

HP System Management Homepage



,

©Copyright 2005 Hewlett-Packard

目次

製品概要	4
HP SIM	4
統合管理ツール	4
その他のリソース	4
関連トピック	5
使用開始	6
関連トピック	6
ログイン	6
関連トピック	9
証明書の自動インポート	9
関連トピック	10
ログアウト	10
関連トピック	10
ソフトウェアのナビゲート	11
情報領域	11
関連トピック	12
HP SMH ページ	12
関連トピック	12
ホームページ	13
ソフトウェアステータスカテゴリ (ボックス)	13
システム全体のステータス/システムステータスの概要	13
組織構成メニュー	13
デフォルトの HP-UX プロパティページ	14
システム	14
オペレーティングシステム	14
ソフトウェア	15
関連トピック	15
設定ページ	16
メニューカテゴリ (HP-UXのみ)	16
System Management Homepage カテゴリ	16
関連手順	16
関連トピック	16
メニュー	17
関連手順	17
関連トピック	17
カスタムメニューの追加	17
関連トピック	18
カスタムメニューの削除	18
関連トピック	18
クレジット	18
関連トピック	18
セキュリティ	18
関連手順	19
関連トピック	19
IP バインディング	19
関連トピック	20
IP 制限ログイン	20
関連トピック	21
ローカルサーバ証明書	21
関連トピック	23
ローカル/Anonymous アクセス	23

関連トピック	24
高信頼性モード	24
高信頼性モードの設定	25
関連トピック	26
信頼済み管理サーバ	26
関連トピック	27
ユーザーグループ	27
関連トピック	29
タスクページ	30
System (HP-UXのみ)	30
関連トピック	30
ツールページ	31
関連トピック	31
ログページ	32
関連手順	32
関連トピック	32
System Management Homepage ログ	32
関連トピック	32
System Management Homepage レガシーログ	33
関連トピック	33
SAM ログ	33
関連トピック	33
トラブルシューティング	34
ブラウザの問題	34
インストールの問題	36
IP アドレスの問題	37
ログインの問題	37
セキュリティの問題	40
その他の問題	43
サービスおよびサポート	43
ご注意	45
保証	45
U.S. Government License	45
Copyright Notice	45
登録商標に関する注意	45
出版履歴	45
リリース履歴	46
用語集	47
索引	52

製品概要

HP System Management Homepage (HP SMH) は、HP-UX、Linux、およびMicrosoft® Windows® オペレーティングシステムで、HP サーバを統合し、単一のシステム管理により管理を簡素化する 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管理ユーティリティからデータを集約することにより、HP SMH は、個々のサーバに対するハードウェア障害、ステータスの監視、パフォーマンスデータ、システムしきい値、診断、およびソフトウェアバージョンコントロールを表示するための、共通の使いやすいインタフェースを提供します。

HP SMH は、HP-UX、Linux (IA32、AMD64、Intel Itanium)、および Windows オペレーティングシステムにインストールすることができます。HP-UX システムの場合、HP SMH は SysMgmtWeb のバンドルタグを持ち、デフォルトでは HP-UX 11i v1 (B.11.11) および HP-UX 11i v2 (B.11.23) のオペレーティング環境とともに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 **System Lists** ページおよび **System** ページから HP SMH に簡単に移動できます。

また、HP SIM を信頼するように HP SMH を設定すると、HP SIM から HP SMH に移動する際に再度ログインする必要がなくなります。これは、HP SIM から HP SMH に初めてアクセスする際に、HP SMH のログインウィンドウで HP SIM の証明書を受け入れることで設定されます。

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。

また、HP SIM ベースのプラグインに直接アクセスする HP SIM ツール (**Configure > HP-UX Configuration** 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 の場合、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、また HP SMH ベースで使用できるようになりました。これには、nPartition Management、Peripheral Devices、Disks and File Systems、Accounts for Users and Groups、Kernel Configuration などの領域が含まれます。

その他のリソース

その他のリソースについては、次のリンクを参照してください。

- Software Depot home の HP SMH: <http://www.hp.com/go/softwaredepot> にジャンプして **Security and manageability** を選択します。 **HP System Management Homepage** リンクを検索します。
- HP ProLiant サーバ 管理ソフトウェア:
<http://h50146.www5.hp.com/products/servers/proliant/essentials>

関連トピック

- HP SMH ページ
- 使用開始

使用開始

HP System Management Homepage (HP SMH) の使用開始にあたっては、以下のガイドラインに従って HP SMH を適切に構成し、ユーザーとセキュリティを適切に設定してください。

以下の手順で HP SMH を構成します。

- HP-UX のオペレーティング環境では、HP SMH がデフォルト設定でインストールされます。
/opt/hpsmh/sbin/envvars および /opt/hpsmh/conf/timeout.conf スクリプトで設定された環境変数を変更することで、構成を変更することができます。
- Linux オペレーティングシステムでは、HP SMH が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 スクリプトで構成できます。
- Windows オペレーティングシステムでは、インストール中に HP SMH 設定を構成することができます。

注記:



HP-UX、Linux、および Windows オペレーティングシステムの構成を変更するには、HP テクニカル ドキュメント Web サイト (<http://docs.hp.com/ja>) の『『HP System Management Homepage Installation Guide』』を参照してください。

以下の手順でユーザーアクセスおよびセキュリティを適切に設定します。

1. ユーザーの権限を効果的に管理するには、ユーザーグループを追加します。「ユーザーグループ」を参照してください。
2. 高信頼性モードを構成します。「高信頼性モード」を参照してください。
3. ローカルアクセスまたは anonymous アクセスを構成します。「ローカル/Anonymous アクセス」を参照してください。

関連トピック

- ログイン
- 証明書の自動インポート
- ログアウト

ログイン

ログインウィンドウで、使用可能な HP Insight マネジメントエージェントを含む、**Home** ページにアクセスすることができます。

以下の手順で Internet Explorer から HP System Management Homepage (HP SMH) にログインします。

1. <https://hostname:2381/> にアクセスします。

注記:

HP-UX サーバをブラウズしている場合、デフォルトでは URI: **http://hostname:2301** を使用する必要があります。



デフォルトでは、HP-UX は自動起動機能が有効な状態でインストールされます。デーモンはポート 2301 でリスンし、要求されたときにポート 2381 で HP SMH の起動のみを行います。そしてタイムアウト期間の後、再び停止します。HP SMH を常にポート 2381 上で実行するように設定することも可能です。詳細は smhstartconfig(1M) コマンドを参照してください。

構成変数の変更手順は、HP テクニカル ドキュメント Web サイト (<http://docs.hp.com/ja>) の『『HP System Management Homepage Installation Guide』』を参照してください。

-
2. この URI を初めてブラウズする場合、その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、HP SMH をブラウズするたびにセキュリティの警告が表示されます。

注記:



ご自身の公開鍵基盤 (PKI) を導入する場合、または、ご自身で作成した証明書を各管理対象システムにインストールする場合は、Certificate Authority ルート証明書を各ブラウザにインストールして、管理用に使用することができます。これを実施すると、セキュリティの警告ダイアログボックスは表示されなくなります。予期しない警告が表示された場合は、間違ったシステムをブラウズしている可能性があります。**Certificate Authority** ルート証明書のインストールに関する詳細は、オンラインヘルプを参照してください。このヘルプはお使いのブラウザから参照できます。

HP Systems Insight Manager (HP SIM) からのリンク経由で HP SMH にアクセスしていて、**Trust By Certificate** オプションが HP SMH で有効になっている場合、**Automatically Import Management Server Certificate** オプションが表示されます (以前に信頼が設定されていない場合)。HP SIM 証明書の自動インポートに関する詳細は、「証明書の自動インポート」を参照してください。

-
3. **Yes** をクリックします。

Anonymous アクセスを有効にしている場合を除き、ログインウィンドウが表示された後に HP SMH 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ー名を入力してください。

ユーザーグループを HP SMH セキュリティ設定にまだ追加していない場合、ユーザーは、Windows では **Administrators** グループのオペレーティングシステムアカウントで、HP-UX および Linux では **root** オペレーティングシステムグループ(デフォルトの root ユーザーを

含むグループ)でログインする必要があります。証明書が認証できない場合、そのユーザーのアクセスは拒否されます。

注記:



ほとんどの場合、Windows では **administrator** が、HP-UX または Linux では **root** が、HP SMH の管理者アクセス権限を持っています。

5. オペレーティングシステムによって認識されるパスワードを入力してください。
6. HP-UX の場合は、**Sign In** をクリックします。Linux および Windows の場合は、**Login** をクリックします。

HP SMH が表示されます。

以下の手順で Mozilla から HP SMH にログインします。

1. **<http://hostname:2381>** にアクセスします。

注記:



HP-UX サーバをブラウズしている場合、デフォルトでは URI: **<http://hostname:2301>** を使用する必要があります。

デフォルトでは、HP-UX は自動起動機能が有効な状態でインストールされます。デーモンはポート 2301 でリスンし、要求されたときにポート 2381 で HP SMH の起動のみを行います。そしてタイムアウト期間の後、再び停止します。HP SMH を常にポート 2381 上で実行するように設定することも可能です。詳細は `smhstartconfig(1M)` コマンドを参照してください。

構成変数の変更手順は、HP テクニカル ドキュメント Web サイト (<http://docs.hp.com/ja>) の『[HP System Management Homepage Installation Guide](#)』を参照してください。

この URI に初めてブラウズする場合、サーバを信頼するかどうかを尋ねる **Website Certified by an Unknown Authority** ダイアログボックスが表示されます。 **Accept this certificate permanently** を選択しない場合、ブラウザを使用するたびに **Website Certified by an Unknown Authority** 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。

Anonymous アクセスを有効にしている場合を除き、ログインウィンドウが表示された後に HP SMH 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ー名を入力してください。

ユーザーグループを HP SMH セキュリティ設定にまだ追加していない場合、ユーザーは、Windows では **Administrators** グループのオペレーティングシステムアカウントで、HP-UX および Linux では **root** オペレーティングシステムグループ(デフォルトの root ユーザーを

含むグループ)でログインする必要があります。証明書が認証できない場合、そのユーザーのアクセスは拒否されます。

注記:



ほとんどの場合、Windows では **Administrator** が、HP-UX または Linux では **root** が、HP SMH の管理者アクセス権限を持っています。

4. オペレーティングシステムによって認識されるパスワードを入力してください。
5. HP-UX の場合は、**Sign In** をクリックします。Linux および Windows の場合は、**Login** をクリックします。

HP SMH が表示されます。

関連トピック

- 使用開始
- 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

Automatically Import Management Server Certificate 機能によって、HP SIM システムから HP System Management Homepage (HP SMH) にアクセスしたときに HP Systems Insight Manager (HP SIM) システム証明書を自動的にインポートすることが可能になります。

注記:



HP SIM 証明書を自動的にインポートするには、管理者アクセス権限で HP SMH にログインする必要があります。

以下の手順で HP SIM 証明書を自動的にインポートします。

1. **HP Systems Insight Manager** または **HP Insight Manager 7** システムから、システムへのリンクを選択してください。

Trust By Certificate オプションが HP SMH で選択されていて (**Settings - Security - Trust Mode**)、アクセスしている HP SIM システムのための証明書が **Trusted Certificates List** にインポートされていない場合、ログインウィンドウに **Automatically Import Management Server Certificate** オプションが表示されます。SERVER NAME から取り込まれた証明書情報により、HP SIM 証明書の詳細が表示されます。

2. デフォルトでは **Automatically Import Management Server Certificate** が選択されています。HP SIM 証明書を **Trusted Certificates List** に追加したくない場合は、このオ

ブションを選択解除してください。ただし、今後このシステムにアクセスするには、ログイン証明書が必要になります。

HP SMH が HP SIM 証明書を自動的にインポートすることを許可している場合は、今後、システムヘシームレスにアクセスできます。ログイン証明書を要求されることはありません。

3. **Automatically Import Management Server Certificate** を選択したままにし、HP SMH 証明書を入力して、**Log In** をクリックして自動的に証明書をインポートします。

注記:



証明書をインポートしたくない場合は、**Automatically Import Management Server Certificate** を選択解除してください。このオプションを選択解除すると、ログイン証明書の入力が必要になります。ただし、管理者証明書はログインには必要ありません。証明書は **Trusted Certificates List** に追加されます。

関連トピック

- 使用開始
- ログイン
- 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、複数の方法があります。

- HP SMH バナーで、HP-UX の場合は **Sign Out** を、Linux および Windows の場合は **logout** をクリックします。

HP System Management Homepage ログインウィンドウが表示されます。

- HP SMH へのログインに使用した 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

- 使用開始
- ログイン
- HP SMH ページ

ソフトウェアのナビゲート

HP System Management Homepage (HP SMH) 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を表示します。また、HP SMH は項目のステータスを定義する野線で囲まれたさまざまなカテゴリ (ボックス) も表示します。詳細に関しては、「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 2 つのフレームに分割されています。

- **ヘッダーフレーム** ヘッダーフレームは、どのページを見ているときでも常に表示されています。リンクにより、現在表示しているページのパスが表示されます。
- **データフレーム** データフレームは、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を表示します。

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) によって、ヘッダーフレームまたはデータフレームに以下の情報領域が表示されます。

- **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** **Support** 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** **Forums** リンクは、HP フォーラムへのリンクを提供します。

- **ヘルプ** **Help** リンクは、別のブラウザウィンドウでヘルプファイルを表示します。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とユーティリティに関連したヘルプファイルの組み合わせが含まれています。

- **システムモデル** **System Model** は、システムのモデルを表示します。サーバ用 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、**Unknown** と表示されます。

- **現在のユーザー** **Current User** は、現在ログインしているユーザーの ID を表示します。現在ログイン中のユーザーが、実際のオペレーティングシステムベースのユーザーである場合、**Log Out** または **Sign Out** リンクが表示されます。Anonymous アクセスが有効になっていて、ページに anonymous でアクセスしている場合は、**Current User** は **hpsmh_anonymous** と表示され、**Log In** 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で、ローカルマシンから HP Web ベースシステムマネジメントソフトウェアにアクセスしている場合は、**Current User** は、どのレベルのアクセスが有効になっているかによって、**hpsmh_local_anonymous** または **hpsmh_local_administrator** を表示し、ローカルアクセスがその下に表示されます。

ヒント:



Backボタンで HP System Management Homepage ログインウィンドウに戻ります。インターフェース内のウィンドウ間を移動するには、ヘッダーフレームで左上のページリンク、または中央のロケーションリンクを使用します。

関連トピック

- 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) では、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設定を構成することができる、最大 5 つのタブ付きページが表示されます。タスク (**Tasks**) ページとツール (**Tools**) 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から情報の提供を受けている場合にのみ表示されます。

表示可能な HP SMH ページは次のとおりです。

- 「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」

関連トピック

- 製品概要
- ソフトウェアのナビゲート
- 使用開始

ホームページ

ホーム (**Home**) 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。また、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 (**Home**) ページの情報は、インテグレートド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、インテグレートド 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、インテグレートド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、カテゴリ別に個別のボックス内に表示されます。各カテゴリ (ボックス) にはリンクがあり、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にジャンプして詳細を確認することができます。

追加のステータスカテゴリ: インテグレートド WBEM のステータスは、追加カテゴリ (ボックス) に表示されます。各カテゴリにはリンクがあり、データを提供している WBEM ソフトウェアにジャンプして詳細を確認することができます。

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。下表は、罫線の色とその定義の一覧です。

インジケータ	説明
青色	不明 (Unknown)
緑色	正常 (OK/Normal)
黄色	劣化/警戒域 (Degraded/Minor)
オレンジ色	障害/最重要警戒域 (Failed/Major)
グレー	ステータスなし (No status)

システム全体のステータス/システムステータスの概要

Overall System Status カテゴリ (HP-UX の場合は **System Status Summary**) では、インテグレートド HP Web ベースシステムマネジメントソフトウェアで提供されているのと同様の、障害または劣化ステータスがある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、または障害あるいは劣化の項目がない場合は、**Overall System Status** カテゴリには **no failed/degraded items** と表示されます。

組織構成メニュー

ホーム (**Home**) ページの左側に組織構成のメニューが表示されます。このメニューには HP Web ベースシステムマネジメントソフトウェアへのリンクがあり、以下のものが含まれます。

- **Integrated Agents** パーティシパントと、それらのエントリーポイント(ある場合)へのリンクが含まれます。エージェントのリンクをクリックすると、その特定のエージェント

にアクセスすることができます。パーティシパントとは、HP System Management Homepage (HP SMH) に含まれる情報を提供しているエージェントを指します。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ければ、**none** と表示されます。

- **Other Agents** HP SMH のパーティシパントではない、表示可能な HP Web ベースシステムマネジメントソフトウェアを一覧表示します。HP Web ベースシステムマネジメントソフトウェアの名前はリンクになっており、エージェントがユーザーインタフェースを提供している場合には、そのエージェントにアクセスすることができます。この情報を提供する HP Web ベースシステムマネジメントソフトウェアがインストールされていなければ、**none** と表示されます。
- **Management Processor** リモート **Insight** ボード **Lights-Out Edition (RiLOE)** ボード、または **Integrated Lights-Out (iLO)** ボードへのリンクを表示します。この情報は HP Insight マネジメントエージェントから提供されます。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ければ、**none** と表示されます。
- **Other Software/Other Links** ProLiant、Integrity、サポート、フォーラムへのリンクを表示します。
- **KEY/Legend** ステータスアイコンと各アイコンの簡単な説明のリストを表示します。
 -  正常 (OK)
 -  劣化 (Degraded)
 -  障害 (Failed)
 -  不明 (Unknown)

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 B8465BA (WBEM Services for HP-UX) と SysFaultMgmt (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。

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。

関連トピック

- [設定ページ](#)
- [タスクページ](#)
- [ツールページ](#)
- [ログページ](#)

設定ページ

設定 (**Settings**) ページには、HP System Management Homepage (HP SMH) とツール (**Tools**) 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」を参照してください。

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を表示します。
- 「セキュリティ」 セキュリティオプションのリンクを表示します。

関連手順

- メニュー
- カスタムメニューの追加
- カスタムメニューの削除
- クレジット
- セキュリティ
- IP バインディング
- IP 制限ログイン
- ローカルサーバ証明書
- ローカル/Anonymous アクセス
- 高信頼性モード
- 信頼済み管理サーバ
- ユーザーグループ

関連トピック

- 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

メニュー (**Menus**) カテゴリには、カスタムメニューの追加と削除を行うためのリンクがあります

- **Settings->Menus->Add Custom Menu**の順に選択します。
- **Settings->Menus->Remove Custom Menu**の順に選択します。

関連手順

- カスタムメニューの追加
- カスタムメニューの削除

関連トピック

- 設定ページ

カスタムメニューの追加

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。

以下の手順で、カスタムメニューを HP SMH に追加します (HP-UXのみ)。

1. **Settings->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の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。たとえば、**Home**、**Tasks**、**Tools** または別のページを指定します。
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。カテゴリを指定しない場合、メニューはどのカテゴリでも表示されます。
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 ページへの 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 ユーザー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 ユーザー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 ユーザーとして実行に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ー権限を持つ HP SMH ユーザーは、実行を許可されたカスタムメニューをユーザーログインの実際のユーザー 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。

関連トピック

- 設定ページ
- メニュー
- カスタムメニューの削除

カスタムメニューの削除

Remove Custom Menu リンクは、カスタムメニューを削除する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、**Settings->Menus->Remove Custom Menu**の順に選択します。

関連トピック

- 設定ページ
- メニュー
- カスタムメニューの追加

クレジット

Credits リンクは、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を表示します。

Credits にアクセスするには、**Settings->System Management Homepage->Credits**の順に選択します。

関連トピック

- 設定ページ

セキュリティ

Security 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 バインディング** **Settings->System Management Homepage->Security->IP Binding**の順に選択します。
- **IP 制限ログイン** **Settings->System Management Homepage->Security->IP Restricted Login**の順に選択します。
- **ローカルサーバ証明書** **Settings->System Management Homepage->Security->Local Server Certificate**の順に選択します。
- **ローカル/Anonymous アクセス** **Settings->System Management Homepage->Security->Local/Anonymous Access**の順に選択します。

- 高信頼性モード **Settings>System Management Homepage>Security>Trust Mode**の順に選択します。
- 信頼済み管理サーバ **Settings>System Management Homepage>Security>Trusted Management Servers**の順に選択します。
- ユーザーグループ **Settings>System Management Homepage>Security>User Groups**の順に選択します。

注記:



ユーザーアカウントを設定するには、管理対象のユーザー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 (**Tools**) ページの下に Users and Groups (ugweb) のユーザーインタフェースが含まれています。

関連手順

- IP バインディング
- IP 制限ログイン
- ローカルサーバ証明書
- ローカル/Anonymous アクセス
- 高信頼性モード
- 信頼済み管理サーバ
- ユーザーグループ

関連トピック

- 設定ページ

IP バインディング

IP バインディングは、いずれの IP アドレスからの要求を HP System Management Homepage (HP SMH) が受け入れるかを指定し、いずれのネットやサブネットからの要求が処理されるかを管理します。

管理者は、HP SMH を構成し、**IP Binding** ウィンドウで指定したアドレスだけをバインド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することができます。

サーバ上の IP アドレスは、マスクが適用された後、入力された IP バインディングアドレスの 1 つに一致すると、バインドされます。

注記:



HP SMH は常に 127.0.0.1 にバインドします。IP バインディングが有効になっていて、サブネット/マスクのペアが構成されていない場合は、HP SMH は

127.0.0.1 に対してのみ使用可能になります。IP バインディング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します。

以下の手順で IP バインディングを設定します。

1. **Settings>System Management Homepage>Security**の順にクリックします。
2. **IP Binding** をクリックします。
3. **IP Binding** ボックスをクリックして、IP バインディングを有効にします。
4. **Subnet IP Address** を入力します。
5. **Netmask** を入力します。
6. **Save Configuration** をクリックして現在の設定を保存するか、**Reset Values** をクリックしてすべての変更をキャンセルします。

Save Configuration をクリックすると、次のメッセージが表示されます。

Setting this value requires restarting HP System Management Homepage which may require you to log in again.

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 から 255 の間の値の 4 つのオクテットで設定しなければなりません (各ネットマスクも同じ)。
 - ネットマスクは最高位ビットを 1 で開始し、すべての 1 が 0 に切り替わるまで、すべて 1 のままです。例: 255.255.0.0, 192.0.0.0, 255.192.0.0。

関連トピック

- セキュリティ
- IP 制限ログイン
- ローカルサーバ証明書
- ローカル/Anonymous アクセス
- 高信頼性モード
- 信頼済み管理サーバ
- ユーザーグループ

IP 制限ログイン

IP 制限ログインによって、システムの IP アドレスに基づき、HP System Management Homepage (HP SMH) がログインアクセスを制限することができます。

アドレス制限は、インストール時に設定するか、または管理者が**IP Restricted Login**ページから設定することができます。

- エクスクルードされている IP アドレスは、それが included ボックスにリストされていても除外されます。
- IP アドレスがインクルードリストにある場合は、ローカルホストとそれらの IP アドレスのみが、ログインアクセスを許可されます。

- IP アドレスがインクルードリストにない場合は、ログインアクセスは、エクスクルードリストにない任意の IP アドレスに許可されます。

以下の手順で、IP アドレスを制限します。

1. **Settings>System Management Homepage>Security**の順にクリックします。
2. **IP Restricted Login** をクリックします。
3. **IP Restricted Login** ボックスを選択して、制限付きログインを有効にします。
4. エクスクルードする IP アドレスを入力します。
5. インクルードする IP アドレスを入力します。
6. **Save Configuration** をクリックして現在の設定を保存するか、**Reset Values** をクリックしてすべての変更をキャンセルします。

Save Configuration をクリックすると、次のメッセージが表示されます。

Setting this value requires restarting the HP System Management Homepage which may require you to log in again.

7. **OK** をクリックします。

関連トピック

- セキュリティ
- IP バインディング
- ローカルサーバ証明書
- ローカル/Anonymous アクセス
- 高信頼性モード
- 信頼済み管理サーバ
- ユーザーグループ

ローカルサーバ証明書

Local Server Certificate リンクでは、当社が生成したものではない証明書を使用可能にすることができます。

以下の手順を実行すると、もともと HP System Management Homepage (HP SMH) によって生成された自己署名の証明書が、Certificate Authority (CA) によって発行されたものに置き換えられます。

- この手順の最初のステップは、HP SMH に **Certificate Request (PKCS #10)** を生成させることです。この要求は、自己署名の証明書に関連付けられたオリジナルの秘密鍵を使用して、証明書要求に対して適切なデータを生成します。秘密鍵は、この手順が終了するまでサーバにあります。
- **PKCS #10** データが作成されたら、次にそれを Certificate Authority に送信します。セキュリティ保護された証明書要求の送信またはセキュリティ保護された証明書の受信に関しては、お客様の会社の方針に従ってください。
- Certificate Authority から **PKCS #7** データが返されたら、最後にこれを HP SMH にインポートします。

- **PKCS #7** データが正常にインポートされると、Windows の場合はオリジナルの \hp\sslshare\cert.pem 証明書ファイル、HP-UX と Linux の場合は /opt/hpsmh/sslshare/cert.pem ファイルが、**PKCS #7** データエンベロープからのシステム証明書で上書きされます。以前の自己署名の証明書に使用されたのと同じ秘密鍵が、新しいインポートされた証明書にも使用されます。キーファイルが存在しないときは、この秘密鍵が起動時にランダムに生成されます。

以下の手順で、証明書を作成します。

1. **Settings>System Management Homepage>Security**の順に選択します。
2. **Local Server Certificate** を選択します。
3. **Organization** や **Organizational Unit** フィールドのデフォルト値を、最大 64 文字までの任意の値で置き換えることができます。
4. **Create PKCS #10 Data** をクリックします。 **PKCS #10 Certificate Request** データが正常に生成され、HP-UX の場合は /opt/hpsmh/sslshare/req_cr.pem に、Linux の場合は /opt/hp/sslshare/req_cr.pem に、Windows の場合は c:\hp\sslshare\req_cr.pem にそれぞれ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. セキュリティ保護された方法を使用して **PKCS #10** 証明書要求データを Certificate Authority に送信し、証明書要求応答データを **PKCS #7** フォーマットの形式で要求します。応答データが Base64 でエンコードされたフォーマットであることを要求します。お客様の組織で自身の公開鍵基盤 (PKI) をお持ちの場合、または証明書サーバが導入されている場合は、**PKCS #10** データを CA マネージャに送信し、**PKCS #7** 応答データを要求します。

注記:



サードパーティの証明書署名者は一般的に有料です。

7. 証明書署名者が **PKCS #7** のエンコードされた証明書要求応答データを送信する際に、**PKCS #7** 証明書要求応答からデータをコピーし、**PKCS #7 Data** フィールドにコピーしたデータをペーストしてください。この場合、次のステップは必要ありません。
8. **Import PKCS #7 Data** をクリックします。生成した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が含まれる管理対象システムを参照します。
11. ブラウザでプロンプトが表示された場合、証明書の表示を選択します。証明書をブラウザにインポートする前に、必ず、署名者が当社ではなくお客様が使用した署名者としてリストされるようにしてください。

注記:



選択した証明書署名者が、**PKCS #7** データではなく Base64 でエンコードされた形式で証明書ファイルを送信する場合は、Base64でエンコードされた証明書ファイルを、HP-UX の場合は /opt/hpsmh/sslshare/req_cr.pem に、Linux の場合は /opt/hp/sslshare/req_cr.pem に、Windows の場合は c:\hp\sslshare\req_cr.pem にコピーし、HP System Management Homepage を再起動します。

関連トピック

- セキュリティ
- IP バインディング
- IP 制限ログイン
- ローカル/Anonymous アクセス
- 高信頼性モード
- 信頼済み管理サーバ
- ユーザーグループ

ローカル/Anonymous アクセス

Local/Anonymous アクセスでは、以下のアクセスに対して適切な設定を選択することができます。

- **Anonymous** アクセス デフォルトでは無効です。 **Anonymous Access** を有効にすると、ユーザーはログインせずに HP System Management Homepage (HP SMH) にアクセスできるようになります。 **Anonymous** を選択すると、任意のローカルユーザーがユーザー名やパスワードを聞かれることなく、限定されたセキュアでないページにアクセスできるようになります。

注意: anonymous アクセスの使用は推奨していません。

- **ローカルアクセス** デフォルトでは無効です。有効にすると、認証を求められずに HP SMH へローカルアクセスできるようになります。ローカルコンソールへのアクセス権限を持つユーザーは、**Administrator** が選択されていれば誰でも完全なアクセス権限が与えられることを意味します。

注意: ご使用の管理サーバソフトウェアでローカルアクセスを有効にしている場合を除き、ローカルアクセスの使用は推奨していません。

以下の手順で、anonymous アクセスを有効にします。

1. **Settings>System Management Homepage>Security**の順に選択します。
2. **Local/Anonymous Access** を選択します。
3. **Anonymous Access** を選択します。
4. **Save Configuration** をクリックして、設定を保存します。

注記:



HP System Management Homepage が HP Systems Insight Manager (HP SIM) と同じマシンで実行されている場合は、HP SIM の特定の機能が働くように、**Local Access (Anonymous)** を有効にする必要があります。**Local Access (Administrator)** や **Anonymous Access** が有効になっている場合も機能しますが、有効にしておく必要はありません。

以下の手順で、ローカルアクセスを有効にします。

1. **Settings>System Management Homepage>Security**の順に選択します。
2. **Local/Anonymous Access** を選択します。
3. **Local Access** を選択してローカルアクセスを有効にします。
4. **Anonymous** または **Administrator** を選択します。
5. **Save Configuration** をクリックして、設定を保存します。

関連トピック

- セキュリティ
- IP バインディング
- IP 制限ログイン
- ローカルサーバ証明書
- 高信頼性モード
- 信頼済み管理サーバ
- ユーザーグループ

高信頼性モード

Trust Mode リンクを使用すると、お使いのシステムに必要なセキュリティを選択することができます。他よりも高いレベルのセキュリティを必要とする状況があります。そのような場合は、以下のセキュリティオプションが使用できます。

- **Trust by Certificate** 信頼できる証明書のある HP Systems Insight Manager (HP SIM) サーバからのみ構成変更を受け入れるように HP System Management Homepage (HP SMH) を設定します。このモードは、送信先サーバに、証明書による認証を提供することを要求します。このモードは、アクセスを許可する前に証明書データを要求し、デジタル署名を確認するため、最もセキュリティが高い方法です。リモートの構成変更をすべて無効にしたい場合は、**Trust by Certificate** を選択したままにし、証明書をインポートせずに信頼できるシステムのリストを空欄のままにしてください。

注記:



このオプションはより安全性が高いため、ご使用を強くお勧めします。

- **Trust by Name** **Trust By Name** フィールドで指定された HP SIM 名を持つサーバからのみ特定の構成変更を受け入れるように HP SMH を設定します。 **Trust By Name** オプションは簡単に設定することができます。たとえば、2 つの別個の区分に 2 つの別個の管理者グループがある、セキュリティ保護されたネットワークがある場合、このオプションを使用します。これにより 1 つのグループが間違えたシステムにソフトウェアをインストールするのを防ぎます。このオプションでは送信された HP SIM サーバ名のみを検証します。

注記:



このオプションは安全性が劣るため、**Trust by Certificate** オプションの使用を強く推奨します。

- **Trust All** 任意のシステムから特定の構成変更を受け入れるように HP SMH を設定します。

注記:



このオプションは安全性が劣るため、**Trust by Certificate** オプションの使用を強く推奨します。

高信頼性モードの設定

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

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

Windows の場合、インポートした HP SIM 証明書は systemdrive \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、管理用権限が必要です。

以下の手順で、証明書による信頼を設定します。

1. **Settings>System Management Homepage>Security**の順に選択します。
2. **Trust Mode** をクリックします。
3. **Trust by Certificate** を選択して、信頼できる証明書を要求します。

4. **Trusted Certificate** をクリックして、信頼済み管理サーバ証明書にアクセスします。
5. **Save Configuration** をクリックして現在の構成を保存するか、**Reset Values** をクリックしてすべての変更をキャンセルします。

サーバ名による信頼を設定するには、以下の手順に従います。

1. **Settings>System Management Homepage>Security**の順に選択します。
2. **Trust Mode** をクリックします。
3. サーバー名による信頼を設定するには、**Trust by Name** を選択します。
4. サーバ名を入力します。
5. **Save Configuration** をクリックして現在の構成を保存するか、**Reset Values** をクリックしてすべての変更をキャンセルします。

サーバ名オプションは、以下の基準を満たさなければなりません。

- 各サーバ名は 64 文字未満にします。
- サーバ名リスト全体の長さは 1,024 文字以内にします。
- 次の特殊文字は使用できません。 `server_name: ~ ' ! @ # $ % ^ & * ( ) + = \ " : ' < > ? , |`
- `server_names` の区切りにはセミコロンを使用します。

以下の手順で、すべてのサーバを信頼するよう設定します。

1. **Settings>System Management Homepage>Security**の順に選択します。
2. **Trust Mode** をクリックします。
3. すべてのサーバを信頼するには、**Trust All** を選択します。
4. **Save Configuration** をクリックして現在の構成を保存するか、**Reset Values** をクリックしてすべての変更をキャンセルします。

関連トピック

- 証明書の自動インポート
- セキュリティ
- IP バインディング
- IP 制限ログイン
- ローカルサーバ証明書
- ローカル/Anonymous アクセス
- 信頼済み管理サーバ
- ユーザーグループ

信頼済み管理サーバ

Trusted Management Servers リンクを使用すると、証明書を **Trusted Certificates List** で管理できます。

- **Import Certificate Data** 証明書は、HP Systems Insight Manager (HP SIM) と HP System Management Homepage (HP SMH) 間の信頼関係を作るために使用されます。
- **Add Certificate From Server** 信頼できる証明書を HP SIM サーバから追加することができます。

以下の手順で、証明書を信頼済み証明書リストにインポートします。

1. **Settings>System Management Homepage>Security>Trusted Management Servers**の順に選択します。
2. **Add Certificate From Server** 領域で、追加する証明書のある HP SIM システムの名前または IP アドレスを入力します。
3. **Import Certificate Data** 領域で、テキストボックスに Base64 エンコードの証明書をカットアンドペーストします。
4. **Import Certificate Data** をクリックします。

以下の手順で、サーバから証明書を追加します。

1. **Settings>System Management Homepage>Security>Trusted Management Servers**の順に選択します。
2. **Add Certificate From Server** 領域で、追加する証明書のある HP SIM サーバの名前を入力します。
3. **Add Certificate From Server** をクリックします。 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提示されます。
4. **Verify the Certificate** ウィンドウの証明書情報を確認し、それ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。

関連トピック

- セキュリティ
- IP バインディング
- IP 制限ログイン
- ローカルサーバ証明書
- ローカル/Anonymous アクセス
- 高信頼性モード
- ユーザーグループ

ユーザーグループ

HP System Management Homepage (HP SMH) は、認証にオペレーティングシステムアカウントを使用し、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管理を可能にします。

Windows の **Administrators** オペレーティングシステムグループのユーザー、または HP-UX や Linux の **root** オペレーティングシステムグループ (デフォルトで root ユーザーを含むグループ) が、**Administrator**、**Operator**、または **User** の HP SMH アクセスレベルに応じたオペレーティングシステムグループを定義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を追加した後、オペレーティングシステム管理者はオペレーティングシステムユーザーをこれらのオペレーティングシステムグループに追加することができます。

HP SMH の各アクセスレベルは、最大で 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 のインストール中に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。HP SMH の起動時に特定のオペレーティングシステムグループが定義されていない場合は、オペレーティングシステムグループが定義されていないことを示す System Management Homepage ログメッセージが表示されます。

HP SMH に使用するアカウントは、ホストオペレーティングシステムで上位レベルのアクセス権限を持っている必要はありません。管理権限を持つ HP SMH ユーザーは HP SMH の各アクセスレベルにオペレーティングシステムユーザーグループを指定することができます。指定すると、各オペレーティングシステムユーザーグループ内のすべてのアカウントが **User Groups** ウィンドウで指定する HP SMH へのアクセス権限を持ちます。Windows 管理者グループおよび HP-UX と Linux ルートグループは、自動的にシステムへの管理アクセス権限が与えられます。

たとえば、HP SMH 管理者アクセスレベルは、ユーザーが作成したオペレーティングシステムグループ Admin1、Admin2、および Admin3 に割り当てることができます。オペレーティングシステムユーザーグループ (Admin1、Admin2、または Admin3) のメンバーであるユーザーはすべて、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レベルのアクセス権限を持っているかどうかに関係なく、HP SMH 上での管理権限が与えられます。

User Groups ウィンドウで HP SMH にユーザーグループを追加することができます。以下のレベルのユーザーグループ権限が使用できます。

- **Administrator Administrator** アクセス権限を持つユーザーは、HP SMH が提供する情報をすべて見ることができます。該当のデフォルトユーザーグループ (Windows では **Administrators**、HP-UX と Linux では **root**) は、常に管理アクセス権限を持っています。
- **Operator Operator** アクセス権限を持つユーザーは、HP SMH が提供す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 アプリケーションは、ほとんどの重要情報へのアクセスを管理者のみに制限しています。
- **User User** アクセス権限を持つユーザーは、HP SMH が提供するほとんどの情報を見ることができます。一部の Web アプリケーションは、**User** アクセス権限を持つユーザーが重要情報を見ることを制限しています。

以下の手順で、管理者グループを追加します。

1. **Settings>System Management Homepage>Security**の順に選択します。
2. **User Groups** をクリックします。
3. **Administrator** セクションで、ユーザーグループ名を入力します。
4. **Save Configuration** をクリックして現在の設定を保存するか、**Clear All Groups** をクリックしてフィールドをクリアするか、**Reset Values** をクリックしてすべての変更をキャンセルします。

以下の手順で、オペレータグループを追加します。

1. **Settings>System Management Homepage>Security**の順に選択します。
2. **User Groups** をクリックします。
3. **Operator** セクションで、ユーザーグループ名を入力します。

4. **Save Configuration** をクリックして現在の設定を保存するか、**Clear All Groups** をクリックしてフィールドをクリアするか、**Reset Values** をクリックしてすべての変更をキャンセルします。

以下の手順で、ユーザーグループを追加します。

1. **Settings>System Management Homepage>Security**の順に選択します。
2. **User Groups** をクリックします。
3. **User** セクションで、ユーザーグループ名を入力します。
4. **Save Configuration** をクリックして現在の設定を保存するか、**Clear All Groups** をクリックしてフィールドをクリアするか、**Reset Values** をクリックしてすべての変更をキャンセルします。

関連トピック

- セキュリティ
- IP バインディング
- IP 制限ログイン
- ローカルサーバ証明書
- ローカル/Anonymous アクセス
- 高信頼性モード
- 信頼済み管理サーバ

タスクページ

タスク (**Tasks**) 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からタスクが提供されていない場合、タスク (**Tasks**) 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ーのユーザー ID で実行されるため、すべての HP SMH ユーザー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ー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ーのユーザー ID で実行されるため、すべての HP SMH ユーザー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ーとしてログインしてください。

関連トピック

- ホームページ
- 設定ページ
- ツールページ
- ログページ

ツールページ

ツール (**Tools**) 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管理ツールへのリンクが表示されます。HP-UX の場合、ツール (**Tools**) ページでは、System Administration Manager (SAM) のメインページ (SAM Functional Area Launcher (FAL) と呼ばれます) に類似した管理ツールへの入口が提供されます。これには、nPartition Management、Peripheral Devices、Disks and File Systems、Accounts for Users and Groups、Kernel Configuration などの領域が含まれます。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。

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からツールが提供されていない場合、ツール (**Tools**) ページは表示されません。

関連トピック

- ホームページ
- 設定ページ
- タスクページ
- ログページ

ログページ

ログ (**Logs**) ページでは、少なくとも以下のログカテゴリを提供します。

- System Management Homepage Log
- System Management Homepage Legacy Log (Linux および Windows のみ)
- SAM Log Viewer (HP-UXのみ)

インストールされた HP Web ベースシステムマネジメントソフトウェアのログはいずれも、このページに表示することができます。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 (**Logs**) 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

関連トピック

- 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 Log には、HP System Management Homepage (HP SMH) のレベル設定変更、成功したログイン試行と失敗したログイン試行が含まれます。これは、直接 HP SMH にログインする場合や HP Systems Insight Manager (HP SIM) からログインする場合のログインまたはアクセスの問題のトラブルシューティングに役立ちます。

注記:



System Management Homepage Log にアクセスするには、HP SMH への管理アクセス権限が必要です。

System Management Homepage Log にアクセスするには、**Logs->System Management Homepage->System Management Homepage Log**の順に選択します。

関連トピック

- ログページ
- System Management Homepage レガシーログ

- SAM ログ

System Management Homepage レガシーログ

Linux や Windows システムに、HP System Management Homepage (HP SMH) 2.0.0 のインストール以前に 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る場合、そのログは **System Management Homepage** カテゴリ内の **System Management Homepage Legacy Log** リンクをクリックして見るすることができます。このログには、新しいバージョンのインストール以前に起こった、セキュリティ関連のイベントに関する履歴情報が含まれます。HP-UX には Legacy Log はありません。

System Management Homepage Legacy Log にアクセスするには、**Logs>System Management Homepage>System Management Homepage Legacy Log**の順に選択します。

注記:



HP System Management Homepage Legacy Log にアクセスするには、HP SMH への管理アクセス権限が必要です。

関連トピック

- ログページ
- System Management Homepage ログ
- SAM 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、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。

SAM Log にアクセスするには、**Logs>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。メッセージが画面の下に表示されます。

関連トピック

- ログページ
- System Management Homepage ログ
- System Management Homepage レガシーログ

トラブルシューティング

注記:



HP-UX、Linux、または Windows オペレーティングシステムにのみ適用と記述されているトピックは、該当するオペレーティングシステムにのみ適用されます。

ブラウザの問題

Windows で **Internet Explorer 6.0** を使用しているときに、**HP System Management Homepage (HP SMH)** にログインすると、セキュリティの警告ダイアログボックスに警告が表示されます。

解決策: 次の 2 種類の警告が表示される場合があります。

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

この警告は、IP アドレスを使用して HP SMH をブラウズしているときに表示されます。また、そのマシン名のローカルホストを使用して、ローカルでブラウズしているときにも表示されます。

- 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。

証明書は HP SMH から発行されます。証明書を **Trusted Certificate List** に追加すると警告は表示されなくなります。

Mozilla ブラウザを 2 個開くと、**HP SMH** への未許可ログインのように表示される場合があります。

解決策: 別々に起動した Mozilla ブラウザはセッションを共有します。

注記:



注: デスクトップから起動すると、Mozilla は別々のセッションを共有します。Internet Explorer ではそれらのセッションは共有されません。

Windows 2003 で **Internet Explorer** から **HP SMH** をブラウズしていると、セキュリティメッセージが表示されたり、ページが部分的にしか表示されません。

解決策: Windows 2003 サーバ上の Internet Explorer 6.0 は、デフォルトのインストールでは異なるセキュリティ設定がなされています。この問題を回避するには、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 度追加します。1 度目は **http://hostname:2301** として、2 度目は **https://hostname:2381** として追加します。別の解決策としては、ブラウザでセキュリティ設定のレベルを下げるか (推奨しません)、ブラウザのセキュリティ設定でクッキーを許可し (保存、およびセッションごとの両方)、アクティブスクリプトを許可します。

ブラウザページにすべてのコンテンツが表示されません。

解決策: フレームサイズはフォントサイズ「中」で最適化されています。ブラウザで、大きな、または小さなフォントを使用している場合は、マウスを使用して手動でフレームレイアウトを調整してください。

システムにアクセスすると、クッキーを受け入れるよう促すプロンプトがブラウザに表示されます。

解決策: ブラウザのクッキーは、ユーザーの状態およびセキュリティを常に把握するために必要です。ブラウザでクッキーを有効にすると、このプロンプト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はどうすればわかりますか。

解決策: サポートされているブラウザは、以下のとおりです。

接続しているサーバタイプにかかわらず HP-UX Itanium または PA-RISC システムで動作している以下のデスクトップブラウザ、または HP-UX サーバでローカルに動作しており、X 経由で任意のデスクトップに表示されるブラウザ。

- Mozilla 1.6

接続しているサーバタイプにかかわらず、Windows Itanium または x86 システムで動作している以下のデスクトップブラウザ。

- Internet Explorer 6.0 以上
- Mozilla 1.5
- Mozilla 1.6

接続しているサーバタイプにかかわらず、Linux IPF または x86 システムで動作している以下のデスクトップブラウザ。

- Mozilla 1.5
- Mozilla 1.6

HP-UXに **http://hostname/2301** でログインすることはできますが、**https://hostname/2381** ではできません。

解決策: デフォルトでは、HP-UX は自動起動機能が有効な状態でインストールされています。デーモンはポート 2301 でリスンし、要求されたときにポート 2381 で HP SMH の起動のみを行います。そしてタイムアウト期間の後、再び停止します。詳細は smhstartconfig(1M) コマンドを参照してください。

Windows 2003 を実行しているローカルマシンで **https://ipaddress:2381** をブラウズすると、**Login** 画面が表示されません。

解決策: Windows 2003 上の Internet Explorer 6.0 では、**Login** ページ全体が表示されずに、代わりに青いバーで **Account Login** テキストのみ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ブラウズしているときにのみ起こります。IP アドレスを URL で指定せずに、**hostname** で指定することで問題を解決できます。

この問題を解決するために以下の URL を使用することを推奨します。

https://hostname:2381

Windows XP システムを **Service Pack 2** に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した。

解決策: Windows XP Service Pack 2 ではソフトウェアファイアウォールが実装されるため、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のアクセスに必要なポートにアクセスするのを妨げてしまいます。この問題を解決するには、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へのブラウザのアクセスを許可するように、ファイアウォールに例外を設定しなければなりません。

以下の対応を推奨します。

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行います。
3. 例外を選択します。
4. ポートの追加をクリックします。

名前とポート番号を入力します。

ファイアウォール保護に以下の例外を追加します。

製品名	ポート番号
HP SMH セキュリティ保護されていないポート:	2301
HP SMH セキュリティ保護されたポート:	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。

この設定はデフォルトの SP2 セキュリティ拡張はそのまま、上記のポートを通るトラフィックを許可します。これら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。ご利用のブラウザとの適切な通信を可能にするために、セキュリティ保護されているポートと保護されていないポートを追加する必要があります。

インストールの問題

HP SMHのインストール中に **Another instance is running.** というエラーメッセージが表示されます。

解決策: 破損ファイルのあるシステムに HP SMH をインストールしようとしたり、インストールを中断するとこのメッセージが表示されます。

この問題を解決するには、HP System Management Homepage システムの \temp ディレクトリにナビゲートし、smhlock.tmp ファイルを削除してください。

HP SMH のインストール中に、**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. というエラーメッセージが表示されます。

解決策: このエラーは、Linux システムでインストールのインスタンスが 2 つ以上起動されると表示されます。HP SMH のインストールは 1 度に 1 つしか実行できません。

IP アドレスの問題

使用しているブラウザで、**IP** アドレスを取得せずにローカルシステムにアクセスできる簡単な方法はありますか。

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することができます。HP-UX では、自動起動のデフォルト設定を有効なままにしておくと、**http://hostname:2301** でローカルシステムにアクセスすることができます。

注記:



localhost という単語は、すべての言語で機能するわけではありません。さらに、ブラウザで設定したプロキシサーバがあれば、プロキシされてはならないアドレスのブラウザリストに 127.0.0.1 を加える必要がある場合があります。

IP 制限ログイン機能を **Windows 2000 Advanced Server** で使用すると、サーバに **IP** アドレスを入力しても想定した結果が得られません。ローカルマシンの **IP** アドレスを認識するにはどうしたらよいですか。

解決策: Microsoft Windows NT 4.0 および Windows 2000 Advanced Server では、ローカルマシンをインクルード、またはエクスクルードするには、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。アドレス 127.0.0.1 は常に **include** セクションに含まれているため、**exclude** セクションに明示的に配置された場合に限り、除外されます。

IP 制限が設定されているにもかかわらず、ローカルホストのアクセスが拒否されません。

解決策: インクルードフィールドにローカルホスト用の IP アドレスを含めない場合でも、ほとんどのユーザーはローカルホストのアクセスをブロックしようとしないうえ、ローカルホストはアクセスを認められます。ローカルホストのアクセスをブロックする必要がある場合は、**IP Restriction** の下の **Exclude** フィールドに **127.0.0.1** と入力します。

IP Restriction の下で、システムのローカル **IP** アドレス、または **127.0.0.1** を **Include** リストに加えていないのに、ローカルでブラウズすることができます。

解決策: ユーザーが意図しないにも関わらず、HP SMH アクセスからユーザー自身をロックしてしまうことへの予防措置として、**Include** リストにローカル IP アドレスが入っていないときでも、ローカルホストの要求は拒否されません。どうしても必要な場合は、ローカルシステムの IP アドレスおよび 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を得ようとするユーザーへのアクセスを拒否することができます。

ログインの問題

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

解決策: 有効な Windows オペレーティングシステムアカウントが設定されていることと、ログインが **Administrators** グループ、または HP SMH オペレーティングシステムグループの 1 つに含まれていることを確認します。

オペレーティングシステムにログインします。要求された場合、パスワードを変更します。

注記:



パスワードを要求するこのプロンプトが表示される場合、オペレーティングシステム管理者が、**user must change the password on next login** オプションが選択された状態でユーザーアカウントを設定しています。

オペレーティングシステム管理者は、今後作成されるログインを、**user must change the password on next login** オプションを選択しない状態で追加することができます。このオプションが選択されていると、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することができます。

HP SMH をアップグレードした後、パスワードが使用できなくなりました。

解決策: HP SMH 2.0 より前のバージョンでは 3 つの固定アカウント(**administrator**、**operator**、**user**)を使用していたのに対し、2.0 以降ではオペレーティングシステムアカウントを使用します。管理者グループ (Linux では root グループ) に属するオペレーティングシステムアカウントはすべて、HP SMH への管理アクセス権限があります。このアクセス権限を用いて、他のオペレーティングシステム アカウントグループのアカウントを、HP SMH への異なるアクセスレベルに割り当てることができます。HP SMH のオンラインヘルプにこのプロセスの詳細な説明があります。これは HP-UX には適用されません。

デフォルト設定を使用して **HP SMH** で使う新しい **Windows** アカウントを作成しましたが、そのアカウントでログインできません。

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た新しいアカウントに **user must change the password on next login** が設定されています。そのアカウントを HP SMH へのログインに使用する前に、このオプションを選択解除する必要があります。

Windows で **Internet Explorer 6.0** を使用し、管理サーバーを通じて IP アドレスで検出されたシステムをブラウズすると、**HP SMH** にログインできません。**anonymous** アクセスが有効になっている場合は、**anonymous** で入ることができますが、ユーザー名が正しくありません。

または

Windows で **Internet Explorer 6.0** を使用し、管理サーバを通じて IP アドレスで検出されたデバイスをブラウズすると、詳細な証明書情報が **Automatic Import Certificate** 画面のテキストボックスに表示されません。

解決策: これらの問題は、次の 2 つの方法で Internet Explorer の設定を調整することで解決できます。

- 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推奨できません。

以下の手順で、設定を変更します。

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. スライダーをクリックして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

- ターゲット HP SMH の IP アドレスをローカルイントラネットゾーンに追加します。

以下の手順で、設定を変更します。

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に、HP SMH システムの IP アドレスを入力します。例: **https://ipaddress**
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。

Windows XP システムを **Service Pack 2** に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した。

解決策: Windows XP Service Pack 2 ではソフトウェアファイアウォールが実装されるため、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 のアクセスに必要なポートにアクセスするのを妨げてしまいます。この問題を解決するには、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へのブラウザのアクセスを許可するように、ファイアウォールに例外を設定しなければなりません。

以下の対応を推奨します。

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行います。
3. 例外を選択します。
4. ポートの追加をクリックします。
名前とポート番号を入力します。

ファイアウォール保護に以下の例外を追加します。

製品名	ポート番号
HP SMH セキュリティ保護されていないポート:	2301
HP SMH セキュリティ保護されているポート:	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。

この設定はデフォルトの SP2 セキュリティ拡張はそのまま、上記のポートを通るトラフィックを許可します。これら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。ご利用のブラウザとの適切な通信を可能にするために、セキュリティ保護されているポートと保護されていないポートを追加する必要があります。

サーバー名を指定した **http://my-server-name:2301** で、**Internet Explorer** から自身のシステムをブラウズすると、有効な **Windows** 管理者アカウントユーザー名とパスワードを使用してもログインすることができません。ただし、自分の **IP** アドレスを指定した **http://my-ip-address:2301** の場合はログインできます。

解決策: サーバのコンピュータ名にアンダースコア (_) が入っていないか確認してください。入っ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。システム名でログインできるようになるはずです。

注記:

システムの名前を変更した後、Microsoft Internet Information Server (IIS) 設定を変更する必要がある場合があります。



これは Microsoft セキュリティパッチ MS01-055 で Internet Explorer 5.5 および 6.0 に追加されたセキュリティ機能で、不適切な名前構文のシステムがクッキー名を設定するのを防ぎます。クッキー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のみを使用しなければなりません (-または.)。Internet Explorer は、システム名にアンダースコア (_) などの英数字以外の文字が含まれる場合、システムからクッキーをブロックします。

セキュリティの問題

Windows XP システムを **Service Pack 2** に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した。

解決策: Windows XP Service Pack 2 ではソフトウェアファイアウォールが実装されるため、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のアクセスに必要なポートにアクセスするのを妨げてしまいます。この問題を解決するには、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へのブラウザのアクセスを許可するように、ファイアウォールに例外を設定しなければなりません。

以下の対応を推奨します。

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行います。
3. 例外を選択します。
4. ポートの追加をクリックします。

名前とポート番号を入力します。

ファイアウォール保護に以下の例外を追加します。

製品名	ポート番号
HP SMH セキュリティ保護されていないポート:	2301
HP SMH セキュリティ保護されているポート:	2381
HP SIM セキュリティ保護されていないポート:	280
HP SIM セキュリティ保護されているポート:	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。

この設定はデフォルトの SP2 セキュリティ拡張はそのまま、上記のポートを通るトラフィックを許可します。これらのポートは 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 に必要で、ポート 280 および 50000 は HP Systems Insight Manager に必要です。アプリケーションとの適切な通信を可能にするために、各製品ごとにセキュリティ保護されているポートと保護されていないポートを追加する必要があります。

X.509 の証明書を直接 HP SMH にインポートできません。

解決策: HP SMH は証明書要求を Base64 でエンコードした PKCS#10 フォーマットで生成します。この証明書要求は CA に供給されます。ほとんどの証明機関 (CA) は、**Settings>HP System Management Homepage** を選択することで HP SMH に直接インポートできる、Base64 でエンコードした PKCS#7 証明書データを返します。

CA が証明書のデータを X.509 フォーマットで返した場合、X.509 証明書ファイルの名前を cert.pem に変更し、\hp\sslshare ディレクトリに配置します。HP SMH を再起動すると、この証明書が使用されるようになります。

PKCS#7 データ証明書データが承認されません。

解決策: Mozilla ブラウザを使用している場合、Notepad またはその他のエディタを使用して証明書要求および応答データのカットアンドペーストを行うと問題が起こる場合があります。こ

の問題を回避するために、CA からの証明書応答ファイルを開くときは常に Mozilla を使用してください。証明書を取り扱う場合は、Mozilla が提供する Select All、Cut、Paste 操作を必ず使用してください。

秘密鍵ファイルがファイルシステムで保護されません。

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、ファイルシステムで秘密鍵ファイルを保護するには、NTFS フォーマットのシステムドライブが必要です。

顧客が作成した証明書 **PKCS#7** データを **Settings->HP System Management Homepage->Security->Trusted Management Servers** の **HP Systems Insight Manager Certificate Data** フィールドに貼り付けるとエラーが出ます。

解決策: 顧客作成証明書 **PKCS#7** データは **Trusted Management Servers** フィールドに入力するものではありません。**PKCS #7** データは、**Settings→HP System Management Homepage→Security→Local Server Certificate** の **Customer Generated Certificates Import PKCS #7 Data** フィールドにインポートする必要があります。**HP Systems Insight Manager Certificate Data** フィールドは、HP SMH がどの HP Systems Insight Manager サーバを信頼するかを設定するのに使用されます。詳細は、「信頼済み管理サーバ」を参照してください。

Windows 2003 Certificate Authority を使用してサードパーティーの証明書を **HP System Management Homepage** に承認させることができません。

解決策: 次の手順で、Windows 2003 Certificate Authority を使用して HP SMH の証明書を作成します。

1. **Settings->HP System Management Homepage->Security->Local Server Certificate** ページをクリックして **PKCS#10** データパケットを作成します。
2. バッファにデータをコピーするには、**Ctrl+C** キーを押します。
3. **http://W2003CA/certsrv** に移動します。**W2003CA** には、お使いの Windows 2003 Certificate Authority システムの名前を指定します。
 - **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。
 - フィールドに **PKCS#10** データを貼り付けるには **Ctrl+V** キーを押します。
4. Windows 2003 Certificate Authority システムで、以下の操作を行います。
 - **Start->すべてのプログラム->管理ツール->証明機関** の順にクリックします。
 - **CA (Local) ⇒ W2003CA/certsrv** の順にクリックします。**W2003CA** には、お使いの Windows 2003 Certificate Authority システムの名前を指定します。
 - 証明書の保留要求を発行します。
5. **http://W2003CA/certsrv** に移動します。**W2003CA** には、お使いの Windows 2003 Certificate Authority システムの名前を指定します。

- 保留中の証明書の要求の状態を選択します。
- **Base64 encoded** および **Download certificate** (**certificate chain** ではなく) を選択してください。
ダウンロードされるファイルは certnew.cer です。
- certnew.cer のファイル名を cert.pem に変更します。

その他の問題

システムに **HP SMH** をインストールできません。

解決策: HP SMH のインストールには、少なくとも 256 色環境の Java バージョンが必要です。これは Windows にのみ適用されます。

マネジメントプロセッサリンクをクリックしたときに、ページを表示できませんというエラーが出ます。

解決法: マネジメントプロセッサの管理者が、マネジメントプロセッサ上の Web サーバがポート 80 以外のポートを使用するように構成しています。現在、HP SMH はそ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 にあるものと見なします。

root 以外で **HP-UX** または **Linux** にインストールできません。

解決策: 適正なアクセス権限を持つために、HP SMH に root 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 に再インストールするために、root アクセスを模倣する目的で **su-** を使用することはできません。

使用しているバージョンの **Linux** で **HP SMH** をインストールできません。

解決策: HP SMH がサポートする Linux のバージョンは、それぞれ特定の RPM パッケージのセットを必要とします。お使いのシステムでどの RPM パッケージが足りないかを調べるには、HP SMH RPM を冗長(非サイレント)モードでインストールすると、足りない RPM パッケージが一覧表示されます(ある場合)。

サービスおよびサポート

基本ハードウェアのサポートの付属として HP System Management Homepage (HP SMH) のサポートが提供されます。当社のサポートページでは HP SMH の製品、サービス、サポート関連のリソースを幅広く提供しています。

- Software Depot home で HP SMH にアクセスしてください。
<http://www.hp.com/go/softwaredepot> にジャンプして **Security and manageability** を選択します。 **HP System Management Homepage** を検索します。

- HP ProLiant サーバ 管理ソフトウェア
(<http://h50146.www5.hp.com/products/servers/proliant/essentials>) にアクセスしてください。多くのシステム管理製品およびサービス関連情報があります。
- メンテナンスとサポート、フォーラム、および HP 製品のトレーニングと教育については、<http://itrc.hp.com>で HP IT リソースセンタにアクセスしてください。
- HP 製品に関する質問に対する回答を得るには、HP サポートフォーラム
(<http://forums.itrc.hp.com>) を参照してください。

お使いの構成を正しく記録することにより、トラブルシューティングの手順を大幅にスピードアップすることができます。次のリストを最新の状態に保ち、HP サービスプロバイダからサポートを受ける場合に参照してください。

- 管理システム作成、モデル、およびシリアルナンバー情報
- オペレーティングシステム情報、バージョンナンバーを含むオペレーティング環境情報 (HP-UX)、適用されたすべてのサービスパックのリスト、パッチ、Compaq SSD バージョン、適用された Insight Agent 名とバージョン
- Linux および Windows のハードウェア構成情報:
 - Survey Utility 出力または Inspect プリントアウト
 - System Configuration Utility プリントアウト
 - Inspect または System Configuration プリントアウトには表示されない、HP あるいは Compaq 以外の装置の詳細

ご注意

保証

本書に記載した内容は、予告なしに変更することがあります。当社では、本書に関して特殊目的に対する適合性、市場性などについては、一切の保証をいたしかねます。また当社は、お客様の誤った操作に起因する損害については、直接、間接、特殊性、偶発的、派生的であるかを問わず、責任を負いかねますのでご了承ください。備品、パフォーマンス等に関連した損傷についても保証いたしかねます。

当社製品および交換用部品に適用される保証書は、最寄のセールスまたはサービス担当までお申し付けください。

U.S. Government License

Proprietary computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

© Copyright 2004-2005 Hewlett-Packard Development Company, L.P. All rights reserved. Reproduction, adaptation, or translation of this document without prior written permission is prohibited, except as allowed under copyright laws.

登録商標に関する注意

すべての HP 9000 コンピュータの、HP-UX 10.20 リリース以降、および HP-UX 11.00 リリース以降 (32および64ビット構成) は、Open Group UNIX 95ブランドの製品です。

Intelおよび、Itaniumは、米国およびその他の国における Intel Corporation の登録商標であり、ライセンスを受けて使用されています。

Java は Sun Microsystems, Inc. の米国における登録商標です。

Linux は Linus Torvalds の米国における登録商標です。

MS-DOSAMicrosoftAおよび Windowsは、米国およびその他の国における Microsoft Corporation の登録商標です。

UNIX は The Open Group の登録商標です。

出版履歴

発行日およびパーツナンバーは、現在の版を示しています。発行日は、新しい版が発行されると変更されます。マニュアルのパーツナンバーは、広範囲の変更があった場合に変更されます。最新版を確実に受け取るには、適切な製品サポートサービスに申し込む必要があります。詳細は、当社のセールスにおたずねください。

本書に関するフィードバックは、当社の Web サイト <http://docs.hp.com/ja> にある「本サイトのマニュアルに関するフィードバック」からお寄せください。

リリース履歴

改訂履歴

改訂 第3版

2005年12月

MPN: 365395-005. 第 3 版では、HP-UX HP SMH v2.2.1 リリースの機能変更が追加されました。また、オンラインヘルプが 8 ヶ国語に翻訳されました。

改訂 第2版

2005年2月

MPN: 365395-004. 第 2 版では、HP-UX HP SMH v2.2 リリースの情報とタスクが追加されました。

改訂 第1版

2004年11月

MPN: 365395-003. 第 1 版には Linux および Windows 情報とタスクが含まれています。

用語集

注意	本書の内容に従わない場合、機器の損傷や情報の損失につながる場合があります。
証明書	主体の公開鍵を含み、主体についての情報を識別する電子文書。証明書は、キーと主体の ID をバインドするために認証局 (CA) によって署名されます。
Certificate Authority (CA)	デジタル署名と公開鍵と秘密鍵のペアを作成するために使用するデジタル証明書を発行する、信頼できるサードパーティー組織あるいは企業。このプロセスでの CA の役割は、固有の証明書を与えられた個人が、本人であることを保証することです。
CA	参照 Certificate Authority
コマンド行インタフェース (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することのできるコマンドのセット。
CLI	参照 コマンド行インタフェース
ドメインネームサービス (DNS)	ドメインネームを IP アドレスに変換するサービス。
DNS	参照 ドメインネームサービス
外部サイト	サードパーティアプリケーションの URL。
グラフィカルユーザーインタフェース (GUI)	プログラムの使用を簡単にするコンピュータのグラフィック機能の利点を生かしたプログラムインタフェース。HP SMH の GUI は Web が利用可能で、Web ブラウザに表示します。
GUI	参照 グラフィカルユーザーインタフェース
インブレース	ローカルで。たとえば、インブレースインストールは、ローカルにインストールするということを意味します。
HP Systems Insight Manager (HP SIM)	HP システム、クラスタ、デスクトップ、ワークステーション、ポータブルなどの、多様なシステムを管理する機能を提供するシステム管理ソフトウェア。HP Systems Insight Manager は HP Insight Manager 7、HP Tootools、HP Servicecontrol Manager の利点を集約し、HP-UX、Linux、Windows を実行する HP ProLiant、HP Integrity、HP 9000 システムを管理するための単一のツールを提供します。中核となる HP Systems Insight Manager ソフトウェアは、すべての HP サーバプラットフォームを管理するために必要な、重要な機能を提供します。HP Systems Insight Manager は拡張も可能で、HP ストレージ、電源、クライアント、およびプリンタ製品用プラグインによって、他に類のない幅広いシステム管理が行えます。迅速な配備、パフォーマンス管理、およびワークロード管理用プラグインによって、システム管理者は、ハードウェア資産の完全なライフサイクル管理を行うために必要な、付加価値のあるソフトウェアを選ぶことができるようになります。HP Systems Insight

	Manager についての詳細は、 http://www.hp.com/jp/hpsim を参照してください。
HP SIM	参照 HP Systems Insight Manager
HP Insight マネジメントエージェント	ユーザー不在時も定期的に情報を収集する、あるいは他のサービスを行うプログラム。
HP バージョンコントロールエージェント (VCA)	システムにインストールされた Insight マネジメントエージェントによって、サーバにインストールされた HP ソフトウェアを確認できるようになります。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ポイントするように構成することができ、バージョン比較とレポジトリからのソフトウェアアップデートを容易にします。
VCA	参照 HP バージョンコントロールエージェント
HP バージョンコントロールレポジトリマネージャ (VCRM)	Insight マネジメントエージェントによって、ユーザー定義のディレクトリまたはレポジトリに保存された HP が提供するソフトウェアを管理できるようになります。
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
HP Web ベースシステムマネジメントソフトウェア	HP の Web 対応製品を管理するソフトウェア。
Integrity Support Pack	特定のオペレーティングシステムとの連携が確認済みの、HP がバンドルした HP 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コンポーネントが含まれます。これらはすべて、同時にインストールして問題がないことが確認されています。
インターネットプロトコル (IP) の範囲	特定の範囲内の IP アドレスを持つシステム。
IP	参照 インターネットプロトコル (IP) の範囲
ProLiant Support Pack	特定のオペレーティングシステムとの連携が確認済みの、HP がバンドルした HP 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コンポーネントが含まれます。これらはすべて、同時にインストールして問題がないことが確認されています。
公開鍵基盤 (PKI)	公開鍵基盤とは、企業がインターネット上の通信と業務取引のセキュリティを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のことです。
PKI	参照 公開鍵基盤
レポジトリ	ユーザー、ノード、ノードグループ、ロール、ツール、および権限を含む、管理対象クラスタについての重要な情報を保存するデータベース。

Red Hat Package Manager (RPM)	Red Hat Package Managerは、個々のソフトウェアパッケージの作成、インストール、照会、検証、アップデート、およびアンインストールを行うために使用する強力なパッケージマネージャです。パッケージは、ファイルのアーカイブと、名前、バージョンおよび説明を含むパッケージ情報で構成されます。
RPM	参照 Red Hat Package Manager
検索条件	すべての情報のセットから、要求されたサブセットの情報を定義するために使用される変数(情報)のセット。フィルター処理することのできる情報セットには、アクション情報、一部のシステム情報などが含まれます。フィルターは、インクルージョンフィルターとそれに続くエクスクリージョンフィルターで構成されます。これら 2 つのフィルタリング動作の結果は、グループと呼ばれます。このフィルターの一例として、表示可能な情報の作成や、管理オペレーションの実行を可能にする SQL 文があります。
Secure HTTP (HTTPS)	Web 経由での安全なデータ送信をサポートする、HTTP プロトコルの拡張機能。
HTTPS	参照 Secure HTTP
Secure Shell (SSH)	ネットワークを介して他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ためのプログラム。また、システム間でのファイル移動を可能にし、セキュリティ保護されていないチャネル上での認証と通信の保護を提供します。
SSH	参照 Secure Shell
Secure Sockets Layer (SSL)	HTTP と TCP の間にある標準プロトコル階層で、クライアントとサーバ間のプライバシーとメッセージの整合性を提供します。一般的に SSL は、サーバ認証を提供し、クライアントが、存在すると主張しているシステムと通信していることを保証します。アプリケーションプロトコルから独立しています。
SSL	参照 Secure Sockets Layer
Secure Task Execution (STE)	管理対象システムからのタスクの安全な実行。HP SMH のこの機能は、タスクを要求しているユーザーがそのタスクを実行する適正な権限を持っていることを保証し、データを覗かれないように保護するために要求を暗号化します。
STE	参照 Secure Task Execution
自己署名の証明書	自身の Certificate Authority (CA) が認証した証明書で、そのため主体と CA が同じです。 参照 証明書, Certificate Authority
シングルログイン	管理対象システムへの再認証を行わずに、HP SIM 内から任意の管理対象システムをブラウズするために、HP Systems Insight Manager (HP SIM) をブラウズする認証されたユーザーに与えられるパーミッション。HP SIM は認証の開始点であり、他の管理対象システムには HP SIM 内からブラウズする必要があります。

ソフトウェアアップデート	ソフトウェアとファームウェアをリモートでアップデートするタスク。
ステータスタイプ	特定のステータスタイプのシステム (Critical, Failed/Major, Degraded/Minor, Normal, and Unknown)。
サーベイユーティリティ	ハードウェアおよびオペレーティングシステム環境構成情報を集めて配信する、エージェント(またはオンラインサービスツール)。情報は、サーバがオンラインの間に収集されます。
HP System Management Homepage (HP SMH)	HTTP および HTTPS で通信するために、HP Web ベースシステムマネジメントソフトウェアスイートで使用される統合ソフトウェア。均一な機能セットおよびセキュリティを HP Web ベースシステムマネジメントソフトウェアに提供します。
HP SMH	参照 HP System Management Homepage
URI	インターネットのリソースにアクセスする方法を提供します。Uniform Resource Locator (URL)は、Uniform Resource Indicator (URI) の一種です。
URL	World Wide Web 上のリソースのグローバルアドレス。Uniform Resource Locator (URL) は、Uniform Resource Indicator (URI) の一種です。
ユーザー	HP System Management Homepage へ有効なログインを持つネットワークユーザー。
ユーザーアカウント	HP System Management Homepage (HP SMH) へのログインに使用されるアカウント。これらのアカウントは、ローカル Windows ユーザー、ドメインアカウント、または HP-UX や Linux のユーザーグループと、HP SMH 内の特権レベルとペーシング属性を関連付けます。
バージョン管理	Windows/Linux ProLiant システムの場合はバージョンコントロールレポジトリマネージャ、HP-UX オペレーティングシステムの場合は Software Distributor。すべての管理対象 ProLiant または Integrity システム用のソフトウェアステータスの概要を提供し、プログラムであらかじめ設定された条件を使用して、システムソフトウェアおよびファームウェアをそれらのシステム上でアップデートすることができます。バージョン管理は、古くなったシステムソフトウェアを実行しているシステムを識別し、利用可能なアップグレードがある場合はそれを示し、アップグレードの理由を示します。HP-UX システムでは、1 つ以上のインストールされた HP-UX システムに対して HP Systems Insight Manager CMS から Software Distributor を起動することができます。
HP-UX System Administration Manager (SAM)	HP-UX 11i v1 (B.11.11) および 11i v2 (B.11.23) システム管理の主インタフェース。
SAM	参照 HP-UX System Administration Manager
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。
WBEM	参照 Web-Based Enterprise Management
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。
parMgr	参照 Partition Manager
Disks & File Systems (fsweb)	HP-UX システム管理タスクに GUI を提供します。fsweb は HP ワークステーションやサーバで稼動する HP-UX 11iv2 (B.11.23) オペレーティングシステム上で実行可能です。Linux と Windows オペレーティングシステムではサポートされません。この製品のバンドルタグは FileSystems です。
fsweb	参照 Disks & File Systems
Kernel Configuration (kcweb)	カーネル構成を管理する GUI を提供します。この GUI を使用して、カーネル調整パラメータの監視と変更、カーネルモジュールの監視と変更、アラームの追加、変更、削除を実行できます。
kcweb	参照 Kernel Configuration
Peripheral Devices (pdweb)	周辺機器を管理する GUI を提供します。
pdweb	参照 Peripheral Devices
Users & Groups (ugweb)	ユーザーとグループを管理する GUI を提供します。
ugweb	参照 Users & Groups

索引

C

copyright notice, 45

H

HP SMH

- anonymous アクセス, 23
- IP 制限ログイン, 20
- IP バインディング, 19
- クレジット, 18
- 使用開始, 6
- 製品概要, 4
- セキュリティ, 18
- 設定, 16
- タスク, 30
- ツール, 31
- トラブルシューティング, 34
- ナビゲート, 11
- ページ, 12
- ホーム, 13
- メニュー, 17
- ユーザーグループ, 27
- ローカルアクセス, 23
- ローカルサーバ証明書, 21
- ログ, 32
- ログアウト, 10
- ログイン, 6

S

SAM

- ログ, 33

U

U.S. government license, 45

く

- クレジット
- HP SMH, 18

こ

ご注意, 45

さ

参照

- トラブルシューティング, 43

し

出版履歴, 45
使用開始

ログアウト, 10

ログイン, 6

証明書

- 高信頼性モード, 24

- 証明書の自動インポート, 9

- 信頼済み管理サーバ証明書, 26

せ

製品概要

- HP SMH, 4

- 使用開始, 6

セキュリティ

- anonymous, 23

- HP SMH, 18

- IP 制限ログイン, 20

- IP バインディング, 19

- 高信頼性モード, 24

- 証明書の自動インポート, 9

- 信頼済み管理サーバ証明書, 26

- ユーザーグループ, 27

- ローカルアクセス, 23

- ローカルサーバ証明書, 21

設定

- HP SMH, 16

た

タスク

- HP SMH, 30

つ

ツール

- HP SMH, 31

と

登録商標に関する注意, 45

トラブルシューティング

- HP SMH, 34

- 参照, 43

な

ナビゲート

- HP SMH, 11

へ

ページ

- HP SMH, 12

ほ

ホーム

- HP SMH, 13

保証, 45

め

メニュー

HP SMH , 17

り

リリース履歴, 45

ろ

ログ

HP SMH , 32

HP SMH レガシーログ, 33

System Management Homepage ログ, 32

SAM ログ, 33