HP System Management Homepage

HP 部品番号: 436304-197
2007年12月
第 15 版

目次

1 製品概要.....7
HP SIM.....7
統合管理ツール.....7
HP-UX System Administration Manager（SAM）の非推奨.....7
追加資料.....8
関連項目.....8

2 開始するには.....9
関連項目.....9
ログイン.....9
Internet ExplorerからのHP System Management Homepage（HP SMH）の起動.....9
MozillaまたはFirefoxからのHP SMHの開始.....10
HP SIMからのHP SMHの開始.....11
HP-UXコマンド ラインからの開始.....12
HP SMH管理サーバ.....12
関連項目.....12
ファイアウォールの設定.....13
Windows.....13
Linux.....13
Red Hat Enterprise Linux 4および5.....13
SUSE Linux Enterprise Server.....15
関連項目.....15
タイムアウトの設定.....15
SMHサービス タイムアウトの設定.....15
SMHセッション タイムアウトの設定.....16
SMH UIタイムアウトの設定（Linux、Windows）.....16
関連項目.....17
証明書の自動インポート.....17
関連項目.....18
ログアウト.....18
関連項目.....18

3 ソフトウェアのナビゲート.....19
[情報領域].....19
関連項目.....19
HP SMHページ.....20
関連項目.....20

4 [ホーム]ページ.....21
ソフトウェア ステータス カテゴリ（ボックス）.....21
システム ステータス サマリ.....21
構成メニュー.....21
デフォルトのHP-UXプロパティ ページ.....22
システム.....22
オペレーティング システム.....23
ネットワーク.....23
ソフトウェア.....23
ストレージ.....23

関連項目.....23

5 [設定]ページ.....25
メニューカテゴリ（HP-UXのみ）.....25
System Management Homepageカテゴリ.....25
関連手順.....25
関連項目.....25
メニュー.....25
関連手順.....25
関連項目.....26
Add Custom Menu.....26
関連項目.....26
Remove Custom Menu.....26
関連項目.....26
クレジット.....27
関連項目.....27
セキュリティ.....27
関連手順.....27
関連項目.....28
[IP バインド].....28
関連項目.....28
[IP限定ログイン].....28
関連項目.....29
[ローカル サーバ証明書].....29
関連項目.....30
マルチホームされた証明書.....31
関連項目.....31
[ローカル/匿名アクセス].....31
関連項目.....32
信頼モード.....32
信頼モードの設定.....33
関連項目.....34
[信頼された管理サーバ].....34
関連項目.....34
[ユーザ グループ].....35
関連項目.....36

6 [タスク]ページ.....37
System（HP-UXのみ）.....37
関連項目.....37

7 [ツール]ページ.....39
関連項目.....39

8 [ログ]ページ.....41
関連手順.....41
関連項目.....41
System Management Homepageログ.....41
関連項目.....41
System Management Homepageレガシー ログ.....41
関連項目.....42
SAMログ.....42

関連項目....42
エラー ログ....42
関連項目....42

9 トラブルシューティング....45
アクセスの問題....45
ブラウザの問題....45
クラスタの問題....47
インストールの問題....47
IPアドレスの問題....47
ログイン時の問題....48
セキュリティの問題....51
その他の問題....53
サービスおよびサポート....53

10 ご注意....55
保証....55
米国政府ライセンス....55
著作権表示....55
商標表示....55
出版履歴....55
リビジョン履歴....55

用語集....57

索引....61

第1章　製品概要

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ベースのインタフェースです。

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フェー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
- 個々のサーバのソフトウェア バージョン コントロール

HP SMHは、HP-UX、Linux（x86、AMD64、およびIntel Itanium）、およびMicrosoft Windowsオペレーティング システムを実行しているサーバにインストールできます。

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。詳細については、「[信頼された管理サーバ]」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さまざまなツールを提供する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が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 インタフェース（GUI）、ターミナル ユーザ インタフェース（TUI）、およびコマンド ライン インタフェース（CLI）を提供します。 `smh`コマンド（`/usr/sbin/smh`）を使用すると、これらのインタフェー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インタフェー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 Window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

追加資料は、以下のWebサイトに掲載されています。

- Software Depot homeのHP SMH http://www.hp.com/go/softwaredepotにアクセスして、**[Security and manageability]**を選択します。HP-UXバージョンの**[HP System Management Homepage]**リンクを検索します。 Linuxの場合は、Software Depot Homeにアクセスして、Linuxを選択します。 **HP Integrity Essentials Foundation Pack for Linux**を検索してください。
- HP ProLiant Essentails 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1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のヘルプ システム** ヘルプ システムには、HP SMHの使用、維持管理、およびトラブルシューティング用のすべての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 ガイド*** ユーザ ガイドには、HP SMHの使用、維持管理、およびトラブルシューティング用のすべてのドキュメントが含まれています。LinuxとWindowsでは、このユーザ 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の場合、印刷されたユーザ ガイドは提供されなくなりました。HP SMHの使用方法、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のオンライン 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で提供される機能を顕著に表しています。 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リリースでは、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リリースでは、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。
- ***sam*(1M)マンページ** HP-UXリリースでは、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の機能変更については、このヘルプ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、HP SMHを適切に設定するためのガイドラインとして、以下の手順を実行し、ユーザとセキュリティ 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。環境変数と`/opt/hpsmh/lbin/envvars`、`/opt/hpsmh/conf.common/smhpd.xml`、および`/opt/hpsmh/conf/timeout.conf`ファイルのタグ値を変更すると設定を変えることができます。
- 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 x86_64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。 Itaniumシステムのperlスクリプトは、`/opt/hp/hpsmh/smhconfig`にあります。
- 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 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. ユーザの権限を効率的に管理するためにユーザ グループを追加します。「[ユーザ グループ]」
2. 信頼モードを設定します。「信頼モード」
3. ローカル アクセスまたは匿名アクセスを設定します。「[ローカル/匿名アクセス]」

関連項目

- ログイン
- ファイアウォールの設定
- 証明書の自動インポート
- ログアウト

ログイン

[アカウント ログイン]ページから、利用可能な*HP Insight マネジメント エージェント*が含まていれる**[ホーム]**ページにアクセスできます。

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

Internet ExplorerでHP SMHにログインするには、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。

注記: HP-UXサーバを参照する場合は、デフォルトで*URI*：**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のみ開始し、タイムアウト時間が経過すると停止します。また、HP SMHを常にポート2381で実行されるように設定することができます。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の[アカウント ログイン]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. 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。

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場合は、管理に使用するブラウザに*認証機関*ルート証明書をインストールできます。認証機関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。予期に反して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、ブラウザのオンライン ヘルプを参照してください。

---

3. **[はい]**をクリックします。

   [アカウント ログイン]ページが表示されます。**[匿名]**アクセスが有効になっている場合は、System Management Homepageが表示されます。

4. オペレーティング システムによって認識されているユーザ名を入力します。

   HP SMHの初期状態は、HP-UXではrootユーザのみアクセスでき、Linuxはrootオペレーティング システム グループに属しているユーザのみアクセスでき、Windowsでは Administratorsオペレーティング システム グループに属しているユーザのみアクセスできるようになっています。ユーザ証明書が本物であることが確認できない場合、ユーザ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でHP SMHにログインしたら、異なるオペレーティング システム グループのユーザにセキュリティの設定を行うアクセス権を与えることができます。

注記: ほとんどの場合、**[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。

---

5. 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。
6. HP-UXでは、**[Sign In]**をクリックします。LinuxおよびWindowsでは、**[ログイン]**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にログインするには、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。

注記: HP-UXサーバを参照する場合は、デフォルトで*URI*：**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のみ開始し、タイムアウト時間が経過すると停止します。また、HP SMHを常にポート2381で実行されるように設定することができます。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の[アカウント ログイン]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。

初めてこのURIにアクセスすると、**[不明な認証局により認証されたWebサイト]**ダイアログ ボックスが表示され、サーバを信頼するかどうかを尋ねられます。**[この証明書を常に受け入れる]**を選択していない場合は、ブラウザを使用するたびに**[不明な認証局により認証された Web サイト]**ダイアログ ボックスが表示されます。

2. **[OK]**をクリックします。

   [アカウント ログイン]ページが表示されます。**[匿名]**アクセスが有効になっている場合は、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名を入力します。

   HP SMHの初期状態は、HP-UXではrootユーザのみアクセスでき、Linuxはrootオペレーティング システム グループに属しているユーザのみアクセスでき、Windowsでは Administratorsオペレーティング システム グループに属しているユーザのみアクセスできるようになっています。ユーザ証明書が本物であることが確認できない場合、ユーザ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でHP SMHにログインしたら、異なるオペレーティング システム グループのユーザにセキュリティの設定を行うアクセス権を与えることができます。

注記: ほとんどの場合、**[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. HP-UXでは、**[Sign In]**をクリックします。LinuxおよびWindowsでは、**[ログイン]**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ブラウザでHP SIMにログインして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 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場合は、管理に使用するブラウザに認証機関ルート証明書をインストールできます。認証機関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。予期に反して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。

   [ログイン]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. ターゲット システムの隣のチェックボックスを選択します。 **[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。 **[すぐに実行]**をクリックします。

   サーバ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コマンドのどちらかを実行して、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インタフェー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 WindowベースのObAMまたはTUIベースのObAMに開く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

デフォルトでは、HP-UXのHP SMH管理サーバは必要なときに開始されます。 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

- ログアウト
- 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、ブラウザがバージョン コントロール レポジトリ マネージャ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、ブラウザがHP Systems Insight Managerとバージョン コントロール レポジトリ マネージャによって使用されるポートにアクセスできるようにする必要があります。

注記: Windows XP Service Pack 2の場合、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 マネージャを実行するために必要です。ブラウザ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。

ファイアウォールの設定を行うには、以下の手順に従ってください。

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。

   製品名およびポート番号をそれぞれ入力する必要があります。

   ファイアウォール保護に、次の例外を追加します。

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

5. **[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。
6. **[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ファイアウォールは、YAST2ユーティリティを使用して設定できます。

ファイアウォールの設定を行うには、以下の手順に従ってください。

1. YAST2を使用するには、**[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て、設定が保存されます。

関連項目

- 開始するには
- ログイン
- 証明書の自動インポート
- ログアウト
- HP SMHページ

タイムアウトの設定

2つのHP SMHタイムアウト設定を変更できます。

- **SMH**サービス タイムアウト—HP SMHサーバが停止するまでの合計時間を分単位で設定します。
- **SMH**セッション タイムアウト—HP SMHGUIセッションが停止するまでの合計時間を分単位で設定します。

注記: **[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。

SMHサービス タイムアウトの設定

HP SMHサービス タイムアウト設定は、分単位でHP SMHタイムアウトを設定することができます。 定義しないか0に設定すると、HP SMHはサービス タイムアウト無しで起動します。サービス タイムアウトがHP SMHセッション タイムアウトよりも少ない場合、HP SMHサーバはHP SMHセッション タイムアウトの3分後に停止します。

HP SMHが「automatic startup on boot」起動モードを使用している場合、サービス タイムアウト無しでHP SMHが起動します。

サービス タイムアウト設定を変更するには、以下の手順に従ってください。

1. 念のため、既存の`/opt/hpsmh/conf/timeout.conf`ファイルを別のディレクトリにコピーします。

2. 以下の手順でtimeout.confファイルを編集します。
   a. テキスト エディタで/opt/hpsmh/conf/timeout.confを開きます。
   b. 以下の行を9分よりも大きい値に指定します。

      ```
      TIMEOUT_SMH=30
      ```

   c. 保存して、ファイルを閉じます。
3. HP SMHサービスを再起動します。

SMHセッション タイムアウトの設定

HP SMHセッション タイムアウト設定は、分単位でHP SMHタイムアウトを設定することができます。セッション タイムアウト時間にユーザの操作がない場合、HP SMH GUIセッションは停止します。

セッション タイムアウトが定義されていない場合、デフォルトの15分に設定されます。

セッション タイムアウト設定を変更するには、以下の手順に従ってください。

1. 念のため、既存のsmhpd.xmlファイルを別のディレクトリにコピーします。
   ファイルは、オペレーティング システムによって、以下の場所に保存されています。
   - **HP-UX**：

     /opt/hpsmh/conf.common/smhpd.xml
   - **Windows**：

     <systemdrive>\hp\hpsmh\conf\smhpd.xml
   - **Linux**：

     /opt/hp/hpsmh/conf/smhpd.xml
2. 以下の手順でsmhpd.xmlファイルを編集します。
   a. テキスト エディタを使用し、smhpd.xmlファイルを開きます。
      - **HP-UX**：

        /opt/hpsmh/conf.common/smhpd.xml
      - **Windows**：

        <systemdrive>\hp\hpsmh\conf\smhpd.xml
      - **Linux**：

        /opt/hp/hpsmh/conf/smhpd.xml
   b. <system-management-homepage>と</system-management-homepage>タグの間に次の行を追加します。

      <session-timeout>*value*</session-timeout>

      *value*には、1～120の値を使用できます。
   c. 保存して、ファイルを閉じます。
3. HP SMHサービスを再起動します。

SMH UIタイムアウトの設定（Linux、Windows）

HP SMH 2.1.5以降は、HP SMH GUIタイムアウトの設定を行うことができます。

注記: GUIタイムアウト設定（smhpd.xml内のui-timeoutタグ）は、WindowsおよびLinuxにインストールされたHP SMHにのみ適用されます。

この設定を変更するには、以下の手順に従ってください。

1. 念のため、既存のsmhpd.xmlファイルを別のディレクトリにコピーします。

2. 手動で以下のタグを追加します。
   a. 起動ドライブの\hp\hpsmh\confディレクトリのsmhpd.xmlファイル（Linux Itanium、Linux x86、およびx86_64の場合は、/opt/hp/hpsmh/conf ）をテキストエディタで開きます。
   b. <system-management-homepage>と</system-management-homepage>タグの間に次の行を追加します。

      <ui-timeout>10**から**3600**間での値を入力**</ui-timeout>

   c. 保存して、ファイルを閉じます。
3. HP SMHサービスを再起動します。

関連項目

- 開始するには
- ログイン
- 証明書の自動インポート
- ログアウト
- HP SMHページ

証明書の自動インポート

[管理サーバ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 System Management Homepage（HP SMH）にアクセスする際にHP Systems Insight Manager（HP SIM）システムの*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]**→**[System Management Homepage]**→**[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、**[アカウント ログイン]**ページに**[管理サーバ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. デフォルトでは、**[管理サーバ証明書の自動インポート]**が選択されています。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、このオプションの選択を解除します。ただし、この選択を解除すると、今後このシステムにアクセスする際にログイン証明書が必要になります。

   HP SMHがHP SIMの証明書を自動的にインポートするように設定すると、今後このシステムにアクセス際にログイン証明書が不要になり、スムーズにアクセスできるようになります。

3. **[管理サーバ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、**[ログイン]**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。

注記: 証明書をインポートしたくない場合は、**[管理サーバ証明書の自動インポート]**の選択を解除してください。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。

関連項目

- 開始するには
- ログイン
- ファイアウォールの設定
- ログアウト
- セキュリティ

ログアウト

HP System Management Homepage（HP SMH）からログアウトするには、2つの方法があります。

- HP SMHバナーから、HP-UXの場合は、**[Sign Out]**をクリック、LinuxおよびWindowsの場合は、**[ログアウト]**をクリックします。HP System Management Homepage**[アカウントログイン]**ページが表示されます。
- HP SMHにログインするために使用したWebブラウザ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
- ログイン
- 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、各ボックスの境界が項目のステータスを示します。詳細については、「[ホーム]ページ」を参照してください。

HP SMHインタフェースは、次の2つのフレームに分割されています。

- **ヘッダ フレーム**　ヘッダ フレームは、表示中のページに関係なく常に表示されます。現在表示中のパスを示します。
- **データ フレーム**　[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 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
  - 「[ホーム]ページ」
  - 「[設定]ページ」
  - 「[タスク]ページ」
  - 「[ツール]ページ」
  - 「[ログ]ページ」
- **サポート**　**[サポート]**リンクは、HPサポート領域へのリンクを提供します。
- **フォーラム**　**[フォーラム]**リンクは、HP フォーラムへのリンクを提供します。
- **ヘルプ**　**[ヘルプ]**リンクにより、独立したブラウザ ウィンドウにヘルプ ファイルが表示されます。ヘルプには、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に関連するすべてのヘルプ ファイルが含まれています。
- **システム モデル**　**[システム モデル]**には、システムのモデルが表示されます。LinuxおよびWindowsでは、サーバ用の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は、**[不明]**と表示されることもあります。HP-UXでは、オペレーティング システムがHP Insightマネジメント エージェントと関係なくシステム モデルを識別できるので表示されます。
- **[現在のユーザ]**　[現在のユーザ]には、現在ログインしているユーザのIDが表示されます。現在のユーザが実際のオペレーティング ベースのユーザの場合は、**[ログアウト]**または**[Sign Out]**リンクが表示されます。匿名アクセスが有効で、ページに匿名アクセスしている場合は、**[現在のユーザ]**に**[hpsmh_anonymous]**と表示され、**[ログイン]**または**[Sign In]**リンクが表示されます。**ローカル アクセス**が有効にされていて、HP Webベース システム マネジメント ソフトウェアにローカル マシンからアクセスしている場合は、**[現在のユーザ]**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、その下にローカル アクセスであることが示されます。local_access_administratorの場合、ログインまたはログアウト リンクは表示されません。

関連項目

- [ホーム]ページ
- [設定]ページ
- [タスク]ページ

- [ツール]ページ
- [ログ]ページ

HP SMHページ

HP System Management Homepage（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、5つのタブ付きページがあります。**[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のみ表示されます。

HP SMHでは、次のページを表示できます。

- 「[ホーム]ページ」
- 「[設定]ページ」
- 「[タスク]ページ」
- 「[ツール]ページ」
- 「[ログ]ページ」

関連項目

- 製品概要
- 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。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の場合、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、統合されたバージョン コントロール、サーバ、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。

ソフトウェア ステータス カテゴリ（ボックス）

HP Webベース システム マネジメント ソフトウェアのステータスは、個々のボックスに表示されるようにカテゴリ分けされています。各カテゴリ（ボックス）には、データを提供しているHP Webベース システム マネジメント ソフトウェアまでたどることができるリンクが含まれています。

追加のステータス カテゴリ：統合されたWBEMのステータスは、追加のカテゴリ（ボックス）に表示されるように設定されています。各カテゴリには、データを提供しているWBEMソフトウェアまでたどることができるリンクが含まれています。

ステータス カテゴリ インジケータ：カテゴリ（ボックス）を囲んでいる罫線は、各カテゴリ内のデータのステータスにより色分けされています。次の表に、色とその定義の一覧を示します。

インジケータ	説明
橙色	メジャー
黄	マイナー
緑	正常
青色	不明
赤	クリティカル
灰色	無効
水色	警告
白	情報

システム ステータス サマリ

[システム ステータス サマリ]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*によって提供される、故障または劣化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、または故障ステータスや劣化ステータスのアイテムがない場合、**[システム ステータス サマリ]**には**[障害/劣化アイテムは存在しません]**と表示されます。

構成メニュー

[ホーム]ページの左側には構成メニューが表示されます。構成メニューには、HP Webベース システム マネジメント ソフトウェアへの次のリンクが含まれています。

- **インテグレーテッド エージェント**　参加者と、該当する場合は、参加者のエントリ ポイントへのリンクが含まれています。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。

- **その他エージェント**　HP System Management Homepageに参加していない、認識可能な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。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インタフェー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。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。
- **[管理プロセッサ]**　リモート**Insight**ボード**Lights-Out Edition**（**RILOE**）または**Integrated Lights-Out**（**iLO**）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。2006年12月リリースのHP-UX HP SMH 2.2.5では、管理プロセッサ リンクとプロパティ ページが追加されました。
- **その他のソフトウェア/その他のリンク**　ProLiant、Integrity、サポート、フォーラムへのリンクを表示します。
- **キー/記号**　ステータスアイコンのリストおよびそれぞれについての簡単な説明が表示されます。

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

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、特に`WBEMServices`（WBEM Services for HP-UX）と`SFM-CORE`（HP-UX System Fault Management）によって異なります。

システム

[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のHS列にも表示されます。 概要の他に、メモリやプロセッサ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するためのリンクがあります。

オペレーティング システム

[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。

ネットワーク

[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。

ソフトウェア

[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。

ストレージ

[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。

関連項目

- [設定]ページ
- [タスク]ページ
- [ツール]ページ
- [ログ]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。

メニューカテゴリ（HP-UXのみ）

このカテゴリでは、HP SMHの任意のページおよびカテゴリに対し、カスタム メニューを追加および削除するためのリンクを提供します。これらのメニューを使用すると、コマンドの実行、Xアプリケーションの起動、または別のWebページまたはWebサイトを起動することができます。「メニュー」も参照してください。

System Management Homepageカテゴリ

このカテゴリでは、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。

- **「クレジット」**　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。
- **「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。

関連手順

- メニュー
- Add Custom Menu
- Remove Custom Menu
- クレジット
- セキュリティ
- [IP バインド]
- [IP限定ログイン]
- [ローカル サーバ証明書]
- [ローカル/匿名アクセス]
- 信頼モード
- [信頼された管理サーバ]
- [ユーザ グループ]

関連項目

- [ホーム]ページ
- [タスク]ページ
- [ツール]ページ
- [ログ]ページ

メニュー

[Menu]カテゴリは、カスタム メニューの追加とカスタム メニューの削除へのリンクを提供します。

- **[設定]→[Menus]→[Add Custom Menu]**の順に選択します。
- **[設定]→[Menus]→[Remove Custom Menu]**の順に選択します。

関連手順

- Add Custom Menu
- Remove Custom Menu

関連項目

- [設定]ページ

Add Custom Menu

[Add Custom Menu]リンクは、カスタム メニューの設定と追加を行うためのオプションを表示します。

HP SMHにカスタム メニューを追加するには以下の手順に従います（HP-UXのみ）。

1. **[設定]→[Menus]→[Add Custom Menu]**の順に選択します。
2. **[Type]**で、メニューを、コマンドの実行、Xアプリケーションの起動、別のWebサイトまたはWebアプリケーションへリンクのいずれのタイプにするかを指定します。
3. **[Page]**で、HP SMHページ内のどのページの下にこのメニューを追加するかを指定します。えば、**[ホーム]**、**[タスク]**、**[設定]**、**[ツール]**、または**[ログ]**を指定することができます。
4. **[Category]**で、メニューを配置するカテゴリ（ボックス）を指定します。既存のカテゴリ名を入力するか、新しいカテゴリを入力して作成することができます。
5. **[Tool Name]**に、指定したページとカテゴリの下に表示させたいメニューの名前を指定します。
6. **[Command/URL]**に、コマンドやXアプリケーションへの実際のコマンドライン、またはリンクのターゲット先となるWebページのURLを入力します。
7. **[Run as root]**の左にあるチェックボックスで、コマンドをrootユーザとして実行するかどうかを指定します。チェックボックスをオンにすると、管理者権限を持つHP SMHユーザのみがこのメニューの実行を許可されます。

注記: メニューの作成と「rootユーザとして実行」が設定されたカスタム メニューを実行できるのは、管理者権限を持つHP SMHユーザーだけです。オペレータ権限またはユーザ権限を持つHP SMHユーザは、実行を許可されたカスタム メニューをユーザ ログインの実際のユーザIDで実行することができます。

これらのカスタムメニューは、`/opt/hpsmh/data/htdocs/xlaunch/custom_menus.js` ファイルに保存され、管理されます。このファイルはシステム間で手動でコピーすることができます。

関連項目

- [設定]ページ
- メニュー
- Remove Custom Menu

Remove Custom Menu

[Remove Custom Menu]リンクは、カスタム メニューの削除を行うためのオプションを表示します。

[Remove a Custom Menu]にアクセスするには、**[設定]→[Menus]→[Remove Custom Menu]**の順に選択します。

関連項目

- [設定]ページ
- メニュー
- Add Custom Menu

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、**[設定]→System Management Homepage→[クレジット]**の順に選択します。

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以下のオプションを提供します。

- **[IP バインド]**　**[設定]→[System Management Homepage]→[セキュリティ]→[IP バインド]**の順に選択します。
- **[IP限定ログイン]**　**[設定]→[System Management Homepage]→[セキュリティ]→[IP限定ログイン]**の順に選択します。
- **[ローカル サーバ証明書]**　**[設定]→[System Management Homepage]→[セキュリティ]→[ローカル サーバ証明書]**の順に選択します。
- **[マルチホーム証明書]**　**[設定]→[System Management Homepage]→[セキュリティ]→[ローカル サーバ証明書]**の順に選択します。
- **[ローカル/匿名アクセス]**　**[設定]→[System Management Homepage]→[セキュリティ]→[ローカル/匿名アクセス]**の順に選択します。
- **信頼モード**　**[設定]→[System Management Homepage]→[セキュリティ]→[信頼モード]**の順に選択します。
- **[信頼された管理サーバ]**　**[設定]→[System Management Homepage]→[セキュリティ]→[信頼された管理サーバ]**の順に選択します。
- **[ユーザ グループ]**　**[設定]→[System Management Homepage]→[セキュリティ]→[ユーザ グループ]**の順に選択します。

注記:　*ユーザ アカウント*を設定するには、管理対象のユーザ アカウントおよびグループ アカウントに対し、オペレーティング システムの各タイプに応じて適切なツールを使用してください。HP-UX 11i v2（B.11.23）の2005年12月以降のリリースでは、ツール（**[ツール]**）ページの下に*Accounts for Users & Groups*（ugweb）のユーザ インタフェースが含まれています。

関連手順

- [IP バインド]
- [IP限定ログイン]
- [ローカル サーバ証明書]
- [ローカル/匿名アクセス]
- 信頼モード
- [信頼された管理サーバ]
- [ユーザ グループ]

関連項目

- [設定]ページ

[IP バインド]

IPバインドは、HP System Management Homepage（HP SMH）がリクエストを受け入れるIPアドレスを指定し、どのネットまたはサブネット経由で送信されたリクエストが処理されるかを制御する手段を提供します。

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。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定義できます。

マスクが適用されると、サーバ上のIPアドレスは、指定されたいずれかのIPバインドアドレスと一致する場合にバインドされます。

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バインドが有効になっていない場合は、すべてのアドレスにバインドされます。

IPバインドを設定するには、以下の手順に従ってください。

1. **[設定]→[HP System Management Homepage]→[セキュリティ]**の順にクリックします。
2. **[IPバインド]**をクリックします。
3. **[IPバインド]**ボックスを選択してIPバインドを有効にします。
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. 現在の設定を保存するには**[設定の保存]**をクリックし、すべての変更をキャンセルするには**[値のリセット]**をクリックします。

   [設定の保存]をクリックすると、次のメッセージが表示されます。

   この値を設定するには、`HP System Management Homepage`**を再起動して ログインしなおす必要があります。**
7. **[OK]**をクリックします。
   - 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。 255.255.0.0, 192.0.0.0, 255.192.0.0.

関連項目

- セキュリティ
- [IP限定ログイン]
- [ローカル サーバ証明書]
- [ローカル/匿名アクセス]
- 信頼モード
- [信頼された管理サーバ]
- [ユーザ グループ]

[IP限定ログイン]

[IP限定ログイン]により、HP System Management Homepage（HP SMH）は、ログ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。

- IPアドレスを除外する設定にした場合、そのIPアドレスは、包含ボックスのリストに含まれていても除外されます。
- IPアドレスが包含リストに含まれている場合、リストにあるIPアドレスだけがログイン アクセスを許可されます（*localhost*は例外）。
- IPアドレスが包含リストに含まれていない場合は、除外リストに含まれていない任意のIP アドレスがログイン アクセスを許可されます。

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. **[設定]→[HP System Management Homepage]→[セキュリティ]**の順にクリックします。
2. **[IP限定ログイン]**をクリックします。
3. **[IP限定ログイン]**ボックスを選択して限定ログインを有効にします。
4. 除外するIPアドレスを入力します。
5. 包含するIPアドレスを入力します。
6. 現在の設定を保存するには**[設定の保存]**をクリックし、すべての変更をキャンセルするには**[値のリセット]**をクリックします。

   [設定の保存]をクリックすると、次のメッセージが表示されます。

   この値を設定するには、`HP System Management Homepage`を再起動して ログインしなおす必要があります。
7. **[OK]**をクリックします。

関連項目

- セキュリティ
- [IP バインド]
- [ローカル サーバ証明書]
- [ローカル/匿名アクセス]
- 信頼モード
- [信頼された管理サーバ]
- [ユーザ グループ]

[ローカル サーバ証明書]

[ローカル サーバ 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 System Management Homepage（HP SMH）で作成された*自己署名の証明書*が、*認証機関（認証機関）*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正しいデータを生成します。このプロセス中、プライベート キーがサーバからなくなることはありません。
- ***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**データが正常に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. **[設定]→[HP System Management Homepage]→[セキュリティ]**の順に選択します。
2. **[ローカル サーバ証明書]**を選択します。
3. オプションの手順として、**[組織]**フィールドや**[組織ユニット]**フィールドのデフォルト値を独自の値（最大64文字）に置き換えることができます。
4. **[PKCS #10データの作成]**をクリックします。**PKCS #10証明書リクエスト** データが正常に作成され、`/opt/hpsmh/sslshare/req_cr.pem`（HP-UX）、`/opt/hp/sslshare/req_cr.pem`（Linux x86およびx86_64上のHP SMH 2.1.4以降の場合、`/opt/hp/hpsmh/data/req_cr.pem`）、または `<systemdrive>\hp\sslshare\req_cr.pem`（HP SMH 2.1.4以降の場合、`<systemdrive>\hp\hpsmh\data\req_cr.pem`）（Windows）に保存されたことを示す画面が表示されます。
5. 証明書データをコピーします。
6. **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。返信データは、Base64コード化フォーマットで作成するように依頼します。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サーバが設置されている場合は、**PKCS #10**データをCAのマネージャに送り、**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。

7. 証明書承認局から証明書承認局から**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]**フィールドに貼り付けます。
8. **[PKCS #7データをインポート]**をクリックします。カスタマ作成証明書が正常に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。
9. HP SMHを再起動します。
10. 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。
11. ブラウザからプロンプトが表示されたら、[証明書を表示]を選択します。ブラウザ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。

注記: 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`/opt/hpsmh/sslshare/req_cr.pem`（HP-UX）、`/etc/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/file.pem`）、または`%SystemDrive%:\hp\sslshare\cert.pem`（Windows）（Windows上のHP SMH 2.1.3以降の場合、`%SystemDrive%:\hp\sslshare\file.pem`）にコピーして、HP SMHを再起動してください。 選択した認証情報署名者が認証情報ファイルを**PKCS #10**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、`/opt/hp/hpsmh/data/req_cr.pem`（Linux x86および x86_64）、`%SystemDrive%:\hp\hpsmh\data\req_cr.pem`（Windows）をコピーして、HP SMHを再起動してください。

関連項目

- ファイアウォールの設定
- セキュリティ
- [IP バインド]

- [IP限定ログイン]
- [ローカル/匿名アクセス]
- 信頼モード
- [信頼された管理サーバ]
- [ユーザ グループ]

マルチホームされた証明書

System Management Homepage（SMH）は、HPが作成していない*証明書*を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）で承認された証明書リクエストを作成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。

1. **[設定]→[System Management Homepage]→[セキュリティ]**を選択します。
2. **[ローカル サーバ証明書]**をクリックします。
3. **[代替名]**フィールド4に値を入力します。
4. **[複数の名前を設定]**をクリックします。

   次のメッセージが表示されます。 **値を設定するには**`System Management Homepage`**を再起動する必要があり、再度ログインする必要があるかもしれません。**
5. **[OK]**をクリックします。

次のリクエストで、サーバが再起動して、ログイン ページに移動します。 この場合、新しい認証情報と別名のセットがブラウザでネゴシエートされます。

注記: 要求される認証情報の別名のデフォルトの値は、SMHの現在の認証情報で設定したものと同じですが、このフィールドは*証明書リクエスト*をエクスポートするために必要に応じて変更することができます。

関連項目

- [ローカル サーバ証明書]
- ファイアウォールの設定
- セキュリティ
- [IP バインド]
- [IP限定ログイン]
- [ローカル/匿名アクセス]
- 信頼モード
- [信頼された管理サーバ]
- [ユーザ グループ]

[ローカル/匿名アクセス]

[ローカル/匿名アクセス]アクセスにより、適切な設定を選択できます。

- **[匿名アクセス]** デフォルトは無効です。**[匿名アクセス]**を有効にすると、ログインせずにHP System Management Homepage（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 ユーザが、ユーザ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制限されたアクセス権を持ちます。

注意：[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]**　デフォルトは無効です。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。

  注意：[ローカルアクセス]は、ユーザの管理サーバ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. **[設定]→[System Management Homepage]→[セキュリティ]**の順に選択します。
2. **[ローカル/匿名アクセス]**を選択します。
3. **[匿名アクセス]**を選択します。
4. **[設定の保存]**をクリックして設定を保存します。

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. **[設定]→[HP System Management Homepage]→[セキュリティ]**の順に選択します。
2. **[ローカル/匿名アクセス]**を選択します。
3. **[ローカル アクセス]**を選択してローカル アクセスを有効にします。
4. **[匿名]**または**[管理者]**を選択します。
5. **[設定の保存]**をクリックして設定を保存します。

関連項目

- セキュリティ
- [IP バインド]
- [IP限定ログイン]
- [ローカル サーバ証明書]
- 信頼モード
- [信頼された管理サーバ]
- [ユーザ グループ]

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。場合によっては、他の状況よりも高いレベルのセキュリティが必要になることがあるため、次に示すセキュリティ オプションが提供されています。

- **[証明書による信頼]**　信頼済み*証明書*を持つHP Systems Insight Manager（HP SIM）サーバからの設定変更だけを受け入れるようにHP System Management Homepage（HP SMH）を設定できます。このモードでは、指定されたサーバが証明書による認証を受ける必要があります。このモードは証明書を必要とし、アクセスを許可する前にデジタル署名を確認するため、最も強力なセキュリティ手段です。どのようなリモート設定変更も有効にしない場合は、**[証明書による信頼]**を選択した状態で、すべての証明書のインポートを避けて信頼済みシステムのリストを空の状態にしておいてください。

注記:　これは、Linux Itaniumのデフォルトの動作です。

注記:　セキュリティ向上の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。このオプション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が2つの部門の2つの管理者グループに分かれていて、一方のグループで誤ったシステムへのソフトウェアのインストールを

防ぎたいというような場合があります。あるグループが誤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ぐことができます。このオプションは、指定したHP SIMサーバだけを確認します。

注記: 他のオプションはセキュリティが低くなるため、**[証明書による信頼]**オプションを使用することをおすすめします。

- **すべて信頼（Trust All）** どのシステムから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。

注記: 他のオプションはセキュリティが低くなるため、**[証明書による信頼]**オプションを使用することをおすすめします。

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。

注記: 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。

[証明書による信頼]を設定するには、以下の手順に従ってください。

1. **[設定]→[HP System Management Homepage]→[セキュリティ]**の順に選択します。
2. **[信頼モード]**をクリックします。
3. 信頼済み証明書を要求する**[証明書による信頼]**を選択します。
4. 現在の設定を保存するには**[設定の保存]**をクリックし、すべての変更をキャンセルするには**[値のリセット]**をクリックします。
5. **[信頼された証明書]**をクリックして信頼された管理サーバ証明書にアクセスします。

[名前による信頼]を設定するには、以下の手順に従ってください。

1. **[設定]→[HP System Management Homepage]→[セキュリティ]**の順に選択します。
2. **[信頼モード]**をクリックします。
3. HP SIMの名前で信頼するには、**[名前による信頼]**を選択します。
4. HP SIMの証明書名を入力します。
5. 現在の設定を保存するには**[設定の保存]**をクリックし、すべての変更をキャンセルするには**[値のリセット]**をクリックします。

HP SIMサーバの認証情報名オプションは、次の条件を満たす必要があります。

- 各HP SIMサーバ認証情報名の最大長は64文字です。
- HP SIMサーバの認証情報名リスト全体の最大長は1,024文字です。
- *SIM**の証明書名***に、~ ' ! @ # $ % ^ & * ( ) + = \ " : ' < >> ? , | のような特殊文字は使用できません。
- *SIM**の証明書名***は、セミコロンで区切ります。

[すべてを信頼]を設定するには、以下の手順に従ってください。

1. **[設定]→[HP System Management Homepage]→[セキュリティ]**の順に選択します。
2. **[信頼モード]**をクリックします。
3. すべてのサーバを信頼する**[すべてを信頼]**を選択します。

4. 現在の設定を保存するには**[設定の保存]**をクリックし、すべての変更をキャンセルするには**[値のリセット]**をクリックします。

関連項目

- 証明書の自動インポート
- セキュリティ
- [IP バインド]
- [IP限定ログイン]
- [ローカル サーバ証明書]
- [ローカル/匿名アクセス]
- [信頼された管理サーバ]
- [ユーザ グループ]

[信頼された管理サーバ]

[信頼された管理サーバ]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。

- **[証明書データのインポート]**　証明書は、HP Systems Insight Manager（HP SIM）とHP System Management Homepage（HP SMH）の間の信頼関係を確立するために使用されます。
- **[サーバから証明書の追加]**　HP SIMサーバ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. **[設定]→[System Management Homepage]→[セキュリティ]→[信頼された管理サーバ]**の順に選択します。
2. **[サーバから証明書の追加]**の領域に、追加する証明書があるHP SIMサーバの名前またはIPアドレスを入力します。
3. **[証明書データのインポート]**の領域に、Base64コード化証明書を切り取ってテキスト ボックスに貼り付けます。
4. **[証明書データのインポート]**をクリックします。

サーバ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. **[設定]→[System Management Homepage]→[セキュリティ]→[信頼された管理サーバ]**の順に選択します。
2. **[サーバから証明書の追加]**の領域に、追加する証明書があるHP SIMサーバの名前を入力します。

   この手順は、次の手順で使用されたBase64コード化証明書がサーバ名を提供しているときは任意となります。
3. **[サーバから証明書の追加]**をクリックします。証明書がリストに追加される前に、検証/確認のために証明書情報が表示されます。
4. **[証明書の確認]**ウィンドウの証明書情報を確認し、その証明書を信頼済み証明書リストに追加する場合は、**[証明書の追加]**をクリックします。

関連項目

- セキュリティ
- [IP バインド]
- [IP限定ログイン]
- [ローカル サーバ証明書]
- [ローカル/匿名アクセス]
- 信頼モード
- [ユーザ グループ]

[ユーザ グループ]

HP System Management Homepage（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rootに含まれている）のユーザは、**[管理者]**、**[オペレータ]**、または**[ユーザ]**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つの異なるオペレーティング システム グループに割り当てることができます。HP SMHのインストールでは、オペレーティング システム グループをHP SMHに割り当てることができます。OSで定義されたオペレーティング システム グループがHP SMHの起動時に定義されていない場合は、定義されていないオペレーティング システム グループが、System Management Homepageのログ メッセージによって示されます。

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。管理者権限を持つHP SMHユーザは、HP SMHの各アクセス レベルに対してオペレーティング システム ユーザ グループを指定できます。 これにより、各オペレーティング システム ユーザ グループに含まれるすべてのアカウントは、**ユーザ グループ**ウィンドウで指定されたHP SMHへのアクセス権を持ちます。Windowsの管理者グループ、Linuxのルート グループ、およびHP-UX rootグループには、自動的に、HP System Management Homepageへの管理者アクセス権が割り当てられます。HP-UXでは、rootユーザのみ自動的にAdministratorsクラスに割り当てられます。rootグループのすべてのユーザ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 グループ]ウィンドウにより、ユーザ グループをHP SMHに追加できます。以下のレベルのユーザ 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 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　[オペレータ]**アクセス権を持つユーザは、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　[ユーザ]**アクセス権を持つユーザは、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]**アクセス権を持つユーザに対して制限されています。

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. **[設定]→[HP System Management Homepage]→[セキュリティ]**の順に選択します。
2. **[ユーザ グループ]**をクリックします。
3. **[管理者]**セクションで、ユーザ グループ名を入力します。
4. 現在の設定を保存するには**[設定の保存]**をクリックし、フィールド内を消去するには**[すべてのグループのクリア]**をクリックし、すべての変更をキャンセルするには**[値のリセット]**をクリックします。

オペレータ 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. **[設定]→[HP System Management Homepage]→[セキュリティ]**の順に選択します。
2. **[ユーザ グループ]**をクリックします。
3. **[オペレータ]**セクションで、ユーザ グループ名を入力します。
4. 現在の設定を保存するには**[設定の保存]**をクリックし、フィールド内を消去するには**[すべてのグループのクリア]**をクリックし、すべての変更をキャンセルするには**[値のリセット]**をクリックします。

ユーザ 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. **[設定]→[HP System Management Homepage]→[セキュリティ]**の順に選択します。
2. **[ユーザ グループ]**をクリックします。
3. **[ユーザ]**セクションで、ユーザ グループ名を入力します。
4. 現在の設定を保存するには**[設定の保存]**をクリックし、フィールド内を消去するには**[すべてのグループのクリア]**をクリックし、すべての変更をキャンセルするには**[値のリセット]**をクリックします。

関連項目

- セキュリティ
- [IP バインド]
- [IP限定ログイン]
- [ローカル サーバ証明書]
- [ローカル/匿名アクセス]
- 信頼モード
- [信頼された管理サーバ]

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

注記: 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。

System（HP-UXのみ）

このカテゴリでは、ログインせずにシステム上でコマンドを容易に実行することが可能な、あらかじめ組み込まれた4つのタスクが提供されます。

- **[Launch X Application]**リンクを使用すると、Xアプリケーションを起動するオプションが表示されます。起動するXアプリケーションのコマンド行を入力します。コマンドはログインしたユーザのユーザIDで実行されるため、すべてのHP SMHユーザがこのタスクを実行できます。
- **[Launch X Application as Root]**リンクを使用すると、Xアプリケーションをroot権限で起動するためのオプションが表示されます。起動するXアプリケーションのコマンド行を入力します。このタスクを実行するには、HP SMH管理者権限を持つユーザとしてログインしてください。
- **[Run Command]**リンクを使用すると、コマンド実行のオプションが表示されます。コマンドはログインしたユーザのユーザIDで実行されるため、すべてのHP SMHユーザがこのタスクを実行できます。
- **[Run Command as Root]**リンクを使用すると、root権限でのコマンド実行のオプションが表示されます。このタスクを実行するには、HP SMH管理者権限を持つユーザとしてログインしてください。

関連項目

- [ホーム]ページ
- [設定]ページ
- [ツール]ページ
- [ログ]ページ

第7章 [ツール]ページ

[ツール]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システム マネジメント ツールへのリンクが表示されます。 HP-UXの場合、**[ツール]**ページでは、*System Administration Manager*（SAM）のメインページ（SAM Functional Area Launcher（FAL）とも呼ばれます）に類似した管理ツールへのエントリ ポイントが提供されます。HP-UXの場合、このページにはXベースの管理アプリケーション用のカテゴリとメニューもいくつか含まれています。 **[ツール]**ページには、以下のリンクが表示されます。

- ユーザおよびグループのアカウント
- 監視設定
- 認証コマンド（PAM）
- ディスクおよびファイル システム
- Distributed Systems Authentication Utilities（DSAU）
- Evweb
- IPMIイベント ビューア
- カーネル設定
- ネットワークおよび通信
- nPartition Management
- 周辺装置
- プリンタ管理
- リソース管理
- Resource Monitor
- Serviceguard
- ソフトウェア管理
- 時刻

注記: これらの各機能領域には、それぞれに関連するオンライン ヘルプがあります。

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

関連項目

- [ホーム]ページ
- [設定]ページ
- [タスク]ページ
- [ログ]ページ

第8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
- System Management Homepageレガシー ログ（LinuxおよびWindowsのみ）
- SAMログ ビューワ（HP-UXのみ）
- System Management Homepageエラー ログ（HP-UXのみ）

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*の任意のログを、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（DSA）ユーティリティ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。

関連手順

- System Management Homepageログ
- System Management Homepageレガシー ログ
- SAMログ
- 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
- [ツール]ページ

System Management Homepageログ

[System Management Homepageログ]には、*HP System Management Homepage*（HP SMH）レベルの設定変更とログ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）からログインするときの、ログ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。

注記:　[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。

[System Management Homepageログ]にアクセスするには、**[ログ]→[System Management Homepage]→[System Management Homepageログ]**の順に選択してください。

関連項目

- [ログ]ページ
- System Management Homepageレガシー ログ
- SAMログ
- エラー ログ

System Management Homepageレガシー ログ

HP System Management Homepage（HP SMH）をインストールする前にLinuxまたはWindowsシステムにに 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た場合は、**System Management Homepage**カテゴリの**[System Management Homepageレガ**

シー ログ]リンクによってそのログを表示することができます。このログには、新しいバージョンをインストールする前に発生したイベントに関するセキュリティ関連の履歴情報が含まれています。HP-UXはレガシー ログを含みません。

System Management Homepageの従来のログにアクセスするには、**[ログ]→[System Management Homepage]→[System Management Homepageレガシー ログ]**の順に選択してください。

注記: **[System Management Homepageレガシー 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。

関連項目

- [ログ]ページ
- System Management Homepageログ
- SAMログ
- エラー ログ

SAMログ

[SAM Log]リンクを使用すると、**[SAM Log Viewer]**にアクセスできます。SAM Log Viewerでは、*HP-UX System Administration Manager*（SAM）ログ ファイルへのWebインタフェースを提供します。新しいWebベースの管理アプリケーションと既存のSAMアプリケーションがこのログ ファイルを使用します。

注記: **[SAMログ]**は、HP-UXシステムのみで使用可能です。

SAM Logにアクセスするには、**[ログ]→[SAM Log]→[SAM Log Viewer]**の順に選択します。

SAMログからのメッセージをフィルタするには、フィルタ条件を選択し、[OK]をクリックします。画面の下にメッセージが表示されます。

関連項目

- [ログ]ページ
- System Management Homepageログ
- System Management Homepageレガシー ログ
- エラー ログ

エラー ログ

[System Management Homepageエラー ログ]には、System Management Homepageモジュールと CGI実行エラー（`stderr`）で生成されたエラー情報が含まれます。

注記: **[System Management Homepageエラー ログ]**は、HP-UXシステムのみで使用可能です。

[System Management Homepageエラー 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。

System Management Homepageエラー ログにアクセスするには、**[ログ]→[System Management Homepage]→[System Management Homepageエラー ログ]**の順に選択してください。

関連項目

- [ログ]ページ
- System Management Homepageログ

- System Management Homepageレガシー ログ
- SAMログ

第9章　トラブルシューティング

注記:　このトピックは、HP-UX、Linux、またはWindowsオペレーティング システムに適用されます。

アクセスの問題

セキュリティに関する**SMH**のドキュメントが不明確

解決策: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。

Linuxでホスト名を入力した後、**HP SMH**が開始されない。

解決策： Linuxでは、64文字以上のホスト名をサポートしていません。

HP SMH上部のフレームにあるブレッドクラム リンクは、内部のプラグイン ページの名前を除く、**HP SMH**メニュー構造内のプラグイン名までの現在の位置のみ表示されます。

解決策： プラグイン ページ内のボタンおよびリンクを使用して、操作をキャンセルするか、別のプラグイン ページに移動します。

ブラウザの問題

HP SMHにログインしてブラウザを閉じても、**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**?**

解決策： 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）]**のチェックを外します。
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]**タブの下の**[タブ]**、**[タブの中のWebページの表示方法を設定します。]**の**[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。

Windows環境で**Internet Explorer 6.0**を使用しています。 **HP System Management Homepage**（**HP SMH**）にログインするときに**[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**?**

解決策： 表示される可能性のある警告は、次の2つです。

- **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。

2つ目の**Mozilla**ブラウザを開くと、**HP SMH**への不正ログインと表示される場合があります。

解決策： 別々に起動された複数のMozillaブラウザは、セッションを共有します。

注記: 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。

Windows 2003で動作する**Internet Explorer**から**HP SMH**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。

解決策： Windows 2003 Serverでは、Internet Explorer 6.0は、デフォルト インストールでのセキュリティ設定が異なります。 この問題を解決するには、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`**として追加してください。この解決策以外には、ブラウザ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のセキュリティ設定を変更する方法があります。

ブラウザ 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**?**

解決策： 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。

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

解決策： ブラウザのCookieは、ユーザ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。

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。

解決策： 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。

Windows 2003で動作するローカル マシンまたはリモート マシンで**`https://`*IPアドレス*`:2381`**にアクセスすると、**[ログイン]**画面が表示されません。

解決策： Windows 2003でInternet Explorer 6.0を使用している場合、完全な**[ログイン]**ページが表示される代わりに、青色のバーに**[アカウント ログイン]**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 システム上からブラウズしたときに発生し、以下の方法で解決できます。

HP System Management Homepageは、javascriptサポートを有効にして、このサイトを信頼済みサイトに追加するまで、このページを表示しません。

HP SMH（バージョン**2.1.5**以前）を使用しているときは、ブラウザ ウィンドウの**[戻る]**ボタンは正しく動作しません。 **[戻る]**ボタンを押すと、前のページが表示されずに現在のページが更新されます。

注記: Itanium用のLinuxでは、バージョン2.1.7までこのように動作します。

解決策： HP SMH内でページを移動する方法として、ブラウザの**[戻る]**ボタンはサポートされません。 HP SMHをナビゲートするには、ブレッドクラム リンク、ナビゲーション ボタン、およびHP SMHページ内で提供されたリンクを使用します。

クラスタの問題

クラスタのフェールオーバが発生した後に、クラスタの**IP**アドレスの**HP SMH**にアクセスできなくなりました。

解決策： HP SMH 2.1.4（SmartStart 7.5以降で利用可能）以降をインストールするか、クラスタに適応させるようにXMLファイルを変更します。

以下の手順を実行することをおすすめします。

1. 念のため、既存のsmhpd.xmlファイルを別のディレクトリにコピーします。
2. 手動でタグを追加します。
   a. 起動ドライブの\hp\hpsmh\confディレクトリのsmhpd.xmlをテキスト エディタで開きます。
   b. <system-management-homepage>と</system-management-homepage>タグの間に次の行を追加します。

      ```
      <monitor-ip-changes>1</monitor-ip-changes>
      ```

   c. ファイルを保存します。
3. クラスタ フェールオーバのターゲットとなるすべてのシステムでこの手順を行います。
4. 両方のシステムのHP SMHサービスを再起動します。

インストールの問題

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。

解決策： 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 Systems Insight Manager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。

HP System Management Homepage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。

解決策： HP SMHのインストール プログラムが、以前に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。

HP System Management Homepageをインストールしていると、**「`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.`」**というエラーが表示されました。

解決策： このエラーは、Linuxシステムでインストール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。

IPアドレスの問題

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

*解決策：*はい、あります。**`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、ブラウザでプロキシ サーバを設定している場合は、ブラウザ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。

Windows 2000 Advanced Serverで**[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**?**

解決策： Microsoft Windows NT 4.0およびWindows 2000 Advanced Serverの場合、ローカル マシンを包含または除外するには、サーバの実際の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]**セクションに含まれています。 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除外されます。

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**?**

解決策： ほとんどのユーザはローカル 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。

[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。

*解決策:*ユーザが誤って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。

ログイン時の問題

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 System Management Homepage**（**SMH**）バージョン**2.1.3**（以降）を実行している**ProLiant**サーバで**Microsoft Windows**オペレーティング システムにログオンした後、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。

（ドライブ）：`\hp\hpsmh\bin\rotatelogs.exe`

解決策： コマンド プロンプト ウィンドウは、サーバや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。

Microsoft Windows 2000 ServerまたはMicrosoft Windows Server 2003（すべてのバージョン）とHP System Manhagement Homepage（SMH）バージョン2.1.3（以降）で構成されたすべてのProLiantサーバで、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。

SMHがサーバ 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]**のチェックを外します。
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。

HP SMH ユーザ 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 グループに権限を与えましたが、そのグループのユーザがログインできない、または**HP SMH**での権限が正しくない。

*解決策：*HP SMHは、Windowsで事前に定義された4つのユーザ グループ、**Administrators**、**Users**、**Guests**、および**Power Users**のみ認識します。 **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。

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**にログインすると、ログインに失敗する。

*解決策：*Windowsシステムのユーザ 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。対処方法は、新しいグループを作成し、HP SMHへのアクセス権を与えます。

Windowsオペレーティング システムを実行しているサーバで**HP SMH**にログインできません。

解決策：

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、ログインが**[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 システムにログインします。 メッセージが表示されたら、パスワードを変更します。

注記: 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 グループの管理者は、**[ユーザは次回ログ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 アカウントを設定しています。

オペレーティング システムの管理者は、将来作成される任意のログインを、**[ユーザは次回ログ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にログ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。

Windows XPオペレーティング システム環境で**HP SMH**にログインできません。

解決策：

- **[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。

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**?**

解決策： HP SMH v2.0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3つの固定アカウント（管理者、オペレータ、およびユーザ）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 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。

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ログインすることができません。

解決策： 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、**[ユーザ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ないと、アカウントを使用してHP SMHにログインすることはできません。

Windows環境で**Internet Explorer 6.0**を使用しています。 管理サーバを経由して**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**にログインできません。 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。

解決策： この問題は、次の2つの方法で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。

  または

- 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。

Internet Explorerでサーバ名（**`http://`サーバ名`: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名とパスワードを使用してもログインできません。 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ログインできます。

解決策： サーバのコンピュータ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。

セキュリティの問題

Windows XPシステムを**Service Pack 2**で更新すると**HP Systems Insight Manager**または**HP** バージョン コントロール レポジトリ マネージャにアクセスできなくなりました。 原因は何ですか**?**

解決策： 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、ブラウザがHP Systems Insight Managerおよびバージョン コントロール レポジトリ マネージャ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、ブラウザがHP Systems Insight Managerとバージョン コントロール レポジトリ マネージャによって使用されるポートにアクセスできるようにする必要があります。

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。

   製品名およびポート番号をそれぞれ入力する必要があります。

   ファイアウォール保護に、次の例外を追加します。

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

5. **[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。
6. **[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 Systems Insight Managerおよびバージョン コントロール レポジトリ マネージャ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 マネージャに、ポート280および5000はHP Systems Insight Managerに必要です。 アプリケーションで正しく通信するには、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。

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**?**

解決策： 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、CAに提供される必要があります。ほとんどの認証機関は、**[設定]→[HP System Management Homepage]→[セキュリティ]→[ローカル サーバ 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。

PKCS #7証明書データが受け入れられないのはなぜですか**?**

解決策： Mozillaブラウザを使用している場合、メモ帳や他のエディタ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、必ず、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、必ず、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。

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**?**

解決策： 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。

[設定]、**[システム マネジメント ホームページ]**、**[セキュリティ]**、**[信頼された 管理サーバ]**の順に選択して、カスタマ作成証明書の**PKCS #7**データを**[HP Systems Insight Manager** 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**?**

解決策： カスタマ作成証明書のPKCS #7データが**[信頼された管理サーバ]**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 証明書]**の順に選択して、.**PKCS #7**データを**[カスタマ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 Systems Insight Managerサーバ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]」を参照してください。

Windows 2003認証機関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**?**

解決策： Windows 2003認証機関を使用して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]→[HP System Management Homepage]→[セキュリティ]→[ローカル サーバ 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）に移動します。
   - **[証明書を要求する]**を選択します。
   - **[証明書の要求の詳細設定]**を選択します。
   - **[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。
   - **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。
   - **[プログラム]→[管理ツール]→[証明機関]**の順にクリックします。
   - **[CA（Local）]**、**[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。
   - 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）に移動します。
   - **[保留中の証明書の要求の状態]**を選択します。
   - **[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）。

     ダウンロード ファイルは、certnew.cerです。
   - certnew.cerというファイル名をcert.pemに変更します。

その他の問題

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

解決策： 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。

[管理プロセッサ]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**?**

解決策： マネジメント プロセッサの管理者は、ポート80以外のポートを使用するようにマネジメント プロセッサ上のWebサーバを設定しています。 HP SMHでは、現在、このパラメータにアクセスできず、マネジメント プロセッサがポート80上にあると想定されています。

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**?**

解決策： 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。

注記: United Linux 1.0またはSUSE SLES 8環境では、su -でルート アクセスを模倣して再インストールすることはできません。

Serviceguard Managerプラグインで、**[Display Consolidated Syslog]**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。

解決策：「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。

[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実際に存在するスワップ領域と、実際のメモリ 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。

解決策： 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 System Management Homepage（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のリソースを提供すします。

- 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、適用されたすべての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10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。当社は、本書に関して特定目的の市場性と適合性に対する保証を含む一切の保証をいたしかねます。

当社は、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。

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 ソフトウェアは秘密情報であり、 その所有、使用、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 ソフトウェア、コンピュータ 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コンピュータのHP-UX Release 10.20以上とHP-UX Release 11.00以上（32ビット設定と64ビット設定の両方）は、Open Group UNIX 95ブランド製品です。

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。内容の小さな変更に対しては増刷の際に対応し、出版日の変更は行いません。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。新版の作成は、記載内容の訂正もしくはドキュメント製品の変更にともなって行われます。新版の作成は、記載内容の訂正もしくはドキュメント製品の変更にともなって行われます。詳細については、HP販売担当者に問い合わせてください。

本書に関するフィードバックは、次の当社Webサイトのフィードバックページからお寄せください。

http://docs.hp.com/ja/feedback.html

リビジョン履歴

出版履歴

改訂 第15版 2007年12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
製品番号: 436304-193。 第10版は、HP SMH v2.1.8リリースで新しいセキュリティの修正を追加し、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リリースでの新しい機能と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 2005年9月
MPN：365395-198。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 2005年6月
MPN：365395-197。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：365395-195。 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：365395-194。 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。
改訂 第1版 2004年11月
MPN：365395-193。第1版は、LinuxとWindowsの情報とタスクを記載しました。

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 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 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。

CA
参照 認証機関.

CLI
参照 コマンド ライン インタフェース.

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 インタフェース.

HP Insightマネジメント エージェント
ユーザが直接その場にいなくても、定期的に情報を収集し、他のサービスを実行するプログラム。

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ベースのインタフェースです。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フェースを提供します。 HP SMHは、HTTPおよびHTTPS経由で通信するHP SMHで使用されるソフトウェアの統合セットです。 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のシステム、クラスタ、デスクトップ、ワークステーション、ポータブルなど、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 ソフトウェアです。HP SIMは、HP Insight マネージャ7、HP Toptools、HP Servicecontrolマネージャ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 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 Systems Insight Manager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 インタフェースです。

HP-UX 11i v3（B.11.31）では、HP SMHがHP-UXシステム管理タスクのプライマリ インタフェースを提供します。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)**
サーバにインストールされたHPのソフトウェアをユーザ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 **(VCRM)**	ユーザ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 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.
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。
parMgr	*参照* Partition Manager.
Partition Manager (parMgr)	HPサーバ 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を使用することで、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 リソースの管理が可能になります。
pdweb	*参照* Peripheral Devicesツール.
Peripheral Devices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 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 Support Packには、ドライバ 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)	ネットワークを介して別のシステムにログインし、そのシステム上でコマンドを実行することを可能にするプログラムです。SSHを使用するとシステム間でファイルを移動することもできます。 また、認証機能やセキュリティ保護されていないチャネル経由で安全に通信する機能を提供します。
Secure Sockets Layer (SSL)	HTTPとTCPの間に位置するプロトコル層。 クライアントとサーバの間のプライバシとメッセージの整合性を実現します。SSLの一般的な使用方法は、サーバの認証です。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。SSLは、アプリケーション プロトコルからは独立しています。
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lsystem-wideおよびper-user（ローカル ユーザおよびNISユーザ）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、クライアント サーバ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。
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.
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（インタフェースなど）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 インタフェース **(GUI)**	コンピュータ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 インタフェース。HP SMHのGUIはWeb対応なので、Webブラウザで表示されます。
コマンド ライン インタフェース **(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 ログイン	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 マネージャとして呼ばれます。すべての管理対象のProLiantまたはIntegrity システムにソフトウェア状態の概要を提供して、それらのシステム上でプログラムによりあらかじめ定義された基準でシステム ソフトウェアとファームウェアをアップデートできます。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確認し、アップグレード可能かを表示し、アップグレードする理由を提供します。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。
マルチホーム	証明書に複数の名前を設定します。
ユーザ	HP System Management Homepageへの有効なログインを持つネットワーク ユーザ。
ユーザアカウント	HP System Management Homepage（HP SMH）にログ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/ドメイン アカウント、HP-UX/Linux のユーザ 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	管理対象クラスタに関する重要な情報（ユーザ、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。
検索基準	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。フィルタは、包含フィルタとその後に続く排除フィルタによって構成されます。これらの2つのフィルタリング操作の結果は、グループと呼ばれます。フィルタの例としては、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。
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。

索引

H
HP SMH
  IP限定ログイン, 28
  IPバインド, 28
  開始するには, 9
  概要, 7
  クレジット, 27
  セキュリティ, 27
  設定, 25
  タイムアウトの設定, 15
  タスク, 37
  ツール, 39
  匿名アクセス, 31
  トラブルシューティング, 45
  ナビゲート, 19
  ファイアウォールの設定, 13
  ページ, 20
  [ホーム], 21
  マルチホームされた証明書, 31
  メニュー, 25, 26
  ユーザ グループ, 35
  ローカル アクセス, 31
  ローカル サーバ証明書, 29
  ログ, 41, 42
  ログアウト, 18
  ログイン, 9

S
SAM
  ログ, 42

U
U.S. government license, 55

あ
アクセス
  信頼関係, 13

え
エラー
  ログ, 42

か
開始するには
  ログアウト, 18
概要
  HP SMH, 7
  使用開始, 9

く
クレジット
  HP SMH, 27

こ
ご注意, 55

さ
参照
  トラブルシューティング, 53

し
出版履歴, 55
使用開始
  信頼関係, 13
  タイムアウトの設定, 15
  ログイン, 9
商標, 55
証明書
  証明書の自動インポート, 17
  信頼された管理サーバ証明書, 34
  信頼モード, 32

せ
セキュリティ
  HP SMH, 27
  IP限定ログイン, 28
  IPバインド, 28
  証明書の自動インポート, 17
  信頼関係, 13
  信頼された管理サーバ証明書, 34
  信頼モード, 32
  タイムアウトの設定, 15
  匿名, 31
  マルチホームされた証明書, 31
  ユーザ グループ, 35
  ローカル アクセス, 31
  ローカル サーバ証明書, 29
設定
  HP SMH, 25

た
タイムアウト
  タイムアウトの設定, 15
タスク
  HP SMH, 37

ち
著作権, 55

つ
ツール
  HP SMH, 39

と
トラブルシューティング
  HP SMH, 45
  参照, 53

な
ナビゲート
  HP SMH, 19

ふ
ファイアウォール
　ファイアウォールの設定, 13

へ
ページ
　HP SMH, 20

ほ
[ホーム]
　HP SMH, 21
保証, 55

め
メニュー
　HP SMH, 25, 26

も
問題
　信頼関係, 13

り
リリース履歴, 55

ろ
ログ
　HP SMH, 41
　HP SMHレガシー ログ, 41
　SAMログ, 42
　System Management Homepageログ, 41
　エラー ログ, 42