HP System Management Homepage

HP 部品番号: 466304-194
2009年11月
第 19 版

目次

表目次

第1章 製品の概要

HP System Management Homepage（HP SMH）は、HP-UX、Linux（x86、AMD64、およびインテル Itanium）、およびMicrosoft® Windows®のオペレーティング システム上で、HPサーバー用の単一のシステム管理を統合して簡素化するWebベースのインターフェイスです。

HP Webベース エージェントおよびマネジメント ユーティリティからのデータを統合することで、HP SMHは次の情報を共通の使いやすいインターフェイスで表示することができます。

- ハードウェア障害およびステータス監視
- パフォーマンス データ
- システム スレッショルド
- 診断
- 個々のサーバーのソフトウェア バージョン コントロール

HP-UXシステムの場合、HP SMHは`SysMgmtWeb`のバンドル タグを持ち、HP-UX 11i v1（B.11.11）、HP-UX 11i v2（B.11.23）、およびHP-UX 11i v3（B.11.31）のオペレーティング環境を含む、すべてのHP-UXバージョンにデフォルトでインストールされます。

HP SIM

HP SMHは、HP Systems Insight Manager（HP SIM）と強固に統合されています。HP SIM内の**[システム リスト]**ページおよび**[システム ページ]**からHP SMHに簡単に移動できます。

注記: デフォルトでHP SIMの証明書を受け入れるようになっています。詳しくは、「[信頼された管理サーバー]」を参照してください。

また、HP SMHベースのプラグインに直接アクセスするHP SIMツール（**[設定]→[HP-UX設定]**カテゴリの下）もいくつかあります。

統合管理ツール

HP SMHは、Webベースのシステム管理のための管理サーバーを提供します。

HP-UXでは、Webベースの管理機能を提供するためにHP-UX System Administration Manager（SAM）の主要な機能が強化されており、HP SMHベースで使用できるようになりました。これには、Partition Management、Peripheral Devices、Disks & File Systems、Users and Groups、Kernel Configurationなどの領域が含まれます。

HP-UX System Administration Manager（SAM）の非推奨

HP-UX System Administration Manager（SAM）は、システム管理タスクを実行するためのツールを提供するHP-UXのシステム管理ツールです。HP-UX 11i v3（B.11.31）リリースでは、SAMは推奨されません。SAMの拡張バージョンであるHP SMHは、HP-UXの管理するためのツールとしておすすめします。

HP SMHは、HP-UXを管理するためにグラフィカル ユーザー インターフェイス（GUI）、ターミナル ユーザー インターフェイス（TUI）、およびコマンド ライン インターフェイス（CLI）を提供します。`smh`コマンド（`/usr/sbin/smh`）を使用すると、これらのインターフェイスにアクセスできます。`smh(1M)`コマンドと同じ動作をする、`sam(1M)`コマンドを使用することもできますが、最初に推奨しない旨のメッセージが表示されます。

管理タスクを実行する多くのアプリケーションは、WebベースGUIインターフェイスおよび拡張されたTUIで利用できるようになりました。ただし、X WindowsベースのObAMまたはTUIベースのObAMを使用するアプリケーションがいくつかあります。

システム管理者のいくつかの機能領域が廃止されました。これらの領域は、HPテクニカル ドキュメントのWebサイト**http://docs.hp.com/ja**からアクセスできる、『HP-UX 11iリリース ノート』にリストされています。

追加資料

- Software Depot home**http://www.hp.com/go/softwaredepot**のHP SMH
  - **HP-UXの場合**

    [Security and manageability]を選択して、次に**HP System Management Homepage [HP-UX]**の順に選択します。
  - **Linuxの場合**

    [Linux]、**[HP Integrity Essentials Foundation Pack for Linux]**の順に選択します。
- HP Insight Essentials Softwareページ**http://www.hp.com/jp/servers/manage**
- **『HP System Management Homepageリリース ノート』**　リリース ノートには、リリースの最新情報、機能と変更点、システム要件、および既知の問題についての説明が記載されています。リリース ノートは、HPテクニカル ドキュメントのWebサイト**http://docs.hp.com/ja**に掲載されています。
- **HP System Management Homepageヘルプ システム**　HP SMHの使用、保守、トラブルシューティングに関するドキュメントが含まれています。HP SMHアプリケーションから、**[ヘルプ]**メニューにアクセスします。
- **『HP System Management Homepageインストレーション ガイド』**　インストレーション ガイドには、HP SMHをインストールして使用開始するための情報が記載されています。このガイドは、HP SMHに関連する基本的な概念、定義、および機能について説明しています。インストレーション ガイドは、HPテクニカル ドキュメントのWebサイト**http://docs.hp.com/ja**に掲載されています。LinuxおよびWindowsリリースでは、インストレーション ガイドは、Management CDおよびHP SMHのマニュアルライブラリ**http://www.hp.com/jp/proliantessentials_manual**から利用可能です。
- **『HP System Management Homepageユーザー ガイド』**　ユーザー ガイドには、HP SMHの使用、保守、トラブルシューティングに関するドキュメントが含まれています。LinuxとWindowsでは、このガイドは、HPテクニカル ドキュメントのWebサイト**http://docs.hp.com/ja**に掲載されています。HP-UXでは、HPは印刷されたユーザー ガイドを用意していません。HP SMHの使用、保守、およびトラブルシューティングについての情報は、HP SMHオンライン ヘルプを参照してください。
- **Next generation single-system management on HP-UX 11i v2（B.11.23）**　HP SMHとそのプラグインを紹介するWhite Paperです。このドキュメントに記載されているHP SMHとプラグインの用途は、HP SMHで提供される機能にハイライトしています。White Paperは、HPテクニカル ドキュメントのWebサイトに**http://docs.hp.com/en/4AA0-4052ENW/4AA0-4052ENW.pdf**として掲載されています。
- `hpsmh(1M)` **マンページ**　HP-UXでは、コマンドラインから`man hpsmh`コマンドを使用してマンページが利用できます。この情報は、LinuxおよびWindowsでは利用できません。
- `smhstartconfig(1M)` **マンページ**　HP-UXでは、コマンドラインから`man smhstartconfig`コマンドを使用してマンページが利用できます。この情報は、LinuxおよびWindowsでは利用できません。

  `smhassist(1M)` **マンページ**　`smhassist`コマンドを使用して、SMHの設定を確認し、依存ソフトウェア、パッチ、または構成エラーがあるかどうかを確認できます。HP-UX 11i v3（B.11.31）およびHP-UX 11i v2（B.11.23）オペレーティング システム リリースでは、マンページは、`man smhassist`コマンドを使用してCLIから使用できます。この情報は、HP-UX 11i v1（B.11.11）、LinuxおよびWindowsオペレーティング システムでは使用できません。
- `sam(1M)` **マンページ**　HP-UXでは、コマンドラインから`man sam`コマンドを使用してマンページを参照できます。この情報は、LinuxおよびWindowsでは利用できません。SAM機能の機能変更については、この文書の前のセクションで説明されています。

関連項目

- 開始するには
- HP SMHページ

第2章 開始するには

HP System Management Homepage（HP SMH）の使用を開始する際は、以下の手順を実行して、HP SMHを適切に設定し、ユーザーとセキュリティ プロパティを設定してください。

HP SMHを設定するには、以下の手順に従ってください。

- HP-UXオペレーティング システム環境では、HP SMHは、デフォルト設定でインストールされます。次のファイルの環境変数とタグ値を変更して、設定を変更することができます。
  - `/opt/hpsmh/lbin/envvars`
  - `/opt/hpsmh/conf.common/smhpd.xml`
  - `/opt/hpsmh/conf/timeout.conf`
- Linuxオペレーティング システム環境では、HP SMHは、デフォルト設定でインストールされます。設定は、`/usr/local/hp` （Linux x86およびx64システムの場合）または`/opt/hp/hpsmh/smhconfig/hpSMHSetup.sh`（Itaniumシステムの場合）にあるperlスクリプト（hpSMHSetup.pl）を使用して変更できます。
- Windowsオペレーティング システム環境では、インストール時にHP SMHを設定できます。

注記: HP-UX、Linux、およびWindowsオペレーティング システムの設定を変更するには、HPテクニカル ドキュメントWebサイト**http://docs.hp.com/ja/**に掲載されている『HP System Management Homepage インストール ガイド』を参照してください。

ユーザー アクセスとセキュリティ プロパティを設定するには、以下の手順に従ってください。

1. ユーザーの権限を効率的に管理するためにユーザー グループを追加します。
   「ユーザー グループ」を参照してください。
2. 信頼モードを設定します。
   「[信頼 モード]」を参照してください。
3. ローカル アクセスまたは匿名アクセスを設定します。
   「[匿名/ローカル アクセス]」を参照してください。

関連項目

- サインイン
- ファイアウォールの設定
- 証明書の自動インポート
- サインアウト

サインイン

[サイン イン]ページから、利用可能なHP Insightマネジメント エージェントが含まれている**[ホーム]**ページにアクセスできます。

[サイン イン ページ]には、次のものがあります。

- **[ユーザー グループ]**設定項目で設定された有効なグループの一部であるアカウントからユーザー名とパスワードを入力する2つのフィールド。
- 入力フィールド下の2つのボタン：
  - **サインイン**　ユーザー名とパスワードの値を検証します。どちらも有効な場合は、HP SMH メイン ページが表示されます。
  - **クリア**　入力値を削除します。
- 疑問符のアイコン（**?**）は、認証メカニズムとサインイン プロセスについての情報のあるフローティング ツールチップ ボックスを表示したり、非表示にしたりします。

表 2-1 ツールチップ ボックス

名前	説明
ユーザー名	ユーザーは、SMHに受け入れられるユーザー グループに含まれる必要があります。
パスワード	ユーザー名とパスワードは、有効なユーザーと一致する必要があります。
サインイン	SMHへのユーザー名サインインを検証します。
クリア	ユーザー名およびパスワード入力フィールドを削除します。
?	ツールチップ ボックスの表示/非表示
チェックボックス	選択されたマネジメント サーバー証明書を自動的にインポートします。これは、HP SIMからSSOを使用し、信頼モードが**TrustByCert**に設定されている場合に適用されます。

注記: サインイン試行でエラーが発生したら、**[サイン イン]**ページに戻ります。

設定メカニズムによって、管理者は画像と**[サイン イン]**ページのメッセージをカスタマイズすることができます。管理者は、カスタム ロゴと警告メッセージを使用することができます。ページがロードされると、HP SMHはパーソナライズされたコンテンツが有効で使用可能かどうかを検証します。コンテンツが使用可能な場合は、HP SMHは標準画像と警告メッセージを使用します。

Internet ExplorerからのHP System Management Homepage（HP SMH）の起動

Internet ExplorerでHP SMHにサインインするには、以下の手順に従ってください。

1. **`https://`*ホスト名*`:2381/`**にナビゲートします。

   初めてこのURIにアクセスすると、**[セキュリティの警告]**ダイアログ ボックスが表示され、サーバーを信頼するかどうかを尋ねられます。証明書をインポートしない場合は、HP SMHにアクセスするたびに**[セキュリティの警告]**が表示されます。

   HP-UXサーバーを参照する場合は、**`http://`*ホスト名*`:2301/`**を使用する必要があります。

   デフォルトでは、HP-UXのインストールは`autostart`機能を有効にします。デーモンはポート2301を監視し、ポート2381からリクエストされたHP SMHを開始し、タイムアウト時間が経過すると停止します。常にポート2381で動作するようにHP SMHを設定することもできます。詳しくは、`smhstartconfig(1M)`コマンドを参照してください。

   `[Start on Boot]`機能が有効な場合（`[autostart]`の代わりに）、メッセージ ウィンドウにセキュリティ機能についての説明が表示されます。2381ポートにリダイレクトされるまで数秒ほど待つか、メッセージの下のリンクをクリックします。[System Management Homepage sign in]ページが表示されます。

   設定を変更する手順については、HPテクニカル ドキュメントWebサイト**http://docs.hp.com/ja/**に掲載されている『HP System Management Homepageインストール ガイド』を参照してください。

   注記: 管理対象の各システムに利用者自身のパブリック キー インフラストラクチャ（PKI）を実装したり、利用者が自分で作成した証明書をインストールしたりするには、管理に使用するブラウザーに認証機関ルート証明書をインストールできます。ルート証明書がインストールされている場合、**[セキュリティの警告]**ダイアログ ボックスは表示されません。このアラートが表示された場合は、間違ったシステムにアクセスしている可能性があります。**認証機関ルート証明書**のインストール手順について詳しくは、ブラウザーのオンライン ヘルプを参照してください。

2. **[はい]**をクリックします。

   [サイン イン]ページが表示されます。インストール中に**[匿名]**アクセスを有効にした場合は、System Management Homepageが表示されます。

3. オペレーティング システムによって認識されているユーザー名を入力します。
   - **HP-UX**　HP SMHは、最初は、ルート ユーザーのみアクセスを許可します。
   - **Linux**　HP SMHは、初期状態で、ルート オペレーティング システム グループに属すユーザーのみアクセスを許可します。
   - **Windows**　HP SMHは、管理者オペレーティング システム グループに属すユーザーのみアクセスを許可します。

   ユーザー証明書が本物であることが確認できない場合、ユーザーはアクセスを拒否されます。

   初期状態でアクセスが許可されたユーザーでHP SMHにログインしたら、他のオペレーティング システム グループのユーザーにセキュリティの設定を行うアクセス権を与えてください。

   [administrator]（Windows）および[root]（HP-UXおよびLinux）は、HP SMHに対する管理者アクセス権を持ちます。
4. オペレーティング システムによって認識されているパスワードを入力します。
5. **[サイン イン]**をクリックします。

   System Management Homepageが表示されます。

MozillaまたはFirefoxからのHP SMHの開始

MozillaまたはFirefoxでHP SMHにサインインするには、以下の手順に従ってください。

1. **`https://ホスト名:2381/`**にナビゲートします。

   HP-UXサーバーを参照する場合は、**`http://ホスト名:2301/`**を使用する必要があります。

   デフォルトでは、HP-UXのインストールは`autostart`機能を有効にします。デーモンはポート2301を監視し、ポート2381からリクエストされたHP SMHを開始し、タイムアウト時間が経過すると停止します。常にポート2381で動作するようにHP SMHを設定することもできます。詳しくは、`smhstartconfig(1M)`コマンドを参照してください。

   `[Start on Boot]`機能が有効な場合（`[autostart]`の代わりに）、メッセージ ウィンドウにセキュリティ機能についての説明が表示されます。2381ポートにリダイレクトされるまで数秒ほど待つか、メッセージの下のリンクをクリックします。[System Management Homepage sign in]ページが表示されます。

   設定を変更する手順については、HPテクニカル ドキュメントWebサイト**http://docs.hp.com/ja/**に掲載されている『HP System Management Homepageインストール ガイド』を参照してください。
2. **[OK]**をクリックします。

   [サイン イン]ページが表示されます。インストール中に**[匿名]**アクセスを有効にした場合は、System Management Homepageが表示されます。
3. オペレーティング システムによって認識されているユーザー名を入力します。
   - **HP-UX**　HP SMHは、最初は、ルート ユーザーのみアクセスを許可します。
   - **Linux**　HP SMHは、初期状態で、ルート オペレーティング システム グループに属すユーザーのみアクセスを許可します。
   - **Windows**　HP SMHは、管理者オペレーティング システム グループに属すユーザーのみアクセスを許可します。

   [administrator]（Windows）および[root]（HP-UXおよびLinux）は、HP SMHに対する管理者アクセス権を持ちます。
4. オペレーティング システムによって認識されているパスワードを入力します。
5. **[サイン イン]**をクリックします。

   System Management Homepageが表示されます。

HP SIMからのHP SMHの開始

WebブラウザーでHP SIMにサインインしてHP SMHを開始するには、以下の手順に従ってください。

1. **https://ホスト名:50000/**にナビゲートします。

   初めてこのリンクにアクセスすると、**[セキュリティの警告]**ダイアログ ボックスが表示され、サーバーを信頼するかどうかを尋ねられます。証明書をインポートしない場合は、Systems Insight Manager（HP SIM）にアクセスするたびに**[セキュリティの警告]**が表示されます。

注記: 管理対象の各システムにカスタムパブリック キー インフラストラクチャ（PKI）を実装したり、利用者が自分で作成した証明書をインストールしたりするには、管理に使用するブラウザーに認証機関ルート証明書をインストールできます。ルート証明書がインストールされている場合、**[セキュリティの警告]**ダイアログ ボックスは表示されません。このアラートが表示された場合は、間違ったシステムにアクセスしている可能性があります。**認証機関ルート証明書**のインストール手順について詳しくは、ブラウザーのオンライン ヘルプを参照してください。

2. **[はい]**をクリックします。

   [サイン イン]ページが表示されます。

3. オペレーティング システムによって認識されているユーザー名を入力します。
4. オペレーティング システムによって認識されているパスワードを入力します。
5. **[サイン イン]**をクリックします。
6. **[ツール]→[システム情報]→[System Management Homepage]**を選択します。
7. リストからターゲット システムを選択します。
8. 対象のシステムの横にあるチェックボックスを選択し、**[適用]**をクリックします。
9. システムの隣にあるチェックボックスを選択して、ターゲット システムを検証します。次に、**[今すぐ実行]**をクリックします。

   サーバーを信頼するかどうかを確認する**[セキュリティの警告]**ダイアログ ボックスが表示されます。証明書をインポートしない場合は、HP SMHにアクセスするたびに**[セキュリティの警告]**が表示されます。

   System Management Homepageが表示されます。

HP-UXコマンド ラインからの開始

samまたはsmhコマンドを実行して、DISPLAY環境変数を設定する場合、HP SMHはデフォルトのWebブラウザーを開きます。DISPLAY環境変数が設定されていない場合は、HP SMHはTUIで開きます。管理タスクを実行する多くのアプリケーションは、WebベースGUIインターフェイスおよび拡張されたTUIで利用できるようになりました。ただし、X WindowsベースのObAMまたはTUIベースのObAMを使用するアプリケーションがいくつかあります。

smh(1M) コマンドを使用することをおすすめします。ただし、sam(1M) コマンドは、継続して利用可能となり、smh(1M) コマンドと同じ動作になります。システム管理者のいくつかの機能領域が廃止されました。これらの領域は、HPテクニカル ドキュメントのWebサイト**http://docs.hp.com/ja**からアクセスできる、『HP-UX 11iリリース ノート』にリストされています。

HP SMH管理サーバー

デフォルトでは、HP-UXのHP SMH管理サーバーは必要なときにのみ開始されます。継続的に実行されません。デーモンは管理サーバーのインスタンスを開始するために、ポート2301を監視します。Linuxでは、起動時にHP SMHが開始します。

関連項目

- 開始するには
- ファイアウォールの設定
- 証明書の自動インポート
- サインアウト
- HP SMHページ

ファイアウォールの設定

Windows

Windows XP Service Pack 2およびWindows Server 2003 SBSを含む特定のオペレーティング システムは、ファイアウォールを実装しているため、ブラウザーがバージョン コントロール レポジトリ マネージャーにアクセスするために必要なポートにアクセスできません。この問題を解決するには、[例外]を使用してファイアウォールを設定し、ブラウザーがHP SIMとバージョン コントロール レポジトリ マネージャーによって使用されるポートにアクセスできるようにしてください。

注記: Windows XP Service Pack 2の場合、このファイアウォール設定によってSP2のセキュリティ強化はデフォルトのままになりますが、トラフィックはポートを経由できるようになります。このポートは、バージョン コントロール レポジトリ マネージャーを実行するために必要です。ブラウザーで正しく通信するには、セキュア ポートと非セキュア ポートの両方を追加する必要があります。

ファイアウォールを設定するには、次のように操作します。

1. **[スタート]→[設定] [コントロール パネル]**の順に選択します。
2. **[Windowsファイアウォール]**をダブルクリックして、ファイアウォールの設定を指定します。
3. **[例外]**を選択します。
4. **[ポートの追加]**をクリックします。
5. 次の製品名およびポート番号情報を入力します。

   ファイアウォール保護に、次の表にある例外を追加します。

   表 2-2 ファイアウォールの例外

製品	ポート番号
HP SMHの非セキュア ポート：	2301
HP SMHのセキュア ポート：	2381

6. **[OK]**をクリックして設定を保存し、**[ポートの追加]**ダイアログ ボックスを閉じます。
7. **[OK]**をクリックして設定を保存し、**[Windowsファイアウォール]**ダイアログ ボックスを閉じます。

Linux

ファイアウォールは、インストールされているLinuxのバージョンによって設定方法が異なります。

Red Hat Enterprise Linux 4および5

以下のリストは、/etc/sysconfig/iptablesファイル内の、Red Hat Enterprise Linux 4および5のiptablesファイアウォール ルールの例を示しています。

```
# Firewall configuration written by redhat-config-securitylevel
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:RH-Firewall-1-INPUT - [0:0]
-A INPUT -j RH-Firewall-1-INPUT
-A FORWARD -j RH-Firewall-1-INPUT
-A RH-Firewall-1-INPUT -i lo -j ACCEPT
-A RH-Firewall-1-INPUT -p icmp --icmp-type any -j ACCEPT
-A RH-Firewall-1-INPUT -p 50 -j ACCEPT
-A RH-Firewall-1-INPUT -p 51 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

```
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 21 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

以下のリストは、/etc/sysconfig/iptablesファイル内の、HP SMHにアクセスを許可するRed Hat Enterprise Linux 4および5のiptablesファイアウォール ルールの新しい値を示しています。

```
# Firewall configuration written by redhat-config-securitylevel
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:RH-Firewall-1-INPUT - [0:0]
-A INPUT -j RH-Firewall-1-INPUT
-A FORWARD -j RH-Firewall-1-INPUT
-A RH-Firewall-1-INPUT -i lo -j ACCEPT
-A RH-Firewall-1-INPUT -p icmp --icmp-type any -j ACCEPT
-A RH-Firewall-1-INPUT -p 50 -j ACCEPT
-A RH-Firewall-1-INPUT -p 51 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 21 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 2301 -j
ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 2381 -j
ACCEPT
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

SUSE Linux Enterprise Server

SUSE Linux Enterprise Server 9および10のファイアウォールは、YAST2ユーティリティを使用して設定します。

ファイアウォールを設定するには、次のように操作します。

1. YAST2ユーティリティで、**[Security & Users]**→**[Firewall]**の順に選択します。
   [Firewall Configuration (Step 1 of 4):Basic Settings]ウィンドウが表示されます。
2. **[次へ]**をクリックします。
   [Firewall Configuration (Step 2 of 4):Services]ウィンドウが表示されます。
3. **[Additional Services]**フィールドに、**2301:2381**と入力し、**[Next]**をクリックします。
   [Firewall Configuration (Step 3 of 4):Features]ウィンドウが表示されます。
4. **[次へ]**をクリックします。
   [Firewall Configuration (Step 4 of 4):Logging Options]ウィンドウが表示されます。

5. **[次へ]**をクリックします。
   設定を保存してファイアウォールを有効にするかどうかを確認するダイアログボックスが表示されます。
6. **[Continue]**をクリックします。
   ファイアウォールが設定され、ユーザーの設定が保存されます。

関連項目

- 開始するには
- サインイン
- 証明書の自動インポート
- サインアウト
- HP SMHページ

証明書の自動インポート

[管理サーバー証明書の自動インポート]機能により、HP SIMシステムからHP SMHにアクセスする際にHP SIM 証明書を自動的にインポートすることができます。

注記: HP SIMの証明書を自動的にインポートするには、HP SMHに対する管理者アクセス権を持つアカウントでログインしている必要があります。

HP SIMの証明書を自動的にインポートするには、以下の手順に従ってください。

1. **HP Systems Insight Manager**または**HP Insightマネージャー7**システムから、システムへのリンクを選択します。
   HP SMH（**[設定]**-**[セキュリティ]**-**[信頼モード]**）で**[証明書による信頼]**オプションが選択されていて、アクセスしているHP SIMシステムの証明書が**[信頼された証明書リスト]**にインポートされていない場合は、**[サイン イン]**ページに**[管理サーバー証明書の自動インポート]**オプションが表示されます。**サーバー名**から取得された証明書情報によって、HP SIMの証明書の詳細が表示されます。
2. HP SIMの証明書を**[信頼された証明書リスト]**に追加しない場合は、**[管理サーバー証明書の自動インポート]**の選択を解除します。このオプションの選択を解除しても ログイン証明書を入力する必要がありますが、管理者証明書がなくてもログインできます。ただし、管理者の証明書はログインする必要はありません。
   HP SMHがHP SIMを自動的にインポートできるようにした場合は、システムへの将来のアクセスはシームレスになります。ログイン証明書は求められません。
3. **[管理サーバー証明書の自動インポート]**が選択された状態で、HP SMHの証明書を入力し、**[サイン イン]**をクリックします。これにより、証明書が自動的にインポートされます。
   証明書が**[信頼済み証明書リスト]**に追加されます。

関連項目

- 開始するには
- サインイン
- ファイアウォールの設定
- サインアウト
- セキュリティ

サインアウト

HP SMHは、以下のいずれかの方法でサインアウトできます。

- HP SMHバナーで、**[サイン アウト]**をクリックします。
  HP System Management Homepage **[サイン イン]**ページが表示されます。
- HP SMHにサインインするために使用したWebブラウザーのすべてのインスタンスを閉じます。

関連項目

- 開始するには
- サインイン
- ファイアウォールの設定
- 証明書の自動インポート
- HP SMHページ

第3章 ソフトウェアのナビゲート

HP System Management Homepage（HP SMH）では、情報を提供するすべてのHP Webベース システム マネジメント ソフトウェアが表示されます。さらに、HP SMHには、各種のカテゴリ（ボックス）が表示され、各ボックスのアイコンが項目のステータスを示します。詳しくは、「[ホーム]ページ」を参照してください。

HP SMHメイン ページは、2つの領域に分かれます。ヘッダーと標準コンテナです。

- **ヘッダー フレーム**　ヘッダー フレームは、どのページを表示しているときでも常に表示されます。さらに、次の4つの下位領域が含まれます。
  - **マスター ヘッダー。**WindowsおよびLinuxで、リンクは、表示中のパス、ユーザー、および**[サイン アウト]**リンクを表示します。

    マスター ヘッダー。HP-UXで、ヘッダーは、表示しているパス、ユーザー情報（ログインしているユーザー）、**サインアウト** リンク、および**[セッション期限なし]**チェックボックスを表示します
  - **メニュー。** 各項目は、次のようなページまたはセクションへの直接のリンクです。
    - [ホーム]
    - [設定]
    - [タスク]
    - [ツール]
    - [ログ]
    - [Webアプリケーション]（WindowsおよびLinuxのみ）
    - [サポート]
    - [ヘルプ]
  - **メイン タイトル領域。** マスター ヘッダーおよびメニューの下の領域は、次の項目を含みます。
    - **タイトル。**　表示中のページのセクションのタイトル。
    - **ホスト名。**　システムの名前。
    - **システム モデル。**　サーバー用のHP Insightマネジメント エージェントがシステムにインストールされていない場合、モデルは**[不明]**と表示されます。
    - **マネジメント プロセッサー。**　マネジメント プロセッサーの名前。
    - **データ ソース**　マネジメント データに含まれるソースを示します。たとえば、WBEM for HP Insight Management WBEM ProviderまたはSNMP for HP Insightマネジメント エージェントなどです。ソースがインストールされていない場合、データ文字列は表示されません。
    - **アイコン。**　クリックすることでアイコンおよびリスト ビュー モードを切り替えることのできるオプション。
    - **ブレッドクラム。**　4つの部分に分かれるメイン タイトルの下の領域。
      - 第1レベル メニュー項目
      - **説明。**　クリックするとWebアプリケーションの可能なすべてのステータスを表示するフローティング ボックスを表示するリンク。

- **更新。** ヘッダーおよび情報領域を再ロードするリンク。
- **時刻。** ページがロードされた時刻を表示します。時刻領域をマウス オーバすると、ページがロードされた日付が表示されます。

- **データ フレーム。** 標準コンテナは、セクションまたはページを次のものとして包含します。
  - ボックス
  - アイコン
  - 図形としてのページ
  - サポート
  - ヘルプ
  - Webアプリケーション

  データ フレームには、システム上のすべてのHP Webベース システム マネジメント ソフトウェアおよびユーティリティのステータスが表示されます。

[情報領域]

ご使用のオペレーティング システム（HP-UX、Linux、またはWindows）により、ヘッダー フレームまたはデータ フレームに次のような情報が表示されます。

- **HP SMH ページ**
  - 「サインイン」
  - 「[ホーム]ページ」
  - 「[設定]ページ」
  - 「[タスク]ページ」
  - 「[ログ]ページ」
  - 「[Webアプリケーション]ページ」
  - 「[サポート]ページ」
  - 「[ヘルプ]ページ」
- **現在のユーザー。** [現在のユーザー]には、サインインしているユーザーIDが表示されます。
  - ユーザーがオペレーティング システム ベース ユーザーの場合は、**[サイン アウト]**リンクが表示されます。
  - 匿名アクセスが有効な場合は、**[現在のユーザー]**に**[hpsmh_anonymous]**が表示され、**[サイン イン]**リンクが表示されます。
  - **ローカル アクセス**が有効にされている場合は、**[現在のユーザー]**に**[hpsmh_local_anonymous]**または**[hpsmh_local_administrator]**（どのレベルのアクセスが有効にされているかによります）と表示され、ユーザー タイプの下にローカル アクセスであることが示されます。
  - ユーザー タイプが**[local_access_administrator]**である場合は、サインインまたはサインアウトリンクは表示されません。
- **ボックス。** ボックスは、項目の一覧に、結果のステータスとともに、Webアプリケーションの結果を表示します。
  - 全体のステータス アイコンは、ボックス内で最も悪いステータスを示します。タイトルとともにタイトル バーに表示されます。
  - タイトル バーの下は、ボックス内の項目の一覧です。各項目では、名前の左にステータス アイコンが表示されることがあります。
  - ボックスのフッタ内には、項目が5行の制限を超えた場合に項目の合計数を含めるためにクリックするとボックスの高さを拡張するリンクのある拡張ラインがあります。

- **ローディング画面。**　項目が選択されると、ページのロード プロセス中にステータス インジケーターが**ローディング画面**として表示されます。これによって、ユーザーは最初に選択した後で他の項目を選択できなくなります。
- **列の数。**　リスト ビュー モードで各行に表示されるボックスまたは列の数は、表示解像度設定で定義されています。たとえば、解像度が800x600に設定されている場合は、1行に3つのボックスのみが表示されます。より解像度が大きければ、ボックスの表示数は4つになります。
- **注。**　注は、右側のセクションで、ほとんどのページで使用されています。これらの注は、コントロールの使用方法と使用すべき値の種類が記述されています。
- **アイコン ビュー。**　アイコンは、項目とセクションに対して表示されます。アイコンをクリックすると、別のページが表示され、その項目がアイコンになります。ボックス内の項目のステータスを表示するには、アイコンをマウス オーバして、インストールされているアプリケーションの**クリティカル**、**メジャー**、**マイナー**および**警告**のステータスの合計を含むツールチップを表示します。
- **タイムアウト警告。**　タイムアウトに設定した時間制限内にSMHにページをロードしない場合に、タイムアウト警告は、右側のページ フッタにフローティング ボックスとして表示されます。
- **ページ内のダイナミック リスト。**　ページに追加または削除したい項目ごとに動的に作成された要素の一覧が表示されます。次のページに対して使用可能です。
  - [IPバインド]
  - [IP限定ログイン]
  - [信頼モード]
  - [Kerberos 認証]
  - [ユーザー グループ]
- **説明：**　インストールされたWebアプリケーションの可能なすべてのステータスを表示するフローティング ボックスを表示するリンク。

表 3-1 ステータス アイコン

アイコン	ステータス
	クリティカル
	メジャー
	マイナー
	警告
	正常
	無効
	不明
	情報

- **マネジメント プロセッサー。**　**リモートInsightボードLights-Out Edition**（**RILOE**）ボードまたは**Integrated Lights-Out**（**iLO**）ボードへのリンクが表示されます。この情報は、HP Insightマネジメント エージェントにより提供されます。この情報を提供するHP Webベース システム マネジメント ソフトウェアがインストールされていない場合は、**なし**と表示されます。

関連項目

- 開始するには
- [ホーム]ページ
- [設定]ページ
- [タスク]ページ
- [ログ]ページ
- [Webアプリケーション]ページ
- [サポート]ページ
- [ヘルプ]ページ

HP SMHページ

HP SMH には、参加しているHP Webベース システム マネジメント ソフトウェアに関連するコンフィギュレーション データへのアクセスや設定を可能にする最大9つのページがあります。**[タスク]**ページおよび**[ツール]**ページは、HP Webベース システム マネジメント ソフトウェアがそれらの情報を提供する場合に表示されます。

HP SMHページには、次のものが含まれます。

- 「開始するには」
- 「[ホーム]ページ」
- 「[設定]ページ」
- 「[タスク]ページ」
- 「[ログ]ページ」
- 「[Webアプリケーション]ページ」
- 「[サポート]ページ」
- 「[ヘルプ]ページ」

関連項目

- 製品の概要
- ソフトウェアのナビゲート
- 開始するには

第4章 [ホーム]ページ

[ホーム]ページでは、サーバーのシステム、サブシステム、およびステータス ビューを提供します。**[ホーム]**ページは、システムのグループ化およびそのステータスについても表示します。**[ホーム]**ページの情報は、統合されたエージェントまたは管理ユーティリティにより提供されます。

HP-UXオペレーティング システムの場合、**[ホーム]**ページには、統合されたWeb-Based Enterprise Management（WBEM）のプロパティ ページおよび管理ユーティリティから提供される情報が含まれます。

LinuxおよびWindowsオペレーティング システムの場合、**[ホーム]**ページには、統合されたバージョン コントロール、サーバー、ストレージの各エージェントから提供される情報が含まれます。

[全体のステータス概要]

[全体のステータス概要]には、統合されたHP Webベース システム マネジメント ソフトウェアの提供する、クリティカル、メジャー、または警告ステータスのすべてのサブシステムへのリンクが表示されます。エージェントがインストールされていない場合、またはクリティカル、メジャー、マイナー、または警告ステータスのアイテムがない場合、**[全体のステータス概要]**には**[アイテムなし]**と表示されます。

[システム ステータス]

[システム ステータス]は、下にラベルのついたステータス アイコンを表示します。特定のwebappが、システム ステータスを示す定義済みの経験則を使用して、**[システム ステータス]**アイコンの値を設定します。webappが[システム ステータス]を設定しない場合は、[全体のステータス概要]ボックスの最も悪いステータスが表示されます。

デフォルトのHP-UXプロパティ ページ

特定のWBEMプロパティ ページが、HP-UX用のHP SMHのインストールの一部として提供されます。どのページが提供されるかは、HP-UXオペレーティングシステムとともに提供されるその他のWBEMプロバイダー、たとえば`WBEMServices`（WBEM Services for HP-UX）と`SFM-CORE`（HP-UX System Fault Management）によって異なります。

[System]

[System]カテゴリでは、システム ハードウェアのWBEM情報を提供します。最初のリンクの**[System Summary]**には、システムID情報と稼働ステータスが含まれます。HP SIMを使用している場合、この稼働ステータスは、HP-UXシステムについてのHP Systems Insight Manager（HP SIM）のHS列にも表示されます。概要の他に、リンクがメモリやプロセッサーなどのサブシステムに関するステータスやその他の情報を表示します。

[Operating System]

[Operating System]カテゴリには、基本オペレーティング システムの構成、利用状況、ステータス、およびその他の情報を表示するためのリンクが含まれます。

[Network]

[Network]カテゴリには、基本ネットワーク システムの構成、利用状況、ステータス、およびその他の情報を表示するためのリンクが含まれます。

[Software]

[System Software]カテゴリには、Software Distributorバンドルおよび製品（パッチ製品を含む）に関する情報を表示するためのリンクが含まれます。

注記: このカテゴリは、Linux Itaniumでは利用できません。

[Storage]

[Storage]カテゴリには、基本ストレージ システムの構成、利用状況、ステータス、およびその他の情報を表示するためのリンクが含まれます。

SysMgmtPlus

SysMgmtPlusは、HP SMHに拡張機能を追加するためのパッケージです。SysMgmtPlusは、Webページに詳しい内容を追加し動的機能を導入することで、SMHのプロパティ ページを内容豊かなものにします。SysMgmtPlusが表示する情報は、システム上に存在するデバイスの情報だけです。

SysMgmtPlusを機能させるには、HP SMHバージョン3.0以降をインストールする必要があります。HP SMHをインストールした後に、SysMgmtPlusを手動でインストールする場合は、HP SMHを再起動する必要があります。

関連項目

- 開始するには
- [ホーム]ページ
- [設定]ページ
- [タスク]ページ
- [ログ]ページ
- [Webアプリケーション]ページ
- [サポート]ページ
- [ヘルプ]ページ

第5章 [設定]ページ

設定（**[設定]**）ページには、HP System Management Homepage（HP SMH）とツール（**[ツール]**）ページに表示されているその他の統合管理ツールの設定ページと構成ページへのリンクがあります。

表 5-1 設定ページ リンク

名前	説明	アクセス
SNMP Webエージェント ボックス（WindowsおよびLinuxのみ）	HP Webベース システム マネジメント ソフトウェアエージェントを設定するためのリンクを提供します。 • **「SMHデータ ソース管理」** HP SMHデータ ソース用のオプションを設定します。 • **「SNMPの設定」** HP Webベース システム マネジメント ソフトウェア エージェント用のオプションを設定します。 • **「UIオプション」** HP Webベース システム マネジメント ソフトウェア エージェント ヘルプ用のオプションを設定します。	メニューから**[設定]**を選択します。
HP SMHデータ ソース カテゴリ（WindowsおよびLinuxのみ）	HP SMHマネジメント データ ソースを変更できます。詳しくは、「SMHデータ ソース管理」を参照してください。	メニューから**[設定]**を選択し、**[SNMP Web エージェント]**ボックスの**[選択]**リンクをクリックします。
SNMP設定カテゴリ（WindowsおよびLinuxのみ）	Webサービスを提供し、Webアプリケーション用のセキュリティおよびHP Systems Insight Manager（HP SIM）の対話を抽象化します。詳しくは、「SNMPの設定」を参照してください。	メニューから**[設定]**を選択し、**[SNMP Web エージェント]**ボックスの**[SNMP設定]**リンクをクリックします。
SNMP設定カテゴリ（WindowsおよびLinuxのみ）	インライン ヘルプ アイコンを表示したり非表示にしたりすることができます。詳しくは、「UIオプション」を参照してください。	メニューから**[設定]**を選択し、**[SNMP Web エージェント]**ボックスの**[UIオプション]**リンクをクリックします。
System Management Homepageボックス	HP SMHを設定するためのリンクを提供します。以下のリンクがあります。 • **「UIプロパティ」** HP SMHの外観のオプションを設定します。 • **「ユーザー初期設定」** HP SMHの表示方法を設定します。 • **「セキュリティ」** セキュリティ オプションのリンクが表示されます。	メニューから**[設定]**を選択します。
UIプロパティ カテゴリ	HP SMHの外観のオプションを設定します。リストおよびアイコン ビューを選択するコントロール、会社に関するカスタム テキストおよび画像を使用するかどうかのコントロール、ボックスおよび項目順タイプの名前順またはステータス順のコントロールがあります。これらのオプションは、ユーザーが特定のオプションを**ユーザー初期設定**で設定してある場合でないかぎり、すべてのユーザーに対してデフォルトのオプションとして機能します。詳しくは、「UIプロパティ」を参照してください。	メニューから**[設定]**を選択し、**[System Management Homepage]**ボックスの**[UIプロパティ]**リンクをクリックします。

名前	説明	アクセス
ユーザー設定カテゴリ	HP SMHの表示方法を設定できます。リスト ビューとアイコン ビューを切り替えることができます。また、ボックスおよび項目順タイプを名前順またはステータス順に切り替えることができます。これらの設定は、設定するユーザーに対して有効です。これらの値は、30日間保管されます。詳しくは、「ユーザー初期設定」を参照してください。	メニューから**[設定]**を選択し、**[System Management Homepage]**ボックスの**[UIプロパティ]**リンクをクリックします。
セキュリティ	HP SMHを設定するためのリンクを提供します。以下のリンクがあります。 • [匿名/ローカル アクセス] • [IPバインド] • [IP限定ログイン] • [ローカル サーバー証明書] • [ポート2301]（WindowsおよびLinuxのみ） • [タイムアウト] • [信頼モード] • [信頼された管理サーバー] • [Kerberos認証]（Windowsのみ） • [ユーザー グループ]	メニューから**[設定]**を選択し、**[System Management Homepage]**ボックスの**[セキュリティ]**リンクをクリックします。

表 5-2 セキュリティ オプション

名前	説明	アクセス
「[匿名/ローカル アクセス]」	管理者が、匿名ユーザーがSMHページにアクセスできるようにするオプションや、管理者または匿名ユーザーとしてローカル コンソールで実行中にSMHへの自動ログインができるようにするオプションを設定できます。詳しくは、「[匿名/ローカル アクセス]」を参照してください。	メニューから**[設定]**を選択し、**[System Management Homepage]**ボックスの**[セキュリティ]**リンクをクリックします。さらに、**[匿名/ローカル アクセス]**リンクをクリックします。
「[IP バインド]」	SMHがバインドされているアドレスを制御することができます。詳しくは、「[IPバインド]」を参照してください。	メニューから**[設定]**を選択し、**[System Management Homepage]**ボックスの**[セキュリティ]**リンクをクリックします。さらに、**[IPバインド]**をクリックします。
「[IP限定ログイン]」	SMHにアクセス可能またはブロックされるアドレスを追加することができます。詳しくは、「[IP限定ログイン]」を参照してください。	メニューから**[設定]**を選択し、**[System Management Homepage]**ボックスの**[セキュリティ]**リンクをクリックします。さらに、**[IP限定ログイン]**をクリックします。
「[ローカル サーバー証明書]」	このカテゴリには、2つのブロックがあり、署名して受信した署名済み証明書を後でインポートするために認証機関（CA）に送ることのできる証明書要求を生成するために使用されます。詳しくは、「[ローカル サーバー証明書]」を参照してください。	メニューから**[設定]**を選択し、**[System Management Homepage]**ボックスの**[セキュリティ]**リンクをクリックします。さらに、**[ローカル サーバー証明書]**リンクをクリックします。
「ポート2301」	ポート2301へのアクセスを設定できます。詳しくは、「ポート2301」を参照してください。	メニューから**[設定]**を選択し、**[System Management Homepage]**ボックスの**[セキュリティ]**リンクをクリックします。さらに、**[ポート2301]**リンクをクリックします。
「タイムアウト」	SMHのタイムアウトの値を設定します。2つのタイムアウトを設定できます。それは、セッション タイムアウトとUIタイムアウトです。詳しくは、「タイムアウト」を参照してください。	メニューから**[設定]**を選択し、**[System Management Homepage]**ボックスの**[セキュリティ]**リンクをクリックします。さらに、**[タイムアウト]**リンクをクリックします。
「[信頼 モード]」	SMHの使用する信頼モードを設定します。3つの信頼モードを設定できます。それらは、証明書による信頼、名前による信頼、すべて信頼です。詳しくは、「[信頼 モード]」を参照してください。	メニューから**[設定]**を選択し、**[System Management Homepage]**ボックスの**[セキュリティ]**リンクをクリックします。さらに、**[信頼モード]**リンクをクリックします。

名前	説明	アクセス
「[信頼された管理サーバー]」	サーバーに格納された証明書を設定し、証明書を追加または削除することができます。詳しくは、「[信頼された管理サーバー]」を参照してください。	メニューから**[設定]**を選択し、**[System Management Homepage]**ボックスの**[セキュリティ]**リンクをクリックします。さらに、**[信頼済みマネジメント サーバー]**リンクをクリックします。
「Kerberos権限手順（Windowsのみ）」	管理者ユーザーがHP SMHへの**Kerberos**認証済みアクセスを持つユーザーと各アクセス レベルを設定できます。詳しくは、「Kerberos権限手順（Windowsのみ）」を参照してください。	メニューから**[設定]**を選択し、**[System Management Homepage]**ボックスの**[セキュリティ]**リンクをクリックします。さらに、**[Kerberos認証]**リンクをクリックします。
「ユーザー グループ」	管理者ユーザーがHP SMHへのアクセス権を持つユーザーのグループと各アクセス レベルを設定できます。詳しくは、「ユーザー グループ」を参照してください。	メニューから**[設定]**を選択し、**[System Management Homepage]**ボックスの**[セキュリティ]**リンクをクリックします。さらに、**[ユーザー グループ]**リンクをクリックします。

関連項目

- [ホーム]ページ
- [タスク]ページ
- [ログ]ページ
- [Webアプリケーション]ページ

SMHデータ ソース管理

[データ ソース]ページでは、HP SMH管理データ ソースを変更できます。

[データ ソース]設定は、HP Insight Management WBEM Providerがインストールされている場合にのみ使用可能です。

注記: ソースがインストールされていない場合は、SMHデータ ソースがデータ ストリングなしで表示されます。

- **SMHデータ ソース：WBEM** HP Insight Management WBEM Providerが、現在、マネジメント データをこのサーバーのSMHページに提供していることを示します。
- **SMHデータ ソース：SNMP** HP Insightマネジメント エージェント（SNMP）が、現在、マネジメント データをこのサーバーのSMHページに提供していることを示します。

データ ソースを設定するには、以下の手順に従ってください。

1. メニューから**[設定]**を選択します。
2. **[SNMP Webエージェント]**ボックスで、**[選択]**リンクをクリックします。
3. **[SNMP]**または**[WBEM]**を選択します。
4. **[選択]**をクリックします。

関連項目

▲ [設定]ページ

SNMPの設定

[SNMP設定]ページは、Webサービスを提供し、webapps用のセキュリティおよびHP SIMの対話を抽象化します。詳しくは、HP Technical Documentation Webサイト**http://docs.hp.com**に掲載されている、『HP Systems Insight Manager 5.2テクニカル リファレンス ガイド』を参照してください。

SNMP設定を設定するには、以下の手順に従ってください。

1. メニューから**[設定]**を選択します。
2. **[SNMP Webエージェント]**ボックスで、**[SNMP設定]**リンクをクリックします。

関連項目

▲ [設定]ページ

UIオプション

[UIオプション]ページにより、インライン ヘルプ アイコンを表示できます。

UIオプションを設定するには、以下の手順に従ってください。

1. メニューから**[設定]**を選択します。
2. **[SNMP Webエージェント]**ボックスで、**[UIオプション]**リンクをクリックします。
3. **[SNMP設定]**の横のチェックボックスのチェックを外し、インライン ヘルプ アイコンを非表示します。

   [SNMP設定]の横のチェック ボックスを選択し、インライン ヘルプ アイコンを表示します。
4. **[選択]**をクリックします。

関連項目

▲ [設定]ページ

UIプロパティ

[UIプロパティ]カテゴリは、HP SMHの外観のオプションを制御します。**[UIプロパティ]**には、次を選択するコントロールがあります。

- リスト ビュー
- アイコン ビュー
- ボックスおよび項目順タイプ
  - 名前順
  - ステータス順
- 最後のオプションは、管理者によって使用され、マスター ヘッダーおよび**[サイン イン]ページ**用のカスタム イメージ、および**[サイン イン]ページ**用のカスタム警告テキストが設定されます。

表 5-3 UIプロパティ オプション

オプション	説明
[プレゼンテーション モード]	リストから選択してデフォルトの表示モードを設定できます。**[プレゼンテーション モード]**には、2つのオプション（**[リスト ビュー]**と**[アイコン ビュー]**）があります。
ボックス順	ボックスが表示される順を指定します。名前順にすると、項目はアルファベット順に表示されます。ステータス順にすると、悪いほう（クリティカル）から良いほう（正常）の順に表示されます。
ボックス項目順	ボックス内の項目が表示される順を指定します。名前順にすると、項目はアルファベット順に表示されます。ステータス順にすると、悪いほう（クリティカル）から良いほう（正常）の順に表示されます。
カスタム テキストおよびイメージの使用	管理者が、**[サイン イン]**ページのカスタム警告メッセージおよび**[サイン イン]**ページの画像およびマスター ヘッダーを設定できるようにします。

[UIプロパティ]を設定するには、以下の手順に従ってください。

1. メニューから**[設定]**を選択します。
2. **[System Management Homepage]**ボックスで、**[UIプロパティ]**リンクをクリックします。
3. **[プレゼンテーション モード]**リストから、**[リスト]**または**[アイコン]**を選択します。
4. **[ボックス オーダー]**リストから、**[ステータス]**または**[名前]**を選択します。
5. **[ボックス アイテム オーダー]**ドロップダウン リストから、**[ステータス]**または**[名前]**のいずれかを選択します。

6. カスタム イメージおよびカスタム警告を使用するには、以下の手順に従ってください。
   a. イメージ ファイルとテキスト ファイルは、それぞれ専用サブディレクトリに配置してください。
      - *SMHBaseDir*/data/htdocs/custom_ui/logo0.jpg（画面画像のロードのため）
      - *SMHBaseDir*/data/htdocs/custom_ui/logo1.jpg（マスター ヘッダー画像のため）
      - *SMHBaseDir*/data/htdocs/custom_ui/warning1.txt（警告テキストのため）

      3つすべてのファイルは、カスタマー画像および警告テキストの表示のために必要です。
   b. **[カスタム テキストおよびイメージの使用]**の横のチェックボックスをクリックします。
7. **[適用]**をクリックします。

関連手順

▲ ユーザー初期設定

関連項目

▲ [設定]ページ

ユーザー初期設定

[ユーザー初期設定]カテゴリは、HP SMHの外観のオプションを制御します。

- リスト ビュー
- アイコン ビュー
- ボックスおよび項目順タイプ
  - 名前順
  - ステータス順

表 5-4 ユーザー設定オプション

オプション	説明
[プレゼンテーション モード]	リストから選択してデフォルトの表示モードを設定できます。**[プレゼンテーション モード]**には、2つのオプション（**[リスト ビュー]**と**[アイコン ビュー]**）があります。
ボックス順	ボックスが表示される順を指定します。名前順にすると、項目はアルファベット順に表示されます。ステータス順にすると、悪いほう（クリティカル）から良いほう（正常）の順に表示されます。
ボックス項目順	ボックス内の項目が表示される順を指定します。名前順にすると、項目はアルファベット順に表示されます。ステータス順にすると、悪いほう（クリティカル）から良いほう（正常）の順に表示されます。

ユーザー設定を設定するには、以下の手順に従ってください。

1. メニューから**[設定]**を選択します。
2. **[System Management Homepage]**ボックスで、**[ユーザー初期設定]**リンクをクリックします。
3. **[プレゼンテーション モード]**リストから、**[リスト]**または**[アイコン]**を選択します。
4. **[ボックス オーダー]**リストから、**[ステータス]**または**[名前]**を選択します。
5. **[ボックス アイテム オーダー]**リストから、**[ステータス]**または**[名前]**を選択します。
6. （HP-UXの場合のみ）セッションの期限切れをさせない場合は、**[Session Never Expires]**の横のチェックボックスをクリックします。

注記: HP SMHサービス タイムアウトは、HP-UXシステムのみで使用可能です。

7. **[適用]**をクリックします。

注記: 各ユーザーは、セッション中の外観を設定することができます。個別のユーザー設定は、UIプロパティ内の設定に優先します。

関連手順

▲ UIプロパティ

関連項目

▲ [設定]ページ

セキュリティ

[セキュリティ]リンクでは、HP SMH自身のセキュリティを管理するためのオプションを提供します。

表 5-5 セキュリティ オプション

名前	説明	アクセス
「[匿名/ローカル アクセス]」	管理者が、匿名ユーザーがSMHページにアクセスできるようにするオプションや、管理者または匿名ユーザーとしてローカル コンソールで実行中にSMHへの自動ログインができるようにするオプションを設定できます。詳しくは、「[匿名/ローカル アクセス]」を参照してください。	メニューから**[設定]**を選択し、**[System Management Homepage]**ボックスの**[セキュリティ]**リンクをクリックします。さらに、**[匿名/ローカル アクセス]**リンクをクリックします。
「[IP バインド]」	SMHがバインドされているアドレスを制御することができます。詳しくは、「[IP バインド]」を参照してください。	メニューから**[設定]**を選択し、**[System Management Homepage]**ボックスの**[セキュリティ]**リンクをクリックします。さらに、**[IPバインド]**をクリックします。
「[IP限定ログイン]」	SMHにアクセス可能またはブロックされるアドレスを追加することができます。詳しくは、「[IP限定ログイン]」を参照してください。	メニューから**[設定]**を選択し、**[System Management Homepage]**ボックスの**[セキュリティ]**リンクをクリックします。さらに、**[IP限定ログイン]**をクリックします。
「[ローカル サーバー証明書]」	このカテゴリには、2つのブロックがあり、署名して受信した署名済み証明書を後でインポートするために認証機関（CA）に送ることのできる証明書要求を生成するために使用されます。詳しくは、「[ローカル サーバー証明書]」を参照してください。	メニューから**[設定]**を選択し、**[System Management Homepage]**ボックスの**[セキュリティ]**リンクをクリックします。さらに、**[ローカル サーバー証明書]**リンクをクリックします。
「ポート2301」	ポート2301へのアクセスを設定できます。詳しくは、「ポート2301」を参照してください。	メニューから**[設定]**を選択し、**[System Management Homepage]**ボックスの**[セキュリティ]**リンクをクリックします。さらに、**[ポート2301]**リンクをクリックします。
「タイムアウト」	SMHのタイムアウトの値を設定します。2つのタイムアウトを設定できます。それは、セッション タイムアウトとUIタイムアウトです。詳しくは、「タイムアウト」を参照してください。	メニューから**[設定]**を選択し、**[System Management Homepage]**ボックスの**[セキュリティ]**リンクをクリックします。さらに、**[タイムアウト]**リンクをクリックします。
「[信頼 モード]」	SMHの使用する信頼モードを設定します。3つの信頼モードを設定できます。それらは、証明書による信頼、名前による信頼、すべて信頼です。詳しくは、「[信頼 モード]」を参照してください。	メニューから**[設定]**を選択し、**[System Management Homepage]**ボックスの**[セキュリティ]**リンクをクリックします。さらに、**[信頼モード]**リンクをクリックします。
「[信頼された管理サーバー]」	サーバーに格納された証明書を設定し、証明書を追加または削除することができます。詳しくは、「[信頼された管理サーバー]」を参照してください。	メニューから**[設定]**を選択し、**[System Management Homepage]**ボックスの**[セキュリティ]**リンクをクリックします。さらに、**[信頼済みマネジメント サーバー]**リンクをクリックします。
「Kerberos権限手順（Windowsのみ）」	管理者ユーザーがHP SMHへの**Kerberos**認証済みアクセスを持つユーザーと各アクセス レベルを設定できます。詳しくは、「Kerberos権限手順（Windowsのみ）」を参照してください。	メニューから**[設定]**を選択し、**[System Management Homepage]**ボックスの**[セキュリティ]**リンクをクリックします。さらに、**[Kerberos認証]**リンクをクリックします。

名前	説明	アクセス
「ユーザー グループ」	管理者ユーザーがHP SMHへのアクセス権を持つユーザーのグループと各アクセス レベルを設定できます。詳しくは、「ユーザー グループ」を参照してください。	メニューから**[設定]**を選択し、**[System Management Homepage]**ボックスの**[セキュリティ]**リンクをクリックします。さらに、**[ユーザー グループ]**リンクをクリックします。

関連項目

- [設定]ページ
- コマンド ライン インターフェイス設定

[匿名/ローカル アクセス]

[匿名/ローカル]アクセスにより、次の設定を選択できます。

- **匿名アクセス**　（デフォルトは無効）。**[匿名アクセス]**を有効にすると、ユーザーはログインせずにHP SMHにアクセスできます。**[匿名]**を選択すると、任意のローカルまたはリモート ユーザーが、ユーザー名およびパスワードの入力を求められることなく、セキュリティ保護されていないページにアクセス権を持ちます。

  警告：[匿名アクセス]を使用することはおすすめできません。

- **ローカル アクセス**　（デフォルトは無効）。**[ローカル アクセス]**を有効にすると、認証を受けずにローカルでHP SMHにアクセスできます。つまり、ローカル コンソールにアクセスできる任意のユーザーが、**[管理者]**を選択することにより、フル アクセス権を獲得できます。

  警告：[ローカル アクセス]は、ユーザーの管理サーバー ソフトウェアがこのアクセスを有効にしていない限り、使用することはおすすめできません。

匿名アクセスを有効にするには、以下の手順に従ってください。

1. メニューから**[設定]**を選択します。
2. **[System Management Homepage]**ボックスで、**[セキュリティ]**リンクをクリックします。
3. **[匿名/ローカル アクセス]**リンクをクリックします。
4. **[匿名アクセス]**の下で、**[保証されていないページへの匿名のユーザー アクセスを許可します]**の横のボックスを選択します。
5. **[適用]**をクリックして設定を適用します。

匿名アクセスを無効にするには、以下の手順に従ってください。

1. メニューから**[設定]**を選択します。
2. **[System Management Homepage]**ボックスで、**[セキュリティ]**リンクをクリックします。
3. **[匿名/ローカル アクセス]**リンクをクリックします。
4. **[匿名アクセス]**の下で、**[保証されていないページへの匿名のユーザー アクセスを許可します]**の横のボックスからチェックを外します。
5. **[適用]**をクリックして設定を適用します。

ローカル アクセスを有効にするには、以下の手順に従ってください。

1. メニューから**[設定]**を選択します。
2. **[System Management Homepage]**ボックスで、**[セキュリティ]**リンクをクリックします。
3. **[匿名/ローカル アクセス]**リンクをクリックします。
4. **[ローカル アクセス]**の下で、**[System Management Homepageの自動ログインを有効にします]**の横のボックスを選択します。
5. **[匿名]**または**[管理者]**を選択します。
6. **[適用]**をクリックして設定を適用します。

ローカル アクセスを無効にするには、以下の手順に従ってください。

1. メニューから**[設定]**を選択します。
2. **[System Management Homepage]**ボックスで、**[セキュリティ]**リンクをクリックします。
3. **[匿名/ローカル アクセス]**リンクをクリックします。

4. **[ローカル アクセス]**の下で、**[System Management Homepageの自動ログインを有効にします]**の横のボックスを選択解除します。
5. **[適用]**をクリックして設定を適用します。

関連手順

- [IP バインド]
- [IP限定ログイン]
- [ローカル サーバー証明書]
- タイムアウト
- [信頼 モード]
- [信頼された管理サーバー]
- ユーザー グループ

関連項目

▲ [設定]ページ

[IP バインド]

IPバインディングは、HP SMHが要求を受け入れるIPアドレスを指定し、処理されるネットおよびサブネット要求についての制御を行います。

管理者は、**[IPバインド]**ウィンドウで指定されたアドレスだけにバインドするようにHP SMHを設定することができます。5つのサブネットIPアドレスとネットマスクを定義することができます。

サーバーのIPアドレスは、マスクの適用後に入力されたIPバインディング アドレスのいずれかに一致する場合に、バインドされます。

WindowsおよびLinux上のHP SMHは、IPv4およびIPv6アドレスの両方をサポートします。

HP-UX上のHP SMHは、現時点では、IPv4アドレスのみをサポートします。

注記: HP SMHは、常に、127.0.0.1にバインドされます。IPバインドが有効になっていて、サブネット/マスク ペアが設定されていない場合、HP SMHは、127.0.0.1に対してのみ利用可能です。IPバインディングが有効でない場合は、すべてのアドレスにバインドします。

IPバインディングを設定するには、次のように操作します。

1. メニューから**[設定]**を選択します。
2. **[System Management Homepage]**ボックスで、**[セキュリティ]**リンクをクリックします。
3. **[IPバインド]**リンクをクリックします。
4. **サブネットIPアドレス**を入力します。
5. **ネットマスク**を入力します。
6. **[追加]**をクリックして、前の手順で入力した**[サブネットIPアドレス]**および**[ネットマスク]**を追加します。

   手順4～7を繰り返して、最大5つのサブネットIPアドレスおよびネットマスクを追加することができます。
7. **[適用]**をクリックし、設定を適用します。

注記: ネットマスクは、IPv4アドレスにのみ適用可能です。

IPアドレスをリストから削除するには、以下の手順に従ってください。

1. メニューから**[設定]**を選択します。
2. **[System Management Homepage]**ボックスで、**[セキュリティ]**リンクをクリックします。
3. **[IPバインド]**リンクをクリックします。
4. 削除するIPアドレスの横のチェックボックスを選択します。

5. **[削除]**をクリックします。
6. **[適用]**をクリックし、設定を適用します。

各IPアドレスおよびネットマスクは、0～255の値を持つ4つのオクテットで構成されている必要があります（各ネットマスクについても同じです）。

ネットマスクは、最上位ビットが1で始まっており、途中まで1が続き、そこから最後までは0が続くという構成（255.255.0.0、192.0.0.0、255.192.0.0など）になっている必要があります。

関連手順

- [匿名/ローカル アクセス]
- [IP限定ログイン]
- [ローカル サーバー証明書]
- 代理名証明書
- ポート2301
- タイムアウト
- [信頼 モード]
- [信頼された管理サーバー]
- Kerberos権限手順（Windowsのみ）
- ユーザー グループ

関連項目

▲ [設定]ページ

[IP限定ログイン]

[IP限定ログイン]により、HP SMHは、サインインを試行するシステムのIPアドレスに基づいてログインアクセスを制限できます。

LinuxおよびWindowsでは、インストール時にアドレス制限を設定できます。すべてのオペレーティングシステムでは、管理者が**[IP限定ログイン]**ページからアドレス制限を設定することができます。以下に注意してください。

- IPアドレスが制限されている場合は、許可ボックスにあっても制限されます。
- IPアドレスが許可リストにある場合は、それらのIPアドレスのみサインインできます。ただし、localhostはそのかぎりではありません。
- IPアドレスが許可リストにない場合、サインイン アクセスは、制限リストにないあらゆるIPアドレスに対して許可されます。

WindowsおよびLinux上のHP SMHは、IPv4およびIPv6アドレスをサポートします。

注記: Windowsオペレーティング システムを実行しているシステムでは、IPv6アドレスの範囲は括弧があってもなくても有効です。

たとえば、Windowsオペレーティング システムを実行しているシステムでは、[2001:db8:c18:1:250:8bff:fee2:5175]-[2001:db8:c18:1:250:8bff:fee2:5180]、および2001:db8:c18:1:250:8bff:fee2:5175-2001:db8:c18:1:250:8bff:fee2:5180の両方の形式が有効です。

HP-UX上のHP SMHは、現時点では、IPv4アドレスのみをサポートします。

IPアドレスを制限するには、以下の手順に従ってください。

1. メニューから**[設定]**を選択します。
2. **[System Management Homepage]**ボックスで、**[セキュリティ]**リンクをクリックします。
3. **[IP限定ログイン]**リンクをクリックします。
4. **IPアドレス**または**IPアドレス範囲**を入力します。

   IPアドレス範囲は、必ず、範囲の下限、ハイフン、範囲の上限の順に入力してください。上限と下限の値も範囲に含まれます。

IPアドレス範囲と単独のIPアドレスは、セミコロンで区切ります。IPv4のIPアドレス範囲は、次のフォーマットで入力してください。192.168.0.1-192.168.0.255IPv6のIPアドレス範囲は、次のフォーマットで入力してください。
2001:db8:c18:1:4c7d:fa25:ccf8:d30c-2001:db8:c18:1:4c7d:fa25:ccf8:d30f

5. **[制限]**または**[許可]**ラジオ ボタンを選択します。
6. **[追加]**をクリックし、設定を追加します。
7. **[適用]**をクリックし、設定を適用します。

IPアドレスをリストから削除するには、以下の手順に従ってください。

1. メニューから**[設定]**を選択します。
2. **[System Management Homepage]**ボックスで、**[セキュリティ]**リンクをクリックします。
3. **[IP限定ログイン]**リンクをクリックします。
4. 削除するIPアドレスの横のチェックボックスを選択します。
5. **[削除]**をクリックします。
6. **[適用]**をクリックし、設定を適用します。

関連手順

- [匿名/ローカル アクセス]
- [IP バインド]
- [ローカル サーバー証明書]
- 代理名証明書
- ポート2301
- タイムアウト
- [信頼 モード]
- [信頼された管理サーバー]
- Kerberos権限手順（Windowsのみ）
- ユーザー グループ

関連項目

▲ [設定]ページ

[ローカル サーバー証明書]

[ローカル サーバー証明書]リンクにより、HPが作成した以外の証明書を使用できます。

このプロセスを使用すると、HP SMHで作成された自己署名の証明書が、認証機関（CA）が発行した証明書に置き換えられます。

- このプロセスの最初の手順は、HP SMHに**証明書リクエスト（PKCS #10）**を作成させることです。このリクエストは、自己署名の証明書に関連したオリジナルのプライベート キーを利用して、証明書リクエストのためのデータを生成します。このプロセス中、プライベート キーがサーバーからなくなることはありません。
- パブリック キー インフラストラクチャ**PKCS #10**データが作成されたら、次の手順はこのデータを認証機関に送ることです。セキュアなリクエストの送信およびセキュアな証明書の受信については企業の規定に従ってください。
- 認証機関が**PKCS #7**データを返したら、最後の手順はこのデータをHP SMHにインポートすることです。
- **PKCS #7**データがインポートされたら、オリジナルの`\hp\sslshare\cert.pem`証明書ファイル（Windows）、`/opt/hpsmh/sslshare/cert.pem`ファイル（HP-UX）、または`/opt/hp/sslshare/cert.pem`（Linux x86およびx86-64上のHP SMH 2.1.3以降の場合、`/etc/opt/hp/sslshare/cert.pem`）は、**PKCS #7**データ エンベロープからのシステムの証明書で上書きされます。新しくインポートされた証明書にも、以前の自己署名の証明書と同じプライベート キーが使用されます。このプライベート キーは、キー ファイルが存在しない場合、起動時にランダムに生成されます。

証明書を作成するには、以下の手順に従ってください。

1. メニューから**[設定]**を選択します。
2. **[System Management Homepage]**ボックスで、**[セキュリティ]**リンクをクリックします。
3. **[ローカル サーバー証明書]**リンクをクリックします。
4. **[PKCS #10データの作成]**ボックスの**[組織]**または**[組織ユニット]**フィールドのデフォルト値を、64文字以下の値に置き換えます。

   指定しない場合は、*Hewlett-Packard Company*が**[組織]**に、*Hewlett-Packard Network Management Software (SMH)*が**[組織ユニット]**に入力されます。

5. **[PKCS #10データの作成]**ボックスの**[作成]**をクリックします。

   PKCS #10証明書リクエスト データが作成され、`/opt/hpsmh/sslshare/req_cr.pem`（HP-UX）、`/etc/opt/hp/sslshare/req_cr.pem`（Linux x86およびx64）、または *systemdrive:*`\hp\sslshare\req_cr.pem`（Windows）に保存されたことを示す画面が表示されます。

6. 証明書データをコピーします。
7. **PKCS #10**証明書リクエスト データを認証機関にセキュアな方法を使用して送り、証明書リクエスト返信データを**PKCS #7**フォーマットで送ってもらうように依頼します。さらに、返信データをBase64コード化フォーマットで送ってもらうように依頼します。

   所属する組織に独自のパブリック キー インフラストラクチャ（PKI）/Certificateサーバーが設置されている場合は、**PKCS #10**データをCAのマネージャーに送り、**PKCS #7**返信データを要求します。

注記: サードパーティ証明書承認局からは、通常、料金が課せられます。

8. 証明書承認局から**PKCS #7**コード化証明書リクエスト返信データが送られてきたら、**PKCS #7**証明書リクエスト返信からこのデータコピーして、**[PKCS #7データのインポート]**ボックスの**[PKCS #7情報]**フィールドに貼り付けます。
9. **[インポート]**をクリックします。

   カスタマー作成証明書がインポートされたかどうかを示すメッセージが表示されます。

10. HP SMHを再起動します。
11. インポートされた証明書を含む管理対象システムをブラウズします。
12. ブラウザーから求められたら、証明書の表示を選択し、ブラウザーに証明書をインポートする前に、使用する署名者が署名者のリストに表示されていて、HPが署名者として表示されていないことを確認します。

    選択した証明書署名者が、証明書ファイルを**PKCS #7**データではなく、Base64コード化フォーマットで送付してきた場合は、Base64コード化ファイルをファイル名`/opt/hpsmh/sslshare/cert.pem`（HP-UX）、`/etc/opt/hp/sslshare/cert.pem`（Linux x86およびx64）、または *systemdrive*`:\hp\sslshare\cert.pem`（Windows）にコピーして、HP SMHを再起動してください。

関連手順

- [匿名/ローカル アクセス]
- [IP バインド]
- [IP限定ログイン]
- タイムアウト
- [信頼 モード]
- [信頼された管理サーバー]
- ユーザー グループ

関連項目

▲ [設定]ページ

代理名証明書

HP SMHでは、HPが作成した以外の証明書をマルチホームまたは複数の名前に設定できます。この機能により、SMHの証明書は利用可能なネットワークの別名やIPなどのマシンの詳細情報を含めることができます。同じようにして、認証機関（CA）で承認された要求を作成することができます。

別名として、2種類の値が可能です。

- DNS名（Linux、Linux.localdomainなど）
- IPアドレス（10.16.165.1;192.168.1.189など）

Administratorユーザー グループ内のユーザーおよびシステム管理者 (Linuxではroot、WindowsではAdministrator）のみがブラウザーから**[代理名]**フィールドを編集することができます。

マルチホーム の設定は、以下の手順に従ってください。

ここでの**代理名**に対する変更は、現在の証明書にのみ影響を与えます。

1. メニューから**[設定]**を選択します。
2. **[System Management Homepage]**ボックスで、**[セキュリティ]**リンクをクリックします。
3. **[ローカル サーバー証明書]**リンクをクリックします。
4. **[現在の証明書]**ボックスで、**[代理名]**フィールドに値を入力します。
5. **[作成]**をクリックします。
6. **[はい]**をクリックします。前の画面が現れ、次のメッセージが表示されます。**成功： 値の変更は成功しました**

この場合、新しい認証情報と別名のセットがブラウザーでネゴシエートされます。

関連手順

- [匿名/ローカル アクセス]
- [IP バインド]
- [IP限定ログイン]
- [ローカル サーバー証明書]
- ポート2301
- タイムアウト
- [信頼 モード]
- [信頼された管理サーバー]
- Kerberos権限手順（Windowsのみ）
- ユーザー グループ

関連項目

▲ [設定]ページ

ポート2301

[ポート2301]リンクは、**ポート2301**を有効にしたり無効にしたりすることができます。デフォルト値は有効で、HP Webベース システム マネジメント ソフトウェアとの互換性を維持しています。

ポート2301を有効または無効にするには、以下の手順に従ってください。

1. メニューから**[設定]**を選択します。
2. **[System Management Homepage]**ボックスで、**[セキュリティ]**リンクをクリックします。
3. **[ポート2301]**リンクをクリックします。

4. **[設定ボックス]**で、**[ポート2301を有効]**をチェックをオンにし、ポート2301を有効にするか、チェックを削除してポート2301を**無効**にします。
5. **[適用]**をクリックします。

関連手順

- [匿名/ローカル アクセス]
- [IP バインド]
- [IP限定ログイン]
- [ローカル サーバー証明書]
- 代理名証明書
- タイムアウト
- [信頼 モード]
- [信頼された管理サーバー]
- Kerberos権限手順（Windowsのみ）
- ユーザー グループ

関連項目

▲ [設定]ページ

タイムアウト

[タイムアウト]リンクは、**[セッション タイムアウト]**および**[UIタイムアウト]**の値を設定するオプションを提供します。

- **[セッション タイムアウト]**値は、SMHセッションでユーザーが非アクティブのままいることのできる分数を示します。ユーザーがログインして、**[セッション タイムアウト]**に指定した時間よりも長く非アクティブのままでいると、ユーザーはユーザー インターフェイスの次のやり取りで、**[サイン イン]**ページにリダイレクトされます。
- **[UIタイムアウト]**値は、SMHユーザー インターフェイス（UI）がWebアプリケーションから要求されるデータを待機する秒数を示します。管理者アクセス権限のあるユーザーは、**[セッション タイムアウト]**を1～60分に設定することができます。デフォルト値は、15分です。管理者アクセス権限のあるユーザーは、**[UIタイムアウト]**を10～3600秒に設定することができます。デフォルト値は、20秒です。

[ユーザー初期設定カテゴリ]で**[Session never expires]**チェックボックスを選択すると、3分ごとにバックグラウンドでリクエストを送信することで、HP SMHセッションがタイムアウトするのを防ぐことができます。このオプションを選択すると、HP SMHサービスがタイムアウトすることも防ぐことができます。詳しくは、「ユーザー初期設定」を参照してください。

注記: [セッション期限なし]オプションは、HP-UXシステムのみで使用可能です。

次の表は、タイムアウトに使用可能な値の範囲をそれぞれの単位で示します。

表 5-6 タイムアウト設定

タイムアウト	範囲
[セッション タイムアウト]	1～60分（WindowsおよびLinux） 6～120分（HP-UX）
[UIタイムアウト]	10～3600秒

セッション タイムアウト

セッション タイムアウトの値を変更するには、以下の手順に従ってください。

1. メニューから**[設定]**を選択します。
2. **[System Management Homepage]**ボックスで、**[セキュリティ]**リンクをクリックします。

3. **[タイムアウト]**リンクをクリックします。
4. **[セッション タイムアウト (分)]**テキストボックスで、WindowsおよびLinuxの場合では、1～60分の値を入力します。

   HP-UXの場合では、6～120分の値を入力します。
5. **[適用]**をクリックします。

UIタイムアウト

UIタイムアウトの値を変更するには、以下の手順に従ってください。

1. メニューから**[設定]**を選択します。
2. **[System Management Homepage]**ボックスで、**[セキュリティ]**リンクをクリックします。
3. **[タイムアウト]**リンクをクリックします。
4. **[UIタイムアウト（秒）]**テキストボックスで、10～3600秒の値を入力します。
5. **[適用]**をクリックします。

関連手順

- [匿名/ローカル アクセス]
- [IP バインド]
- [IP限定ログイン]
- [ローカル サーバー証明書]
- 代理名証明書
- ポート2301
- [信頼 モード]
- [信頼された管理サーバー]
- Kerberos権限手順（Windowsのみ）
- ユーザー グループ

関連項目

▲ [設定]ページ

[信頼 モード]

[信頼モード]リンクは、ご使用のシステムに必要なセキュリティを選択することができます。他よりも高レベルのセキュリティが必要になる場合があります。したがって、以下のセキュリティ オプションが与えられています。

- **証明書による信頼**　信頼済み証明書を持つHP SIMサーバーからの設定変更だけを受け入れるようにHP SMHを設定できます。このモードでは、証明書による認証を提供する、提出されたサーバーが必要です。このモードは最もセキュリティの高い方法になります。証明書のデータを必要とし、デジタル署名を確認してからアクセスを許可するからです。リモートでの設定変更を可能にしたくない場合は、**[証明書による信頼]**を選択したままにし、さらにいずれの証明書もインポートしないようにして信頼システムのリストを空のままにしておきます。

  これは、Linux Itaniumのデフォルトの動作です。

  このオプションはより安全であるため、このオプションを使用することをおすすめします。
- **名前による信頼**　**[名前による信頼]**フィールドで指定された名前のHP SIMサーバーからの設定変更だけを受け入れるようにHP SMHを設定できます。たとえば、2つの部門に2つの管理者グループがある安全なネットワークの場合にこのオプションを使用できます。これにより、あるグループが

間違ったシステムにソフトウェアをインストールすることを防止できます。このオプションは、指定したHP SIMサーバーだけを確認します。

他のオプションより安全であるため、**証明書による信頼**オプションを使用することを強くおすすめします。

- **すべて信頼**　システムからの特定の設定変更も受け入れるようにHP SMHを設定できます。[すべて信頼]モードを設定する状況の例としては、セキュリティ保護されたネットワーク上にあって、ネットワーク内の全員が信頼関係を結んでいる場合が挙げられます。

  他のオプションより安全であるため、**証明書による信頼**オプションを使用することを強くおすすめします。

信頼モードの設定

HP-UX環境の場合、インポートされたHP SMH証明書は、`/opt/hpsmh/certs`ディレクトリに保存されます。

Linux環境の場合、インポートされたHP SMH証明書は、`/opt/hp/hpsmh/certs`ディレクトリに保存されます。

Windows環境の場合、インポートされたHP SIM証明書は、*システムドライブ*`\hp\hpsmh\certs`ディレクトリに保存されます。

このディレクトリにアクセスするには管理者権限を持っている必要があります。

証明書によって信頼するには、次のように操作します。

1. メニューから**[設定]**を選択します。
2. **[System Management Homepage]**ボックスで、**[セキュリティ]**リンクをクリックします。
3. **[信頼モード]**リンクをクリックします。
4. **[セキュアな信頼モード]**ボックスで、**[証明書による信頼]**ラジオ ボタンをクリックします。

   このオプションを選択すると、**信頼証明書**を使用してHP SIMが署名した**セキュリティ タスク実行**および**シングル ログイン リクエスト**要求を受け入れるようにHP SMHを設定します。
5. **[適用]**をクリックします。

名前によって信頼するには、次のように操作します。

1. メニューから**[設定]**を選択します。
2. **[System Management Homepage]**ボックスで、**[セキュリティ]**リンクをクリックします。
3. **[信頼モード]**リンクをクリックします。
4. **[その他の信頼モード]**ボックスで、**[名前による信頼]**ラジオ ボタンをクリックします。
5. **[サーバー証明書名]**テキストボックスに、サーバー証明書名を入力します。
6. **[追加]**をクリックします。

   [追加]をクリックすると、**サーバー証明書名**が次の条件を満たすかどうかが確認されます。

   - 各HP SIMサーバーの証明書名は64文字未満でなければならない
   - 次の無効な文字が含まれていない：~ ' ! @ # $ % ^ & * ( ) + = / " : ' < > ? , |
   - サーバー証明書名がリストに存在しない

   検証テストによって値が受け入れられると、**サーバー証明書名**がリスト テーブルの新しい行として追加されます。手順5～6を行うことで、最大5つの**サーバー証明書名**を追加することができます。5つより多くの証明書名を入力すると、`No more names can be added`というアラートが表示されます。
7. **[適用]**をクリックして設定を保存します。

   このオプションを選択すると、一覧の名前のサーバーにあるHP SIMからの**セキュア タスク実行**および**シングル サインオン**要求のみを受け入れるようにHP SMHが設定されます。

サーバー証明書名をリストから削除するには、以下の手順に従ってください。

1. メニューから**[設定]**を選択します。
2. **[System Management Homepage]**ボックスで、**[セキュリティ]**リンクをクリックします。
3. **[信頼モード]**リンクをクリックします。

4. **[その他の信頼モード]**ボックスで、削除する**サーバー証明書名**を確認し、その名前の横のチェックボックスをクリックします。
5. **[削除]**をクリックします。
6. **[適用]**をクリックします。

すべてのサーバーを信頼するには、次のように操作します。

1. メニューから**[設定]**を選択します。
2. **[System Management Homepage]**ボックスで、**[セキュリティ]**リンクをクリックします。
3. **[信頼モード]**リンクをクリックします。
4. **[その他の信頼モード]**ボックスで、**[すべての信頼]**ボタンをクリックします。
5. **[適用]**をクリックします。

   [すべての信頼]オプションを選択すると、任意のHP SIMサーバーからの**セキュア タスク実行**および**シングル サインオン**要求を受け入れるようにHP SMHが設定されます。

関連手順

- [匿名/ローカル アクセス]
- [IP バインド]
- [IP限定ログイン]
- [ローカル サーバー証明書]
- 代理名証明書
- ポート2301
- タイムアウト
- [信頼された管理サーバー]
- Kerberos権限手順（Windowsのみ）
- ユーザー グループ

関連項目

▲ [設定]ページ

[信頼された管理サーバー]

証明書は、HP SIMまたはInsightマネージャー7とHP SMHとの信頼関係を確立します。**[信頼済みマネジメント サーバー]**リンクにより、**信頼済み証明書リスト**内の証明書を管理できます。以下に注意してください。

- **[証明書データのインポート]**　証明書は、HP SIMとHP SMHの間の信頼関係を確立します。
- **[サーバーから証明書の追加]**　HP SIMサーバーから信頼済み証明書を追加できます。

証明書を信頼済み証明書リストに追加するには、以下の手順に従ってください。

1. メニューから**[設定]**を選択します。
2. **[System Management Homepage]**ボックスで、**[セキュリティ]**リンクをクリックします。
3. **[信頼済みマネジメント サーバー]**リンクをクリックします。
4. **[証明書の追加]**領域で、**[証明書データのインポート]**ラジオ ボタンをクリックします。
5. Base64コード化証明書をテキストボックスにコピーして貼り付けます。
6. **[インポート]**をクリックします。

サーバーから証明書を追加するには、以下の手順に従ってください。

1. メニューから**[設定]**を選択します。
2. **[System Management Homepage]**ボックスで、**[セキュリティ]**リンクをクリックします。
3. **[信頼済みマネジメント サーバー]**リンクをクリックします。
4. **[証明書情報の入手]**領域で、**[証明書情報の入手]**ラジオボタンをクリックします。

5. **[サーバー名]**テキストボックスに、HP SIMサーバーのIPアドレスまたはサーバー名を入力します。
6. **[追加]**をクリックします。

関連手順

- [匿名/ローカル アクセス]
- [IP バインド]
- [IP限定ログイン]
- [ローカル サーバー証明書]
- タイムアウト
- [信頼 モード]
- ユーザー グループ

関連項目

▲ [設定]ページ

Kerberos権限手順（Windowsのみ）

ユーザーが**Kerberos**領域でのサービスを認証する場合は、一連の手順を行って認証を実行する必要があります。クライアント（ユーザーのマシン）は、Kerberosサーバーから証明書を入手する必要があります。サーバーは、Authentication Server（AS）およびTicket Granting Server（TGS）です。

ASおよびTGSは、同じマシン上に存在し、Key Distribution Center（KDC）といわれます。

Kerberos認証手順

Kerberos領域でユーザーが安全なサービスにアクセスするプロセスの概要は、次のとおりです。

このプロセスは、初期状態でユーザーが**Kerberos**領域にログインしてKerberosで保護されたサービスに最初にアクセスをしようとするときにのみ発生します。

1. ユーザーは、ドメインのユーザー名およびパスワードを使用してシステム（クライアント）にログインします。
2. ユーザーのパスワードはハッシュされ、このハッシュがユーザーの秘密鍵になります。
3. ユーザーがサービスへのアクセスを試みると、メッセージが、ユーザーがそのサービスにアクセスしようとしていることをASに伝えます。
4. ユーザーがASデータベース内にある場合は、クライアントに2つのメッセージが返されます。
   a. クライアント/TGSセッション キーはユーザーの秘密鍵によって暗号化され、TGSとの通信で使用されます。
   b. Ticket-Granting Ticket（TGT）は、TGSの秘密鍵によって暗号化されます。**チケット**は、個人識別のために**Kerberos**で使用されます。TGTによって、クライアントは、ネットワーク サービスと通信するためのその他のチケットを入手できます。
5. これらの2つのメッセージを受信したら、クライアントは、クライアント/TGSセッション キーの含まれるメッセージを復号します。

次のプロセスは、ユーザーがサービスを認証しようとするたびに発生します。

1. ユーザーがサービスを要求すると、クライアントはTGSに次の2つのメッセージを送信します。
   - TGTおよび要求されたサービスからなるメッセージ
   - 認証符号。受信済みのクライアント/TGSセッション キーによって暗号化されたクライアントのIDと現在のタイムスタンプから構成されます。

   タイムスタンプは、**Kerberos**で、複製攻撃を回避するために使用されます。マシン間のクロック スキューは、特定の限度を超えることができません。
2. TGSは認証符号を復号し、クライアントに次の2つのメッセージを返します。
   - TGSから受信したクライアント-サーバー チケット
   - 別の認証符号。クライアント/サーバー セッション キーによって暗号化されたクライアントのIDと現在のタイムスタンプから構成されます。

3. サービスは、クライアント-サーバー チケットをそれ自体の秘密鍵によって復号し、識別のために、受信したタイムスタンプに1を足したタイムスタンプで、メッセージをクライアントに送信します。このメッセージは、クライアント/サーバー セッション キーで暗号化されます。
4. クライアントは、メッセージを復号し、タイムスタンプを確認します。正しければ、サービスに要求を発行することができ、想定どおりに応答が返されます。

HP SMH Kerberos**認証**

HP SMHは、**Kerberos** シングル サインオン（SSO）を提供します。これによって、**Kerberos**領域のユーザーが**[サイン イン]**ページにユーザー名およびパスワードを入力することなくログインすることができます。許可されたユーザーがHP SMHにアクセスし、有効な**Kerberos**証明書を持っている場合は、**ホーム**ページがHP SMH内に表示されます。

Kerberos認証は、HP SMH内の特別な`URL /proxy/Kerberos`を使用して行われます。このURLにアクセスすることで、SMHは要求内に**Kerberos**証明書を検索し、ユーザー認証を実行します。

ユーザーが有効な**Kerberos**証明書を持っていない場合、または認証プロセス中にエラーが発生した場合は、**[サイン イン]**ページが表示され、エラー メッセージが表示されます。たとえば、認証に関わるマシン間のクロック スキューが大きすぎる場合は、エラー メッセージが表示され、**[サイン イン]**ページに移動されます。

Kerberos認証は、次のローカル アクセス状況では動作しません。

- KDC（AD）がインストールされたマシンからHP SMHにアクセスする
- HP SMHがインストールされたマシンからHP SMHにアクセスする

認証エラーが発生すると、システム管理者は、SMH HTTPサーバー エラー ログを確認してエラーについての情報を入手する必要があります。

たとえば、マシン間のクロック スキューが大きすぎる場合は、次のログ メッセージが書き込まれます。

```
Thu Jun 25 16:55:09 2009] [error] client 2001:db8:c18:1:b8ca:fcdf:d49d:b5c6]
mod_spnego: Kerberos SSO (QueryContextAttributes) failed;SSPI: The function
requested is not supported\r\n(-2146893054).
```

以下のレベルのユーザー権限を利用できます。

- **管理者　[管理者]**アクセス権を持つユーザーは、HP SMHによって提供されるすべての情報を表示できます。該当するデフォルトのユーザー グループ（Windowsオペレーティング システムでは[administrators]、HP-UXおよびLinuxではroot）は、常に、管理者アクセス権を持ちます。
- **オペレーター　[オペレーター]**アクセス権を持つユーザーは、HP SMHによって提供されるほとんどの情報を表示し、設定することができます。一部のWebアプリケーションでは、最も重要な情報へのアクセスが[管理者]のみに制限されています。
- **ユーザー　[ユーザー]**アクセス権を持つユーザーは、HP SMHによって提供されるほとんどの情報を表示できます。一部のWebアプリケーションでは、重要な情報の表示が、**[ユーザー]**アクセス権を持つユーザーに対して制限されています。

Kerberosを有効化または無効化したり、許可された**Kerberos**グループ リストにグループを追加したりするには、アクセスのレベルごとに以下の手順を行います。

Kerberosのサポートは、ユーザーごとに提供されます。

Kerberos**管理者**

Kerberos管理者を追加するには、以下の手順に従ってください。

1. メニューから**[設定]**を選択します。
2. **[System Management Homepage]**ボックスで、**[セキュリティ]**リンクをクリックします。
3. **[Kerberos認証]**リンクをクリックします。
4. **[Kerberos設定]**領域で、**[Kerberosサポートの有効]**の横のボックスを選択します。
5. **[グループ名]**テキストボックスに、*group@REALM*フォーマットまたは*REALM\group*で名前を入力します。

   英数字およびアンダースコアのみが使用できます。~ ' ! # $ % ^ & * ( ) + = / " : ' < > ? , | ;などの特殊文字は使用できません。

6. **[タイプ]**の横の**[管理者]**ラジオ ボタンをクリックします。
7. **[追加]**をクリックします。入力した値は、リスト テーブルの新しい行として追加されます。

   手順5～7を繰り返して、続けて管理者アクセス権を持つグループを追加することができます。
8. **[適用]**をクリックします。

Kerberos管理者を削除するには、以下の手順に従ってください。

1. メニューから**[設定]**を選択します。
2. **[System Management Homepage]**ボックスで、**[セキュリティ]**リンクをクリックします。
3. **[Kerberos認証]**リンクをクリックします。
4. HP SMHから削除するダイナミック リストで、**[グループ名]**の横のチェックボックスをクリックします。
5. **[削除]**をクリックします。
6. **[適用]**をクリックします。

Kerberosオペレーター

Kerberosオペレーターを追加するには、以下の手順に従ってください。

1. メニューから**[設定]**を選択します。
2. **[System Management Homepage]**ボックスで、**[セキュリティ]**リンクをクリックします。
3. **[Kerberos認証]**リンクをクリックします。
4. **[Kerberos設定]**領域で、**[Kerberosサポートの有効]**の横のボックスを選択します。
5. **[グループ名]**テキストボックスに、*group@REALM*フォーマットまたは*REALM\groupname*で名前を入力します。

   英数字およびアンダースコアのみが使用できます。~ ' ! # $ % ^ & * ( ) + = / " : ' < > ? , | ;などの特殊文字は使用できません。
6. **[タイプ]**の横の**[オペレーター]**ラジオ ボタンをクリックします。
7. **[追加]**をクリックします。入力した値は、リスト テーブルの新しい行として追加されます。

   手順5～7を繰り返して、続けてオペレーター アクセス権を持つグループを追加することができます。
8. **[適用]**をクリックします。

Kerberosオペレーターを削除するには、以下の手順に従ってください。

1. メニューから**[設定]**を選択します。
2. **[System Management Homepage]**ボックスで、**[セキュリティ]**リンクをクリックします。
3. **[Kerberos認証]**リンクをクリックします。
4. HP SMHから削除するダイナミック リストで、**[グループ名]**の横のチェックボックスを選択します。
5. **[削除]**をクリックします。
6. **[適用]**をクリックします。

Kerberosユーザー

Kerberosユーザーを追加するには、以下の手順に従ってください。

1. メニューから**[設定]**を選択します。
2. **[System Management Homepage]**ボックスで、**[セキュリティ]**リンクをクリックします。
3. **[Kerberos認証]**リンクをクリックします。
4. **[Kerberos設定]**領域で、**[Kerberosサポートの有効]**の横のボックスを選択します。
5. **[グループ名]**テキストボックスに、*group@REALM*フォーマットまたは*REALM\groupname*で名前を入力します。

   英数字およびアンダースコアのみが使用できます。~ ' ! # $ % ^ & * ( ) + = / " : ' < > ? , | ;などの特殊文字は使用できません。
6. **[タイプ]**の横の**[ユーザー]**ラジオ ボタンをクリックします。

7. **[追加]**をクリックします。入力した値は、リスト テーブルの新しい行として追加されます。
   手順5～7を繰り返して、続けてユーザー アクセス権を持つグループを追加することができます。
8. **[適用]**をクリックします。

Kerberosユーザーを削除するには、以下の手順に従ってください。

1. メニューから**[設定]**を選択します。
2. **[System Management Homepage]**ボックスで、**[セキュリティ]**リンクをクリックします。
3. **[Kerberos認証]**リンクをクリックします。
4. HP SMHから削除するダイナミック リストで、**[グループ名]**の横のチェックボックスを選択します。
5. **[削除]**をクリックします。
6. **[適用]**をクリックします。

関連手順

- [匿名/ローカル アクセス]
- [IP バインド]
- [IP限定ログイン]
- [ローカル サーバー証明書]
- 代理名証明書
- ポート2301
- タイムアウト
- [信頼 モード]
- [信頼された管理サーバー]
- ユーザー グループ

関連項目

▲ [設定]ページ

ユーザー グループ

HP SMHでは、認証にオペレーティング システム アカウントが使用され、オペレーティング システム アカウント グループ レベルでオペレーティング システム アカウントのアクセス レベルを管理することができます。

オペレーティング システム グループの**[管理者]**（Windows）またはオペレーティング システム グループの**[root]**（LinuxおよびHP-UX）（デフォルトでユーザーrootに含まれている）のユーザーは、**[管理者]**、**[オペレーター]**、または**[ユーザー]**のHP SMHアクセス レベルに対応するオペレーティング システム グループを定義できます。オペレーティング システム グループを追加すると、オペレーティング システムの管理者は、オペレーティング システムのユーザーをこれらのオペレーティング システム グループに追加できます。

HP SMHの各アクセス レベルは、最大5つのオペレーティング システム グループに割り当てることができます。HP SMHのインストールによって、オペレーティング システムをHP SMHに割り当てることができます。HP SMHでは、指定されたオペレーティング システム グループがオペレーティング システムに定義されていない場合はオペレーティング システムを追加することができません。

HP SMHに使用されるアカウントは、ホスト オペレーティング システムで上位アクセスを持つ必要はありません。管理HP SMHユーザーは、HP SMHの各アクセス レベルに対するオペレーティング システム ユーザー グループを指定することができます。その結果、各オペレーティング システム グループのすべてのアカウントが**[ユーザー グループ]**ウィンドウで指定されたHP SMHにアクセスできるようになります。

注記: すべてのユーザー グループは、HP System Management Homepageホスト システムに存在しなければなりません。

Windowsの管理者グループ、Linuxのルート グループ、およびHP-UXのルート グループには、HP SMHへの管理者アクセス権が割り当てられます。HP-UXでは、ルート ユーザーのみが管理者クラスに割り当てられます。ルート グループのすべてのユーザーが割り当てられるわけではありません。

たとえば、HP SMHの管理者アクセス レベルを、ユーザーが作成したオペレーティング システム グループのAdmin1、Admin2、およびAdmin3に割り当てることができます。このオペレーティング システム グループ（Admin1、Admin2、またはAdmin3）のメンバーになっているすべてのユーザーには、そのアカウントがホスト オペレーティング システムで上位アカウントを持っている場合でも、持っていない場合でも、HP SMHに対する管理者権限が付与されます。

[ユーザー グループ]ページにより、ユーザー グループをHP SMHに追加できます。以下のレベルのユーザー グループ権限を利用できます。

- **管理者** **[管理者]**アクセス権を持つユーザーは、HP SMHによって提供されるすべての情報を表示できます。デフォルトのユーザー グループ（Windowsオペレーティング システムでは **[administrators]**、HP-UXおよびLinuxでは**root**）は、常に、管理者アクセス権を持ちます。
- **オペレーター** **[オペレーター]**アクセス権を持つユーザーは、HP SMHによって提供されるほとんどの情報を表示し、設定することができます。一部のWebアプリケーションでは、最も重要な情報へのアクセスが[管理者]のみに制限されています。
- **ユーザー** **[ユーザー]**アクセス権を持つユーザーは、HP SMHによって提供されるほとんどの情報を表示できます。一部のWebアプリケーションでは、重要な情報の表示が、**[ユーザー]**アクセス権を持つユーザーに対して制限されています。

管理者グループ

管理者グループを追加するには、以下の手順に従ってください。

1. メニューから**[設定]**を選択します。
2. **[System Management Homepage]**ボックスで、**[セキュリティ]**リンクをクリックします。
3. **[ユーザー グループ]**リンクをクリックします。
4. **[グループ]**領域で、**[グループ名]**テキストボックスにグループの名前を入力します。

   すべてのユーザー グループは、HP System Management Homepageホスト システムに存在しなければなりません。

   英数字およびアンダースコアのみが使用できます。~ ' ! @ # $ % ^ & * ( ) + = / " : ' < > ? , | ;などの特殊文字は使用できません。
5. **[タイプ]**の横の**[管理者]**ラジオ ボタンをクリックします。
6. **[追加]**をクリックします。入力した値は、リスト テーブルの新しい行として追加されます。

   手順4～6を繰り返して、最大5つの**管理者グループ**を続けて追加することができます。
7. SMHに追加するダイナミック リストで、**[グループ名]**の横のチェックボックスを選択します。
8. **[適用]**をクリックします。

管理者グループを削除するには、以下の手順に従ってください。

1. メニューから**[設定]**を選択します。
2. **[System Management Homepage]**ボックスで、**[セキュリティ]**リンクをクリックします。
3. **[ユーザー グループ]**リンクをクリックします。
4. SMHから削除するダイナミック リストで、**[グループ名]**の横のチェック ボックスを選択します。
5. **[適用]**をクリックします。

オペレーター グループ

オペレーター グループを追加するには、以下の手順に従ってください。

1. メニューから**[設定]**を選択します。
2. **[System Management Homepage]**ボックスで、**[セキュリティ]**リンクをクリックします。

3. **[ユーザー グループ]**リンクをクリックします。
4. **[グループ]**領域で、**[グループ名]**テキストボックスにグループの名前を入力します。

   すべてのユーザー グループは、HP System Management Homepageホスト システムに存在しなければなりません。

   英数字およびアンダースコアのみが使用できます。~ ' ! @ # $ % ^ & * ( ) + = / " : ' < > ? , | ;などの特殊文字は使用できません。
5. **[タイプ]**の横の**[オペレーター]**ラジオ ボタンをクリックします。
6. **[追加]**をクリックします。入力した値は、リスト テーブルの新しい行として追加されます。

   手順4～6を繰り返して、最大5つの**オペレーター グループ**を続けて追加することができます。
7. SMHに追加するダイナミック リストで、**[グループ名]**の横のチェックボックスを選択します。
8. **[適用]**をクリックします。

オペレーター グループを削除するには、以下の手順に従ってください。

1. メニューから**[設定]**を選択します。
2. **[System Management Homepage]**ボックスで、**[セキュリティ]**リンクをクリックします。
3. **[ユーザー グループ]**リンクをクリックします。
4. SMHから削除するダイナミック リストで、**[グループ名]**の横のチェック ボックスを選択します。
5. **[適用]**をクリックします。

ユーザー グループ

ユーザー グループを追加するには、以下の手順に従ってください。

1. メニューから**[設定]**を選択します。
2. **[System Management Homepage]**ボックスで、**[セキュリティ]**リンクをクリックします。
3. **[ユーザー グループ]**リンクをクリックします。
4. **[グループ]**領域で、**[グループ名]**テキストボックスにグループの名前を入力します。

   すべてのユーザー グループは、HP System Management Homepageホスト システムに存在しなければなりません。

   英数字およびアンダースコアのみが使用できます。~ ' ! @ # $ % ^ & * ( ) + = / " : ' < > ? , | ;などの特殊文字は使用できません。
5. **[タイプ]**の横の**[ユーザー]**ラジオ ボタンを選択します。
6. **[追加]**をクリックします。入力した値は、リスト テーブルの新しい行として追加されます。

   手順4～6を繰り返して、最大5つの**ユーザー グループ**を続けて追加することができます。
7. SMHに追加するダイナミック リストで、**[グループ名]**の横のチェックボックスを選択します。
8. **[適用]**をクリックします。

ユーザー グループを削除するには、以下の手順に従ってください。

1. メニューから**[設定]**を選択します。
2. **[System Management Homepage]**ボックスで、**[セキュリティ]**リンクをクリックします。
3. **[ユーザー グループ]**リンクをクリックします。
4. SMHから削除するダイナミック リストで、**[グループ名]**の横のチェック ボックスを選択します。
5. **[適用]**をクリックします。

関連手順

- [匿名/ローカル アクセス]
- [IP バインド]
- [IP限定ログイン]
- [ローカル サーバー証明書]
- 代理名証明書
- ポート2301
- タイムアウト

- [信頼 モード]
- [信頼された管理サーバー]
- Kerberos権限手順（Windowsのみ）

関連項目

▲ [設定]ページ

第6章 [タスク]ページ

[タスク]ページには、参加しているHP Webベース システム マネジメント ソフトウェアから提供されるルーチン タスクへのリンクが表示されます

HP Webベース システム マネジメント ソフトウェアがタスクを提供しない場合、**[タスク]**ページは表示されません。

関連項目

- 開始するには
- [ホーム]ページ
- [設定]ページ
- [タスク]ページ
- [ログ]ページ
- [Webアプリケーション]ページ
- [サポート]ページ
- [ヘルプ]ページ

第7章 [ログ]ページ

少なくとも、**[ログ]**ページは次のログ カテゴリを提供します。

- System Management Homepageログ
- Httpdエラー ログ（WindowsおよびLinux）
- System Management Homepageエラー ログ（HP-UX）

インストールされているHP Webベース システム マネジメント ソフトウェアのログは、このページに表示できます。たとえば、HPバージョン コントロール エージェントがインストールされている場合、バージョン コントロール エージェントログへのリンクが、**[ログ]**ページに表示されます。別の例として、Distributed Systems Administration Utilities（DSAU）がインストールされている場合、System Log Viewerへのリンクが、**[ログ]**ページに表示されます。各ログファイルは、合計40のログ エントリーを1ページに表示する複数のページに分割されます。

注記: このインストールでは、WindowsおよびLinuxの場合、古いsmh.logファイルが、人間の読める英語のみのログとして予備に保管されます。ユーザー インターフェイスからは使用できません。古いログを読むには、ファイルに直接アクセスしてください。新しいログ メッセージは、このファイルに書き込まれません。

`smh_enc.log`（`Windows`**および**`Linux`）および`smh.log`（`HP-UX`）には、次のフォーマットのコード化されたエントリーが含まれます。

表 7-1 ログのコード化されたエントリー

タイプ	説明
深刻度	記録されたイベントの深刻度。深刻度は、次のとおりです。 • 情報（5） • 警告（6） • マイナー（3） • メジャー（4） • クリティカル（8）
タイムスタンプ	イベントの発生した時刻。UTC1970年1月1日00時00分00秒からの秒数で表されます。
ID	ログ メッセージID。翻訳されたログ メッセージを特定するために使用します。
引数	%sや%dなどの引数変換修飾子を使用するログ メッセージでprintf()によって使用される引数。

デフォルトのログの位置

表 7-2 デフォルトのログの位置

位置	説明
`C:\hp\hpsmh\logs`	Windowシステムでのデフォルトのログの位置（すべてのログ）です。
`/var/spool/opt/hp/hpsmh/logs/`	Linuxシステムでのデフォルトのログの位置（エラー ログとアクセス ログ）です。
`/opt/hp/hpsmh/logs`	Linuxシステムでのデフォルトのログの位置（SMHログ）です。

ログの位置の変更

注記: ログの位置を変更できるのは、アクセス ログとエラー ログのみです。

1. コマンド`smhconfig -O "new log location"`を入力します。
   新しいログ ディレクトリが作成されます。
2. コマンド`smhconfig -r`を入力します。
   SMHアプリケーションが再起動します。

関連手順

- System Management Homepageログ
- Httpdエラー ログ

関連項目

- [ホーム]ページ
- [設定]ページ
- [タスク]ページ
- [Webアプリケーション]ページ

System Management Homepageログ

[System Management Homepageログ]には、HP System Management Homepage（HP SMH）の設定変更とサインインの成功や失敗も含まれます。HP SMHに直接、またはHP Systems Insight Manager（HP SIM）からサインインするときの、サインインやアクセスの問題時のトラブルシューティングに役立ちます。

[System Management Homepageログ]にアクセスするには、HP SMHに対する管理者アクセス権が必要です。

HP SMHログにアクセスするには、メニューから **[ログ]** にアクセスし、**[System Management Homepage]** ボックスの**[System Management Homepageログ]**リンクをクリックします。

関連項目

- [ログ]ページ
- Httpdエラー ログ

Httpdエラー ログ

[Httpd Errorログ]には、HP SMHモジュール、Kerberos設定エラー、およびCGI実行エラー（`httpd`）で生成されたエラー情報が含まれます。これは、サーバーの起動またはサーバーの操作で問題が発生したときに最初に確認する場所です。なぜなら、ログには問題の経過と解決方法の障害が記録されていることが多いからです。

[Httpd Errorログ]は、HP-UXではそのまま利用できますが、`smhpd.xml`ファイルにある*`httpd-error-log`*タグを追加することによって、WindowsおよびLinuxで認識することはできます。

[Httpd Errorログ]にアクセスするには、HP SMHに対する管理者アクセス権が必要です。

HP SMH 3.x以降では、`smhconfig`ツールを次のように使用して、`httpd`エラー ログをHP SMHユーザーインターフェイスに表示することができます。

エラー ログの表示を有効にするには、以下のようにしてください。

```
smhconfig -p or --httpd-error-log True
```

エラー ログの表示を無効にするには、以下のようにしてください。

```
smhconfig -p or --httpd-error-log False
```

新しい設定を適用するには、HP SMHを再起動する必要があります。

HP SMHサービスを再起動するには、以下のようにしてください。

```
smhconfig -r
```

Httpdエラー ログにアクセスするには、以下のようにしてください。

メニューから **[ログ]** を選択し、**[System Management Homepage]**ボックスの**[Httpd Errorログ]**リンクをクリックします。

関連項目

- [ログ]ページ
- System Management Homepageログ

サポートされる言語

HP SMHは、サポートされている言語用の翻訳済み文字列が含まれるPHPファイルを保持しています。サポートされる言語ごとに、`data/htocs/`*`lang`*`/`ディレクトリに`log_messages.php`という名前のファイルがあります。ここで、*`lang`*は、言語に対する2文字のサフィックスです。`log_messages.php` ファイルには、翻訳済みメッセージ文字列の配列と、翻訳済み深刻度の配列が含まれています。

次の表に、SMHのサポートする言語のロケール名を示します。

表 7-3 サポートされる言語のロケール名

言語	Linuxロケール名	Windowsロケール名
英語	en_US.UTF-8	english
日本語	ja_JP.UTF-8	japanese
ドイツ語	de_DE.UTF-8	german
スペイン語	es_ES.UTF-8	spanish
フランス語	fr_FR.UTF-8	french
イタリア語	it_IT.UTF-8	italian
韓国語	ko_KR.UTF-8	korean
簡体字中国語	zh_CN.UTF-8	chinese-simplified
繁体字中国語	zh_TW.UTF-8	chinese-traditional

次の表には、サポートされる各言語に基づいた、`log_messages.php`ページのサフィックスを示します。

表 7-4 サポートされる言語のサフィックス

言語	サフィックス
英語	en
日本語	ja
ドイツ語	de
スペイン語	es
フランス語	fr
イタリア語	it
韓国語	ko
簡体字中国語	zh
繁体字中国語	zh

関連手順

- System Management Homepageログ
- Httpdエラー ログ

関連項目

- [ホーム]ページ
- [設定]ページ
- [タスク]ページ
- [Webアプリケーション]ページ

第8章 [Webアプリケーション]ページ

[Webアプリケーション]ページには、HP System Management Homepage（HP SMH）にインストールされたWebアプリケーションの一覧があります。次のHP Webベース システム マネジメント ソフトウェアへのリンクがあります。

[統合されたエージェント]　Webアプリケーション名を一覧表示します。参加者は、HP SMHに含まれている情報を提供するエージェントです。この情報を提供するHP Webベース システム マネジメント ソフトウェアがインストールされていない場合は、情報メッセージが表示されます。

[他のエージェント]　表示できるHP Webベース システム マネジメント ソフトウェアを一覧表示します。HP Webベース システム マネジメント ソフトウェアの名前により、リンクが提供されるため、そのエージェントがユーザー インターフェイスを提供する場合は、エージェントにアクセスすることが可能です。リンクをクリックすると、webappが新しいブラウザー ウィンドウに開きます。この情報を提供するHP Webベース システム マネジメント ソフトウェアがインストールされていない場合は、情報メッセージが表示されます。

Webアプリケーション プラグインの無効化

1. `/opt/hp/hpsmh/webapp`（Linuxシステムの場合）および`C:\hp\hpsmh\webapp`（Windowsシステムの場合）にあるWebアプリケーション ディレクトリにアクセスします。
2. Webアプリケーション ディレクトリに「disabled」という新しいディレクトリを作成します。
3. 無効にしたいWebアプリケーションに対応するxmlファイルを、Webアプリケーション ディレクトリから「disabled」ディレクトリにコピーします。
4. `smhconfig -r`コマンドを実行して、SMHアプリケーションを再起動します。

関連項目

- 開始するには
- [設定]ページ
- [タスク]ページ
- [ログ]ページ
- [サポート]ページ
- [ヘルプ]ページ

第9章 [サポート]ページ

サポート ページは、HP Essentialsソフトウェアについての情報と、HPサポートおよび公式フォーラムからのガイダンスの入手方法を提供します。このページには、次のような、HP System Management Homepageサーバー ドメイン外のヘルプへのリンクも用意されています。

- Insight Essentialsソフトウェア情報
- Integrity Essentialsソフトウェア情報
- サポート リンク

  HP-UXの場合は、このリンクから、ITリソース センター（ITRC）のホーム ページが開かれます。
- フォーラム リンク

  HP-UXの場合は、このリンクから、ITリソース センター（ITRC）のフォーラム ページが開かれます。

関連項目

- 開始するには
- [ホーム]ページ
- [設定]ページ
- [タスク]ページ
- [ログ]ページ
- [Webアプリケーション]ページ
- [ヘルプ]ページ

第10章 [ヘルプ]ページ

ヘルプ ページは、HP System Management Homepage（HP SMH）およびそのWebアプリケーションのヘルプを提供します。

ヘルプ ページには、次のリンクがあります。

- **[System Management Homepageヘルプ]**　HP SMHインフラストラクチャおよびその設定とログページについての情報が含まれます。残りのエントリーは、システムにインストールされたWebアプリケーション（ヘルプ システムを提供するもの）に関連付けられたヘルプ システムにリンクします。
- **[クレジット]**　オープン ソース ライセンスおよびクレジットに関する情報が表示されます。

HP SMHヘルプにアクセスするには、以下の手順に従ってください。

1. **[ヘルプ]**をクリックします。
2. **[System Management Homepageヘルプ]**リンクをクリックします。

[クレジット]にアクセスするには、以下の手順に従ってください。

1. **[ヘルプ]**をクリックします。
2. **[クレジット]**リンクをクリックします。

[検索フォーム]

[検索フォーム]セクションには、HP SMHヘルプを検索するための検索用語を入力するフィールドがあります。

検索を実行するには、以下の手順に従ってください。

1. **[検索フォーム]**セクションの**[検索条件]**テキストボックスで、検索用語を入力します。
2. **[検索]**をクリックします。
   検索条件が有効な場合は、クエリに一致するすべての文書の一覧が表示されます。

関連手順

▲ [クレジット]

関連項目

- 開始するには
- [ホーム]ページ
- [設定]ページ
- [タスク]ページ
- [ログ]ページ
- [Webアプリケーション]ページ
- [サポート]ページ

[クレジット]

[クレジット]リンクにより、オープン ソース ライセンスおよびクレジットに関する情報が表示されます。

クレジットにアクセスするには、**[ヘルプ]**を選択し、**[クレジット]**リンクをクリックします。

関連項目

▲ [設定]ページ

第11章 コマンド ライン インターフェイス設定

コマンド ライン インターフェイス（CLI）は、コマンド ラインからこれらの値を設定するための管理権限アクセスを与えます。CLIを使用して、設定オプションを変更可能にする必要なセキュリティ チェックを含む、設定オプションを変更することができます。

注記: --kerberos、--user-kerberos、--operator-kerberos、--admin-kerberos、--max-threadsおよび--win32-disable-acceptexオプションは、Windowsオペレーティング システムでのみ使用可能です。

注記: 「-」から始まる長いオプションには、引数の前にオプションの記号「=」があります。

一部のCLIオプションでは、コマンドのオプションの概要にある大文字の単語として記述された特別な引数が必要です。これらの引数のフォーマットの説明は、次の表のとおりです。

表 11-1 CLI引数

引数タイプ	説明
DIR	HP SMHサービスが書き込みアクセスできるディレクトリへのパス。
FILE	ファイルへのパス。
GROUPLIST	セミコロンで区切られたグループ名の一覧。
IPBINDLIST	セミコロンで区切られた、IPv6アドレスおよびIPv4アドレス/ネットワーク ペアまたはそのいずれか。
IPLIST	セミコロンで区切られたIPアドレスの一覧。
NUM	設定されるオプションによって異なる範囲での数値。
NAMELIST	セミコロンで区切られたホスト名およびIPアドレスの一覧。
XENAMELIST	信頼済みサーバー ホスト名の一覧。

匿名アクセス

匿名アクセスは、セキュリティ保護されていないページへの匿名ユーザーのアクセス（ローカル匿名アクセスを含む）を可能にします。次のコマンドは、匿名アクセス設定を有効または無効にします。

```
smhconfig -a|--anonymous-access [=] True | False
```

ローカル アクセス

ローカル アクセス コマンドは、指定したローカル システムへのアクセスを適用し、ローカル アクセス権限を匿名または管理者に設定します。ローカル アクセスを選択すると、ローカル コンソールにアクセスできるユーザーはユーザー名とパスワードを聞かれることなく匿名または管理者アクセスを許可されます。

次のコマンドは、ローカル アクセスを有効または無効にします。

```
smhconfig -L|--localaccess-enabled [=] True | False
```

次のコマンドは、ローカル ユーザー権限を設定します。

```
smhconfig -l|--local-access [=] administrator | anonymous
```

IP限定ログイン

IPアドレスを、ユーザー タイプによって明示的に許可または制限することができます。IPアドレスが明示的に制限されている場合は、明示的に許可されていても制限されます。IPアドレスが許可リストに含まれる場合、それらのIPアドレスのみがログイン アクセスを許可されます。許可リストにIPアドレスがない場合、ログイン アクセスは、制限リストにないあらゆるIPアドレスに対して許可されます。

次のコマンドは、IP制限ログインを有効または無効にします。

```
smhconfig -P|--ip-restricted-login [=] True | False
```

IPアドレス内包 IPアドレス許可コマンドは、次のように実行します。

```
smhconfig -i|--ip-restricted-include [=] IPLIST
```

以下に、*IPLIST*のフォーマット例を示します。

122.23.44.1-122.23.44.255;172.84.100.35;172.168.10.5;168.172.10.1-168.172.10.128

IPアドレス除外　IPアドレス制限コマンドは、次のように実行します。

```
smhconfig -e|--ip-restricted-exclude [=] IPLIST
```

以下に、*IPLIST*のフォーマット例を示します。

122.23.44.1-122.23.44.255;172.84.100.35;172.168.10.5;168.172.10.1-168.172.10.128

注記:　IPv4およびIPv6アドレス範囲がサポートされます。

[IPバインド]

IPバインドは、HP SMHが、IPバインド リストで設定されているアドレスのみを監視できるようにします。IPバインドが有効でIPバインド リストが空の場合は、HP SMHはローカルでのみアクセスできます。

IPバインド コマンドは、次のように実行します。

```
smhconfig -g|--ip-binding [=] True | False
```

IPバインド リスト　IPバインドが有効な場合に使用されるIPバインド リストを設定するには、次のコマンドを使用します。

```
smhconfig -I|--ip-binding-list [=] IPBINDLIST
```

*IPBINDLIST*は、セミコロンで区切られたIPアドレスやIPアドレス/ネットマスク ペアである必要があります。

以下に、*IPBINDLIST*のフォーマット例を示します。

122.23.44.1-122.23.44.255;172.84.100.35;172.168.10.5;168.172.10.1-168.172.10.128

信頼モード

HP SMHは、Systems Insight Manager（HP SIM）またはInsightマネージャー 7（IM 7）セキュリティ タスク実行リクエストおよびシングル ログイン リクエストをさまざまなセキュリティ レベル（すべて信頼から信頼済み証明書のあるHP SIMまたはInsightマネージャー 7のみまでの範囲）で信頼します。

- **すべて信頼**　このコマンドは、あらゆるHP SIMまたはInsightマネージャー 7サーバーからのすべてのセキュリティ タスク実行およびシングル ログイン リクエストを受け入れるようにhttpサーバーを設定します。

  ```
  smhconfig -t|--trust-mode [=] TrustByAll
  ```

- **名前による信頼**　このコマンドは、一覧にあるHP SIMまたはInsightマネージャー 7サーバーからのセキュリティ タスク実行およびシングル ログイン リクエストのみを受け入れるようにHP SMHを設定します。

  ```
  smhconfig -t|--trust-mode [=] TrustByName
  ```

  信頼済みサーバー名リストをTrustByName信頼モードに設定するには、次のコマンドを使用します。

  ```
  smhconfig -X|--xe-name-list [=] XENAMELIST
  ```

  *XENAMELIST*は、信頼するSystems Insight ManagerまたはInsightマネージャー 7サーバーの一覧で、コンマまたはセミコロンを区切り文字に使用します。以下に、名前リストのフォーマットの例を示します。

  server1,server2.domain1;server3,server4.domain2

- **信頼済み証明書**　このコマンドは、証明を使用してHP SIMまたはInsightマネージャー 7とHP SMH間の信頼関係を確立します。信頼モードは、次のコマンドを使用してTrustByCertに設定されます。

  ```
  smhconfig -t|--trust-mode [=] TrustByCert
  ```

  信頼済み証明書は、次のコマンドを使用して信頼済み証明書リストに追加されます。

  ```
  smhconfig -C|--trust-certificate [=] FILE
  ```

  *FILE*は、信頼済み証明書リストに追加する、Base64コード化証明書が含まれるファイルの名前です。

サービスの再起動

新しいコンフィギュレーション設定の適用完了時にHP SMHを再起動してください。

```
smhconfig -r|--restart
```

プログラム管理者ログインの拒否

HP Webベース システム マネジメント ソフトウェアまたはVCAログイン要求を拒否または受け入れてください。

```
smhconfig -j|--reject-prog-admin-login [=] true|false
```

Win32DisableAcceptEX

AcceptEX()は、Microsoft WinSock v2 APIで、特定の環境においてBSD style accept() APIを使用するよりもパフォーマンスを改善します。いくつかの一般的なWindows製品（通常、ウイルス スキャンや仮想プライベート ネットワーク パッケージ）には、AcceptEx()の動作に干渉するバグがあります。次のようなエラーが発生した場合：

```
[error] (730038) An operation was attempted on something that is not a socket::
winnt_accept: AcceptEx failed. Attempting to recover.
```

次のディレクティブを使用して、AcceptEx()の使用を無効にしてください。

```
smhconfig -w|--win32-disable-acceptex [=] True | False
```

注記: Win32DisableAcceptEXは、Windowsオペレーティング システムでのみ使用できる機能です。

SSL v2の無効化

デフォルトで、HP SMHではSSL v2が無効になっています。SSL v2を有効にし直すには、次のスイッチを使用します。

```
smhconfig -s|--disable-sslv2 [=] True | False
```

ログ ローテーション

ログ ファイルは、大きくなって管理しにくくなることがあります。次のスイッチは、ログ ファイルが、5M（デフォルトのサイズ）に達したときに自動的にローテーションできるようにします。オプションをオフにして次のローテーションでログ ファイルを上書きさせるか、オプションをオンにして新しいファイルを作成し前のファイルが古いファイルと印を付けるかのいずれかです。

```
smhconfig -A|--rotate-logs [=] 0 | 1 | 2
```

ここで、0=オフ、1または2=オンです。

ローテーション ログ サイズ

ログ ファイルは、大きくなって管理しにくくなることがあります。次のスイッチでは、ユーザーがログファイルのサイズを設定できます。

```
smhconfig -z|--rotate-log-size [=] size
```

ここで、sizeは、1～9MBの値です。

可能な最大スレッド数

[可能な最大スレッド数]の値によって、ユーザーは、ページ要求のためにHP SMHが作成するスレッドの最大数を増やしたり減らしたりすることができます。Windowsのデフォルトは、64です。

注記: 可能な最大スレッド数は、Windowsオペレーティング システムでのみ使用できます。

```
smhconfig -M|--max-threads [=] max-number-of-threads
```

ここで、*max-number-of-threads*は、64～512の範囲の数字です。

可能な最大スレッド数は、Windowsでのみ使用できます。

セッションの最大数

デフォルトで、HP SMHは128のユーザー セッションをサポートします。この数字は、session-maximum設定を使用して、32に下げたり500に上げたりすることができます。

```
smhconfig -S|--session-maximum [=] maximum-number-of-sessions
```

セッション タイムアウト

デフォルトのセッション タイマは、15分に設定されています。セッション タイムアウトは、1分から60分に設定できます。

```
smhconfig -U|--session-timeout [=] session-timeout-in-minutes
```

ログ レベル

デフォルトで、HP SMHエラー メッセージのロギング レベルはerrorに設定されています。ログ レベルが設定されると、設定されたログ レベルと同じまたはそれより大きなすべてのイベントがログ ファイルに書き込まれます。ログ レベル オプションは、Windowsでは *SystemDrive:*\hp\hpsmh\logs、Linuxでは/var/spool/opt/hp/hpsmh/logsの下のerror_logファイルにのみ影響を与えます。

重要度の低い順に、次の値が使用できます。

表 11-2 ログ レベル

値	説明
emerg	緊急 - システムが使用できません
alert	すぐに対処する必要があります
crit	クリティカル状態
error	エラー状態
warn	警告状態
notice	正常であるが有意状態
info	情報
デバッグ	デバッグレベルのメッセージ

```
smhconfig -v|--log-level [=] logging-level
```

注記: ログ レベルは、HTTPエラー ログに書き込まれる新しいメッセージにのみ影響を与えます。システムのソフト再起動を実行する必要があります。

ポート2301

ポート2301は、HP SMHが2301を監視するかどうかを決定します。値が**True**に設定されると、HP SMHはポート2301を監視します。値が**False**に設定されると、HP SMHはポート2301を監視しません。

デフォルトでは、ポート2301を監視します。

```
smhconfig -T|--port2301 [=] True | False
```

マルチホームされた証明書代理名リスト

multihomedオプションを使用して、証明書の**name**を設定することができます。

コンソールで単一のコマンドを使用してmultihomed値でsmhconfigを実行するときは、hpsmhdサービスを再起動することが重要です（<--restartオプション）。

```
smhconfig -u|--multihomed [=] NAMELIST
smhconfig -u|--multihomed [=] NAMELIST --restart
```

*NAMELIST*は、セミコロンで区切られたIPアドレスおよびホスト名の一覧である必要があります。

カスタムUI

カスタムUIを有効にすると、サインインおよびヘッダ画像をカスタマイズしたり、サインイン ページに小さなテキストを追加したりすることができます。HP SMHインストール パスの hpsmh/data/htdocs/custom_uiディレクトリにあるHP SMH README.txtを参照してください。

```
smhconfig -c|--custom-ui [=] True | False
```

Httpdエラー ログ

httpd error logオプションを使用すると、httpd error_logログ ファイルをユーザー インターフェイスから表示できるようにするかどうかを決めることができます。

```
smhconfig -p|--httpd-error-log [=] True | False
```

アイコン ビュー

アイコン ビューを使用すると、デフォルトのビュー モードを、デスクトップのファイル マネージャの外観のようにアイコンを表示するように設定するか（True）、項目をボックスに表示する従来のリストを表示するか（False）を設定することができます。

```
smhconfig -n|--iconview [=] True | False
```

ボックス順

ボックス順は、ボックスを表示するために使用する順序づけ方法を定義します。**name**を選択して英数字順にボックスを配置するか、**status**を選択して最も悪いステータス（クリティカル）から最も良いステータス（正常）の順にボックスを表示することができます。

```
smhconfig -x|--box-order [=] Name | Status
```

ボックス項目順

ボックス項目順は、ボックス内の項目を表示するために使用する順序づけ方法を定義します。**name**を選択して英数字順にボックスを配置するか、**status**を選択して最も悪いステータス（クリティカル）から最も良いステータス（正常）の順にボックスを表示することができます。

```
smhconfig -b|--box-item-order [=] Name | Status
```

Kerberos認証

Kerberos認証サポートを有効または無効にするには、以下の手順に従ってください。

```
smhconfig -k|--Kerberos [=] True | False
```

管理者Kerberosユーザー　管理者権限のあるKerberosドメインからのユーザーのKerberosグループを設定するには、次のコマンドを使用してください。

```
smhconfig –m|--admin-kerberos [=] GROUPLIST
```

注： GROUPLISTは、単一のKerberosグループ、またはセミコロンで区切られたKerberosグループ名の一覧です。

注記:　–admin-kerberosは、Windowsオペレーティング システムでのみ使用できます。

オペレータKerberosユーザー　オペレータ権限のあるKerberosドメインからのユーザーのKerberosグループを設定するには、次のコマンドを使用してください。

```
smhconfig –R|--operator-kerberos [=] GROUPLIST
```

注： GROUPLISTは、単一のKerberosグループ、またはセミコロンで区切られたKerberosグループ名の一覧です。

注記:　–operator-kerberosは、Windowsオペレーティング システムでのみ使用できます。

ユーザーKerberosユーザー　ユーザー権限のあるKerberosドメインからのユーザーのKerberosグループを設定するには、次のコマンドを使用してください。

```
smhconfig -K|--user-kerberos [=] GROUPLIST
```

注： GROUPLISTは、単一のKerberosグループ、またはセミコロンで区切られたKerberosグループ名の一覧です。

注記: -user-kerberosは、Windowsオペレーティング システムでのみ使用できます。

ユーザー グループ

ユーザー グループは、HP SMHの機能にアクセスして変更するポリシー一式です。既存の有効なオペレーティング システム グループのみをグループ リストに追加することができます。

グループをHP SMHユーザー タイプに追加するには、以下を実行してください。

[Administrators] 管理者アクセス権を持つユーザーは、HP SMH全体で提供されるすべての情報を表示して設定できます。

デフォルトのユーザー グループ（Microsoft社製オペレーティング システムでは[管理者]、Linuxではroot）は、常に、管理者アクセス権を持ちます。

ドメインの一部であるWindowsシステムは、あらゆるレベルのアクセス用にドメイン グループおよびローカル グループを指定することができます。

```
smhconfig -d|--admin-group [=] [ groupList ]
```

オペレータ オペレータ アクセス権を持つユーザーは、HP System Management Homepageによって提供されるほとんどの情報を表示し、設定することができます。一部のWebアプリケーションでは、最も重要な情報へのアクセスが[管理者]のみに制限されています。

```
smhconfig -E|--operator-group [=] [ groupList ]
```

ユーザー ユーザー アクセス権を持つユーザーは、HP System Management Homepageによって提供されるほとんどの情報を表示できます。一部のWebアプリケーションでは、重要な情報の表示が、ユーザー アクセス権を持つユーザーに対して制限されています。

```
smhconfig -G|--user-group [=] [ GROUPLIST ]
```

ここで、*groupList*は、単一のオペレーティング システム グループ、またはセミコロンで区切られたオペレーティング システム グループ名の一覧です。

ヘルプ メッセージ

画面にヘルプメッセージを表示するには、次のコマンドを使用してください。

```
smhconfig -h|--help
```

ファイルベース コマンド ライン インターフェイス

コマンド ライン インターフェイス（CLI）オプションを使用すると、設定パラメータのあるファイルをコマンド ラインに渡すことができます。CLIは、ファイルを解析して引数を処理します。CLIへの入力用のファイルを使用するコマンドは、次のとおりです。

```
smhconfig -f configFile
```

コマンド ライン インターフェイスファイル構造 CLIファイル構造フォーマットには、コメント用の#文字、設定するパラメータを示す括弧付きのキーワード、およびパラメータ値が含まれています。CLIファイル構造フォーマットの例は、次のとおりです。

Characters placed after the # on a given line are not parsed.

smhconfig用の設定ファイルの例は、次のとおりです。

```
# SMH configruation file for smhconfig
[anonymous-access]
false
[localaccess-enabled]
true
[localaccess-type]
administrator
```

```
[user-group]
users
```

コマンド ライン ログ リーダー

コマンド ライン ログの読み出しツールは、SMHのログ メッセージをUIを使わずに読み取るためのコマンド ライン ツールを提供します。コマンドは次のとおりです。

```
smhlogreader [options]
```

[options]には、次のものがあります。

`-h|--help`。ヘルプ メッセージを表示します。

`-f|--file FILE`。「FILE」にはファイルへのパスを指定します。

`--from FROM`。「FROM」はメッセージの範囲を示すために使用します。このオプションには、最初のメッセージのIDを指定します。

`--to TO`。「TO」は、メッセージの範囲を示すために使用します。このオプションには、最後のメッセージのIDを指定します。

`--lang LANG`。「LANG」はログ メッセージの表示に使われる言語です。

重要: smhlogreader CLIでは、1つのコマンドの中でこれらのオプションを組み合わせて使用することもできます。

たとえば、`smhlogreader --lang LANG --from FROM --to TO --file FILE`と入力できます。

---

smhlogreader CLIで使用できるさまざまなオプション：

- ヘルプ

  コマンドを実行してこのツールのヘルプ メッセージを表示できます。

  次のコマンドは、smhlogreader CLIのヘルプ メッセージを表示します。

  ```
  smhlogreader -h|--help
  ```

- バージョン

  コマンドを実行して、SMHのバージョンを表示できます。

  次のコマンドは、SMHのバージョン番号を表示します。

  ```
  smhlogreader --version
  ```

- 言語

  メッセージの表示に使う言語を選択できます。

  次のコマンドを使用して、メッセージの表示に使う言語を選択できます。

  ```
  smhlogreader --lang en|ja
  ```

  SMHのログとUIは、デフォルトでは、英語を意味する「en」と日本語を意味する「ja」をサポートします。

注記: メッセージを正しく表示するには、メッセージの表示に必要なフォントをシステムにインストールする必要があります。たとえば、Windowsの日本語以外のバージョンでログを日本語で参照するには、日本語フォントをインストールする必要があります。

- ログの読み取り

  最新のメッセージのリストを表示します。

  次のコマンドは、最新のメッセージのリストを表示します。

  ```
  smhlogreader
  ```

- 範囲

  smhlogreader CLIが表示するメッセージの範囲を設定できます。

  次のコマンドは、ユーザーが選択した範囲内のメッセージのリストを表示します。

```
smhlogreader --from VALUE --to VALUE
```

たとえば、最も新しいものから順に5つのメッセージを表示するには、`smhlogreader --from 1 --to 5`コマンドを使用します。

- ファイルベースのコマンド ライン ログの読み取り

  smhlogreader CLIでは、正しくフォーマットされたログ ファイルを入力として使用できます。

  次のコマンドを使用すると、正しくフォーマットされたログ ファイルを入力として使用できます。また、このコマンドはログ ファイルをバックアップします。

  ```
  smhlogreader –f|--file FILE
  ```

関連項目

▲ [設定]ページ

第12章 ファイルの位置

表 12-1 HP SMHファイルの位置

説明	Windows	Linux	HP-UX
HP SMHのルート HP SMHインストールのルート。	*SystemDrive*\hp\hpsmh	/opt/hp/hpsmh	/opt/hpsmh
HP SMHの実行可能ファイル HP SMHのバイナリ ファイル。webappは、このファイルの存在を検出してHP SMHがシステムにインストールされていることを確認することができます。	*SystemDrive* \hp\hpsmh\bin\hpsmhd.exe	/opt/hp/hpsmh/sbin/hpsmhd	/opt/hpsmh/lbin
証明書およびキー ファイル HP SMHで使用される証明書およびプライベート キー ファイル。これは、複数の管理アプリケーションによって使用される共有された位置です。キーは、1024ビットの場合と2048ビットの場合があります。	*SystemDrive* \hp\sslshare\cert.pem *SystemDrive* \hp\sslshare\file.pem	/etc/opt/hp/sslshare /cert.pem /etc/opt/hp/sslshare /file.pem	/opt/hpsmh/sslshare
HP SMH XML設定 このファイルは、HP SMH自体によってのみ変更されます。	*SystemDrive* \hp\hpsmh\conf\smhpd.xml	/opt/hp/hpsmh/conf /smhpd.xml	/opt/hpsmh/conf.common /smhpd.xml
HP SMH confファイル confファイルは、起動時およびディスク上のバージョン変更のたびに再生成されます。	*SystemDrive* \hp\hpsmh\conf\smhpd.conf	/opt/hp/hpsmh/conf /smhpd.conf	/opt/hpsmh/conf
2381ドキュメント ルート ポート2381（HTTPS）で提供される文書用のルート。	*SystemDrive* \hp\hpsmh\data\htdocs	/opt/hp/hpsmh/data/htdocs	/opt/hpsmh/data/htdocs
2301ドキュメント ルート ポート2301で提供される文書用のルート。セキュリティ上の制限によって、特定のHP SMH文書のみ、このディレクトリ（HTTP）外で提供することができます。	*SystemDrive* \hp\hpsmh\data\isdocs	/opt/hp/hpsmh/data/isdocs	/opt/hpsmh/data/isdocs
cgi-binルート 実行可能コンテンツのルート。	*SystemDrive* \hp\hpsmh\data\cgi-bin	/opt/hp/hpsmh/data/cgi-bin	/opt/hpsmh/data/cgi-bin
ヘルプのルート ヘルプ ファイルの置かれるルート。	*SystemDrive* \hp\hpsmh\data\help	/opt/hp/hpsmh/data/help	/opt/hpsmh/data/help
Webapp XMLファイル webapp XML設定ファイルのあるルート。	*SystemDrive* \hp\hpsmh\webapp	/opt/hp/hpsmh/webapp	/opt/hpsmh/webapp

関連項目

第13章 トラブルシューティング

注記: 注記がある場合、そのトピックはHP-UX、Linux、またはWindowsオペレーティング システムのいずれかに限って適用される場合があります。

13.1 アクセスの問題

13.13.1.1 セキュリティに関するSMHのドキュメントが不明確

HP System Management Homepage（HP SMH）は、`/etc/securetty`を使用しません。`/etc/securetty`について詳しくは、`login(1)`を参照してください。

13.13.1.2 Linuxでホスト名を入力した後、HP SMHが開始されない。

Linuxでは、64文字以上のホスト名をサポートしていません。

13.2 ブラウザーの問題

13.13.2.1 HP SMHにサインインしてブラウザーを閉じても、HP SMHのセッションが終了しない。閉じた後にInternet Explorerを開くと、認証情報なしでHP SMHにログインできてしまう。どうすればこの問題を解決することができますか?

HP SMHのショートカットで認証情報を確認させるには、2つの解決策があります。

解決策1:

1. **[ツール]**、**[インターネット オプション]**を選択します。
2. **[詳細設定]**タブを選択します。
3. **[設定] [ブラウズ]**の下にある**[ショートカットの起動時にウィンドウを再使用する（タブ ブラウズが無効である場合）]**の選択を解除します。
4. **[OK]**をクリックします。

解決策2:

1. **[ツール]**、**[インターネット オプション]**を選択します。
2. **[全般]**タブの下で、**[タブ:] [タブの中のWebページの表示方法を設定します。]**を検索します。**[設定]**をクリックします。
3. **[他のプログラムのリンクを開く方法：]**から、3番目の**[現在のタブまたはウィンドウ]**を選択します。
4. **[タブ ブラウズの設定]**ウィンドウの**[OK]**をクリックします。
5. **[OK]**をクリックして、**[インターネット オプション]**を閉じます。

13.13.2.2 Windows環境でInternet Explorer 6.0を使用しています。HP System Management Homepage（HP SMH）にサインインするときに**[セキュリティの警告]**ダイアログ ボックスで警告が表示されるのはなぜですか?

次の2つの警告がありえます。

- 警告1: **セキュリティ証明書上の名前が無効であるか、またはサイト名と一致しません。**

  IPアドレスを使用してHP SMHにアクセスすると、この警告が表示されます。また、マシン名にlocalhostを使用してローカル アクセスする場合にも、この警告が表示されます。

- 警告2: **このセキュリティ証明書は、信頼する会社から発行されていません。証明書を表示して、この証明機関を信頼するかどうか決定してください。**

  HP SMHによって証明書が発行されています。証明書は**[信頼された証明書リスト]**に追加でき、追加すると警告が表示されなくなります。

13.13.2.3 2つ目のMozillaブラウザーを開くと、HP System Management Homepageへの不正サインインと表示される場合があります。

別々に起動された複数のMozillaブラウザーは、セッションを共有します。

デスクトップから起動する場合、個別のセッションはMozillaで共有されます。ただし、Internet Explorerでは共有されません。

13.13.2.4 Windows 2003で動作するInternet ExplorerからHP System Management Homepageにアクセスすると、セキュリティ メッセージが表示されたり、ページの一部しか表示されなかったりします。

Windows 2003 Serverでは、Internet Explorer 6.0は、デフォルトのセキュリティ設定が異なります。この問題を防止するには、各管理対象システムをローカル イントラネット ゾーンに2回追加します。1回は**`http://`*ホスト名*`:2301`**として、もう1回は**`https://`*ホスト名*`:2381`**としてです。この解決策以外には、ブラウザーのセキュリティ設定のレベルを下げる（おすすめしません）方法、またはCookie（保存されているものとセッションごとの両方）とアクティブ スクリプトを許可するようにブラウザーのセキュリティ設定を変更する方法があります。

13.13.2.5 ブラウザー ページにコンテンツの一部が表示されません。原因は何ですか?

フレーム サイズは、中くらいのサイズのフォント用に最適化されています。より大きな、またはより小さなフォントを使用するように切り替えた場合は、フレームのレイアウトを、マウスを使用して手動で調整してください。

13.13.2.6 システムにアクセスする際にブラウザーがCookieの受け入れを求めるのはなぜですか?

ブラウザーのCookieは、ユーザーの状態とセキュリティを追跡するために必要です。ブラウザーでCookieを有効にする必要があり、有効にすると、Cookieの受け入れを求めるメッセージは表示されなくなります。

13.13.2.7 HP-UXに**`http://`*ホスト名*`:2301/`**ではログインできますが、**`https://`*ホスト名*`:2381/`**ではできません。

デフォルトでは、HP-UXのインストールは`autostart`機能を有効にします。デーモンはポート2301を監視し、ポート2381からリクエストされたHP SMHのみ開始し、タイムアウト時間が経過すると停止します。詳しくは、`smhstartconfig(1M)`コマンドを参照してください。

13.13.2.8 Windows 2003で動作するローカル マシンで**`https://`*IPアドレス*`:2381`**にアクセスすると、**[サイン イン]**画面が表示されません。

Windows 2003でInternet Explorer 6.0を使用している場合、完全な**[サイン イン]**ページが表示される代わりに、青色のバーに**[Account Sign in]**というテキストだけが表示されることがあります。この問題は、ローカル システムまたはリモート システムでアクセスする場合に発生します。

この問題を解決するには、Javascriptのサポートを有効にして、このサイトを信頼済みサイトのリストに追加してください。

13.3 インストールの問題

13.13.3.1 Windowsシステムで証明書をインポートするために`setup.exe /r`を実行すると、インストールに失敗する。

証明書をインポートまたはコピーするときに`setup.exe /r`を使用しないでください。その代わりに、HP SIMの**[エージェントの設定および修復]**ツールを使用してください。

13.13.3.2 HP SMHをインストールしていると、「`another instance is running.`」というエラーが表示されました。

HP SMHのインストール プログラムが、壊れたファイルを持つシステムまたはインストールが中止されたシステムへのインストールを試みました。

この問題を解決するには、HP SMHシステムの`\temp`ディレクトリに移動して、`smhlock.tmp`ファイルを削除してください。

13.13.3.3 HP SMHをインストールしていると、次のエラーが表示されました。 `error: cannot get exclusive lock on /var/lib/rpm/Packages error: cannot open Packages index using db3 - Operation not permitted (1) error: cannot open Packages database in /var/lib/rpm.`

このエラーは、Linuxシステムでインストール処理の複数のインスタンスを起動すると表示されます。HP SMHのインストールは、一度に1つずつしか実行できません。

13.4 IPアドレスの問題

13.13.4.1 IPv6アドレスでHP SMHにアクセスすると、いつセキュリティ警告が表示されますか?

IPv6アドレスを使用するには、以下のブラウザーが必要です。

- **Windows OS** Internet Explorer 7
- **Linux OS** Mozilla Firefox

注： Internet Explorer 6は、IPv6アドレスを処理できません。詳しくは、**http://blogs.msdn.com/ie/archive/2007/02/20/ipv6-uris-in-ie7.aspx**およびMicrosoft社のサポート ページ**http://support.microsoft.com/kb/325414**を参照してください。

セキュリティ保護されたページを表示すると、Internet Explorer 7は、ページを信頼済サイト ゾーンに追加するかどうかを尋ねてきます。**[追加]**をクリックしても、メッセージがまた表示されます。この場合は、Internet Explorer 7がIPv6 URLの処理に失敗しています。なぜなら、Internet Explorer parserは、コロンをIPアドレスとポート番号の区切り文字として使用するからです。たとえば、次のファイルを作成します。

- IPv4では、HP SMHのIPアドレスは**`https://127.0.0.1:2381`**となることがあります。IPアドレスは127.0.0.1で、ポート番号が2381です。
- IPv6では、HP SMHのIPアドレスは**`https://[2001:db8:c18:1:21a:4bff:fe4c:c8e0]:2381`**となることがあります。この場合、IPアドレスは、2001:db8:c18:1:21a:4bff:fe4c:c8e0でポート番号は2381です。Internet Explorerはコロンを区切り文字として検索し、[2001をIPアドレスとして使用します。

IPv6アドレスでアクセスするときのセキュリティ警告を回避するには、次のいずれかを選択してください。

- IPv6アドレスでサポートされたDNS名を使用します。
- ポート番号なしでローカル イントラネット サイトまたはInternet Explorer 7の信頼済みサイトにリテラルIPv6アドレスを追加します。たとえば、ポート番号を追加せずに**`http://[ 2001:db8:c18:1:250:8bff:fee2:4ed8]`**および**`https://[ 2001:db8:c18:1:250:8bff:fee2:4ed8]`**を追加します。

13.13.4.2 IPアドレスを調べずにブラウザーで簡単にローカル システムにアクセスする方法はありますか?

はい。**`https://`***`hostname`***`:2381`**または**`https://127.0.0.1:2381`**でローカル システムにアクセスできます。HP-UXでは、デフォルト設定の`autostart`を有効にしている場合は、**`http://hostname:2301`**でローカル システムにアクセスできます。

注記: 「localhost」という文字列は、一部の言語では使用できません。また、ブラウザーでプロキシ サーバーを設定している場合は、ブラウザーのプロキシを使用しないアドレスのリストに127.0.0.1を追加しなければならない場合があります。

13.13.4.3 **[IP限定ログイン]**機能を使用する場合、使用しているサーバーのIPアドレスを入力しても機能しません。ローカル マシンのIPアドレスがこの機能によって確実に認識されるようにするには、どうすればよいでしょうか?

ローカル マシンを制限する場合は、サーバーのIPアドレスに加えて127.0.0.1を入力します。127.0.0.1というアドレスは、常に**[IPアドレス包括リスト]**セクションで許可されています。このアドレスは、**[IPアドレス除外リスト]**セクションに明示的に含まれている場合にのみ制限されます。

13.13.4.4 IPアドレス制限を設定しているのに、localhostアクセスが拒否されません。このようなことがなぜ起きるのでしょうか?

ほとんどのユーザーはローカル ホスト アクセスをブロックしようとしないため、ローカル ホストのIPアドレスが[IPアドレス包括リスト]フィールドに含まれていない場合、ローカル ホストにはアクセス権が付与されます。localhostアクセスをブロック**しなければならない**場合は、**[IP限定ログイン]**の**[IPアドレス除外リスト]**フィールドに**`127.0.0.1`**を入力してください。

13.13.4.5 **[IP限定ログイン]**でシステムのローカルIPアドレスや127.0.0.1が**[IPアドレス包括リスト]**リストに含まれていないのに、システムにローカルにアクセスできます。

ユーザーが誤ってHP SMHへのアクセスからロックアウトされることを防止するために、localhostリクエストは、ローカルIPアドレスが**[IPアドレス包括リスト]**リストに含まれていなくても拒否されません。必要な場合は、ローカル システムのIPアドレスと127.0.0.1を**[IPアドレス除外リスト]**リストに追加すると、ローカル システムからのアクセスの試みがすべて拒否されます。

13.5 サインインの問題

13.13.5.1 SMHがデスクトップで対話を許可するように設定されていると、HP SMHバージョン2.1.3（以降）を実行しているProLiantまたはIntegrityサーバーでWindowsオペレーティング システムにサイン インした後、画面にROTATELOGS.EXEコマンド プロンプトが表示される。この現象が発生した場合は、1つまたは2つの小さなコマンド プロンプト ウィンドウに以下のようなメッセージが表示されます。

```
(drive) :\hp\hpsmh\bin\rotatelogs.exe
```

コマンド プロンプト ウィンドウは、サーバーやSMHのパフォーマンスおよび機能には影響されませんので、無視してください。

Windows 2000 ServerまたはWindows Server 2003（すべてのバージョン）とHP SMHバージョン2.1.3（以降）で構成されたすべてのProLiantまたはIntegrityサーバーで、SMHがデスクトップで対話を許可している場合、影響される場合があります。

HP SMHがサーバー デスクトップの対話を禁止するには、以下の手順に従ってください。

1. **[スタート]→[プログラム]→[管理ツール]→[サービス]**の順に選択します。
2. HP System Management Homepageの**[プロパティ]**をクリックします。
3. **[ログオン]**タブをクリックします。
4. **[デスクトップとの対話をサービスに許可]**の選択を解除します。
5. **[適用]**をクリックし、**[OK]**をクリックします。
6. HP System Management Homepageサービスを再起動します。

13.13.5.2 HP SMH **ユーザー グループ**設定ページから、**Backup Operators**、**Administrator**、**Operator**、および**User**などのWindowsで定義されたユーザー グループに権限を与えたが、そのグループのユーザーがサインインできない、またはHP SMHでの権限が正しくない。

HP SMHは、Windowsの定義した4つのユーザー グループ、**Administrators**、**Users**、**Guests**、および**Power Users**のみを認識します。**Backup Operators**など他のWindowsのグループは認識されません。

注記: Linuxでは、グループは、groupaddとしてシステム ツールを使用して前もって作成しておく必要があります。

13.13.5.3 Windowsシステムで**Backup Operators**グループに定義された管理者アカウントでHP SMHにサインインすると、サインインに失敗する。

Windowsシステムのユーザー グループは、**Administrators**、**Users**、**Guests**、および**Power Users**のみ認識されます。**Backup Operators**など他のWindowsのグループは認識されません。新しいグループを作成し、それを使用してHP SMHへのアクセスを提供してください。

13.13.5.4 Windowsオペレーティング システムを実行しているサーバーでHP SMHにサインインできません。

以下の手順を実行してください。

1. Windowsオペレーティング システムの有効なアカウントが設定されていることと、サインインが**[管理者]**グループまたはHP SMHのいずれかのオペレーティング システム グループに含まれていることを確認してください。
2. オペレーティング システムにサインインし、メッセージが表示されたらパスワードを変更します。

   このパスワード メッセージが表示される場合、オペレーティング システムの管理者は、**[ユーザーは次回サインオン時にパスワードの変更が必要]**を選択した状態でユーザー アカウントを設定しています。

オペレーティング システム グループの管理者は、将来作成される任意のサインインを、**[ユーザーは次回サインオン時にパスワードの変更が必要]**オプションを選択せずに追加することができます。さらに、このオプションが選択されている場合、HP SMHにサインインする前にオペレーティング システムでパスワードを変更できます。

13.13.5.5 Windows XPオペレーティング システム環境でHP SMHにサインインできません。

[プログラム]→[管理ツール]→[ローカル セキュリティ ポリシー]の順に選択し、**[ネットワーク アクセス：ローカルアカウントの共有とセキュリティ モデル]**のポリシーを**[Guestのみ]**から**[クラシック]**に変更します。

13.13.5.6 Web管理対象製品をアップグレードするとパスワードを使用できなくなるのはなぜですか?

HP SMH 2.0以降がオペレーティング システム アカウントを使用するのに対して、それまでのバージョンは固定アカウント（**管理者**、**オペレーター**、および**ユーザー**）を使用します。管理者グループ（Linuxの場合はルート グループ）に含まれるすべてのオペレーティング システム アカウントは、HP SMHに対する管理者アクセス権を持ちます。このアカウントでアクセスすると、他のオペレーティング システム アカウント グループにHP SMHへの異なるアクセス レベルを割り当てることができます。このプロセスについて詳しくは、HP SMHのオンライン ヘルプを参照してください。「ユーザー グループ」を参照してください。

注記: これは、HP-UXには適用されません。

13.13.5.7 HP SMHに使用するためにデフォルト設定でWindowsの新しいアカウントを作成しましたが、このアカウントを使用してサインインすることができません。

デフォルトでは、Windowsオペレーティング システムで作成される新しいアカウントは、**[検索条件ユーザーは次回ログオン時にパスワードの変更が必要]**に設定されます。このオプションの選択を解除して、アカウントを使用してHP SMHにログインできるようにしてください。

13.13.5.8 Windows環境でInternet Explorer 6.0を使用しています。管理サーバーを経由してIPアドレスによって検出されたシステムにアクセスする場合、HP SMHにサインインできません。匿名アクセスが有効になっていると、匿名でアクセスできますが、ユーザー名が使用できません。

または

Windows環境でInternet Explorer 6.0を使用しています。管理サーバーを経由してIPアドレスによって検出されたデバイスにアクセスする場合、**[管理サーバー証明書 自動インポート]**画面のテキスト ボックスに証明書の詳細情報が表示されません。

この問題は、次の方法でInternet Explorerの設定を調整することによって解決できます。

- Internet Explorerの**[プライバシー]**設定を**[中]**から**[低]**に変更します。（このオプションの使用はおすすめできません。）

  設定を変更するには、以下の手順に従ってください。

  1. Internet Explorerで、**[ツール]**、**[インターネット オプション]**の順にクリックします。
  2. **[プライバシー]**をクリックします。
  3. スライド バーをクリックしたまま、**[低]**にドラッグします。
  4. **[適用]**をクリックします。
  5. **[OK]**をクリックします。

     変更が保存されます。

- 対象のHP SMHのIPアドレスをローカル イントラネットのゾーンに追加します。

  設定を変更するには、以下の手順に従ってください。

  1. Internet Explorerで、**[ツール]**、**[インターネット オプション]**の順にクリックします。
  2. **[セキュリティ]**をクリックします。
  3. **[イントラネット]**を選択します。
  4. **[サイト]**、**[詳細設定]**の順にクリックします。

5. **[次のWebサイトをゾーンに追加する]**フィールドに、HP SMHシステムのIPアドレス（**`https://`*IPアドレスなど***）を入力します。
6. **[追加]**をクリックします。
7. **[OK]**をクリックします。
8. **[OK]**を再度クリックします。
9. **[OK]**をクリックします。

   変更が保存されます。

13.13.5.9 Internet Explorerでサーバー名（**`http://サーバー名:2301`**）を使用してシステムにアクセスする場合、Windowsの有効な管理者アカウントのユーザー名とパスワードを使用してもサインインできません。ただし、IPアドレス（**`http://`*IPアドレス*`:2301`**）を使用してシステムにアクセスするとサインインできます。

サーバーのコンピューター名にアンダースコア（_）が含まれていないか確認してください。含まれている場合は、削除するか、「_」（アンダーバー）の代わりに「-」（ダッシュ）を使用してください。これで、システム名を使用してログインできるようになります。

注記: システムの名前を変更した後に、Microsoft Internet Information Server（IIS）の設定を変更しなければならない場合があります。

これは、Internet Explorer 5.5または6.0用のMicrosoftセキュリティ パッチMS01-055によって追加されたセキュリティ機能です。この機能により、不適切な名前構文を持つシステムがCookie名を設定できなくなります。Cookieを使用するドメインは、ドメイン名およびシステム名に英数字（-または.）しか使用できません。Internet Explorerは、システム名にアンダースコア（_）などの他の文字が含まれている場合に、そのシステムからのCookieをブロックします。

13.6 セキュリティの問題

13.13.6.1 Service Pack 2を使用してWindows XPシステムをアップデートした後、HP SIMやHPバージョン コントロール レポジトリ マネージャーにアクセスできなくなります。原因は何ですか?

Windows XP Service Pack 2は、ソフトウェア ファイアウォールを実装しており、このため、ブラウザーがHP SIMおよびバージョン コントロール レポジトリ マネージャーにアクセスするために必要なポートにアクセスできません。この問題を解決するには、[例外]を使用してファイアウォールを設定し、ブラウザーがHP SIMとバージョン コントロール レポジトリ マネージャーによって使用されるポートにアクセスできるようにしてください。

以下の手順を実行することをおすすめします。

1. **[スタート]→[設定]→[コントロール パネル]**の順に選択します。
2. **[Windowsファイアウォール]**をダブルクリックして、ファイアウォールの設定を指定します。
3. **[例外]**を選択します。
4. **[ポートの追加]**をクリックします。
5. 製品名とポート番号を入力します。

   ファイアウォール保護に、次の例外を追加します。

表 13-1 ファイアウォール保護の例外

製品	ポート番号
HP SMH非セキュア ポート：	2301
HP SMHセキュア ポート：	2381
HP SIM非セキュア ポート：	280
HP SIMセキュア ポート：	50000

6. **[OK]**をクリックして設定を保存し、**[ポートの追加]**ダイアログ ボックスを閉じます。
7. **[OK]**をクリックして設定を保存し、**[Windowsファイアウォール]**ダイアログ ボックスを閉じます。

この設定によって、SP2のセキュリティ強化はデフォルトのままになりますが、トラフィックは上記のポートを経由できるようになります。このポートは、HP SIMおよびバージョン コントロール レポジトリ マネージャーを実行するために必要です。ポート2301および2381はバージョン コントロール レポジトリ マネージャーに、ポート280および5000はHP SIMに必要です。アプリケーションで通信するには、各製品について、セキュア ポートと非セキュア ポートを追加する必要があります。

13.13.6.2 X.509証明書を直接HP SMHにインポートできないのはなぜですか?

HP SMHは、証明書リクエストをBase64コード化PKCS #10フォーマットで生成します。この証明書リクエストは、認証機関に提供される必要があります。ほとんどのCAは、**[設定]→[HP System Management Homepage]→[セキュリティ]→[ローカル サーバー証明書]**の順に選択することによってHP SMHに直接インポートできるBase64コード化PKCS #7証明書データを返します。

CAがX.509フォーマットの証明書データを返す場合は、X.509証明書ファイルの名前を`cert.pem`に変更して、`\hp\sslshare`ディレクトリに保存してください。HP SMHを再起動すると、この証明書が使用されます。

13.13.6.3 PKCS #7証明書データが受け入れられないのはなぜですか?

Mozillaブラウザーを使用している場合、メモ帳や他のエディターで証明書のリクエストおよび応答データを切り取って貼り付けると問題が発生することがあります。この問題を回避するために、CAからのどの証明書応答ファイルもMozillaを使用して開いてください。証明書に関する作業では、Mozillaで提供されている[Select All]、[Cut]、および[Paste]操作を使用してください。

13.13.6.4 プライベート キー ファイルがファイル システムによって保護されないのはなぜですか?

Windowsオペレーティング システムを使用している場合、プライベート キー ファイルがファイル システムによって保護されるには、システム ドライブがNTFSフォーマットである必要があります。

13.13.6.5 **[設定]→[SMH]→[セキュリティ]→[信頼された管理サーバー]**の順に選択して、カスタマー作成証明書のPKCS #7データを[HP SIM 証明書データ]フィールドに貼り付けると、エラーが表示されるのはなぜですか?

カスタマー作成証明書のPKCS #7データが**[信頼された管理サーバー]**フィールドの日付と関連がありません。**[設定]**、**→[HP System Management Homepage]**、**[セキュリティ]**、**→[ローカル サーバー証明書]**の順に選択して、**.PKCS #7**データを**[カスタマーによって生成された証明書を、PKCS #7 データにインポート]**フィールドにインポートしてください。**[HP Systems Insight Manager証明書データ]**フィールドは、HP SMHでHP SIMサーバーを信頼するために使用します。詳しくは、「[信頼された管理サーバー]」を参照してください。

13.13.6.6 Windows 2003CAを使用してサードパーティの証明書をHP SMHに付与できないのはなぜですか?

Windows 2003CAを使用してHP SMH用の証明書を作成するには、以下の手順に従ってください。

1. **[設定]→[SMH]→[セキュリティ]→[ローカル サーバー 証明書]**ページの順にクリックして、PKCS #10データ パケットを作成します。
2. **Ctrl**+**C**キーを押してデータをバッファーにコピーします。
3. **`http://`***`W2003CA`***`/certsrv`**（*`W2003CA`*はWindows 2003 認証機関システムの名前）に移動し、以下の手順を行います。
   a. **[証明書を要求する]**を選択します。
   b. **[証明書の要求の詳細設定]**を選択します。
   c. **[Base64エンコードCMCまたはPKCS #10 ファイルを使用して証明書の要求を送信するか、またはBase64エンコードPKCS #7ファイルを使用して更新の要求を送信する]**を選択します。
   d. **Ctrl**+**V**キーを押して**PKCS #10**データをフィールドに貼り付けます。

4. Windows 2003 認証機関システムで次の手順を実行します。
   a. **[スタート]→[すべてのプログラム]→[管理ツール]→[証明機関]**の順にクリックします。
   b. **[証明機関(ローカル)]**、**[W2003CA/certsrv]**（*W2003CA*はWindows 2003 認証機関システムの名前）の順にクリックします。
   c. 保留リクエスト証明書を発行します。
5. **http://***W2003CA***/certsrv**（*W2003CA*はWindows 2003 認証機関システムの名前）に移動し、以下の手順を行います。
   a. **[保留中の証明書の要求の状態]**を選択します。
   b. **[Base64エンコード]**と**[証明書のダウンロード]**を選択します（**証明書チェーン**は選択しないでください）。
   c. ダウンロード ファイルは、`certnew.cer`です。
   d. `certnew.cer`というファイル名を`cert.pem`に変更します。

13.13.6.7 Bastilleを使用するときのセキュリティ オプションを教えてください。

Bastilleは、HP-UXホストのセキュリティを向上させるシステム強化プログラムです。デーモン、システム設定、およびファイアウォールをさらに安全になるように設定します。rcp(1)やrlogin(1)のような不要なサービスやツールを停止したり、WebサーバーおよびDNSなどの共通インターネット サービスの脆弱性を制限したりすることができます。

注記: 現在、HP System Management HomepageはPartition Managerをサポートしていません。

システムをロック ダウンするためにBastilleの使用する機能の1つは、IPフィルタリングです。Partition ManagerでIPフィルタリングを使用する際の要件については、Partition Managerのオンライン ヘルプを参照してください。Bastilleの対話型ユーザー インターフェイスを使用するときは、Bastilleの尋ねる質問に答えるにあたってこれらの問題に注意してください。また、Bastilleには、`/etc/opt/sec-mgmt/bastille`にある次のファイルで表される3つのインストール時のセキュリティ オプションもあります。

- **HOST.config** ホストベース ロックダウン。IPFilter設定なし。この設定を使用すると、Partition Managerには影響を与えません。
- **MANDMZ.config** 緊密なロックダウン。ただし、共通管理プロトコルおよびツールの使用する一部のネットワークは開いたままにします。たとえば、この設定を使用してもWBEMは動作します。この設定でPartition Managerを起動するには、SSHを使用するか、ポート2301および2381を有効にするように変更する必要があります。ポート2301および2381が無効なシステムでPartition Managerの起動を有効にするには、エントリーを追加してIPフィルタリングを調整します。たとえば次のとおりです。

  pass in quick proto tcp from any to any port = 2301 flags S/0xff keep state keep frags

  pass in quick proto tcp from any to any port = 2381 flags S/0xff keep state keep frags

  これらを、`/etc/opt/sec-mgmt/bastille/ipf.customrules`に追加してからBastilleを起動します。

  詳しくは、`ipf(5)`を参照してください。
- **DMZ.config** 緊密なロックダウン。この設定でPartition Managerを起動するには、SSHを使用する必要があります。

  また、Bastilleが有効なシステムをリモートで管理するときに、BastilleはPartition Managerに影響を与えます。HOST.configまたはMANDMZ.config設定が使用されている場合、証明書を正常に転送した後で、Partition Managerは上述のように動作します。ただし、DMZ.config設定は、WBEMトラフィックをブロックし、Partition Managerがシステムをリモートで管理できなくします。

  Bastilleについて詳しくは、`bastille(1M)`および『Bastille User Guide』を参照してください（`/opt/sec-mgmt-bastille/docs/user-guide.txt`にインストールされています）。

13.7 その他の問題

13.13.7.1 HP SMHの3.xから2.xへのダウングレードに問題があります。

HP SMHの3.xから2.xに正常にダウングレードするには、HP SMHサービスを停止し、以下の手順に従ってダウングレードを実行してください。

1. `$/etc/init.d/hpsmhd stop`
2. `$rpm --oldpackage --U hpsmh-`*`old version`*`.rpm`

13.13.7.2 HP SMHをシステムにインストールできないのはなぜですか?

HP SMHをインストールするには、ロードするために256色以上を必要とするJavaバージョンが必要です。

注記: これは、Windowsのみ適用されます。

13.13.7.3 **[マネジメント プロセッサー]**リンクをクリックすると、ページが表示できないことを示すエラーが表示されるのはなぜですか?

マネジメント プロセッサーの管理者は、ポート80以外のポートを使用するようにマネジメント プロセッサー上のWebサーバーを設定しています。HP SMHは、そのパラメーターにアクセスできず、マネジメント プロセッサーがポート80にあると想定します。

13.13.7.4 rootではない場合にHP-UXまたはLinux環境にHP SMHをインストールできないのはなぜですか?

適切なアクセス権を持つには、HP SMHのルートとしてログインする必要があります。

13.13.7.5 Serviceguard Managerプラグインで、**[統合された syslog の表示]**ボタンを選択すると再度認証が必要になるか、「ページが見つかりません」というエラーが発生する場合があります。

「ページが見つかりません」というエラーが表示されたら、ブラウザーの**[更新]**ボタンを押して、ページを正しく表示させます。または、再度認証する必要があります。

13.13.7.6 [Memory Utilization]プロパティ ページの**[Total Swap Space Size]**フィールドの値には、デバイスまたはファイル システムとしてシステムに存在するスワップ領域と、メモリ リソースとして存在していない擬似スワップ サイズが含まれます。実際のデバイスおよびファイル システムのスワップ領域は、このページには表示されません。

現在、HP SMHプロパティ ページから実際のデバイスおよびファイル システムのスワップ領域のサイズを取得することはできません。HP-UXコマンドラインから、`swapinfo`コマンドを使用すると、この情報を取得することができます。

サービスおよびサポート

HP SMHに対するサポートは、基本となるハードウェアのサポートの補助として提供されています。HP サポート ページは、製品、サービス、およびサポートに関するさまざまなHP SMHのリソースを提供します。

- Software Depot homeでHP SMHにアクセスします。**http://www.hp.com/go/softwaredepot**にアクセスして、**[Security and manageability]**を選択します。**[HP System Management Homepage]**リンクを検索します。Software Depot homeのLinuxリンクを選択するとLinux Integrityのサポートが表示されます。**HP Integrity Essentials Pack for Linux**を検索してください。
- HP ProLiant Essentials softwareページ**http://www.hp.com/servers/manage**にアクセスします。豊富なシステム マネジメント製品およびサービス関連の情報が掲載されています。
- HP製品のメンテナンス/サポート、フォーラム、トレーニング/教育HPについての情報は、ITリソース センター**http://itrc.hp.com**にアクセスしてください。
- HP製品についてのご質問は、HPサポート フォーラム**http://forums.itrc.hp.com**にお問い合わせください。

各自の設定を詳しく記録しておくと、トラブルシューティング プロセスを大幅にスピードアップできます。HPのサービス窓口からサポートを受ける場合は、現状を維持して、以下を参照してください。

- 管理システムのメーカー、モデル、およびシリアル番号情報
- バージョン番号、適用されたService Packのリスト、HP PSPのバージョン、および適用されたInsight エージェントの名前とバージョンなどの、オペレーティング システム情報、オペレーティング環境情報（HP-UX）
- LinuxおよびWindowsの場合ハードウェア コンフィギュレーション情報
  - Surveyユーティリティの出力、またはHP Insight Diagnosticsからの出力、または[システムの参照(Inspect)]の印刷出力
  - システム コンフィギュレーション ユーティリティの印刷出力
  - [システムの参照（Inspect）]ユーティリティまたはシステム コンフィギュレーション ユーティリティの印刷出力に示されない、HP製およびコンパック製以外の装置の説明

第14章 ご注意

保証

本書の内容は、将来予告なしに変更されることがあります。Hewlett-Packardは、本書に関して、いかなる種類の保証（特定の目的のための商品性または適合性に関する黙示の保証を含む）もいたしません。本書の記載事項の誤り、またはマテリアルの提供、性能、使用により発生した損害については責任を負いかねますのでご了承ください。

Hewlett-Packard製品に適用される特定保証条項の複写、および交換部品は、最寄の販売保守事務所から入手できます。

米国政府ライセンス

本書で取り扱っているコンピューター ソフトウェアは秘密情報であり、その保有、使用、または複製には、HPから使用許諾を得る必要があります。FAR 12.211および12.212に従って、商業用コンピューター ソフトウェア、コンピューター ソフトウェア ドキュメンテーション、および商業用製品の技術データ（Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items）は、ベンダー標準の商業用使用許諾のもとで米国政府に使用許諾が付与されます。

著作権表示

商標表示

すべてのHP 9000コンピューター上のHP-UX Release 10.20以降およびHP-UX Release 11.00以降（32ビット構成および64ビット構成）は、Open Group UNIX 95ブランドの製品です。

Intel®およびItanium®は、米国ならびにその他の国におけるIntel Corporationの商標または登録商標です。

Javaは、Sun Microsystems, Incの米国における商標です。

Linuxは、Linus Torvalds氏の米国における登録商標です。

MS-DOS®、Microsoft®、およびWindows®は、米国およびその他の国におけるMicrosoft Corporationの商標または登録商標です。

UNIXは、The Open Groupの米国ならびに他の国における登録商標です。

出版履歴

出版の日付と部品番号は、最新版ができるたびに変更します。出版の日付と部品番号は、最新版ができるたびに変更します。マニュアルの部品番号は、改訂が行われるたびに変更します。新版が使用可能になったときに新版を受け取るため、適切な製品サポート サービスを受けてください。詳細については、HP販売担当者に問い合わせてください。

本書に関するご意見は、次の住所にお寄せください。

Hewlett-Packard Company HP-UX Learning Products 3404 East Harmony Road Fort Collins, Colorado 80528-9599

本書に関するフィードバックは、次の当社Webサイトまでお寄せください。**http://docs.hp.com/ja/feedback.html**

リビジョン履歴

出版履歴
改訂 第19版　　2009年11月
MPN：466304-194。HP System Management Homepageヘルプのこのエディションには、WindowsおよびLinux HP SMH 6.0.0リリースの製品の変更および問題点の修正に対応する更新内容が含まれています。
改訂 第18版　　2009年3月

MPN：466304-193。HP System Management Homepageヘルプのこのエディションには、WindowsおよびLinux HP SMH 3.0.0リリースのIntegrityアップデートが含まれています。
改訂 第17版　　2009年3月
MPN: 466304-192。HP System Management Homepageヘルプのこのエディションには、HP-UX HP SMH 3.0.0リリースの製品の変更および問題点の修正に対応する更新内容が含まれています。製品の変更点は次のとおりです。

- HP SMHの新しいルック&フィール
- ユーザー設定可能なユーザー インターフェイス（UI）プロパティ
- セッションおよびユーザー タイムアウト（UI）のユーザー制御
- HP SMH構成に関わる問題のデバッグに役立つ`smhassist`コマンド

改訂 第16版　　2008年11月
MPN：466304-191。HP System Management Homepage 3.0の初版は、次を含む、LinuxとWindowsの情報とタスクを記載しました。

- 新しいユーザー インターフェイス
- WindowsでのKerberosのサポート
- コマンド ライン インターフェイスのサポート
- ポート2301の無効化機能
- ユーザー設定可能なユーザー インターフェイス プロパティ
- セッションおよびユーザー タイムアウトのユーザー制御
- ログのローカリゼーション
- IPv6のサポート

改訂 第15版　　2008年2月
MPN：436304-197。第15版は、HP SMH v2.1.11リリースでのWindowsとLinuxの新しいハードウェアサポートとログ ファイル サイズのコントロール、代理名証明書のサポートを行う新しい機能を追加し、オンライン ヘルプは2つの言語に翻訳しました。
改訂 第14版　　2007年12月
MPN：436304-198。第14版は、HP-UX HP SMH v2.2.7リリースの新しい機能を追加し、HP-UXリリース用にオンライン ヘルプを9ヶ国語に翻訳しました。
改訂 第13版　　2007年8月
MPN：436304-196。第13版は、HP SMH v2.1.10-00リリースのIPF LinuxとWindowsの新しい機能を追加し、オンライン ヘルプを2ヶ国語に翻訳しました。
改訂 第12版　　2007年6月
MPN：436304-195。第12版は、HP SMH v2.1.10リリースで修正された新しいセキュリティを追加し、オンライン ヘルプを2ヶ国語に翻訳しました。
改訂 第11版　　2007年6月
MPN：436304-194。第11版は、HP-UX HP SMH v2.2.6リリースの新しい機能を追加し、HP-UXリリース用にオンライン ヘルプを9ヶ国語に翻訳しました。
改訂 第10版　　2007年4月
MPN：436304-193。第10版は、HP SMH v2.1.8リリースで修正された新しいセキュリティを追加し、オンライン ヘルプを2ヶ国語に翻訳しました。
改訂 第9版　　2007年2月
MPN：436304-191。第9版は、HP-UX HP SMH v2.2.5リリースの新しい機能を追加し、HP-UXリリース用にオンライン ヘルプを9ヶ国語に翻訳しました。
改訂 第8版　　2007年1月
MPN: 436304-192。第8版は、HP SMH v2.1.7リリースで新しいオペレーティング システムおよびブラウザーのサポートを追加し、オンライン ヘルプを2ヶ国語に翻訳しました。
改訂 第7版　　2006年12月
MPN：365395-199。第7版は、HP-UX HP SMH v2.2.5リリースで修正された不具合を追加し、HP-UXリリース用にオンライン ヘルプを9ヶ国語に翻訳しました。
改訂 第6版　　2006年11月
オンライン ヘルプ システムの改版履歴に間違いがありました。HP System Management Homepageの第6版は、存在しません。
改訂 第5版　　2006年9月

MPN：365395-008。第5版は、HP-UX HP SMH v2.2.4リリースで変更された機能を追加し、HP-UXリリース用にオンライン ヘルプを9ヶ国語に翻訳しました。
改訂 第4版 2006年6月
MPN：365395-007。第4版は、HP-UX HP SMH v2.2.3リリースで変更された機能を追加し、オンライン ヘルプを9ヶ国語に翻訳しました。
改訂 第3版 2005年12月
MPN：365395-005。第3版は、HP-UX HP SMH v2.2.1リリースで変更された機能を追加し、オンライン ヘルプを9ヶ国語に翻訳しました。
改訂 第2版 2005年2月
MPN：365395-004。第2版は、HP-UX HP SMH v2.2リリースの情報とタスクを追加しました。

用語集

Accounts for Users & Groupsツール (ugweb)
HP-UX Accounts for Users and Groups（ugweb）ツールは、ローカル システム上のユーザー アカウントおよびグループ アカウントの管理に使用します。このツールは、NISシステム上のユーザー アカウントの管理にも使用できます。ugwebツールは、HP-UX System Administration Manager（SAM）ツールまたはHP SMHから起動することができます。

AS
参照 Kerberos認証サーバー.

CA
参照 認証機関.

CLI
参照 コマンド ライン インターフェイス.

Disks and File Systemsツール (fsweb)
HP-UX Disks and File Systems（fsweb）ツールは、ファイル システム、論理ボリューム、およびディスクの管理に使用します。Disks and File Systemsツールは、HP-UX System Administration Manager（SAM）ツールまたはHP SMHから起動することができます。

DNS
参照 ドメイン ネーム サービス.

evweb
参照 System Fault Managementツール.

fsweb
参照 Disks and File Systemsツール.

GUI
参照 グラフィカル ユーザー インターフェイス.

HP Insightマネジメント エージェント
ユーザーの介在なしに、情報を定期的に収集したり、その他のサービスを実行したりするプログラム。

HP SIM
参照 HP Systems Insight Manager.

HP SMH
参照 HP System Management Homepage.

HP System Management Homepage (HP SMH)
HP System Management Homepage（HP SMH）は、HP-UX、Linux、およびMicrosoft Windowsのオペレーティング システム上で、HPサーバー用の単一のシステム管理を統合して簡素化するWebベースのインターフェイスです。HP SMHは、HPのWebベースのエージェントおよび管理ユーティリティからのデータを統合することによって、単一のサーバーのハードウェア障害/ステータス監視情報、パフォーマンス データ、システム スレッショルド、診断情報、およびソフトウェア バージョン管理情報を表示するための使いやすい共通インターフェイスを提供します。HP SMHは、HP Webベース システム マネジメント ソフトウェアのスイートによって使用されるソフトウェアに組み込まれた一部で、HTTPおよびHTTPSを介して通信します。HP Webベース システム マネジメント ソフトウェアに一定の機能とセキュリティのセットを提供します。

HP Systems Insight Manager (HP SIM)
HP製のシステム、クラスター、デスクトップ、ワークステーション、ハンドヘルドなど、さまざまなシステムを管理できるシステム マネジメント ソフトウェア。HP SIMは、HP Insight マネージャー7、HP Toptools、HP Servicecontrolマネージャーの長所を組み合わせることにより、Windows、Linux、HP-UXを実行しているHP ProLiantシステム、HP Integrityシステム、HP 9000システムを管理する、統一されたツールとしてお使いいただけます。HP SIMソフトウェアの中核部分では、すべてのHP製サーバー プラットフォームの管理に必要な機能を提供します。また、HP SIMは、HP製ストレージ、電源、クライアント、プリンター製品用のプラグインにより広範囲なシステム管理を提供するように拡張することもできます。Rapid Deployment Pack、Performance Management Pack、Workload Management Packのプラグインは、ハードウェア資産の完全なライフサイクルの管理機能を追加したソフトウェアをシステム管理者が選択することができます。HP SIMについて詳しくは、HPのWebサイト **http://www.hp.com/jp/hpsim**を参照してください。

HP Webベース システム マネジメント ソフトウェア
HP製Web対応製品を管理するソフトウェア。

HP-UX System Administration Manager (SAM)
HP-UX 11i v1（B.11.11）およびHP-UX 11i v2（B.11.23）では、システム管理のプライマリ インターフェイスです。

HP-UX 11i v3（B.11.31）では、HP SMHがHP-UXシステム管理のタスクとしてプライマリ インターフェイスを提供します。既存のSAM機能はそのまま利用できます。

HPバージョン コントロール エージェント (VCA)
サーバーにインストールされたHPのソフトウェアをユーザーが確認できるようにするために、そのシステムにインストールされているInsightマネジメント エージェント。HPバージョン コントロール エージェントは、HPバージョン コントロール レポジトリ マネージャーを参照す

るように設定できるため、バージョンの比較やレポジトリからのソフトウェアの更新が簡単になります。

HPバージョン コントロール レポジトリ マネージャー (VCRM) ユーザーが定義するディレクトリ/レポジトリに格納されたHP提供のソフトウェアをユーザーが管理できるようにするInsightマネジメント エージェント。

HTTPS *参照* Secure HTTP.

Integrity Support Pack HPによって、1つにバンドルされ、特定のオペレーティング システムで動作することが確認されたHPのソフトウェア コンポーネントのセット。Integrity Support Packには、ドライバー コンポーネント、エージェント コンポーネント、およびアプリケーションとユーティリティのコンポーネントが含まれています。これらはすべて一緒にインストールできることが確認されています。

IP *参照* インターネット プロトコル（IP）レンジ.

kcweb *参照* Kernel Configurationツール.

KDC *参照* Kerberos Key Distribution Center.

Kerberos MITで開発された信頼のできる他社認証プロトコル。異なったホストとユーザーがお互いを認証して確認することができます。

Kerberos Key Distribution Center Kerberos Key Distribution Center。Authentication ServerおよびTicket Granting Serverから構成されます。

Kerberos Ticket Granting Server ユーザーがパスワードを一度しか入力する必要がなくなるように、間接的なレイヤーを追加します。チケットとセッション キーは、その後すべてのチケットで使用されるパスワードから入力されます。通常のサービスにアクセスする前に、ユーザーはTGSと通信するためにAuthentication Server（AS）からチケットを要求します。このチケットは、ticket granting ticket（TGT）と呼ばれます。initial ticketということもあります。TGT用のセッション キーはユーザーの長期キーを使用して暗号化されます。したがって、ユーザーに対するASの応答から復号するにはパスワードが必要になります。

Kerberos認証サーバー ユーザー アカウント記録の認証のみを目的とするサービス。ASは、ユーザーの導入機能として、およびASに登録された共有秘密鍵を使用したサービスとして動作します。

Kernel Configurationツール (kcweb) HP-UX Kernel Configuration（kcweb）ツールは、カーネル調整、モジュール、およびアラームの管理に使用します。Kernel Configurationツールは、HP-UX System Administration Manager（SAM）ツールまたはHP SMHから起動することができます。

MIT マサチューセッツ工科大学。

parMgr *参照* Partition Manager.

Partition Manager (parMgr) HPサーバー システム上のnPartitionsの構成および管理に適したGUIをシステム管理者に提供します。コマンドやパラメーターを覚えていなくても、コンプレックスの構成タスクを実行することができます。グラフィカルなディスプレイでnPartitions、セル、I/Oシャーシやその他のコンポーネントを選択し、メニューからアクションを選択するだけです。Partition Managerを使用して、次のタスクを実行することができます。nPartitionsの作成、変更、削除、コンプレックス内のnPartitions構成の検証、コンプレックスの潜在的な構成やハードウェア問題のチェック、コンプレックスのハードウェア リソースの管理

注記: 現在、HP System Management HomepageはPartition Managerをサポートしていません。

pdweb *参照* Peripheral Deviceツール.

Peripheral Device ツール (pdweb) HP-UX Peripheral Device（pdweb）ツールは、I/OデバイスおよびOLRADカードをすばやく簡単に表示することができます。また、再起動しないでもカードの追加や交換をサポートする、システムのホットプラグPCIスロットの管理に役立ちます。すべてのHP-UXシステムでは、pdwebはI/Oデバイスを表示し、選択したデバイスのデバイス ファイルを作成することができます。Peripheral Deviceツールは、HP-UX System Administration Manager（SAM）ツールまたはHP SMHから起動することができます。

PKI *参照* パブリック キー インフラストラクチャ.

ProLiantまたはIntegrity Support Pack

	HPによって、1つにバンドルされ、特定のオペレーティング システムで動作することが確認されたHPのソフトウェア コンポーネントのセット。ProLiantまたはIntegrity Support Packには、ドライバー コンポーネント、エージェント コンポーネント、およびアプリケーションとユーティリティのコンポーネントが含まれています。これらはすべて一緒にインストールできることが確認されています。
Red Hat Package Manager (RPM)	強力なパッケージ マネージャーで、個々のソフトウェア パッケージをビルド、インストール、クエリ、確認、アップデート、およびアンインストールするために使用できます。パッケージは、ファイルのアーカイブと、名前、バージョン、説明などのパッケージ情報で構成されます。
RPM	*参照* Red Hat Package Manager.
SAM	*参照* HP-UX System Administration Manager.
Secure HTTP (HTTPS)	Web経由でのデータの安全な送信を支援する拡張されたHTTPプロトコル。
Secure Shell (SSH)	ネットワーク経由で他のシステムにサインインして、そのシステムでコマンドを実行することを可能にするプログラム。また、SSHを使用すると、あるシステムから別のシステムにファイルを移動でき、安全でない経路でも安全な認証と通信を提供します。
Secure Sockets Layer (SSL)	HTTPとTCPの間にあって、クライアントとサーバーの間でプライバシやメッセージ整合性を提供する標準プロトコル層。SSLの一般的な使用方法は、サーバーの認証です。これにより、クライアントは、システムがそれであると主張するところのシステムと通信していることを確信できます。これは、アプリケーションのプロトコルに依存しません。
Security Attributes Configurationツール (secweb)	HP-UX Security Attributes Configuration（secweb）ツールは、セキュリティ属性のIsystem-wideおよびper-user（ローカル ユーザーおよびNISユーザー）値の表示や設定に使用します。また、アカウントのロック情報も提供します。Security Attributes Configurationツールは、HP-UX System Administration Manager（SAM）ツールまたはHP SMHから起動することができます。
secweb	*参照* Security Attributes Configurationツール.
SSH	*参照* Secure Shell.
SSL	*参照* Secure Sockets Layer.
STE	*参照* セキュア タスク実行.
Surveyユーティリティ	ハードウェアとオペレーティング システムの設定情報を収集および配信するエージェント（またはオンライン サービス ツール）。この情報は、サーバーがオンラインのときに収集されます。
System Fault Managementツール (evweb)	System Fault Management（evweb）ツールは、WBEMインジケーターの表示および管理に使用します。evwebツールは、HP SMHから起動することができます。
TGS	*参照* Kerberos Ticket Granting Server.
ugweb	*参照* Accounts for Users & Groupsツール.
URI	インターネット上のリソースにアクセスする方法を提供します。URL（Uniform Resource Locator）は、URI（Uniform Resource Indicator）の種類です。
URL	World Wide Web上のリソースのグローバル アドレス。URL（Uniform Resource Locator）は、URI（Uniform Resource Indicator）の種類です。
VCA	*参照* HPバージョン コントロール エージェント.
VCRM	*参照* HPバージョン コントロール レポジトリ マネージャー.
WBEM	*参照* Web-Based Enterprise Management.
Web-Based Enterprise Management (WBEM)	多様なリソースの監視や制御を行うための共通モデル（記述など）とプロトコル（インターフェイスなど）を定義する、プラットフォームやリソースに依存しない DMTF（Distributed Management Task Force）標準。HP WBEM Services for HP-UXは、このDMTF WBEM標準をHP-UXに実装した製品です。
インターネット プロトコル（IP）レンジ	指定された範囲に含まれるIPアドレスを持つシステム。
インプレース	限定的に、インプレース インストールは、ローカルにインストールすることを意味します。

グラフィカル ユーザー インターフェイス (GUI) コンピューターのグラフィック機能を利用してプログラムを簡単に使用できるようにするプログラム インターフェイス。HP SMHのGUIはWeb対応なので、Webブラウザーで表示されます。

コマンド ライン インターフェイス (CLI) オペレーティング システムのコマンド シェルから直接実行できる一連のコマンド。

シングル サインオン 管理対象システムごとに認証を受けなくてもHP Systems Insight Manager（HP SIM）から任意の管理対象システムにアクセスできるように、HP SIMにアクセスしている認証済みユーザーに与えられる権限。HP SIMは最初の認証ポイントであり、他の管理対象システムにはHP SIMからアクセスする必要があります。

ステータス タイプ HP SMHで定義される指定されたステータス タイプ（重大、障害/メジャー、劣化/マイナー、正常、および不明）のシステム。

セキュア タスク実行 (STE) 管理対象システムからのタスクの安全な実行。HP SMHのこの機能により、タスクを要求するユーザーがそのタスクを実行するための適切な権限を持っていることが保証されます。また、データを盗聴から保護するために要求が暗号化されます。

ソフトウェアの更新 ソフトウェアやファームウェアをリモート更新するためのタスク。

ドメイン ネーム サービス (DNS) ドメイン名をIPアドレスに変換するサービス。

バージョン コントロール Windows/Linux ProLiantまたはIntegrityシステム、およびHP-UXオペレーティング システムのソフトウェア ディストリビュータのために、Windowsシステムにインストールされたバージョン コントロール レポジトリ マネージャーとして呼ばれます。管理対象のすべてのProLiantまたはIntegrityシステムのソフトウェア ステータスの概要を提供し、それらのシステム上であらかじめ設定された条件に基づいて自動的にシステム ソフトウェアとファームウェアのアップデートを行うことができる。バージョン コントロールは、古いシステム ソフトウェアを実行しているシステムを識別して、アップグレードを利用できるかどうかを示し、アップグレードの理由を提供する。HP-UXシステムでは、ソフトウェア ディストリビュータは、複数のHP-UXに対してHP Systems Insight Manager CMSから起動することができます。

パブリック キー インフラストラクチャ (PKI) 企業がインターネット上での通信と商取引をセキュリティ保護することを可能にするソフトウェア、暗号化技術、およびサービスの組み合わせ。

プリンシパル Kerberos領域に提示されたユーザーまたはサービス/ホストで、お互いに認証することができます。

マルチホーム 証明書に複数の名前を設定します。

ユーザー HP System Management Homepageへの有効なサインインを持つネットワーク ユーザー。

ユーザー アカウント HP System Management Homepage（HP SMH）にサインインするために使用されるアカウント。これらのアカウントは、Windowsのローカル ユーザー/ドメイン アカウント、HP-UX/Linuxのユーザー アカウントにHP SMH内での権限レベルとページング属性を関連付けます。

レポジトリ 管理対象クラスターに関する重要な情報（ユーザー、ノード、ノード グループ、ロール、ツール、権限など）を保存するデータベース。

外部サイト 他社製アプリケーションのURL。

検索条件 要求されている情報のサブセットをすべての情報のセットから定義するために使用される変項（情報）のセット。フィルタリングできる情報セットには、動作情報や一部のシステム情報などがあります。フィルターは、許可フィルターとその後の制限フィルターで構成されます。これら2つのフィルタリング処理の結果は、グループと呼ばれる。フィルターの例としては、表示可能な情報を作成したり管理動作を実行させたりするSQLステートメントなどがあります。

注意 示されている手順に従わないと装置が損傷したりデータが消失する場合がある付加的な説明。

統合されたエージェントと他のエージェント

[ツール]ページの[統合されたエージェント]エリアには、該当する場合、参加者とそのエントリー ポイントへのリンクが含まれます。エージェントのリンクをクリックすると、特定のエージェントにアクセスできます。参加者とは、HP System Management Homepage（HP SMH）に含まれている情報を提供するエージェントのことです。この情報を提供するHP Web

ベース システム マネジメント ソフトウェアがインストールされていない場合は、**[なし]**と表示されます。

[ツール]ページの[その他のエージェント]エリアには、認識されているがHP SMHに参加していないHP Webベース システム マネジメント ソフトウェアがリストされます。HP Webベース システム マネジメント ソフトウェアの名前により、リンクが提供されるため、そのエージェントがユーザー インターフェイスを提供していれば、エージェントにアクセスすることが可能です。この情報を提供するHP Webベース システム マネジメント ソフトウェアがインストールされていない場合は、**[なし]**と表示されます。

自己署名の証明書 認証機関（CA）自体の証明書。このため、対象とCAは同じです。
参照 証明書, 認証機関.

証明書 対象のパブリック キーとその対象に関する識別情報含む電子文書。証明書は、認証機関（CA）によって署名され、キーと対象識別情報を結合します。

認証機関 (CA) 電子署名とパブリック-プライベート キー ペアを作成するために使用される電子証明書を発行する信頼された第三者機関または企業。このプロセスでのCAの役割りは、固有の証明書を付与された個人が、その個人がそうであると主張するところの者であることを保証することです。

領域 Kerberosドメイン。通常、大文字の、ネットワークのドメイン名です。たとえば、smhkerberos.comのKerberos領域は、慣例的に`SMHKERBEROS.COM`と呼ばれています。

索引