HPシステム マネジメント ホームページ

製品番号：365395-195

2005年02月, 1 版

目次

製品概要

システム マネジメント ホームページ製品概要

システム マネジメント ホームページは、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。システム マネジメント ホームページは、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。

システム マネジメント ホームページは、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およびItaniumプロセッサ ファミリ）環境にインストールできます。Windowsオペレーティング システム環境では、インストール時にシステム マネジメント ホームページを設定できます。Linuxオペレーティング システム環境では、システム マネジメント ホームページは、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。

追加情報

追加情報については、HPのWebサイトhttp://www.hp.com/jp/servers/manageを参照してください。

関連項目

- システム マネジメント ホームページ概要 [11]

開始するには

使用を開始するには

システム マネジメント ホームページの使用を開始する際は、システム マネジメント ホームページ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」の項 [23]
2. 信頼モードを設定します。 -「信頼モード」の項 [20]
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」の項 [19]

関連手順

- ログイン [5]
- ログアウト [7]

関連項目

- IPバインド [16]
- IP限定ログイン [17]
- ローカル/匿名 アクセス [19]
- ローカル サーバ証明書 [18]
- 信頼された管理サーバ [22]
- 信頼モード [20]
- ユーザ グループ [23]

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 エージェントにアクセスできます。

Internet Explorerを使用してシステム マネジメント ホームページ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`**にアクセスします。
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、システム マネジメント ホームページ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。

注：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、システム マネジメント ホームページで[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」の項 [7]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、システム マネジメント ホームページが表示されます。

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 グループをシステム マネジメント ホームページのセキュリティ設定に追加していない場合、ユーザは、[管理者]グループ（Windows環境の場合）または[root]グループ（Linux環境の場合）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、[管理者]（Windows環境の場合）および[root]（Linux環境の場合）は、システム マネジメント ホームページに対する管理者アクセス権を持ちます。

   [パスワード]フィールドに正しいパスワードを入力します。パスワードは、そのユーザのオペレーティング システムベースのパスワードを使用してください。

5. [ログイン]をクリックします。システム マネジメント ホームページが表示されます。

Mozillaを使用してシステム マネジメント ホームページ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**にアクセスします。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[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。[この証明書を常に受け入れる]を選択していない場合は、アクセスするたびに[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、その後にシステム マネジメント ホーム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るユーザ名を入力します。ユーザ グループをシステム マネジメント ホームページのセキュリティ設定に追加していない場合、ユーザは、[管理者]グループ（Windows環境の場合）または[root]グループ（Linux環境の場合）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、[管理者]（Windows環境の場合）および[root]（Linux環境の場合）は、システム マネジメント ホームページに対する管理者アクセス権を持ちます。

4. [パスワード]フィールドに正しいパスワードを入力します。パスワードは、そのユーザのオペレーティング システムベースのパスワードを使用してください。

5. [ログイン]をクリックします。システム マネジメント ホームページが表示されます。

関連項目

- ログアウト [7]

- 証明書の自動インポート [7]

ログアウト

システム マネジメント ホームページからのログアウト

システム マネジメント ホームページからログアウトするには、[システム マネジメント ホームページ]バナーの[ログアウト]をクリックするか、ログインした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

- ログイン [5]

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

[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システムからシステム マネジメント ホームページ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、システム マネジメント ホームページ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。

   システム マネジメント ホームページで[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。

   ログインについて詳しくは、「ログイン」の項 [5]を参照してください。

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。

システム マネジメント ホームページが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、システム マネジメント ホームページの証明書を入力し、[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。

関連項目

- ログイン [5]
- ログアウト [7]
- ローカル/匿名 アクセス [19]
- ローカル サーバ証明書 [18]
- 信頼された管理サーバ [22]
- ユーザ グループ [23]

ソフトウェアのナビゲート

はじめに

システム マネジメント ホームページでは、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、システム マネジメント ホームページには、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 [12]の「ステータス ボックス インジケータ」を参照してください。システム マネジメント ホームページは、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 [9]
- [データ フレーム] [9]

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。上部にあるリンクは、現在表示中のパスを示します。

ヘッダには、次の情報が表示されます。

- [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サポート フォーラムに問い合わせて、HP製品に関する疑問への回答を得ることができます。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。

[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。

関連項目

- [ホーム]タブ [12]
- [設定]タブ [14]
- [ツール]タブ [26]
- [タスク]タブ [27]
- [ログ]タブ [28]

タブ

タブ

システム マネジメント ホームページには、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。[ツール]タブおよび[タスク]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。

システム マネジメント ホームページでは、次のタブを表示できます。

- [ホーム]タブ [12]
- [設定]タブ [14]
- [タスク]タブ [27]
- [ツール]タブ [26]
- [ログ]タブ [28]

関連項目

- [ホーム]タブ [12]
- [設定]タブ [14]
- [ツール]タブ [26]
- [タスク]タブ [27]
- [ログ]タブ [28]

システム マネジメント ホームページ概要

システム マネジメント ホームページ

システム マネジメント ホームページでは、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、システム マネジメント ホームページには、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 [12]の「ステータス ボックス インジケータ」を参照してください。

システム マネジメント ホームページ内のナビゲートについては、ソフトウェアのナビゲート [9]を参照してください。

関連項目

- タブ [10]
- [ホーム]タブ [12]
- [設定]タブ [14]
- [ツール]タブ [26]
- [タスク]タブ [27]
- [ログ]タブ [28]

[ホーム]タブ

[ホーム]

[ホーム]タブは、システム マネジメント ホームページに表示されます。[ホーム]タブには、次の情報が表示されます。

- システム全体のステータス [12]
- ソフトウェアのステータス [12]
- 構成メニュー [12]

システム全体のステータス

[全体のシステムステータス]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、[全体のシステムステータス]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。

- [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、システム マネジメント ホームページ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]　システム マネジメント ホームページに参加していない、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]　付加価値ソフトウェアに関する情報、およびProLiant Essentials Value Added Softwareなどのソフトウェア情報を含むHPのWebサイト http://www.hp.com/jp/servers/proliantessentialsのページへのリンクが表示されます。ProLiant Essentials Value Added Softwareについて詳しくは、HPのWebサイト http://www.hp.com/jp/servers/proliantessentialsを参照してください。
- [キー]　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

関連項目

- [設定]タブ [14]
- [ツール]タブ [26]
- [タスク]タブ [27]
- [ログ]タブ [28]

[設定]タブ

[設定]

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。システム マネジメント ホームページをインストールすると、[システムマネジメントホームページ]セクションだけが表示され、システムマネジメント ホームページの設定を表示または編集することができます。

[設定]セクション

このセクションには、参加しているHP Insightマネジメント エージェントのリストが表示されます。参加している各Insightマネジメント エージェントには、すでにオプションが定義されています。

[システム マネジメント ホームページ]セクション

このセクションには、システム マネジメント ホームページ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]」の項 [14]　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]」の項 [15]　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 [16]
- IP限定ログイン [17]
- ローカル/匿名 アクセス [19]
- ローカル サーバ証明書 [18]
- 信頼モード [20]
- 信頼された管理サーバ [22]
- ユーザ グループ [23]

関連項目

- [ホーム]タブ [12]
- [ツール]タブ [26]
- [タスク]タブ [27]
- [ログ]タブ [28]

[クレジット]

[クレジット]

[クレジット]リンクにより、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。

関連項目

- [ホーム]タブ [12]
- [設定]タブ [14]
- [ツール]タブ [26]
- [タスク]タブ [27]
- [ログ]タブ [28]

[セキュリティ]

[セキュリティ]

[システム マネジメント ホームページ - 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]、[システム マネジメント ホームページ]、[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]、[システム マネジメント ホームページ]、[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]、[システム マネジメント ホームページ]、[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]、[システム マネジメント ホームページ]、[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]、[システム マネジメント ホームページ]、[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]、[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]の順に選択します。
- [ユーザ グループ]　[設定]、[システム マネジメント ホームページ]、[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 [16]
- IP限定ログイン [17]
- ローカル/匿名 アクセス [19]
- ローカル サーバ証明書 [18]
- 信頼モード [20]
- 信頼された管理サーバ [22]
- ユーザ グループ [23]

関連項目

- [ホーム]タブ [12]
- [設定]タブ [14]
- [ツール]タブ [26]
- [タスク]タブ [27]

- [ログ]タブ [28]

IPバインド

IPバインドは、システムマネジメントホームページ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システム マネジメントホームページ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

システム マネジメント ホームページは、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、システム マネジメント ホームページは、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]、[システム マネジメント ホームページ]、[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。

   IA-32プラットフォームの場合

   この値を設定するには、システム マネジメント ホームページを再起動して ログインしなおす必要があります。

   Itaniumプラットフォームの場合

   SMHサービスが再起動されるまで、新しいSMH設定は有効になりません。
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。

関連項目

- IP限定ログイン [17]
- ローカル/匿名 アクセス [19]
- ローカル サーバ証明書 [18]
- 信頼モード [20]
- 信頼された管理サーバ [22]
- ユーザ グループ [23]

IP限定ログイン

[IP 限定 ログイン]により、システム マネジメント ホームページは、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。

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]、[システム マネジメント ホームページ]、[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IP限定ログインを有効にします。
4. 除外するIPアドレス（**`1.1.1.1;2.2.2.2-3.4.5.6`**など）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。

   IA-32プラットフォームの場合

   この値を設定するには、システム マネジメント ホームページを再起動して ログインしなおす必要があります。.

   Itaniumプラットフォームの場合

   SMHサービスが再起動されるまで、新しいSMH設定は有効になりません。
7. [OK]をクリックします。

関連項目

- IPバインド [16]
- ローカル/匿名 アクセス [19]
- ローカル サーバ証明書 [18]
- 信頼モード [20]
- 信頼された管理サーバ [22]
- ユーザ グループ [23]

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。このプロセスを実行すると、システム マネジメント ホームページ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、システム マネジメント ホームページ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。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システム マネジメント ホームページ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。

PKCS #10を作成するには、以下の手順に従ってください。

1. [設定]、[システム マネジメント ホームページ]、[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、`c:\hp\sslshare\req_cr.pem`（Windowsの場合）または`/opt/hp/sslshare/req_cr.pem`（Linuxの場合）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. システム マネジメント ホームページを停止します。

10. システム マネジメント ホームページを再起動します。

11. インポートされた証明書を含む管理対象システムをブラウズします。

12. ブラウザ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。また、プロンプトが表示されないようにルートのCA証明書をネットワーク上のすべてのブラウザにインポートすることもできます。

    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/hp/sslshare/cert.pemにコピーして、システム マネジメント ホームページを再起動してください。

関連項目

- IPバインド [16]
- IP限定ログイン [17]
- ローカル/匿名 アクセス [19]
- 信頼モード [20]
- 信頼された管理サーバ [22]
- ユーザ グループ [23]

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]　デフォルトでは、[匿名 アクセス]は無効にされています。[匿名アクセス]を有効にすると、ログインせずにシステム マネジメント ホームページ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]　[ローカル アクセス]では、認証を受けずにローカルでシステム マネジメント ホームページ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。

ローカル アクセスおよび匿名アクセスの有効化

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]、[システム マネジメント ホームページ]、[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：このシステム マネジメント ホームページが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]、[システム マネジメント ホームページ]、[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

- IPバインド [16]
- IP限定ログイン [17]
- ローカル サーバ証明書 [18]
- 信頼モード [20]
- 信頼された管理サーバ [22]
- ユーザ グループ [23]

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]　[証明書による信頼]モードでは、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システム マネジメント ホームページを設定できます。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： このオプションの使用をおすすめします。

- [名前による信頼]　[名前による信頼]モードでは、[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システム マネジメント ホームページを設定できます。[名前による信頼]オプションは設定が簡単で、悪意のない不正アクセスを防ぎます。[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。このオプションを設定すれば、指定された名前のHP Systems Insight Managerサーバからの要求しか受け入れません。

- [すべてを信頼]　[すべてを信頼]モードでは、どのシステムからの設定変更も受け入れるようにシステム マネジメント ホームページを設定できます。たとえば、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、[すべてを信頼]オプションを使用することができます。

信頼モードの設定

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。

Linux環境の場合、インポートされたシステム マネジメント ホームページ証明書は、/opt/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]、[システム マネジメント ホームページ]、[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。

- サーバ名リスト全体の最大長は1,024文字です。
- 各サーバ名の最大長は63文字です。
- **サーバ名**には、以下の文字列を使用できません。

  Itaniumプラットフォームの場合、サーバ名は、RFC 952によって規定されている規格に準拠している必要があります。つまり、ピリオド（.）で区切られた名前のリストであり、各名前は、英字（大文字および小文字）、数字、またはマイナス記号（-）によって構成されている必要があります。また、最初が英字で、最後が英数字でなければなりません。RFC 952について詳しくは、RFCのWebサイト http://www.rfc-editor.org/rfc/rfc952.txtを参照してください。

  ~ ' ! @ # $ % ^ & * ( ) + = \ " : ' < > ? , |

- **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]、[システム マネジメント ホームページ]、[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]、[システム マネジメント ホームページ]、[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。

関連項目

- 証明書の自動インポート [7]
- IPバインド [16]
- IP限定ログイン [17]
- ローカル/匿名 アクセス [19]
- ローカル サーバ証明書 [18]
- 信頼された管理サーバ [22]
- ユーザ グループ [23]

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とシステム マネジメント ホームページ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]、[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。
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]、[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。
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、[Add Certificate to Trust List]をクリックします。

関連項目

- IPバインド [16]
- IP限定ログイン [17]
- ローカル/匿名 アクセス [19]
- ローカル サーバ証明書 [18]
- 信頼モード [20]
- ユーザ グループ [23]

ユーザ グループ

ユーザ グループ

システム マネジメント ホームページでは、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。

[管理者]（LinuxおよびHP-UXの場合は[root]）オペレーティング システム グループのユーザは、[管理者]、[オペレータ]、または[ユーザ]のシステム マネジメント ホームページアクセス 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。

システム マネジメント ホームページの各アクセス 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。システム マネジメント ホームページのインストールでは、オペレーティング システム グループをシステム マネジメント ホームページ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 グループがシステム マネジメント ホームページ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、システム マネジメント ホームページのログ メッセージによって示されます。

システム マネジメント ホームページ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。管理者権限を持つシステム マネジメント ホームページユーザは、システム マネジメント ホームページの各アクセス 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」の項 [23]ページで指定されたシステム マネジメント ホームページへのアクセス権を持ちます。Windowsの管理者グループと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、システム マネジメント ホームページの管理者アクセス 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、システム マネジメント ホームページ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 グループをシステム マネジメント ホームページに追加できます。

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、システム マネジメント ホームページ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[管理者]、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、システム マネジメント ホームページ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、システム マネジメント ホームページ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]、[システム マネジメント ホームページ]、[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]、[システム マネジメント ホームページ]、[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]、[システム マネジメント ホームページ]、[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。

関連項目

- IPバインド [16]
- IP限定ログイン [17]
- ローカル/匿名 アクセス [19]
- ローカル サーバ証明書 [18]
- 信頼モード [20]
- 信頼された管理サーバ [22]

[ツール]タブ

[ツール]

[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。

関連項目

- [ホーム]タブ [12]
- [設定]タブ [14]
- [タスク]タブ [27]
- [ログ]タブ [28]

[タスク]タブ

[タスク]

[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。

関連項目

- [ホーム]タブ [12]
- [設定]タブ [14]
- [ツール]タブ [26]
- [ログ]タブ [28]

[ログ]タブ

[ログ]

[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。リンクをクリックすることにより、表示されているログのエントリ ポイントにアクセスできます。

[ログ]タブは、次のログ オプションを提供します。

- [ログ]、[システム マネジメント ホームページ]、[システム マネジメント ホームページ ログ]の順に選択します。
- [ログ]、[システム マネジメント ホームページ]、[システム マネジメント ホームページ レガシー ログ]の順に選択します。

関連手順

- システム マネジメント ホームページ ログ [28]
- システム マネジメント ホームページ レガシー ログ [29]

関連項目

- [ホーム]タブ [12]
- [設定]タブ [14]
- [ツール]タブ [26]
- [タスク]タブ [27]

システム マネジメント ホームページ ログ

[システムマネジメントホームページログ]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

[システム マネジメント ホームページ ログ]にアクセスするには、システム マネジメント ホームページに対する管理者アクセス権が必要です。

[システム マネジメント ホームページ ログ]にアクセスするには、[ログ]、[システム マネジメント ホームページ]、[システム マネジメント ホームページ ログ]の順に選択してください。

関連項目

- [ログ]タブ [28]
- システム マネジメント ホームページ レガシー ログ [29]
- [設定]タブ [14]
- [ツール]タブ [26]
- [タスク]タブ [27]

システム マネジメント ホームページ レガシー ログ

システム マネジメント ホームページ2.0.0をインストールする前にシステムに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、[システム マネジメント ホームページ 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

[システム マネジメント ホームページ ログ]にアクセスするには、システム マネジメント ホームページの[管理者]グループのメンバーである必要があります。

システム マネジメント ホームページの従来のログにアクセスするには、[ログ]、[システム マネジメント ホームページ]、[システム マネジメント ホームページ レガシー ログ]の順に選択してください。

関連項目

- [ログ]タブ [28]
- システム マネジメント ホームページ ログ [28]

トラブルシューティング

ブラウザの問題

Windows環境でInternet Explorer 6.0を使用しています。システム マネジメント ホームページ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システム マネジメント ホームページにアクセスすると、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、信頼済みと選択されたいない会社によって作成されています。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。**

  システム マネジメント ホームページ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、システム マネジメント ホームページ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からシステム マネジメント ホームページにアクセスすると、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。

IA-32プラットフォームの場合

- Internet Explorer 6.0
- Mozilla 1.5
- Mozilla 1.6

Itaniumプラットフォームの場合

- Internet Explorer 6.0以降

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、URLとして

`https://localhost:2381`を使用することをおすすめします。

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、ファイアウォールの設定を変更します。
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。

この設定により、Windows XP Service Pack 2のデフォルト セキュリティ強化を変更することなく、上記のポート経由でのトラフィックを許可できます。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

システム マネジメント ホームページ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：システムマネジメントホームページ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、システム マネジメント ホームページシステムの`\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。

システム マネジメント ホームページ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。システム マネジメント ホームページのインストールは、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：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。

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、常に包含セクションに含まれています。このアドレスは、[Exclude]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。なぜですか?

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[Include]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 Restriction]の[Exclude]フィールドに**127.0.0.1**を入力してください。

[IP Restriction]でシステムのローカルIPアドレスや127.0.0.1が[Include]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：ユーザが誤ってシステム マネジメント ホームページ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[Include]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[Exclude]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 システム環境でシステム マネジメント ホームページ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]グループまたはシステム マネジメント ホームページ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、[user must change the password on next logon]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、システム マネジメント ホームページ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： システム マネジメント ホームページ 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、システム マネジメント ホームページ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 グループにシステム マネジメント ホームページ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、システム マネジメント ホームページのオンライン ヘルプを参照してください。

システムマネジメントホームページ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システム マネジメント ホームページ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、システム マネジメント ホームページ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

- 対象のシステム マネジメント ホームページの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、システム マネジメント ホームページシステムの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、ファイアウォールの設定を変更します。
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。

この設定により、Windows XP Service Pack 2のデフォルト セキュリティ強化を変更することなく、上記のポート経由でのトラフィックを許可できます。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。

注：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、ファイアウォールの設定を変更します。
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：	5000

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。

この設定により、Windows XP Service Pack 2のデフォルト セキュリティ強化を変更することなく、上記のポート経由でのトラフィックを許可できます。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証明書を直接システム マネジメント ホームページにインポートできないのはなぜですか?

解決策：システム マネジメント ホームページは、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]、[システム マネジメント ホームページ]の順に選択することによってシステム マネジメント ホームページ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。システム マネジメント ホームページを再起動すると、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]、[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]フィールドに含まれていません。[設定]、[システム マネジメント ホームページ]、[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、システム マネジメント ホームページ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」の項 [22]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システム マネジメント ホームページ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システム マネジメント ホームページ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]、[システム マネジメント ホームページ]、[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`**に移動します。

   注： `W2003CA`は、Windows 2003 認証機関システムの名前に置き換えてください。

   1. [Request a certificate]を選択します。
   2. [Advanced certificate request]を選択します。
   3. [Submit a certificate request by using a base...]を選択します。
   4. 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。

   1. [スタート]、 [プログラム]、[管理ツール]、[証明機関]の順にクリックします。

   2. [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。

   3. 保留リクエスト証明書を発行します。

5. **`http://W2003CA/certsrv`**に移動します。

   注： `W2003CA`は、Windows 2003 認証機関システムの名前に置き換えてください。

   1. [View the status of a pending certificate request]を選択します。

   2. [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。

   3. `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

システム マネジメント ホームページ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：システム マネジメント ホームページ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。

[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。システム マネジメント ホームページでは、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。

ルートではない場合に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、システム マネジメント ホームページ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の環境でシステムマネジメントホームページをインストールできないのはなぜですか?

解決策：システム マネジメント ホームページ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、システム マネジメント ホームページ 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システム マネジメント ホームページ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システムマネジメントホームページが含まれています。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。

サービスおよびサポート

サービスおよびサポート

システム マネジメント ホームページ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。

- http://www.hp.com/jp/servers/manageにアクセスしてください。このWebサイトは、システム管理製品専用です。このサイトには、豊富な製品情報やサービス関連情報が掲載されています。
- HPのサポート ホーム ページやWebサイトにアクセスしてください。電話番号、オンラインツール、および情報が掲載されています。

- 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 フォーラムのURL（英語）は、次の場所にあります。http://forums.itrc.hp.com

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PC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
- ハードウェア設定情報
  - 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
  - システム情報の参照（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製またはコンパック製以外の装置の説明

用語集

Domain Name Service (DNS)	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、Windows、Linux、HP-UXを実行するHP ProLiant、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 (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。
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範囲	指定された範囲に含まれるIPアドレスを持つシステム。

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。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 (HTTPS)	Web経由でのデータの安全な送信を支援する拡張されたHTTP プロトコル。
Secure Shell (SSH)	ネットワーク経由で他のシステムにログインして、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 (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。
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。
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 (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。システム マネジメント ホームページの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 (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。

システム マネジメント ホームページ	HTTPおよびHTTPS経由で通信するHPの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。
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。
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
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 (STE)	管理対象システムからのタスクの安全な実行。システム マネジメント ホームページのこの機能により、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 アップデート	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 (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。
バージョン コントロール	ユーザ システムのHPオペレーティング システム ドライバ、HP Systems Insight Managerエージェント、HPユーティリティ、およびファームウェアのバージョンを確認する機能。最新のソフトウェアとファームウェアのバージョンを記録したバージョン コントロール データベース（VCDB）とユーザ システムのバージョンを比較しますこの結果、バージョン コントロールは、ソフトウェアが最新の場合はそのことを示します。また、アップグレードが使用可能な場合は、そのことを示し、その理由を提供します。 バージョン情報は、システムのシステム リンクとして表示されます。

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。
ユーザ	システム マネジメント ホームページ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	システム マネジメント ホームページ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 アカウントまたはLinuxのユーザ アカウントにシステム マネジメント ホームページ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