HP System Management Homepage

製品番号：365395-194

2005年5月, 2 版

目次

製品の概要

製品の概要

System Management Homepageは、単一システム管理用の統合インタフェースを提供するWebベースのアプリケーションです。System Management Homepage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。

System Management Homepageは、HP-UX、Microsoft® Windows®オペレーティング システム環境およびLinuxオペレーティング システム（IA32 AMD64およびIntel Itanium）環境にインストールできます。

- HP-UXオペレーティング システム環境では、System Management Homepageは、デフォルト設定でインストールされます。`/opt/hpsmh/lbin/envvars`および`/opt/hpsmh/conf/timeout.conf`スクリプトの環境変数で変更できます。
- Linuxオペレーティング システム環境では、System Management Homepage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`にあるPerlスクリプトによって変更できます。
- 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System Management Homepageを設定できます。

注:

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『System Management Homepageインストール ガイド』を参照してください。

追加資料

追加資料は、これらのWebサイトに掲載されています。

- Software Depot homehttp://www.hp.com/go/softwaredepotのSystem Management Homepage
- HP ProLiant Server Management Softwareページhttp://www.hp.com/servers/manage

関連トピック

- System Management Homepageの概要
- 開始するには

開始するには

System Management Homepageの使用を開始する際は、System Management Homepage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 グループ項
2. 信頼モードを設定します。 - 信頼モード項
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/匿名アクセス項

関連手順

- ログイン
- ログアウト

関連トピック

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

ログイン

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

Internet Explorerを使用してSystem Management Homepage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:

デフォルトの設定を変更して`autostart`を無効にし`start on boot`を有効にしていて、HP-UXシステムを参照するのにInternet Explorerを使用している場合は、ポート2381を使用してください。デフォルトのインストール設定のままの場合は、次のURIを使用してください。 **`http://ホスト名:2301/`**

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System Management Homepage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。

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『System Management Homepageインストール ガイド』を参照してください。

2. このリンクに初めてアクセスすると、サーバを信頼するかどうかを尋ねる[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、System Management Homepage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:

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。

HP Systems Insight Managerからリンクを使用してこのページにアクセスしている場合、System Management Homepageで[証明書による信頼]オプションが有効になっていて、信頼が設定されていないと、[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。 HP Systems Insight Managerの証明書の自動インポートについて詳しくは、証明書の自動インポート項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るユーザ名を入力します。

   ユーザ グループをSystem Management Homepageのセキュリティ設定に追加していない場合、ユーザは、[administrators]グループ（Windows）またはオペレーティング システム グループ[root]（HP-UXおよびLinux）（デフォルトでユーザrootに含まれている）のオペレーティング システム アカウントでログインする必要があります。 証明書が認証されない場合、ユーザのアクセスは拒否されます。

注:

ほとんどの場合、[administrators]（Windows）および[root]（HP-UXおよびLinux）は、System Management Homepage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を使用してSystem Management Homepageにログインするには、以下の手順に従ってください。

1. **http://ホスト名:2381/**にナビゲートします。

   デフォルトの設定を変更して`autostart`を無効にし`start on boot`を有効にしていて、HP-UXシステムを参照するのにMozillaを使用している場合は、ポート2381を使用してください。 デフォルトのインストール設定のままの場合は、次のURIを使用してください。
   http://ホスト名:2301/

   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System Management Homepage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。

   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『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System Management Homepage 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。

   [匿名]アクセスが有効になっていない場合は、[アカウント ログイン]ページが表示され、その後に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るユーザ名を入力します。

   ユーザ グループをSystem Management Homepageのセキュリティ設定に追加していない場合、ユーザは、[administrators]グループ（Windows）またはオペレーティング システム グループ[root]（HP-UXおよびLinux）（デフォルトでユーザrootに含まれている）のオペレーティング システム アカウントでログインする必要があります。 証明書が認証されない場合、ユーザのアクセスは拒否されます。

注:

ほとんどの場合、[administrators]（Windows）および[root]（HP-UXおよびLinux）は、System Management Homepage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。

関連トピック

- ログアウト
- 証明書の自動インポート

ログアウト

System Management Homepageからログアウトするには、いくつかの方法があります。

- System Management Homepage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。

  System Management Homepageログインが表示されます。

- System Management Homepage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。

関連トピック

- ログイン

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 Systems Insight ManagerシステムからSystem Management Homepageにアクセスする際にHP Systems Insight Manager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:

HP Systems Insight Managerの証明書を自動的にインポートするには、System Management Homepage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 Systems Insight Manager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。

   System Management Homepage（[設定]-[セキュリティ]-[信頼モード]ウィンドウ）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 Systems Insight Manager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 Systems Insight Manager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 Systems Insight Manager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。

System Management HomepageがHP Systems Insight Manager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、System Management Homepage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。

注:

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。証明書は、[信頼された証明書リスト]に追加されます。

関連トピック

- ログイン
- ログアウト
- ローカル/匿名アクセス
- ローカル サーバ証明書
- 信頼された管理サーバ
- ユーザ グループ

ソフトウェアのナビゲート

はじめに

System Management Homepage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、System Management Homepageには、各種のボックスが表示され、各ボックスの境界が、ボックスに含まれている項目のステータスを示します。詳しくは、[ホーム]タブの「ソフトウェアのステータス」を参照してください。

System Management Homepage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]
- [データ フレーム]

[ヘッダ フレーム]

[ヘッダ フレーム]は、表示中のタブ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。

- タブSystem Management Homepageタブには、次のものが含まれます。
  - [ホーム]タブ
  - [設定]タブ
  - [タスク]タブ
  - [ツール]タブ
  - [ログ]タブ
- [サポート]　[サポート]リンクにより、[ProLiant Server Management]ページにアクセスできます。[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リソースを提供するために用意されています。サポートにアクセスするには、HPのWebサイトhttp://www.hp.com/jp/servers/manageを参照してください。
- [フォーラム]　HP製品についてのご質問は、HPサポート フォーラムにお問い合わせください。HPサポート フォーラムにアクセスするには、HPのWebサイトhttp://forums.itrc.hp.com（英語）を参照してください。

- [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。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、[システム モデル]に[不明]と表示されることもあります。
- [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 システム ベース ユーザの場合は、[ログアウト]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]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。

関連トピック

- [ホーム]タブ
- [設定]タブ
- [タスク]タブ
- [ツール]タブ
- [ログ]タブ

タブ

System Management Homepage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]タブおよび[ツール]タブは、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。

System Management Homepageでは、次のタブを表示できます。

- [ホーム]タブ
- [設定]タブ
- [タスク]タブ
- [ツール]タブ
- [ログ]タブ

関連トピック

- [ホーム]タブ
- [設定]タブ
- [タスク]タブ
- [ツール]タブ
- [ログ]タブ

System Management Homepageの概要

System Management Homepage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、System Management Homepageには、各種のボックスが表示され、各ボックスの境界が、ボックスに含まれている項目のステータスを示します。詳しくは、[ホーム]タブの「ソフトウェアのステータス」を参照してください。

System Management Homepage内のナビゲートについては、ソフトウェアのナビゲートを参照してください。

関連トピック

- タブ
- [ホーム]タブ
- [設定]タブ
- [タスク]タブ
- [ツール]タブ
- [ログ]タブ

[ホーム]タブ

[ホーム]タブは、System Management Homepageに表示されます。[ホーム]タブには、次の情報が表示されます。

- システム ステータス サマリ
- ソフトウェアのステータス
- 構成メニュー

注:

HP Webベース システム マネジメント ソフトウェアで利用できる情報によっては、コンピュータ、システム、オペレーティング システム、およびネットワークを含む他の情報ボックスが表示されます。

システム ステータス サマリ

[システム ステータス サマリ]ボックスには、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]ボックスには[障害/劣化アイテムは存在しません]と表示されます。

ソフトウェアのステータス

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、[ステータス]ボックスに表示されるように設定されています。各ボックスには、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。

ステータス ボックス インジケータ

インジケータ	説明
青色	不明
緑色	OK
黄色	劣化
橙色	故障
灰色	ステータスなし

構成メニュー

[ホーム]タブ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。

- [システム モデル]　HP-UXの場合、System Management Homepageを実行しているシステムのモデルの一覧が表示されます。
- [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。

  注：参加者は、System Management Homepageに含まれている情報を提供するエージェントです。
- [その他のエージェント]　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。
- [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。
- その他のソフトウェア/その他のリンク　ProLiant Essentials Value Added Softwareを含むソフトウェア情報を掲載したHPのWebサイトhttp://www.hp.com/jp/servers/proliantessentials上に各ソフトウェアのページへのリンクを含むValue Added Softwareに関する情報が提供されています。
- 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。
  - OK
  - 劣化
  - 故障
  - 不明

関連トピック

- [設定]タブ
- [タスク]タブ
- [ツール]タブ
- [ログ]タブ

[設定]タブ

このセクションには、各種HP Webベース システム マネジメント ソフトウェアの設定または設定ページへのリンクが含まれています。System Management Homepageをインストールすると、[System Management Homepage]セクションだけが表示され、System Management Homepageの設定を表示または編集することができます。

[System Management Homepage]セクション

このセクションには、System Management Homepageを設定するためのリンクと次のリンクが表示されます。

- [クレジット]項　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]項　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

- IPバインド
- IP限定ログイン
- ローカル/匿名アクセス
- 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

関連トピック

- [ホーム]タブ
- [タスク]タブ
- [ツール]タブ
- [ログ]タブ

[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。

関連トピック

- [ホーム]タブ
- [設定]タブ
- [タスク]タブ
- [ツール]タブ
- [ログ]タブ

[セキュリティ]

[System Management Homepage - セキュリティ]リンクでは、次のセキュリティ オプションが提供されます。

- 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。
- 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。

関連手順

- IPバインド
- IP限定ログイン
- ローカル/匿名アクセス
- 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

関連トピック

- [ホーム]タブ
- [設定]タブ
- [タスク]タブ
- [ツール]タブ
- [ログ]タブ

IPバインド

IPバインドは、System Management Homepage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]ページで指定されたアドレスだけにバインドするようにSystem Management Homepage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:

System Management Homepage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、System Management Homepage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]->[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。[IPバインド]ページが表示されます。
3. [IPバインド]を選択してIPバインドを有効にします。
4. 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、`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.

関連トピック

- IP限定ログイン
- ローカル/匿名アクセス
- 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

IP限定ログイン

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

アドレス制限はインストール時に設定できます。 また、管理者は、[IP限定ログイン]ページで設定できます。

- 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]->[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。[IP限定ログイン]ページが表示されます。
3. [IP限定ログイン]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、`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。

関連トピック

- IPバインド
- ローカル/匿名アクセス
- 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

ローカル サーバ証明書

[ローカル サーバ 証明書]ページにより、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、System Management Homepage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、System Management Homepage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System Management Homepage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）または`/opt/hpsmh/sslshare/cert.pem`ファイル（HP-UXおよびLinux）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]->[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）、または`c:\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。
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：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データをコピーして、[PKCS #7データ]フィールドに貼り付けます。この場合、次の手順は省略してください。
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. System Management Homepageを再起動する。
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：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/req_cr.pem（HP-UX）、/opt/hp/sslshare/req_cr.pem（Linux）、またはc:\hp\sslshare\req_cr.pem（Windows）にコピーして、System Management Homepageを再起動してください。

関連トピック

- 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System Management Homepageにアクセスできます。

  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System Management Homepage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。[匿名]を選択すると、任意のローカルユーザが、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：ローカル アクセスの使用は、管理サーバ ソフトウェアが許可していない場合にはおすすめできません。

匿名およびローカル アクセス アクセスの有効化

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。

   注：このSystem Management HomepageがHP Systems Insight Managerと同じマシン上で動作している場合、HP Systems Insight Managerの特定の機能を動作させるには、[ローカル アクセス(匿名)]を有効にしておかなければなりません。[ローカル アクセス (管理者)]または[匿名 アクセス]が有効になっている場合も機能は動作しますが、これらは必要ではありません。

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]->[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。

関連トピック

- 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]オプションにより、ご使用のシステムに必要なセキュリティ レベルを選択できます。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サーバからの設定変更だけを受け入れるようにSystem Management Homepage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:

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 Systems Insight Managerサーバからの設定変更だけを受け入れるようにSystem Management Homepageを設定できます。[名前による信頼]オプションは設定が簡単です。[名前による信頼]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、提出されたHP Systems Insight Managerのサーバ名のみを確認します。

注:

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。

- [すべてを信頼]　どのシステムからの設定変更も受け入れるようにSystem Management Homepageを設定できます。

注:

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System Management Homepage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System Management Homepage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 Systems Insight Manager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:

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]

[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]->[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。[信頼モード]ページが表示されます。
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. [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。
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。

[名前による信頼]

サーバ名オプションは、以下の基準を満たす必要があります。

- 各サーバ名の最大長は63文字です。
- サーバ名リスト全体の最大長は1,024文字です。
- **サーバ名**には、特定の文字列を使用できません。 ~ ' ! @ # $ % ^ & * ( ) + = \ " : ' < > ? , |
- **サーバ名**はセミコロンで区切ります。

[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]->[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。[信頼モード]ページが表示されます。
3. サーバ名によって信頼する[名前による信頼]を選択します。
4. サーバ名を入力します。
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。

[すべてを信頼]

[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]->[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。[信頼モード]ページが表示されます。
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。

関連トピック

- 証明書の自動インポート
- IPバインド
- IP限定ログイン
- ローカル/匿名アクセス
- ローカル サーバ証明書
- 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証明書]ページにより、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とSystem Management Homepage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 Systems Insight Managerサーバから信頼済み証明書を追加できます。

証明書のインポート

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. 追加する証明書があるHP Systems Insight Managerシステムの名前またはIPアドレスを入力します。 [サーバから証明書の追加]をクリックします。
3. 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。

サーバからの証明書の追加

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. 追加する証明書があるHP Systems Insight Managerサーバの名前を入力します。 [サーバから証明書の追加]をクリックします。
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。

関連トピック

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

ユーザ グループ

System Management Homepage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System Management Homepage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。

System Management Homepage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。 System Management Homepage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System Management Homepageに割り当てることができます。 指定されたオペレーティング システム グループがSystem Management Homepage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。

System Management Homepage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System Management Homepageユーザは、System Management Homepage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 グループ項ページで指定されたSystem Management Homepageへのアクセス権を持ちます。 Windowsの管理者グループとHP-UXおよびLinuxのルート グループには、自動的に、システムへの管理者アクセス権が割り当てられます。

たとえば、System Management Homepage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、System Management Homepageに対する管理者権限が付与されます。

ユーザ グループの追加

[ユーザ グループ]ページにより、ユーザ グループをSystem Management Homepage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、System Management Homepage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（Microsoft社製オペレーティング 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、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。

- [ユーザ]　[ユーザ]アクセス権を持つユーザは、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]アクセス権を持つユーザに対して制限されています。

管理者グループの追加

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]->[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。 [ユーザ グループ]ページが表示されます。
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 グループの追加

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]->[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。 [ユーザ グループ]ページが表示されます。
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 グループの追加

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]->[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。 [ユーザ グループ]ページが表示されます。
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。

関連トピック

- IPバインド
- IP限定ログイン
- ローカル/匿名アクセス
- 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

[タスク]タブ

[タスク]タブには、参加しているHP Webベース システム マネジメント ソフトウェアにより提供されるタスク指向ページへのリンクが表示されます。

注:

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]タブは表示されません。

関連トピック

- [ホーム]タブ
- [設定]タブ
- [ツール]タブ
- [ログ]タブ

[ツール]タブ

[ツール]タブには、参加しているHP Webベース システム マネジメント ソフトウェアにより提供されるツール指向ページへのリンクが表示されます。

注:

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]タブは表示されません。

関連トピック

- [ホーム]タブ
- [設定]タブ
- [タスク]タブ
- [ログ]タブ

[ログ]タブ

[ログ]タブには、各種のログ情報が表示されます。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、このタブに表示できます。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。

[ログ]タブは、次のログ オプションを提供します。

- [ログ]->[System Management Homepage]->[System Management Homepageログ]の順に選択します。
- LinuxおよびWindowsの場合、[ログ]->System Management Homepage->System Management Homepageレガシー ログの順に選択します。

関連手順

- System Management Homepageログ
- System Management Homepageレガシー ログ

関連トピック

- [ホーム]タブ
- [設定]タブ
- [タスク]タブ
- [ツール]タブ

System Management Homepageログ

[System Management Homepageログ]には、主として、セキュリティ関連のイベントが含まれており、参加しているHP Webベース システム マネジメント ソフトウェアのセキュリティの問題のトラブルシューティングに役立ちます。

注:

[System Management Homepageログ]にアクセスするには、System Management Homepage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。

関連トピック

- [ログ]タブ
- System Management Homepageレガシー ログ
- [設定]タブ
- [タスク]タブ

- [ツール]タブ

System Management Homepageレガシー ログ

System Management Homepage 2.0.0をインストールする前にLinuxまたはWindowsシステムに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レガシー ログ]リンクによってそれら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。

注:

[System Management Homepageログ]にアクセスするには、System Management Homepageの[管理者]グループのメンバーである必要があります。

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:

HP-UXはレガシー ログを含みません。

関連トピック

- [ログ]タブ
- System Management Homepageログ

トラブルシューティング

注:

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。

ブラウザの問題

Windows環境でInternet Explorer 6.0を使用しています。 System Management Homepage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は無効か、サイトの名前と一致しません。**

  IPアドレスを使用してSystem Management Homepage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: セキュリティ証明書は、信頼していない会社によって発行されています。 証明書を確認して、 CA を信頼するかどうかを決定してください。**

  System Management Homepage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、System Management Homepage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： 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。

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。

使用しているブラウザがサポートされているかどうかを調べるには、どうすればよいでしょうか?

解決策： 次のブラウザがサポートされています。

どのサーバタイプにも接続できるHP-UX ItaniumまたはPA-RISCシステムで動作する以下のデスクトップ ブラウザ、またはHP-UXサーバ上のローカルで動作しているブラウザ、およびXを通してどのデスクトップにも表示されるブラウザを使用できます。

- Mozilla 1.6

どのサーバタイプにも接続できるWindows Itaniumまたはx86システムで動作する以下のデスクトップ ブラウザを使用できます。

- Internet Explorer 6.0以降
- Mozilla 1.5
- Mozilla 1.6

どのサーバタイプにも接続できるLinux IPFまたはx86システムで動作する以下のデスクトップ ブラウザを使用できます。

- Mozilla 1.5
- Mozilla 1.6

HP-UXに**http://ホスト名/2301/**ではログインできますが、**http://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System Management Homepage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 システムでアクセスする場合にのみ発生します。 この問題は、URLにIPアドレスを指定せずに`localhost`を使用すると解決します。

この問題を解決するために、次のURLを使用することをおすすめします。

https://localhost:2381

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す。 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、ファイアウォールを設定を変更します。
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。

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、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。

インストール時の問題

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： System Management Homepage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、System Management Homepage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。

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。 System Management Homepage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://localhost: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：「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System Management Homepage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

Windowsオペレーティング システム環境でSystem Management Homepageにログインできません。

解決策： 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System Management Homepage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。

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： 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、[user must change the password on next logon option]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、System Management Homepage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。

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： System Management Homepage 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）を使用していました。 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、System Management Homepage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System Management Homepage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、System Management Homepageのオンライン ヘルプを参照してください。 これは、HP-UXには適用されません。

System Management Homepage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、[user must change the password on next login]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System Management Homepage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、System Management Homepage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、[Automatic Import Certificate]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System Management Homepage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、System Management Homepage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。

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す。 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、ファイアウォールを設定を変更します。
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

製品	ポート番号
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。

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、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。

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、_の代わりに-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： 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、ファイアウォールを設定を変更します。

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System Management Homepageにインポートできないのはなぜですか?

解決策： System Management Homepage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]->[System Management Homepage]の順に選択することによってSystem Management Homepage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。 System Management Homepageを再起動すると、この証明書が使用されます。

PKCS#7フォーマットの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]->[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]フィールドに含まれていません。 [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、System Management Homepageによって信頼されるHP Systems Insight Managerサーバを設定するために使用されます。 詳しくは、信頼された管理サーバ項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System Management Homepage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System Management Homepage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]->[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。
   - [Request a certificate]を選択します。
   - [Advanced certificate request]を選択します。
   - [Submit a certificate request by using a base]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。
   - [View the status of a pending certificate request]を選択します。
   - [Base64 encoded]と[Download certificate]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

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： System Management Homepage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。 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。 System Management Homepage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、System Management Homepageのルートとしてログインする必要があります。

注： 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。

現在使用しているバージョンのLinuxの環境でSystem Management Homepageをインストールできないのはなぜですか?

解決策： System Management Homepageをサポートするバージョンの Linuxには、それぞれ、専用のRPMパッケージ セットが必要です。 システムに不足しているRPMパッケージを確認するには、System Management Homepage RPMをverbose（非サイレント）モードでインストールします。 これにより、不足しているRPMパッケージが示されます。

一部のMcAfee製品をインストールするとSystem Management Homepageにアクセスできないのはなぜですか?

解決策： McAfeeは、McAfee製品と一部のWeb対応製品が使用不能になる可能性のある非互換性の製品を（Webサイトで）公表しています。 非互換製品のリストには、HP System Management Homepageが含まれています。 この非互換性は、Windows 2000環境で発生します。 McAfeeのWebサイトでは、この問題について次のように説明しています。

「Internet connectivity issues caused by incompatible Layered Service Providers:

- (LSP) CR13346

Product Versions

- All McAfee VirusScan 7 versions
- All McAfee Internet Security 5 versions
- All McAfee Firewall 4 versions

Operating Systems

- Windows 2000/XP
- Windows 98/Millennium
- System Information

Connection to the Internet:

You might experience Internet connectivity issues when McAfee Products are used in conjunction with other applications, which include a Layered Service Provider (LSP.) Most applications, which include a LSP, do coexist successfully. Those that are known to conflict with the McAfee LSP are listed below:」

- 「Either uninstall the third-party application or uninstall the McAfee product.」

McAfeeは、Network Associates社の事業単位です。

System Management Homepageヘルプ メニューからパーティション マネージャ ヘルプを選択すると、ブランク ページが表示されるのはなぜですか?

解決策：特定の状況において、System Management Homepageヘルプ メニューからパーティション マネージャ ヘルプを選択するときに、Webブラウザにブランク ページが表示されることがあります。 この場合、ブラウザの[更新]ボタンを使用して問題を解決できます。

サービスおよびサポート

System Management Homepage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 ページの目的は、各種の製品、サービス、およびサポート関連リソースを提供することです。特に、以下の目的でこのページを使用できます。

- HP ProLiant Server Management Softwareページhttp://www.hp.com/servers/manageにアクセスしてください。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 System Management Homepageページhttp://software.hp.comにアクセスしてください。
- 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、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

用語集

Domain Name Service	ドメイン名をIPアドレスに変換するサービス。
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 Systems Insight Manager	HP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。 HP Systems Insight Managerは、HP Insightマネージャ7、HP Toptools、HP Servicecontrol Managerの長所を組み合わせて設計された単一のツールで、HP-UX、Linux、およびWindowsを実行するHP ProLiant、HP Integrity、HP 9000システムの管理に使用できます。コアHP Systems Insight Managerソフトウェアは、すべてのHP製サーバ プラットフォームの管理に必要な必須機能を提供します。また、HP Systems Insight Manager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を使用することにより、機能を拡張できます。 この機能拡張によって、これらの製品を含んだ非常に広範なシステム管理が可能になります。迅速な配備、性能管理、および作業負荷管理用のプラグインも用意されているため、システム管理者は、現在保有しているハードウェア資産の完全なライフサイクル管理実現に必要な付加価値ソフトウェアをピックアップできます。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バージョン コントロール エージェント	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	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。
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。
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	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。
Secure HTTP	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	ネットワーク経由で他のシステムにログインして、そのシステムでコマンドを実行するためのプログラム。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	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。
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、サーバがオンラインのときに収集されます。
System Management Homepage	HTTPおよびHTTPS経由で通信するHP Webベース システム マネジメント ソフトウェアで使用されるソフトウェアの統合セット。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。
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。
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。
外部サイト	他社製アプリケーションのURL。
グラフィカル ユーザ インタフェース	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。System

	Management HomepageのGUIはWeb対応なので、Webブラウザで表示されます。
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。
コマンド ライン インタフェース	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。
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。
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 Systems Insight Manager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 Systems Insight Manager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 Systems Insight Managerからアクセスする必要があります。
ステータス タイプ	指定されたステータス タイプ（重大、メジャー、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	管理対象システムからのタスクの安全な実行。System Management Homepage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。
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。
認証機関	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。
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	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。
ユーザ	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	System Management Homepage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System Management Homepage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。

索引