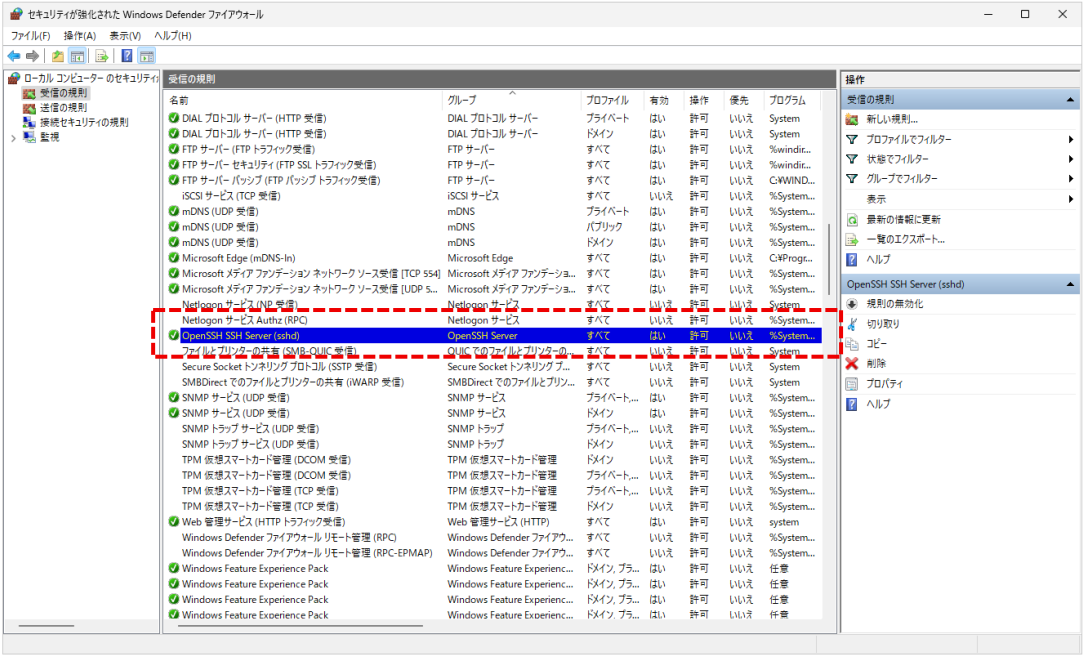
（２）「OpenSSH SSH Server」サービスの状態を確認します。
「サーバーマネージャー」を起動し、「ツール」「サービス」を選択します。



「OpenSSH SSH Server」が「実行中」であることを確認します。



「セキュリティが強化された Windows Defender ファイアウォール」の「受信の規則」で「OpenSSH SSH Server」が「許可」設定であることを確認します。



第3章 PCNS で電源管理を行うサーバの連携設定手順

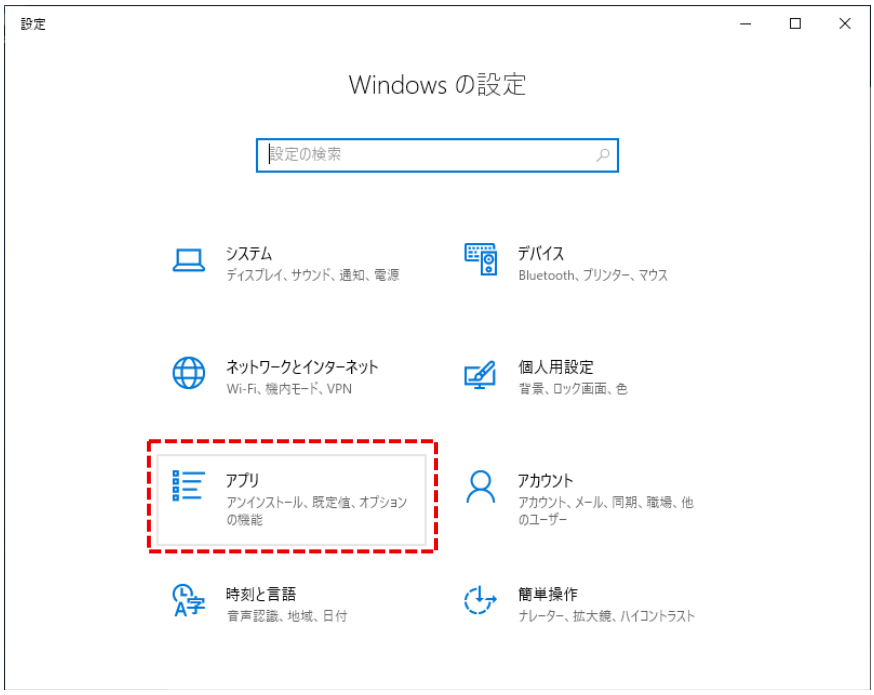
3.1. Windows環境の連携設定

3.1.1. OpenSSH クライアントの準備

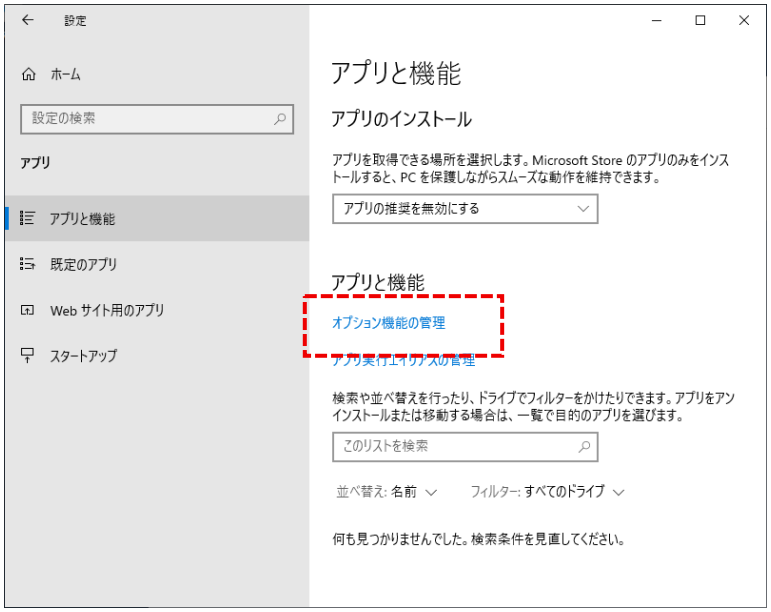
「SSC 連携対応スクリプト」は OpenSSH を利用しています。OpenSSH クライアントを利用できるよう設定します。

（1） PCNS を導入している Windows 環境から、OpenSSH クライアントが使えるよう設定してください。Windows Server 2019 以降または Windows 11 は、OpenSSH は Windows の機能として提供されています。OepnSSH クライアント機能が有効となっていることをご確認ください。手順は下記の通りです。

[設定より][アプリ]選択



[アプリと機能]→[オプション機能の管理]選択



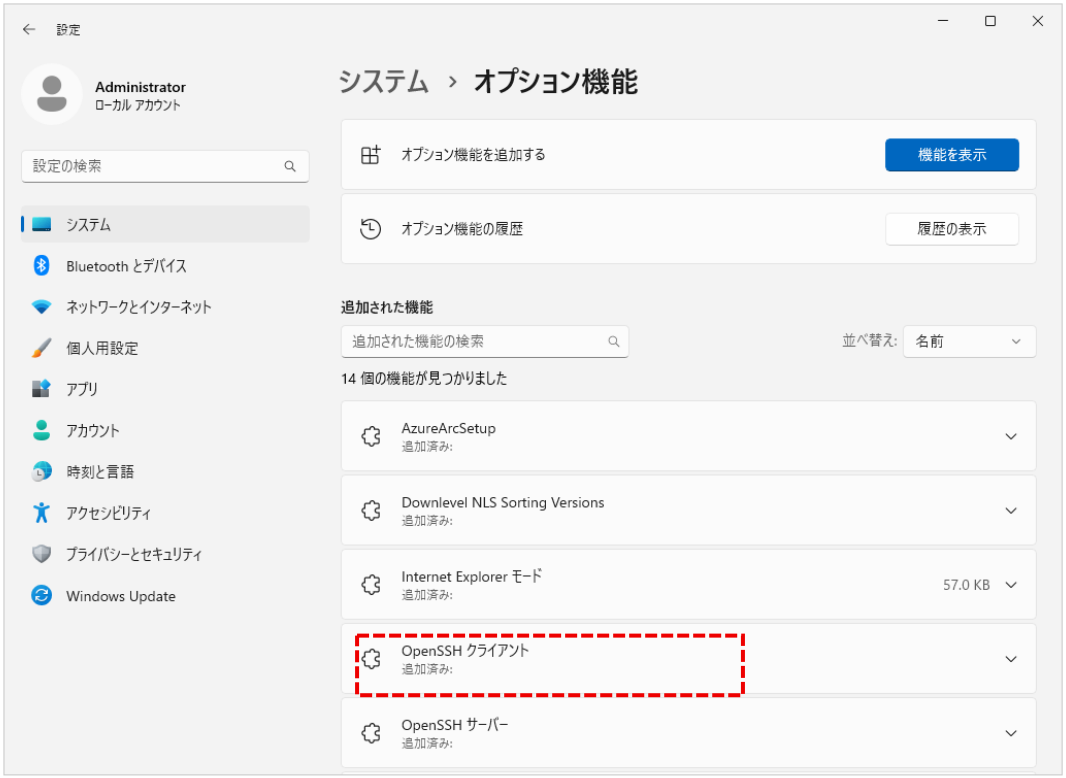
[OpenSSH クライアント]があることを確認

※Windows Server 2019 以降または Windows 11 でインターネット非接続環境の場合、インターネット接続された別環境で OepnSSH のダウンロードを行い。個別でのインストールが必要です。Microsoft による GitHub の OepnSSH フォークリポジトリに OepsnSSH が公開されております。
ダウンロードならびにインストールは下記 URL を参照ください。

https://github.com/powershell/Win32-OpenSSH/releases

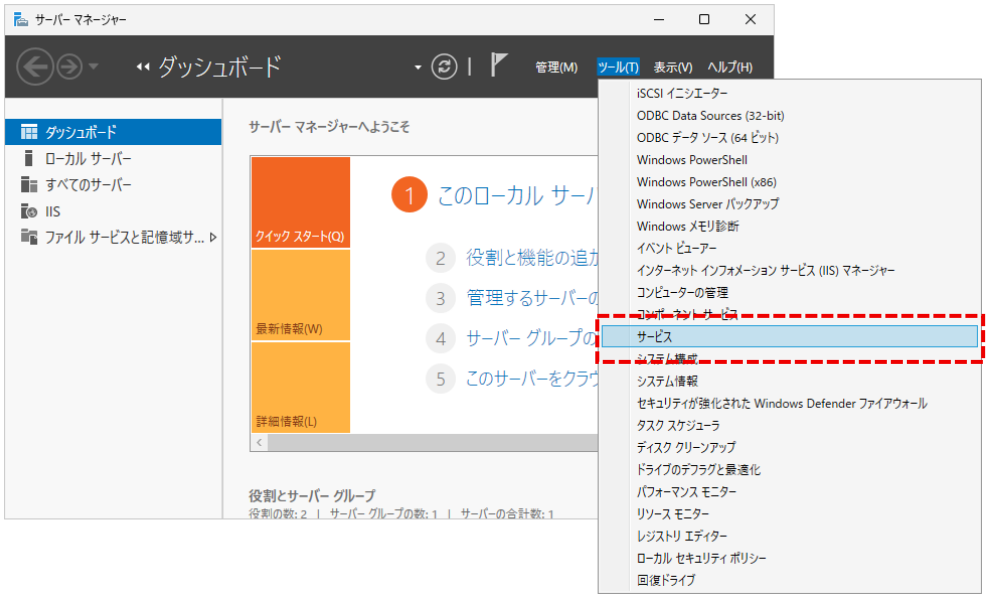
上記 URL から OepnSSH をダウンロードならびにインストールをした場合は、OpenSSH をインストールしたフォルダの絶対パスを環境変数 Path に追加してください。

※Windows Server 2025 は「アプリ」「システム」「オプション機能」で「OpenSSH クライアント」が追加済みであることを確認

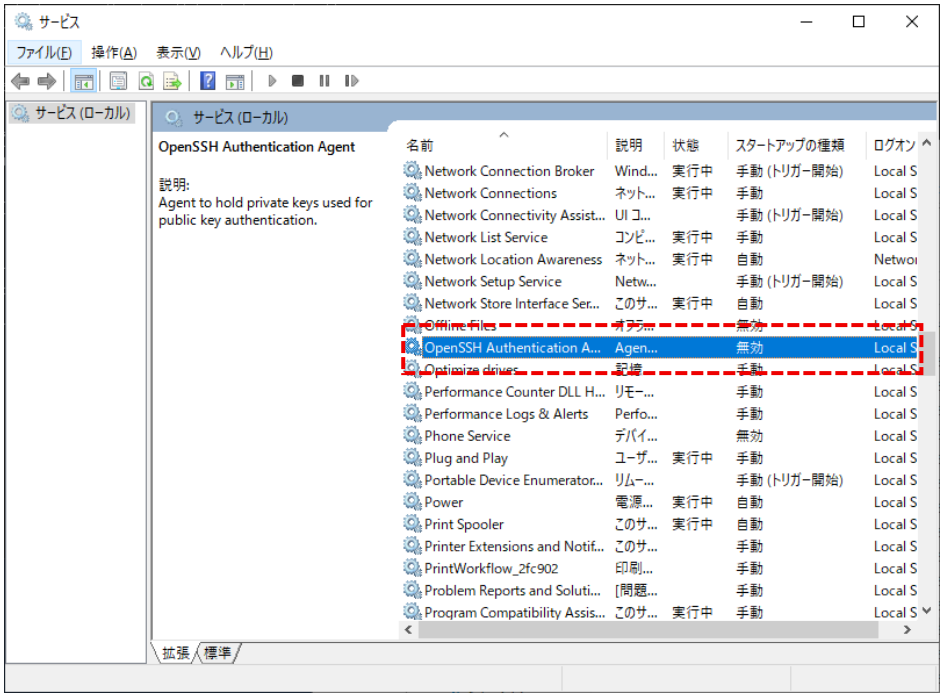


（２）　制御端末である Windows サーバにて、「OenSSH Authentication Agent」サービスの起動設定をしてください。手順は下記の通りです

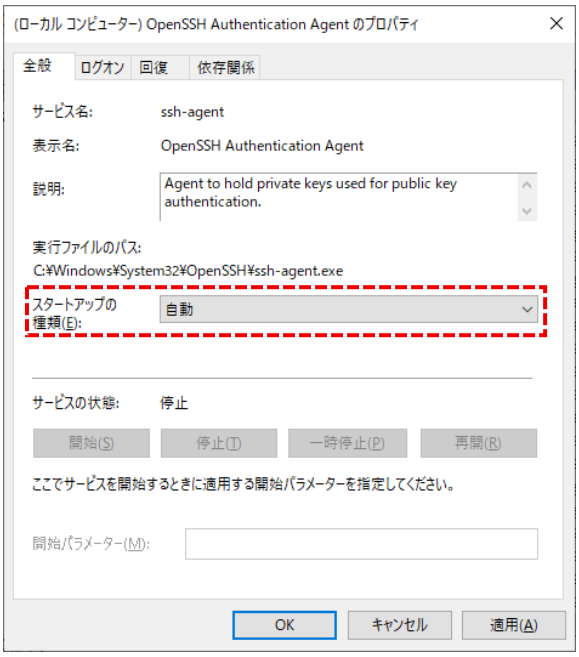
「サーバーマネージャー」を起動し、「ツール」「サービス」を選択します。



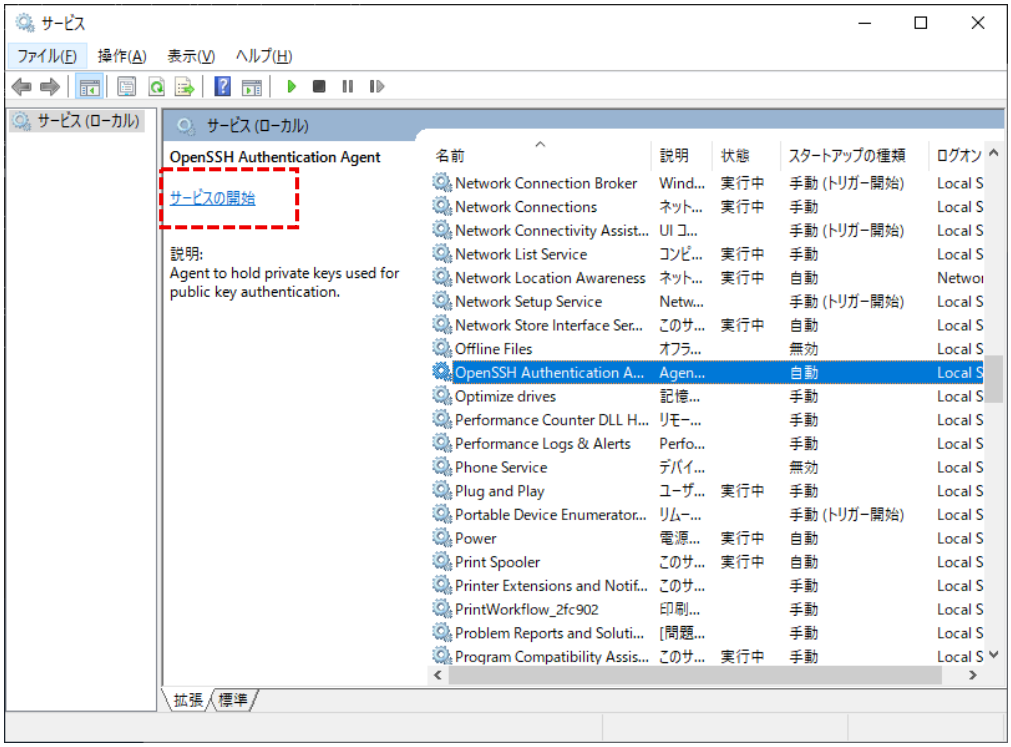
[OenSSH Authentication Agent]選択→右クリック→[プロパティ]



[スタートアップの標準]を[自動]に変更→[OK]



[サービス開始]をクリック



（3） SSC 管理サーバに接続するための公開鍵ならびに秘密鍵を作成してください。具体的には、Administrator あるいは Administrator 権限を持つユーザにて管理者権限でコマンドプロンプトを開き、下記コマンドを入力してください。

```
C:¥Users¥Administrator> ssh-keygen -t ed25519 -f id_pcnsuser
Generating public/private ed25519 key pair.
Enter passphrase (empty for no passphrase): ←空入力でEnterキー
Enter same passphrase again:                ←空入力でEnterキー
Your identification has been saved in id_pcnsuser.
Your public key has been saved in id_pcnsuser.pub.
The key fingerprint is:
SHA256:xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
administrator@xxxxxxx
The key's randomart image is:
+--[ED25519 256]--+
|             xxxx|
|                x|
|             x xx|
|             .x.x|
|        x  .xx xx|
|         x xxxx x|
|        x xxxxxxx|
|         xxxxxxxx|
|          xxxxxxx|
+----[SHA256]-----+

C:¥Users¥Administrator> dir    ←鍵が生成されていること確認
2020/04/17  16:04    <DIR>          .
2020/04/17  16:04    <DIR>          ..
2020/04/17  16:04               419 id_pcnsuser      ←秘密鍵
2020/04/17  16:04               112 id_pcnsuser.pub ←公開鍵
```

（4） 秘密鍵を「OenSSH Authentication Agent」サービスに登録します。

```
C:¥Users¥Administrator> ssh-add  “C:¥Users¥Administrator¥id_acuser”
Identity added: C:¥Users¥Administrator¥id_acuser (administrator@xxx)
```

（５）　公開鍵を SSC 管理サーバに導入します。
SSC 管理サーバの 下記ファイルに公開鍵(id_pcnsuser.pub)の内容を追記
例）
%programdata%¥ssh¥¥administrators_authorized_keys

```
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIPhAySzmf/Qg9Sy946uDuyG/
```

3.1.2. Windows 環境の連携設定(サーバシャットダウン時)

PCNS(Windows)を導入したサーバのシャットダウン時の連携は PCNS の「シャットダウン設定」を用います。

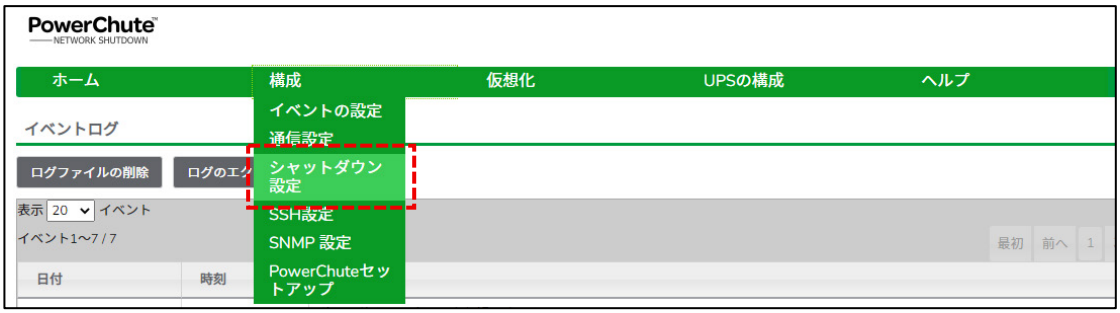
（１）SSC 連携対応スクリプトの準備

項目「1.3. SSC 連携設定用ファイルのダウンロード（２）」の SSC 連携対応スクリプト「ac_pvm_on.bat」ファイルを PCNS インストールのディレクトリ配下の「C:¥Program Files¥APC¥PowerChute¥user_files」にコピーし、SSC 管理サーバの情報に修正します。

```
@echo off
rem ---- SSC 管理サーバユーザ名 ----
set REMOTE_USER=administrator

rem ---- SSC 管理サーバホスト名・IP アドレス ----
set REMOTE_HOST=172.16.1.15

rem ---- SERVER_NAME は SSC 登録サーバ名に変更
set SERVER_NAME=Sample_Name

rem ---- REMOTE_CMD_DIR は SSC 管理サーバ内の ac_pvm.exe の
ディレクトリに変更 ----
set REMOTE_CMD_DIR="C:¥Program Files (x86)¥AUTORC¥"
```

（２）SSC 連携対応スクリプトの登録

PowerChute Network Shutdown の WEB UI で「構成」「シャットダウン設定」を選択します。



「コマンド実行」を選択し「コマンドファイルのフルパス」で SSC 連携対応スクリプト「ac_pvm_on.bat」を登録、所要時間に「10 秒」程度を設定し、「適用」を選択します。

UPS でグループ設定を行なっている場合は対象サーバ接続している UPS グループで「コマンド実行」をチェックし、「コマンドファイルのパス」で SSC 連携対応スクリプト「ac_pvm_on.bat」を登録、所要時間に「10 秒」程度を設定し、「適用」を選択します。

3.1.3. Windows 環境の連携設定(サーバ起動時)

PCNS(Windows)を導入したサーバの起動時の連携はWindows OSのタスクスケジューラを用いて設定します。

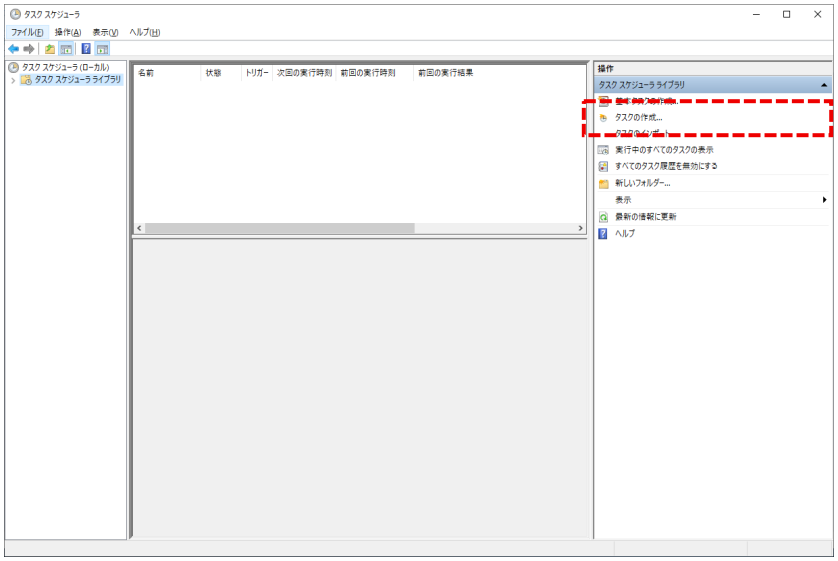
（1） SSC連携対応スクリプトの準備

項目「1.3. SSC連携設定用ファイルのダウンロード（２）」の連携対応スクリプト「ac_pvm_off.bat」ファイルをPCNSインストールのディレクトリ配下の「C:¥Program Files¥APC¥PowerChute¥user_files」にコピーし、SSC管理サーバの情報に修正します。

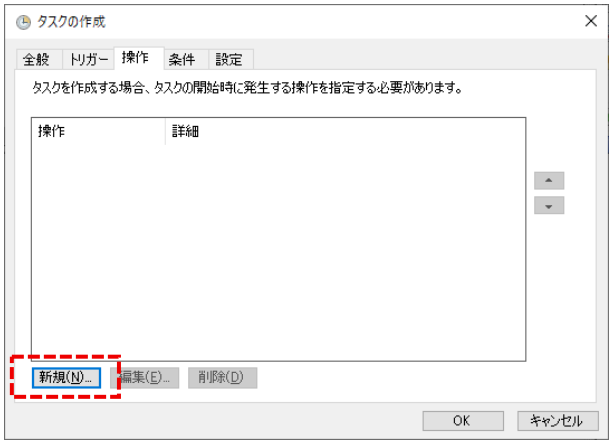
```
@echo off
rem ---- SSC管理サーバユーザ名 ----
set REMOTE_USER=administrator

rem ---- SSC管理サーバホスト名・IPアドレス ----
set REMOTE_HOST=172.16.1.15

rem ---- SERVER_NAMEはSSC登録サーバ名に変更
set SERVER_NAME=Sample_Name

rem ---- REMOTE_CMD_DIRはSSC管理サーバ内のac_pvm.exeの
ディレクトリに変更 ----
set REMOTE_CMD_DIR="C:¥Program Files (x86)¥AUTORC¥"
```

（2） タスクスケジューラに連携対応スクリプトを登録します。
「サーバーマネージャー」を起動し、「ツール」「タスクスケジューラ」を選択します。

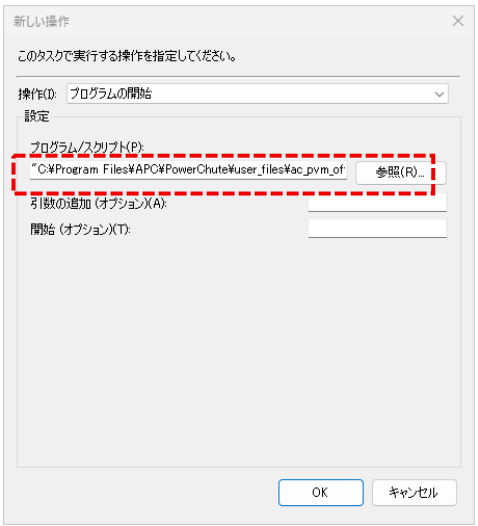
[タスクスケジューラライブラリ]→[タスクの作成...]を選択します。



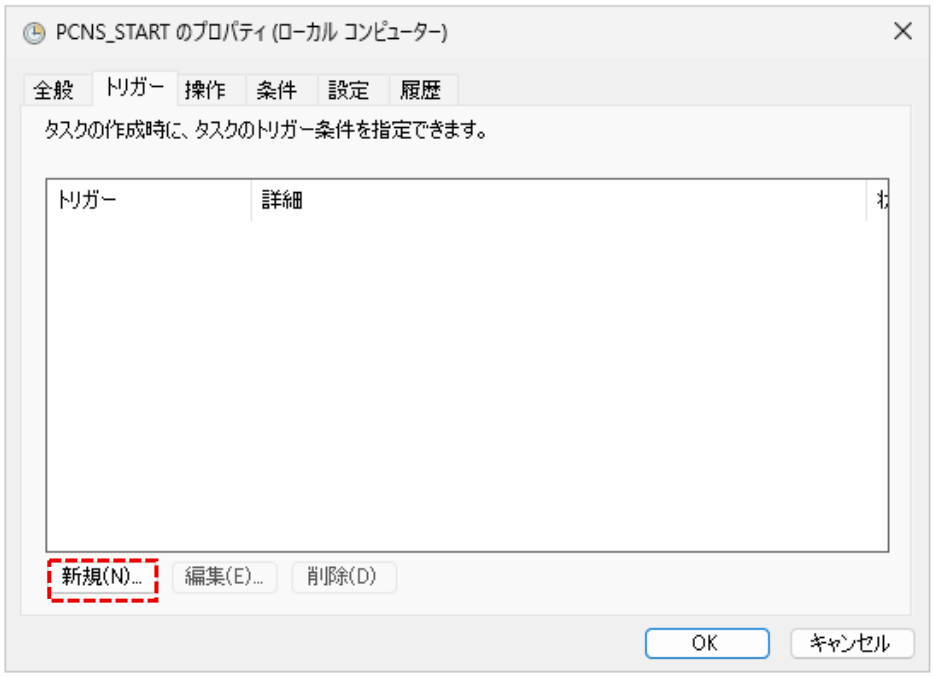
[操作]タブ→[新規]を選択します。



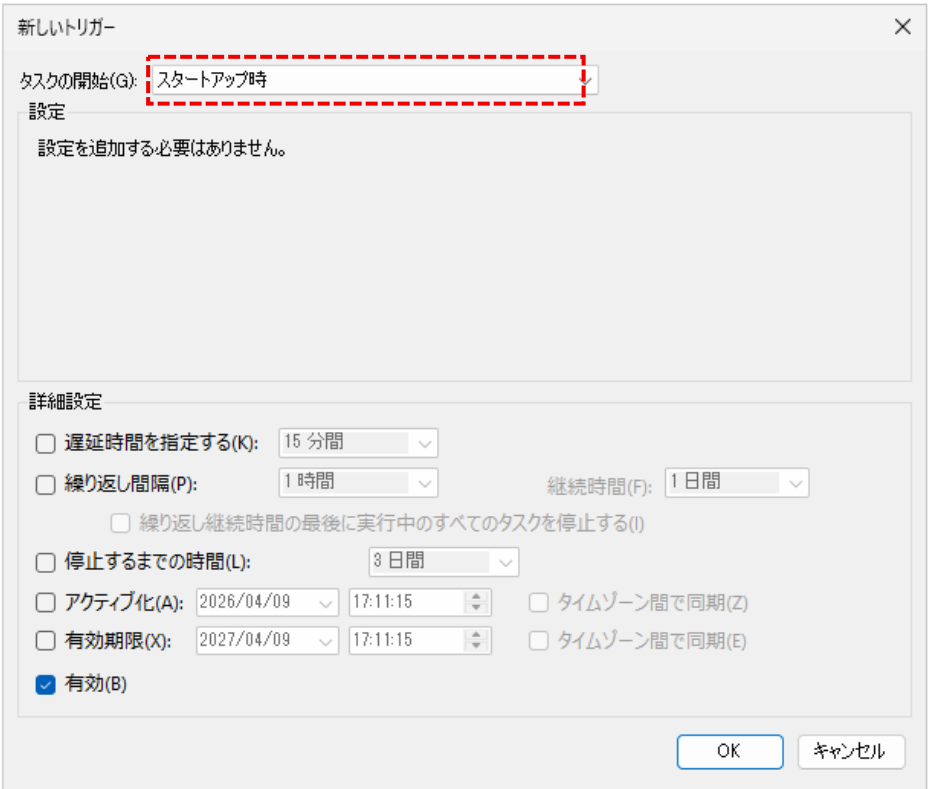
[プログラム/スクリプト]に「ac_pvm_off.bat」のフルパスを登録→[OK]を選択します。



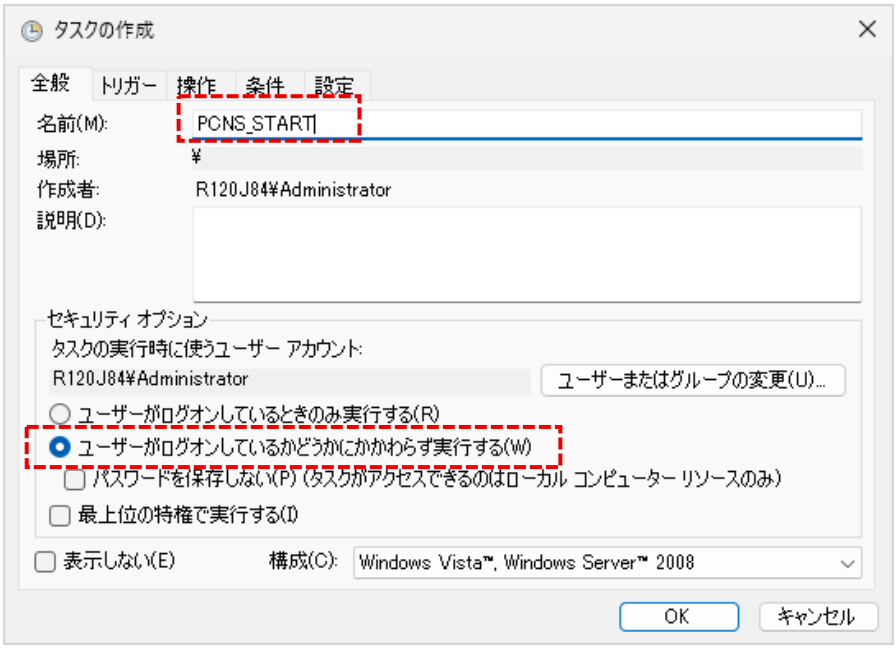
[トリガー]タブ→[新規]を選択します。



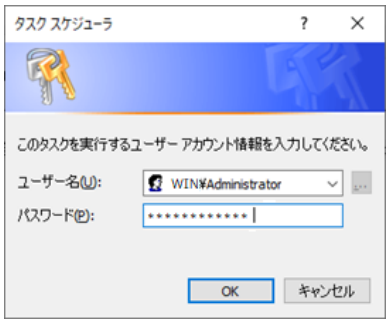
[新しいトリガー]→[タスクの開始]→[スタートアップ時]を選択します。



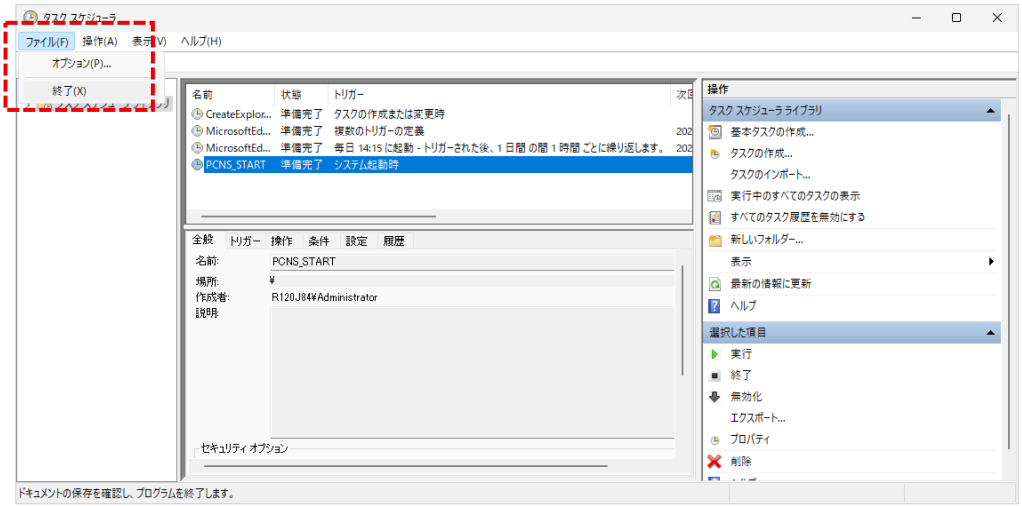
[全般]タブ→[名前]に「PCNS_START」、[セキュリティオプション]に「ユーザがログオンしているかどうかに関わらず実行する」を選択します。



パスワード入力→[OK]を選択します。



[ファイル]→[終了]を選択します。



3.2. Linux環境の連携設定

3.2.1. SSH クライアントの準備

「SSC 連携対応スクリプト」は SSH を利用しています。SSC 管理サーバに接続するための公開鍵ならびに秘密鍵を作成してください。root 権限で下記コマンドを入力してください。作成された秘密鍵「id_pcns」は「/root/.ssh」に「id_rsa」でリネームしてコピーするか「/root/.ssh/config」ファイルに登録してください。

例）

```
[root@r120d31 ~]# ssh-keygen -t ed25519 -f id_pcns
Generating public/private ed25519 key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in id_pcns
Your public key has been saved in id_pcns.pub
The key fingerprint is:
SHA256:zPS931VbpW1xC/U+8ZNgQiHdqmP6F5O6LH8WMwl5fEY root@r120d31
The key's randomart image is:
+--[ED25519 256]--+
|         ..oo  . |
|          o. ..E.|
|         .  .++.o+|
|       + .  =ooo*O|
|        S o = *=B|
|         + .  O .*|
|        o o + +..|
|       . .  = + ..|
|        ..+.+ . .|
+----[SHA256]-----+
[root@r120d31 ~]# ls
id_pcns.pub   id_pcns
```

公開鍵を SSC 管理サーバに導入します。

SSC 管理サーバの 下記ファイルに公開鍵(id_pcns.pub)の内容を追記

例）

%programdata%¥ssh¥¥administrators_authorized_keys

```
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIPhAySzmf/Qg9Sy946uDuyG/
```

3.2.2. Linux 環境の連携設定(サーバシャットダウン時)

PCNS(Linux)を導入したサーバのシャットダウン時の連携は PCNS の「シャットダウン設定」を用います。

（１）SSC 連携対応スクリプトの準備

項目「1.3. SSC 連携設定用ファイルのダウンロード（２）」の SSC 連携対応スクリプト「ac_pvm_on.sh」ファイルを PCNS インストールのディレクトリ配下の「/opt/APC/PowerChute/user_files」にコピーし、SSC 管理サーバの情報に修正します。

パーミッションを変更します。

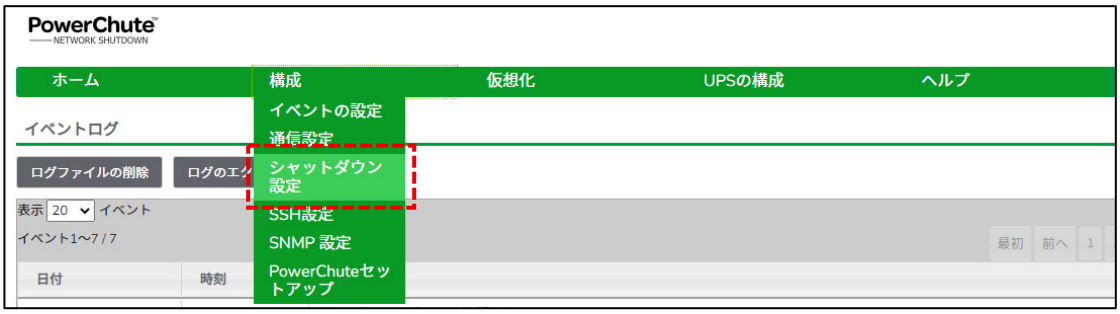
```
[root@r120d31]# cd /opt/APC/PowerChute/user_files/
[root@r120d31 user_files]# chmod 755 ac_pvm_on.sh
```

vi 等のエディタで SSC 管理サーバの情報に修正します。

```
#!/bin/bash

# ---- SSC 管理サーバユーザ名 ----
REMOTE_USER="administrator"

# ---- SSC 管理サーバホスト名・IP アドレス ----
REMOTE_HOST="172.16.1.15"

# ---- SAMPLE_NAME は SSC 登録サーバ名に変更
SERVER_NAME="Sample_Name"

# ---- REMOTE_CMD_DIR は SSC 管理サーバ内の ac_pvm.exe のディレクトリに変更 ----
REMOTE_CMD_DIR="C:/Program Files (x86)/AUTORC/"
```

（２）SSC 連携対応スクリプトの登録

PowerChute Network Shutdown の WEB UI で「構成」「シャットダウン設定」を選択します。



「コマンド実行」を選択し「コマンドファイルのフルパス」で SSC 連携対応スクリプト「ac_pvm_on.ssh」を登録、所要時間に「10 秒」程度を設定し、「適用」を選択します。

3.2.3. Linux 環境の連携設定(サーバ起動時)

PCNS(Linux)を導入したサーバの起動時の連携はサービスを用いて設定します。

（１）SSC 連携対応スクリプトの準備

項目「1.3. SSC 連携設定用ファイルのダウンロード（２）」の SSC 連携対応スクリプト「ac_pvm_off.sh」ファイルを PCNS インストールのディレクトリ配下の「/opt/APC/PowerChute/user_files」にコピーし、SSC 管理サーバの情報に修正します。

パーミッションを変更します。

```
[root@r120d31]# cd /opt/APC/PowerChute/user_files/
[root@r120d31 user_files]# chmod 755 ac_pvm_off.sh
```

vi 等のエディタで SSC 管理サーバの情報に修正します。

```
#!/bin/bash

# ---- SSC 管理サーバユーザ名 ----
REMOTE_USER="administrator"

# ---- SSC 管理サーバホスト名・IP アドレス ----
REMOTE_HOST="172.16.1.15"

# ---- SAMPLE_NAME は SSC 登録サーバ名に変更
SERVER_NAME="Sample_Name"

# ---- REMOTE_CMD_DIR は SSC 管理サーバ内の ac_pvm.exe のディレクトリに変更 ----
REMOTE_CMD_DIR="C:/Program Files (x86)/AUTORC/"
```

（２）SSC 連携対応スクリプトをサービスに登録
PowerChute Network Shutdown の WEB UI で「構成」「シャットダウン設定」を選択します。

サービス「ac_pvm.service」を以下の内容で作成します。

```
[root@r120d31]# cd /usr/lib/systemd/system
[root@r120d31 system]# vi ac_pvm.service
```

vi 等のエディタで SSC 管理サーバの情報に修正します。

```
[Unit]
Description=ssc maintenance mode
After=sshd.service

[Service]
Type=simple
ExecStart=/opt/APC/PowerChute/user_files/ac_pvm_off.sh
Restart=on-failure
RemainAfterExit=yes
User=root

[Install]
WantedBy=multi-user.target
```

サービス「ac_pvm.service」を登録します。

```
[root@r120d31 system]# systemctl enable ac_pvm
Created symlink /etc/systemd/system/multi-
user.target.wants/ac_pvm.service →
/usr/lib/systemd/system/ac_pvm.service.
[root@r120d31 system]# systemctl daemon-reload
```

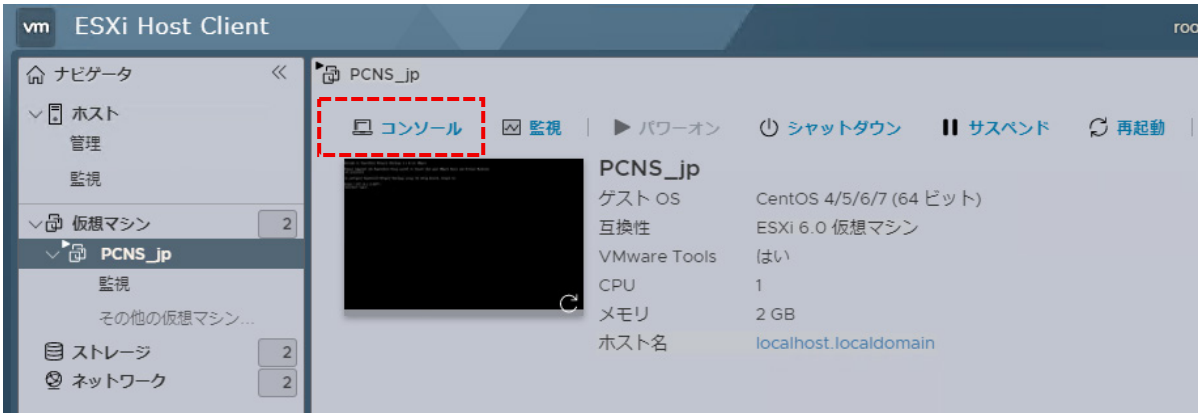
3.3. VMware ESX/ESXi環境(デプロイしたPCNS環境より制御)の連携設定

3.3.1. SSH クライアントの準備

（１）デプロイされた PCNS 環境の SSH 有効化

・「https://ESXi サーバーの IP アドレス」で「ESXi Host Client」に接続する

・PCNS をデプロイした「仮想マシン」の「コンソール」を起動する



・以下のコマンドを実行する

systemctl start sshd」

※アクセスが拒否される場合は以下の root ログイン許可も実施してください。

元の 00-complianceascode-hardening.conf ファイルのコピーを作成します。

```
# cp /etc/ssh/sshd_config.d/00* /etc/ssh/sshd_config.d/SavedConfig.txt
```

root ログイン許可を変更します。

```
# sed -i 's/PermitRootLogin no/PermitRootLogin yes/g'
/etc/ssh/sshd_config.d/00*
```

sshd サービスを再起動します。

```
# systemctl restart sshd
```

（２）SSH 用の鍵を生成

「SSC 連携対応スクリプト」は SSH を利用しています。SSC 管理サーバに接続するための公開鍵ならびに秘密鍵を作成してください。root 権限で下記コマンドを入力してください。作成された秘密鍵「id_pcns」は「/root/.ssh」に「id_rsa」でリネームしてコピーするか「/root/.ssh/config」ファイルに登録してください。

例）

```
[root@r120d31 ~]# ssh-keygen -t ed25519 -f id_pcns
Generating public/private ed25519 key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in id_pcns
Your public key has been saved in id_pcns.pub
The key fingerprint is:
SHA256:zPS931VbpW1xC/U+8ZNgQiHdqmP6F5O6LH8WMwl5fEY root@r120d31
The key's randomart image is:
+--[ED25519 256]--+
|         ..oo  . |
|          o. ..E.|
|         .  .++.o+|
|       + . =ooo*O|
|        S o = *=B|
|         + .  O .*|
|        o o + +..|
|       . .  = + ..|
|        ..+.+ . .|
+----[SHA256]-----+
[root@r120d31 ~]# ls
id_pcns.pub   id_pcns
```

3.3.2. デプロイした PCNS 環境の連携設定(サーバシャットダウン時)

デプロイした PCNS 環境(Linux)の連携設定(サーバシャットダウン時)は「3.2.2. Linux 環境の連携設定(サーバシャットダウン時)」を参照願います。

3.3.3. デプロイした PCNS 環境の連携設定(サーバ起動時)

デプロイした PCNS 環境(Linux)の連携設定(サーバ起動時)は「3.2.3. Linux 環境の連携設定(サーバ起動時)」を参照願います。

3.4. VMware ESX/ESXi環境(SSC管理サーバ上のPCNS(Windows)環境より制御)の連携設定

3.4.1. SSC 管理サーバ上の PCNS(Windows)環境の連携設定(サーバシャットダウン時)

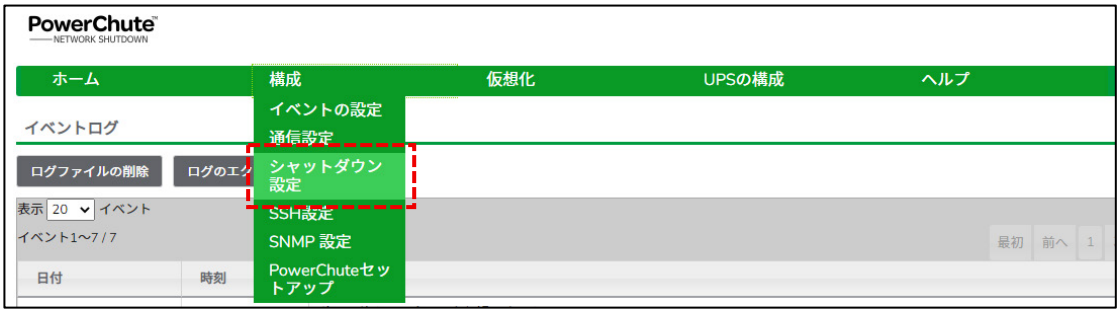
SSC 管理サーバ上に PCNS(Windows)を導入した環境で、VMware ESX/ESXi サーバのシャットダウンを行う場合の連携は PCNS の「シャットダウン設定」を用います。

（１）SSC 連携対応スクリプトの準備

項目「1.3. SSC 連携設定用ファイルのダウンロード（２）」の SSC 連携対応スクリプト「ac_pvm_on_sv.bat」「ac_pvm_on_sv.csv」の 2 ファイルを PCNS インストールのディレクトリ配下の
「C:¥Program Files¥APC¥PowerChute¥user_files」にコピーし、
「ac_pvm_on_sv.csv」に PCNS の UPS に登録されている VMware ESX/ESXi サーバの情報に修正します。
例）対応する PCNS 登録の UPS に VMware ESXi のサーバが一台登録されている場合は、「SANMPE_SEVER_NAME1」を SSC に登録されている、ホスト名に変更してください。

```
id,ssc_server_name
1,esxi43
```

（２）SSC 連携対応スクリプトの登録
PowerChute Network Shutdown の WEB UI で「構成」「シャットダウン設定」を選択します。



「コマンド実行」を選択し「コマンドファイルのフルパス」で SSC 連携対応スクリプト「ac_pvm_on_sv.bat」を登録、所要時間に「10 秒」程度を設定し、「適用」を選択します。

UPS でグループ設定を行なっている場合は対象サーバ接続している UPS グループで「コマンド実行」をチェックし、「コマンドファイルのパス」で SSC 連携対応スクリプト「ac_pvm_on_sv.bat」を登録、所要時間に「10 秒」程度を設定し、「適用」を選択します。

3.4.2. SSC 管理サーバ上の PCNS(Windows)環境の連携設定(サーバ起動時)

PCNS(Windows)環境の連携設定(サーバ起動時)は VMware EWSX/ESXi サーバの起動スクリプト(local.sh)を編集し SSC 連携コマンドを登録します。

（１）SSH 用の鍵を生成

SSC 連携対応スクリプト」は SSH を利用しています。SSC 管理サーバに接続するための公開鍵ならびに秘密鍵を作成してください。root 権限で下記コマンドを入力してください。作成された秘密鍵「id_pcns」は「/root/.ssh」に「id_rsa」でリネームしてコピーするか「/root/.ssh/config」ファイルに登録してください。

※FIPS モード設定されている場合は、許可された暗号化形式を利用願います。

例）

```
[root@r120d73:~] /usr/lib/vmware/openssh/bin/ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (//.ssh/id_rsa):
//.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in //.ssh/id_rsa
Your public key has been saved in //.ssh/id_rsa.pub
The key fingerprint is:
SHA256:AdI82eEFwHgffinhBuCQBiiKDmhNsAC5eecOddyUI/4 root@r120d80.NECE.local
The key's randomart image is:
+---[RSA 3072]----+
|*+o.o*o+o+.      |
|= ++..XoB.       |
|==o .+ Xo+ .     |
|B...o + B.o      |
|+. + . oSo       |
| .. .   E        |
|   o             |
|    .            |
|                 |
+----[SHA256]-----+
```

Firewall 設定で「sshClient」を許可します
コマンドは以下です
「esxcli network firewall ruleset set --ruleset-id=sshClient --enabled=true」

```
[root@r120d73:~] esxcli network firewall ruleset list
Name                        Enabled  Enable/Disable configurable  Allowed IP configurable
--------------------------  -------  ---------------------------  -----------------------
sshServer                      true                        false                     true
sshClient                     false                         true                     true
...

[root@r120d73:~] esxcli network firewall ruleset set --ruleset-id=sshClient --enabled=true

[root@r120d73:~] esxcli network firewall ruleset list
Name                        Enabled  Enable/Disable configurable  Allowed IP configurable
--------------------------  -------  ---------------------------  -----------------------
sshServer                      true                        false                     true
sshClient                      true                         true                     true
```

公開鍵を SSC 管理サーバに導入します。
SSC 管理サーバの 下記ファイルに公開鍵(//.ssh/id_rsa.pub)の内容を追記
例）
%programdata%¥ssh¥¥administrators_authorized_keys

```
ssh-ed25519 AAAAC3NzaC1lZDI[redacted]
```

（２）OS 起動時に実行されるスクリプト(local.sh)の編集

以下の local.sh に SSC 連携スクリプトを追記する

```
例）
[root@r120d73:~] cd /etc/rc.local.d/
[root@r120d73:/etc/rc.local.d]vi local.sh
```

連携スクリプト修正は以下の「/etc/rc.local.d/local.sh」の赤字部分です。

例）local.sh の編集例

```
root@r120d73:/etc/rc.local.d] cat local.sh
#!/bin/sh ++group=host/vim/vmvisor/boot

# local configuration options

# Note: modify at your own risk!  If you do/use anything in this
# script that is not part of a stable API (relying on files to be in
# specific places, specific tools, specific output, etc) there is a
# possibility you will end up with a broken system after patching or
# upgrading.  Changes are not supported unless under direction of
# VMware support.

# Note: This script will not be run when UEFI secure boot is enabled.

# SSC Maintenance Mode OFF - START
SSH=/bin/ssh
SSH_USER=administrator
SSH_HOST=172.16.1.15

AC_PVM="C:¥¥work¥¥SSC¥¥ac_pvm.exe"
MAINTE_FLAG="-M OFF"
TARGET_HOST="R110C023"

echo ${SSH} -l ${SSH_USER} ${SSH_HOST} ¥"${AC_PVM}¥" ${MAINTE_FLAG}
${TARGET_HOST}
${SSH} -l ${SSH_USER} ${SSH_HOST} ¥"${AC_PVM}¥" ${MAINTE_FLAG}
${TARGET_HOST}
# SSC Maintenance Mode OFF - STOP

exit 0
```

SSC 管理サーバのユーザー名に変更

SSC 管理サーバの IP に変更

SSC に登録されているホスト名に変更