HP SiteScope

ソフトウェア・バージョン : 11.30

デプロイメント・ガイド

ドキュメント・リリース日 : 2015 年 5 月
ソフトウェア・リリース日 : 2015 年 3 月

ご注意

保証

HP 製品，またはサービスの保証は，当該製品，およびサービスに付随する明示的な保証文によってのみ規定されるものとします。ここでの記載で追加保証を意図するものは一切ありません。ここに含まれる技術的，編集上の誤り，または欠如について，HP はいかなる責任も負いません。

ここに記載する情報は，予告なしに変更されることがあります。

権利の制限

機密性のあるコンピュータ・ソフトウェアです。これらを所有，使用，または複製するには，HP からの有効な使用許諾が必要です。商用コンピュータ・ソフトウェア，コンピュータ・ソフトウェアに関する文書類，および商用アイテムの技術データは，FAR 12.211 および 12.212 の規定に従い，ベンダの標準商用ライセンスに基づいて米国政府に使用許諾が付与されます。

著作権について

商標について

Adobe ® および Acrobat ® は，Adobe Systems Incorporated の商標です。

Intel ®，Pentium ®，および Intel ® Xeon ® は，米国およびその他の国における Intel Corporation の商標です。

iPod は Apple Computer, Inc. の商標です。

Java は，Oracle Corporation およびその関連会社の登録商標です。

Microsoft ®，Windows ®，Windows NT ®，および Windows ® XP は，Microsoft Corporation の米国登録商標です。

Oracle は，Oracle Corporation およびその関連会社の登録商標です。

UNIX ® は The Open Group の登録商標です。

ドキュメントの更新情報

このマニュアルの表紙には，以下の識別番号が記載されています。

- ソフトウェアのバージョン番号は，ソフトウェアのバージョンを示します。
- ドキュメント・リリース日は，ドキュメントが更新されるたびに変更されます。
- ソフトウェア・リリース日は，このバージョンのソフトウェアのリリース日を示します。

最新の更新情報をチェックする，またはご使用のドキュメントが最新版かどうかを確認するには，次のサイトをご利用ください。**https://softwaresupport.hp.com**

このサイトを利用するには，HP Passport への登録とサインインが必要です。HP Passport ID の取得登録は，次の Web サイトから行うことができます。**https://hpp12.passport.hp.com/hppcf/createuser.do**

または，HP ソフトウェア・サポート・ページの［**登録**］リンクをクリックします。

適切な製品サポート・サービスをお申し込みいただいたお客様は，更新版または最新版をご入手いただけます。詳細は，HP の営業担当にお問い合わせください。

サポート

次の HP ソフトウェア・サポート・オンライン Web サイトを参照してください。
https://softwaresupport.hp.com

HP ソフトウェアが提供する製品，サービス，サポートに関する詳細情報をご覧いただけます。

HP ソフトウェア・オンラインではセルフソルブ機能を提供しています。お客様の業務の管理に必要な対話型の技術支援ツールに素早く効率的にアクセスいただけます。HP ソフトウェア・サポート Web サイトのサポート範囲は次のとおりです。

- 関心のある技術情報の検索
- サポート・ケースとエンハンスメント要求の登録とトラッキング
- ソフトウェア・パッチのダウンロード
- サポート契約の管理
- HP サポート窓口の検索
- 利用可能なサービスに関する情報の閲覧
- 他のソフトウェア・カスタマとの意見交換
- ソフトウェア・トレーニングの検索と登録

一部を除き，サポートのご利用には，HP Passport ユーザとしてご登録の上，サインインしていただく必要があります。また，多くのサポートのご利用には，サポート契約が必要です。HP Passport ID を登録するには，以下の Web サイトにアクセスしてください。

https://hpp12.passport.hp.com/hppcf/createuser.do

アクセス・レベルの詳細情報については，次の URL を参照してください。

https://softwaresupport.hp.com/web/softwaresupport/access-levels

HP Software Solutions Now（英語）は HPSW のソリューションと統合に関するポータル Web サイトです。このサイトでは，お客様のビジネスニーズを満たす HP 製品ソリューションを検索したり，HP 製品間の統合に関する詳細なリストや ITIL プロセスのリストを閲覧することができます。このサイトの URL は **http://h20230.www2.hp.com/sc/solutions/index.jsp** です。

目次

保証 2
権利の制限 2
著作権について 2
商標について 2

第1部: SiteScope の紹介 10
第1章: SiteScope の概要 11
第2章: SiteScope エディション 12
SiteScope エディションの概要 12
機能比較表 13
コミュニティ・エディションに含まれていないモニタ 15
コミュニティ・エディション 16
トライアル・エディション 18
Commercial エディション 19
Premium/Ultimate・エディション 20
System Collector エディション 22
Load Testing エディション 24
Failover エディション 26
第3章: SiteScope ライセンス 27
SiteScope ライセンスの概要 27
インスタントオン・ライセンス 28
ライセンス・エディション 29
ライセンス容量タイプ 30
ライセンスのインポートおよびアップグレード 31
SiteScope エディション・ライセンスのアップグレード 32
SiteScope for Load Testing インストール環境のライセンスの Premium エディションへのアップグレード 33
ライセンス容量の増加 33
SiteScope ライセンスのインポート 34
ライセンス有効期限 35
コミュニティ・ライセンスへのダウングレード 35
ライセンスの注意事項および制限事項 36
第4章: スタートアップ・ロードマップ 38
第5章: デプロイメントの方法と計画 39
エンタープライズ・システム監視の方法 39
ビジネス・システム・インフラストラクチャの評価 41
SiteScope サーバのサイズ設定 42

ネットワークの場所と環境 42
Windows 環境の場合に考慮する事項 43
Linux 環境の場合に考慮する事項 43
第6章: SiteScope のサイズ設定 45
SiteScope のサイズ設定の概要 45
SiteScope キャパシティ・カリキュレータ 45
サポートされているモニタとソリューション・テンプレート 47
Windows プラットフォーム上での SiteScope のサイズ設定 48
SiteScope のサイズ設定 48
Microsoft Windows オペレーティング・システムのチューニング 49
一般的な保守の推奨事項 49
Linux プラットフォーム上での SiteScope のサイズ設定 50
オペレーティング・システムのチューニング 51
Java 仮想マシンのチューニング 52
一般的な保守の推奨事項 53
トラブルシューティングおよび制限事項 54
第7章: エージェントレス監視について 55
SiteScope 監視機能の概要 55
エージェントレス監視環境について 56
SiteScope の監視の方法 56
ファイアウォールと SiteScope のデプロイメント 58
モニタの権限と資格情報 59
第2部: SiteScope をインストールする前に 60
第8章: インストールの概要 61
第9章: インストール要件 62
システム要件 62
システムのハードウェア要件 62
認定されている構成 63
Windows の場合のサーバ・システム要件 64
Linux のサーバ・システム要件 64
クライアントのシステム要件 65
SiteScope の容量に関する制限事項 67
SiteScope サポート・マトリックス 67
HP Business Service Management 統合サポート・マトリックス 67
HP Operations Manager（HPOM）統合サポート・マトリックス 68
HP Operations Agent サポート・マトリックス 69
負荷テストのための HP SiteScope のサポート・マトリックス 69
HP Network Node Manager i（NNMi）サポート・マトリックス 70
第10章: SiteScope のアップグレード 71
アップグレードを実行する前に 71
32 ビットから 64 ビットの SiteScope への移行 73

既存の SiteScope インストールのアップグレード 74
SiteScope 構成データのバックアップ 76
設定データのインポート 76
SiteScope 10.x から SiteScope 11.13 または 11.24 へのアップグレード 76
SiteScope 11.13 または 11.24 から SiteScope 11.30 へのアップグレード 78
トラブルシューティングおよび制限事項 81

第3部: SiteScope のインストール 84
第11章: インストール・ワークフロー 85
インストール・バージョンのタイプ 85
インストールの流れ 86
Linux インストールの準備 90
Oracle Enterprise Linux 環境への SiteScope のインストール 90
CentOS 6.2 環境への SiteScope のインストール 91
CentOS 6.2 で実行する HP Cloud Services インスタンスへの SiteScope のインストール 92
トラブルシューティングおよび制限事項 93
第12章: インストール・ウィザードを使用してインストール 95
X11 サーバがインストールされていないマシンへのインストール・ウィザードを使用した SiteScope のインストール 113
第13章: コンソール・モードを使用した Linux へのインストール 114
第14章: サイレント・モードでの SiteScope のインストール 122
サイレント・モードでの SiteScope のインストールについて 122
サイレント・インストールの実行 123
第15章: SiteScope 設定ツールの使用 124
Windows プラットフォームでの設定ツールの実行 124
Linux プラットフォームでの設定ツールの実行 131
コンソール・モードでの設定ツールの実行 135
サイレント・モードでの設定ツールの実行 141
サイレント設定の実行 142
第16章: SiteScope のアンインストール 144
Windows プラットフォームからの SiteScope のアンインストール 144
SiteScope とその上にインストールされた任意のマイナー・マイナー・バージョンのアンインストール方法 144
Linux プラットフォームからの SiteScope のアンインストール 145
SiteScope とその上にインストールされた任意のマイナー・マイナー・バージョンのアンインストール方法 145

第4部: SiteScope の安全な稼働 148
第17章: SiteScope プラットフォームのセキュリティ強化 149
概要 149
SiteScope ユーザ設定の設定 149
パスワードの暗号化 150

TLS（Transport Layer Security）を使用した SiteScope へのアクセス 150
スマート・カード認証 150
共通基準認定 151
FIPS 140-2 コンプライアンシー 152
カスタム・キーを使用したデータの暗号化 152
ユーザ・アカウントのセキュリティを保護するための推奨事項 152
ログイン時に表示される警告バナーの設定 155
第18章: セキュアな接続を経由して通信するための SiteScope の設定 156
セキュアな接続を必要とするようにするための SiteScope の設定 156
スマート・カード認証の設定 156
クライアント証明書認証を必要とするよう SiteScope を設定 157
第19章: 高度な強化設定 158
証明書の失効を検証するための SiteScope の設定 158
クライアント証明書が有効な場合の Firefox の使用 158
認証局証明書の SiteScope トラストストアへのインポート 159
JMX リモート・アクセスの無効化 159
バックアップした設定の復元 159
SiteScope でのフレーミング・フィルタの設定 160
第20章: SiteScope が FIPS 140-2 対応モードで機能するための設定 162
FIPS 140-2 コンプライアンシーの概要 162
FIPS 140-2 対応モードの有効化 163
FIPS 140-2 対応モードの無効化 168
トラブルシューティングおよび制限事項 168
第21章: データ暗号化にカスタム・キーを使用するための SiteScope の設定 170
キー管理の概要 170
データ暗号化のカスタム・キーを使用するように SiteScope を設定する方法 171
暗号化キーを変更した後に FIPS 対応モードを有効化または無効化する方法 172
データ暗号化のカスタム・キーを使用して設定データをエクスポートおよびインポートする方法 172
第22章: セキュア接続で BSM と通信するための SiteScope の設定 174
セキュア接続が必要な BSM サーバに SiteScope を接続する設定 174
クライアント証明書が必要な BSM サーバに SiteScope を接続する設定 174
SiteScope でクライアント証明書が必要な場合に SiteScope に接続するための BSM の設定 174
第23章: 強化ツールの使用 176
強化ツールの実行方法 176
セキュアな接続を要求するように SiteScope を構成するための強化ツールのを使用方法 178
証明書の失効を確認するように SiteScope を設定するための強化ツールの使用方法 179
認証局の証明書を SiteScope トラストストアにインポートするための強化ツールの使用方法 181
クライアント証明書が必要な BSM サーバに SiteScope を接続するように設定するための強化ツールの使用方法 182

FIPS 140-2 対応モードを有効化するための強化ツールの使用方法 184
データ暗号化のためにキー管理を有効にするための強化ツールの使用方法 184
SiteScope と SiteScope パブリック API クライアント証明書認証を設定するための強化ツールの使用方法 184
JMX リモート・アクセスを設定するための強化ツールの使用方法 185
バックアップ済みの設定を復元するための強化ツールの使用方法 185
強化ツールの制限事項とトラブルシューティング 186
第24章: USGCB（FDCC）準拠デスクトップの設定 189

第5部: 作業の開始と SiteScope へのアクセス 191
第25章: インストール後の管理 192
第26章: Microsoft ホットフィックスのインストール 195
第27章: SiteScope を使った作業の開始 197
SiteScope サービスの開始の概要 197
Windows プラットフォームでの SiteScope サービスの開始と停止 197
Linux プラットフォームでの SiteScope プロセスの開始と停止 198
SiteScope への接続 199
SiteScope クラシック・インタフェース 200
トラブルシューティングおよび制限事項 200

付録 205
付録A: SiteScope のTomcat サーバとの IIS の統合 206
Apache Tomcat サーバ・ファイルの設定 206
トラブルシューティング 208
IIS の設定 209
付録B: SiteScope と SiteMinder との統合 213
SiteMinder との統合について 213
統合の要件 214
統合のプロセス 214
SiteMinder ポリシー・サーバの設定 215
SiteMinder を使用するための SiteScope の設定 216
IIS の設定 216
さまざまな SiteScope ロールの権限の定義 217
SiteScope へのログオン 217
注意事項とガイドライン 217
付録C: セキュア接続を使用するための SiteScope の手動による設定 219
TLS の使用に向けた SiteScope の準備 219
認証局からの証明書の使用 220
自己署名証明書の使用 222
Tomcat 上の TLS 用の SiteScope の設定 223
相互 TLS 構成用の SiteScope の設定 225
SiteScope を TLS デプロイメントの BSM サーバに接続するための設定 226

クライアント証明書が必要な BSM サーバに SiteScope を接続する設定 226
BSM サーバがクライアント証明書を必要とするときの SiteScope でのトポロジ・ディスカバリ・エージェントの設定方法 229
トラブルシューティング 232
付録D: HTTPS を使用した SiteScope レポートおよびクラシック・ユーザ・インタフェースへのアクセス 233
SiteScope の証明書を使った作業について 233
認証局からの証明書の使用 233
自己署名証明書の使用 235
ドキュメントに関するフィードバックの送信 238

第1部: SiteScope の紹介

第1章: SiteScope の概要

HP SiteScope は，サーバ，オペレーティング・システム，ネットワーク・デバイス，ネットワーク・サービス，アプリケーション，アプリケーション・コンポーネントなどから構成される，分散 IT インフラストラクチャの可用性とパフォーマンスの確保を目的とする，エージェントレス監視ソリューションです。

SiteScope は Web ベースでインフラストラクチャを監視し，軽量で柔軟にカスタマイズでき，実運用システムにデータ収集エージェントをインストールする必要がありません。SiteScope は，インフラストラクチャの動作を確認するために必要な情報をリアルタイムで提供します。ユーザは常に問題の通知を受け，それらが重大なものになる前にボトルネックを解決できます。

SiteScope には，テンプレート，テンプレート変更適用ウィザード，自動テンプレート・デプロイメントなどのさまざまなツールが用意されており，これにより，一連の標準化されたモニタ・タイプと設定を使用して単一の構造を展開できます。SiteScope テンプレートは組織全体に迅速に配備でき，素早く更新できるため，監視インフラストラクチャがテンプレートの標準セットに準拠した状態を確実に維持できます。

SiteScope にはまた，さまざまなメディアでイベント情報の伝達と記録に使用できる警告タイプも用意されています。警告テンプレートは，組織のニーズに合わせてカスタマイズできます。

SiteScope は，Business Service Management（BSM），Network Node Manager i（NNMi），HP Software-as-a-Service，LoadRunner/Performance Center など，ほかの HP 製品の監視基盤としても機能します。SiteScope を配備し，BSM のサービス・レベル管理などのその他の HP ソリューションを追加することで，堅牢なインフラストラクチャ監視システムを作成し，ビジネスの視点から IT インフラストラクチャやサービス・レベルを管理できます。

SiteScope は HP Operations Manager（HPOM）製品と連携できるため，エージェントレスとエージェント・ベースのインフラストラクチャ管理を組み合わせて強力な機能を実現できます。HPOM のエージェントとして使用すると，SiteScope ターゲットは Operations Manager Service ビュー・マップに自動的に追加されます。これにより，HPOM は SiteScope のデータとモニタの状態をシームレスに表示できます。イベント統合では，SiteScope 警告およびモニタ・メトリクスの状態が HPOM に直接送信されます。エージェントレスおよびエージェント・ベースの監視の機能を組み合わせることで，強力で徹底した監視ソリューションを使用できます。HPOM 製品の使用方法の詳細については，HPOM のドキュメントを参照してください。

第2章: SiteScope エディション

本章の内容

- 「SiteScope エディションの概要」(12ページ)
- 「機能比較表」(13ページ)
- 「コミュニティ・エディション」(16ページ)
- 「トライアル・エディション」(18ページ)
- 「Commercial エディション」(19ページ)
- 「Load Testing エディション」(24ページ)
- 「Failover エディション」(26ページ)

SiteScope エディションの概要

SiteScope では，異なる機能を提供するさまざまなエディションを用意しています。

SiteScope は組み込みの **Community** エディション・ライセンスでインストールされます。このエディションでは，SiteScope の一部の機能を期間制限なしで無料で使用できます。また，無償の 1 回限りの **Trial** エディションもあります。このエディションでは，SiteScope のすべての機能を 30 日間試用できます。

Community エディションに含まれている機能を拡張するには，**Premium**，**Ultimate**，または **System Collector** のいずれかのエディションにアップグレードします。また，無償の **Load Testing** エディションもあります。このエディションは，HP SiteScope for Load Testing をインストールするとすぐに使用可能になります。Community，Premium，Ultimate の各エディションはすべてのユーザが利用できますが，System Collector と Load Testing エディションはそれぞれ，HP Operations Manager 統合と HP Load Runner/Performance Center によって提供されます。

追加のライセンスをインポートすることによって，SiteScope の機能と容量を追加できます。これにより，組織のニーズおよびインフラストラクチャの要件に合わせて SiteScope の規模を効率的かつ柔軟に変更できます。ライセンスの購入またはライセンス容量の追加の詳細については，HP の営業担当にお問い合わせいただくか，HP SiteScope 製品ページの「お問い合わせ」リンクをクリックしてください。

ライセンスの詳細については，「SiteScope ライセンス」(27ページ)を参照してください。

機能比較表

下記の表は，さまざまな SiteScope エディションで使用可能な機能を示します。

機能	SiteScope エディション			HP 製品のみで使用可能	
	コミュニティ	試用版	プレミアム/アルティメット	システム・コレクタ	Load Testing
ライセンス期間	Instant-on（永久）	30 日	定期 または永久	定期または永久	Instant-on（永久）
ライセンス付与モデル	25 個の OSI 25 個の URL （固定容量）	25 個の OSI 25 個の URL 10 トランザクション （固定容量）	OSI，URL，トランザクション （ユーザ決定の数量）	OSI （ユーザ決定の数量）	25 個の OSI 25 個の URL （固定容量）
ノード・ロック[1]	x	x	✔	✔	x
サポート・モデル	SiteScope コミュニティ	Web/電話	Web/電話	Web/電話	電子メール
ユーザ・アカウント	1	無制限	無制限	無制限	無制限
データ保存期間	30 日間 [2]	30 日間 [2]	無制限	無制限	無制限
警告	電子メール，イベントコンソールのみ	✔	✔	✔	✔
レポート作成	クイック・レポートのみ	✔	✔	✔	✔
Multi-View，イベント・コンソール	✔	✔	✔	✔	✔
解析	✔	✔	✔	✔	✔
モニタ・タイプ	「コミュニティ・エディションに含まれていないモニタ」(15ページ)に示されている	すべてのモニタ	すべてのモニタ	すべてのモニタ	Web スクリプトおよび統合モニタを除くすべてのモニタ

機能	SiteScope エディション			HP 製品のみで使用可能	
	コミュニティ	試用版	プレミアム/アルティメット	システム・コレクタ	Load Testing
	もの以外のすべてのモニタ。				
ソリューション・テンプレート	x	すべてのソリューション・テンプレート	すべてのソリューション・テンプレート	すべてのソリューション・テンプレート	HP Quality Center，HP QuickTest Professional，HP Service Manager，HP Vertica，Operating System Host（AIX，Linux，Microsoft Windows，Solaris）
ユーザ定義テンプレート	✔ CSV または XML ファイルを経由したデプロイを除く	✔	✔	✔	✔
API	x	✔	✔	✔	✔
統合	x	✔	✔	✔	汎用データ統合
高可用性（フェイルオーバー）	x	x	✔	✔	x
更新とパッチ	x	x （パッチ経由で更新可能）	✔	✔	✔
サポートされるプラットフォーム（インストール）	さまざまな Windows および Linux 64 ビット・プラットフォーム（サポートされるバージョンのリストについては「システム要件」(62ページ)を参照してください）。				
多言語 UI のサポート	10 言語（『SiteScope の使用ガイド』多言語環境のセクションのサポートされる言語のリストを参照してください）。				

[1] 一部のライセンス・エディションはライセンスの悪用を避けるためノード・ロックされています。ノード・ロックとは，ライセンスが特定のマシンのみで有効になることです。

[2] ログ・プリファレンスで日次ログの数を設定しても，保持される日次ログの数には影響しません。

コミュニティ・エディションに含まれていないモニタ

- Active Directory レプリケーション・モニタ
- Amazon Web Services モニタ
- COM+ サーバ・モニタ
- HP Vertica JDBC モニタ
- 統合モニタ
- Microsoft Exchange モニタ - Microsoft Exchange 2007 メッセージ・トラフィック，Microsoft Exchange。 Microsoft Exchange ベース（廃止されたモニタ :Microsoft Exchange 5.5/2000/2003 のメッセージ・トラフィック，Microsoft Exchange 2003 メールボックス，Microsoft Exchange 2003 パブリック・フォルダ）
- Microsoft Lync モニタ - アーカイブ・サーバ，音声ビデオ会議サーバ， Director サーバ，エッジ・サーバ，フロント・エンド・サーバ，仲介サーバ，監視および CDR サーバ，Registrar サーバ
- Oracle データベース ソリューション・テンプレート - Oracle 10g アプリケーション・サーバ，Oracle 9i アプリケーション・サーバ，Oracle データベース・モニタ
- SAP モニタ - SAP CCMS，SAP CCMS 警告，SAP Java Web アプリケーション・サーバ，SAP パフォーマンス， SAP ワーク・プロセス
- Siebel モニタ - Siebel アプリケーション・サーバ，Siebel ログ，Siebel Web サーバ
- VMware データストア・モニタ
- VMware ホスト・モニタ - VMware ホスト CPU， VMware ホスト・メモリ，VMware ホスト・ネットワーク， VMware ホスト状態，VMware ホスト・ストレージ
- WebLogic アプリケーション・サーバ・モニタ
- Web スクリプト・モニタ
- WebSphere モニタ - WebSphere アプリケーション・サーバ，WebSphare MQ 状態，WebSphere パフォーマンス・サーブレット・モニタ

コミュニティ・エディション

コミュニティ・エディションは無料で期間に制限なく SiteScope の限定的な機能を提供します。このエディションは通常の SiteScope インストールの実行後に自動的にアクティブ化されます。

注: コミュニティ・エディションは SiteScope のマイナー・バージョンまたはマイナーマイナー・バージョンの各リリースではリリースされません。バージョン・タイプの詳細については，「インストール・バージョンのタイプ」(85ページ)を参照してください。

下記の表で，コミュニティ・エディションと SiteScope の商用エディションとの主な相違点の一部を示します。

機能	説明
ライセンス期間	**コミュニティ・エディション:** このエディションには有効期限はありません。ライセンス・ファイルをインポートすることによって他のエディションで上書き可能です。他に商用エディションが存在しない、または有効でないときは再びアクティブ化されます。 **商用エディション:** 定期または永久。商用エディションのライセンスの期限が切れたときに何が起こるかの詳細については，「ライセンス有効期限」(35ページ) を参照してください。
容量	**コミュニティ・エディション:** このエディションには，最大 25 個の OS インスタンスと 25 個の URL を監視できる容量が備わっていますが，その容量は固定されていて拡張できません。モニタの実行中にこの容量を超過すると，すべてのモニタが一時停止となり，エラーがログに表示されます。たとえば，ダイナミック VMware モニタの OSi 容量消費は，検出された VM の数に応じてモニタの実行中に変化する場合があります。 **商用エディション:** ユーザは必要な監視の要件に応じて OS インスタンス，URL，およびトランザクション・ライセンス容量を購入できます。
ユーザ管理	**コミュニティ・エディション:** 1 ユーザ・アカウント（管理者）。 **商用エディション:** 無制限のユーザおよびユーザ・ロール，認証と承認のための LDAP 統合に対するサポート。
ソリューション・テンプレート・モニタ	**コミュニティ・エディション:** • ソリューション・テンプレートとそれらの依存するモニタは使用できません。 • 「コミュニティ・エディションに含まれていないモニタ」(15ページ) に示されているモニタは使用できません。 • 他のモニタはすべて使用可能です。 **商用エディション:** すべてのモニタおよびソリューション・テンプレートが使用可能です。

機能	説明
データ保存期間	**コミュニティ・エディション :** • モニタ・データの履歴が 30 日間のみ保持されます（ただし，ログ・ファイルは削除されません）。ログ・プリファレンスで日次ログの数を設定しても，保持される日次ログの数には影響しません。 • クイック・レポートは過去 30 日間のデータを表示します。 **商用エディション** 無制限
警告アクション	**コミュニティ・エディション :** 電子メールとイベント・コンソールの警告アクションのみが有効になります。 **商用エディション :** すべての警告アクションが有効になります。
API	**コミュニティ・エディション :** サポートされていません。 **商用エディション :** サポート
統合	**コミュニティ・エディション :** サポートされていません。 **商用エディション :** サポート
高可用性（フェイルオーバー）	**コミュニティ・エディション :** サポートされていません。コミュニティ・エディションを使用して SiteScope フェイルオーバー・マシンを SiteScope に接続しようとすると，例外がプライマリ SiteScope からフェイルオーバー SiteScope に返されてユーザ・インタフェースに表示されます。対応するメッセージもプライマリ SiteScope の error.log に書き込まれます。 **商用エディション :** サポート
テンプレート・デプロイメント	**コミュニティ・エディション :** CSV テンプレート・デプロイメント（ユーザ・インタフェース経由）および自動テンプレート・デプロイメントはサポートされていません。 **商用エディション :** すべてサポート
アップグレード	コミュニティ・エディションをプレミアム，アルティメット，またはシステム・コレクタ・エディションにアップグレードできます。詳細については，「ライセンスのインポートおよびアップグレード」(31ページ)を参照してください。

トライアル・エディション

SiteScope Trial エディションを使用する場合の仕様を次に示します。

機能	説明
エディション・タイプ	無償で 1 回限り使用できる試用版。
エディション期間	30 日
容量	Community エディションからアクティブ化した場合，試用版には最大 25 個の OS インスタンス，25 個の URL，10 個のトランザクションを監視できる容量が含まれます。 **注 :** 試用版の容量は固定されており，拡張や更新はできません。
機能	SiteScope の全機能。詳細については，「機能比較表」(13ページ)を参照してください。
ノード・ロック	No
アクティベーション	Community エディションを使用しているときに，［**プリファレンス**］ > ［**一般プリファレンス**］ > ［**ライセンス**］ > ［**Trial エディション**］を選択すると使用可能になります。これは 1 回のみ起動できます。その後，このボタンは常時使用不可になります。
非アクティブ化	［**プリファレンス**］ > ［**一般プリファレンス**］ > ［**ライセンス**］を選択します。［インストールされているライセンス］テーブルで［**Trial**］行を選択し，［**ライセンスの削除**］をクリックします。 これにより，SiteScope は以前のエディション（ほかのエディションを購入していなかった場合は Community エディション）に戻ります。
アップグレード	Trial エディションは，Premium，Ultimate，または System Collector の各エディションで上書きできます。詳細については，「ライセンスのインポートおよびアップグレード」(31ページ)を参照してください。
有効期	ライセンスは 30 日後に自動的に期限が切れ，SiteScope は Community エディションに

機能	説明
限	戻ります。機能は，現在アクティブなライセンス・エディションの機能に従って削減されます。

Commercial エディション

SiteScope には次の商用エディションがあります。次の表は，これらのエディションを使用するための仕様を示します。

各エディションで使用可能な機能のリストは，「機能比較表」(13ページ)を参照してください。

- 「Premium/Ultimate・エディション」(20ページ)
- 「System Collector エディション」(22ページ)

Premium/Ultimate・エディション

機能	説明
エディション・タイプ	商用エディション。
エディション期間	定期または永久
容量	必要な OSi，URL，およびトランザクション容量を購入します（最小容量は設定されていません）。 ライセンス購入の照会（または追加の容量が必要な場合）については，HP の営業担当にお問い合わせいただくか，HP SiteScope 製品ページの「お問い合わせ」リンクを使用してください。
機能	完全な SiteScope 機能
ノード・ロック	はい（ライセンスが特定のマシンのみで有効です）。
アクティベーション	ライセンスを購入した後，[**プリファレンス**] > [**一般プリファレンス**] > [**ライセンス**] と選択し，[**ライセンス ファイル**] ボックスに SiteScope ライセンス・ファイルへのパスを入力するか，[**選択**] ボタンをクリックして，ライセンス・ファイルを選択します。
非アクティブ化	[**プリファレンス**] > [**一般プリファレンス**] > [**ライセンス**] を選択します。[インストールされているライセンス] テーブルで，[**Premium/Ultimate**] 行を選択し，[**ライセンスの削除**] を選択します。Premium または Ultimate エディションのライセンスを削除するときは，Premium または Ultimate エディションの容量タイプ行もすべて削除する必要があります（[OSi]，[URL]，および [トランザクション]）。 ほかのエディションを購入していない場合は，これにより，SiteScope は前のエディションか Community エディションに戻ります。
アップグレード	Premium エディションは，Ultimate または System Collector エディションで上書きできます。詳細については，「ライセンスのインポートおよびアップグレード」(31ページ)を参照してください。

機能	説明
有効期限	ライセンスは，アクティブなエディションですべての容量タイプに対する期間が終了すると期限切れになります。SiteScope はライセンスが期限切れになる 7 日前にユーザに通知メッセージを送信し，［ライセンス］パネルにこの情報を表示します。 期限が切れると,SiteScope は自動的にそのエディション（および機能）を階層内の前の商用エディション（存在する場合）にダウングレードします。それ以外の場合は，Community エディションがアクティブなエディションになります。
容量のダウングレード	OSi，URL，またはトランザクションの容量を超過すると，SiteScope は次を行います。 1. ダイアログ・ボックスが開いて，警告メッセージが表示されます。 2. 余分なモニタを削除するか，ライセンス容量を増やすようにユーザに警告する日次メッセージを送信します（最大 7 日間）。容量が超過した期間が 7 日間を超えると，SiteScope はすべてのモニタを一時停止します。

System Collector エディション

機能	説明
エディション・タイプ	HP Operations Manager 統合で提供される SiteScope のバージョンの一つ。
エディション期間	定期または永久
容量	必要な OSi 容量を購入してください（最低限必要な容量は設定されていません）。 ライセンス購入の照会（または追加の容量が必要な場合）については，HP の営業担当にお問い合わせいただくか，HP SiteScope 製品ページの「お問い合わせ」リンクを使用してください。
機能	SiteScope の全機能。
ノード・ロック	はい（ライセンスが特定のマシンのみで有効です）。
アクティベーション	ライセンスを購入した後，[**プリファレンス**] > [**一般プリファレンス**] > [**ライセンス**] と選択し，[**ライセンス ファイル**] ボックスに SiteScope ライセンス・ファイルへのパスを入力するか，[**選択**] ボタンをクリックして，ライセンス・ファイルを選択します。
非アクティブ化	[**プリファレンス**] > [**一般プリファレンス**] > [**ライセンス**] を選択します。[インストールされているライセンス] テーブルで [**System Collector**] 行を選択し，[**ライセンスの削除**] をクリックします。System Collector エディションのライセンスを削除するときは，System Collector エディションの容量タイプの行（[OSi]，[URL]，[トランザクション]）もすべて削除する必要があります。 ほかのエディションを購入していない場合は，これにより，SiteScope は前のエディションか Community エディションに戻ります。
アップグレード	System Collector のライセンスは上書きできませんが，Premium または Ultimate エディションのライセンスをインポートすれば，URL とトランザクションの容量を増やすことができます。詳細については，「ライセンスのインポートおよびアップグレード」(31ページ)を参照してください。

機能	説明
有効期限	アクティブなエディションの OS インスタンス容量の期間が終了すると，ライセンスの期限が切れます。SiteScope はライセンスが期限切れになる 7 日前にユーザに通知メッセージを送信し，［ライセンス］パネルにこの情報を表示します。 期限が切れると,SiteScope は自動的にそのエディション（および機能）を階層内の前の商用エディション（存在する場合）にダウングレードします。それ以外の場合は，Community エディションがアクティブなエディションになります。
容量のダウングレード	OSi，URL，またはトランザクションの容量を超過すると，SiteScope は次を行います。 1. ダイアログ・ボックスが開いて，警告メッセージが表示されます。 2. 余分なモニタを削除するか，ライセンス容量を増やすようにユーザに警告する日次メッセージを送信します（最大 7 日間）。容量が超過した期間が 7 日間を超えると，SiteScope はすべてのモニタを一時停止します。

Load Testing エディション

HP LoadRunner または HP Performance Center で SiteScope Load Testing エディションを使用するための仕様を以下に示します。

機能	説明
エディション・タイプ	HP LoadRunner および HP Performance Center に付属して提供される，無料で使用可能な SiteScope のバージョン
エディション期間	永久
容量	25 個の OS インスタンス，25 個の URL **注：** このライセンスは，拡張できない固定された容量で提供されます。
機能	「機能比較表」(13ページ) を参照してください。
ノード・ロック	No
アクティベーション	SiteScope for Load Testing をインストールした後，自動的にアクティブ化されます。
非アクティブ化	ユーザはエディション・ライセンスを削除できません。
アップグレード	Load Testing エディションをプレミアム，アルティメット，またはシステム・コレクタ・エディションにアップグレードできます。詳細については，「ライセンスのインポートおよびアップグレード」(31ページ)を参照してください。 **注 :**Load Testing エディションのアップグレードには，「SiteScope for Load Testing インストール環境のライセンスの Premium エディションへのアップグレード」(33ページ)で説明されている追加の設定が必要です。
有効期限	なし（ライセンスは永久です）
容量のダウングレード	ライセンス容量を超過すると，SiteScope は次の動作を行います。 1. ダイアログ・ボックスが開いて，警告メッセージが表示されます。 2. ユーザにライセンス容量を超過していると警告するメッセージを毎日（7 日間ま

機能	説明
	で）送信します。容量が超過した期間が 7 日間を超えると，SiteScope はすべてのモニタを一時停止します。

Failover エディション

SiteScope Failover エディションを使用する場合の仕様を次に示します。

機能	説明
エディション・タイプ	SiteScope Failover は，冗長性を高め，SiteScope サーバで可用性に関する問題が発生したとき場合に自動的なバックアップ保護を提供します。Failover エディション・ライセンスは，Premium，Ultimate および System Collector エディションに無償で付属しています。
エディション期間	SiteScope Failover は，Premium，Ultimate または System Collector エディション・ライセンスを搭載するプライマリ SiteScope に依存します。
機能	完全な SiteScope 機能
アクティベーション	SiteScope Failover をインストールした後に，Failover ライセンスをインポートする必要があります。 Failover サーバがプライマリ SiteScope サーバ（Premium，Ultimate または System Collector エディション・ライセンスを搭載）が同期の状態になった後にのみ正常に機能し始めます。
非アクティブ化	［**プリファレンス**］>［**一般プリファレンス**］>［**ライセンス**］を選択します。［インストールされているライセンス］テーブルで，［**Failover**］の行を選択し，［**ライセンスの削除**］を選択します。Failover エディション・ライセンスを削除すると，すべての Failover エディションのすべての容量タイプの行（OSi，URL，トランザクション）も削除されます。
期限 / 容量ダウングレード	SiteScope Failover は，Premium，Ultimate または System Collector エディション・ライセンスを搭載するプライマリ SiteScope に依存します。プライマリ SiteScope エディション・ライセンスの期限切れと同時に Failover ライセンスも期限切れになり，SiteScope Failover マシンでアクティブなエディションが存在しなくなります。

第3章: SiteScope ライセンス

本章の内容

- 「SiteScope ライセンスの概要」(27ページ)
- 「ライセンスのインポートおよびアップグレード」(31ページ)
- 「ライセンス有効期限」(35ページ)
- 「SiteScope ライセンスのインポート」(34ページ)
- 「ライセンスの注意事項および制限事項」(36ページ)

SiteScope ライセンスの概要

SiteScope ライセンスでは，同時に作成可能なモニタの数と使用可能なモニタのタイプを管理します。監視を行う環境のニーズに応じて適切なタイプと容量のライセンスを購入してください。作成可能な SiteScope モニタの数は次の 2 つの要因によって決まります。

- 特定のライセンス容量タイプ（OS インスタンス，URL，トランザクション）について購入した監視容量。
- 使用する SiteScope モニタのタイプ。

SiteScope ライセンスを購入して SiteScope を登録することにより，重要な権利および権限が与えられます。登録ユーザは，HP の全製品に関するテクニカル・サポートや情報を利用できるようになり，無償でアップデートとアップグレードを受けられます。

また，HP ソフトウェア・サポート・サイトへのアクセス権も付与されます。このアクセス権を使用して，「セルフ・ソルブ技術情報検索」での技術情報の検索や，SiteScope ドキュメントのアップデートのダウンロードを行うことができます。

モニタ用の新規ライセンス・モデル

SiteScope のライセンス資格モデルは，ポイント・ベース・モデルから，SiteScope が監視するオブジェクトのタイプに基づく容量タイプ モデルに変更されました。監視対象オブジェクトには，オペレーティング・システム・インスタンス（OSi），VuGen スクリプトを実行するモニタのトランザクション，URL の 3 つのタイプがあります。

利用可能なライセンス容量タイプは，インストール・タイプおよび選択した SiteScope のエディションによって異なります。つまり，組織のニーズとインフラストラクチャの要件を満たすように SiteScope デプロイメントの規模を柔軟に調整することができます。

ライセンスの仕組みについての詳細は，次の各項を参照してください。

- 「インスタントオン・ライセンス」(28ページ)
- 「ライセンス・エディション」(29ページ)
- 「ライセンス容量タイプ」(30ページ)

ソリューション・テンプレートの新規ラインセンス・モデル

ソリューション・テンプレートでは，ソリューションごとに個別のライセンスが不要になりました。今後は，すべてのソリューション・テンプレートが，Premium，Ultimate，System Collector の各エディション・ライセンスで自動的に使用可能になります。ソリューション・テンプレートのライセンス消費量は，ソリューション・テンプレートからデプロイされるモニタに応じて計算されます。

インスタントオン・ライセンス

SiteScope を使用するには，有効なライセンスが必要です。ライセンスは，選択したセットアップのタイプに応じて自動的にアクティブ化（インスタントオン）されます

- **HP SiteScope：** *Community* エディション・ライセンスは，通常の SiteScope のインストールが完了次第，即座に使用可能になります。この無償エディションでは，SiteScope の一部の機能を期間制限なしで使用できます。SiteScope エディションをアップグレードすることにより，いつでも初期デプロイメントの監視容量を拡張して，SiteScope が提供するすべての機能を利用できます。使用可能な SiteScope の各エディションの一覧については，「ライセンス・エディション」(29ページ)を参照してください。
- **HP SiteScope for Load Testing：** *Load Testing* エディション・ライセンスは，HP SiteScope for Load Testing のインストールが完了次第，即座に利用可能になります。このセットアップの種類は，HPLoadRunner または HPPerformance Center をインストールする場合のみ使用できます。

注: SiteScope Failover インストールでは，*Failover* エディション・ライセンスが，Premium，Ultimate および System Collector エディションに無償で付属しています。SiteScope Failover をインストールしたら，Failover ライセンス・ファイルをインポートする必要があります。

ライセンス・エディション

モニタする環境のタイプに従ってSiteScope エディションおよび容量モデル（「ライセンス容量タイプ」(30ページ)を参照）を選択することによって，初期の SiteScope デプロイメントをアップグレードできます。

次のエディションから選択できます。

ライセンス・エディション	説明
トライアル・エディション	SiteScope は無料の 1 回限定の試用版ライセンスを提供します。このライセンスでは，すべての SiteScope 機能を 30 日間使用できます。詳細については，「トライアル・エディション」(18ページ)を参照してください。
プレミアム/アルティメット・エディション	統合，SiteScope API，SiteScope フェイルオーバ，およびエンタープライズ・モニタおよびテンプレートを含む，すべての SiteScope 機能を提供します。 プレミアム・エディションとアルティメット・エディションの機能は同じですが，バンドルされる統合のみが異なります。詳細については，HP の営業担当にお問い合わせください。 詳細については，「Premium/Ultimate・エディション」(20ページ)を参照してください。
システム・コレクタ	HPOM アプリケーションで SiteScope モニタを使用できるようにする HP Operations Manager 統合に含まれる SiteScope のバージョン。詳細については，「System Collector エディション」(22ページ)を参照してください。
Load Testing	LoadRunner または Performance Center アプリケーションでユーザが SiteScope モニタを定義および使用できるようにする HP LoadRunner/Performance Center に付属する SiteScope のバージョンです。詳細については，「Load Testing エディション」(24ページ)を参照してください。

各エディションで使用可能な機能の比較については，「機能比較表」(13ページ)を参照してください。

ライセンス購入の照会（または追加の容量が必要な場合）については，HP の営業担当にお問い合わせいただくか，HP SiteScope 製品ページの「お問い合わせ」リンクを使用してください。ライセンスを所有している場合にライセンス・キー・ファイルが必要な場合は，HP Licensing for Software Portal を使用してください。

ライセンス容量タイプ

次の表に，異なる容量タイプ，ライセンスの使用状況を計算するために使用されるルール，および各ライセンス容量タイプがサポートするモニタの説明を示します。

容量タイプ	説明
OSi ライセンス	**サポートされているモニタ：**URL，URL 内容，URL リスト，URL シーケンス，Web スクリプト，Web サービス，リンク・チェック，XML メトリクス，およびフリーのモニタ（コンポジット，フォーミュラ・コンポジット，Amazon Web Services，e ビジネス・トランザクション，および統合モニタ）を除くすべてのモニタ。
	ライセンス消費：一般的に，各モニタ対象リモート・サーバについて，そのリモート・サーバに設定されているモニタの数に関わらず，1 つの OSi ライセンス・インスタンスが消費されます。たとえば，同一のオペレーティング・システムまたはホスト上にある CPU，ディスク・スペース，メモリ・モニタを使用している場合，1 つのOS インスタンスがライセンスから差し引かれます。 **例外：** • カスタム・モニタ，SNMP トラップ，および Microsoft Windows ダイアルアップは，15 のモニタに対して 1 つの OS インスタンスを消費します。 • HP Vertica JDBC モニタは，監視対象のサーバに対して 1 つの OS インスタンスを，また監視対象のノードに対して 1 つの OS インスタンスを消費します。 • Solaris ゾーン・モニタは，監視対象のサーバ・プロパティに対して 1 つの OS インスタンスを，また監視対象のゾーンに対して 1 つの OS インスタンスを消費します。 • VMware データストア・モニタは，データストアごとに 1 つの OS インスタンスを消費します。 • VMware ホストは，監視対象ホストごとに 1 つの OS インスタンス・ライセンス，および監視対象仮想マシンごとに 1 つの OS インスタンス・ライセンスを消費します。VMware のベスト・プラクティスでは，VM ゲストの（vSphere における）オブジェクト名をゲスト自体のサーバ名（またはマシン名）と同一のものに設定することを推奨しています。名前をこのように設定している場合，SiteScope では同一サーバのすべてのモニタに対して 1 つの OS インスタンスのみが使用されます。vSphere オブジェクト名がゲスト・サーバ名と異なる場合，SiteScope ではゲスト・サーバ名を持つすべての VMware モニタに対して 1 つの OS インスタンスが使用され，vSphere オブジェクト名を持つすべてのモニタに対して 1 つの OS インスタンスが使用されます。 **注：**OS インスタンスは異なるエディション間で集計されません。これは，各エディション・タイプで OS インスタンス・ライセンスのコストが異なるためです。ただし，OS インスタンスは，同一エディションの異なる OS ライセンス間で集計されます（たとえば，それぞれが OS インスタンスを含む複数の Premium エディション・ライセンスがある場合）。

容量タイプ	説明
URL ライセンス	**サポートされているモニタ：**URL，URL 内容，URL リスト，URL シーケンス，Web サービス，リンク・チェック，XML メトリクス。 **ライセンス消費：** • 監視対象 URL または URL ステップごとに 1 つの URL ライセンス・インスタンスを消費します。 • URL ライセンスはエディション間で集計されます。ただし，独自の URL ライセンスがあるコミュニティ，試用版，Load Testing エディションは対象外となります。
トランザクション・ライセンス	**サポートされているモニタ：**VuGen スクリプト・トランザクションを使用する Web スクリプト・モニタ。 **ライセンス消費：** • VuGen スクリプト・トランザクションごとに 1 つのトランザクション・ライセンスが消費されます。 • トランザクション・ライセンスはエディション間で集計されます。ただし，トランザクション監視をサポートしないコミュニティおよび Load Testing エディションは対象外となります。

ライセンスのインポートおよびアップグレード

SiteScope のインストールには，無料の Community エディション・ライセンスが含まれています。

Community エディションに搭載される機能から SiteScope を拡張するには，必要に応じた容量タイプ（OSi，URL またはトランザクション）を搭載する SiteScope エディションを購入し，そのライセンス・ファイル・キーを SiteScope にインポートする必要があります。

次の場合に SiteScope ライセンスをインポートできます。

- SiteScope 設定ウィザードを使用したインストール中，または
- ［一般プリファレンス］ページ（「SiteScope ライセンスのインポート」(34ページ)を参照），API または SiteScope 設定ツール（「SiteScope 設定ツールの使用」(124ページ)を参照）を使用したインストール後

階層において上位のエディション・ライセンスをインポートすると，インポートしたライセンスのエディションに応じてアクティブなエディションの機能がアップグレードされます。ライセンスのアップグレードの詳細については，「SiteScope エディション・ライセンスのアップグレード」(32ページ)を参照してください。

Premium，Ultimate および System Collector エディションのライセンス容量を増やすこともできます。詳細については，「ライセンス容量の増加」(33ページ)を参照してください。

SiteScope エディション・ライセンスのアップグレード

既存のライセンス・エディションは，より上位のエディションのライセンスを購入することにより，いつでもアップグレードできます。

SiteScope Community エディションから SiteScope Premium エディションまたは Ultimate エディションにアップグレードすると，SiteScope で使用可能な機能が追加されるという利点が得られます。SiteScope Community エディションで使用可能な機能と，SiteScope のほかのエディションで使用可能な機能の比較については，「機能比較表」(13ページ)を参照してください。

エディション・ライセンスは，次の階層に従ってアップグレードできます。

インストール環境の種類	エディションの階層	利用可能なエディション・アップグレード			利用可能な容量増加	
		プレミアム	アルティメット	システム・コレクタ	トランザクション/URL	OSi
SiteScope	コミュニティ	✔	✔	✔		
	試用版	✔	✔	✔		
	System Collector（バンドル）					✔
	プレミアム		✔	✔	✔	✔
	Ultimate（バンドル）			✔	✔	✔
SiteScope for Load Testing[1]	Load Testing	✔				
	プレミアム				✔	✔
SiteScope Failover	Failover					

[1] SiteScope for Load Testing インストール環境のライセンスを Premium エディションにアップグレードするには，追加の設定が必要です。詳細については，「SiteScope for Load Testing インストール環境のライセンスの Premium エディションへのアップグレード」(33ページ)を参照してください。

エディション・ライセンスをアップグレードするには，次の手順で行います。

1. 必要な SiteScope エディションを購入します。ライセンス購入の照会（または追加の容量が必要な場合）については，HP の営業担当にお問い合わせいただくか，HP SiteScope 製品ページの「お問い合わせ」リンクを使用してください。ライセンスを所有している場合にライセンス・キー・ファイルが必要な場合は，HP Licensing for Software Portal を使用してください。
2. ライセンス・ファイルをインポートします。詳細については，「SiteScope ライセンスのインポート」(34ページ)を参照してください。

> **注:** SiteScope 11.30 にアップグレード後，［ライセンス］パネルが現在のライセンスにより更新されるまでしばらくの時間がかかる場合があります。

SiteScope for Load Testing インストール環境のライセンスの Premium エディションへのアップグレード

> **注:** SiteScope for Load Testing インストール環境を使用する場合，BSM との統合はサポートされません。

SiteScope for Load Testing インストール環境のライセンスを Premium エディションにアップグレードするときは，Premium エディションの機能をすべて利用できるように，次の変更を行う必要があります。

1. SiteScope で［**プリファレンス**］>［**インフラストラクチャ プリファレンス**］>［**カスタム設定**］を選択し，次のようにプロパティ値を変更します。
   - disableRepeatedSchedules=false
   - disableReports=false
   - MultiViewDashboardEnabled=true

   > **注:** _disableRepeatedSchedules=true，_disableReports=true，_MultiViewDashboardEnabled=false プロパティを **<SiteScope ルート・ディレクトリ>\groups\master.config** ファイルから削除し，SiteScope を再起動することもできます。
2. SiteScope を再起動します。

ライセンス容量の増加

作成可能な SiteScope モニタの数は次の 2 つの要因によって決まります。

- 特定のライセンス容量タイプ（OS インスタンス，URL，トランザクション）に対して購入した監視容量。
- 使用する SiteScope モニタのタイプ。

監視環境のニーズに応じて，，Premium，Ultimate および System Collector エディションのライセンス容量を増やすこともできます。試用版，Community，および Load Testing エディションの容量は固定されているため，増やすことができません。

注: 追加の容量を購入し，インポートする場合：

- OSi 容量タイプは，現在のエディションに対してのみ有効です。ライセンス容量は，前回のエディションからの OSi 容量と集約されません。
- URL 容量タイプは，現在の，Premium，Ultimate または System Collector エディションにインポートしたときに，前回のエディションからの URL 容量と集約されます。
- トランザクション容量タイプは，現在の，Premium，Ultimate または System Collector エディションにインポートしたときに，前回のエディションからのトランザクション容量と集約されます。

ライセンス容量を増やすには，次の手順で行います。

1. 必要とする OS インスタンス，URL，トランザクション容量を購入します。ライセンス購入の照会（または追加の容量が必要な場合）については，HP の営業担当にお問い合わせいただくか，HP SiteScope 製品ページの「お問い合わせ」リンクを使用してください。
2. ライセンス・ファイルをインポートします。詳細については，「SiteScope ライセンスのインポート」(34ページ)を参照してください。

SiteScope ライセンスのインポート

HP からライセンス・ファイルを受け取ったら，SiteScope ユーザ・インタフェース経由で SiteScope にライセンス・キーをインポートします。

SiteScope にライセンスをインポートするには，次の手順を実行します。

1. Web ブラウザから，変更する SiteScope インスタンスを開きます。SiteScope サービスまたはプロセスが稼働している必要があります。
2. ［**プリファレンス**］>［**一般プリファレンス**］を選択して，［**ライセンス**］パネルを展開します。
3. ［**ライセンス ファイル**］ボックスに SiteScope ライセンス・ファイルのパスを入力するか，［**選択**］ボタンをクリックしてライセンス・ファイルを選択します。
4. ［**インポート**］をクリックします。ライセンスのインポートが正常に完了したら，インポートされたライセンスに関する情報が［インストールされているライセンス］テーブルに表示されます。ここに含まれるのは，ライセンス・エディション，容量タイプと詳細（使用可能な容量，使用済み容量，残りの容量），有効期限，およびライセンスのステータスです。

   注: SiteScope 11.30 にアップグレード後，［ライセンス］パネルが現在のライセンスにより更新されるまでしばらくの時間がかかる場合があります。

ライセンス有効期限

エディション・ライセンスの有効期限

時間ベースのライセンスの場合，SiteScope はライセンスが期限切れになる 7 日前にユーザに警告メッセージを送信します。

エディションのライセンスの有効期限が切れると，ライセンスはエディション階層内の 1 つ前の有効なライセンスに自動的にダウングレードされます（「SiteScope エディション・ライセンスのアップグレード」(32ページ)を参照）。それ以外の場合，コミュニティ・エディションがアクティブになります。これは，ユーザがライセンスを削除した場合も同様です。

SiteScope 機能は，アクティブなエディションの定義で使用可能な機能に基づき，ただちに減らされます。

注: ユーザはコミュニティまたは Load Testing エディションのライセンスを，**［プリファレンス］ > ［一般プリファレンス］ > ［ライセンス］**の［インストールされているライセンス］テーブルから削除できません。

容量ライセンスの有効期限切れ

OSi，URL，またはトランザクションのライセンスの容量が超過した場合，SiteScope の動作は次のようになります。

1. 警告メッセージを表示するダイアログ・ボックスを開きます。
2. ユーザにライセンス容量が超過しているというメッセージを送信します。SiteScope では 7 日間まで毎日通知を送信します。

このときにユーザが超過モニタを削除していないか，ライセンス容量を増やしていない場合，SiteScope はすべてのモニタを一時停止します。容量が超過していなかったモニタ・タイプでも一時停止になります。モニタが一時停止になっている間，SiteScope からモニタを削除できます。

コミュニティ・ライセンスへのダウングレード

小要ライセンスの有効期限が切れて，他に商用エディションが存在していないか有効なものがない場合，コミュニティ・エディションのライセンスが自動的にアクティブなライセンスになります。コミュニティ・エディションでサポートされないすべての機能はただちに無効になります。

次の表に，ライセンスのダウングレードによる機能への影響を示します。

機能	説明
モニタ	コミュニティ・エディションのライセンス容量が超過すると，すべてのモニタは一時停止になり，メッセージがユーザ・インタフェースに表示されます。 コミュニティ・エディションで使用できない作成されたモニタ（エンタープライズ・モニタおよび Amazon Web Services モニタなど）はすべて実行を停止し，無効

機能	説明
	になります。
ユーザ・アカウント	ユーザは他のユーザ・アカウント（通常または LDAP）でログインする機能や他のユーザアカウントを編集する機能を失います。これは SiteScope 管理者アカウントには適用されません。
データ保存期間	すべての日次ログがファイルシステムで保持されていますが，ユーザが見ることができるレポートおよび分析データは過去 30 日分のみです。
警告	警告アクションはコミュニティ・エディションでは使用できず，無効になっています（電子メールとイベント・コンソール警告アクションのみが可能です）。
レポート	スケジュール設定されたレポートは送信されず，クイック・レポートをユーザ・インタフェースからアクティブ化されます。
API	すべての公開および秘密 SiteScope API はブロックされます。
統合	すべての統合が停止または無効になっています。
SiteScope Failover	SiteScope Failover はエラー・メッセージを得て，プライマリ SiteScope からのデータの同期を停止します。

ライセンスの注意事項および制限事項

コミュニティ・エディション

コミュニティ・エディションは SiteScope のマイナー・バージョンまたはマイナーマイナー・バージョンの各リリースではリリースされません。バージョン・タイプの詳細については，「インストール・バージョンのタイプ」(85ページ)を参照してください。

BSM と統合された SiteScope

- SiteScope がデータを BSM に送信するよう設定されていて，SiteScope ライセンスが期限切れになると，SiteScope は BSM への（トポロジも含めた）すべてのデータの送信を停止します。SiteScope ではライセンスの有効期限が切れると自動的に BSM へのログ記録とデータ・フローが無効になるため，BSM へのログ記録とデータ・フローを有効にするには，SiteScope ライセンスの更新時に，**［プリファレンス］ > ［統合プリファレンス］ > ［BSM 統合］ > ［BSM 統合のメイン設定］**の［**Business Service Management へのログ記録をすべて無効にする**］チェック・ボックスの選択を解除する必要があります。
- SiteScope プレミアム，アルティメット，またはシステム・コレクタ・エディションのライセンスの有効期限が切れた後に（そのため BSM との統合が無効になった場合に），SiteScope からモニタを削除すると，モニタは BSM から削除されません。BSM の［**SiteScope トポロジ・アップグレー**

ドの整合性］ビューから**［RTSM 管理］ > ［IT ユニバース・マネージャ］**で，手動でモニタを削除する必要があります。

第4章: スタートアップ・ロードマップ

本項では，SiteScope を起動して実行するまでの，基本的な手順ごとのロードマップを説明します。

1. **SiteScope のコピーを登録します。**

   SiteScope のコピーを登録すると，HP の全製品に関するテクニカル・サポートや情報にアクセスできるようになります。また，更新とアップグレードも受けられます。HP ソフトウェア・サポートのサイトで，SiteScope のコピーを登録できます。

2. **ヘルプの入手先について参照します。**

   SiteScope ヘルプに加え，HP サービスや HP ソフトウェア・サポートなどの支援に関する情報を確認してください。

3. **SiteScope のデプロイメント計画を立てます。**

   SiteScope ソフトウェアをインストールする前に，完全なデプロイメントの計画を作成します。「デプロイメントの方法と計画」(39ページ)を参考にしてください。詳細なデプロイメント計画のベスト・プラクティスについては，HP の営業担当者までお問い合わせください。

4. **SiteScope のインストール**

   SiteScope アプリケーションのデプロイの基本手順を理解するには，「インストールの概要」(61ページ)を参照してください。SiteScope の安全なデプロイに関する情報については，「SiteScope プラットフォームのセキュリティ強化」(149ページ)を参照してください。

5. **SiteScope にログオンし，システムの管理を開始します。**

   Web ブラウザを使用して，SiteScope Web インタフェースにログインします。基本的なプラットフォームおよびモニタ管理作業全体について説明している，「インストール後の管理」(192ページ)のチェックリストを使用して，SiteScope を実運用に向けてデプロイする準備をします。

6. **SiteScope をビジネス・ユーザおよびシステム・ユーザに公開します。**

   SiteScope のユーザが定義され，監視データの受信が可能な状態で運用が開始されたら，ビジネス・ユーザおよびシステム・ユーザに対して，SiteScope の監視機能，レポート機能，および警告機能にアクセスして利用する方法を説明するプロセスを開始します。

SiteScope の使用と管理の詳細については，SiteScope ヘルプを参照してください。

第5章: デプロイメントの方法と計画

本章の内容

- 「エンタープライズ・システム監視の方法」(39ページ)
- 「ビジネス・システム・インフラストラクチャの評価」(41ページ)
- 「SiteScope サーバのサイズ設定」(42ページ)
- 「ネットワークの場所と環境」(42ページ)
- 「Windows 環境の場合に考慮する事項」(43ページ)
- 「Linux 環境の場合に考慮する事項」(43ページ)

エンタープライズ・システム監視の方法

SiteScope のデプロイは，リソース計画，システム・アーキテクチャ設計，綿密に計画された高い導入戦略が必要となるプロセスです。本章では，SiteScope のデプロイメントと使用を成功させるための方法と検討する必要のある項目について説明します。

注: 次の情報を参考にして，インストールを始める前の準備を行ってください。詳細なデプロイメント計画のベスト・プラクティスについては，HP のプロフェッショナル・サービス担当者までお問い合わせください。

システム監視を効果的に行うには，一貫した方法が不可欠です。しかし，エンタープライズ監視ソリューションへの取り組み，開発，およびデプロイの方法は，必ずしも明白ではありません。ソリューションでは，IT インフラストラクチャの役割や，それを組織の成功に結びつける方法を検討する必要があります。システム監視は，組織の主要な目的を達成するために組織によって使用されるサービスの可用性や機能を確認するツールです。システム監視を計画するためのガイドとして次の内容を参考にしてください。

監視対象

エンタープライズ・システムを効果的に管理するには，多層的な監視方法を使用します。SiteScope には，これを実行するためのツールが用意されています。あるレベルでは，インフラストラクチャ内の個々のハードウェアの要素を監視して，それらが実行され利用可能であることを確認します。監視対象に，システム上の主要なサービスやプロセスを加えます。これには，低レベルのオペレーティング・システムのプロセスや，主要なアプリケーションの動作状況やパフォーマンスを示すプロセスも含まれています。この上のレベルでは，ビジネス・プロセスのトランザクションを監視して，主要なアプリケーションやサービスが利用可能で期待どおりに機能していることを確認します。

イベントを表すしきい値レベル

エンタープライズ・ビジネスに成功するには，情報システムの可用性とパフォーマンスが重要です。モニタに設定するしきい値は，監視するシステムまたはビジネス・プロセスの性質によって決定します。

システム・チェックの頻度

システムをチェックする頻度はイベントしきい値の設定と同様に重要です。ミッション・クリティカルな情報システムの可用性は，アクセス可能な期間中は定期的にチェックする必要があります。多くの場合，システムは 1 日 24 時間，週 7 日利用できなくてはなりません。各モニタの［頻度］設定を使用して，SiteScope がシステムをチェックする**頻度**を制御します。チェックを行う時間間隔が長すぎると，問題の検出が遅れる可能性があります。頻繁にチェックしすぎると，すでにビジー状態のシステムを不要にロードする可能性があります。

イベント検出時のアクション

監視アプリケーションとして，SiteScope には問題を検出するツールが用意されています。イベントしきい値が発行されたら，SiteScope 警告を使用して通知をタイムリーに送信できます。一般的に使用される警告アクションは電子メール通知です。SiteScope には，ほかのシステムと統合できるそのほかの警告タイプが含まれています。

異なる警告トリガ条件で複数の警告定義を定義することにより，警告をエスカレーションするためのスキーマを作成できます。検出されたイベントと警告アクション間の関係をカスタマイズするには，警告の［**発行条件設定**］を使用します。

利用できなくなったシステムに依存するシステムの監視や警告発行を無効にするイベント・アクションが存在することがあります。一連の警告のカスケーディングを避けるには，SiteScope グループおよびモニタの依存オプションを使用できます。

実行可能な自動応答

問題が検出された場合に理想的なのは，問題に自動的に対応して解決することです。すべてのシステムに対してこれは不可能ですが，SiteScope 警告は，さまざまな状況に対応する柔軟かつ強力な自動修正アクションのためのツールを提供します。お使いの環境で発生する可能性のある問題のうち，自動応答で対処できるものを検討する必要があります。

ビジネス・システム・インフラストラクチャの評価

1. アーキテクチャやデプロイメントに関する決定を行う前に，技術的な要件とビジネス要件を収集します。この段階のアクションは次のとおりです。
   - 監視するすべてのビジネス・アプリケーションのリストを作成します。このとき，注文処理，アカウントのアクセス機能，データ・クエリ，更新，およびレポーティングなど，エンド・ツー・エンドのサービスを検討する必要があります。
   - ビジネス・アプリケーションをサポートするサーバのリストを作成します。これには，フロントエンド Web インタフェース，バックエンド・データベース，およびアプリケーション・サーバをサポートするサーバを含める必要があります。
   - ビジネス・アプリケーションをサポートするネットワーク・デバイスのリストを作成します。これには，ネットワーク・アプリケーションおよび認証サービスが含まれます。
   - 監視するハートビート要素を特定します。ハートビート要素は，特定のビジネス・システムまたはリソースの可用性の基礎的なインジケータとして機能するサービスです。
   - 各システムのために監視するリソースを表示するモニタのテンプレートの枠組みを設定します。
2. 動作状況を監視するビジネス・システムの関係者と主要な成果物を特定します。成果物は次のように特定します。
   - 生成するレポートは何か。
   - イベント検出時に実行する警告アクションは何か。
   - 警告の送信先は誰か。
   - SiteScope を表示して管理を行うためにアクセスが必要なユーザは誰か。
   - どのような SiteScope 要素がどの関係者にアクセス可能である必要があるか
   - サービス・レベル・アグリーメントに対するしきい値は何か（必要な場合）。
3. システム監視機能が動作する制約を理解します。これには，使用できるプロトコル，ユーザ認証要件，ビジネスの機密データを含むシステムへのアクセス，およびネットワーク・トラフィックの制限が含まれます。

SiteScope サーバのサイズ設定

SiteScope が稼働するサーバのサイズを正しく設定することが，監視のデプロイメントに成功する基礎となります。サーバのサイズ設定は，次のいくつかの要因によって決定します。

- SiteScope インストール環境で実行されるモニタ・インスタンスの数
- モニタの平均実行頻度
- プロトコルの種類と監視するアプリケーションの種類
- レポート作成用にサーバ上で保持する必要のある監視データの量

必要なモニタの数を見積もるための出発点は，環境内のサーバ数，それぞれのオペレーティング・システム，および監視するアプリケーションを知ることです。

実行されるモニタ数の見積もりに基づいた，推奨されるサーバのサイズ設定の表については，「Windows プラットフォーム上での SiteScope のサイズ設定」(48ページ)または「Linux プラットフォーム上での SiteScope のサイズ設定」(50ページ)を参照してください。

ネットワークの場所と環境

大半の SiteScope 監視は，ネットワーク環境でサーバやアプリケーションに要求を行う，Web またはネットワーク・クライアントをエミュレートすることにより実行されます。このため，SiteScope はネットワーク全体にわたって，サーバ，システム，およびアプリケーションにアクセスできなければなりません。これは，SiteScope をインストールする場所を決定する目安となります。

システム，サーバ，およびアプリケーションを監視するために SiteScope が使用する方法は，次の 2 つのカテゴリに分類できます。

- **標準ベースのネットワーク・プロトコル** HTTP，HTTPS，SMTP，FTP，および SNMP が含まれます。
- **プラットフォーム固有のネットワーク・サービスおよびネットワーク・コマンド** NetBIOS，telnet，rlogin，およびセキュア・シェル（SSH）が含まれます。

インフラストラクチャの監視ではプラットフォーム固有のサービスを利用します。エージェントレス・ソリューションとして監視するには，SiteScope がインフラストラクチャ内の多くのサーバに対して，頻繁にログインと認証を行う必要があります。パフォーマンスおよびセキュリティ上の理由から，SiteScope は同じドメイン内にデプロイし，できるだけ監視するシステム要素に近付けることをお勧めします。また，SiteScope を該当のネットワーク認証サービス（たとえば Active Directory，NIS，または LDAP）と同じサブネット内に置くこともお勧めします。必要に応じて，HTTP または HTTPS を使用して，SiteScope インタフェースをリモートでアクセスおよび管理できます。

注: 大量の監視アクティビティが WAN（Wide Area Network）上での通信を必要とする位置に SiteScope をデプロイしないでください。

ヒント: ファイアウォール越しにサーバを監視するには，サーバの可用性の監視に異なるプロト

コルとポートが必要となります。そのため，セキュリティ上の理由から，SiteScope を使用しないことをお勧めします。SiteScope のライセンスは，ファイアウォールの両側にある別々の SiteScope のインストールをサポートします。HTTP または HTTPS を使用して，1 台のワークステーションから 2 つ以上の異なる SiteScope に同時にアクセスできます。

Windows 環境の場合に考慮する事項

SiteScope のインストールには，管理者権限を持つアカウントを使用する必要があります。また，SiteScope サービスの実行にも，管理者権限を持つユーザ・アカウントを使用することをお勧めします。ローカル・システム・アカウントも使用できますが，リモート Windows サーバへの接続プロファイルの設定に影響します。

また，SiteScope はリモート・マシン上で Windows パフォーマンス・レジストリを使用し，サーバのリソースと可用性を監視します。この監視機能を有効にするには，リモート・マシン用のリモート・レジストリ・サービスをアクティブにする必要があります。

Linux 環境の場合に考慮する事項

Linux 環境では，SiteScope を root ユーザとしてインストールする必要があります。SiteScope がインストールされた後，SiteScope を実行する権限のある非 root ユーザ・アカウントを作成できます（SiteScope Web サーバが特権ポート上で実行されない限り，root ユーザが実行する必要はありません）。 SiteScope を実行する権限のある非 root ユーザの設定の詳細については，「SiteScope を実行する権限のある非 root ユーザ・アカウントの設定」(44ページ)を参照してください。

SiteScope を使用したリモート UNIX サーバのエージェントレス監視のセットアップに関する追加情報を以下に示します。

- **リモート・ログイン・アカウント・シェル：** SiteScope は，アプリケーションとして，ほとんどの一般的な UNIX シェルで正常に実行できます。SiteScope は，リモート UNIX サーバと通信する場合，Bourne シェル（sh）または tsch シェルのどちらかと通信します。したがって，これらのシェルのうちの 1 つを使用するため，各リモート UNIX サーバ上の関連するログイン・アカウントにはシェル・セットが必要です。

  注: シェル・プロファイルは，リモート・マシンと通信するために SiteScope が使用するログイン・アカウントにのみ設定します。リモート・マシン上のその他のアプリケーションおよびアカウントは，現在定義されているシェルを使用できます。

- **アカウント権限 :**リモート UNIX サーバを監視する場合，コマンド権限の設定を解決しなければならないことがあります。リモート UNIX サーバからサーバ情報を取得するために SiteScope が実行するほとんどのコマンドは，リモート・サーバの **/usr/bin** ディレクトリにあります。ただし，メモリの情報を取得するコマンドなど，一部のコマンドは **/usr/sbin** にあります。**/usr/sbin** コマンド

は通常，root ユーザまたはその他の高い権限を持つユーザのために予約されているため，これら 2 つは違う場所にあります。

注: SiteScope には高いアカウント権限が必要ですが，セキュリティ上の理由から，root アカウントを使用した SiteScope の実行や，リモート・サーバで root ログイン・アカウントを使用するような SiteScope の設定は行わないことをお勧めします。

権限に問題がある場合は，コマンドを実行する権限を持つ別のユーザとして SiteScope にログインするか，または SiteScope が使用しているユーザ・アカウント用に権限を変更する必要があります。

SiteScope を実行する権限のある非 root ユーザ・アカウントの設定

SiteScope は，root ユーザ・アカウントから Linux にインストールする必要があります。SiteScope がインストールされた後，SiteScope を実行する権限のある非 root ユーザ・アカウントを作成できます。

注: すべてのサーバ監視機能を使用するには SiteScope に高いアカウント権限が必要ですが，root アカウントからの SiteScope の実行や，リモート・サーバへのアクセスに root アカウントを使用するような SiteScope の設定は行わないことをお勧めします。

SiteScope を実行する権限のある非 root ユーザ・アカウントを作成するには，次の手順で行います。

1. 新しいユーザを追加します。useradd newuser
2. SiteScope インストール・フォルダの権限を変更します。chmod 755 /opt/HP/SiteScope/ -R
3. SiteScope インストール・フォルダの所有権を変更します。chown newuser /opt/HP/SiteScope/ -R
4. 新しいユーザとしてログインします。su newuser
5. インストール・フォルダに移動します。cd /opt/HP/SiteScope
6. SiteScope を実行します。./start

注: HP Operations Manager イベントおよび測定値の統合を有効にするには，SiteScope マシン上の HP Operations Agent は SiteScope と同じユーザ（つまり非 root ユーザ）で実行する必要があります。詳細は，『HP Operations Manager for UNIX - HTTPS Agent Concepts and Configuration Guide』の「Configure an Agent to run Under an Alternative User on UNIX」を参照してください。

第6章: SiteScope のサイズ設定

本章の内容

- 「SiteScope のサイズ設定の概要」(45ページ)
- 「SiteScope キャパシティ・カリキュレータ」(45ページ)
- 「Windows プラットフォーム上での SiteScope のサイズ設定」(48ページ)
- 「Linux プラットフォーム上での SiteScope のサイズ設定」(50ページ)
- 「トラブルシューティングおよび制限事項」(54ページ)

SiteScope のサイズ設定の概要

標準の SiteScope 設定では何千ものモニタを実行できますが，最適なパフォーマンスを得るには SiteScope がインストールされているサーバのサイズ設定が必要となる場合があります。設定はそれぞれ異なるため，SiteScope キャパシティ・カリキュレータを使用し，運用している SiteScope の設定がサイズ設定を必要としているかどうかを検証する必要があります。

SiteScope が稼働するサーバのサイズを正しく設定することが，監視のデプロイメントに成功する基礎となります。最適なサイズ設定を行うために，HP では，次の SiteScope サーバ環境を強くお勧めします。

- SiteScope をスタンドアロン・サーバとして実行する。最良の結果を得るには，サーバ上で実行するプログラムを SiteScope のみにします。BSM，BMC，HP LoadRunner，データベース，Web サーバなどは，SiteScope サーバにインストールしないようにしてください。
- SiteScope の 1 つのインスタンスのみを 1 つのサーバ上で実行します。1 つのサーバ上で SiteScope の複数のインスタンスを実行すると，サーバ・リソースの問題が発生する可能性があります。この推奨事項は，システム状況 で使用される SiteScope のインスタンスにも当てはまります。
- SiteScope Failover には，プライマリ SiteScope サーバと同様のサイズ設定が必要です。

SiteScope キャパシティ・カリキュレータ

SiteScope には，システムの動作を予測し，SiteScope のキャパシティ・プランニングを実行するためのツールが用意されています。SiteScope を実行しているシステムの CPU とメモリの詳細，タイプ別のモニタ数，モニタの実行頻度を入力します。この入力が終わると，モニタ タイプごとの予測される CPU 使用率とメモリ使用率，特定の作業負荷に推奨されるシステム要件などがカリキュレータによって表示されます。この情報から，設定にチューニングが必要かどうかを判断できます。

注: SiteScope キャパシティ・カリキュレータは Windows 版で実行されている SiteScope のみでサポートされ，「サポートされているモニタとソリューション・テンプレート」(47ページ) に記載されている 64 ビットのモニタおよびソリューション・テンプレートに対応しています。

SiteScope キャパシティ・カリキュレータを使用するには，次の手順で行います。

1. カリキュレータを使用する前に，SiteScope サーバでの負荷を見積もり，ハードウェア要件を判断するために本書のシステム要件と推奨事項を使用します。

   詳細については，「システムのハードウェア要件」(62ページ)を参照してください。
2. 次から利用可能な SiteScope キャパシティ・カリキュレータを開きます。
   - SiteScope インストール・フォルダ :**<SiteScope root directory>\tools\SiteScopeCapacityCalculator.xls**
   - HP ソフトウェア・サポート・サイト。
3. SiteScope がインストールされているオペレーティング・システムに対応する［**モニタの使用方法**］タブを選択します。SiteScope 11.30 では，64 ビット・オペレーティング・システムしかサポートされていません。
4. ［**Requirements**］セクションで，次の情報を入力します。
   - 平均 CPU 使用率
   - CPU タイプ
   - メモリ・ヒープ・サイズ（メガバイト単位）
   - 64 ビット・システムにインストールする場合は，SiteScope が BSM と統合されている場合は TRUE を選択し，スタンドアロン SiteScope の場合は FALSE を選択します。
5. ［**Monitors**］セクションで，各タイプのモニタの数と，各モニタの更新頻度を入力します。
6. 結果と推奨事項が［**Results and Recommendations**］セクションに表示されます。予期された結果と実際の結果の 30 ~ 40% の相違は許容範囲とみなします。

サポートされているモニタとソリューション・テンプレート

SiteScope キャパシティ・カリキュレータでは，次のモニタとソリューション・テンプレートがサポートされます。

モニタ：

- CPU
- データベース・カウンタ
- データベース・クエリ（64 ビットのみ）
- ディレクトリ・モニタ（64 ビットのみ）
- ディスク領域
- DNS モニタ
- ファイル・モニタ（64 ビットのみ）
- JMX モニタ（64 ビットのみ）
- ログ・ファイル・モニタ（32 ビットのみ）
- メモリ・モニタ
- Microsoft IIS サーバ・モニタ
- Microsoft SQL Server モニタ（32 ビットのみ）
- Microsoft Windows イベント・ログ・モニタ（32 ビットのみ）
- Microsoft Windows リソース・モニタ
- Ping モニタ
- SAP CCMS モニタ（32 ビットのみ）
- サービス・モニタ
- Siebel アプリケーション・サーバ・モニタ（32 ビットのみ）
- MIB による SNMP モニタ
- UNIX リソース・モニタ（64 ビットのみ）
- URL モニタ
- URL リスト・モニタ（64 ビットのみ）
- WebLogic アプリケーション・サーバ・モニタ（32 ビットのみ）
- Web サービス・モニタ（64 ビットのみ）
- WebSphere アプリケーション・サーバ・モニタ（32 ビットのみ）

ソリューション・テンプレート：

- Microsoft Exchange 2003 ソリューション・テンプレート（32 ビットのみ）
- Siebel ソリューション・テンプレート（32 ビットのみ）

注: SiteScope 32 ビット・モニタは廃止されているため，SiteScope 11.30 へのアップグレード後は機能しません。詳細については，「32 ビットから 64 ビットの SiteScope への移行」(73ページ)を参照してください。

Windows プラットフォーム上での SiteScope のサイズ設定

Windows プラットフォームにインストールされている SiteScope のサイズ設定を行う場合は，SiteScope と Windows オペレーティング・システムで次のサイズ設定手順を実行する必要があります。

1. **SiteScope のサイズ設定を行います。**

   最初に SiteScope をサイズ設定し，少なくとも 24 時間 SiteScope を稼働してから次の手順に進むことをお勧めします。詳細については，「SiteScope のサイズ設定」(48ページ)の手順を参照してください。

2. **Windows オペレーティング・システムのチューニング**

   SiteScope をサイズ設定して少なくとも 24 時間待機したら，Windows オペレーティング・システムのチューニングを行い，その後，サイズ設定パラメータの変更を有効にするために SiteScope サーバを再起動する必要があります。詳細については，「Microsoft Windows オペレーティング・システムのチューニング」(49ページ)の手順を参照してください。

3. **一般的な保守の推奨事項**

   また，いくつかの一般的な保守の推奨事項に従って，最適なチューニングを行ってください。詳細については，「一般的な保守の推奨事項」(49ページ)を参照してください。

注:

- 変更するすべてのファイルまたはパラメータのバックアップを行い，必要に応じてバックアップから復元できるようにしておくことをお勧めします。
- 設定に効果がない場合，ファイルやパラメータをむやみに増やしたり減らしたりしないでください。詳細な分析やトラブルシューティングについては，HP ソフトウェア・サポートにお問い合わせください。

SiteScope のサイズ設定

SiteScope のサイズ設定では，本当に必要な場合にだけ，モニタが［**エラーを検証**］オプションを使用することを確認する必要があります。このオプションはごくわずかのモニタに使用されなければならず，それらは，監視対象のリモート・マシンのネットワーク問題やサーバ負荷の問題によって，誤った「**データなし**」警告を受けた履歴を持つモニタなどです。

この機能を有効にすると，失敗したモニタは，警告条件がチェックされる前にスケジューラをバイパスしてすぐに再実行されます。このような特別な実行が多数発生すると，スケジューラが大きく混乱し，SiteScope のパフォーマンスを低下させる可能性があります。モニタが接続の問題で失敗する場合は，［接続タイムアウト］に設定されている時間が経過してモニタが終了するまでエラーの検証が終了しない可能性があります。この間，標準設定では，モニタ・スレッドと接続が 2 分間ロックされ

ます。この遅延により，ほかのモニタの待機や，失敗したモニタのスキップが発生することがあります。

SiteScope をサイズ設定するには，次の手順を実行します。

1. モニタごとに，［**プロパティ**］タブを選択して［**モニタの実行設定**］パネルを開き，［**エラーを検証**］が選択されているかどうかを調べます。このオプションが必要でないモニタでは，チェック・ボックスをクリアします。

   ヒント: 複数のモニタの場合，［**グローバル検索と置換**］を使用してこのタスクを実行することをお勧めします。

2. Windows オペレーティング・システムのチューニングを行う前に，少なくとも 24 時間 SiteScope を実行します。

Microsoft Windows オペレーティング・システムのチューニング

Microsoft Windows オペレーティング・システムのチューニングでは，設定ツールを使用していくつかのパラメータを変更する必要があります。また，いくつかの一般的な保守の推奨事項に従って，最適なチューニングを行ってください。

Microsoft Windows オペレーティング・システムをチューニングは，次の手順で行います。

1. 設定ツールを実行し，［**サイズ変更**］オプションを選択します。

   このツールにより，JVM ヒープ・サイズが 4096 MB，デスクトップ・ヒープ・サイズが 8192 KB，ファイル・ハンドル数が 18,000 に増加します。また，SiteScope 実行ファイルのポップアップ警告が無効になります。詳細については，「Windows プラットフォームでの設定ツールの実行」(124ページ)を参照してください。

   注: 設定ツールでサポートされるのは，標準設定の SiteScope サービス名だけです。サービス名を変更した場合は，設定ツールを実行せず，HP ソフトウェア・サポートにお問い合わせください。

2. パラメータの変更を反映させるために，SiteScope サーバを再起動します。
3. 必要に応じて，［**プリファレンス**］ > ［**インフラストラクチャ プリファレンス**］でほかのサイズ設定関連パラメータを設定します。

   ヒント: 最適なパフォーマンスを得るには，これらの設定に標準設定値を使用することをお勧めします。

一般的な保守の推奨事項

次に，Windows 上の SiteScope をサイズ設定するための一般的な保守の推奨事項について説明します。

- **適切なモニタ頻度を決定する。**

  モニタの実行頻度を確認し，モニタが適切な間隔で実行されていることを確認します。たとえば，ほとんどのディスク・モニタは 5 分間隔で実行する必要はありません。通常は，おそらく /var，/tmp，および swap 以外のすべてのボリュームについては，15 分，30 分，または 60 分間隔が適切です。モニタ頻度を小さくすることで 1 分間に稼働するモニタの数が少なくなり，パフォーマンスと処理能力が改善されます。

- **グループ構造を最適化する。**

  グループ構造には，SiteScope の使いやすさと SiteScope のパフォーマンスの最適化を考慮してください。構造の深さを最小限に抑えるように，トップレベルのグループの数も最小限に抑えるのが理想的です。

  グループ構造に 50 を超えるトップレベルのグループがある場合，またはグループ構造が 5 階層より深い場合，パフォーマンスが低下する可能性があります。

- **SiteScope 設定エラーを解決する。**

  状況モニタを使用して，モニタ設定のエラーを解決します。エラーが少数でも，パフォーマンスや安定性の低下につながる可能性があります。これらのエラーを解決する方法については，HP ソフトウェア・サポートにお問い合わせください。

- **SiteScope サーバの物理的な位置を計画する。**

  SiteScope サーバは，ローカル・ネットワーク上でその監視対象マシンにできるだけ近い場所に設置することをお勧めします。十分な容量があり遅延の低い接続環境では許容可能な場合がありますが，WAN 接続を経由して監視することはお勧めしません。

Linux プラットフォーム上での SiteScope のサイズ設定

Linux オペレーティング・システム上で SiteScope のサイズ設定を行うには，いくつかのパラメータを変更する必要があります。また，いくつかの一般的な保守の推奨事項に従って，最適なチューニングを行ってください。

1. **オペレーティング・システムのチューニング**

   SiteScope インスタンス用の適切なスレッド数を設定し，Linux オペレーティング・システム・パラメータを設定します。詳細については，「オペレーティング・システムのチューニング」(51ページ)の手順を参照してください。

2. **Java 仮想マシンのチューニング**

   JVM ヒープ・サイズとスレッド・スタック・サイズを設定し，パラレル・ガベージ・コレクションを実装します。詳細については，「Java 仮想マシンのチューニング」(52ページ)の手順を参照してください。

3. **一般的な保守の推奨事項**

   また，いくつかの一般的な保守の推奨事項に従って，最適なチューニングを行ってください。詳細については，「一般的な保守の推奨事項」(53ページ)を参照してください。

オペレーティング・システムのチューニング

オペレーティング・システムのチューニングでは，SiteScope インスタンス用の適切な数のモニタと，Linux オペレーティング・システムのパラメータを設定する必要があります。

実行中モニタの最大数の設定

［**実行中モニタの最大数**］設定は，［**プリファレンス**］ > ［**インフラストラクチャ プリファレンス**］ > ［**サーバ設定**］で行えます。詳細については，SiteScope ヘルプの「SiteScope の使用」にある「プリファレンス」セクションを参照してください。

ヒント: 最適のパフォーマンスを得るには，この設定に標準設定値を使用することをお勧めします。

Linux オペレーティング・システム パラメータの設定

Linux オペレーティング・システムは大量のスレッドをサポートできます。この機能を有効にするには，SiteScope サーバで次の手順で行います。

Linux オペレーティング・システムのパラメータを設定するには，次の手順で行います。

1. **カーネル・ファイル記述子の制限を変更します。**
   a. **/etc/system** ファイルを編集して次の行を追加します。

      set rlim_fd_max=8192

      注: 標準設定は 1024 です（この制限は root ユーザには適用されません）。値「8192」は，SiteScope の最大のインスタンスにも対応します。小さな値を試すより，この大きな値を使用してください。これにより，小さな値で不十分だった場合に，マシンを再起動する必要がなくなります。

   b. サーバを再起動します。
2. **ユーザのランタイムの制限を変更します。**
   a. **<SiteScope のルート・ディレクトリ>\bin ディレクトリ**で，SiteScope スタートアップ・スクリプト，**start-monitor**，**start-service** に次の行を追加します。

      ulimit -n 8192

   b. 次のパラメータが次の最小値であることを確認します。詳細については，UNIX システム管理者にお問い合わせください。

パラメータ	最小値
コア・ファイル・サイズ（ブロック）	制限なし
データ・セグメント・サイズ（キロバイト）	制限なし

パラメータ	最小値
ファイル・サイズ（ブロック）	制限なし
開くファイル数	8192
パイプ・サイズ（512 バイト）	10
スタック・サイズ（キロバイト）	8192
CPU 時間（秒）	制限なし
最大ユーザ・プロセス数	8192
仮想メモリ（キロバイト）	制限なし

ランタイムの制限の変更後に，SiteScope アプリケーションまたはサーバを再起動する必要はありません。

Java 仮想マシンのチューニング

最適なパフォーマンスを得るために JVM を設定する必要があります。

JVM を設定するには，次の手順で行います。

1. **ヒープ領域を増やします。**

   標準設定では，SiteScope の Java のヒープ領域は 512 MB に設定されています。これは大量インスタンスの通常運用には不十分です。

   Java ヒープ領域は，**<SiteScope のルート・ディレクトリ>\bin** ディレクトリで **start-service** スクリプトと **start-monitor** スクリプトを変更することで，4096 MB（高負荷の場合に推奨されるヒープ・サイズ）まで増やせます。

   SiteScope の起動時のパフォーマンスを高めるには，最小ヒープ・サイズと最大ヒープ・サイズが等しくなるように設定することをお勧めします。たとえば，-Xmx4096m –Xms512m を -Xmx4096m –Xms4096m のように変更します。

2. **スレッド・スタック・サイズ（-Xss）を減らします。**

   SiteScope によって作成された各スレッドは，-Xss で割り当てられているメモリ量を使用してスタックをインスタンス化します。標準設定の UNIX JRE の最大スレッド・スタック・サイズ，-Xss は，スレッドごとに 512 KB メモリです。

   <SiteScope のルート・ディレクトリ>\bin\start-monitor の Java コマンド・ラインに指定されていない場合，標準設定の最大スレッド・スタック・サイズが使用されます。標準設定のサイズは，使用できるメモリを超過することによって，スレッドの数を制限できます。

   4000 以上のモニタから成るインスタンスは，128 KB の -Xss を利用できます。

一般的な保守の推奨事項

Linux プラットフォームで SiteScope のサイズ設定を行うには，一般的な保守の推奨事項があります。

- **状況モニタを使用する。**

  可能な限り，特にリモート UNIX 接続を使用するすべてのモニタで，［**依存対象**］で状況モニタを利用します。状況モニタにより，複数のマシンが使用不能になった場合や SSH 接続スレッドがロックされた場合に，それを検出することでサーバのパフォーマンスの低下を防ぐことができます。

- **エラーを検証する機能の使用を最小限に抑える。**

  ［**モニタの実行設定**］パネルで［**エラーを検証**］オプションを有効にすると，停止したモニタは，警告条件がチェックされる前にスケジューラをバイパスしてすぐに再実行されます。このような特別な実行が多数発生すると，スケジューラが大きく混乱し，SiteScope のパフォーマンスを低下させる可能性があります。モニタが接続の問題で失敗する場合は，［接続タイムアウト］に設定されている時間が経過してモニタが終了するまでエラーの検証が終了しない可能性があります。この間，標準設定では，モニタ・スレッドと接続が 2 分間ロックされます。この遅延により，ほかのモニタの待機や，失敗したモニタのスキップが発生することがあります。

- **SSH および内部 Java ライブラリを使用する。**

  SSH 接続方法を使用してリモート・プリファレンスを定義する場合，可能な限り，SSH および内部 Java ライブラリ・オプションを使用します。内部 Java ライブラリは，サードパーティ製の Java ベースの SSH クライアントです。このクライアントにより，Telnet およびホストのオペレーティング・システムの SSH クライアント経由のパフォーマンスやスケーラビリティが大幅に改善されます。このクライアントは，SSH1，SSH2，公開鍵認証などをサポートします。

  接続キャッシュが有効であることを確認します（［新規 Microsoft Windows リモート サーバ］，［Microsoft Windows リモート サーバの編集］，［新規 UNIX リモート サーバ］，［UNIX リモート サーバの編集］の各ダイアログ・ボックスで［**詳細設定**］を展開し，［**接続キャッシュの無効化**］チェック・ボックスをクリアします）。［**最大接続数**］を調整して，特定のサーバに対して稼働するすべてのモニタをタイムリーに実行できるようにする必要があります。

- **適切なモニタ頻度を決定する。**

  モニタの実行頻度を確認し，モニタが適切な間隔で実行されていることを確認します。たとえば，ほとんどのディスク・モニタは 5 分間隔で実行する必要はありません。通常は，おそらく /var，/tmp，swap 以外のすべてのボリュームについては，15 分，30 分，または 60 分間隔が適切です。モニタ頻度を小さくすることで 1 分間に稼働するモニタの数が少なくなり，パフォーマンスと処理能力が改善されます。

- **グループ構造を最適化する。**

  グループ構造には，SiteScope の使いやすさと SiteScope のパフォーマンスの最適化を考慮してください。構造の深さを最小限に抑えるように，トップレベルのグループの数も最小限に抑えるのが理想的です。

  グループ構造に 50 を超えるトップレベルのグループがある場合，またはグループ構造が 5 階層より深い場合，パフォーマンスが低下する可能性があります。

- **SiteScope 設定エラーを解決する。**

  状況モニタを使用して，モニタ設定のエラーを解決します。エラーが少数でも，パフォーマンスや安定性の低下につながる可能性があります。これらのエラーを解決する方法については，HP ソフトウェア・サポートにお問い合わせください。

- **SiteScope サーバの物理的な位置を計画する。**

  SiteScope サーバは，ローカル・ネットワーク上でその監視対象マシンにできるだけ近い場所に設置することをお勧めします。WAN や低速ネットワーク・リンクを監視する場合は，通常，ネットワークがボトルネックになります。このため，監視の実行に時間がかかる場合があります。十分な容量があり遅延の低い接続環境では許容可能な場合がありますが，WAN 接続を経由して監視することはお勧めしません。

- **ローカル・ユーザ・アカウントを使用する。**

  ローカル・ユーザ・アカウントは，UNIX Remote Authentication の Directory サービス・アカウントに適しています。ローカル・ユーザ・アカウントにより，認証に対する Directory サービス・サーバへの依存を回避します。これによって，認証が迅速に行われ，Directory サービス・サーバがダウンしても接続の失敗を避けることができます。

  SiteScope のインスタンスが非常に大量な場合，Directory サービス・サーバのパフォーマンスに悪影響を及ぼす可能性があります。Directory サービス・サーバは監視対象サーバに近い場所に設置することをお勧めします。

トラブルシューティングおよび制限事項

問題 : JVM が「スワップ領域不足」エラーでクラッシュする。

以下の方法でスワップ領域不足エラーを検出できます。

1. ターゲットの SiteScope サーバで仮想バイト・カウンタを監視するために Microsoft Windows リソース・モニタを作成します。
2. 次のしきい値に設定します。

   ［エラー条件］ > = 7.9 GB

   ［警告条件］ > = 7.8 GB

   （このプロセスは値が 8 GB に達するとクラッシュします）

解決方法 :

1. JVM ヒープ・サイズを小さくします。JVM ヒープ・サイズの変更についての詳細は，「Windows プラットフォームでの設定ツールの実行」(124ページ)を参照してください。
2. 動作している現在のモニタ数を削減して（［**プリファレンス**］ > ［**インフラストラクチャ プリファレンス**］ > ［**サーバ設定**］ > ［**モニタ プロセスの最大数**］で），SiteScope が使用するスレッド数を減らします。

第7章: エージェントレス監視について

本章の内容

- 「SiteScope 監視機能の概要」(55ページ)
- 「エージェントレス監視環境について」(56ページ)
- 「モニタの権限と資格情報」(59ページ)

SiteScope 監視機能の概要

本項では，SiteScope のエージェントレス監視の概念について説明します。エージェントレス監視では，監視対象のサーバ上にエージェント・ソフトウェアをデプロイすることなく監視を行うことができます。このため，SiteScope のデプロイメントと保守は，ほかのパフォーマンス / 運用監視ソリューションに比べてかなり簡単です。エージェント・ベースの監視方法とは異なり，SiteScope では次の方法によって総所有コストを削減しています。

- インフラストラクチャの各コンポーネントの詳細なパフォーマンス・データの収集
- 実運用システムで監視エージェントを実行するための余分なメモリまたは CPU の能力が不要
- すべての監視コンポーネントを中央のサーバに集約することによる保守時間および保守費用の削減
- 監視エージェントを更新するための実運用システムのオフライン化が不要
- ほかのエージェントと共存するための監視エージェントのチューニングが不要
- 実運用中のサーバへの物理的なアクセスやソフトウェア配布操作を待つ必要がなくなることによる，インストール時間の短縮化
- 不安定なエージェントが引き起こす実運用サーバでのシステム・ダウンタイムの可能性の減少

SiteScope は，多様なモニタ・タイプを備えた多機能な運用監視ソリューションであり，システムやサービスをさまざまなレベルで監視できます。モニタ・タイプの多くは，特殊な環境に合わせてさらにカスタマイズできます。

企業や組織は複数のソリューションを頻繁にデプロイメント，保守して，その運用や可用性をさまざまなレベルで監視しなければなりません。運用の監視は，次の表で説明するように，いくつかのレベルまたは層に分類できます。

モニタ・タイプ	説明
サーバの状態	CPU 利用率，メモリ，格納領域，主要なプロセスやサービスのステータスなど，サーバ・マシンのリソースを監視
Web プロセスとコンテンツ	主要な URL の可用性，主要な Web ベースのプロセスの機能，および主要なテキスト・コンテンツを監視

モニタ・タイプ	説明
アプリケーション・パフォーマンス	Web サーバ，データベース，その他のアプリケーション・サーバなどの，ミッション・クリティカルなアプリケーションのパフォーマンス統計情報を監視
ネットワーク	サービスの接続性と可用性を監視

エージェントレス監視環境について

大半の SiteScope 監視は，ネットワーク環境でサーバやアプリケーションに要求を行う，Web またはネットワーク・クライアントをエミュレートすることにより実行されます。このため，SiteScope はネットワーク全体にわたって，サーバ，システム，およびアプリケーションにアクセスできなければなりません。

本項の内容

- 「SiteScope の監視の方法」(56ページ)
- 「ファイアウォールと SiteScope のデプロイメント」(58ページ)

SiteScope の監視の方法

システム，サーバ，およびアプリケーションを監視するために SiteScope が使用する方法は，次の 2 つのカテゴリに分類できます。

- **標準ベースのネットワーク・プロトコル**

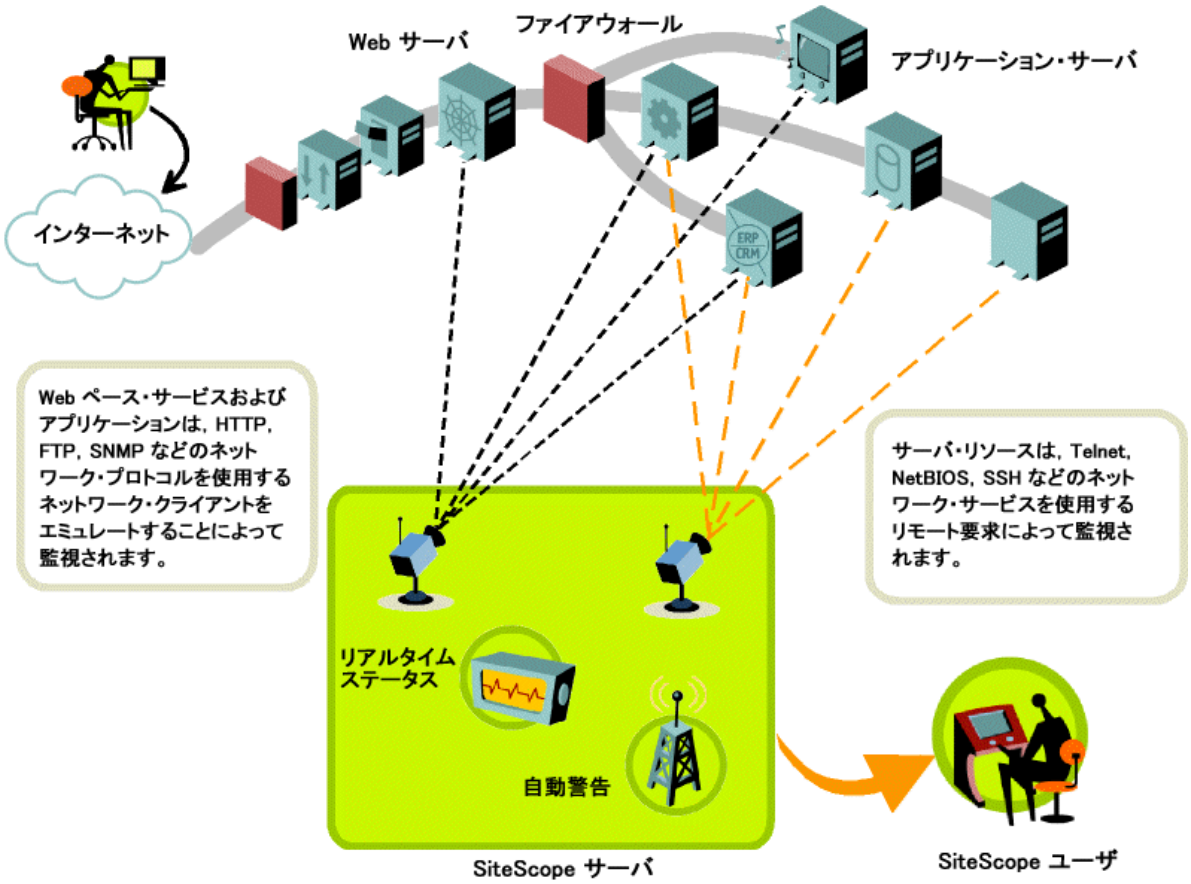
  このカテゴリには，HTTP，HTTPS，FTP，SMTP，SNMP，および UDP を使用した監視が含まれます。これらのタイプのモニタは一般に，SiteScope が稼働しているプラットフォームやオペレーティング・システムとは独立しています。たとえば，Linux にインストールされた SiteScope は，Windows，HP-UX，Solaris を実行しているサーバ上の Web ページ，ファイルのダウンロード，電子メールの送信，SNMP データを監視できます。

- **プラットフォーム固有のネットワーク・サービスおよびネットワーク・コマンド**

  このカテゴリには，クライアントとしてリモート・マシンにログインして情報を要求するモニタ・タイプが含まれます。たとえば，SiteScope は Telnet または SSH を使用してリモート・サーバにログインし，ディスク領域，メモリ，またはプロセスに関する情報を要求できます。Microsoft Windows プラットフォームでは，SiteScope は Windows パフォーマンス・カウンタ・ライブラリも利用します。プラットフォーム固有のサービスを利用するモニタ・タイプの場合，異なるオペレーティング・システム間の監視には，いくつかの制限があります。

  次の図に，SiteScope によるエージェントレス監視の概要を示します。SiteScope は，リモート・

マシン上のサービスに，パフォーマンスと可用性に関するデータを収集するよう依頼します。



SiteScope サーバ・モニタ（たとえば，CPU，ディスク領域，メモリ，サービス）は，次のプラットフォーム上でサーバ・リソースを監視できます。Windows，AIX，CentOS，FreeBSD，HP iLO，HP-UX，HP/UX，HP/UX 64 ビット，Linux，MacOSX，NonStopOS，OPENSERVER，Red Hat Enterprise Linux，SCO，SGI Irix，Solaris Zones，Sun Fire X64 ILOM，Sun Solaris，SunOS，Tru64 5.x，Tru64 4.x 以前（Digital），Ubuntu Linux。

注: Linux で実行されている SiteScope から Windows マシン上のサーバ・リソース（CPU 利用率，メモリなど）を監視するには，SSH 接続が必要です。この方法で監視する各 Windows マシンには，セキュア・シェル・サーバをインストールする必要があります。この機能を有効にする方法の詳細については，SiteScope ヘルプの「SiteScope の使用」にある「セキュア・シェル（SSH）を使用した SiteScope の監視」セクションを参照してください。

SiteScope にはアダプタ設定テンプレートが用意されており，これにより UNIX オペレーティング・システムのその他のバージョンを監視するように SiteScope の機能を拡張できます。詳細については，SiteScope ヘルプの「UNIX オペレーティング・システム・アダプタ」を参照してください。

SiteScope によってリモートからシステム・データにアクセスされる各サーバでは，ログイン・アカウントを有効にしておく必要があります。監視対象のサーバのログイン・アカウントは，SiteScope がインストールされ実行されているアカウントに合わせて設定する必要があります。たとえば，

SiteScope が **sitescope** というユーザ名のアカウントで実行されている場合，この SiteScope インストール環境によって監視されるサーバ上のリモート・ログイン・アカウントには，**sitescope** ユーザ用に設定されたユーザ・ログイン・アカウントが必要です。

ファイアウォールと SiteScope のデプロイメント

ファイアウォール越しにサーバを監視するには，サーバの監視に異なるプロトコルとポートが必要となります。そのため，セキュリティ上の理由から，SiteScope を使用しないことをお勧めします。SiteScope のライセンスは，ファイアウォールの両側にある別々の SiteScope をサポートします。HTTP または HTTPS 経由で，1 台のワークステーションから 2 つ以上の SiteScope にアクセスできます。

次の表に，標準的な監視環境で SiteScope が監視および警告発行のために一般的に使用するポートの一覧を示します。

SiteScope 関数：	**使用される標準ポート**
SiteScope Web サーバ	ポート 8080
SiteScope レポート	ポート 8888
FTP モニタ	ポート 21
メール・モニタ	ポート 25（SMTP），110（POP3），143（IMAP）
ニュース・モニタ	ポート 119
Ping モニタ	ICMP パケット
SNMP モニタ	ポート 161（UDP）
URL モニタ	ポート 80,443
リモート Windows 監視	ポート 139
電子メール警告	ポート 25
Post 警告	ポート 80,443
SNMP トラップ警告	ポート 162（UDP）
リモート UNIX ssh	ポート 22
リモート UNIX Telnet	ポート 23
リモート UNIX rlogin	ポート 513

モニタの権限と資格情報

各モニタにアクセスするには，ユーザ権限と資格情報が必要となります。必要な権限と資格情報，および各モニタで使用される対応プロトコルの詳細については，SiteScope ヘルプにある『モニタ・リファレンス ・ガイド』の「モニタの権限と資格情報」セクションを参照してください。

第2部: SiteScope をインストールする前に

第8章: インストールの概要

SiteScope は，単一サーバとしてインストールされます。Windows プラットフォームでは単一アプリケーションとして，Linux プラットフォームでは単一アプリケーションまたはさまざまなプロセスとして実行されます。

監視環境のデプロイメントおよび管理を容易にするために，SiteScope をインストールする前に考慮する計画の手順とアクションがいくつかあります。

SiteScope アプリケーションのデプロイメントに関する手順の概要を次に示します。

1. **SiteScope アプリケーションをインストールして実行するサーバを準備します。**

   注:

   - 1 台のマシンに複数の SiteScope をインストールしないでください。
   - SiteScope サーバの障害に備え，SiteScope Failover を使用して可用性のバックアップ監視を提供する場合は，**<SiteScope ルート・ディレクト >\sisdocs\pdfs\SiteScopeFailover.pdf** にある『HP SiteScope Failover Guide』を参照してください。

2. **SiteScope のインストール実行ファイルを入手します。**

   詳細については，「インストールの流れ」(86ページ)を参照してください。

3. **アプリケーションをインストールするディレクトリを作成し，必要に応じてユーザ権限を設定します。**

   注: SiteScope 11.30 をインストールするには，新しいディレクトリを作成する必要があります。以前のバージョンの SiteScope に使用しているディレクトリにバージョン 11.30 をインストールしないでください。

4. **SiteScope のインストール実行ファイルを実行するか，または準備した場所にアプリケーションをインストールするようスクリプトに指定してインストール・スクリプトを実行します。**

   詳細については，「インストールの流れ」(86ページ)を参照してください。

5. **必要に応じて，サーバを再起動します（Windows へのインストールの場合のみ）。**

6. **互換性のある Web ブラウザを使用して SiteScope に接続し，SiteScope が実行されることを確認します。**

   詳細については，「作業の開始と SiteScope へのアクセス」(191ページ)を参照してください。

7. **インストール後の手順を実行し，SiteScope を実運用で使用する準備を整えます。**

   詳細については，「インストール後の管理」(192ページ)を参照してください。

第9章: インストール要件

本章の内容

- 「システム要件」(62ページ)
- 「SiteScope の容量に関する制限事項」(67ページ)
- 「SiteScope サポート・マトリックス」(67ページ)

システム要件

本項では，サポートされているオペレーティング・システム別に，SiteScope を実行するための最小システム要件と推奨事項を示します。

注:
- SiteScope を 32 ビットの Windows または Linux オペレーティング・システムにインストールする，または SiteScope を 32 ビット・アプリケーションとして 64 ビットの Windows オペレーティング・システムにインストールすることは，サポートされなくなりました。SiteScope は，64 ビット・アプリケーションとしてのみインストールおよび実行が可能です。
- Solaris プラットフォームでの SiteScope の実行は廃止されたため，Solaris インストーラは提供されなくなりました。
- 異なる環境に SiteScope をインストールする場合のトラブルシューティングや制限事項については，「トラブルシューティングおよび制限事項」(93ページ)を参照してください。

本項の内容

- 「システムのハードウェア要件」(62ページ)
- 「Windows の場合のサーバ・システム要件」(64ページ)
- 「Linux のサーバ・システム要件」(64ページ)
- 「クライアントのシステム要件」(65ページ)

システムのハードウェア要件

ハードウェア要件の仕様 :

コンピュータおよびプロセッサ	1 コア/2000 MHz 以上
メモリ	2 GB 以上 高負荷環境の場合，一般的には 8 GB ~ 16 GB
ハード・ディスクの空き容量	10 GB 以上

ネットワーク・カード	物理ギガビット・ネットワーク・インタフェース・カード × 1（最低）

仮想化要件の仕様 :

- サポート対象のすべてのオペレーティング・システムで，VMware 仮想マシンと Hyper-V 仮想マシンの使用がサポートされます（「Windows の場合のサーバ・システム要件」(64ページ)，「Linux のサーバ・システム要件」(64ページ)を参照してください）。
- パフォーマンスと安定性を向上させるには（特に，高負荷 SiteScope 環境の場合），物理ハードウェアを使用することをお勧めします。
- VMware の場合は，ゲスト・オペレーティング・システムに VMware Tools をインストールする必要があります。

認定されている構成

次の構成は，BSM と統合された SiteScope のインストールのための高負荷環境で認定されています。

オペレーティング・システム	Microsoft Windows Server 2012 R2（64 ビット）
システム・タイプ	ACPI マルチプロセッサ x64 ベースの PC
CPU	Intel Xeon（R）x5650 物理プロセッサ × 4（各 2.67 GHz）
合計物理メモリ（RAM）	16 GB
Java ヒープ・メモリ	8192 MB
モニタの総数	24,000
リモート・サーバの総数	2,500
1 分間のモニタ実行数	3,500

注:

- モニタの容量と速度は，以下を始めとするさまざまな要因に大きく影響される可能性があります。SiteScope サーバ・ハードウェア，オペレーティング・システム，パッチ，サードパーティ製のソフトウェア，ネットワーク設定およびアーキテクチャ，監視対象サーバの位置に対する SiteScope サーバの位置，リモート接続プロトコルの種類，モニタの種類と種類ごとの分布，監視頻度，監視実行時間，Business Service Management 統合，およびデータベースのログ記録。
- 高負荷下で作業している場合は，初めて BSM に接続する前に全モニタを一時停止してください。

Windows の場合のサーバ・システム要件

認定されている Microsoft Windows オペレーティング・システムのバージョンを次に示します。

- Microsoft Windows Server 2008 R2 SP1 Standard/Enterprise/Datacenter Edition（64 ビット）
- Microsoft Windows Server 2012 Standard/Datacenter Edition（64 ビット）
- Microsoft Windows Server 2012 R2 Standard Edition（64 ビット）

Linux のサーバ・システム要件

認定されている Linux オペレーティング・システムのバージョンを次に示します。

- Oracle Enterprise Linux（OEL）6.0-6.5（64 ビット）
- CentOS 6.2（64 ビット）
- Red Hat ES/AS Linux 5.5-5.8，6.0-6.5（6.0，6.2，6.4，6.5 が認定済み）（64 ビット）

注:

- OEL 環境と CentOS 環境を手動で設定してから SiteScope をインストールする必要があります。詳細については，「Oracle Enterprise Linux 環境への SiteScope のインストール」(90ページ)および「CentOS 6.2 環境への SiteScope のインストール」(91ページ)を参照してください。
- SiteScope を HPOM または BSM と統合する場合は，HP Operations Agent をインストールする前に Red Hat ES Linux 6.0（64 ビット）環境の依存関係を設定する必要があります（エージェントは，HPOM または BSM にイベントを送信し，メトリクス・データを保存するために必要です）。エージェントの依存関係とインストールの設定の詳細については，SiteScope ヘルプまたは HP ソフトウェア統合サイトにある『HP Operations Manager 製品との統合』ガイドを参照してください。
- SiteScope が Red Hat Linux にインストールされると，SiteScope サーバの状況モニタには SwapIns/sec，SwapOuts/sec，PageIns/sec，PageOuts/sec カウンタに対する sar -W コマンドと sar -B コマンドの有効な出力が必要です。これらのコマンドが動作しない場合，は表示されず，これらのカウンタが **n/a** として表示されます。これらのコマンドを実行できるようにするには，1 日に一度実行するコマンド "**/usr/local/lib/sa/sadc -**" を追加して crontab を編集します。
- Red Hat Linux 環境で実行する SiteScope サーバまたはリモート・サーバ上での CPU およびメモリの使用率を監視できるようにするには，**sysstat** パッケージを SiteScope サーバおよび監視中のすべてのリモート・サーバにインストールする必要があります（同梱されていません）。
- NPTL（Native POSIX Threading Library）搭載の Red Hat Linux 9 は，サポートされません。
- Linux の SiteScope で特定のレポート要素を表示するには，SiteScope を実行しているサーバで X Window システムがインストールされ，稼働している必要があります。

クライアントのシステム要件

SiteScope クライアントは，次を使用しているすべての Microsoft Windows オペレーティング・システムでサポートされています。

サポートされているブラウザ: SiteScope UI	• Microsoft Internet Explorer 9，10，11 **Internet Explorer 10 の注記事項：** • 警告レポート，モニタ・レポート，サーバ中心のレポートは，互換性モードが［**ドキュメント モード: Quirks**］の場合にのみサポートされます。標準設定の［**ドキュメント モード: IE5 Quirks**］はサポートされません。**quirks** モードを有効にするには，警告，モニタ，またはサーバ中心のレポートを開き，F12 を押します。開発者ツールで，**［ドキュメント モード］ > ［Quirks］**を選択します。 • Internet Explorer 10 が［開始］画面から使用されている場合，Java などのアドオンに対するサポートはありません。SiteScope を Internet Explorer 10 で使用するには，Internet Explorer デスクトップ・モードに切り替えて java をインストールする必要があります。詳細については，http://windows.microsoft.com/en-us/internet-explorer/install-java#ie=ie-10 を参照してください。 • Mozilla Firefox（最新認定バージョン）:31.2.0 ESR • Safari 8.0，Mac OS（10.10 Yosemite） **前提条件：** • ブラウザがサードパーティの cookie を受け入れて、セッション・クッキーを許可するように設定する必要があります。 • ブラウザで JavaScript の実行が有効になるよう設定する必要があります。 • ブラウザが SiteScope アプリケーションからのポップアップを許可している必要があります。 • （Safari の場合のみ）Java プラグインは **［環境設定］ > ［セキュリティ］ > ［Web サイト設定を管理］**で，［**安全でないモードで実行**］を個別の Web サイト（SiteScope ホスト）またはすべてのサイトに対して設定する必要があります。
サポートされているブラウザ: 統合コンソール（Multi-View，イベント・コンソール）	• Google Chrome（最新認定バージョン）: 34.0.1847.137 m • Mozilla Firefox（最新認定バージョン）:31.2.0 ESR • Safari（最新認定バージョン）:8.0 for Mac • Internet Explorer 9, 10, 11 **注：** Internet Explorer 9 はサポートされますが，下記のような制限があります。

	• Microsoft Windows 7 N Edition ではサポートされません。 • Microsoft Windows Server 2008 ではサポートされません。 • Safari が搭載された iPad 3（最新のアップデートが搭載された iOS 7） • Chrome 34.0.1847 が搭載された Android タブレット（フル HD 表示）
サポートされているブラウザ：MyBSM の SiteScope Multi-View ページ	• Internet Explorer 9, 10, 11 **注：** Internet Explorer 8 を使用して MyBSM の Multi-View ページにアクセスすることはできますが，この操作は正式にはサポートされなくなりました。Internet Explorer 8 ではイベント・コンソールと，統合コンソールのタブの機能が動作しないため，サポート対象のブラウザのいずれかに切り替えることをお勧めします。
Java プラグイン（SiteScope ユーザ・インタフェースを開くために必要）	• **サポート：** JRE バージョン 6 または 7（JRE 7 update 67 が最新の認定バージョン） • **推奨：** JRE 7（SiteScope の次のリリースで JRE バージョン 6 のサポートが廃止される予定です） **ヒント：** Java は SiteScope インストールの一部としてインストールされており，別個にパッチを適用したり更新しないようにしてください。Java のバージョンは **<SiteScope インストール・ディレクトリ>\java\bin** に移動して，次のコマンド・ラインを実行することによって確認できます。 java -server -fullversion

SiteScope の容量に関する制限事項

- SiteScope が BSM と統合されている場合に，負荷が非常に高い処理を実行すると，SiteScope に問題が発生することがあります。次のガイドラインに従ってください。
  - 3,000 を超えるモニタにテンプレート変更適用ウィザードを一度に実行しないでください。
  - モニタ・デプロイメント・ウィザードを実行して，3,000 を超えるモニタを一度に作成しないでください。
  - 1 回の操作で 3,000 を超えるモニタのコピーおよび貼り付けを実行しないでください。
  - グローバル検索と置換を実行して，2,500 を超えるモニタの Business Service Management 統合プロパティを一度に変更しないでください。
- SSH 接続を使用するモニタを 1000 個以上作成することはお勧めできません（モニタの実行頻度，接続数などに標準設定のパラメータ設定を使用した場合）。SSH を使用するモニタを 1000 個以上実行する必要がある場合は，SiteScope サーバを 1 台追加してください。

ヒント: SiteScope には，システムの動作を予測し，SiteScope のキャパシティ・プランニングを実行するためのツールが備わっています。詳細については，「SiteScope キャパシティ・カリキュレータ」(45ページ)を参照してください。

SiteScope サポート・マトリックス

本項の内容

- 「HP Business Service Management 統合サポート・マトリックス」(67ページ)
- 「HP Operations Manager（HPOM）統合サポート・マトリックス」(68ページ)
- 「HP Operations Agent サポート・マトリックス」(69ページ)
- 「負荷テストのための HP SiteScope のサポート・マトリックス」(69ページ)
- 「HP Network Node Manager i（NNMi）サポート・マトリックス」(70ページ)

注: SiteScope 11.30 とほかの製品との共存については，テストされておらず，認定もされていません。そのようなデプロイメントはサポート対象外であり，お勧めできません。

HP Business Service Management 統合サポート・マトリックス

HP SiteScope バージョン	HP Business Service Management バージョン

	9.25	9.2x	9.1x	9.0x	8.x
SiteScope 11.3x	√ （推奨）	√	√	√	√

HP Operations Manager（HPOM）統合サポート・マトリックス

最新の認定サービス・パックを含んでいる，サポート・マトリックスの最新のバージョンについては，HP 統合サイトを確認してください。
(http://support.openview.hp.com/sc/solutions/index.jsp#tab=tab3）。

HPOM バージョン	**SiteScope 11.3x 統合**			
	イベント統合	**ノード・ディスカバリ統合**	**モニタ・ディスカバリ統合**	**テンプレート統合**
HPOM for Windows 8.1x（パッチ OMW_00149）	サポート	サポート	サポート	サポートされていません
HPOM for Windows 9.0	サポート	パッチ OMW_00097/98 以降でサポート（32 ビット/64 ビット）	サポート	パッチ 159 でサポート
HPOM for Linux/Solaris 9.0	サポート	サポートされていません	サポート	サポート
HPOM for Linux/Solaris 9.10	サポート	パッチ 9.10.200 以降でサポート	サポート	パッチ 9.10.210 およびホットフィックス QCCR1A125751，または 9.10.210 以降のパッチでサポート
HPOM for Linux/Solaris 9.20	サポート	サポート	サポート	サポート

注: HP Operations Manager のハードウェアとソフトウェア設定要件については，HP ソフトウェア・サポート・サイトで該当するバージョンの Operations Manager for Windows/UNIX のインストール・ガイドを参照してください。

HP Operations Agent サポート・マトリックス

HP SiteScope バージョン	HP Operations Agent バージョン
11.0x	8.60.70
11.1x	8.60.501
11.20 - 11.22	11.02.011
11.23	11.02.011, 11.13*
11.24	11.02.011, 11.13**, 11.14**
11.30	11.14***
*インストール済みの HP Operations Agent 11.02 の認定バージョンへのアップグレードとしてサポートされます。 **HP Operations Agent は別途インストールされ，SiteScope 設定ツールを使用して設定される必要があります。 ***HP Operations Agent は SiteScope インストーラまたは SiteScope 設定ツールに含まれなくなりました。代わりに，エージェントを手動でインストールして，設定する必要があります。詳細については，SiteScope ヘルプまたは HP ソフトウェア統合サイトにある『HP Operations Manager 製品との統合』ガイドを参照してください。	

注:

- HP Operations Agent のインストールには Microsoft Installer 4.5 以降が必要です。
- HP Operations Agent のインストール要件の詳細については，HP ソフトウェア・サポート・サイトから入手できる『HP Operations Agent 11.14 インストール・ガイド』を参照してください。

負荷テストのための HP SiteScope のサポート・マトリックス

本リリースでサポートされている LoadRunner と Performance Center のバージョンの一覧については，次の HP 統合サイトを参照してください。

- HP Performance Center :http://support.openview.hp.com/sc/solutions/integrations.jsp?intid=599
- HP LoadRunner :http://support.openview.hp.com/sc/solutions/integrations.jsp?intid=587

注: アクセスには HP Passport ログインが必要です（HP Passport に登録するには，http://h20229.www2.hp.com/passport-registration.html にアクセスしてください）。

HP Network Node Manager i（NNMi）サポート・マトリックス

最新の認定サービス・パックを含んでいる，サポート・マトリックスの最新のバージョンについては，HP 統合サイトを確認してください。
(http://support.openview.hp.com/sc/solutions/index.jsp#tab=tab3）。

統合	対応バージョン
イベント統合	SiteScope バージョン 11.10 以降 NNMi バージョン 9.10 以降（9.21 が最新の認定 NNMi バージョン）
メトリクス統合	SiteScope バージョン 11.10 以降 NNMi バージョン 9.10 以降 NNM iSPI Performance for Metrics バージョン 9.10 以降（9.22 が最新の NNMi 認定バージョン）

第10章: SiteScope のアップグレード

本章の内容

- 「アップグレードを実行する前に」(71ページ)
- 「32 ビットから 64 ビットの SiteScope への移行」(73ページ)
- 「既存の SiteScope インストールのアップグレード」(74ページ)
- 「SiteScope 構成データのバックアップ」(76ページ)
- 「設定データのインポート」(76ページ)
- 「SiteScope 10.x から SiteScope 11.13 または 11.24 へのアップグレード」(76ページ)
- 「SiteScope 11.13 または 11.24 から SiteScope 11.30 へのアップグレード」(78ページ)
- 「トラブルシューティングおよび制限事項」(81ページ)

アップグレードを実行する前に

本項では，お使いのシステムと運用への支障の可能性を最小限に抑えながら，既存の SiteScope インストールを HP SiteScope 11.30 にアップグレードする方法について説明します。

SiteScope は，下位互換性を持つように設計されています。このため，新しいバージョンの SiteScope をインストールし，既存の SiteScope インストールからモニタ設定を転送できます。

SiteScope をアップグレードする前に，次の点を考慮してください。

- SiteScope が，「システム要件」(62ページ) に示されている，サポートされている Windows または Linux 環境にインストールされている必要があります。
- SiteScope が HP Operations Manager または BSM と統合されているときに，SiteScope がイベントを送信したり，測定値データのデータ・ストレージとして動作するようにするには，HP Operations Agent を SiteScope サーバにインストールする必要があります。エージェントのインストールの詳細については，SiteScope ヘルプまたは HP ソフトウェア統合サイトにある『HP Operations Manager 製品との統合』ガイドを参照してください。
- SiteScope 11.13 または 11.24 は，設定ツールを使用して現在の SiteScope 設定データのバックアップを作成し，現在の SiteScope バージョンをアンインストールし，SiteScope 11.30 をインストールし，設定データを SiteScope にインポートして戻すことによって 11.30 にアップグレードできます。アップグレードの詳細については，「既存の SiteScope インストールのアップグレード」(74ページ)を参照してください。
- SiteScope 10.x からアップグレードする場合は，最初に SiteScope 11.13 または 11.24 にアップグレードしてから SiteScope 11.13 または 11.24 を SiteScope 11.30 にアップグレードできます。アップグレードの方法については，「SiteScope 10.x から SiteScope 11.13 または 11.24 へのアップグレード」(76ページ)を参照してください。

注意事項および制限事項

- クロスプラットフォームのアップグレードはサポートされていません。
- SiteScope の Windows 設定を Linux デプロイメントにインポートするときに（NetBIOS または WMI 接続タイプを備えた Windows リモートを追加する場合など），問題が発生する可能性があります。プラットフォーム固有のモニタ設定（WinInet オプションを備えた URL モニタ，Windows リモートでのファイル・モニタ，またはスクリプト・モニタなどの）がないことを確認します。
- 次のモニタは廃止されました。これらのモニタは，SiteScope の以前のバージョンで設定されていた場合，アップグレードの実行後も引き続き SiteScope で表示されます（ただし 32 ビット専用モニタは機能しません）。これらのモニタは SiteScope 11.24 以前のバージョンでサポートされます。

32 ビット専用モニタ（64 ビット環境では実行不可）	**32/64 ビット・モニタ**
• Microsoft Exchange 2003 のメールボックス[1] • Microsoft Exchange 2003 のメールボックス，パブリック・フォルダ[1] • Microsoft Windows Media Player [2] • Real Media Player[2] • Sybase • Tuxedo	• Microsoft Exchange 5.5 のメッセージ・トラフィック[1] • Microsoft Exchange 2000/2003 のメッセージ・トラフィック[1] • Microsoft Windows ダイアルアップ[2]
注意事項： [1] Microsoft Exchange 2007 以降に移行することを推奨します。 [2] 今後のバージョンでも使用できない予定です。	

32 ビットから 64 ビットの SiteScope への移行

SiteScope 11.30 では，64 ビットのオペレーティング・システムおよび 64 ビットの Java バージョンのみがサポートされます。結果として，SiteScope 32 ビットのインストーラおよび 64 ビットでの SiteScope 32 ビットのインストーラは SiteScope 11.30 では提供されなくなりました。

SiteScope 11.30 から，Web Script モニタは 64 ビットでサポートされています。モニタを使用するには，HP Load Generator 12.02 を SiteScope サーバにインストールし，Load Generator へのパスを指定する必要があります。詳細については，『SiteScope モニタ・リファレンス ・ガイド』の「Web スクリプト・モニタ」セクションを参照してください

他の 32 ビット・モニタは廃止されるため，SiteScope 11.13 または 11.24 を SiteScope 11.30 にアップグレードした後は機能しなくなります。影響があるモニタ，推奨される代替モニタのリスト，およびより詳細な情報については，「アップグレードを実行する前に」(71ページ)の「注意事項および制限事項」セクションを参照してください。

SiteScope 10.x（32 ビット・バージョン）から SiteScope 11.30（64 ビット・バージョン）にアップグレードするには，次の手順を実行します。

1. 「SiteScope 10.x から SiteScope 11.13 または 11.24 へのアップグレード」(76ページ)の手順を実行します。
2. 「SiteScope 11.13 または 11.24 から SiteScope 11.30 へのアップグレード」(78ページ) の手順を実行します（手順 5 で，必ず SiteScope を 64 ビット・マシンにインストールします)。

既存の SiteScope インストールのアップグレード

注: このトピックには，現在のバージョンの SiteScope を SiteScope 11.30 にアップグレードする手順が記載されています。SiteScope をインストールして，アップグレードを実行しない場合は，「インストール・ワークフロー」(85ページ)を参照してください。

ご使用のバージョンの SiteScope をアップグレードする場合は，次の手順を実行することをお勧めします。

1. **SiteScope プロセス/サービスが停止していることを確認します（インストール前にインストーラがプロセスを自動的に停止します）。**

   詳細については，「Windows プラットフォームでの SiteScope サービスの開始と停止」(197ページ)または「Linux プラットフォームでの SiteScope プロセスの開始と停止」(198ページ)を参照してください。

2. **現在のバージョンの SiteScope の設定ツールを使用して SiteScope モニタ設定データのバックアップ・コピーを作成します。**

   設定ツールを使用して，現在の SiteScope インストール・ディレクトリのバックアップを作成します。この作業は，現在ご使用の SiteScope から SiteScope データをエクスポートすることにより行えます。エクスポートしたデータは，後で SiteScope にインポートして使用します。詳細については，「SiteScope 構成データのバックアップ」(76ページ)を参照してください。

3. **現在のバージョンの SiteScope をアンインストールした後，SiteScope 11.30 をインストールします。**

   SiteScope のアンインストールの詳細については，「SiteScope のアンインストール」(144ページ)を参照してください。

   SiteScope 11.30 は，クリーンなディレクトリ構造にインストールします。SiteScope をインストールするために作成する新規ディレクトリは，SiteScope という名前にしてください。SiteScope 11.30 のインストールの詳細については，「インストールの流れ」(86ページ)を参照してください。

4. **新しい SiteScope ライセンスをインポートします。**

   SiteScope の以前のバージョンから SiteScope 11.30 にアップグレードするには，HP サポート更新担当者に連絡して，まず製品契約の移行を依頼します。契約の移行が完了したら，［マイ ソフトウェア アップデート］ポータル（https://h20575.www2.hp.com/usbportal/softwareupdate.do）に移動し，［**Get Licensing**］（ライセンスの取得）タブをクリックして新しいライセンス・キーを取得します。

   ライセンス・キーを受け取ったら，SiteScope を開き，［**プリファレンス**］＞［**一般プリファレンス**］を選択し，［**ライセンス**］パネルを展開します。新しいライセンス・ファイルをインポートします。SiteScope が機能し始めます。

   注: ライセンスの購入に関する問い合わせについては（または追加の容量が必要な場合），HP の営業担当に問い合わせるか，HP SiteScope 製品ページの「問い合わせ」リンクを使用

してください。

5. **HP Operations Agent をインストールして設定します（SiteScope を HPOM または BSM に統合する場合に必要です）。**

   エージェントのインストールと設定の詳細については，SiteScope ヘルプまたは HP ソフトウェア統合サイトにある『HP Operations Manager 製品との統合』ガイドを参照してください。

6. **Microsoft ホットフィックスをインストールします。**

   SiteScope の拡張性およびパフォーマンスを向上させるため，Microsoft ホットフィックスをインストールすることをお勧めします。詳細については，「Microsoft ホットフィックスのインストール」(195ページ)を参照してください。

7. **モニタ設定データをインポートします。**

   インストール後に設定ツールを使用して，（手順 2 の）モニタ設定データをインポートします。詳細については，「設定データのインポート」(76ページ)を参照してください。

8. **（任意）以前のバージョンの SiteScope からデータをインポートした後，バッチ・ファイルまたは start コマンド・シェル・スクリプトを実行して SiteScope を起動します。**

   モニタが実行するまでの時間が 15 分を超える場合に，アップグレード後 SiteScope 自身が再起動されないようにするには，**<SiteScope ルート・ディレクトリ>\bin** ディレクトリから **go.bat** ファイルを実行するか（Windows プラットフォーム），<installpath>/SiteScope/start 構文を使用して start コマンド・シェル・スクリプトを実行し（Linux プラットフォーム），SiteScope を起動します。

9. **SiteScope Failover を使用する場合は，対応する SiteScope Failover バージョンでフェイルオーバー・サーバをアップグレードしてください。**

   プライマリ・サーバをアップグレードした後，対応する SiteScope Failover バージョンでフェイルオーバー・サーバをアップグレードして，フェイルオーバー・サーバをアップグレードしたプライマリ・サーバに接続します。詳細については，『SiteScope Failover Guide』の「Upgrading SiteScope Failover」セクションを参照してください。

SiteScope 構成データのバックアップ

SiteScope のアップグレードに備える最も簡単な方法は，設定ツールを使用して現在の SiteScope のインストール・ディレクトリと必要なそのサブディレクトリをすべてバックアップすることです。設定ツールを使用して，後で SiteScope にインポートするために，現在の SiteScope からテンプレート，ログ，モニタ設定ファイル，サーバ証明書，スクリプトなどの SiteScope データをエクスポートできます。ユーザ・データが **.zip** ファイルにエクスポートされます。

または，SiteScope インストールを手動でバックアップできます。詳細については，「SiteScope を起動できない場合に SiteScope インストールのバックアップとリカバリを行う」(202ページ)を参照してください。

注: SiteScope データのエクスポート時に **<SiteScope>\htdocs** ディレクトリはコピーされないため，このディレクトリのバックアップを作成して，アップグレード後に SiteScope 11.30 ディレクトリにコピーして，古いレポートを参照できるようにする必要があります。

設定ツールを使用して SiteScope データをエクスポートする方法の詳細については，「SiteScope 設定ツールの使用」(124ページ)を参照してください。

または，インストール・プロセスの一部として SiteScope データをエクスポートできます。詳細については，「インストール・ワークフロー」(85ページ)を参照してください。

設定データのインポート

SiteScope のアップグレード後，設定ツールを使用して，以前のバージョンの SiteScope からモニタ設定データをコピーできます。詳細については，「SiteScope 設定ツールの使用」(124ページ)を参照してください。

または，手動でバックアップを作成した場合は，新しいインストール・ディレクトリからバックアップしたすべてのフォルダとファイルを削除して，バックアップしたフォルダとファイルをインストール・ディレクトリにコピーする必要があります。詳細については，「SiteScope を起動できない場合に SiteScope インストールのバックアップとリカバリを行う」(202ページ)を参照してください。

SiteScope 10.x から SiteScope 11.13 または 11.24 へのアップグレード

SiteScope では SiteScope 10.x から 11.30 への直接のアップグレードがサポートされていないので，最初に SiteScope 11.13 または 11.24 にアップグレードしてから SiteScope 11.30 にアップグレードする必要があります。

注: SiteScope 10.x バージョンは，SiteScope 11.13 または 11.24 にアップグレードする前に SiteScope 10.14 にアップグレードすることをお勧めします。

アップグレードを実行するには，次の手順で行います。

1. SiteScope サービスを停止します。
2. SiteScope 10.x から SiteScope 設定をエクスポートします（SiteScope 10.14 にアップグレードしてから実行することをお勧めします）。
   a. SiteScope 10.x フォルダをバックアップします（システムの一時フォルダにコピーします）。
   b. 次の手順で SiteScope 設定をエクスポートします。
      - SiteScope 設定ツールを起動して（［**スタート**］ > ［**プログラム**］ > ［**HP SiteScope**］ > ［**設定ツール**］），［**次へ**］をクリックします。
      - ［**設定のインポート**］/［**設定のエクスポート**］を選択し，［**次へ**］をクリックします。
      - ［**設定のエクスポート**］を選択し，［**次へ**］をクリックします。
      - SiteScope 10.x インストール・ディレクトリおよびエクスポートしたデータを保存するターゲット・ディレクトリの場所を選択します。バックアップ・ファイル名を入力します。古いデータのレポートを生成する場合は，［**ログ ファイルを含める**］を選択します。
      - エクスポートが完了した後，**［次へ］/［完了］**をクリックします。
      - さまざまなモニタで使用されるサードパーティ製のライブラリと jar（SAP クライアント，JDBC ドライバなど）を一時ディレクトリにコピーします。これらのファイルはエクスポートに含まれていないからです。
3. SiteScope 10.x をアンインストールします。
   a. ［**スタート**］ > ［**設定**］ > ［**コントロール パネル**］ > ［**プログラムの追加と削除**］を選択します。
   b. アンインストール・ウィンドウを起動します。［**次へ**］を 2 回クリックしてアンインストールが開始します。
   c. アンインストールが完了した後，［**完了**］をクリックします。
   d. SiteScope ディレクトリの下にある残りのファイルをすべて削除します。
   e. ［**SiteScope**］サービスがアンインストールで Windows サービスから削除されたことを確認します。［SiteScope］サービスがまだ表示される場合は，コマンド・プロンプトから sc delete SiteScope を実行して手動で削除できます。
   f. サーバを再起動します。
4. SiteScope 11.10 または 11.20 をインストールした後，HP ソフトウェア・サポート・サイトの［**ソフトウェア パッチ**］セクションから最新のマイナー・マイナー・バージョン（11.13 または 11.24）をインストールします。
5. 次の手順で SiteScope 11.13 または 11.24 にデータをインポートします。
   - 設定ツールを実行し（［**スタート**］ > ［**プログラム**］ > ［**HP SiteScope**］ > ［**設定ツール**］），［**次へ**］をクリックします。
   - ［**設定のインポート**］を選択し，［**次へ**］をクリックします。

- ［**次へ**］をクリックします。
- 10.x のインストールから以前にエクスポートされた **.zip** ファイルを選択し，ターゲット・ディレクトリが正しいことを確認して［**次へ**］をクリックします。
- インポートが完了した後，［**完了**］をクリックします（設定ツールが閉じます）。

注: 設定ツールを再度実行し，［**サイズ変更**］オプションを選択します。

- 以前生成したレポートを使用する場合は，既存の **<SiteScope>\htdoc** フォルダを **\htdocs** フォルダで置き換えます。**\htdocs** フォルダは，手順 2a で以前の SiteScope からバックアップしたフォルダです。

6. SiteScope 10.x の設定を使用して，SiteScope 11.13 または 11.24 を起動します。SiteScope で設定がアップグレードされます。
7. 「SiteScope 11.13 または 11.24 から SiteScope 11.30 へのアップグレード」(78ページ)の手順に進みます。

SiteScope 11.13 または 11.24 から SiteScope 11.30 へのアップグレード

SiteScope 11.13 または 11.24 から SiteScope 11.30 にアップグレードするには，次の手順を実行することをお勧めします。

アップグレードを実行するには，次の手順で行います。

1. SiteScope サービスを停止します。
2. SiteScope 11.13 または 11.24 フォルダをバックアップします（システムの一時フォルダにコピーします）。
3. SiteScope 11.13 または 11.24 から SiteScope 設定をエクスポートします。
   - SiteScope 設定ツールを起動して（［**スタート**］ > ［**プログラム**］ > ［**HP SiteScope**］ > ［**設定ツール**］），［**次へ**］をクリックします。
   - ［**設定のエクスポート**］を選択し，［**次へ**］をクリックします。
   - ［設定のエクスポート］画面で，SiteScope 11.13 または 11.24 のインストール・ディレクトリおよびエクスポートしたデータを保存するターゲット・ディレクトリの場所を選択します。バックアップ・ファイル名を入力します。古いデータのレポートを生成する場合は，［**ログ ファイルを含める**］を選択します。
   - エクスポートが完了した後，**［次へ］/［完了］**をクリックします。
   - さまざまなモニタで使用されるサードパーティ製のライブラリと jar（SAP クライアント，

JDBC ドライバなど）を一時ディレクトリにコピーします。これらのファイルはエクスポートに含まれていないからです。

4. SiteScope 11.13 または 11.24 をアンインストールします（［**スタート**］ > ［**設定**］ > ［**コントロール パネル**］ > ［**プログラムの追加と削除**］）。
   a. アンインストール・ウィンドウを起動します。［**次へ**］を 2 回クリックしてアンインストールが開始します。
   b. アンインストールが完了した後，［**完了**］をクリックします。
   c. SiteScope ディレクトリ下の残りのファイルをすべて削除します。
   d. ［**SiteScope**］サービスがアンインストールで Windows サービスから削除されたことを確認します。［SiteScope］サービスがまだ表示される場合は，コマンド・プロンプトから sc delete SiteScope を実行して手動で削除できます。
   e. サーバを再起動します。
5. SiteScope 11.30 をインストールします。
   a. SiteScope 11.30 インストーラを実行して［**次へ**］をクリックします。
   b. 使用許諾契約に同意して［**次へ**］をクリックします。
   c. SiteScope 11.30 用のディレクトリを選択し，［**次へ**］をクリックします。
   d. ［**HP SiteScope**］インストール タイプを選択し，［**次へ**］をクリックします。
   e. 標準設定のポートはそのままにして，［**次へ**］をクリックします。標準設定のポートが使用されている場合は，代わりに 8088 を入力します。
   f. ライセンスを空白のままにして［**次へ**］をクリックします。
   g. ［サマリ］画面で［**次へ**］をクリックします。
   h. インストールが完了した後，［**次へ**］をクリックします（インストーラ・ウィンドウが閉じます）。
   i. （手順 3 で）一時フォルダにコピーされたサードパーティ製のライブラリと jar を復元します。
   j. SiteScope サービスを停止します。
6. 監視アカウントで実行するように SiteScope サービスを設定します。
7. SiteScope へデータをインポートします。
   - 設定ツールを実行し（［**スタート**］ > ［**プログラム**］ > ［**HP SiteScope**］ > ［**設定ツール**］），［**次へ**］をクリックします。
   - ［**設定のインポート**］を選択し，［**次へ**］をクリックします。
   - ［設定のインポート］画面で，11.13 または 11.24 のインストール環境から以前にエクスポートした zip ファイルを選択し，ターゲット・ディレクトリが正しいことを確認してから［**次へ**］をクリックします。
   - インポートが完了した後，［**完了**］をクリックします（設定ツールが閉じます）。

> **注:** 設定ツールを再度実行し，［**サイズ変更**］オプションを選択します。

- 以前生成したレポートを使用する場合は，既存の **<SiteScope>\htdoc** フォルダを **\htdocs** フォルダで置き換えます。**\htdocs** フォルダは，手順 2 で以前の SiteScope からバックアップしたフォルダです。

8. **master.config** ファイルのデータの減少および他のパラメータを変更します。
   - **< SiteScope ルート > \groups\master.config** ファイルを開きます。
   - 行 **_topazEnforceUseDataReduction=** を **_topazEnforceUseDataReduction=false** に変更します。

     > **注:** このパラメータが存在しない場合は，パラメータを追加して false を設定してください。

   - 行 **_suspendMonitors=** を **_suspendMonitors=true** に変更します。
   - パラメータ **_disableHostDNSResolution=true** を追加します。

     > **注:** すべてのパラメータはアルファベット順になるように追加する必要があります。

   - **master.config** ファイルを保存して閉じます。
9. SiteScope サービスを開始します。SiteScope は設定をアップグレードして，自動的に再起動します。ユーザ・インタフェースを使用してログインして，［**プリファレンス**］ > ［**統合設定**］で BSM への統合が正しいことを確認します。
10. HP サポート更新担当者に連絡して，製品契約の移行を依頼します。契約の移行が完了したら，［マイ ソフトウェア アップデート］ポータル（https://h20575.www2.hp.com/usbportal/softwareupdate.do）に移動し，［**Get Licensing**］（ライセンスの取得）タブをクリックして新しいライセンス・キーを取得します。

    ライセンス・キーを取得したら，SiteScope を開き，［**プリファレンス**］ > ［**一般プリファレンス**］を選択し，［**ライセンス**］パネルを展開して，新しいライセンス・ファイルをインポートします。

    > **注:** ライセンス購入の照会（または追加の容量が必要な場合）については，HP の営業担当にお問い合わせいただくか，HP SiteScope 製品ページの「お問い合わせ」リンクを使用してください。

11. SiteScope を停止します。
12. **master.config** ファイルを開いて，次の手順を実行します。
    - **_suspendMonitors=true** を **_suspendMonitors=** に変更し，モニタの一時停止を解除します。
    - **_topazEnforceUseDataReduction= false** を **_topazEnforceUseDataReduction=** に変更し，データの減少を有効にします。

- パラメータ **_disableHostDNSResolution=false** の値を変更します。
- **master.config** ファイルを保存して閉じ，SiteScope を起動します。

トラブルシューティングおよび制限事項

このセクションでは，SiteScope のアップグレードのトラブルシューティングおよび制限事項について説明します。

- 「アップグレード後の最初の SiteScope の再起動に時間がかかる場合がある」(81ページ)
- 「SiteScope がカスタマ ID を取得できない」(81ページ)
- 「アクション・タイプに応じて標準設定警告アクションの名前が指定される」(82ページ)
- 「BSM/ServiceCenter または Service Manager の統合」(82ページ)
- 「SiteScope をアップグレードできない」(82ページ)
- 「BSM と統合を行う場合の SiteScope の別のサーバへの移動」(82ページ)

注: セルフ・ソルブ技術情報検索でも，SiteScope のアップグレードに関するその他の情報を確認できます。技術情報を利用するには，HP パスポート ID を使ってログオンする必要があります。

アップグレード後の最初の SiteScope の再起動に時間がかかる場合がある

問題 : アップグレード後の最初の SiteScope の再起動に時間がかかる（15 分を超える）場合があります。15 分後モニタが実行を開始しなかった場合，SiteScope は自分自身で再起動します。

考えられる解決策 :

モニタが実行するまでの時間が 15 分を超える場合に，SiteScope 自身が再起動されないようにするには，**<SiteScope ルート・ディレクトリ>\bin** ディレクトリから **go.bat** ファイルを実行するか（Windows プラットフォーム），**<installpath>/SiteScope/start** 構文を使用して start コマンド・シェル・スクリプトを実行し（Linux プラットフォーム），SiteScope を起動します。

稼働していないターゲット環境のすべてのモニタを無効にします。この操作により，システムが応答するまでの待機時間が短縮されます。

SiteScope がカスタマ ID を取得できない

問題 : バージョン 9.0 より前の SiteScope の場合，SiteScope が BSM に接続されると，SiteScope は，**<SiteScope ルート・ディレクトリ>\cache\persistent\TopazConfiguration** の下にある設定ファイルにカスタマ ID を格納します。

9.x にアップグレードした後に初めて SiteScope をロードする場合，SiteScope は，設定ファイルを読み取り，BSM 接続の詳細を取得することを試みます。このファイルが壊れていると（エクスポート設

定が不適切であるためにファイルが壊れる場合があります），SiteScope は，カスタマ ID を取得できない場合があり，そのときは，BSM からカスタマ ID の取得を試みます。再起動中に BSM がダウンすると，SiteScope はカスタマ ID を取得できず，SiteScope 自身で再起動を実行します。

考えられる解決策 : アップグレード後に SiteScope を起動する前に，SiteScope に接続されているすべての BSM が稼働していることを確認します。

アクション・タイプに応じて標準設定警告アクションの名前が指定される

問題 :警告アクションは SiteScope 9.0 で追加されました。SiteScope 9.0 以降のバージョンにアップグレードすると，標準設定警告アクションが作成され，アクション・タイプに応じて名前が指定されます（電子メール，ページャ，SMSなど）。これは，標準設定の名前をアクションを保持する警告と連結する必要がある場合，問題となる可能性があります。

考えられる解決策 : アップグレードの前に，**<SiteScope ルート・ディレクトリ>\groups** にある **master.config** ファイルを開き，連結で使用する区切り文字を含むように **_ AlertActionCompositeNameDelimiter** キーを変更します。

BSM/ServiceCenter または Service Manager の統合

この項目は，10.00 より前のバージョンから SiteScope をアップグレードして，BSM/ServiceCenter または Service Manager 統合を操作する場合に該当します。SiteScope で ServiceCenter モニタを設定するときに，**peregrine.jar** というファイルが作成され，SiteScope マシン上の **WEB-INF\lib** ディレクトリに配置されます。このファイルは，SiteScope のアップグレード中に削除されるため，アップグレード前にバックアップする必要があります。アップグレードが完了したら，バックアップした **peregrine.jar** ファイルを **WEB-INF\lib** ディレクトリに戻します。

SiteScope をアップグレードできない

アップグレード・プロセスが失敗した場合は，<**SiteScope ルート・ディレクトリ>\logs** ディレクトリにある **upgrade.log** ファイルで，アップグレードが失敗した理由を確認してください。

Windows 環境への SiteScope のインストール時にアップグレード・プロセスが失敗した場合は，SiteScope は何度でも再起動の実行を試みます。

考えられる解決策 : SiteScope のインストールを再度実行します。

BSM と統合を行う場合の SiteScope の別のサーバへの移動

このプロセスは，SiteScope サーバを（新しいホスト名と IP アドレスを持つ）新しいハードウェアに移動して，BSM 統合を行う場合に該当します。次の手順で行って統合への影響を最小限に抑えます。

1. 現在の SiteScope インストール環境のバックアップを作成します。詳細については，「SiteScope 構成データのバックアップ」(76ページ)を参照してください。

2. 新しいハードウェアに SiteScope をインストールして，SiteScope 設定データを SiteScope インストール・ディレクトリにインポートします。詳細については，「設定データのインポート」(76ページ)を参照してください。
3. 以前のハードウェアで使用したポート番号を使用して SiteScope サーバを設定します。
4. BSM で次の手順を実行します。
   - 新しい SiteScope ページの SiteScope プロファイルで関連するフィールドを更新します。
   - HOSTS テーブルの SiteScope マシンに関する情報を更新します。

第3部: SiteScope のインストール

第11章: インストール・ワークフロー

本章の内容

- 「インストール・バージョンのタイプ」(85ページ)
- 「インストールの流れ」(86ページ)
- 「Linux インストールの準備」(90ページ)
- 「Oracle Enterprise Linux 環境への SiteScope のインストール」(90ページ)
- 「CentOS 6.2 環境への SiteScope のインストール」(91ページ)
- 「CentOS 6.2 で実行する HP Cloud Services インスタンスへの SiteScope のインストール」(92ページ)
- 「トラブルシューティングおよび制限事項」(93ページ)

インストール・バージョンのタイプ

SiteScope は 64 ビットのアプリケーションとしてインストールされ，動作します。自己抽出型の実行可能ファイルおよびパッケージ・フォルダとして利用できます。メジャー・リリースまたはマイナー・リリースの場合，このファイルは SiteScope インストーラ・パッケージ（zip ファイル）として利用できます。

マイナーマイナー・リリースおよびパッチ・リリースの場合，このファイルは HP ソフトウェア・サポート・サイトの**ソフトウェア・パッチ**・ポートレットからダウンロードできます。

注: SiteScope マイナーマイナー・リリースおよびパッチ・リリースは，SiteScope Failover または System Health などの非標準インストール上ではなく，標準 SiteScope インストール上にのみインストールする必要があります。

最新のバージョンをインストールするには，SiteScope 11.30，，そのマイナーマイナー・バージョンの最新の累積 / 中間パッチ（11.30 の「パッチ」の項の HP サポート・サイトに表示される）の順にインストールする必要がありますします。

公式名	バージョン・タイプ	例	インストール
重要警戒域 Minor	完全なインストーラ・リリース	10.0, 11.0 10.10, 11.30 例のファイル名 : HPSiteScope_11.30_setup.exe	クリーンなシステムにインストールを行い，以前のリリース設定をインポートします。最初の起動時にアップグレードが実行されます。

公式名	バージョン・タイプ	例	インストール
マイナーマイナー（パッチ）	対応するメジャーまたはマイナー・リリースからの不具合修復の集合	10.11（10.10 上） 11.01（11.00 上） 11.24（11.20 または 11.2x 上） 例のファイル名： HPSiS1122_11.24_setup.exe	マイナーマイナー・パッチは，それに対応するリリース上にインストールされます。この場合，アップグレードは不要です。
累積 / 中間 / 公開パッチ	緊急を要する不具合の公式の修正を含むパッケージ	SS1122130529 SS<ver><date> 例のファイル名： SS1122130529-11.22.000-WinNT4.0.msi	単一の専用メジャー，マイナーまたはマイナーマイナー・リリース上にのみ適用可能です。

インストールの流れ

このトピックには，SiteScope 11.30 のインストールに関する指示が記述されています。

注: SiteScope の既存のバージョンをアップグレードする場合は，「既存の SiteScope インストールのアップグレード」(74ページ)の手順に従ってください。

1. **インストールの前提条件（Linux の場合のみ）**
   a. 適切なインストール場所を選択し，アカウントの権限を設定します。詳細については，「Linux インストールの準備」(90ページ)を参照してください。
   b. 次のいずれかのプラットフォームに SiteScope をインストールする場合は，SiteScope をインストールする前に手動で環境を設定する必要があります。

プラットフォーム	インストールの前提条件
Oracle Enterprise Linux 6.0，6.1	「Oracle Enterprise Linux 環境への SiteScope のインストール」(90ページ)を参照してください。
CentOS 6.2	「CentOS 6.2 環境への SiteScope のインストール」(91ページ)を参照してください。

プラットフォーム	インストールの前提条件
CentOS 6.2 オペレーティング・システムで実行する HP Cloud Services（HPCS）インスタンス	「CentOS 6.2 で実行する HP Cloud Services インスタンスへの SiteScope のインストール」(92ページ)を参照してください。
Red Hat ES/AS Linux 6.0	SiteScope を HPOM または BSM と統合する場合は，HP Operations Agent をインストールする前に Red Hat ES Linux 6.0（64 ビット）環境の依存関係を設定する必要があります（エージェントは，HPOM または BSM にイベントを送信し，メトリクス・データを保存するために必要です）。エージェントの依存関係とインストールの設定の詳細については，SiteScope ヘルプまたは HP ソフトウェア統合サイトにある『HP Operations Manager 製品との統合』ガイドを参照してください。

2. **SiteScope 11.30 のダウンロード**

   a. SiteScope のインストール先のマシンにプラットフォーム固有のインストーラ・パッケージ（**SiteScope_11.30_Windows.zip** または **SiteScope_11.30_Linux.zip**）をダウンロードします。SiteScope は，次に示すように HP Systems から入手できます。

カスタマ	ダウンロード・オプション
評価版のカスタマの場合	電子ダウンロード評価版へのリンク HP 認定ソフトウェア・パートナー用の HP Software Partner Central （上記のリンクでは，HP Passport のアカウントが必要です。http://h20229.www2.hp.com/passport-registration.html で HP Passport の登録を行ってください。）
新規カスタマの場合	電子ソフトウェア・ダウンロード。カスタマは，ソフトウェアをダウンロードできるリンクを電子メールにより受け取ります。このリンクは注文に対して固有です。
既存のカスタマの更新の場合	https://h20575.www2.hp.com/usbportal/softwareupdate.do **前提条件：** i. 上記のリンクにアクセスするには HP Passport アカウントが必要です。SSO ポータルを介して更新を受信するには SAID（Support Agreement ID）

カスタマ	ダウンロード・オプション
	が必要です。HP Passport の登録を行うには，http://h20229.www2.hp.com/passport-registration.html を参照してください。SAID のアクティブ化の詳細については，ソフトウェア・サポート・オンライン・サイトの FAQ を参照してください。 ii. ソフトウェアの更新には，新しいライセンス・キーが必要です。HP サポート更新担当者に連絡して，まず製品契約の移行を依頼します。契約の移行が完了したら，［マイ ソフトウェア アップデート］ポータル（https://h20575.www2.hp.com/usbportal/softwareupdate.do）に移動し，［**Get Licensing**］（ライセンスの取得）タブをクリックして新しいライセンス・キーを取得します。 **ソフトウェアの更新をダウンロードするには，次の手順を実行します。** i. ［**マイ ソフトウェア アップデート**］を選択します。 ii. ［**Application Performance Management**］を展開し，必要な HP SiteScope 11.30 Software E-Media を選択し，［**ソフトウェア アップデートの入手**］をクリックします。 iii. ［選択済みの製品］タブで，必要な製品アップデートの［**ソフトウェアの入手**］をクリックし，サイトの指示に従ってソフトウェアをダウンロードします。

b. 圧縮ファイルを適当なディレクトリに抽出します。

3. **SiteScope 11.30 をインストールします。**

次のインストール・オプションのいずれかを使用して SiteScope をインストールします。

オペレーティング・システム	インストール・オプション
Windows	• 実行可能なユーザ・インタフェース（インストール・ウィザード）。詳細については，「インストール・ウィザードを使用してインストール」(95ページ)を参照してください。 • サイレント・インストール :詳細については，「サイレント・モードでの SiteScope のインストール」(122ページ)を参照してください。
Linux	• 実行可能なユーザ・インタフェース（インストール・ウィザード）。詳細については，「インストール・ウィザードを使用してインストール」(95ページ)を参照してください。

オペレーティング・システム	インストール・オプション
	• コマンド・ライン入力によるコンソール・モード・インストール・スクリプト。詳細については，「コンソール・モードを使用した Linux へのインストール」(114ページ)を参照してください。 • サイレント・インストール :詳細については，「サイレント・モードでの SiteScope のインストール」(122ページ)を参照してください。

注:

- コンソール・モード・インストールは，Windows インストールでサポートされていません。
- 既存バージョンの SiteScope がインストールされている場合は，アンインストールしてから SiteScope 11.30 をインストールする必要があります。
- 以前に設定ツールを使用して SiteScope データをエクスポートした場合は（詳細については，「SiteScope 設定ツールの使用」(124ページ)を参照），ユーザ・データの **.zip** ファイルをインポートできます。
- サードパーティ製のミドルウェアおよびドライバがある場合，それらは手作業でコピーまたはインストールする必要があります。

4. **HP Operations Agent をインストールして設定します（SiteScope を HPOM または BSM に統合する場合に必要です）。**

   エージェントのインストールと設定の詳細については，SiteScope ヘルプまたは HP ソフトウェア統合サイトにある『HP Operations Manager 製品との統合』ガイドを参照してください。

5. **Microsoft ホットフィックスをインストールします。**

   SiteScope の拡張性およびパフォーマンスを向上させるため，Microsoft ホットフィックスをインストールすることをお勧めします。詳細については，「Microsoft ホットフィックスのインストール」(195ページ)を参照してください。

6. **SiteScope への接続**

   詳細については，「SiteScope への接続」(199ページ)を参照してください。

Linux インストールの準備

お使いの環境によっては，Linux に SiteScope をインストールするための準備で，適切なインストール先の場所の選択や，アカウント権限の設定が必要になります。

Linux に SiteScope をインストールするための準備は，次の手順で行います。

1. SiteScope アプリケーションをインストールする場所（/opt/HP/SiteScope）で，SiteScope のインストールと操作を行うために十分なディスク領域を使用できることを確認します。
2. SiteScope アプリケーションを実行する非 root ユーザ・アカウントを作成して，このユーザに /opt/HP/SiteScope に対するアカウント権限を設定します。そのアカウントの標準のシェルを設定します。詳細については，「SiteScope を実行する権限のある非 root ユーザ・アカウントの設定」(44ページ)を参照してください。

注:

- インストール中は，Linux インストール・ディレクトリを変更できません。インストール完了後に変更することもお勧めしません。
- すべてのサーバ監視機能を使用するには SiteScope に高いアカウント権限が必要ですが，root アカウントからの SiteScope の実行や，リモート・サーバへのアクセスに root アカウントを使用するような SiteScope の設定は行わないことをお勧めします。
- サイレント・インストールを使用して SiteScope をインストールすることもできます。詳細については，「サイレント・モードでの SiteScope のインストール」(122ページ)を参照してください。

Oracle Enterprise Linux 環境への SiteScope のインストール

SiteScope を Oracle Enterprise Linux にインストールするには，事前に次の依存関係を環境にインストールする必要があります。

- glibc-2.12-1.25.el6.i686.rpm
- glibc-common-2.12-1.25.el6.i686.rpm
- nss-softokn-freebl-3.12.9-3.el6.i686.rpm
- libXau-1.0.5-1.el6.i686.rpm
- libxcb-1.5-1.el6.i686.rpm
- libX11-1.3-2.el6.i686.rpm

Oracle Enterprise Linux で提供される yum パッケージ・マネージャを使用して，次のコマンドを実行して依存関係をインストールできます。

```
yum install -y glibc glibc-common nss-softokn-freebl libXau libxcb libX11 libXext
```

これらの依存関係は，すべての Red Hat ベースのシステムの標準のリポジトリ（**/etc/yum.repos.d**）にあります。

CentOS 6.2 環境への SiteScope のインストール

CentOS 6.2（64 ビット）環境に SiteScope をインストールする前に，次の追加ライブラリのいずれかが Linux 環境にインストールされていることを確認します（最初のオプションの使用が推奨されます）。

- 次のコマンドを実行して，**glibc.i686** および **libXp.i686** ライブラリをインストールします。

  [root@centos ~]# yum install glibc.i686 libXp.i686

- JRE がインストールされ，パスが正しく書き込まれていることを確認します。

  [root@centos ~]# java -version
  java version "1.6.0_22"
  OpenJDK Runtime Environment (IcedTea6 1.10.6) (rhel-1.43.1.10.6.el6_2-x86_64)
  OpenJDK 64-Bit Server VM (build 20.0-b11, mixed mode)

  「コマンドが見つかりません」というエラーが表示された場合，JRE をインストールする必要があります。これを行うには, 次のコマンドを使用します。

  root@centos ~]# yum install java-1.6.0-openjdk

注: 通常，CentOS インストールにはこれらのすべてのライブラリがすでにインストールされています。この場合，インストーラは，JRE が glibc および libXp に依存し始めた直後に glibc.i686 を使用します。SiteScope にはそれ自体の Java があるため，JRE はインストーラを実行するときにのみ必要とされます。

CentOS 6 サーバに SiteScope をインストールする際のヒント：

CentOS 6.2 サーバのホスト名を確認して，ホストが解決されていることを確認してください。

1. hostname コマンドを実行して，ホスト名を取得します。
2. ping <ホスト名> を実行します。ping 要求が成功すると，ホストはすでに解決可能です。
3. 失敗した場合，ifconfig を使用して IP を検索します。
4. echo "<IP> <ホスト名>" >> /etc/hosts を実行して，ホスト名に対応する IP を含む文字列を hosts ファイルに追加します。
5. ping <ホスト名> を再度実行して，ホストが解決されていることを確認します。

   ホスト名が解決されない場合，それが SiteScope が起動しない原因である可能性があります。

CentOS 6.2 で実行する HP Cloud Services インスタンスへの SiteScope のインストール

SiteScope は，CentOS 6.2 オペレーティング・システムで実行する HP Cloud Services（HPCS）インスタンスでサポートされています。

HPCS に SiteScope をインストールするためのヒント

1. **HP Cloud Services サーバのホスト名を確認して，ホストが解決されていることを確認してください。**
   a. hostname コマンドを実行して，ホスト名を取得します。
   b. ping <ホスト名> を実行します。ping 要求が成功すると，ホストはすでに解決可能です。
   c. 失敗した場合，ifconfig を使用して IP を検索します。
   d. echo "<IP> <ホスト名>" >> /etc/hosts を実行して，ホスト名に対応する IP を含む文字列を hosts ファイルに追加します。
   e. ping <ホスト名> を再度実行して，ホストが解決されていることを確認します。
2. **スワップ サイズを確認します。**
   a. free コマンドを実行して，スワップが作成されていることを確認します。
   b. スワップが作成されていない場合：

      ```
      [root@centos ~]# free | grep Swap
      Swap: 0 0 0
      ```

      次のコマンドを実行します。

      2 GB ファイルの作成：

      ```
      [root@centos ~]# dd if=/dev/zero of=/swapfile bs=1M count=2048
      ```

      スワップとして初期化します。

      ```
      [root@centos ~]# mkswap /swapfile
      ```

      有効化します。

      ```
      [root@centos ~]# swapon /swapfile
      ```

   c. スワップを再度確認します。

      ```
      root@centos ~]# free | grep Swap
      Swap: 2097144 0 2097144
      ```

3. **追加のライブラリをインストールします。**

   詳細については，「CentOS 6.2 環境への SiteScope のインストール」(91ページ)を参照してください。

セキュリティ・グループ設定

IP プロトコル	開始ポート	終了ポート	タイプ	CIDR IPS
tcp	8080	8080	IP	0.0.0.0/0
tcp	22	22	IP	0.0.0.0/0
tcp	8888	8888	IP	0.0.0.0/0
icmp	-1	-1	IP	0.0.0.0/0

HPCS への SiteScope のインストール

HPCS に SiteScope をインストールするには，次の手順を実行します。

1. 現在のディレクトリを SiteScope インストーラがある場所に変更して，SiteScope インストーラを実行します。

   [root@centos ~]# sh ./HPSiteScope_11.30_setup.bin -i console

2. コンソール・モードを使用して，SiteScope をインストールします。詳細については，「コンソール・モードを使用した Linux へのインストール」(114ページ)を参照してください。
3. インストールが終了したら，SiteScope を実行します。

   [root@centos ~]# /opt/HP/SiteScope/start

4. SiteScope サービスが起動されるまで数分待機してから，必要なプロセスが実行中であることを確認してください。

   [root@centos ~]# ps -ef | grep SiteScope | grep -v grep |awk '{print $3}'84758477

   最後のコマンドには，SiteScope プロセスのプロセス ID が表示されます。プロセスが 2 つあれば，SiteScope サーバは正常に起動しています。

注意事項および制限事項

Operations Manager 統合は CentOS 6.2 サーバにインストールされた SiteScope 11.30 では現在サポートされていません。

トラブルシューティングおよび制限事項

本項では，SiteScope のインストールに関するトラブルシューティングおよび制限事項について説明します。

- 「コンソール・モードで Linux に SiteScope をインストールできないことがある」(94ページ)
- 「HP Operations Agent のインストール・エラー - ログ・ファイルを確認してください」(94ページ)

- 「SiteScope のアンインストール後に SiteScope をインストールできない」(94ページ)

コンソール・モードで Linux に SiteScope をインストールできないことがある

開いている X セッション数が多すぎる場合，コンソール・モードを使用して Linux Red Hat 環境に SiteScope をインストールできないことがあります。

回避策 : 一部の X セッションを閉じるか，DISPLAY 変数の設定を解除します。

HP Operations Agent のインストール・エラー - ログ・ファイルを確認してください

HP Operations Agent のインストール中にエラーが発生した場合，またはインストール・ステータスを確認する場合は，次のログ・ファイルを確認できます。

- SiteScope ログ。これはインストールが正常に完了したかどうかを表示するだけです。

  ログ・ファイル名 :**HPSiteScope_config_tool.log**

  ログ・ファイルの場所 :

  - **win- %temp%**（Windows プラットフォームの場合）
  - **/temp** または **/var/temp**（UNIX/Linux プラットフォームの場合）

    （「installOATask」の結果を検索）

- HP Operations Agent ログ・ファイル。

  ログ・ファイル名 :**oainstall.log**，**oapatch.log**

  ログ・ファイルの場所 :

  - **%ovdatadir%\log**（Windows プラットフォームの場合）
  - **/var/opt/OV/log/**（UNIX/Linux プラットフォームの場合）

SiteScope のアンインストール後に SiteScope をインストールできない

SiteScope のアンインストール後にインストールを実行しても，完了しないで，「Windows Scripting Host を有効にしてください」というメッセージが表示されます。この原因は，Windows が PATH 環境変数内の %SystemRoot% 変数を解決できないことです（%SystemRoot% がパスに含まれていない場合も同様）。

回避策 : PATH 環境変数内の %SystemRoot% 変数を，**C:\Windows\system32** の実際のパスで置き換えます。

第12章: インストール・ウィザードを使用してインストール

インストール・ウィザードを使用してサポート対象の Windows または Linux 環境に SiteScope をインストールするには，次の手順を実行します。サポート対象環境のリストについては，「システム要件」(62ページ)を参照してください。

X11 ライブラリがすでにサーバにインストールされている場合は，インストール・ウィザードが自動的に実行されます。これらのライブラリがインストールされていない場合は，次のいずれかを実行してください。

- X11 サーバがインストールされていないマシンに，グラフィック・モードで SiteScope をインストールします。詳細については，「X11 サーバがインストールされていないマシンへのインストール・ウィザードを使用した SiteScope のインストール」(113ページ)を参照してください。
- コンソール・モードで，Linux プラットフォームに SiteScope をインストールします。詳細については，「コンソール・モードを使用した Linux へのインストール」(114ページ)を参照してください。

注:

- サイレント・インストールを使用して SiteScope をインストールすることもできます。詳細については，「サイレント・モードでの SiteScope のインストール」(122ページ)を参照してください。
- SiteScope の既存のバージョンをアップグレードする場合は，「既存の SiteScope インストールのアップグレード」(74ページ) の手順に従ってください。
- SiteScope 内から直接に HP Operations Agent をインストールするオプションは，設定ウィザードおよび設定ツールから削除されています。代わりに，エージェントを手動でインストールして，設定する必要があります。SiteScope が HPOM または BSM と統合されている場合（BSM のプロファイル・データベースを使用してパフォーマンス・グラフ作成で測定値データをグラフ化する場合を除く），イベントの送信および測定値データの保存を行うためにエージェントが必要です。エージェントのインストールと設定の詳細については，SiteScope ヘルプまたは HP ソフトウェア統合サイトにある『HP Operations Manager 製品との統合』ガイドを参照してください。

SiteScope をインストールするには，次の手順で行います。

1. SiteScope インストール・パッケージを入手します。
   a. SiteScope のインストール先のマシンにプラットフォーム固有のインストーラ・パッケージ（**SiteScope_11.30_Windows.zip** または **SiteScope_11.30_Linux.zip**）をダウンロードしま

す。SiteScope は，次に示すように HP Systems から入手できます。

カスタマ	ダウンロード・オプション
評価版のカスタマの場合	電子ダウンロード評価版へのリンク HP 認定ソフトウェア・パートナー用の HP Software Partner Central **注：** 上記のリンクでは，HP Passport のアカウントが必要です。http://h20229.www2.hp.com/passport-registration.html で HP Passport の登録を行ってください。
新規カスタマの場合	電子ソフトウェア・ダウンロード。カスタマは，ソフトウェアをダウンロードできるリンクを電子メールにより受け取ります。このリンクは注文に対して固有です。
既存のカスタマの更新の場合	https://h20575.www2.hp.com/usbportal/softwareupdate.do **前提条件：** i. 上記のリンクにアクセスするには HP Passport アカウントが必要です。SSO ポータルを介して更新を受信するには SAID（Support Agreement ID）が必要です。HP Passport の登録を行うには，http://h20229.www2.hp.com/passport-registration.html を参照してください。SAID のアクティブ化の詳細については，ソフトウェア・サポート・オンライン・サイトの FAQ を参照してください。 ii. ソフトウェアの更新には，新しいライセンス・キーが必要です。HP サポート更新担当者に連絡して，まず製品契約の移行を依頼します。契約の移行が完了したら，［マイ ソフトウェア アップデート］ポータル（https://h20575.www2.hp.com/usbportal/softwareupdate.do）に移動し，［**Get Licensing**］（ライセンスの取得）タブをクリックして新しいライセンス・キーを取得します。 **ソフトウェアの更新をダウンロードするには，次の手順を実行します。** i. ［**マイ ソフトウェア アップデート**］を選択します。 ii. ［**Application Performance Management**］を展開し，必要な HP SiteScope 11.30 Software E-Media を選択し，［**ソフトウェア アップデートの入手**］をクリックします。 iii. ［選択済みの製品］タブで，必要な製品アップデートの［**ソフトウェアの入手**］をクリックし，サイトの指示に従ってソフトウェアをダウンロードします。

b. 圧縮ファイルを適当なディレクトリに抽出します。

2. OS の指示に従って SiteScope のインストールを実行します。SiteScope は 64 ビットのアプリケーションとしてのみインストールされます。

   Windows の場合：

   a. **HPSiteScope_11.30_setup.exe** を実行します。

   b. OS およびアーキテクチャに基づき，実行ファイルの名前の前に SiteScope のインストール元の場所を入力します。

      例：

      <SiteScope のインストール>\HPSiteScope_11.30_setup.exe

   Linux の場合：

   a. **ルート**・ユーザとしてサーバにログインします。

   b. 次を入力して，インストーラを実行します。**./HPSiteScope_11.30_setup.bin**.

   > **注:** サーバで Microsoft ターミナル・サーバ・サービスが動作している場合，SiteScope のインストール時に，このサービスがインストール・モードである必要があります。サービスが正しいモードでない場合，ウィザードはエラー・メッセージを表示してインストールを完了します。**change user** コマンドを使用して，インストール・モードに切り替えます。詳細については，Microsoft サポート・サイト（http://support.microsoft.com/kb/320185）を参照してください。

3. ロケールの選択画面が表示されます。

   表示された言語から，SiteScope のインストールで使用する言語を選択します。インストーラには，OS ロケールに応じて異なる言語セットが表示されます。SiteScope ユーザ・インタフェースでサポートされる言語のリストについては，SiteScope の使用ガイド の「SiteScope での多言語化」の項を参照してください。

   ［**OK**］をクリックして，インストールを続けます。［初期化］画面が表示されます。

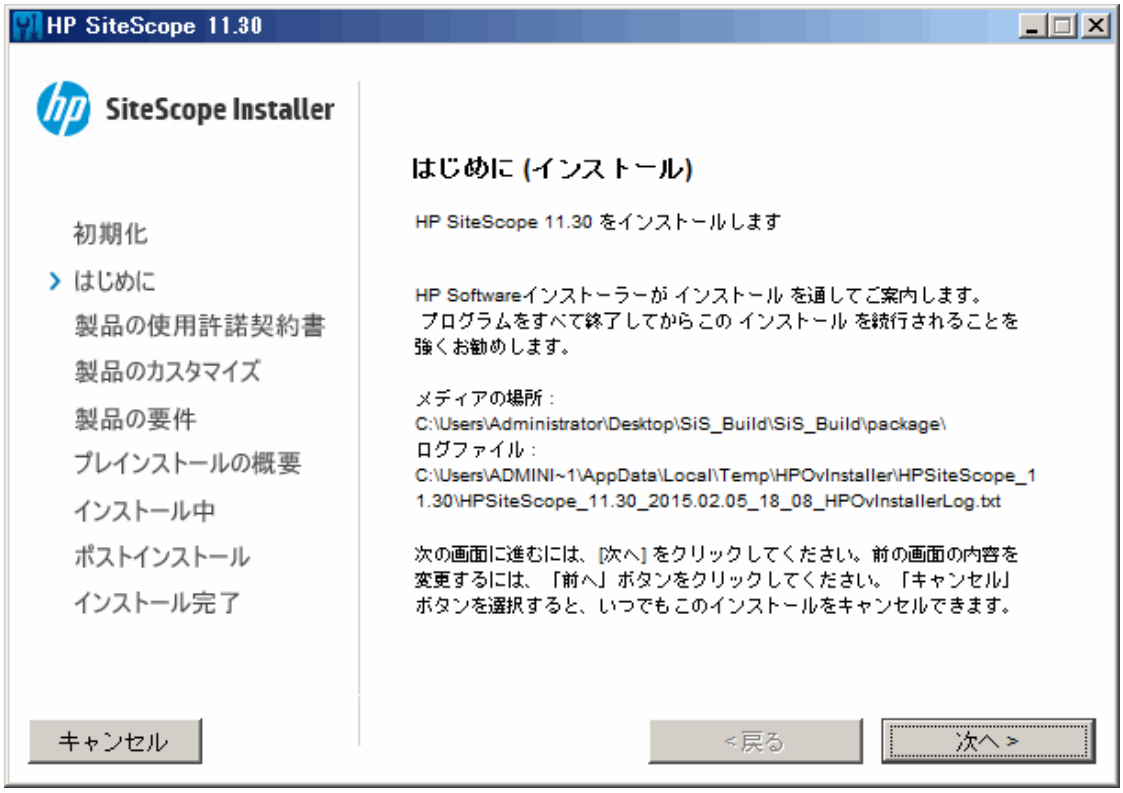
システム上で稼働しているアンチウイルス・プログラムが検出されると，警告内容を調べてからインストールを続行するように求められます。

4. ［**アプリケーションの要件チェックの警告**］画面に警告が表示される場合は，内容を読み，画面の指示に従ってください。

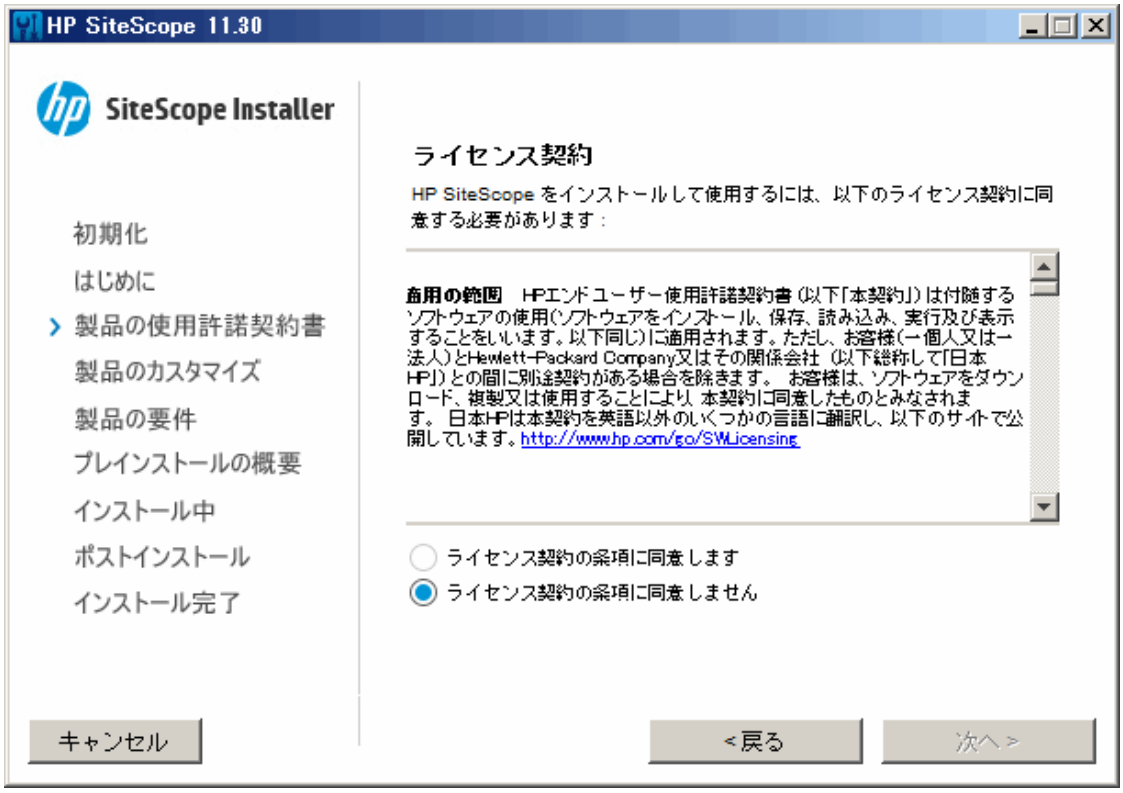
   ウイルス対策プログラムが検出された場合，ウイルス対策プログラムを無効化せずに SiteScope をインストールできるか試してください。

   ［**続行**］をクリックして，インストールを続けます。

5. 表示される［はじめに（インストール）］画面で，［**次へ**］をクリックします。



6. 使用許諾契約画面が開きます。



SiteScope の使用許諾契約を確認します。

SiteScope をインストールするには，［**ライセンス契約の条項に同意します**］を選択して，［**次へ**］をクリックします。

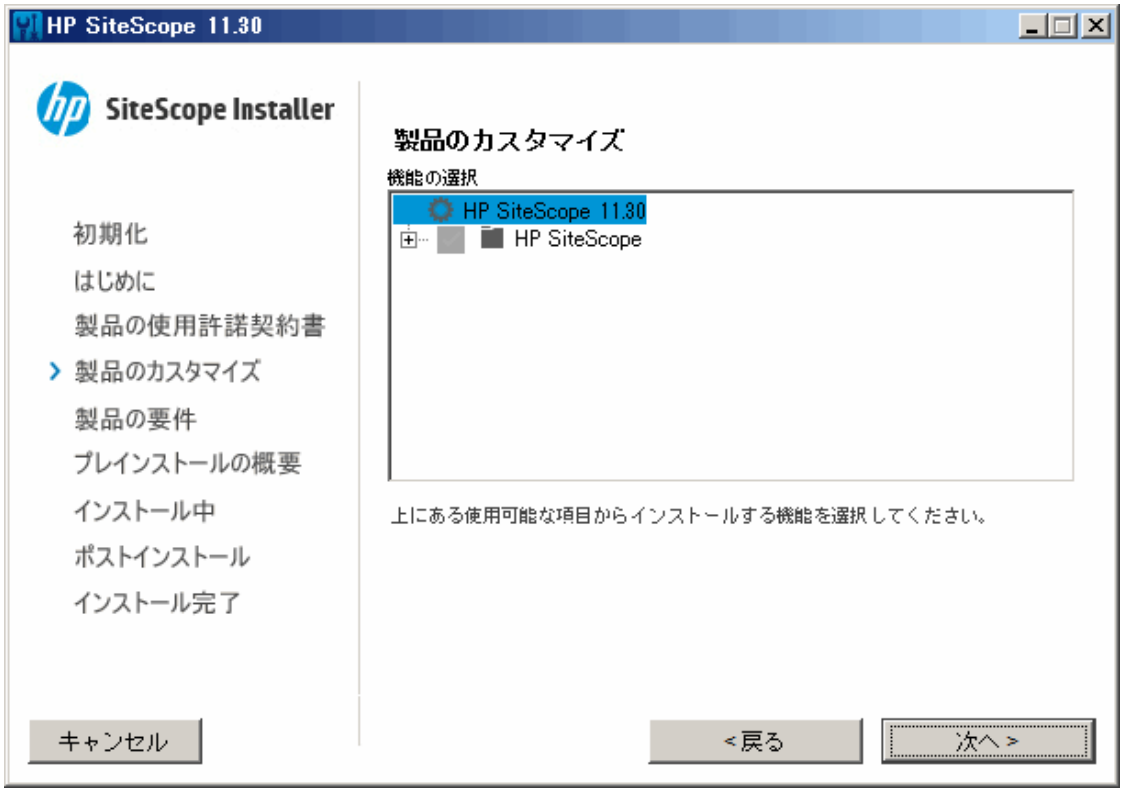
7. ［製品のカスタマイズ］画面で，SiteScope セットアップの種類を選択します。

- **HP SiteScope :** 標準の SiteScope です。
- **HP SiteScope Failover :** このインストールでは，プライマリ SiteScope サーバに障害が発生した場合，インフラストラクチャの可用性の監視のバックアップを提供します。
- **HP SiteScope for Load Testing :** HP LoadRunner または HP Performance Center をインストールする場合のみ使用できます。ユーザは，LoadRunner または Performance Center アプリケーションで SiteScope モニタを定義および使用できるようになります。SiteScope はネイティブ LoadRunner および Performance Center モニタを補完する追加のモニタ機能を提供します。詳細については，該当する LoadRunner または Performance Center のドキュメントを参照してください。

  注: Linux プラットフォームにインストールする場合は，このインストール・オプションを使用できません。

［**次へ**］をクリックして次に進みます。

8. ［機能の選択］画面で，インストール・オプションを選択します。

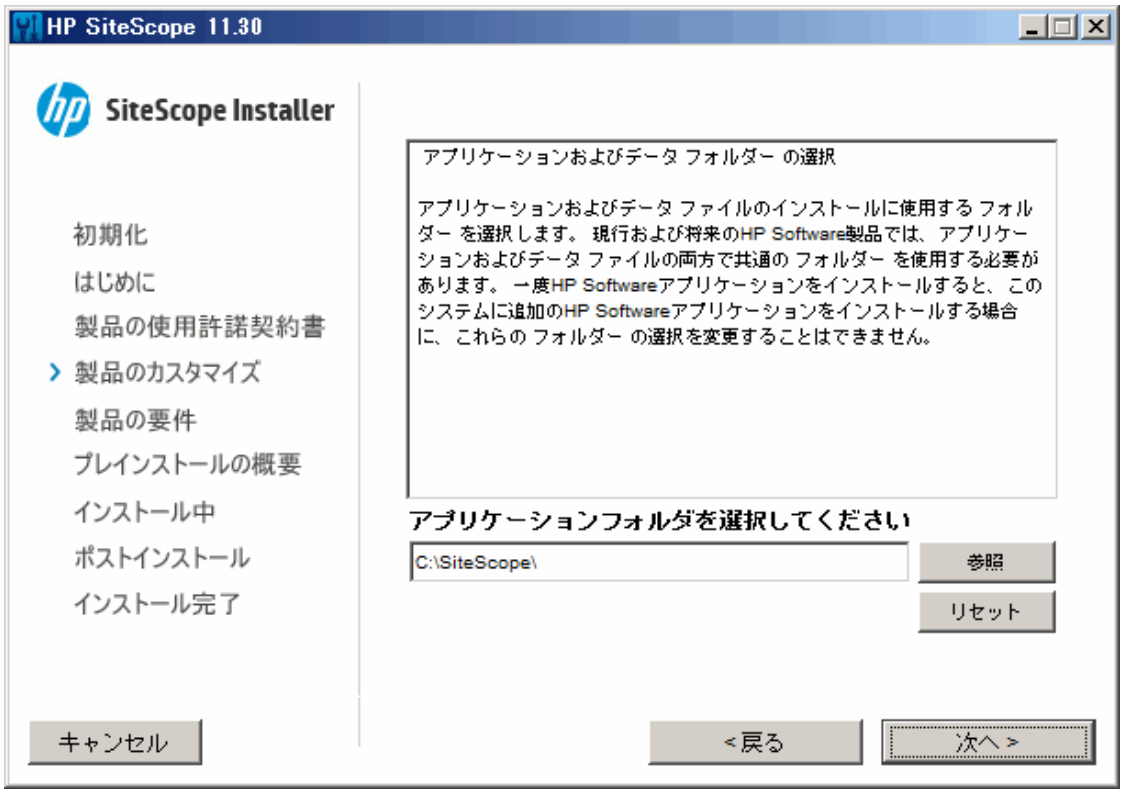


- **HP SiteScope :** SiteScope を 64 ビットのオペレーティング・システムに 64 ビット・アプリケーションとしてインストールします。

［**次へ**］をクリックして次に進みます。

9. Linux プラットフォームにインストールする場合，SiteScope は **/opt/HP/SiteScope/** フォルダに自動的にインストールされます。手順 10 に進みます。

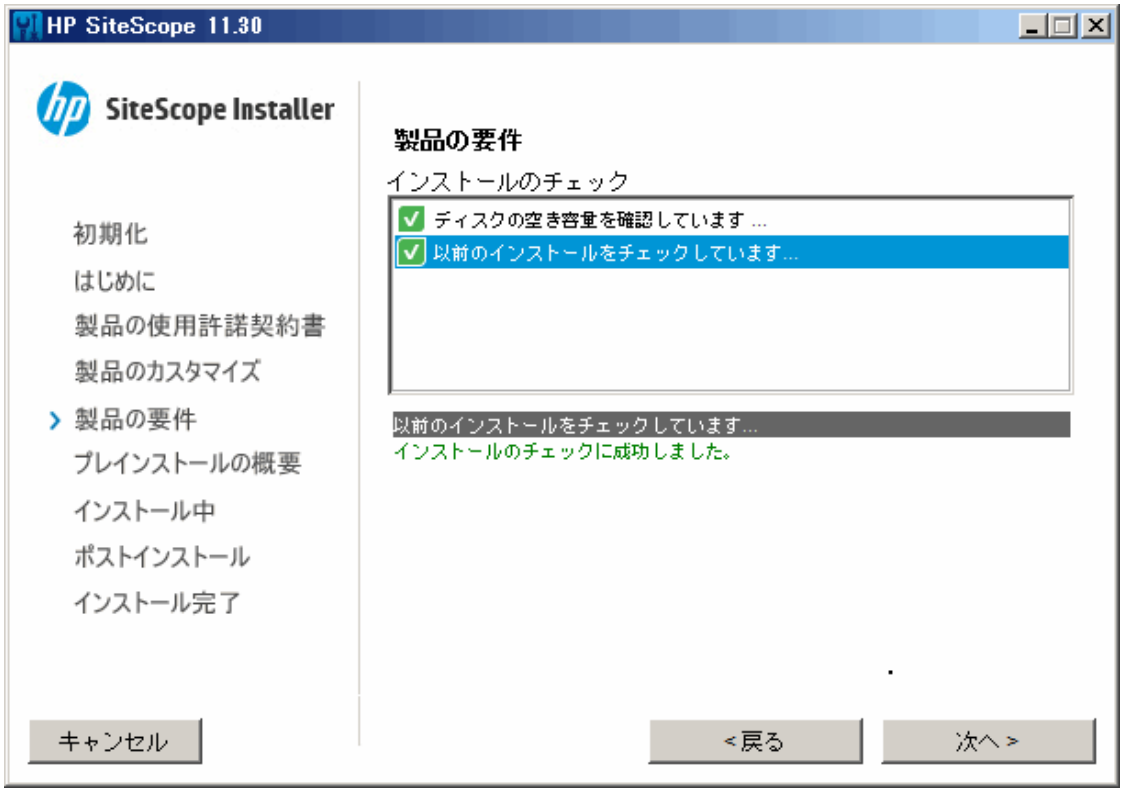
   ［アプリケーションおよびデータ フォルダの選択］画面が開きます。



標準設定のディレクトリを受け入れるか，［**参照**］をクリックして別のディレクトリを選択します。別のディレクトリを選択した場合，インストール・パスの名前にスペースやラテン文字以外の文字を含めないでください。また，パス名は **SiteScope** というフォルダ名（大文字と小文字が区別されます）で終了していなければなりません。標準設定のインストール・パスを復元するには，［**リセット**］をクリックします。

［**次へ**］をクリックして次に進みます。

10. ［インストールのチェック］画面が開いて，検証が実行されます。

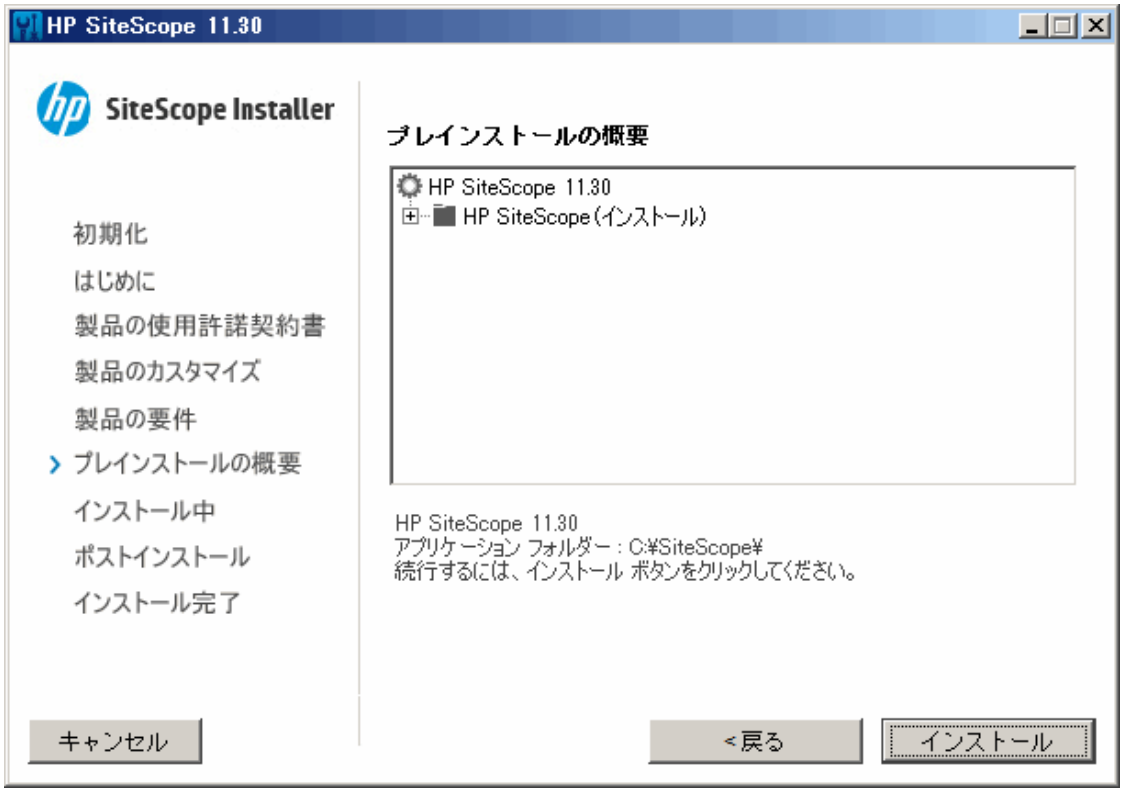


空きディスク容量の検証が正常に完了したら，［**次へ**］をクリックします。

空きディスク容量の検証に失敗した場合は，次の手順で行います。

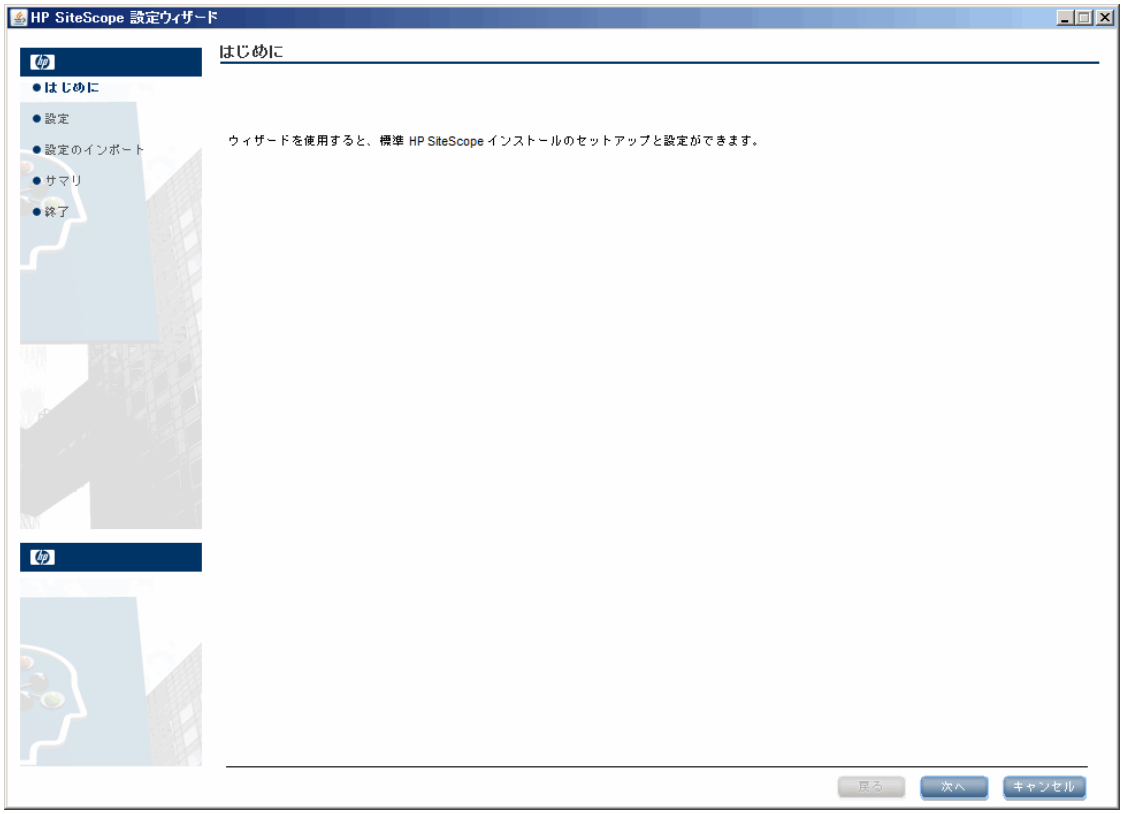
- Windows のディスクのクリーンアップ・ユーティリティなどを使用して，ディスク領域を開放します。
- 手順 9 および 10 を繰り返します。

11. ［プレインストールの概要］画面で，［**インストール**］をクリックします。



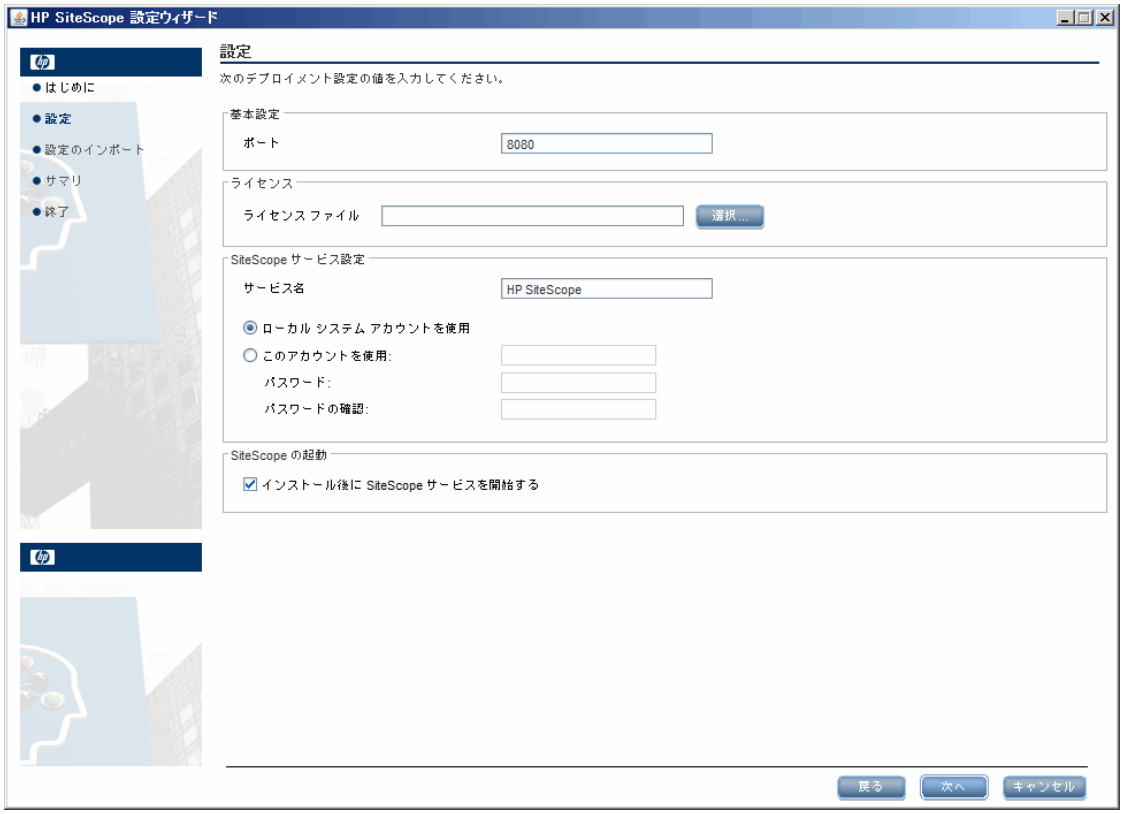
12. インストール画面が開き，必要な SiteScope ソフトウェア・コンポーネントが選択されて，インストールされます。インストール中は，各ソフトウェア・コンポーネントおよびインストールの進行状況が画面に表示されます。

13. SiteScope コンポーネントのインストールが終了すると，SiteScope 設定ウィザードの［はじめに］画面が開きます。



［**次へ**］をクリックします。

14. SiteScope 設定ウィザードの［設定］画面が開きます。



必要な設定情報を入力し，［**次へ**］をクリックします。

- **ポート：**SiteScope のポート番号。指定したポート番号が使用中の場合（エラー・メッセージが表示される場合）は，別のポートを入力します。必要に応じて，後で設定ツールを使用してポートを変更できます。標準設定では，ポート 8080 です。

- **ライセンス・ファイル：**ライセンス・ファイルのパスを入力するか，［**選択**］をクリックして SiteScope ライセンス・キー・ファイルを選択します。通常の SiteScope インストール後では SiteScope Community エディション・ライセンスが自動的にアクティブ化されないため，現時点でライセンス情報を入力する必要はありません。Community エディションの制限された機能から SiteScope の機能を拡張するには，商用エディションのライセンスを購入する必要があります（「SiteScope エディション・ライセンスのアップグレード」(32ページ) 参照）。

- **ローカル・システム・アカウントを使用**（Linux インストールでは無効）:インストール時の標準設定では，SiteScope はローカル・システム・アカウントとして実行されるように設定されています。このアカウントはローカル・コンピュータに対する広範な権限を保持していて，ほとんどのシステム・オブジェクトにアクセスできます。ローカル・システム・アカウントの下で実行されている SiteScope は，SiteScope に設定されているサーバの資格情報を使用してリモート・サーバに接続しようとします。

  注: SiteScope サービスを，ドメイン管理権限を持つユーザとしてログオンすることをお勧めします。 これは，ローカル・システム・アカウントが十分な権限を持たない場合があるためです（ローカル・システム・アカウントは，ドメイン環境では管理者ユーザ権限を持ち，非ドメイン環境ではビルトインの管理者ユーザ権限を持ちます）。

- **このアカウントを使用**（Linux インストールでは無効）:SiteScope サービスのユーザ・アカウントを変更する場合に選択します。SiteScope サービスを，ドメイン管理権限を持つユーザとしてログオンするように設定できます。これにより，SiteScope にドメイン内のサーバ・データを監視するためのアクセス権限が付与されます。リモート・サーバにアクセスできるアカウントおよびパスワードを入力し，確認のためにパスワードを再入力します。

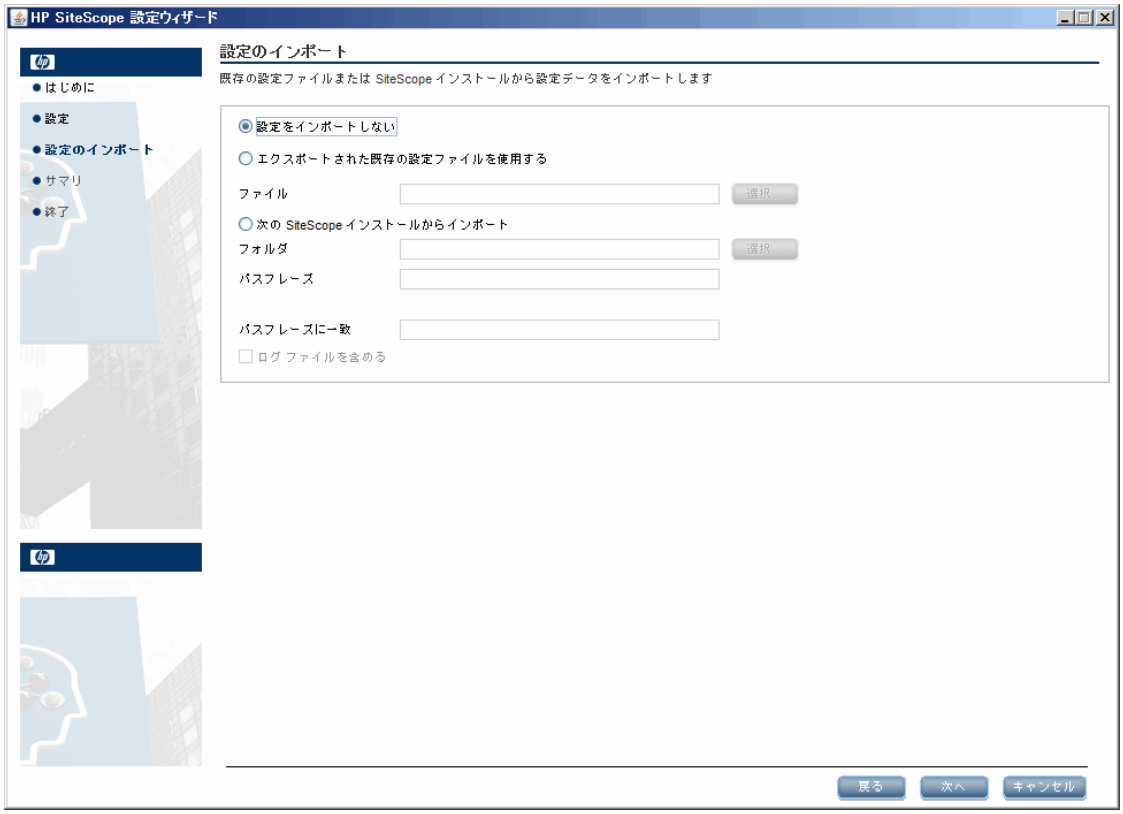
  注: SiteScope がインストールされ，カスタム・ユーザ・アカウントとして実行するように設定されている場合，使用するアカウントには**サービスとしてログオン**権限が必要です。ユーザにログオン・サービスへのアクセス権を付与するには，次の手順で行います。

  i. Windows の［コントロール パネル］で，［**管理ツール**］をダブルクリックします。
  ii. ［ローカル セキュリティ ポリシー］をダブルクリックし，**［ローカル ポリシー］>［ユーザ権利の割り当て］>［サービスとしてログオン］**を選択します。
  iii. ［**ユーザまたはグループの追加**］をクリックして，ログオン・サービス・アクセス権を付与するユーザを選択して，［**OK**］をクリックします。
  iv. ［**OK**］をクリックして，更新したポリシーを保存します。

- **サービス名**（Linux インストールでは無効）: SiteScope サービスの名前。マシンに以前のバージョンの SiteScope がインストールされている場合は，SiteScope サービスに別の名前を入力します。標準のサービス名は SiteScope です。

- **インストール後に SiteScope サービスを開始する**（Linux インストールでは無効）:インストールが完了すると，SiteScope サービスは自動的に起動します。

15. ［設定のインポート］画面が開き，既存の SiteScope 設定データを新しい SiteScope にインポートできるようになります。



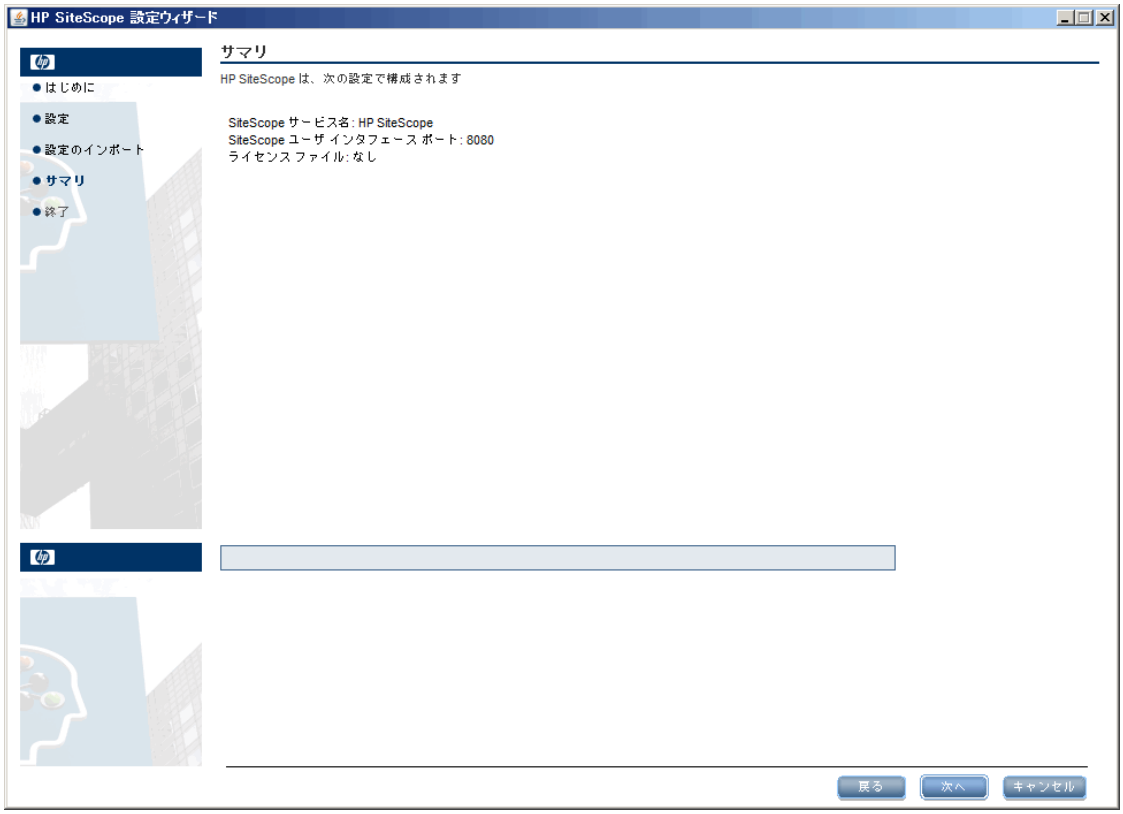
次のいずれかのオプションを選択し，［**次へ**］をクリックします。

- **設定をインポートしない**
- **エクスポートされた既存の設定ファイルを使用する**: エクスポートされた既存の設定ファイルにある，テンプレート，ログ，モニタ設定ファイルなどの SiteScope データを使用できます。SiteScope データは設定ツールを使用してエクスポートされ，**.zip** 形式で保存されます。［**選択**］ボタンをクリックし，インポートするユーザ・データ・ファイルに移動します。
- **次の SiteScope インストールからインポート**:［**選択**］ボタンをクリックして，設定データのインポート元の SiteScope インストール・フォルダに移動します。
  - **ログ ファイルを含める** : 選択した SiteScope インストール・フォルダからログ・ファイルをインポートできるようになります。
- キー管理暗号化を使用して実行するように SiteScope を設定した場合は，SiteScope サーバのキーストアのパスフレーズを［**パスフレーズ**］ボックスに入力します。［**パスフレーズに一致**］ボックスでパスフレーズを確認します。詳細については，「データ暗号化にカスタム・キーを使用するための SiteScope の設定」(170ページ)を参照してください。標準設定の SiteScope 暗号化を使用する場合，これらのボックスは無効です。

注:

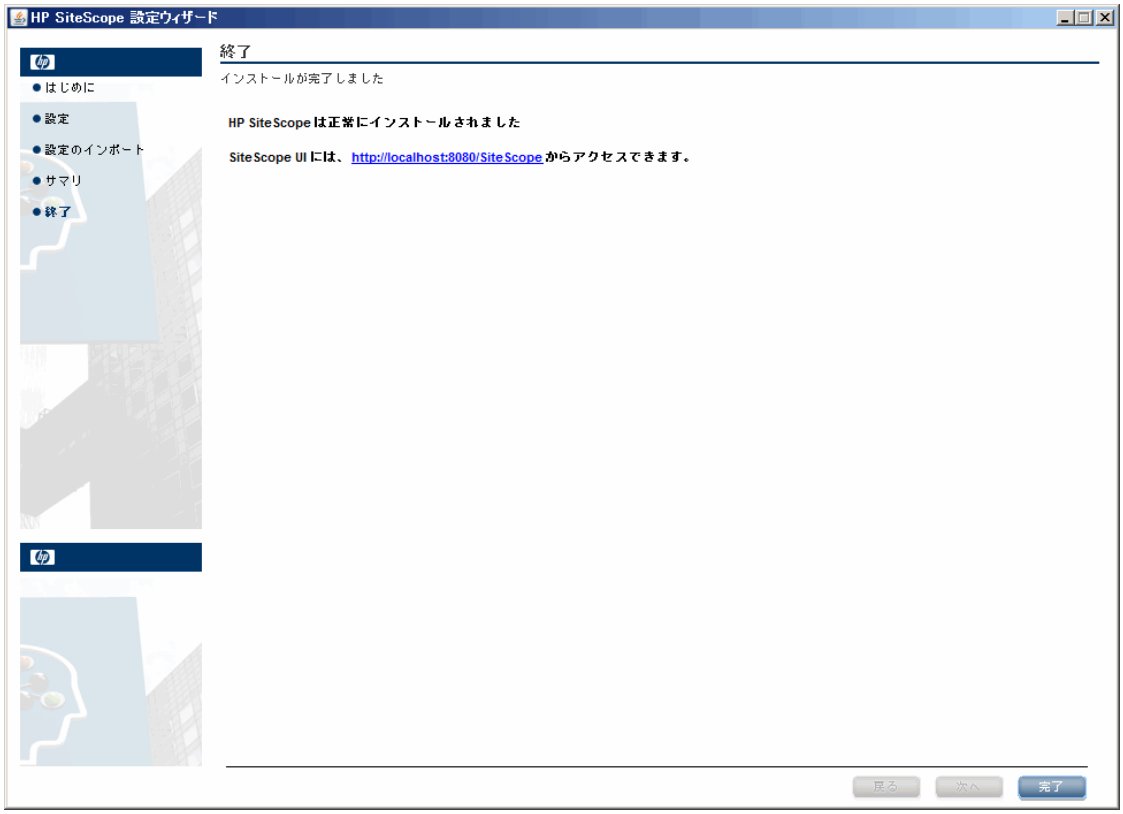
- SiteScope 間で設定データを移動する場合は，設定データの取得元の SiteScope サーバが，データ・インポート先の SiteScope サーバと同じタイム・ゾーン内にあることを確認してください。
- インポートされた設定に期限切れの証明書が含まれている場合，設定のインポート時に標準設定の SiteScope キーストア内にマージされます。これにより，SSL 証明書のモニタがエラー状態になる場合があります。これを回避するために，設定データをエクスポートする前に期限切れの証明書を削除する必要があります。

16. ［サマリ］画面が開きます。



情報が正しいことを確認し，［**次へ**］をクリックして次に進みます。選択内容を変更するには，［**戻る**］をクリックして前の画面に戻ります。

17. ［終了］画面が開きます。



SiteScope ユーザ インタフェース にアクセスするには，現在の SiteScope の接続アドレスをクリックします。

注: 構成設定画面で［インストール後に SiteScope サービスを開始する］を選択しなかった場合は，SiteScope サービスを起動してから，SiteScope に接続する必要があります。詳細については，「SiteScope を使った作業の開始」(197ページ)を参照してください。

［**完了**］をクリックして，SiteScope 設定ウィザードを閉じます。

18. インストールが終了したら，［インストールの完了］ウィンドウが開き，使用したインストール・パスおよびインストール・ステータスのサマリが表示されます。

インストールに失敗した場合は，［**インストールの完了**］ウィンドウの［**ログ ファイルを表示します**］リンクをクリックして Web ブラウザでログ・ファイルを表示し，インストール・ログ・ファイルにエラーがないか確認します。

インストールされたパッケージの詳細については，［**詳細**］タブをクリックしてください。

インストール・プログラムを閉じる場合は，［**完了**］をクリックします。

インストール・プログラムがサーバを再起動する必要があると判断した場合は，サーバを再起動するように求められます。

19. 利用可能な最新機能については，インストールした SiteScope と同じ場所から，最新の SiteScope パッチをダウンロードしてインストールしてください。SiteScope インタフェースへのアクセスの詳細については，「SiteScope への接続」(199ページ)を参照してください。

20. Linux 環境に SiteScope をインストールした場合は，SiteScope インストール・ディレクトリに権限を設定して，SiteScope アプリケーションを実行するために使用されるユーザ・アカウントに対して，読み込み，書き込み，および実行の権限を付与します。これらの権限は，SiteScope インストール・ディレクトリに含まれるすべてのサブディレクトリに対して設定する必要があります。

X11 サーバがインストールされていないマシンへのインストール・ウィザードを使用した SiteScope のインストール

以下のいずれかで，X11 サーバがインストールされていないマシンにインストール・ウィザードを使用して SiteScope をインストールできます。

- VNC サーバを使用する（多くの Linux システムで，VNC サーバは標準設定でインストールされている）
- DISPLAY 環境変数を編集して，別のマシンの X サーバを使用するようにプログラムを設定する

VNC サーバを使用して，X11 がインストールされていないマシンに SiteScope をインストールするには，次の手順で行います。

1. コマンド・ラインで vncserver を実行します。プログラムが起動したら，パスワードを選択し，VNC サーバで使用されるディスプレイ（通常は: 1）を選択します。
2. 以下のフォーマットを使用し，VNC クライアントから SiteScope マシンに接続します。その際は，hostname:display の形式を使用します。たとえば，sitescope.company.name:1 と入力します。
3. 表示されるコンソールで SiteScope インストール・ディレクトリに移動して，通常どおりにインストールを実行します。

X をリダイレクトして，X11 がインストールされていないマシンに SiteScope をインストールするには，次の手順で行います。

1. X サーバがインストールされた Linux システムを実行するか，Windows に X サーバをインストールします（xming など）。
2. X アクセス制御によって，SiteScope が接続できることを確認します。Linux プラットフォームの場合は，man xhost を実行してマニュアルを参照してください。Windows プラットフォームの場合は，X サーバの実装に関するドキュメントを参照してください。
3. SiteScope マシンで **export DISPLAY=x-server.machine.name:display** を実行します（display は通常 0）。
4. 同じシェル内の SiteScope インストール・ディレクトリに移動して，通常どおりインストールを実行します。

第13章: コンソール・モードを使用した Linux へのインストール

SiteScope は，コマンド・ラインまたはコンソール・モードを使用して Linux にインストールできます。SiteScope をリモート・サーバにインストールする場合，または，ユーザ・インタフェースを使用してインストール・オプションを使用できない何らかの理由がある場合は，このオプションを使用します。

注: HP Operations Agent をインストールするオプションは SiteScope コンソール・モードから削除されています。代わりに，エージェントを手動でインストールして，設定する必要があります。SiteScope が HPOM または BSM と統合されている場合（BSM のプロファイル・データベースを使用してパフォーマンス・グラフ作成で測定値データをグラフ化する場合を除く），イベントの送信および測定値データの保存を行うためにエージェントが必要です。エージェントのインストールと設定の詳細については，SiteScope ヘルプまたは HP ソフトウェア統合サイトにある『HP Operations Manager 製品との統合』ガイドを参照してください。

コンソール・モードを使用して Linux に SiteScope をインストールするには，次の手順で行います。

1. SiteScope のインストール先のマシンにインストーラ・パッケージ（**SiteScope_11.30_Linux.zip**）をダウンロードします。または，SiteScope のインストールに使用するユーザ・アカウントがアクセス可能なディスクまたはネットワーク上の場所に SiteScope セットアップ・ファイルをコピーします。

   SiteScope は，次に示すとおり HP Systems から入手できます。

カスタマ	ダウンロード・オプション
評価版のカスタマの場合	電子ダウンロード評価版へのリンク HP 認定ソフトウェア・パートナー用の HP Software Partner Central （上記のリンクでは，HP Passport のアカウントが必要です。http://h20229.www2.hp.com/passport-registration.html で HP Passport の登録を行ってください。）
新規カスタマの場合	電子ソフトウェア・ダウンロード。カスタマは，ソフトウェアをダウンロードできるリンクを電子メールにより受け取ります。このリンクは注文に対して固有です。
既存のカスタマの更新の場	https://h20575.www2.hp.com/usbportal/softwareupdate.do **前提条件：** a. 上記のリンクにアクセスするには HP Passport アカウントが必要です。SSO ポー

カスタマ	ダウンロード・オプション
合	タルを介して更新を受信するには SAID（Support Agreement ID）が必要です。HP Passport の登録を行うには，http://h20229.www2.hp.com/passport-registration.html を参照してください。SAID のアクティブ化の詳細については，ソフトウェア・サポート・オンライン・サイトの FAQ を参照してください。 b. ソフトウェアの更新には，新しいライセンス・キーが必要です。HP サポート更新担当者に連絡して，まず製品契約の移行を依頼します。契約の移行が完了したら，［マイ ソフトウェア アップデート］ポータル（https://h20575.www2.hp.com/usbportal/softwareupdate.do）に移動し，［**Get Licensing**］（ライセンスの取得）タブをクリックして新しいライセンス・キーを取得します。 **ソフトウェアの更新をダウンロードするには，次の手順を実行します。** a. ［**マイ ソフトウェア アップデート**］を選択します。 b. ［**Application Performance Management**］を展開し，必要な HP SiteScope 11.30 Software E-Media を選択し，［**ソフトウェア アップデートの入手**］をクリックします。 c. ［選択済みの製品］タブで，必要な製品アップデートの［**ソフトウェアの入手**］をクリックし，サイトの指示に従ってソフトウェアをダウンロードします。

2. 次のコマンドを実行します。

```
HPSiteScope_11.30_setup.bin -i console
```

インストール・スクリプトによって，Java 仮想マシンが初期化されて，インストールが開始されます。

3. ロケールの選択画面が表示されます。

```
Preparing to install...
Extracting the JRE from the installer archive...
Unpacking the JRE...
Extracting the installation resources from the installer archive...
Configuring the installer for this system's environment...

Launching installer...

===============================================================================
Choose Locale...
----------------

    1- Deutsch
  ->2- English
    3- Espa?ol
    4- Fran?ais
    5- Italiano
    6- Nederlands
    7- Portugu?s  (Brasil)

CHOOSE LOCALE BY NUMBER:
```

番号を入力して目的のロケールを選択し，ENTER キーを押して続行します。

4. 確認画面が表示されます。

   ENTER キーを押して続行します。

5. ［はじめに］画面が表示されます。

```
===============================================================================
Introduction
------------

Welcome to the installation for HP SiteScope 11.30
HP Software Installer will guide you through the installation. It is strongly
recommended that you quit all programs before continuing with this
installation.

Application Media Location :
/install/SiteScope/3497/SiteScope/LinuxSetup/packages/
Installation Log File : /tmp/HPOvInstaller/HPSiteScope_11.30/HPSiteScope_11.30_
2014.09.10_15_02_HPOvInstallerLog.txt
Respond to each prompt to proceed to the next step in the installation.
If you want to change something on a previous step, type 'back'.
You may cancel this installation at any time by typing 'quit'.

PRESS <ENTER> TO CONTINUE:
```

ENTER キーを押して，インストールを続行します。

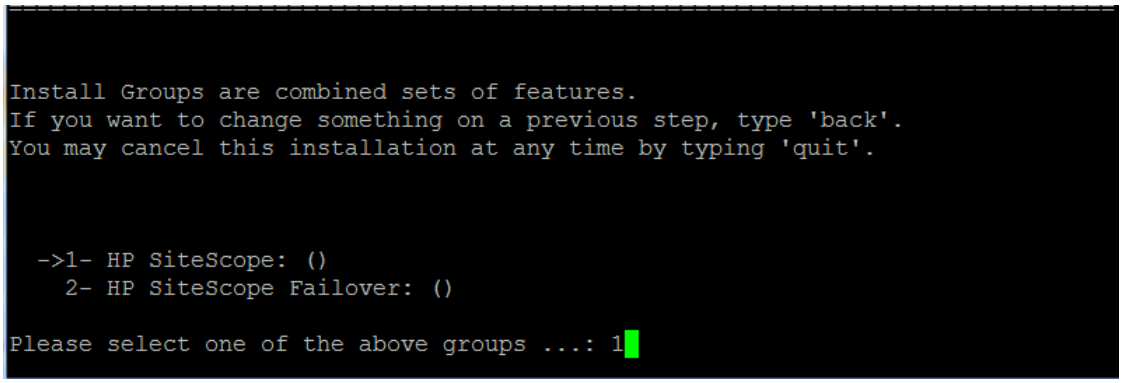
6. 使用許諾契約のテキストが表示されます。SiteScope 使用許諾契約は，数ページにわたって表示されます。表示される各ページを確認してください。次のページに進むには，ENTER キーを押します。使用許諾契約のすべてのページを確認したら，使用許諾契約に同意するか同意しないかを指定します。

```
ライセンス契約の条項に同意します。  (Y/N): Y
```

SiteScope をインストールするには，使用許諾契約に同意する必要があります。標準設定の選択は，使用許諾契約に同意しないになっています。使用許諾契約に同意して，インストールを続行する場合は，Y を入力します。

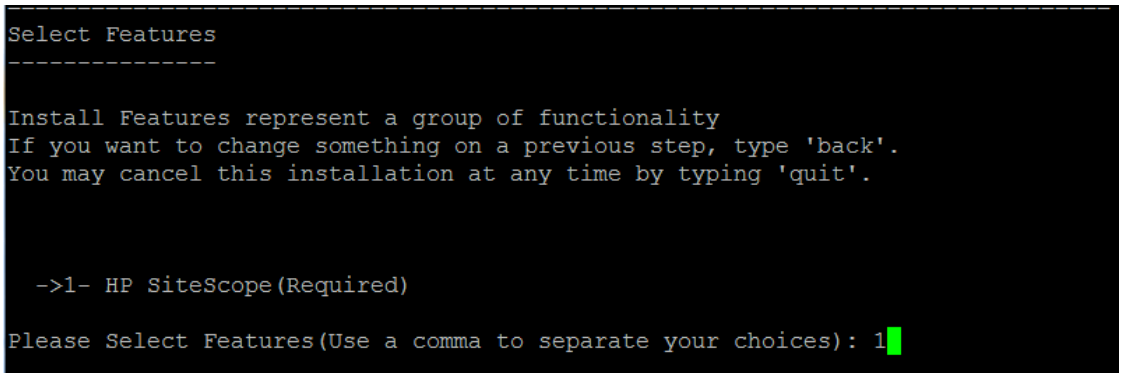
注: SiteScope 使用許諾契約を読んだ後にインストールをキャンセルする場合は，N を入力します。

7. SiteScope のセットアップの種類を選択する画面が開きます。



使用に適した種類を選択します。セットアップの種類の番号を入力し，ENTER キーを押して続行します。

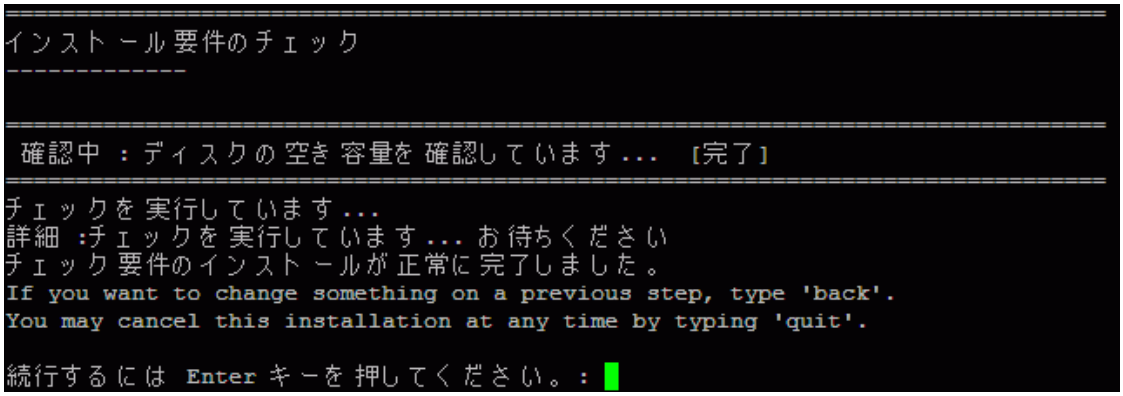
8. ［機能の選択］画面が開きます。



1（必須）を入力して，SiteScope をインストールします。

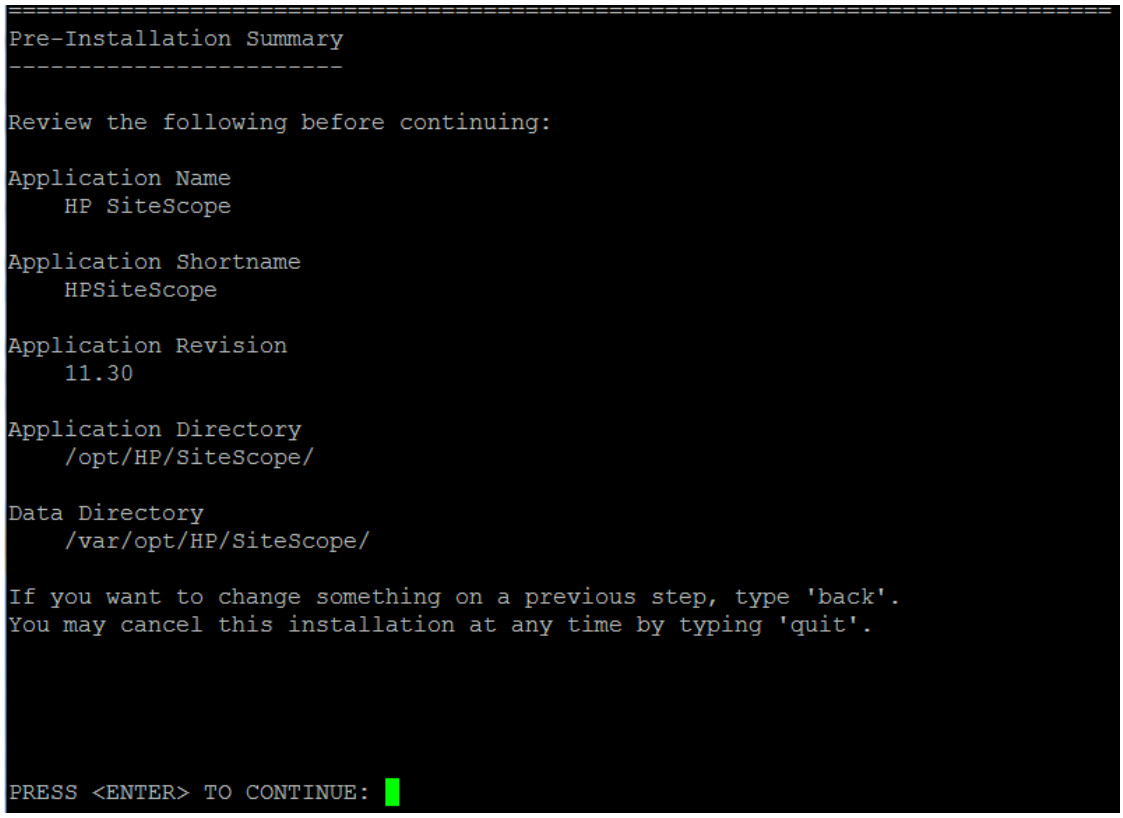
ENTER キーを押して，インストールを続行します。

9. ［インストール要件のチェック］画面が開きます。



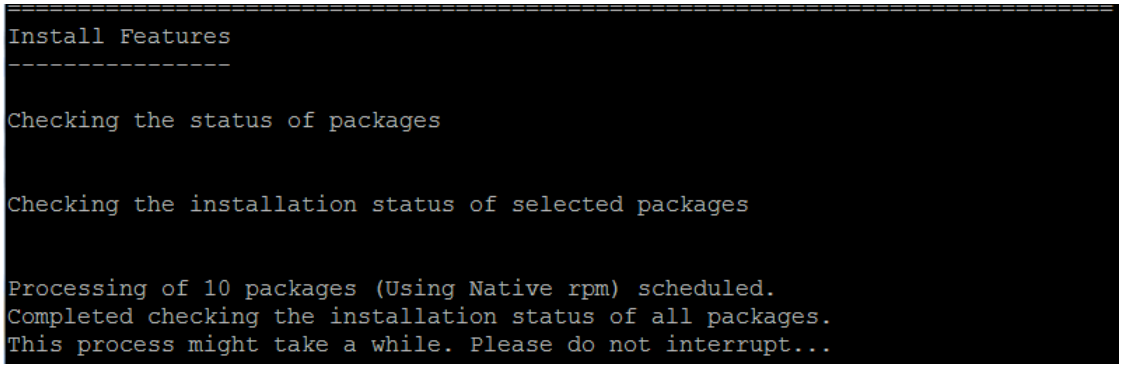
ENTER キーを押して，インストールを続行します。

10. ［プレインストールの概要］画面が開きます。



ENTER キーを押して，インストールを続行します。

11. ［インストール機能］画面が開き，インストール・プロセスが開始されます。



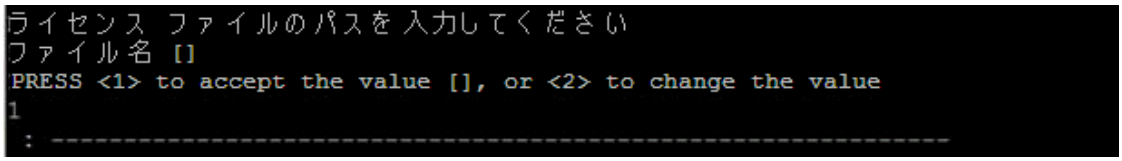
インストール・プロセスが完了すると，インストール後の設定画面が表示されます。

12. ポートに関するプロンプトが表示されます。

1 を入力して，標準設定のポート 8080 を受け入れるか，または 2 を入力してポートを変更し，ポート変更を求めるプロンプトで別の番号を入力します。

ENTER キーを押して，インストールを続行します。

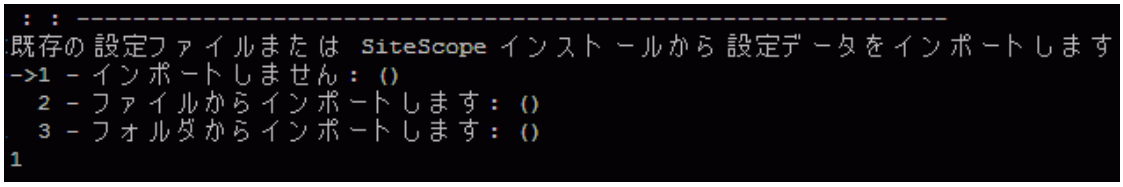
13. ライセンス・ファイル・パスを求めるプロンプトが表示されます。



1 を入力して，ライセンス・ファイル・パスを空のまま残すか（通常の SiteScope インストールの後にSiteScope Community エディションのライセンスが自動的にアクティブ化されるため，SiteScope を使用するためのライセンス情報をこの時点で入力する必要はありません），または 2 を入力して，次のテキスト・ボックスにライセンス・ファイルのパスを入力します。

ENTER キーを押して，インストールを続行します。

14. 設定データのインポート画面が開きます。



データをインポートしない場合は，1 を入力します。

エクスポートされた既存の設定ファイルから，テンプレート，ログ，モニタ設定ファイルなどの SiteScope データを使用する場合は，2 を入力します。このオプションを選択した場合は，次のテキスト・ボックスに設定ファイルのパスを入力します。

SiteScope インストール・ディレクトリから設定データをインポートするには，3 を入力します。このオプションを選択した場合は，設定データのインポート元の SiteScope インストール・フォルダのパスを入力します。

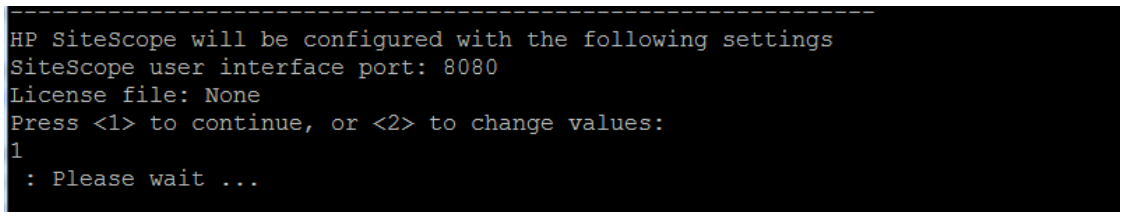
キー管理データ暗号化を使用して実行するように SiteScope を設定した場合は，SiteScope サーバのキーストアのパスフレーズを入力し，同じパスフレーズを再度入力して確認します。詳細については，「データ暗号化にカスタム・キーを使用するための SiteScope の設定」(170ページ)を参照してください。

ENTER キーを押して，インストールを続行します。

注:

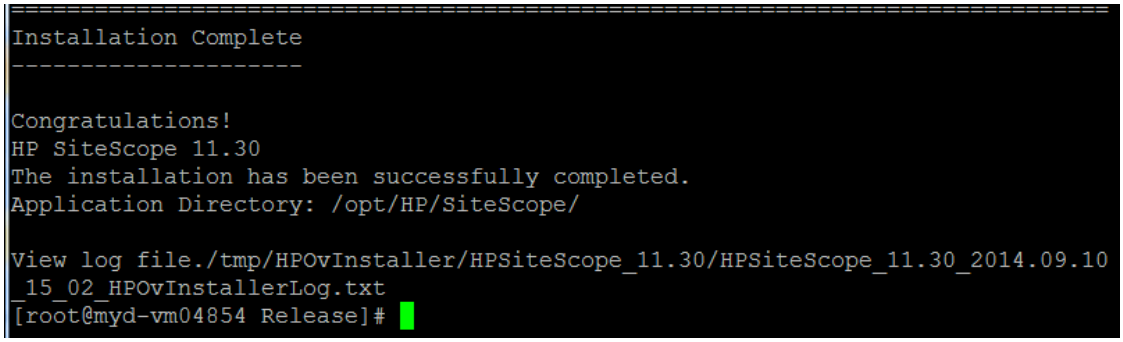
- SiteScope 間で設定データを移動する場合は，設定データの取得元の SiteScope サーバが，データ・インポート先の SiteScope サーバと同じタイム・ゾーン内にあることを確認してください。
- インポートされた設定に期限切れの証明書が含まれている場合，設定のインポート時に標準設定の SiteScope キーストア内にマージされます。これにより，SSL 証明書のモニタがエラー状態になる場合があります。これを回避するために，設定データをエクスポートする前に期限切れの証明書を削除する必要があります。

15. 確認のためのインストール・パラメータがコンソールに表示されます。



指定したパラメータを使用してインストールを続ける場合は 1 を入力し，前のダイアログに戻って変更する場合は 2 を入力して，ENTER キーを押します。

インストール・プロセスが完了します。インストールのステータス・メッセージが表示されます。



16. SiteScope のインストール後，SiteScope インストール・ディレクトリに権限を設定して，SiteScope アプリケーションを実行するために使用されるユーザ・アカウントに対して，読み込み，書き込み，および実行の権限を付与します。これらの権限は，SiteScope インストール・ディレクトリに含まれるすべてのサブディレクトリに対して設定する必要があります。

    SiteScope アプリケーションを実行する非 root ユーザの作成，およびアカウント権限の設定の詳細については，「SiteScope を実行する権限のある非 root ユーザ・アカウントの設定」(44ページ)を参照してください。

17. SiteScope へ接続するには，「Linux プラットフォームでの SiteScope プロセスの開始と停止」(198ページ)の手順に従います。

第14章: サイレント・モードでの SiteScope のインストール

本章の内容

- 「サイレント・モードでの SiteScope のインストールについて」(122ページ)
- 「サイレント・インストールの実行」(123ページ)

サイレント・モードでの SiteScope のインストールについて

サイレント・インストールを使用して SiteScope をインストールできます。サイレント・インストールでは，セットアップ画面を移動して選択値を入力することなく，バックグラウンドですべてのセットアップ・プロセスを実行します。入力する代わりに，すべての設定パラメータには，応答ファイルで定義する値が割り当てられます。複数の異なる設定にサイレント・インストールを実行するには，複数の応答ファイルを作成します。

注意事項および制限事項

サイレント・インストールを実行する前に，次の点を考慮してください。

- サイレント・モードでインストールを実行する場合，メッセージはまったく表示されません。代わりに，インストールが正常に完了したかどうかなどのインストール情報が記録されたログ・ファイルを表示できます。インストール・ログ・ファイルは次の場所にあります。
  - Windows プラットフォームの場合 : **%tmp%\HPOvInstaller\HPSiteScope_11.30**
  - Linux プラットフォームの場合 : **/tmp/HPOvInstaller/HPSiteScope_11.30**
- SiteScope インストール・パス（prodInstallDir=<Installation_path>）は，その名前の部分にスペースや非ラテン文字を含めずに入力し，最後を **SiteScope** という名前のフォルダで終わらせるように指定します（フォルダ名は大文字と小文字を区別して指定する必要があります）。
- SiteScope 内から直接に HP Operations Agent をインストールするオプションは削除されました。代わりに，エージェントを手動でインストールして，設定する必要があります。SiteScope が HPOM または BSM と統合されている場合（BSM のプロファイル・データベースを使用してパフォーマンス・グラフ作成で測定値データをグラフ化する場合を除く），イベントの送信および測定値データの保存を行うためにエージェントが必要です。エージェントのインストールと設定の詳細については，SiteScope ヘルプまたは HP ソフトウェア統合サイトにある『HP Operations Manager 製品との統合』ガイドを参照してください。

サイレント・インストールの実行

ovinstallparams.ini ファイルを使用して，サイレント・インストールを実行します。このファイルの形式は非常に特殊であるため，サンプル・ファイル **ovinstallparams.ini** を使用してサイレント・インストール・ファイルを作成します。

注: サンプルの **ovinstallparams.ini** ファイルは，**<SiteScope インストール・ディレクトリ>\examples\silent_installation** フォルダから SiteScope をインストールした後にのみ使用できます。

SiteScope 11.30 のサイレント・インストールを行うには，次の手順を実行します。

1. **<SiteScope インストール・ディレクトリ>\examples\silent_installation** フォルダにある **ovinstallparams.ini** ファイルに移動します。
2. このファイルのコピーを作成し，作成したコピーをインストールの必要性に応じて変更します。
3. SiteScope インストール・ファイル（**HPSiteScope_11.30_setup.exe** または **HPSiteScope_11.30_setup.bin**）が置かれているセットアップ・フォルダにこのファイルをコピーします。
4. **-i silent** フラグを指定して，コマンド・ラインからインストーラを実行します。Windows では，**待機**モードを指定します。例：

   start /wait HPSiteScope_11.30_setup.exe -i silent（Windows の場合）

   HPSiteScope_11.30_setup.bin -i silent（Linux の場合）

サイレント・モードで SiteScope をアンインストールするには，次の手順を実行します。

Linux の場合は，次を実行します。

/opt/HP/SiteScope/installation/bin/uninstall.sh -i silent

Windows の場合は，次を実行します。

%SITESCOPE_HOME%\installation\bin\uninstall.bat -i silent

第15章: SiteScope 設定ツールの使用

本章の内容

- 「Windows プラットフォームでの設定ツールの実行」(124ページ)
- 「Linux プラットフォームでの設定ツールの実行」(131ページ)
- 「コンソール・モードでの設定ツールの実行」(135ページ)
- 「サイレント・モードでの設定ツールの実行」(141ページ)

Windows プラットフォームでの設定ツールの実行

設定ツールは，ある SiteScope から別の SiteScope に設定データを移動するのに便利なユーティリティです。後で SiteScope にインポートするために，現在の SiteScope からテンプレート，ログ，モニタ設定ファイル，スクリプト，サーバ証明書などの SiteScope データをエクスポートできます。ウィザードを使用して，Windows レジストリ・キーでのサイズ変更による SiteScope のパフォーマンスの最適化，SiteScope に割り当てられているポートの変更，および HP Operations Agent のインストールの完了も実行できます。

インストール・プロセス中に SiteScope データをエクスポートした場合，設定ツールを使用してそのデータをインポートできます。または，設定ツールを使用して，インストール・プロセスの一部としてではなく独立して現在の SiteScope からデータをエクスポートすることもできます。以前のバージョンの SiteScope でモニタ設定ファイルを作成または変更した場合は，それらを現在の SiteScope ディレクトリにインポートする必要があります。

注:

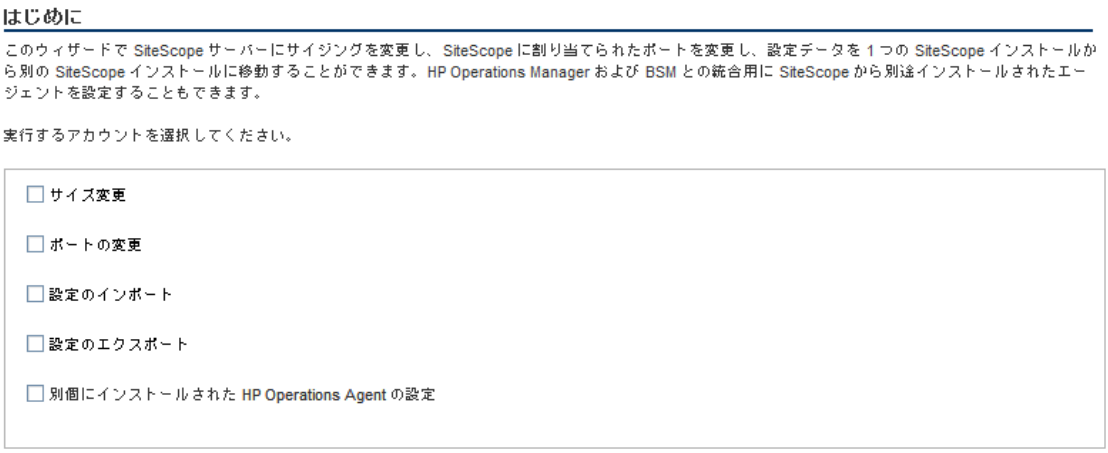
- また，Windows プラットフォーム上で，設定ツールをコンソール・モードで実行することもできます。詳細については，「コンソール・モードでの設定ツールの実行」(135ページ)を参照してください。
- HP Operations Agent を SiteScope 内から直接インストールおよびアンインストールするオプションは，設定ツールから削除されました。代わりに，エージェントを手動でインストールして，設定する必要があります。SiteScope が HPOM または BSM と統合されている場合，エージェントでイベントを送信し，メトリック・データを保存する必要があります（BSM 内のプロファイル・データベースを使用してパフォーマンス・グラフ作成にメトリクス・データを使用する場合を除く)。エージェントのインストールと設定の詳細については，SiteScope ヘルプまたは HP ソフトウェア統合サイトにある『HP Operations Manager 製品との統合』ガイドを参照してください。
- データをエクスポートまたはインポートする前に SiteScope サービスを停止し，データのエクスポートまたはインポートの後にサービスを再起動する必要があります。詳細については，

「Windows プラットフォームでの SiteScope サービスの開始と停止」(197ページ)を参照してください。

- SiteScope の同じバージョンに設定をインポートする場合，新しいテンプレート例がインポートされるように，すべてのテンプレート例コンテナの名前を変更するか，コンテナを削除する必要があります。
- SiteScope 間で設定データを移動する場合は，設定データの取得元の SiteScope サーバが，データ・インポート先の SiteScope サーバと同じタイム・ゾーン内にあることを確認してください。
- インポートされた設定に期限切れの証明書が含まれている場合，設定のインポート時に標準設定の SiteScope キーストア内にマージされます。これにより，SSL 証明書のモニタがエラー状態になる場合があります。これを回避するために，設定データをエクスポートする前に期限切れの証明書を削除する必要があります。
- 次のフォルダにあるファイルは，設定データをインポートするときに上書きできません: **templates.os**，**templates.post**，**templates.health**，**templates.applications**，**conf\ems**。
- 設定ツールで，データのエクスポート時にサーバ証明書とスクリプトを含めることがサポートされます。以前のバージョンの SiteScope からデータをエクスポートするときにサーバ証明書とスクリプトを含める方法については，「既存の SiteScope インストールのアップグレード」(74ページ)を参照してください。

SiteScope 設定ツールを実行するには，次の手順を実行します。

1. SiteScope サーバで，［**スタート**］＞［**すべてのプログラム**］＞［**HP SiteScope**］＞［**設定ツール**］を選択します。SiteScope 設定ウィザードが開きます。
2. 実行するアクションを選択してから，［**次へ**］をクリックします。



- **サイズ変更 :** Windows レジストリ・キーの JVM ヒープ・サイズ，デスクトップ・ヒープ・サイズ，およびファイル・ハンドル数を増やして，SiteScope のパフォーマンスを最適化できます。詳細については，手順 3 を参照してください。

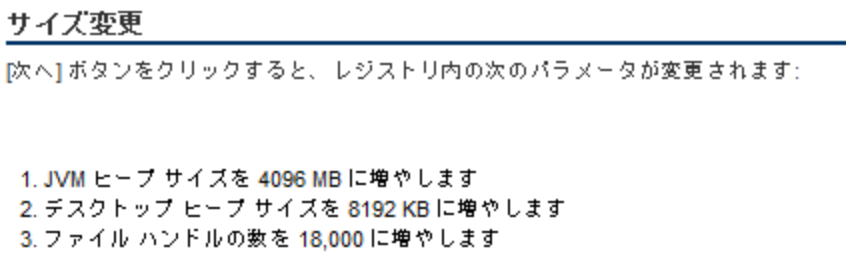
  注: go.bat ファイルを <SiteScope インストール・ディレクトリ>\bin ディレクトリで実

行して SiteScope を起動する場合，**go.bat** ファイルを開いて，**-Xmx1024m** パラメータを必要に応じて最大 **-Xmx8192m**（8 GB の場合）まで増やします。

- **ポートの変更：** SiteScope サーバで使用されるポートを変更できるようにします。詳細については，手順 4 を参照してください。
- **設定のインポート：**エクスポートされた設定データ（**.zip**）ファイル，または既存の SiteScope インストールから設定データをインポートできるようにします。詳細については，手順 5 を参照してください。
- **設定のエクスポート：**後で SiteScope にインポートするために，現在の SiteScope からテンプレート，ログ，モニタ設定ファイルなどの SiteScope データをエクスポートできるようにします。詳細については，手順 6 を参照してください。
- **別個にインストールされた HP Operations Agent の設定:** HP Operations エージェントのインストールを完了するために必要です。エージェントによって，SiteScope が HP Operations Manager または BSM ゲートウェイ・サーバと統合されている場合に，イベントを送信し，メトリクス・データのデータ・ストレージとして機能するように SiteScope または SiteScope Failover を設定できます。詳細については，手順 7 を参照してください。

注: このオプションは，HP Operations Agent 11.14 が SiteScope サーバにインストールされていない場合は無効になっています。エージェントのインストールと設定の詳細については，SiteScope ヘルプまたは HP ソフトウェア統合サイトにある『HP Operations Manager 製品との統合』ガイドを参照してください。

3. ［**サイズ変更**］オプションを選択した場合は，Windows レジストリのパラメータが一覧表示された［サイズ変更］画面が開きます。



Windows レジストリ・キーに次の変更を加えることで，SiteScope のパフォーマンスを最適化できます。

- **JVM ヒープ・サイズ：**値が 512 MB から 4096 MB に変更されます。JVM ヒープ・サイズの詳細については，http://java.sun.com/j2se/1.5.0/docs/guide/vm/gc-ergonomics.html（英語サイト）を参照してください。
- **デスクトップ・ヒープ・サイズ：**値が 512 KB から 8192 KB に変更されます。デスクトップ・ヒープ・サイズの詳細については，http://support.microsoft.com/kb/126962 を参照してくだ

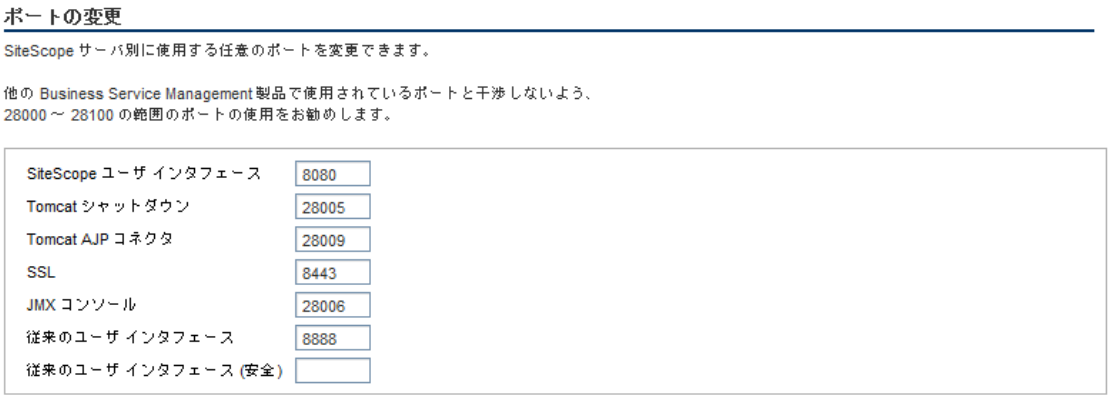
さい。

注: サイズ変更は，SiteScope サーバの物理メモリが，設定ツールによって設定された最大 JVM ヒープ・サイズ（Xmx）（64 ビット・インストール済み環境の場合は 4 GB）よりも大きい場合にのみ実行できます。

［**次へ**］をクリックして，サイズ設定操作を完了します。

- **ファイル・ハンドル：** 値は，10,000 から 18,000 ファイル・ハンドルに増加します。ファイル・ハンドルの変更の詳細については，http://support.microsoft.com/kb/326591 を参照してください。

4. ［**ポートの変更**］オプションを選択した場合は，［ポートの変更］画面が開きます。



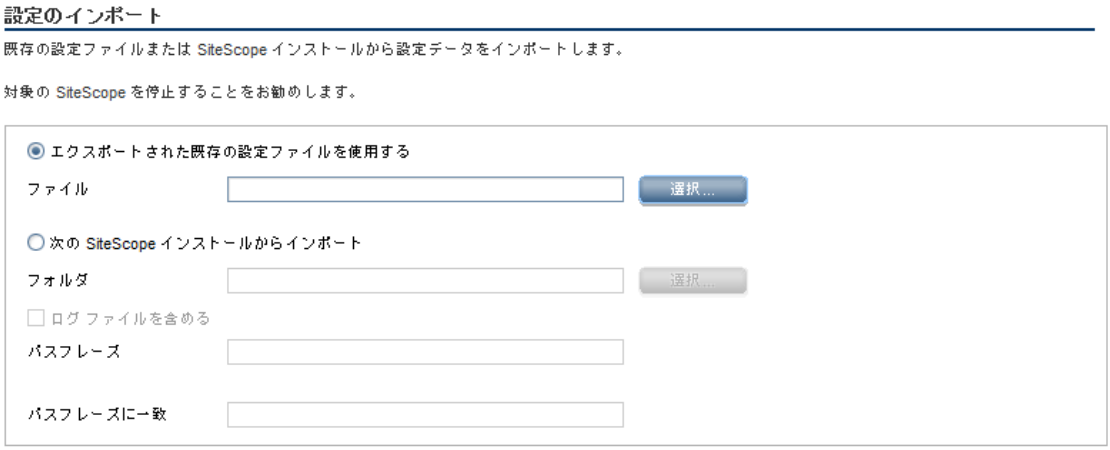
必要に応じて，SiteScope サーバで使用されるポートを変更します。ポート番号には，1 ~ 65534 の数字を指定する必要があります。従来のユーザ・インタフェースを除くすべてのコンポーネントで，ポートは必須です。

注: ほかの Business Service Management 製品で使用されるポートの妨げとならないように，28000 ~ 28100 のポートを使用することをお勧めします。

［**次へ**］をクリックして，ポートの変更操作を完了します。

注: ポート変更操作を完了した後，**［スタート］ > ［すべてのプログラム］ > ［HP SiteScope］ > ［HP SiteScope を開く］** でポートが更新されます。

5. ［**設定のインポート**］オプションを選択した場合は，［設定のインポート］画面が開きます。

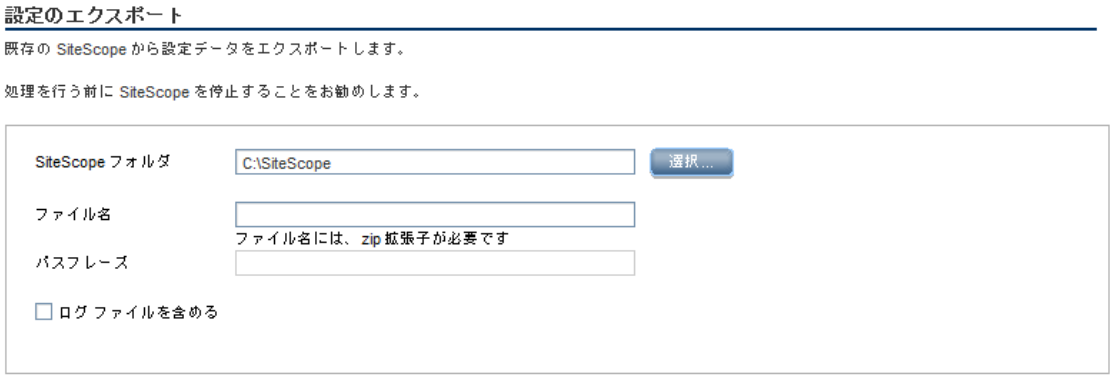


注: データをインポートする前に SiteScope サービスを停止し，データのインポート後にサービスを再起動する必要があります。詳細については，「Windows プラットフォームでの SiteScope サービスの開始と停止」(197ページ)を参照してください。

- ［**エクスポートされた既存の設定ファイルを使用する**］を選択した場合は，インポートするユーザ・データの名前を入力します。
- ［**次の SiteScope インストールからインポート**］を選択した場合は，ユーザ・データ・ファイルをインポートする SiteScope インストール・ディレクトリを入力します。ログ・ファイルもインポートする場合は，［**ログ ファイルを含める**］を選択します。
- キー管理データ暗号化を使用して実行するように SiteScope が設定されていた場合，SiteScope サーバのパスフレーズを**パスフレーズ** ボックスに入力します。［**パスフレーズに一致**］ ボックスに同じパスフレーズを入力して，パスフレーズを確定します。詳細については，「データ暗号化にカスタム・キーを使用するための SiteScope の設定」(170ページ)を参照してください。標準設定の SiteScope 暗号化を使用する場合，これらのボックスは無効です。

［**次へ**］をクリックして，インポート操作を完了します。

6. ［**設定のエクスポート**］オプションを選択した場合，［設定のエクスポート］画面が開きます。



- ［**SiteScope フォルダから**］ボックスに表示されている標準設定のディレクトリをそのまま使用するか，SiteScope インストール・ディレクトリの完全パスを入力します。たとえば，表示されているディレクトリ・パスを使用しない場合，インストール・ディレクトリのパスが D:\SiteScope11_0\SiteScope であれば，D:\SiteScope11_0\SiteScope と入力します。

- ［**ファイル名**］に，ユーザ・データ・ファイルをエクスポートする既存のディレクトリ，およびエクスポートしたユーザ・データ・ファイルの名前を入力します。この名前は **.zip** で終わる必要があります。ログ・ファイルもエクスポートする場合は，［**ログ ファイルを含める**］を選択します。

- キー管理データ暗号化を使用して実行するように SiteScope が設定されていた場合，SiteScope サーバのキーストアに使用されるパスフレーズを［**パスフレーズ**］ボックスに入力します。詳細については，「データ暗号化にカスタム・キーを使用するための SiteScope の設定」(170ページ)を参照してください。このボックスは，標準設定の SiteScope 暗号化が使用される場合は無効です。

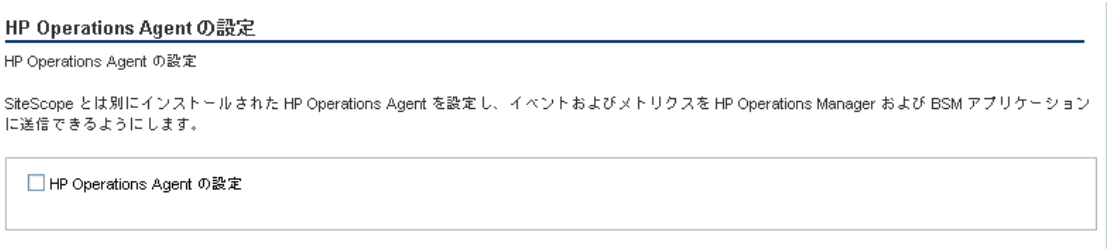
注:

- データをエクスポートする前に SiteScope サービスを停止し，データのエクスポート後にサービスを再起動する必要があります。詳細については，「Windows プラットフォームでの SiteScope サービスの開始と停止」(197ページ)を参照してください。

- **\htdocs** ディレクトリは SiteScope データのエクスポート時にコピーされないため，このディレクトリのバックアップを作成し，アップグレード後にそれを SiteScope 11.30 ディレクトリにコピーして，古いレポートを参照できるようにする必要があります。

［**次へ**］をクリックして，エクスポート操作を完了します。

7. ［**別個にインストールされた HP Operations Agent の設定**］オプションを選択した場合は，［HP Operations Agent の設定］画面が開きます。



［**HP Operations Agent の設定**］を選択します。これは，HP Operations エージェントのインストールを完了するために必要です。エージェントによって，SiteScope が HP Operations Manager または BSM ゲートウェイ・サーバと統合されている場合に，イベントを送信し，メトリクス・データのデータ・ストレージとして機能するように SiteScope を設定できます。

イベントの送信およびメトリクス・データのレポートの詳細については，SiteScope ヘルプまたは HP ソフトウェア統合サイトにある『HP Operations Manager 製品との統合』ガイドを参照してください。

［**次へ**］をクリックして，インストール操作を完了します。

8. ［サマリ］画面が開いて，設定ステータスが表示されます。

［**完了**］をクリックして，ウィザードを閉じます。

アップグレード後に SiteScope を起動するには，**<SiteScope のルート・ディレクトリ>\bin** ディレクトリの **go.bat** ファイルを実行します。これにより，監視を実行するまでに 15 分以上かかった場合に SiteScope が自動的に再起動されるのが回避されます。

Linux プラットフォームでの設定ツールの実行

設定ツールは，ある SiteScope から別の SiteScope に設定データを移動するのに便利なユーティリティです。後で SiteScope にインポートするために，現在の SiteScope からテンプレート，ログ，モニタ設定ファイル，スクリプト，サーバ証明書などの SiteScope データをエクスポートできます。ウィザードを使用して，SiteScope サーバで使用されるポートの変更および HP Operations Agent のインストールの完了も実行できます。

インストール・プロセス中に SiteScope データをエクスポートした場合，設定ツールを使用してそのデータをインポートできます。または，設定ツールを使用して，インストール・プロセスの一部としてではなく独立して現在の SiteScope からデータをエクスポートすることもできます。以前のバージョンの SiteScope でモニタ設定ファイルを作成または変更した場合は，それらを現在の SiteScope ディレクトリにインポートする必要があります。

注:

- また，Linux プラットフォーム上で，設定ツールをコンソール・モードで実行することもできます。詳細については，「コンソール・モードでの設定ツールの実行」(135ページ)を参照してください。
- HP Operations Agent を SiteScope 内から直接インストールおよびアンインストールするオプションは，設定ツールから削除されました。代わりに，エージェントを手動でインストールして，設定する必要があります。SiteScope が HPOM または BSM と統合されている場合，エージェントでイベントを送信し，メトリック・データを保存する必要があります（BSM 内のプロファイル・データベースを使用してパフォーマンス・グラフ作成にメトリクス・データを使用する場合を除く)。エージェントのインストールと設定の詳細については，SiteScope ヘルプまたは HP ソフトウェア統合サイトにある『HP Operations Manager 製品との統合』ガイドを参照してください。
- SiteScope 間で設定データを移動する場合は，設定データの取得元の SiteScope サーバが，データ・インポート先の SiteScope サーバと同じタイム・ゾーン内にあることを確認してください。
- インポートされた設定に期限切れの証明書が含まれている場合，設定のインポート時に標準設定の SiteScope キーストア内にマージされます。これにより，SSL 証明書のモニタがエラー状態になる場合があります。これを回避するために，設定データをエクスポートする前に期限切れの証明書を削除する必要があります。
- 次のフォルダにあるファイルは，設定データをインポートするときに上書きできません: **templates.os**，**templates.post**，**templates.health**，**templates.applications**，**conf\ems**。
- SiteScope 設定ツールで，データのエクスポート時にサーバ証明書とスクリプトを含めることがサポートされます。以前のバージョンの SiteScope からデータをエクスポートするときにサーバ証明書とスクリプトを含める方法については，「既存の SiteScope インストールのアップグレード」(74ページ)を参照してください。
- 4 GB を超えるメモリが必要な，負荷のかかった環境で SiteScope を使用する場合，次のようにして，サーバで JVM ヒープ・サイズを手動で増やす必要があります。

a. **SiteScope/bin/start-service** ファイルを開いて編集します。
b. 最後の行で， **-Xmx4096m** パラメータの値をより高い値に変更します。必要に応じて，最大 **-Xmx8192m**（8 GB の場合）まで増やします。

SiteScope 設定ツールを実行するには，次の手順を実行します。

1. SiteScope サーバで次のどちらかを実行します。
   a. グラフィック・モードで，<SiteScope install Directory>/bin/config_tool.sh を実行します。
   b. コンソール・モードで，<SiteScope install Directory>/bin/config_tool.sh -i console を実行します。

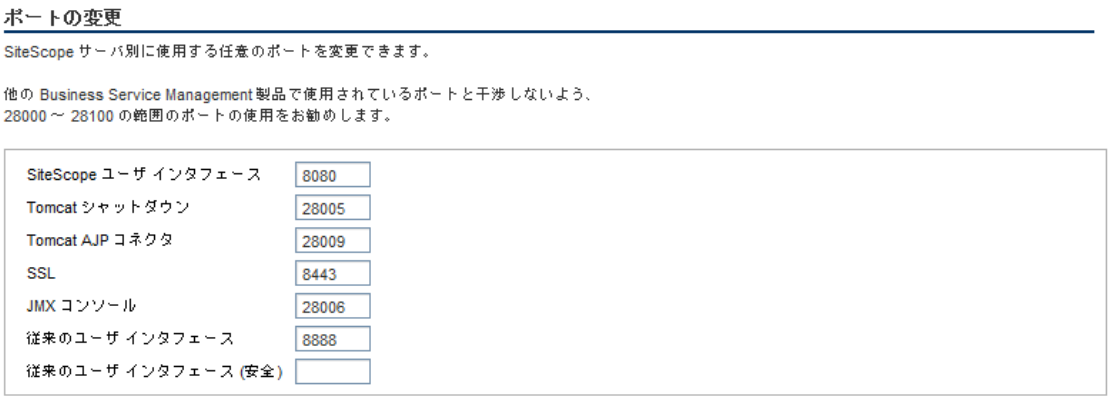
   SiteScope 設定ウィザードが開きます。

   ［**次へ**］をクリックします。
2. ［はじめに］画面で実行するアクションを選択してから，［**次へ**］をクリックします。

- **ポートの変更 :** SiteScope サーバで使用されるポートを変更できるようにします。詳細については，手順 3 を参照してください。
- **設定のインポート :** エクスポートされた設定データ（**.zip**）ファイル，または既存の SiteScope インストールから設定データをインポートできるようにします。詳細については，手順 5 を参照してください。
- **設定のエクスポート :** 後で SiteScope にインポートするために，現在の SiteScope からテンプレート，ログ，モニタ設定ファイルなどの SiteScope データをエクスポートできるようにします。詳細については，手順 4 を参照してください。
- **別個にインストールされた HP Operations Agent の設定:** HP Operations エージェントのインストールを完了するために必要です。エージェントによって，SiteScope が HP Operations Manager または BSM ゲートウェイ・サーバと統合されている場合に，イベントを送信し，メトリクス・データのデータ・ストレージとして機能するように SiteScope を設定できます。詳細については，手順 6 を参照してください。

注: このオプションは，HP Operations Agent 11.14 が SiteScope サーバにインストールされていない場合は無効になっています。エージェントのインストールと設定の詳細については，SiteScope ヘルプまたは HP ソフトウェア統合サイトにある『HP Operations Manager 製品との統合』ガイドを参照してください。

3. ［**ポートの変更**］オプションを選択した場合は，［ポートの変更］画面が開きます。



必要に応じて，SiteScope サーバで使用されるポートを変更します。ポート番号には，1 ～ 65534 の数字を指定する必要があります。従来のユーザ・インタフェースを除くすべてのコンポーネントで，ポートは必須です。

注: ほかの Business Service Management 製品で使用されるポートの妨げにならないように，28000 ～ 28100 の範囲のポートを使用することをお勧めします。

［**次へ**］をクリックして，ポートの変更操作を完了します。

4. ［**設定のエクスポート**］オプションを選択した場合，［設定のエクスポート］画面が開きます。

注: データをエクスポートする前に SiteScope サービスを停止し，データのエクスポート後にサービスを再起動する必要があります。詳細については，「Linux プラットフォームでの SiteScope プロセスの開始と停止」(198ページ)を参照してください。

- ［**SiteScope フォルダから**］ボックスに表示されている標準設定のディレクトリをそのまま使用するか，SiteScope インストール・ディレクトリの完全パスを入力します。たとえば，表示されているディレクトリ・パスを使用しない場合，インストール・ディレクトリのパスが /opt/9_0/SiteScope であれば，/opt/9_0/SiteScope と入力します。

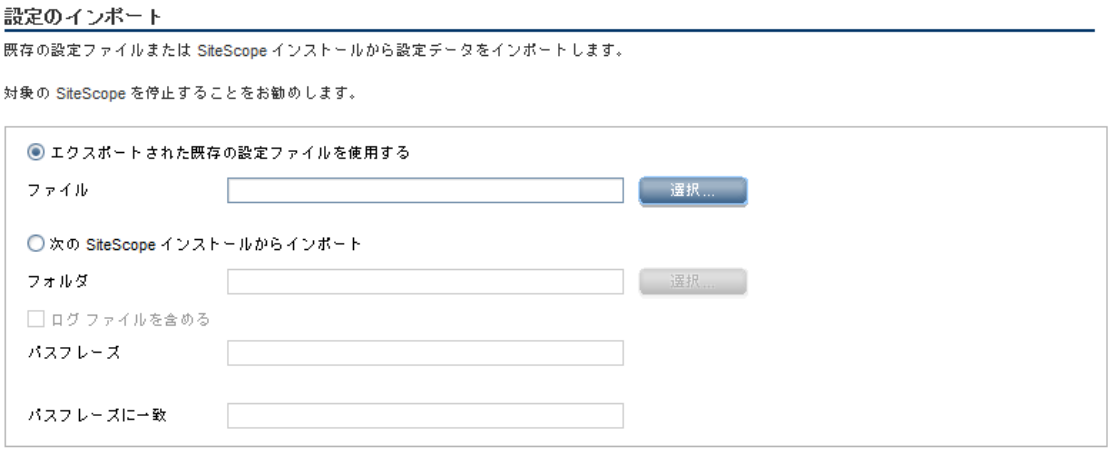
- ［**ファイル名**］に，ユーザ・データ・ファイルをエクスポートする既存のディレクトリ，およびエクスポートしたユーザ・データ・ファイルの名前を入力します。この名前は **.zip** で終わる必要があります。

- キー管理データ暗号化を使用して実行するように SiteScope が設定されていた場合，SiteScope サーバのキーストアに使用されるパスフレーズを**パスフレーズ** ボックスに入力します。詳細については，「データ暗号化にカスタム・キーを使用するための SiteScope の設定」(170ページ)を参照してください。このボックスは，標準設定の SiteScope 暗号化が使用される場合は無効です。

- ログ・ファイルもエクスポートする場合は，［**ログ ファイルを含める**］を選択します。

［**次へ**］をクリックして，エクスポート操作を完了します。

5. ［**設定のインポート**］オプションを選択した場合は，［設定のインポート］画面が開きます。



注: データをインポートする前に SiteScope サービスを停止し，データのインポート後にサービスを再起動する必要があります。詳細については，「Linux プラットフォームでの SiteScope プロセスの開始と停止」(198ページ)を参照してください。

- ［**エクスポートされた既存の設定ファイルを使用する**］を選択した場合は，インポートするユーザ・データの名前を入力します。

- ［**次の SiteScope インストールからインポート**］を選択する場合，ユーザ・データ・ファイルをインポートする SiteScope インストール・ディレクトリを入力します。

- ログ・ファイルもインポートする場合は，［**ログ ファイルを含める**］を選択します。

- キー管理データ暗号化を使用して実行するように SiteScope が設定されていた場合，SiteScope サーバのパスフレーズを**パスフレーズ** ボックスに入力します。［**パスフレーズに一致**］ ボックスに同じパスフレーズを入力して，パスフレーズを確定します。詳細については，「データ暗号化にカスタム・キーを使用するための SiteScope の設定」(170ページ)を参照してください。標準設定の SiteScope 暗号化を使用する場合，これらのボックスは無効です。

［**次へ**］をクリックして，インポート操作を完了します。

6. ［**別個にインストールされた HP Operations Agent の設定**］オプションを選択した場合は，［HP Operations Agent の設定］画面が開きます。

［**HP Operations Agent の設定**］を選択します。これは，HP Operations エージェントのインストールを完了するために必要です。エージェントによって，SiteScope が HP Operations Manager または BSM ゲートウェイ・サーバと統合されている場合に，イベントを送信し，メトリクス・データのデータ・ストレージとして機能するように SiteScope を設定できます。

イベントの送信およびメトリクス・データのレポートの詳細については，SiteScope ヘルプまたは HP ソフトウェア統合サイトにある『HP Operations Manager 製品との統合』ガイドを参照してください。

［**次へ**］をクリックして，設定操作を完了します。

7. ［サマリ］画面が開きます。

［**完了**］をクリックして，ウィザードを閉じます。

コンソール・モードでの設定ツールの実行

設定ツールは，コマンド・ラインまたはコンソール・モードを使用して実行できます。SiteScope をリモート・サーバに設定する場合，または，ユーザ・インタフェースを使用できない何らかの理由がある場合は，このオプションを使用します。

注:

- HP Operations Agent を SiteScope 内から直接インストールおよびアンインストールするオプションは，設定ツールから削除されました。代わりに，エージェントを手動でインストールして，設定する必要があります。SiteScope が HPOM または BSM と統合されている場合，エージェントでイベントを送信し，メトリック・データを保存する必要があります（BSM 内のプロファイル・データベースを使用してパフォーマンス・グラフ作成にメトリクス・データを使用する場合を除く)。エージェントのインストールと設定の詳細については，SiteScope ヘル

プまたは HP ソフトウェア統合サイトにある『HP Operations Manager 製品との統合』ガイドを参照してください。

- 次のフォルダにあるファイルは，設定データをインポートするときに上書きできません: **templates.os**，**templates.post**，**templates.health**，**templates.applications**，**conf\ems**。
- 4 GB を超えるメモリが必要な，負荷のかかった環境で SiteScope を使用する場合，次のようにして，サーバで JVM ヒープ・サイズを手動で増やす必要があります。
  a. **SiteScope/bin/start-service** ファイルを開いて編集します。
  b. 最後の行で， **-Xmx4096m** パラメータの値をより高い値に変更します。必要に応じて，最大 **-Xmx8192m**（8 GB の場合）まで増やします。

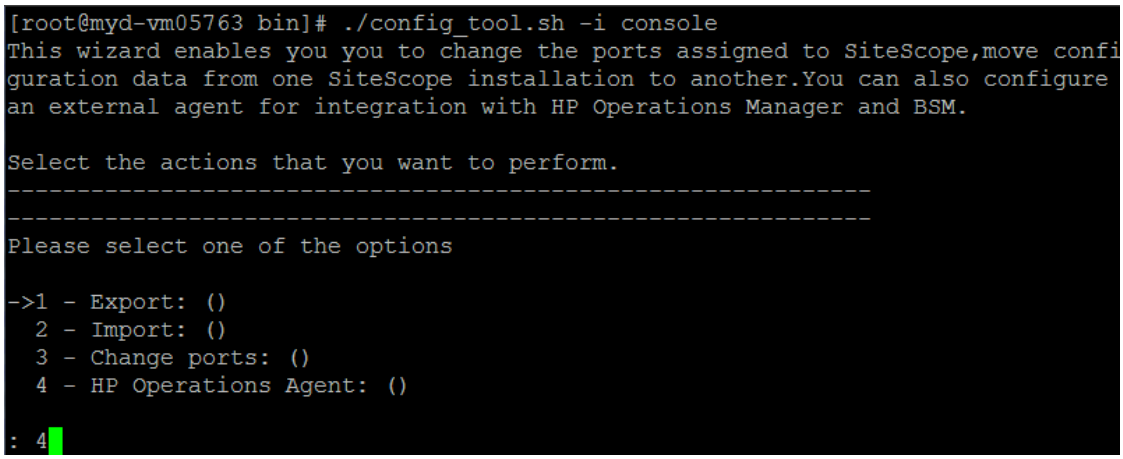
コンソール・モードで設定ツールを実行するには，次の手順を実行します。

注: 次の手順では，Linux 環境で設定ツールを実行する方法を示すスクリーン・キャプチャが示されています。

1. 次のコマンドを実行します。

   /bin/config_tool.sh -i console（Linux の場合），または <SiteScope root>\bin\config_tool.bat -i console（Windows の場合）。

2. 設定選択画面が表示されます。



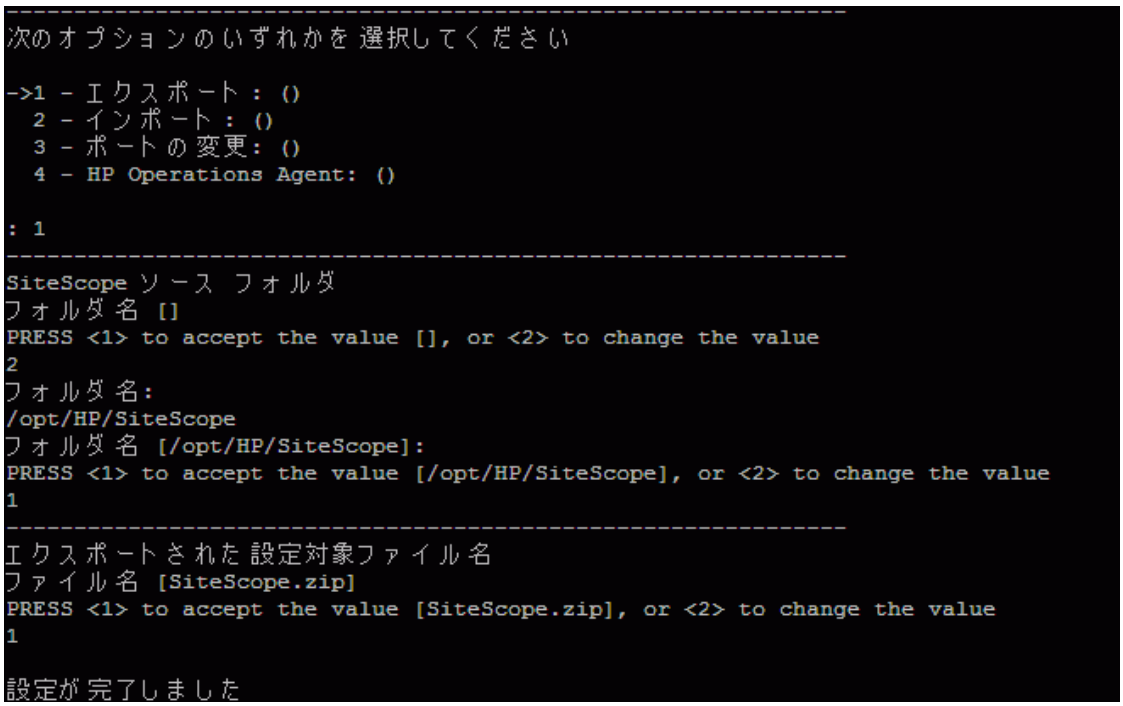
   実行する設定アクションを選択します。

   - SiteScope データをエクスポートするには，1 を入力します。
   - エクスポートされた設定データ（.zip）ファイル，または既存の SiteScope インストールから設定データをインポートするには，2 を入力します。
   - SiteScope サーバで使用するポートを変更するには，3 を入力します。
   - HP Operations Agent のインストールを完了するには，4 を入力します（エージェントによっ

て SiteScope がメトリクスとイベントを HP Operations Manager と BSM アプリケーションに送信できるようになります）。

ENTER キーを押して続行します。

3. ［**エクスポート**］オプションを選択した場合は，設定のエクスポート画面が開きます。



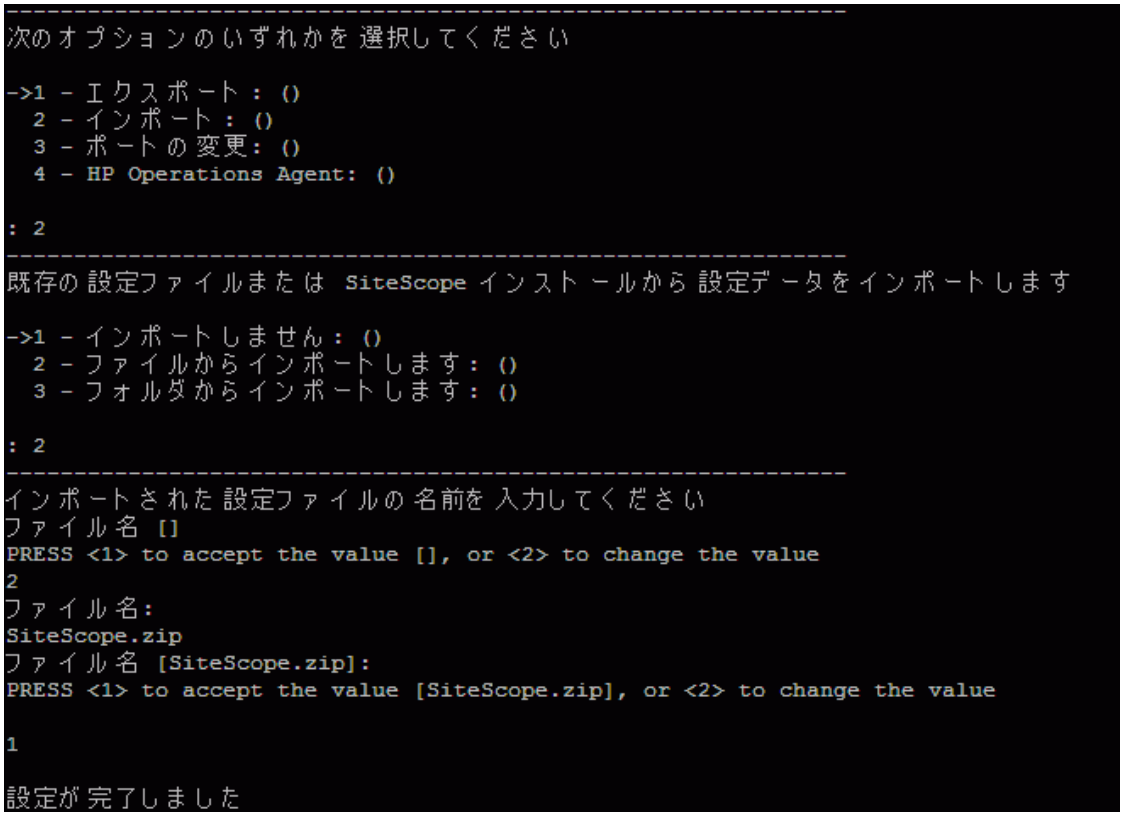
- **SiteScope ソース・フォルダ**については，次の手順を実行します。
  - [] で指定されたデフォルト・ディレクトリを受け入れるには，1 を入力します。
  - デフォルトの値を変更するには，2 を入力し，SiteScope インストール・ディレクトのフル・パスを入力します。たとえば，表示されているディレクトリ・パスを使用しない場合，インストール・ディレクトリのパスが /opt/HP/SiteScope であれば，/opt/HP/SiteScope と入力します。

  ENTER キーを押して，インストールを続行します。

- **エクスポートされた設定対象ファイル名**では，次の操作を実行します。
  - **SiteScope.zip** というファイルにデータをエクスポートするには，1 を入力します。
  - エクスポートされるユーザ・データ・ファイルの名前を変更するには，2 を入力します。この名前は **.zip** で終わる必要があります。

  ENTER キーを押して，エクスポート操作を完了します。

4. ［**インポート**］オプションを選択した場合は，設定のインポート画面が開きます。



次のように設定データ・オプションを選択します。

- 設定データをインポートしない場合は，1を入力します。
- ファイルから設定データをインポートするには，2 を入力します。このオプションを選択した場合は，次の操作を実行します。
  - [] で指定されたデフォルトのファイル名を受け入れるには，1 を入力します。
  - この値を変更するには，2 を入力し，設定データをインポートするファイルの名前を入力します。この名前をそのまま使用するには，1 を入力します。
- SiteScope インストール・ディレクトリから設定データをインポートするには，3 を入力します。このオプションを選択した場合は，次の操作を実行します。
  - [] で指定されたデフォルト・ディレクトリを受け入れるには，1 を入力します。
  - この値を変更するには，2 を入力し，ユーザ・データ・ファイルをインポートする SiteScope インストール・ディレクトリを入力します。この名前を受け入れるには，1 を入力します。

ENTER キーを押して，インポート操作を完了します。

注: インポートされた設定に期限切れの証明書が含まれている場合，設定のインポート時に標準設定の SiteScope キーストア内にマージされます。これにより，SSL 証明書のモ

ニタがエラー状態になる場合があります。これを回避するために，設定データをエクスポートする前に期限切れの証明書を削除する必要があります。

5. ［**ポートの変更**］オプションを選択した場合は，［ポートの変更］画面が開きます。

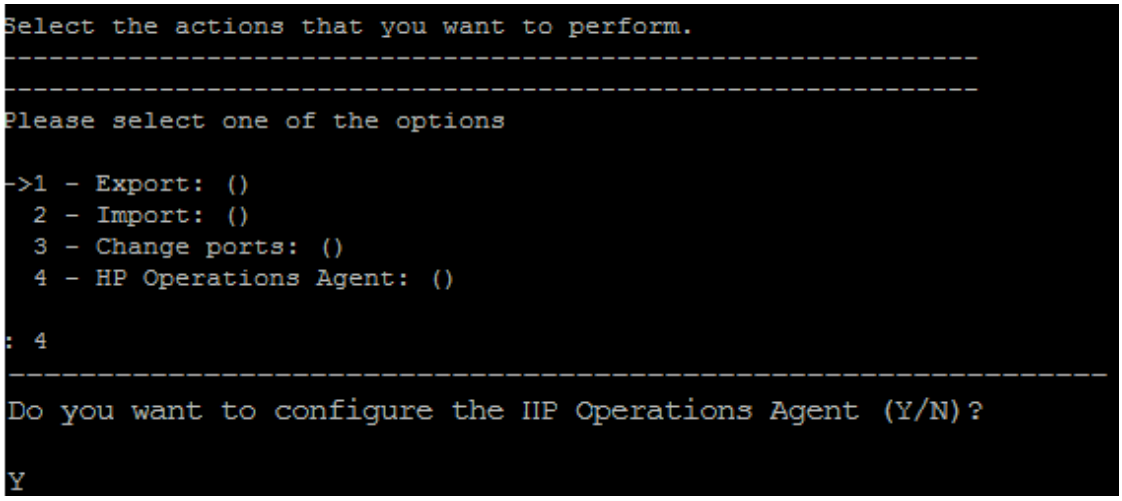
```
: 3
------------------------------------------------------------
SiteScope ユーザ インタフェース ポート
ポート [8080]
PRESS <1> to accept the value [8080], or <2> to change the value
1
------------------------------------------------------------
Tomcat シャットダウン ポート
ポート [28005]
PRESS <1> to accept the value [28005], or <2> to change the value
1
------------------------------------------------------------
Tomcat AJP コネクタ ポート
ポート [28009]
PRESS <1> to accept the value [28009], or <2> to change the value
1
------------------------------------------------------------
SSL ポート
ポート [8443]
PRESS <1> to accept the value [8443], or <2> to change the value
1
------------------------------------------------------------
JMX コンソール ポート
ポート [28006]
PRESS <1> to accept the value [28006], or <2> to change the value
1
------------------------------------------------------------
従来のユーザ インタフェース ポート
ポート [8888]
PRESS <1> to accept the value [8888], or <2> to change the value
1
------------------------------------------------------------
従来のユーザ インタフェース (安全) ポート
ポート []
PRESS <1> to accept the value [], or <2> to change the value
1

設定が完了しました
```

必要に応じて，SiteScope サーバで使用されるポートを変更します。ポート番号には，1 ~ 65534 の数字を指定する必要があります。従来のユーザ・インタフェースを除くすべてのコンポーネントで，ポートは必須です。

注: ほかの BSM 製品で使用されるポートの妨げとならないように，28000 ~ 28100 のポートを使用することをお勧めします。

ENTER キーを押して，ポート変更操作を完了します。

6. ［**HP Operations Agent**］オプションを選択した場合は，HP Operations Agent 画面が開きます。



Y を入力して，HP Operations Agent のインストールを完了します。

エージェントのインストールが完了したら，SiteScope サーバを再起動することをお勧めします。

HP Operations Agent を使用するメトリクス・データのレポートの詳細については，SiteScope ヘルプまたは HP ソフトウェア統合サイトにある『HP Operations Manager 製品との統合』ガイドを参照してください。

注: BSM でプロファイル・データベースを使用してパフォーマンスのグラフ作成を行うためにメトリクス・データを使用する場合，HP Operations Agent は必要ありません。プロファイル・データベースは，より強固で拡張性の高いデータ・ソースであり，HP Operations Integration を設定する必要がないため，推奨されるオプションです。

サイレント・モードでの設定ツールの実行

SiteScope 設定ツールをサイレント・モードで実行できます。これにより，［設定ツール］画面を移動して選択内容を入力しなくても，SiteScope の現在のバージョンから SiteScope 設定データのバックアップ・コピーを作成できます。入力する代わりに，すべての設定パラメータには，応答ファイルで定義する値が割り当てられます。

サイレント設定を実行する前の考慮事項

サイレント設定を実行する前に，次の点を考慮してください。

- サイレント・モードで設定を実行すると，メッセージはまったく表示されません。代わりに，設定が正常に完了したかどうかなどの設定情報が記録されたログ・ファイルを表示できます。設定ログ・ファイルは次の場所にあります。
  - Windows プラットフォームの場合 : **%tmp%\HPSiteScope_config_tool.log**
  - Linux プラットフォームの場合 : **/tmp/HPSiteScope_config_tool.log**
- SiteScope 間で設定データを移動する場合は，設定データの取得元の SiteScope サーバが，データ・インポート先の SiteScope サーバと同じタイム・ゾーン内にあることを確認してください。
- インポートされた設定に期限切れの証明書が含まれている場合，設定のインポート時に標準設定の SiteScope キーストア内にマージされます。これにより，SSL 証明書のモニタがエラー状態になる場合があります。これを回避するために，設定データをエクスポートする前に期限切れの証明書を削除する必要があります。
- SiteScope の同じバージョンに設定をインポートする場合，新しいテンプレート例がインポートされるように，すべてのテンプレート例コンテナの名前を変更するか，コンテナを削除する必要があります。
- データをエクスポートまたはインポートする前に SiteScope サービスを停止し，データのエクスポートまたはインポートの後にサービスを再起動する必要があります。詳細については，「Windows プラットフォームでの SiteScope サービスの開始と停止」(197ページ)および「Linux プラットフォームでの SiteScope プロセスの開始と停止」(198ページ)を参照してください。
- 次のフォルダにあるファイルは，設定データをインポートするときに上書きできません: **templates.os**，**templates.post**，**templates.health**，**templates.applications**，**conf\ems**。
- エクスポート設定オプションを選択した場合は，次の手順を実行します。
  - **\htdocs** ディレクトリは SiteScope データのエクスポート時にコピーされないため，このディレクトリのバックアップを作成し，アップグレード後にそれを SiteScope ディレクトリにコピーして，古いレポートを参照できるようにする必要があります。
  - 設定ツールで，データのエクスポート時にサーバ証明書とスクリプトを含めることがサポートされます。以前のバージョンの SiteScope からデータをエクスポートするときにサーバ証明書

とスクリプトを含める方法については，「既存の SiteScope インストールのアップグレード」(74ページ)を参照してください。

- サイズ設定オプション（Windows プラットフォームでのみ使用可能）を選択した場合は，次の手順を実行します。
  - サイズ設定の変更は，SiteScope サーバの物理メモリが，設定ツールによって設定された最大 JVM ヒープ・サイズ（Xmx）である 4 GB よりも大きい場合にのみ実行できます。
  - **go.bat** ファイルを **<SiteScope インストール>\bin ディレクトリ**で実行して SiteScope を起動する場合，**go.bat** ファイルを開いて，**-Xmx4096m** パラメータを必要に応じて最大 **-Xmx8192m**（8 GB の場合）まで増やします。
- ポートの変更オプションを選択した場合，ほかの Business Service Management 製品で使用されるポートの妨げにならないように，28000 ~ 28100 の範囲のポートを使用することをお勧めします。
- 4 GB を超えるメモリが必要な，負荷のかかった環境で SiteScope を使用する場合，次のようにして，サーバで JVM ヒープ・サイズを手動で増やす必要があります。
  a. **SiteScope/bin/start-service** ファイルを開いて編集します。
  b. 最後の行で， **-Xmx4096m** パラメータの値をより高い値に変更します。必要に応じて，最大 **-Xmx8192m**（8 GB の場合）まで増やします。
- HP Operations Agent を SiteScope 内から直接インストールおよびアンインストールするオプションは，設定ツールから削除されました。代わりに，エージェントを手動でインストールして，設定する必要があります。SiteScope が HPOM または BSM と統合されている場合，エージェントでイベントを送信し，メトリック・データを保存する必要があります（BSM 内のプロファイル・データベースを使用してパフォーマンス・グラフ作成にメトリクス・データを使用する場合を除く）。エージェントのインストールと設定の詳細については，SiteScope ヘルプまたは HP ソフトウェア統合サイトにある『HP Operations Manager 製品との統合』ガイドを参照してください。

サイレント設定の実行

configtoolparams.txt ファイルを使用して，サイレント設定を実行できます。このファイルは非常に特殊な形式であるため，**<SiteScope のインストール・ディレクトリ>\examples\silent_config_tool** フォルダにあるサンプル・ファイルを使用してサイレント設定ファイルを作成してください。

SiteScope のサイレント設定を実行するには，次の手順を実行します。

1. **<SiteScope インストール・ディレクトリ>\examples\silent_config_tool** フォルダにある **configtoolparams.txt** ファイルに移動します。
2. このファイルのコピーを作成し，任意の場所に保存します。
3. ファイルを開き，（サンプル・ファイルの説明に従って）設定のニーズに合わせて変更し，ファイルを保存します。
4. **-i silent** および **-f <answers file>** フラグを指定して，コマンド・ラインから設定を実行します。

   例 :

config_tool -i silent -f c:\configtoolparams.txt（Windows の場合）

または

./config_tool.sh -i silent -f /opt/configtoolparams.txt（Linux の場合）

第16章: SiteScope のアンインストール

本章の内容

- 「Windows プラットフォームからの SiteScope のアンインストール」(144ページ)
- 「Linux プラットフォームからの SiteScope のアンインストール」(145ページ)

Windows プラットフォームからの SiteScope のアンインストール

SiteScope 11.30 とその上にインストールされた任意のマイナー・マイナー・バージョン（パッチ）をサーバ・マシンからアンインストールすることも，SiteScope のマイナー・マイナー・バージョンのみをサーバ・マシンからアンインストールすることもできます。Windows プラットフォーム上で稼働している SiteScope の場合，SiteScope には，コンピュータから SiteScope ソフトウェアをアンインストールするためのプログラムが含まれています。

SiteScope とその上にインストールされた任意のマイナー・マイナー・バージョンのアンインストール方法

1. SiteScope サービスを停止します。
   a. ［**スタート**］ > ［**すべてのプログラム**］ > ［**管理ツール**］ > ［**サービス**］を選択します。［サービス］ダイアログ・ボックスが開きます。
   b. サービスの一覧から **SiteScope** サービスを選択します。SiteScope が稼働している場合は，右クリックして操作メニューを表示し，［**停止**］を選択します。サービスの［状態］に，サービスが停止したことが示されるまで待ってから，［サービス］ウィンドウを閉じます。
2. SiteScope をアンインストールします。
   a. ［**スタート**］ > ［**すべてのプログラム**］ > ［**HP SiteScope**］ > ［**HP SiteScope のアンインストール**］を選択します。
   b. ロケールの選択画面で，表示言語を選択して［**OK**］をクリックします。
   c. ［アプリケーションのメンテナンス］画面で，［**アンインストール**］を選択し，［**次へ**］をクリックします。
   d. ［プレアンインストールの概要］画面で，［**アンインストール**］をクリックします。

      アンインストール処理中は，各ソフトウェア・コンポーネントとそのアンインストールの進捗状況が画面に表示されます。

      アンインストール・プロセスが完了した時点で［アンインストールの完了］ウィンドウが開かれ，アンインストール・プロセスの概要が表示されます。
   e. ［アンインストール完了］ウィンドウで［**完了**］をクリックし，アンインストール・プログ

ラムを閉じます。

［**ログ ファイルを表示します**］リンクからアンインストール・ログ・ファイルにアクセスし，Web ブラウザで開くことができます。削除されたパッケージの詳細については，［詳細］タブをクリックしてください。

3. HP Operations Agent を設定解除してアンインストールします。

   SiteScope サーバにインストールされた HP Operations Agent を削除する場合は，HP Operations Agent を設定解除してからアンインストールする必要があります。

   a. HP Operations Agent を手動で設定解除するには，次のコマンドを実行します。

      i. msiexec /x <SiteScope root directory>\installation\components\oa_policy_signing_tool\win64\HPOprIAPA-09.00.111-Win5.2_64-release.msi /quiet

      ii. <SiteScope root directory>\installation\components\oa_template_management\all\install.bat -remove windows64

   b. SiteScope サーバにインストールされている Agent をアンインストールするには，『HP Operations Agent 11.14 インストール・ガイド』（https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM01001255）の説明を参照してください。

4. アンインストール・プロセスが完了したときに，要求された場合はマシンを再起動します。

Linux プラットフォームからの SiteScope のアンインストール

SiteScope 11.30 とその上にインストールされた任意のマイナー・マイナー・バージョン（パッチ）をサーバ・マシンからアンインストールすることも，SiteScope のマイナー・マイナー・バージョンのみをサーバ・マシンからアンインストールすることもできます。SiteScope が Linux プラットフォームで稼働している場合，SiteScope インストール環境には，SiteScope ソフトウェアをコンピュータからアンインストールするスクリプトが含まれています。スクリプトを実行できない場合は，SiteScope ファイルおよびディレクトリを手作業で削除します。

SiteScope とその上にインストールされた任意のマイナー・マイナー・バージョンのアンインストール方法

1. SiteScope ディレクトリでスクリプトを実行することが許可されているアカウントを使用して，SiteScope が稼働しているマシンにログオンします。通常は，SiteScope を実行しているアカウントを使用します。
2. **<インストール・パス>/SiteScope** ディレクトリに含まれている **stop** シェル・スクリプトを実行して SiteScope を停止します。スクリプトを実行するコマンド・ラインの例は，**SiteScope/stop** です。

   SiteScope が停止したことを示すメッセージが表示されます。

```
$
$ ./stop
Stopped SiteScope process (6252)
Stopped SiteScope monitoring process (6285)
$
```

3. X Windows モードで作業している場合は，次のコマンドを実行します。
   /opt/HP/SiteScope/installation/bin/uninstall.sh
4. コンソール・モードで作業する場合は，**/opt/HP/SiteScope/installation/bin/uninstall.sh -i console** コマンドを実行して SiteScope 11.30 をアンインストールします。
5. HP ソフトウェア・インストーラが起動します。ロケールを指定し，ENTER キーを押します。

```
Preparing to install...
Extracting the JRE from the installer archive...
Unpacking the JRE...
Extracting the installation resources from the installer archive...
Configuring the installer for this system's environment...
Preparing CONSOLE Mode Installation...

===============================================================================
Choose Locale...
----------------

    1- Deutsch
  ->2- English
    3- Fran?ais

CHOOSE LOCALE BY NUMBER: 2
===============================================================================
HP Software Installer
---------------------


PRESS <ENTER> TO CONTINUE: 2
```

6. 1 と入力して ENTER キーを押し，SiteScope をアンインストールすることを確定します。

```
===============================================================================
Maintenance Selection
---------------------

Modify, repair or uninstall the application
If you want to change something on a previous step, type 'back'.
You may cancel this installation at any time by typing 'quit'.



  ->1- Uninstall        Uninstall the application from your computer.

Please select one of the options...: 1
```

7. パッケージ・アンインストールの状態メッセージが表示され，アンインストールが完了します。

8. HP Operations Agent を設定解除してアンインストールします。

   SiteScope サーバにインストールされた HP Operations Agent を削除する場合は，HP Operations Agent を設定解除してからアンインストールする必要があります。

   a. HP Operations Agent を手動で設定解除するには，Linux ターミナルで次のコマンドを実行します。

      i. rpm -e HPOprIAPA

      ii. <SiteScope root directory>\installation\components\oa_template_management\all\install.sh -remove linux64

   b. SiteScope サーバにインストールされている Agent をアンインストールするには，『HP Operations Agent 11.14 インストール・ガイド』（https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM01001255）の説明を参照してください。

第4部: SiteScope の安全な稼働

第17章: SiteScope プラットフォームのセキュリティ強化

本章の内容

- 「概要」(149ページ)
- 「SiteScope ユーザ設定の設定」(149ページ)
- 「パスワードの暗号化」(150ページ)
- 「TLS（Transport Layer Security）を使用した SiteScope へのアクセス」(150ページ)
- 「スマート・カード認証」(150ページ)
- 「共通基準認定」(151ページ)
- 「FIPS 140-2 コンプライアンシー」(152ページ)
- 「カスタム・キーを使用したデータの暗号化」(152ページ)
- 「ユーザ・アカウントのセキュリティを保護するための推奨事項」(152ページ)
- 「ログイン時に表示される警告バナーの設定」(155ページ)

概要

本章では，SiteScope プラットフォームのセキュリティを強化するために使用できる，いくつかの設定オプションについて説明します。

SiteScope は，システムの可用性を監視するツールとして，セキュリティで保護する処置が取られていない場合に使用するとシステム・セキュリティを危険にさらす可能性のあるシステム情報にアクセスすることになります。本項に示す設定とセットアップ・オプションを使用して，SiteScope プラットフォームを保護する必要があります。

注意: 2 種類の SiteScope 製品インタフェースを提供するアクティブな Web サーバが 2 つあります（SiteScope Web サーバおよび SiteScope とともに提供される Apache Tomcat サーバ）。SiteScope へのすべてのアクセスを制限するには，これら両方のサーバに適切な設定を適用する必要があります。

SiteScope ユーザ設定の設定

SiteScope ユーザ・プロファイルは，SiteScope インタフェースにアクセスするためにユーザ名およびパスワードが要求された際に使用します。インストール後，SiteScope が稼働しているサーバに HTTP アクセスできるユーザは通常，SiteScope にアクセス可能になります。

標準設定では，SiteScope は 1 つのユーザ・アカウントとともにインストールされ，このアカウントには，標準設定のユーザ名またはパスワードは定義されません。これが管理者アカウントです。

製品のインストールおよびアクセス後，このアカウントにユーザ名とパスワードを定義する必要があります。また，ほかのユーザが製品へどのようにアクセスでき，どのアクションを実行できるかを制御するために，ほかのユーザのアカウント・プロファイルを作成することもできます。ユーザ・アカウントの作成の詳細については，SiteScope ヘルプの「SiteScope の使用」で「ユーザ管理プリファレンス」セクションを参照してください。

パスワードの暗号化

すべての SiteScope パスワードは，TDES（Triple Data Encryption Standard）と呼ばれる方法を使用して暗号化されます。TDES は，2 つまたは 3 つの異なる鍵を使用して，64 ビットのテキスト・ブロックごとに Data Encryption Algorithm を 3 重に適用します。その結果，不正ユーザが元のパスワードを複製することが非常に困難になります。

TLS（Transport Layer Security）を使用した SiteScope へのアクセス

SiteScope は，製品インタフェースへのアクセスを制御するために TLS を使用するように設定できます。詳細については，「セキュアな接続を経由して通信するための SiteScope の設定」(156ページ)を参照してください。

注: TLS（Transport Layer Security）は Secure Sockets Layer（SSL）の新しい名前です。現在でも SiteScope ユーザ・インタフェースでは SSL への参照が含まれています。SiteScope では，これらの用語は同じ意味で使用されています。

スマート・カード認証

スマート・カードはセキュアなシステムでユーザを識別するために使用する物理デバイスです。スマート・カードに証明書を格納しておくことで，ユーザ ID を確認し，セキュアな環境へのユーザのアクセスを許可できます。

SiteScope はスマートカードを使用したユーザ認証をサポートします。スマート・カード認証を設定すると，SiteScope にログインするのに有効なスマート・カードが必要になります。SiteScope では，次に示すさまざまなタイプのスマート・カードを使用できます。

- **CAC：** Common Access Card（通称 CAC カード）は，米国国防総省で使用されているスマート・カードです。米軍の政府関連システムで作業をする際には常に，このスマート・カードが必要になります。
- **PIV：** 軍と同様，連邦政府の職員や民間機関の請負業者にもスマート・カードが必要です。この用途には，CAC と類似の PIV カード（Personal Identification Verification）と呼ばれる標準規格が使用

されています。PIV カードが CAC と若干異なるのは，発行機関に応じて，さまざまな情報を書き込むことができる点です。PIV カードでは，CAC が使用しているのとは異なる一連の CA（認証局）サーバを使用します。PIV カードには，連邦施設や連邦情報システムの加入者へのアクセス許可，該当するすべての連邦アプリケーションにおける適切なレベルのセキュリティの確保，および各種標準規格を採用している連邦組織間の相互運用性の確保を実現するために，PIV システムで必要とされるユーザ別の固有のデータが書き込まれます。

スマート・カード認証の設定方法の詳細については，「スマート・カード認証の設定」(156ページ)を参照してください。

注: 市場には多数のスマート・カード・ベンダが存在します。クライアント証明書を使用するためのさまざまな組み合わせのすべてをサポートするため，**<SiteScope root>\groups\master.config** ファイルでは次の各パラメータを使用できます。

- _clientCertificateAuthJITCComplianceEnforcementEnabled
- _clientCertificateAuthSmartCardEnforcementEnabled
- _clientCertificateAuthIsGetUidFromSubject
- _clientCertificateAuthAllowLocalUsers
- _clientCertificateSubjectAlternativeNamesGeneralName
- _clientCertificateAuthEnabled

JITC（Joint Interoperability Test Command）認証

JITC は，軍部や政府の各部門で使用されるテクノロジをテストする米国軍の組織です。JITC は，グローバルな「ネット中心型の」軍事力を取得および配備するためのテスト，評価，および認証サービスを実施します。

SiteScope は現在，JITC によるテストと評価を受けています。JITC 認証は，CAC およびスマート・カードによる認証ログインをサポートするために必要な共通基準認定の 1 つです。

注: この項は，評価プロセスが完了次第，更新されます。

共通基準認定

HP SiteScope では，全業界標準および政府認定プログラムに準拠した業界をリードするモニタリング・ソフトウェアを提供できるように取り組んでいます。

HP SiteScope は，評価保証レベル（EAL）2+ の共通基準認定の取得過程にあります。共通基準のような認定が、連邦政府のセキュリティ政策にとって根本的に重要になります。今日の高度な攻撃およびデータ盗難から政府のカスタマを保護することに加えて，これらのセキュリティ認定は HP のグローバル・ビジネス・カスタマのニーズも同時に支援します。

IT セキュリティ評価の共通基準（略して共通基準といいます）はコンピュータ・セキュリティ認定の国際的な標準です。共通基準は製品が約束された機能を実行し，安全性と安定性の両方を満たす形で

構築されていることを立証するものです。結果の検証と評価は独立したテスト機関によって行われています。これはまた，セキュリティ製品の連邦としての購買に際してのU.S. 政府による要件です。

FIPS 140-2 コンプライアンシー

共通基準認定の目的において，SiteScope は FIPS 140-2 対応モードで動作するように設定できます。FIPS 140-2（Federal Information Processing Standard 140-2）は暗号化モジュールのセキュリティ要件です。FIPS 140-2 は，米国政府およびカナダ政府の両政府によって義務付けられた共同取り組みである CMVP（Cryptographic Module Validation Program）の監視下にあります。

現時点では，SiteScope 11.30 のみが FIPS 140-2 対応モードで機能するように設定可能な SiteScope のバージョンです。

FIPS 140-2，および SiteScope を FIPS 140-2 対応モードで動作するための設定に関する詳細については，「SiteScope が FIPS 140-2 対応モードで機能するための設定」(162ページ)を参照してください。

カスタム・キーを使用したデータの暗号化

標準設定では，SiteScope は標準の暗号化アルゴリズムを使用して永続データを暗号化します（永続データには，すべての定義済みのモニタ，グループ，警告，テンプレート，そのほかの SiteScope エンティティの設定データが含まれます）。強化ツールのキー管理を使用して，永続データの暗号化に使用する暗号化キーを変更できます。

詳細については，「データ暗号化にカスタム・キーを使用するための SiteScope の設定」(170ページ)を参照してください。

ユーザ・アカウントのセキュリティを保護するための推奨事項

次の表に，SiteScope で使用できるさまざまなアカウントとそれらのアカウントのセキュリティを保護するための手順を示します。

ユーザ・アカウント	説明	強化手順
標準設定（管理者）	標準設定では，SiteScope は 1 つのユーザ・アカウントとともにインストールされ，このアカウントには，標準設定のユーザ名またはパスワードは定義されません。	このアカウントとその権限へのアクセスを制限するため，製品をインストールおよび起動したら，ユーザのログイン名とログイン・パスワードを含めるように管理者アカウント・プロファイルを編集することをお勧めします。これによりログイン・

ユーザ・アカウント	説明	強化手順
		ページが表示されて，SiteScope にアクセス可能になります。 ほかのユーザについてもアカウント・プロファイルを作成して，ほかのユーザに与えられるアクセス許可と実行可能な操作を管理する必要があります。詳細については，SiteScope ヘルプの「SiteScope の使用」にある「ユーザ管理プリファレンス」セクションを参照してください。 **注 :** ほかのアカウントを作成するには，ユーザ・ログイン名およびパスワードを含めるように最初に管理者アカウント・プロファイルを編集する必要があります。
統合ビューア	標準設定では，HPOM イベントからのドリルダウンに使用する統合ビューア・ユーザが設定されます。これは，表示権限と，グループとモニタをリフレッシュする権限が与えられた正規ユーザです。詳細については，『HP Operations Manager 製品との統合』を参照してください。	すでに HPOM 統合または BSM 統合を行っている場合は，統合ビューア・アカウント・プロファイルの事前定義のログイン・パスワードを変更することをお勧めします。 HPOM / BSM 統合を行っていない場合は，このユーザを無効化または削除できます。
SiteScope サービス・ユーザ	**Windows の場合 :** 標準設定では，SiteScope はローカル・システム・アカウントで実行されるようにインストールされます（ただし，この標準設定は，Linux インストール環境には適用されません）。このアカウントはローカル・コンピュータに対する広範な権限を保持していて，ほとんどのシステム・オブジェクトにアクセスできます。ローカル・システム・アカウントの下で実行されている SiteScope は，SiteScope に設定されているサーバの資格情報を使用してリモート・サーバに接続しようと	**Windows の場合 :** ドメイン管理者権限を持つユーザとしてログオンするよう SiteScope サービスを設定することをお勧めします。 これにより，SiteScope にドメイン内のサーバ・データを監視するためのアクセス権限が付与されます。リモート・サーバにアクセスできるアカウントおよびパスワードを入力し，確認のためにパスワードを再入力します。ドメイン環境ではドメイ

ユーザ・アカウント	説明	強化手順
	します。 **Linux の場合：** Linux 環境では，SiteScope を root ユーザとしてインストールする必要があります。	ン管理者ユーザを，非ドメイン環境では組み込みの管理者ユーザを使用します。 この設定は，インストール中（「SiteScope のインストール」を参照），またはインストール後に変更できます。 詳細については，「インストール・ウィザードを使用してインストール」(95ページ)を参照してください。 **Linux の場合：** SiteScope がインストールされた後，SiteScope を実行する権限のある非 root ユーザ・アカウントを作成できます（SiteScope Web サーバが特権ポート上で実行されない限り，root ユーザが実行する必要はありません）。SiteScope を実行する権限のある非 root ユーザの設定の詳細については，「ユーザ・アカウントのセキュリティを保護するための推奨事項」(152ページ)を参照してください。
JMX ユーザ	JMX は，標準設定では，SiteScope サーバに対するリモート・アクセス権を保有しています（JMX プロトコルを使用した接続は強化ツールを使用して設定できます）。	SiteScope のセキュリティ保護を高めるため，強化ツールを使用して JMX によるリモート・アクセスを無効にすることをお勧めします。詳細については，「JMX リモート・アクセスを設定するための強化ツールの使用方法」(185ページ)を参照してください。
API ユーザ	一般に，このようなユーザは存在しません（SiteScope には，認証を必要としない多数の API が用意されています）。	古い未使用の API ユーザを無効にする必要がある場合は，［**プリファレンス**］＞［**インフラストラクチャ プリファレンス**］＞［**カスタム設定**］で［**古い API を無効化**］を true に設定

ユーザ・アカウント	説明	強化手順
		します。

ログイン時に表示される警告バナーの設定

ユーザが SiteScope にログオンするときにユーザに対して安全なシステムにログインしようとしていることを伝える警告メッセージを表示するように SiteScope を設定できます。

ログイン時に表示されるメッセージを設定するには，次の手順を実行します。

1. **<SiteScope のルート・ディレクトリ>\templates.fips\banner.txt** ファイルをテキスト・エディタで開き，ログイン・スクリーンで表示されるテキストを入力します。
2. **<SiteScope のルート・ディレクトリ>\groups\master.config** ファイルをテキスト・エディタで開き，プロパティ **_isLogonWarningBannerDisplayed=** の値を **true** に変更します。

   ユーザが SiteScope にログオンするときは常に，通知メッセージが表示されます。ユーザは SiteScope を使用可能な状態になる前にこのメッセージを確認する必要があります。

第18章: セキュアな接続を経由して通信するための SiteScope の設定

本章の内容

- 「セキュアな接続を必要とするようにするための SiteScope の設定」(156ページ)
- 「スマート・カード認証の設定」(156ページ)
- 「証明書の失効を検証するための SiteScope の設定」(158ページ)

セキュアな接続を必要とするようにするための SiteScope の設定

インタフェース（UI および API）へのセキュアなアクセスを必要とするよう SiteScope を設定できます。この操作は次によって行います。

1. SiteScope サーバの FQDN に対して発行されたサーバ証明書を取得します。
2. セキュアなチャネルのみからのアクセス要求に応答するよう SiteScope を設定します。

これは次のいずれかによって行えます。

- 強化ツールを使用して，SiteScope がこの設定を実行するように設定します（推奨される方法）。詳細については，「セキュアな接続を要求するように SiteScope を構成するための強化ツールのを使用方法」(178ページ)を参照してください。
- SiteScope を TLS を使用するように手動で設定する。詳細については，「セキュア接続を使用するための SiteScope の手動による設定」(219ページ)を参照してください。

スマート・カード認証の設定

スマート・カードはセキュアなシステムでユーザを識別するために使用する物理デバイスです。スマート・カードに証明書を格納しておくことで，ユーザ ID を確認し，セキュアな環境へのユーザのアクセスを許可できます。

SiteScope はスマートカードを使用したユーザ認証をサポートします。スマート・カード認証を設定すると，SiteScope にログインするのに有効なスマート・カードが必要になります。

SiteScope は，各ユーザが手動でユーザ名とパスワードを入力する標準的な形式の代わりに，これらの証明書を使用するよう設定できます。各カードに保存されている証明書からユーザ名を抽出する方法を定義します。

SiteScope でスマート・カード認証の設定がされている場合，ユーザは有効なスマート・カードでのみ SiteScope にログインできます。手動でユーザ名とパスワードを入力してログインするオプションは，スマート・カードの設定が無効にならない限り，すべてのユーザに対してロックされます。

スマート・カード認証が BSM で設定されていて，SiteScope を BSM と統合する場合，SiteScope スマート・カード認証を BSM クライアント証明書を認証するよう設定する必要があります。詳細については，「セキュア接続が必要な BSM サーバに SiteScope を接続する設定」(174ページ)を参照してください。

同様に，SiteScope でスマート・カード認証の設定がされていて，BSM を SiteScope と通信可能にしようという場合，最初に BSM を SiteScope のクライアント証明書で認証するよう設定する必要があります。詳細については，「セキュア接続が必要な BSM サーバに SiteScope を接続する設定」(174ページ)を参照してください。

注 : スマート・カード強制が有効の場合，サポートされているブラウザは Windows オペレーティング・システムで実行している Internet Explorer のみになります。

スマート・カード強制が無効で，クライアント証明書認証が有効になっている場合に Firefox で SiteScope を使用するには，「クライアント証明書が有効な場合の Firefox の使用」(158ページ)を参照してください。

ヒント: スマートカードの詳細については，『Smart Card Authentication Configuration Guide』（https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM01134341）を参照してください。

クライアント証明書認証を必要とするよう SiteScope を設定

SiteScope を TLS で機能するよう設定した場合（「セキュアな接続を必要とするようにするための SiteScope の設定」(156ページ)を参照），クライアント証明書認証を必要とするように SiteScope と SiteScope 公開 API クライアントを設定できます。

この操作は，強化ツールを使用することによって行えます。詳細については，「SiteScope と SiteScope パブリック API クライアント証明書認証を設定するための強化ツールの使用方法」(184ページ)を参照してください。

第19章: 高度な強化設定

本章の内容

- 「証明書の失効を検証するための SiteScope の設定」(158ページ)
- 「クライアント証明書が有効な場合の Firefox の使用」(158ページ)
- 「認証局証明書の SiteScope トラストストアへのインポート」(159ページ)
- 「JMX リモート・アクセスの無効化」(159ページ)
- 「バックアップした設定の復元」(159ページ)
- 「SiteScope でのフレーミング・フィルタの設定」(160ページ)

証明書の失効を検証するための SiteScope の設定

クライアント証明書の失効を検証するよう SiteScope を設定するには強化ツールを使用します。詳細については，「証明書の失効を確認するように SiteScope を設定するための強化ツールの使用方法」(179ページ)を参照してください。

クライアント証明書が有効な場合の Firefox の使用

スマート・カード強制が無効で，クライアント証明書認証が有効になっている場合，Firefox で SiteScope ユーザ・インタフェースを開くには，次の手順を実行する必要があります。

1. ユーザ個人の証明書を，次のように Firefox にインポートします。
   a. Firefox では，［**ツール**］>［**オプション**］>［**詳細**］>［**暗号化**］>［**証明書を表示**］に移動します。［証明書マネージャ］ダイアログ・ボックスが開きます。
   b. ［**インポート...**］をクリックして，ユーザ個人の証明書を **.pfx**（または**.p12**）ファイル形式で開きます。［パスワード入力］ダイアログ・ボックスが開きます。
   c. この証明書のバックアップを暗号化するためにパスワードを入力して，［**OK**］をクリックします。証明書は，［証明書マネージャ］ダイアログ・ボックスに表示され，証明書が Firefox に追加されていることを確認します。
2. ユーザ個人の証明書を，次のようにクライアント JRE にインポートします。
   a. JRE で，Java コントロール・パネルを開きます。
   b. ［**セキュリティ**］>［**証明書**］に移動して，証明書のタイプとして［クライアント認証］を選択します。
   c. ［**インポート**］をクリックして，Firefox にインポートしたクライアント証明書を開きま

す。

d. ［**OK**］をクリックします。 個人の証明書が JRE に表示されます。

3. SiteScope URL を Firefox に入力します。［ユーザ識別のリクエスト］ダイアログ・ボックスが開きます。手順 1 で作成した個人の証明書を識別として選択します。

認証局証明書の SiteScope トラストストアへのインポート

SiteScope がクライアント証明書を信頼するには，SiteScope がクライアント証明書を発行した認証局を信頼する必要があります。SiteScope が認証局を信用するには，認証局の証明書が SiteScope サーバとメイン・トラストストアに保存されている必要があります。

SiteScope サーバ・トラストストアは，クライアント（APIおよびブラウザ）からのすべての受信接続要求の認証を担います。

SiteScope メイン・トラストストアは，SiteScope インストール・ディレクトリの Java ディレクトリに位置している，認証局の Java トラストストアです。トラストストアは，SiteScope 証明書管理を担います。

認証局証明書を SiteScope サーバおよびメインのトラストストアにインポートするには，強化ツールを使用します。詳細については，「認証局の証明書を SiteScope トラストストアにインポートするための強化ツールの使用方法」(181ページ)を参照してください。

JMX リモート・アクセスの無効化

JMX は標準設定で SiteScope サーバへのリモート・アクセスが可能です。このアクセスを無効にできます。

注: SiteScope のセキュリティを完全にするには，JMX リモート・アクセスを無効にすることをお勧めします。

JMX リモート・アクセスを設定するために強化ツールを使用します。詳細については，「JMX リモート・アクセスを設定するための強化ツールの使用方法」(185ページ)を参照してください。

バックアップした設定の復元

強化ツールを実行すると，既存の SiteScope 設定は自動的にバックアップされます。バックアップされた設定を復元するには，「バックアップ済みの設定を復元するための強化ツールの使用方法」(185ページ)を参照してください。

SiteScope でのフレーミング・フィルタの設定

注: このトピックは，SiteScope 11.30 IP1 をインストールした場合のみを対象にしています。

フレームは，コンテナに依存しないコンテンツを表示する Web ページまたはブラウザのウィンドウの一部で，独自にコンテンツを読み込むことができます。SiteScope のフレーミングは，標準設定で有効になっています。

他のサイトによる SiteScope のフレーミングを許可しない場合，または部分フレーミングのみを許可する場合は，次の手順を実行する必要があります。

1. **<SiteScope root directory>\groups** にある **master.config** ファイルを開き，必要に応じて **_disableFramingFiltering** プロパティを設定します。
   - **True :** フィルタが無効になり，すべての Web ページからの SiteScope のフレーミングが許可されます（これは標準設定です）。
   - **False :** フィルタが有効になり，BSM，HPOM，Performance Center などの HP 製品を含む Web ページからの SiteScope のフレーミングが禁止されます。たとえば，BSM がホストするユーザ・インタフェースは動作しなくなります。
   - **スマート : _framingFilteringPlugsClasses** プロパティにリストされているプラグに基づいて，SiteScope の部分フレーミングが有効になります。
2. 部分フレーミングを使用する場合は，フィルタによって適用するプラグを作成し，そのプラグを **_framingFilteringPlugsClasses** プロパティに追加します。
   a. **master.config** ファイルの **_framingFilteringPlugsClasses** プロパティに移動します。標準設定では，このプロパティには次の設定済みのプラグが含まれます。
      - com.mercury.sitescope.web.request.framing.plugs.LWSSOPlug。ライトウェイト・シングル・サインオン（LW-SSO）トークンで要求を送信できます。
      - com.mercury.sitescope.web.request.framing.plugs.BSMPlug。BSM の SAM 管理から要求を送信できます。
      - com.mercury.sitescope.web.request.framing.plugs.PerformanceCenterPlug。Performance Center からの要求を許可します。

      設定済みのプラグは，プロパティから削除することによって無効にできます。
   b. 独自のプラグを追加するには，次の手順を実行します。
      i. インタフェースを実装する必要があるプラグを記述します。
      com.mercury.sitescope.web.request.framing.IFramingPlug

      このインタフェースは，**<SiteScope root directory>\WEB-INF\lib\ss_webaccess.jar** にあります。プラグをコンパイルするには，この jar を classpath に配置する必要があります。

要求名を *exampleParameter* としたパラメータを true に設定した場合に、パラメータのフレーミングを許可するプラグの例を次に示します。

```
package com.company.sitescope.examples.plug
import javax.servlet.ServletRequest;
import com.mercury.sitescope.web.request.framing.IFramingPlug;
public class ExamplePlug implements IFramingPlug{
  @Override
    public boolean isAuthorized(ServletRequest request) {
      //この要求が認証された製品から送信されているかどうかを判定するコードを追加します。
      if (request == null){
         return false;
      }
      HttpServletRequest httpServletRequest = (HttpServletRequest)request;
      if (httpServletRequest.getParameter("exampleParameter") == null){
      return false;
      }

      return "true".equalsIgnoreCase((String)httpServletRequest.getParameter("exampleParameter"));
      }
}
```

ii. クラスの完全修飾名を **master.config** ファイルの **_framingFilteringPlugsClasses** プロパティに追加します（カンマで区切ります）。

たとえば，com.company.sitescope.examples.plug.ExamplePlug をリストに追加する必要があります。

iii. 独自に作成したすべてのプラグを含む jar を作成し，それを **<SiteScope ルート・ディレクトリ>\WEB-INF\lib** フォルダに追加します。

3. SiteScope を再起動します（**master.config** ファイルを変更したときは必須です）。

第20章: SiteScope が FIPS 140-2 対応モードで機能するための設定

本章の内容

- 「FIPS 140-2 コンプライアンシーの概要」(162ページ)
- 「FIPS 140-2 対応モードの有効化」(163ページ)
- 「FIPS 140-2 対応モードの無効化」(168ページ)
- 「トラブルシューティングおよび制限事項」(168ページ)

FIPS 140-2 コンプライアンシーの概要

FIPS 140-2（Federal Information Processing Standard）は，米国政府およびカナダ政府の暗号化および暗号化モジュールに対する認定標準です。この標準では，ソリューション全体に含まれる個々の暗号化コンポーネントに対して個別の認定が求められます。この標準は，コンピュータ・システムで使用されるプロシージャ，アーキテクチャ，アルゴリズムおよびその他の手法を定義するために開発されました。完全な FIPS ドキュメントは，National Institute of Standards and Technology（NIST）からオンラインで入手できます。

FIPS 140-2 対応モードで運用するには，SiteScope 管理者が SiteScope 強化ツールを使用して FIPS 140-2 モードを有効にする必要があります。SiteScope は，起動時に自己テストを実行し，暗号化モジュールの整合性チェックを実行してから，キーイング・マテリアルを再生成します。これにより，SiteScope が FIPS 140-2 モードで動作します。

FIPS モードを有効にする理由：

組織は，次の場合に SiteScope を FIPS モードで使用する必要があります。

- 連邦政府の機関または請負業者である場合。
- 高度な攻撃やデータ窃盗からビジネスを保護するためにセキュリティを強化する場合。

ソフトウェア要件

FIPS コンプライアンスでは，オペレーティング・システムおよびブラウザがバージョンおよび設定について特定の要件を満たす必要があります。

SiteScope でサポートされるすべてのブラウザは FIPS モードに対応しますが，オペレーティング・システムのすべてが FIPS の要求する暗号化要求を処理できるわけではありません。その結果，SiteScope が通常サポートするオペレーティング・システムの一部が FIPS モードに対応しません。

FIPS モードで動作するには，次のオペレーティング・システムのいずれかに SiteScope がインストールされている必要があります。

- Windows Server 2008 R2（64-ビット）

- Windows Server 2012 R2（64-ビット）

JDBC ドライバ

SiteScope を FIPS モードで実行するには，SiteScope に付属する標準設定のドライバの代わりに JDBC ドライバを使用することを考慮する必要があります。

FIPS 非対応アプリケーションに接続された SiteScope

FIPS が認定していないアルゴリズムを使用するアプリケーションに SiteScope が接続されている場合，SiteScope とそのアプリケーション間の接続は FIPS 準拠ではありません（FIPS-140-2 モードが SiteScope で有効化されている場合でも）。

FIPS 140-2 対応モードの有効化

セキュア接続を使用するときに FIPS 140-2 対応モードで実行するように SiteScope を有効化するには，次の手順を実行する必要があります。

- 「手順 1 :LDAP 統合の設定」(163ページ)
- 「手順 2 :FIPS 140-2 対応モード用の Windows オペレーティング・システムの設定」(164ページ)
- 「手順 3 :SiteScopeHardeningToolRuntime の実行 」(165ページ)
- 「手順 4 :SiteScope サーバへの JMX リモート・アクセスの無効化 」(165ページ)
- 「手順 5 :SSL の設定」(166ページ)
- 「手順 6 :クライアント認証の設定」(167ページ)

注: キー管理データ暗号化を有効にする場合（標準の暗号化よりも強度の高い暗号化），FIPS 140-2 モードを有効化または無効化した後にこの手順を実行する必要があります。キー管理データ暗号化をすでに設定している場合は，「暗号化キーを変更した後に FIPS 対応モードを有効化または無効化する方法」(172ページ)の手順に従う必要があります。

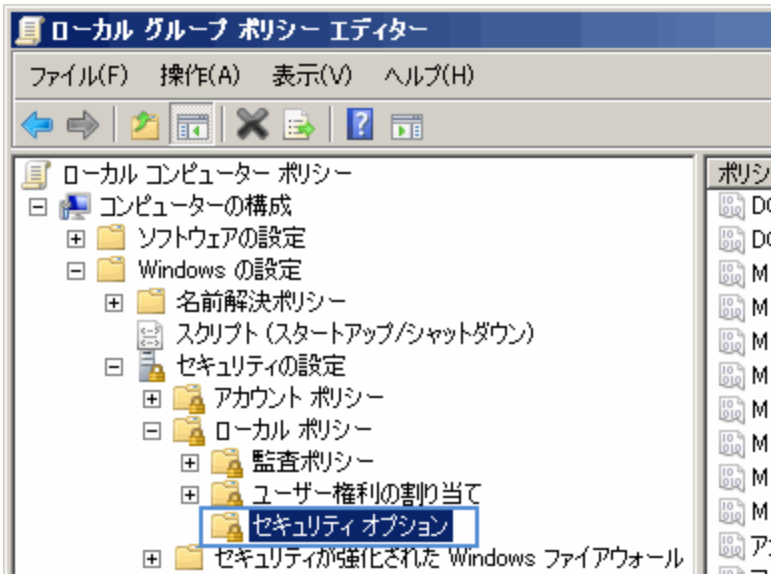
手順 1 :LDAP 統合の設定

LDAP ユーザの認証を有効化して，クライアント証明書を使用して SiteScope にログインする必要があります。

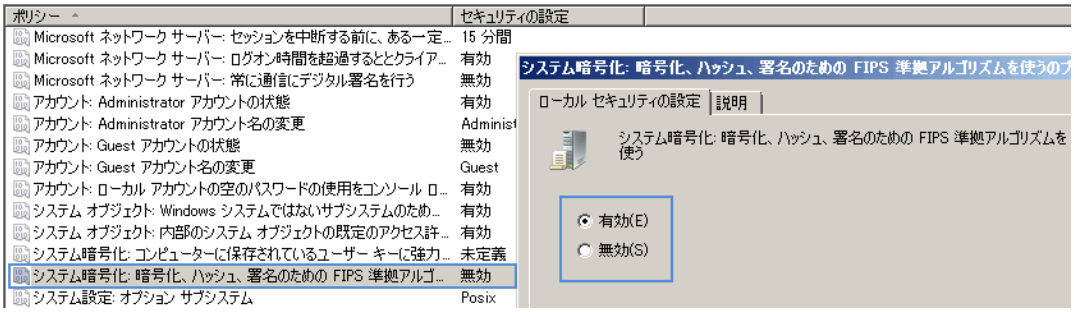
1. SiteScope 上で LDAP サーバを設定します。詳細については，SiteScope ヘルプにある SiteScope の使用ガイドの「SiteScope が LDAP 認証を使用するように設定する方法」を参照してください。
2. LDAP ユーザの SiteScope ユーザ管理で新規ロールを作成します。
3. SiteScope 管理者のログイン名を LDAP に存在するユーザの電子メールに変更します。これは，クライアント証明書のユーザと同じである必要があります（「手順 6 :クライアント認証の設定」(167ページ)の手順 3 で入力したユーザ)。パスワードは入力しないでください。

手順 2 :FIPS 140-2 対応モード用の Windows オペレーティング・システムの設定

1. FIPS 140-2 対応モード用に Windows オペレーティング・システムを設定します。
   a. 管理資格情報を使用してコンピュータにログオンします。
   b. ［**スタート**］ > ［**ファイル名を指定して実行**］をクリックし，「gpedit.msc」と入力して ENTER キーを押します。ローカル・グループ・ポリシー・エディタが開きます。
   c. ローカル・グループ・ポリシー・エディタで，**コンピュータの構成**ノードの［**Windows の設定**］をダブルクリックし，［**セキュリティの設定**］をダブルクリックします。
   d. ［**セキュリティの設定**］ノードで，［**ローカル ポリシー**］をダブルクリックし，［**セキュリティ オプション**］をクリックします。



   e. 詳細ペインで，［**システム暗号化: 暗号化、ハッシュ、署名のための FIPS 準拠アルゴリズムを使う**］をダブルクリックします。
   f. ［システム暗号化: 暗号化、ハッシュ、署名のための FIPS 準拠アルゴリズムを使う］ダイアログ・ボックスで，［**有効**］をクリックし，［**OK**］をクリックしてダイアログ・ボックスを閉じます。



g. ローカル・グループ・ポリシー・エディタを閉じます。

h. このセキュリティ・オプションが有効化されたことを確認します。

i. レジストリ・エディタを開きます。［**スタート**］ > ［**ファイル名を指定して実行**］をクリックし，「regedit」と入力して ENTER キーを押します。レジストリ・エディタが開きます。

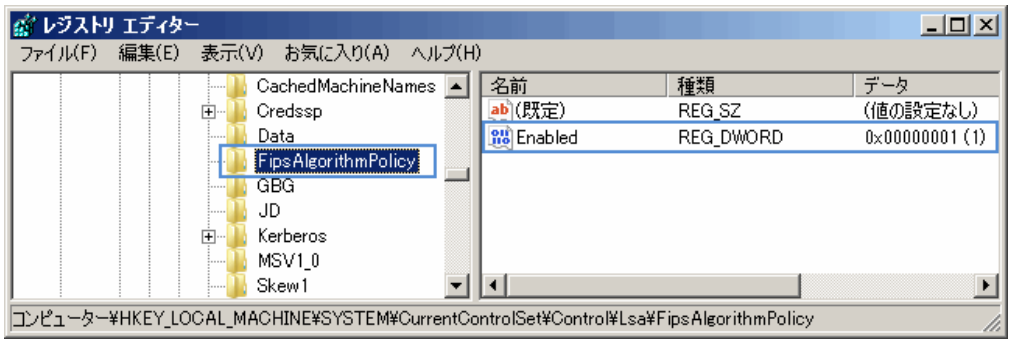
ii. 次のキーを見つけ，値を確認します。

- キー :**HKLM\System\CurrentControlSet\Control\Lsa\FIPSAlgorithmPolicy\Enabled**.

  このレジストリ値は現在の FIPS 設定を反映しています。この設定が有効な場合の値は 1 です。設定が無効な場合は 0 です。

- 値 : **1**.

iii.



ヒント: 追加の情報については，次を参照してください。

- http://technet.microsoft.com/en-us/library/cc750357.aspx
- http://support.microsoft.com/kb/811833

手順 3 :SiteScopeHardeningToolRuntime の実行

1. **SiteScopeHardeningToolRuntime.zip** ファイルを SiteScope インストーラ・パッケージの **\Tools** フォルダから SiteScope サーバにコピーします。

   a. ファイルの内容を **<SiteScope ルート・ディレクトリ>\tools\SiteScopeHardeningTool** フォルダに抽出します。

   b. 次のコマンド・ラインを実行して強化ツールを起動します。

   <SiteScope ホーム・ディレクトリ>\tools\SiteScopeHardeningTool\runSSLConfiguration.bat

手順 4 :SiteScope サーバへの JMX リモート・アクセスの無効化

強化ツールを使用して，SiteScope サーバへの JMX リモート・アクセスを無効化します。

1. 強化ツールを実行します。詳細については，「強化ツールの実行方法」(176ページ)を参照してください。

2. ［JMX リモート アクセスの設定］オプションを選択します。
3. ツールの指示に従って，JMX リモート・アクセスを無効化します。

ヒント: 設定の変更は，強化ツールを終了した後，有効になります。

手順 5 :SSL の設定

1. 次のコマンド・ラインを実行して強化ツールを起動します。

   <SiteScope ホーム・ディレクトリ>\tools\SiteScopeHardeningTool\runSSLConfiguration.bat
2. 1 を入力して，［SiteScope の強化設定］オプションを選択します。
3. 作成するバックアップ・ファイルに使用する名前を入力します。この手順は，FIPS 140-2 モードを無効化し，強化ツールを実行する前に存在していた前の SiteScope 設定を復元する場合に必要です。詳細については，「FIPS 140-2 対応モードの無効化」(168ページ)を参照してください。
4. 2 を入力して，［SSL（https）上で機能するように SiteScope スタンドアロンを設定する］オプションを選択します。
5. y を入力して，SSL 上で機能するように SiteScope を設定することを確認します。
6. y を入力して，SiteScope をFIPS 140-2 対応にすることを確認します。
7. FIPS 140-2 対応モードが正常に設定されたら，次の方法のいずれかを選択して，SiteScope サーバ証明書を保持するための SiteScope サーバ・キーストアを作成します。
   - **.pkcs12 形式のサーバ・キーストアをインポートします。**

     ツールで，SiteScope SSL 認証のキーが存在する別名を選択するように求められます。

     注: クライアント証明書認証用に後で SiteScope と SiteScope パブリック API クライアントを設定する場合（「クライアント証明書認証を必要とするよう SiteScope を設定」(157ページ)を参照），SiteScope はこの別名を使用して SiteScope API のクライアント・トラストストアにキーをエクスポートします。

     ツールの指示に従います。

   - **認定された証明書認証サーバで要求に署名することで，サーバのキーストアを作成します。**

     このオプションを選択すると，新しいキーストアが作成され，署名済みの証明書の認証局に対するキー要求が生成されます。その後，生成された証明書はキーストアにインポートされます。

     ツールによって，サーバのキーストア・パラメータを入力するように求められます。一般名には，マシンで使用しているものと同じ URL（FQDN を使用している場合はそれを含める）を入力し（例 : yourserver.domain.com），別名には，マシンの名前（例 : yourserver）を入力する必要があります。
8. 署名済みの SiteScope サーバ証明書をコピーして，認証局サーバによって署名された証明書を作成します。
9. 認証局サーバから受信した署名済みの証明書への完全パスを入力します。

10. 上記の証明書の発行に使用したルート CA 証明書への完全パスを入力します。
11. yes と入力して，認証局サーバから受信した証明書を信頼することを示します。証明書が SiteScope サーバ・キーストアに追加されます。

手順 6:クライアント認証の設定

1. クライアント証明書認証の SiteScope サーバ・トラストストアのパスワードを入力します。パスワードは少なくとも 6 文字の長さである必要があり，特殊文字を含めることができません。標準設定のパスワードは changeit です。
2. Y を入力して，クライアント証明書認証を有効にすることを確認します。

   クライアント認証を有効にすると，SiteScope で，ハンドシェイク時に完全なクライアント認証が実行され，クライアント証明書が抽出されます。このクライアント証明書は，SiteScope ユーザ管理（LDAP）システムで照合されチェックされます。詳細については，「手順 1 :LDAP 統合の設定」(163ページ)を参照してください。
3. クライアント証明書 AlternativeSubjectName フィールドにクライアント証明書の username プロパティを入力します。標準設定の username は Other Name です。
4. Y を入力して，スマート・カードの実施を有効にすることを確認します。

   スマート・カードの実施を有効にすると，SiteScope でクライアント証明書がハードウェア・デバイスから発行されたことが検証され，SiteScope トラストストアに追加されます。

   スマート・カードの実施の詳細については，「スマート・カード認証の設定」(156ページ)を参照してください。
5. Enter Y を入力して，CA 証明書を SiteScope トラストストアに追加することを確認します。

   注: SiteScope がクライアント証明書を信頼するには，SiteScope がクライアント証明書を発行した認証局を信頼する必要があります。SiteScope が認証局を信頼するには，認証局の証明書が SiteScope サーバのトラストストアにインポートされている必要があります。
6. CER 形式のルート CA 証明書への完全パスを入力します。
7. CA 証明書が SiteScope トラストストアに追加されます。

   証明書がキーストアにすでに存在する場合は，メッセージが表示されます。yes と入力して，証明書を SiteScope トラストストアに追加することを確認します。
8. （任意）SiteScope サーバのトラストストアに追加の CA 証明書を追加するには，Y を入力し，手順 1 ~ 3 を繰り返します。

   注: 追加の CA 証明書は不要です。
9. Q を入力して，強化ツール・プロセスを完了します。

FIPS 140-2 対応モードの無効化

FIPS 140-2 対応モードが有効な状態でセキュア接続を使用している場合は，強化ツールの FIPS の無効化オプションを使用して，FIPS 140-2 対応モードを無効にすることはできません。代わりに，FIPS が有効にされた以前に存在していた SiteScope 設定を復元する必要があります。

非セキュア接続を使用して FIPS 140-2 対応モードを有効化した場合は，強化ツールの FIPS 140-2 対応モード無効化オプションを使用します。

セキュア接続の FIPS 140-2 対応モードの無効化

1. 次のコマンド・ラインを実行して強化ツールを起動します。
   <SiteScope ホーム・ディレクトリ>\tools\SiteScopeHardeningTool\runSSLConfiguration.bat
2. 2 を入力して，［バックアップから SiteScope 設定を復元する］オプションを選択します。
3. 利用可能なバックアップのリストから復元するバックアップ設定の番号を入力します。
4. y を入力して，選択したバックアップ設定を復元することを確認します。
5. Q を入力して，強化ツール・プロセスを完了します。

非セキュア接続の FIPS 140-2 対応モードの無効化

1. 次のコマンド・ラインを実行して強化ツールを起動します。
   <SiteScope ホーム・ディレクトリ>\tools\SiteScopeHardeningTool\runSSLConfiguration.bat
2. 1 を入力して，［SiteScope の強化設定］オプションを選択します。
3. ツールでプロンプトが表示されたら，［非セキュア接続の FIPS 140-2 コンプライアンシーを設定する］オプションを選択します。
4. 2 を入力して，FIPS 140-2 対応モードを無効にします。
5. y を入力して，FIPS 140-2 対応モードを無効にすることを確認します。
6. Q を入力して，強化ツール・プロセスを完了します。

トラブルシューティングおよび制限事項

制限事項：

- SiteScope を FIPS 140-2 モードで動作する場合，SSH 接続には SSH2 のみがサポートされます。
- SiteScope を FIPS 140-2 モードで動作する場合，URL モニタ，URL ツールおよび［新規 HTTP 受信者］/［HTTP 受信者の編集］ダイアログ・ボックスの［**TLS より SSL を優先**］オプションが無視されます（FIPS 140-2 モードでは TLS を使用した認証が必須)。

トラブルシューティング：

- **問題：**FIPS 140-2 モードが有効な場合，証明書管理を使用してリモート・ホストから SiteScope に証明書をインポートできない。

  回避策：ファイルから証明書をインポートします。SiteScope ユーザ・インタフェースの［証明書管理］ページを使用するか，次のコマンドを手動で実行します。

  ```
  keytool -import -file <信頼済み証明書ファイル> -alias <信頼済み証明書名> -keypass <パスワード> -keystore <トラスト・ストア・ファイル（SiteScope\java\lib\security\cacerts）> -storepass <パスワード> -providername JsafeJCE  – storetype PKCS12
  ```

第21章: データ暗号化にカスタム・キーを使用するための SiteScope の設定

本章の内容

- 「キー管理の概要」(170ページ)
- 「データ暗号化のカスタム・キーを使用するように SiteScope を設定する方法」(171ページ)
- 「暗号化キーを変更した後に FIPS 対応モードを有効化または無効化する方法」(172ページ)
- 「データ暗号化のカスタム・キーを使用して設定データをエクスポートおよびインポートする方法」(172ページ)

キー管理の概要

標準設定では，SiteScope は標準の暗号化アルゴリズムを使用して永続データを暗号化します（永続データには，**<SiteScope ルート>\persistency** ディレクトリで検出されたすべての定義済みのモニタ，グループ，警告，テンプレート，そのほかの SiteScope エンティティの設定データが含まれます）。

強化ツールのデータ暗号化オプションとしてキー管理を使用して，SiteScope 永続データの暗号化に使用する暗号化キーを変更できます。暗号化キーを変更することで，標準の SiteScope 暗号化よりも強度の高い暗号化を実現できます。

データ暗号化のキー管理の使用は，次の SiteScope ツールでサポートされています。強化ツール，永続ビューア，永続ログ。データ暗号化のキー管理は，SiteScope が FIPS 140-2 対応モードのときに動作するように設定することもできます。

キー管理を有効にする場合は，データ暗号化にカスタム・キーを使用するように SiteScope を設定します。この操作は，新規キーの生成および永続データの暗号化で SiteScope が使用するパスフレーズを入力することで実行できます。後で SiteScope にインポートするため，現在の SiteScope から SiteScope 永続データをエクスポートときに，このパスフレーズを入力する必要があります。永続データをインポートする場合（インストール時，または SiteScope 設定ツールを使用したインストール後の操作），SiteScope サーバ・キーにこのパスフレーズを入力する必要があります。このキーは永続として保存されません。

- FIPS 140-2 対応モード（「SiteScope が FIPS 140-2 対応モードで機能するための設定」(162ページ)を参照）を有効化または無効化する場合，キー管理データ暗号化をいったん無効にして再度有効化する手間を回避するため，キー管理データ暗号化を有効にする前に実行する必要があります。
- SiteScope データの暗号化で使用する暗号化キーを変更した後に，FIPS 140-2 対応モードを有効化または無効化するには，「暗号化キーを変更した後に FIPS 対応モードを有効化または無効化する方法」(172ページ)に記載される手順に従ってください。

トラブルシューティングおよび制限事項

- データ暗号化のキー管理は，Linux プラットフォームにインストールされた SiteScope ではサポートされていません。
- SiteScope Failover を使用して，プライマリ SiteScope のバックアップ・インフラストラクチャの監視を提供する場合，データ暗号化のキー管理はサポートされません（プライマリ SiteScope および SiteScope Failover サーバの両方でサポートされません）。標準設定のキー暗号化を使用する SiteScope で SiteScope Failover を使用している場合に，強化ツールを使用して SiteScope をキー管理データ暗号化に切り替えると，設定のミラーリング時に **high_availability.log** で UNEXPECTED_SHUTDOWN エラーが発生します。

データ暗号化のカスタム・キーを使用するように SiteScope を設定する方法

キー管理を使用すると，SiteScope 設定データ（永続データ）の暗号化に使用される暗号化キーの管理および変更を行うことができます。

注: FIPS 140-2 対応モード（「FIPS 140-2 コンプライアンシーの概要」(162ページ)を参照）で SiteScope を使用する場合，データ暗号化のキー管理をいったん無効にして再度有効化する手間を回避するため，暗号化キーを変更する前に，FIPS 対応モードを設定する必要があります。データの暗号化で使用する暗号化キーをカスタマイズした後に FIPS モードに変更を加える場合は，「暗号化キーを変更した後に FIPS 対応モードを有効化または無効化する方法」(172ページ)に記載される手順に従ってください。

1. SiteScope をインストールします。

   詳細については，「インストール・ワークフロー」(85ページ)を参照してください。
2. SiteScope を開始します（SiteScope 永続データを生成するため）。
3. SiteScope を停止します。
4. 強化ツールを実行します。
   a. ツールで求められたら，［キー管理データ暗号化を有効化または再暗号化する］オプションを選択します。
   b. 1 を入力して，カスタム・キーを使用して永続データを再暗号化します。設定を暗号化するための暗号化キーを変更することで，標準の SiteScope 暗号化よりも強度の高い暗号化を実現できます。

      永続データを標準のキー暗号化に復元するには，2 を入力します。
   c. カスタム・キーを使用して永続データを再暗号化することを確認します。
   d. カスタム・キーに使用する新規パスフレーズを入力します（このパスフレーズは，すでに使用中のパスフレーズではありません。暗号化の新規反復のためのパスフレーズです）。パスフレーズには空白スペースやエスケープされた文字を含めることができません。

SiteScope で，新規キーが生成され，永続データを暗号化するために使用されます。

注: このカスタム・キーを使用して暗号化された SiteScope 設定データを SiteScope 設定ウィザードまたは SiteScope 設定ツールを使用してエクスポートまたはインポートするときに，このパスフレーズを入力する必要があります。このパスフレーズは，エクスポートした設定の zip ファイルに格納されません。

5. SiteScope を開始します。

暗号化キーを変更した後に FIPS 対応モードを有効化または無効化する方法

データを暗号化するために使用する SiteScope キーを変更した後に FIPS 140-2 対応モードを有効化または無効化する場合は，次の手順を実行する必要があります。

注: 下記の順序で手順を実行しないと，SiteScope のデータ損失が発生する場合があります。

1. データ暗号化のキー管理を無効にします（「データ暗号化のカスタム・キーを使用するように SiteScope を設定する方法」(171ページ)の手順 4 を参照し，2 を入力して標準の暗号化を復元します）。
2. FIPS 140-2 対応モードを有効化 / 無効化します。詳細については，「FIPS 140-2 対応モードの有効化」(163ページ)を参照してください。
3. データ暗号化のキー管理を有効化します（「データ暗号化のカスタム・キーを使用するように SiteScope を設定する方法」(171ページ)の手順 4 から続行し，1 を入力して，カスタム・キーを使って永続データを暗号化します）。

データ暗号化のカスタム・キーを使用して設定データをエクスポートおよびインポートする方法

データ暗号化のキー管理を使用するように SiteScope を設定する場合，SiteScope が使用するパスフレーズを入力して，新規キーを生成します。SiteScope はこのキーを使用して永続データを暗号化します。後でこの暗号化データを SiteScope にエクスポートまたはインポートする場合，同じパスフレーズを SiteScope サーバ・キーに入力する必要があります。

1. 後で SiteScope にインポートするため，現在の SiteScope から SiteScope 設定データをエクスポートします。

- SiteScope 設定ツールを使用する場合 :
  i. 設定のエクスポート画面で，SiteScope サーバのキーストアに使用するパスフレーズを［**パスフレーズ**］ボックスに入力します。このボックスは，標準設定の SiteScope 暗号化が使用される場合は無効です。
  ii. ［**次へ**］をクリックして，エクスポート操作を完了します。カスタム・キーを使用して，設定データが暗号化され，エクスポートされます。

  注: 標準設定の SiteScope 暗号化を使用する場合，これらの入力フィールドは無効です。

- 設定ツールを使用して，コンソール・モードで設定ツールを実行する場合 :設定のエクスポート画面で，SiteScope サーバのキーストアに使用するパスフレーズを求められたら，それを入力して，ENTER キーを押してエクスポート操作を完了します。

- サイレント・モードを使用する場合 :**ovinstallparams.ini** ファイルの関連セクションにキー管理データ暗号化のパスフレーズを入力します。

2. SiteScope 設定データをインポートします。
   - ユーザ・インタフェース（SiteScope 設定ウィザードでのインストール時，または SiteScope 設定ツールでのインストール後）:
     i. 設定のインポート画面で，インポートするユーザ・データ（zip）ファイルの名前を入力するか，ユーザ・データ・ファイルのインポート元である SiteScope インストール・ディレクトリを入力します。
     ii. ［**パスフレーズ**］ボックスに，SiteScope サーバ・キーストアに使用するパスフレーズを入力します。［**パスフレーズに一致**］ ボックスに同じパスフレーズを入力して，パスフレーズを確定します。

     注: 標準設定の SiteScope 暗号化を使用する場合，これらのボックスは無効です。

     iii. ［**次へ**］をクリックして，インポート操作を完了します。

   - コンソール・モード（インストール時，または設定ツールを使用したインストール後）:設定のインポート画面で，SiteScope サーバ・キーに使用するパスフレーズを求められたら，それを入力して，ENTER キーを押してインポート操作を完了します。

   - サイレント・インストール :**ovinstallparams.ini** ファイルの関連セクションにデータ暗号化に使用するカスタム・キーのパスフレーズを入力します。

   カスタム・キーを使用して，インポートした設定データが暗号化されます。

第22章: セキュア接続で BSM と通信するための SiteScope の設定

本章の内容

- 「セキュア接続が必要な BSM サーバに SiteScope を接続する設定」(174ページ)
- 「クライアント証明書が必要な BSM サーバに SiteScope を接続する設定」(174ページ)
- 「SiteScope でクライアント証明書が必要な場合に SiteScope に接続するための BSM の設定」(174ページ)

セキュア接続が必要な BSM サーバに SiteScope を接続する設定

セキュア接続が必要な BSM サーバに SiteScope が接続されるように設定するには，SiteScope と BSM の間に信用を確立してセキュア通信を有効にする必要があります。つまり，SiteScope は BSM サーバの証明書を発行した認証局を信用する必要があります。SiteScope が認証局を信用するには，認証局の証明書が SiteScope サーバとメイン・トラストストアに保存されている必要があります。詳細については，「認証局証明書の SiteScope トラストストアへのインポート」(159ページ)を参照してください。

クライアント証明書が必要な BSM サーバに SiteScope を接続する設定

SiteScope を設定して，クライアント証明書が必要な BSM サーバに接続できます。これには，BSM サーバ証明書を SiteScope キーストアにインポートする操作が含まれます。

強化ツールを使用してこれを行うことをお勧めします。詳細については，「クライアント証明書が必要な BSM サーバに SiteScope を接続するように設定するための強化ツールの使用方法」(182ページ)を参照してください。

また，「クライアント証明書が必要な BSM サーバに SiteScope を接続する設定」(226ページ)の手動での手順を使用することもできます。

SiteScope でクライアント証明書が必要な場合に SiteScope に接続するための BSM の設定

BSM で，ゲートウェイとデータ処理サーバの両方で次の手順を実行します。

1. **<SiteScope ホーム>\templates.certificates\BSMClientKeystore** ファイルを SiteScope マシン・ファイルから BSM マシン上の任意のフォルダにコピーします。
2. BSM を停止します。
3. **<HP BSM のルート・ディレクトリ>\EjbContainer\bin\product_run.bat** を編集して，次を追加します。

   ```
   set SECURITY_OPTS=-Djavax.net.ssl.keyStore=FULL_PATH_TO_COPIED_BSMClientKeyStore_File
   -Djavax.net.ssl.keyStorePassword=PASSWORD_FOR_BSMClientKeyStore_File -
   Djavax.net.ssl.keyStoreType=JKS

   set JAVA_OPTS=%JAVA_OPTS% %SECURITY_OPTS%
   ```

   FULL_PATH_TO_COPIED_BSMClientKeyStore_File はキーストアのパスで，PASSWORD_FOR_BSMClientKeyStore_File はキーストアのパスワードです。
4. BSM を再起動します。
5. システム可用性管理（SAM）管理で BSM と SiteScope を設定します。
6. ［**SAM 管理**］ > ［**新規 SiteScope**］/［**SiteScope の編集**］ > ［**分散設定**］で［**ゲートウェイ サーバ名/IP アドレス**］プロパティをセキュアなリーバス・プロキシの完全修飾ドメイン名（FQDN）に変更します。

第23章: 強化ツールの使用

強化ツールは，SiteScope の全強化，または部分的強化を実行するように SiteScope を設定できるコマンド・ライン・ツールです。

注: このツールを実行するたびに既存の SiteScope 設定の完全なバックアップが実行されるため，バックアップされた設定にロール・バックできます。詳細については，「バックアップ済みの設定を復元するための強化ツールの使用方法」(185ページ)を参照してください。

強化ツールを使用して，次のタスクを実行できます。

- 「強化ツールの実行方法」(176ページ)
- 「セキュアな接続を要求するように SiteScope を構成するための強化ツールのを使用方法」(178ページ)
- 「証明書の失効を確認するように SiteScope を設定するための強化ツールの使用方法」(179ページ)
- 「認証局の証明書を SiteScope トラストストアにインポートするための強化ツールの使用方法」(181ページ)
- 「クライアント証明書が必要な BSM サーバに SiteScope を接続するように設定するための強化ツールの使用方法」(182ページ)
- 「FIPS 140-2 対応モードを有効化するための強化ツールの使用方法」(184ページ)
- 「データ暗号化のためにキー管理を有効にするための強化ツールの使用方法」(184ページ)
- 「SiteScope と SiteScope パブリック API クライアント証明書認証を設定するための強化ツールの使用方法」(184ページ)
- 「JMX リモート・アクセスを設定するための強化ツールの使用方法」(185ページ)
- 「バックアップ済みの設定を復元するための強化ツールの使用方法」(185ページ)

強化ツールの実行方法

このトピックでは，強化ツールを開いて実行する方法について説明します。この章の各トピックで説明されているほかのタスクを実行するには，まず，このトピックの手順を実行する必要があります。

1. クライアント証明書のみを使用して SiteScope にログインする場合は LDAP ユーザ認証が必要です。LDAP ユーザ認証を有効にするには，強化ツールを実行する前に LDAP 統合を設定します。
   a. SiteScope 上で LDAP サーバを設定します。詳細については，SiteScope ヘルプの「SiteScope の使用ガイド」の項にある「SiteScope が LDAP 認証を使用するように設定する方法」を参照してください。
   b. LDAP ユーザの SiteScope ユーザ管理で新規ロールを作成します。

c. SiteScope 管理者のログイン名を，LDAP で検索した特定のユーザの電子メール アドレスに変更します。パスワードは入力しないでください。

2. SiteScope サービスを停止します。

Windows :

- **go.bat** から SiteScope を実行している場合は，コマンド・ライン・ターミナルを閉じるか，**CTRL+C** を押します。
- SiteScope をサービスとして実行している場合は，次の手順を実行します。
  i. Windows エクスプローラで，**サービス**を検索します。［コンポーネント サービス］ウィンドウが開きます。
  ii. 左側のペインで，［**サービス (ローカル)**］を選択します。
  iii. 中央のペインのサービス一覧から ［**HP SiteScope**］を選択します。
  iv. サービス一覧の左側の領域で，［**サービスの停止**］をクリックします。

Linux :

次のコマンド・ラインを実行します。

```
cd /opt/HP/SiteScope/
./stop
```

注意: SiteScope の実行中に強化ツールを実行しないでください。

3. 次のコマンド・ラインを実行してツールを起動します。

Windows :

<SiteScope ホーム・ディレクトリ>\tools\SiteScopeHardeningTool\runSSLConfiguration.bat

Linux :

./opt/HP/SiteScope/tools/SiteScopeHardeningTool/runSSLConfiguration.sh

強化ツールが開きます。

4. ツールに入力を促すメッセージが表示されたら，［SiteScope 強化設定］オプションを選択します。既存の SiteScope 設定は自動的にバックアップされます。
5. 入力を促すメッセージが表示されたら，後でバックアップを復元する必要が生じた場合に容易に識別できるようにバックアップの説明を入力します。バックアップした設定を復元する方法については，「バックアップ済みの設定を復元するための強化ツールの使用方法」(185ページ)を参照してください。

注: 強化ツールを使用する際には，**/opt/HP/SiteScope/Tomcat/conf** ディレクトリにある Tomcat 設定ファイル **server.xml** が上書きされるため，強化ツールを実行する前の同ファイルに対する変更内容はすべて失われます。これらの変更内容を復元するには，強化ツールの実行後にこのファイルに対して実行前に行った変更を再適用する必要があります。

6. ツールに表示されているタスクの一覧から 1 つまたは複数のタスクの組み合わせを選択します。

強化ツールを使用して設定タスクを実行する方法の詳細については，この章のほかのトピックを参照してください。

注: 設定の変更は，強化ツールを終了した後，有効になります。

セキュアな接続を要求するようにSiteScopeを構成するための強化ツールのを使用方法

注: SiteScope が FIPS 140-2 互換モードで動作できるようにするには，「FIPS 140-2 対応モードの有効化」(163ページ)の手順に従います。

強化ツールを使用して，セキュアな接続（https）を要求するように SiteScope を設定できます。

1. 強化ツールを実行します。詳細については，「強化ツールの実行方法」(176ページ)を参照してください。
2. ツールに入力を促すメッセージが表示されたら，［SSL（https）経由で動作するように SiteScope Standalone を構成する］オプションを選択します。

   または，強化ツールで使用可能なすべての強化設定タスクを実行する場合は，［すべての SiteScope 強化設定（すべての設定オプション）］オプションを選択します。
3. SiteScope を SSL 経由で動作させることを確認します。
4. SiteScope を FIPS 140-2 準拠で構成するかどうかを確認します。詳細については，「FIPS 140-2 対応モードの有効化」(163ページ)を参照してください。
5. 次のいずれかの方法を使用して，SiteScope サーバ証明書を保持するための SiteScope サーバ・キーストアを作成します。
   - **サーバ・キーストアを .jks フォーマットでインポートします。**

     ツールで，SiteScope SSL 認証のキーが存在する別名を選択するように求められます。

     注: クライアント証明書認証用に後で SiteScope と SiteScope パブリック API クライアントを設定する場合（「クライアント証明書認証を必要とするよう SiteScope を設定」(157ページ)を参照），SiteScope はこの別名を使用して SiteScope API のクライアント・トラストストアにキーをエクスポートします。

     ツールの指示に従います。
   - **認定された証明書認証サーバで要求に署名することで，サーバのキーストアを作成します。**

     このオプションを選択すると，新しいキーストアが作成され，署名済みの証明書の認証局に対するキー要求が生成されます。その後，生成された証明書はキーストアにインポートされます。

ツールによって，サーバのキーストア・パラメータを入力するように求められます。一般名にはマシンの URL（yourserver.domain.com など）を入力し，別名にはマシンの名前（yourserver など）を入力することをお勧めします。

- **サーバのキーストアを .pfx フォーマットでサーバ証明書からインポートします。**

  このオプションを選択すると，**.pfx** フォーマットで証明書からキーストアが作成されます。この証明書には，そのプライベート・キーが含まれている必要があります。

  キーストアが作成されるたびに，強化ツールによって，キーストアのパスワードとプライベート・キーが同じであることが自動的に確認されます。

6. クライアント証明書のユーザ名プロパティを入力します。標準設定の username は Other Name です。

   サーバ証明書はサーバ・キーストアにインポートされます。証明書の別名がツールに表示されます。

7. SiteScope クライアント認証を有効にするかどうかを確認します。

   クライアント TLS 認証を有効にすると，SiteScope は TLS ハンドシェイク時に完全なクライアント TLS 認証を実行して，クライアント証明書を抽出します。このクライアント証明書は，SiteScope ユーザ管理システムの内容と照合されます。

8. スマート・カードの実施を有効化するかどうかを確認します。

   スマート・カードの実施を有効化すると，クライアント証明書がハードウェア・デバイスに記録されているものかどうかが SiteScope によって確認されます。スマート・カードの実施の詳細については，「スマート・カード認証の設定」(156ページ)を参照してください。

9. SiteScope サーバ・トラストストアのパスワードを入力します。標準設定のパスワードは changeit です。

   SiteScope がクライアント証明書を信頼するには，SiteScope がクライアント証明書を発行した認証局を信頼する必要があります。SiteScope が認証局を信用するには，認証局の証明書が SiteScope サーバとメイン・トラストストアに保存されている必要があります。認証局証明書を SiteScope トラストストアにインポートする方法については，「認証局の証明書を SiteScope トラストストアにインポートするための強化ツールの使用方法」(181ページ)を参照してください。

10. Q を入力して，強化ツール・プロセスを完了します。

証明書の失効を確認するように SiteScope を設定するための強化ツールの使用方法

強化ツールを使用して，クライアント証明書の失効を確認するように SiteScope を設定するには，次の方法があります。

- **証明書失効リスト（CRL）**

  CRL リストを使用してクライアント証明書が失効しているかどうかを確認します。CRL リストの URL は，クライアント証明書にプロパティとして記載されています。CRL リストはローカル・サーバにダウンロードされます。ローカル・サーバのキャッシュに格納されている CRL リストの存続期間を入力するよう求めるメッセージが表示されます。

  次の表に，CRL の存続期間を示します。

CRL 値	説明
-1	CRL をローカルのキャッシュに格納し，サーバ側で変更された場合のみ再ロードします。パフォーマンスを高めるには，この値を使用することをお勧めします。
0	失効確認要求があるたびに，CRL を再ロードします。
≥1	CRL の存続期間を秒単位で指定します。指定された期間が経過すると，CRL を再ロードします。

- **オンライン証明書ステータス・プロトコル（OCSP）**

  リモート・サーバとの接続を介してクライアント証明書が失効しているかどうかを確認します。SiteScope は，クライアント証明書のシリアル番号をリモート・サーバに送って，応答を待ちます。標準設定の OCSP 応答側 URL は，クライアント証明書にプロパティとして記載されていますが，この URL は上書きできます。

クライアント証明書が失効しているかどうかの確認には，CRL のみ，または CRL と OCSP の両方を使用できます。

クライアント証明書が失効しているかどうかを確認するには，次の手順を実行します。

1. 強化ツールを実行します。詳細については，「強化ツールの実行方法」(176ページ)を参照してください。
2. ［CRL と OCSP を使用した SiteScope SSL 証明書の失効確認を設定する］オプションを選択します。
3. ツールの指示に従います。

   フォワード HTTP プロキシをアクティブ化するよう求めるメッセージが表示されます。

   フォワード HTTP プロキシをアクティブ化すると，すべての証明書失効要求がプロキシを介して CRL と OCSP の URL にリダイレクトされます。

   必要なら，連邦情報処理規格（FIPS）出版物 140-2 に準拠するよう SiteScope を設定することもできます。詳細については，「SiteScope が FIPS 140-2 対応モードで機能するための設定」(162ページ)を参照してください。

   設定の変更は，強化ツールを終了した後，有効になります。

認証局の証明書を SiteScope トラストストアにインポートするための強化ツールの使用方法

認証局の証明書を SiteScope トラストストアにインポートする方法の詳細については，「認証局証明書の SiteScope トラストストアへのインポート」(159ページ)を参照してください。

認証局の証明書を SiteScope トラストストアにインポートするには，次の手順を実行します。

1. 前提条件（セキュア接続を要求するように SiteScope を設定する場合）

   認証局の証明書を SiteScope トラストストアにインポートする前に，SiteScope サーバ証明書を SiteScope サーバ・キーストアにインポートして，TLS を介して SiteScope が機能するように設定する必要があります。詳細については，「セキュアな接続を要求するように SiteScope を構成するための強化ツールのを使用方法」(178ページ)を参照してください。
2. 強化ツールを実行します。詳細については，「強化ツールの実行方法」(176ページ)を参照してください。
3. ツールでプロンプトが表示されたら，［CA 証明書を SiteScope のメイン トラストストアとサーバ トラストストアにインポートする］オプションを選択します。
4. ツールの指示に従います。

ヒント：

- このツールでは，標準 Windows フォーマットのファイル・パスのみを使用できます。UNIX フォーマットではファイル・パス内の空白スペースが，空白スペースを示すバックスラッシュ（\）で置き換えられるため，このバックスラッシュを削除する必要があります。

形式	ファイルのパス
Windows	**/user/temp dir/certificate.cer**
UNIX	**/user/temp\ dir/certificate.cer** 次に変更します： **/user/temp dir/certificate.cer**

- 設定の変更は，強化ツールを終了した後，有効になります。

クライアント証明書が必要なBSMサーバにSiteScopeを接続するように設定するための強化ツールの使用方法

強化ツールを使用してクライアントTLS認証を設定し，BSM統合を行えます。このツールを使用して，BSMがSiteScopeと統合されるようにSiteScopeを設定できます。また，このツールを使用して，クライアントの証明書認証を使用するTLSに対応するようにSiteScope Failoverを設定することもできます。いずれの場合でも，次の手順に従う必要があります。

注: BSM統合を行うためにTLSクライアント認証を設定する前に，SiteScopeサーバ証明書をSiteScopeサーバ・キーストアにインポートし，TLSを介してSiteScopeが機能するように設定する必要があります。詳細については，「セキュアな接続を要求するようにSiteScopeを構成するための強化ツールのを使用方法」(178ページ)を参照してください。

これをまだ行っていない場合は，強化ツールによって完全なSiteScope強化設定を実行するように要求されます。

BSM統合を行うためにクライアントのTLSクライアント認証を設定するには，次の手順を実行します。

1. 強化ツールを実行します。詳細については，「強化ツールの使用」(176ページ)を参照してください。
2. ［BSM 統合を行えるようにSiteScopeクライアント証明書認証を設定する］オプションを選択します。
3. ツールの指示に従います。
   a. プロンプトが表示されたら，BSMサーバ証明書を発行した認証局の証明書に対して，**.cer**フォーマットで完全なパスを入力します。 このBSMサーバ証明書はSiteScopeトラストストアにインポートされます。
   b. プロンプトが表示されたら，BSMサーバの証明書を信用することを確定します。このBSMサーバ証明書はキーストアにインポートされます。
   c. プロンプトが表示されたら，次のいずれかの手法を選択してSiteScopeサーバ・キーストアを作成し，SiteScopeサーバ証明書を入れます。
      - **サーバ・キーストアを .jks フォーマットでインポートします。**

        ツールによって，SiteScope TLS認証用のキーが置かれている別名を選択するように求められます。

        注: クライアント証明書認証用に後でSiteScopeとSiteScopeパブリックAPIクライアントを設定する場合（「クライアント証明書認証を必要とするようSiteScopeを設定」(157ページ)を参照），SiteScopeはこの別名を使用してSiteScope APIのクライアント・トラストストアにキーをエクスポートします。

- **認定された証明書認証サーバで要求に署名することで，サーバのキーストアを作成します。**

  このオプションを選択すると，新しいキーストアが作成され，署名済みの証明書の認証局に対するキー要求が生成されます。その後，生成された証明書はキーストアにインポートされます。

  ツールによって，サーバのキーストア・パラメータを入力するように求められます。一般名にはマシンの URL（anyserver.domain.com など）を入力し，別名にはマシンの名前（anyserver など）を入力することをお勧めします。

- **サーバのキーストアを .pfx フォーマットでサーバ証明書からインポートします。**

  このオプションを選択すると，**.pfx** フォーマットで証明書からキーストアが作成されます。この証明書には，そのプライベート・キーが含まれている必要があります。

  キーストアが作成されるたびに，強化ツールによって，キーストアのパスワードとプライベート・キーが同じであることが自動的に確認されます。

d. プロンプトが表示されたら，BSM を認証するために使用されるクライアント・キーストアのパスワードを入力します。SiteScope によって BSM クライアント証明書のキーストアが作成されます。

e. プロンプトが表示されたら，ディスカバリ・エージェント **TrustStore MAMTrustStoreExp.jks** のパスワードを入力します。標準設定のパスワードは logomania です。標準設定のパスワードは変更しないことを強くお勧めします。

   設定の処理中に，SiteScope は BSM サーバの証明書を自動的に SiteScope トラストストアにインポートします。

f. プロンプトが表示されたら，BSM サーバの証明書を信用することを確定します。

   BSM サーバ証明書が SiteScope キーストアにインポートされます。

ヒント :

- このツールでは，標準 Windows フォーマットのファイル・パスのみを使用できます。UNIX フォーマットではファイル・パス内の空白スペースが，空白スペースを示すバックスラッシュ（\）で置き換えられるため，このバックスラッシュを削除する必要があります。

形式	ファイルのパス
Windows	**/user/temp dir/certificate.cer**
UNIX	**/user/temp\ dir/certificate.cer** 次に変更します : **/user/temp dir/certificate.cer**

- 設定の変更は，強化ツールを終了した後，有効になります。

FIPS 140-2 対応モードを有効化するための強化ツールの使用方法

強化ツールを使用して SiteScope が FIPS 140-2 に準拠するように設定できます。FIPS 140-2 は，National Institute of Standards and Technology（NIST）が管理する暗号化モジュール検証プログラムで，暗号化モジュールのセキュリティ要件を指定します。

詳細については，「FIPS 140-2 対応モードの有効化」(163ページ)を参照してください。

データ暗号化のためにキー管理を有効にするための強化ツールの使用方法

強化ツールでキー管理を使用して，SiteScope で永続データを暗号化するために使用される暗号化キーを変更できます。これは，SiteScope で使用される標準的な手法よりもより強力な暗号化手法です。

詳細については，「データ暗号化のカスタム・キーを使用するように SiteScope を設定する方法」(171ページ)を参照してください。

SiteScope と SiteScope パブリック API クライアント証明書認証を設定するための強化ツールの使用方法

次のように強化ツールを使用して，クライアント証明書認証を行えるように SiteScope と SiteScope パブリック API クライアントを設定します。

1. 強化ツールを実行します。詳細については，「強化ツールの実行方法」(176ページ)を参照してください。
2. ［クライアント証明書認証を行えるように SiteScope と SiteScope パブリック API クライアントを構成する］オプションを選択します。
3. ツールの指示に従います。

ヒント：

- SiteScope パブリック API に対して LDAP ユーザ認証を有効にすると，API クライアント証明書から抽出されたユーザ名が LDAP サーバによって認証されます。
- SiteScope サーバのトラストストアに対する認証を署名するクライアント証明書を追加するように要求されると，その証明書が SiteScope サーバのトラストストアとメイン・ト

ラストストアにインポートされます。作成された API 設定ファイルは **API_Configuration** ディレクトリのスクリプト・ディレクトリの下に置かれます。

- このツールでは，標準 Windows フォーマットのファイル・パスのみを使用できます。UNIX フォーマットではファイル・パス内の空白スペースが，空白スペースを示すバックスラッシュ（\）で置き換えられるため，このバックスラッシュを削除する必要があります。

形式	ファイルのパス
Windows	**/user/temp dir/certificate.cer**
UNIX	**/user/temp\ dir/certificate.cer** 次に変更します : **/user/temp dir/certificate.cer**

- 設定の変更は，強化ツールを終了した後，有効になります。

JMX リモート・アクセスを設定するための強化ツールの使用方法

次のように強化ツールを使用して，SiteScope サーバに対する JMX リモート・アクセスを有効または無効に設定できます。

1. 強化ツールを実行します。詳細については，「強化ツールの実行方法」(176ページ)を参照してください。
2. ［JMX リモート アクセスの設定］オプションを選択します。
3. ツールの指示に従います。

ヒント: 設定の変更は，強化ツールを終了した後，有効になります。

バックアップ済みの設定を復元するための強化ツールの使用方法

強化ツールを実行すると，既存の SiteScope 設定は自動的にバックアップされます。強化ツールを使用してバックアップ済みの設定を復元するには，次の手順を実行します。

1. 強化ツールを実行します。詳細については，「強化ツールの実行方法」(176ページ)を参照してください。
2. ［バックアップから SiteScope 設定を復元］オプションを選択します。

3. ツールの指示に従います。

ヒント :

- バックアップ名には，バックアップの作成日時が含まれています。
- 設定の変更は，強化ツールを終了した後，有効になります。

強化ツールの制限事項とトラブルシューティング

本項では，強化ツールを使用する際のトラブルシューティングおよび制限事項について説明します。

制限事項

SiteScope を英語以外のオペレーティング・システムにインストールした場合は，強化ツールを使用して TLS を使用するように SiteScope を設定できません。その場合は，『HP SiteScope デプロイメント・ガイド』の付録に記載されている手動の手順を使用します。

トラブルシューティング

- **強化ツールで，UNIX 形式のファイル・パスを使用できません。**

  原因 : このツールでは，標準 Windows フォーマットのファイル・パスのみを使用できます。

  解決方法: UNIX 形式では，ファイル・パスにスペースが含まれる場合，スペースの前にバックスラッシュ（\）を挿入して後にスペースが続くことを示しますが，強化ツールではこのバックスラッシュを削除する必要があります。

形式	ファイルのパス
Windows	**/user/temp dir/certificate.cer**
UNIX	**/user/temp\ dir/certificate.cer** 次に変更します : **/user/temp dir/certificate.cer**

- **ツールの終了時に，ファイルのコピー時に問題が発生したことを知らせるエラー・メッセージが表示されます。**

  原因 : この問題は，設定ツールが，作成された設定ファイルの 1 つを見つけることができない場合に発生します。これは，設定ツールをコマンド・ラインから実行していない場合に起こります。その場合，作成したファイルは設定ツール・ディレクトリに配置されません。

  解決方法 :

a. 設定ツール・ディレクトリに作成されているライブラリ（たとえば，**API_Configuration**，**tmp_<number>**，**BSM_Int** など）をすべて削除します。
b. コマンド・ライン・ターミナルを開きます。
c. コマンド・ラインで設定ツール・ディレクトリに移動します。
d. コマンド・ラインから設定ツールを実行します。詳細については，「強化ツールの使用」(176ページ)を参照してください。

- **SiteScope の認証を設定した後，SiteScope に Web ブラウザ経由でアクセスすると，認証証明書のオプションが表示されず，ログインに失敗します。**

  原因: SiteScope トラストストアに認証局の証明書（CA 証明書）が格納されていません。そのため，それらの認証局によって署名されたクライアント証明書が SiteScope によって要求されません。

  解決方法 : CA 証明書を SiteScope のメインおよびサーバのトラストストアにインポートして，必要な CA 証明書を追加します。詳細については，「認証局証明書の SiteScope トラストストアへのインポート」(159ページ)を参照してください。

- **SiteScope 公開 API 呼び出しが NumberFormatException で終了します。**

  原因 : -useSSL パラメータが false に設定された状態で API 呼び出しが実行されました。

  解決方法 : -useSSL パラメータを true に設定して API 呼び出しを実行します。

- **SiteScope 公開 API 呼び出しが ConnectException: Connection refused で終了します。**

  原因 : API 呼び出しが，TLS ポート以外のポートに接続しようとしています。

  解決方法 : -port パラメータを TLS 認証ポート 8443 に設定します。

- **SiteScope 公開 API 呼び出しが (500) Internal Server Error で失敗します。**

  原因 : -login パラメータが，正しい TLS ユーザ名に設定されていません。

  解決方法 : -login パラメータを SITESCOPE_CERTIFICATE_AUTHENTICATED_USER に設定します。

- **ブラウザ経由で SiteScope にアクセスしようとすると，次のメッセージが表示されます。「ユーザが有効な SiteScope ユーザではありません。SiteScope 管理者にお問い合わせください。」**

  原因 : TLS 認証を使用するように SiteScope を設定するとき，クライアント TLS 認証とスマートカードの導入が有効化されていますが，SiteScope ユーザ管理で LDAP サーバが設定されていません。

  解決方法 1 :

  a. 強化ツールを実行します。

  > **注:** クライアント証明書のみを使用して SiteScope にログインする場合は，強化手順を実行する前に SiteScope で LDAP サーバを設定する必要があります。SiteScope の強化後，ログインに使用されるユーザ名がクライアント証明書から抽出され，LDAP サーバと照合されて，次のプロパティが **<SiteScope root>\groups\master.config** ファイルに追加されます（これらのプロパティは変更しないでください）。

- **_clientCertificateAuthIdentityPropertyName** : 接続に使用するユーザ名を表すクライアント証明書プロパティを SiteScope に示します。
- **_clientCertificateAuthIsAPIRealLDAPUserRequired** : SiteScope API の呼び出し時に LDAP を介してユーザ名認証を実行する必要があることを SiteScope に示します。
- **_clientCertificateAuthUsernamePropertyNameInSubjectField** : API 呼び出しに使用されたクライアント証明書内でユーザ名を検索するときに使用するプロパティ。

b. 強化ツールを実行する前にバックアップした SiteScope 設定を復元します（「バックアップした設定の復元」(159ページ)を参照してください）。
c. LDAP サーバを設定します。
d. 強化ツールを再実行します。

解決方法 2 :

a. **<SiteScope root directory>\groups** にある **master.config** ファイルを開き，次の各プロパティの値を false に変更します。
   - _clientCertificateAuthEnabled
   - _clientCertificateAuthIsAPIRealLDAPUserRequired
   - _clientCertificateAuthSmartCardEnforcementEnabled
b. SiteScope を再起動します。
c. LDAP サーバを設定します。
d. **master.config** ファイルを開きます。
e. 上記の各プロパティを元の値に変更します。
f. SiteScope を再起動します。

第24章: USGCB（FDCC）準拠デスクトップの設定

USGCB（米国政府共通設定基準，旧名 FDCC （連邦政府共通デスクトップ基準））は，主としてセキュリティに焦点をあてた効率的な構成設定の改善と維持についてガイダンスを提供する，デスクトップ構成に関する標準です。

SiteScope は USGCB（FDCC）準拠のクライアントで認定されています。準拠している状態を有効にするには，SiteScope URL を信頼されたサイトのセキュリティ・ゾーンおよび許可されたポップアップの一覧に追加する必要があります。ファイルのダウンロードを許可することも推奨されます。

USGCB（FDCC）の詳細については，次のサイトを参照してください。

- http://usgcb.nist.gov/usgcb/microsoft_content.html
- http://nvd.nist.gov/fdcc/index.cfm

前提条件：

「クライアントのシステム要件」(65ページ) に示されている，SiteScope によってサポートされている最新の JRE バージョンをインストールします。

Windows 7 でグループ・ポリシー・エディタ（gpedit.msc）を有効化する方法：

1. SiteScope URL を信頼されたサイトのセキュリティ・ゾーン に追加します。
   a. 次のコマンドを実行してグループ・ポリシー・エディタを開きます。run gpedit.msc。
   b. 次の順に移動します。［**コンピュータの構成**］ > ［**管理用テンプレート**］ > ［**Windows コンポーネント**］ > ［ **Internet Explorer**］ > ［**インターネット コントロール パネル**］ > ［**セキュリティ ページ**］。
      i. 右側の設定パネルで，［**サイトとゾーンの割り当て一覧**］をダブルクリックし，［**有効**］オプションを選択して［**表示**］をクリックします。［コンテンツを表示］ダイアログ・ボックスで［**追加**］をクリックします。
      ii. ［**追加するアイテムの名前を入力してください**］ボックスで，SiteScope サーバの名前を入力します。たとえば，http://MySiteScope.com と入力します。SiteScope を HTTPS を通して使用する場合，https://MySiteScope.com と入力します。
      iii. ［**追加するアイテムの値を入力してください**］ボックスで，ゾーンの種類を示す数を入力します。

値	ゾーンの種類	説明
1	イントラネット・ゾーン	ローカル・ネットワーク上のサイト
2	信頼済みサイト・ゾーン	信頼済みサイトに追加されているサイト

値	ゾーンの種類	説明
3	インターネット・ゾーン	インターネット上のサイト
4	制限付きサイト・ゾーン	制限付きサイトに特定的に追加されているサイト

2. SiteScope URL を許可されたポップアップの一覧に追加します。
   a. 次のコマンドを実行してグループ・ポリシー・エディタを開きます。run gpedit.msc。
   b. 次の順に移動します。**［コンピュータの構成］ > ［管理用テンプレート］ > ［Windows コンポーネント］ > ［Internet Explorer］**。
      i. 右側の設定パネルで，［**許可されたポップアップの一覧**］をダブルクリックし，［**有効**］オプションを選択して［**表示**］をクリックします。［コンテンツを表示］ダイアログ・ボックスで［**追加**］をクリックします。
      ii. ［**追加するアイテムの名前を入力してください**］ボックスで，SiteScope サーバの名前を入力します。たとえば，http://MySiteScope.com と入力します。SiteScope を HTTPS を通して使用する場合，https://MySiteScope.com と入力します。
3. ファイルのダウンロードの許可（オプションで，ログ・グラバとリリース・ノートに使用されます）。
   a. 次のコマンドを実行してグループ・ポリシー・エディタを開きます。run gpedit.msc。
   b. 次の順に移動します。［**コンピュータの構成**］ > ［**管理用テンプレート**］ > ［**Windows コンポーネント**］ > ［ **Internet Explorer**］ > ［**セキュリティの機能**］ > ［**ファイル ダウンロードの制限**］。右側の設定パネルで，［**Internet Explorer プロセス**］をダブルクリックし，［**無効**］オプションを選択します。

第5部: 作業の開始と SiteScope へのアクセス

第25章: インストール後の管理

本章では，SiteScope のインストール後に実行する推奨手順を説明します。

✓	ステップ
	SiteScope サポートの登録。詳細については，「スタートアップ・ロードマップ」(38ページ)を参照してください。
	SiteScope の拡張性およびパフォーマンスを向上させるため，Microsoft ホットフィックスをインストールすることをお勧めします。詳細については，「Microsoft ホットフィックスのインストール」(195ページ)を参照してください。
	SiteScope の以前のバージョンからアップグレードする場合は，設定ツールを使用して，モニタおよびグループの設定データを以前の SiteScope インストールから新しいインストールに転送します。設定ツールの使用方法の詳細については，「SiteScope 設定ツールの使用」(124ページ)を参照してください。
	Web ブラウザを使用して，SiteScope Web インタフェースにログオンします。詳細については，「SiteScope への接続」(199ページ)を参照してください。
	新しいインストール済み環境は Community ライセンスで自動的にアクティブになります。これにより，機能制限付きで SiteScope を無期限に使用できるようになります。SiteScope エディションを SiteScope のすべての機能を使用できるエディションにアップグレードする場合，SiteScope ヘルプの「SiteScope の使用」にある［一般プリファレンス］セクションの説明に従って，［一般プリファレンス］ページに，インストール中またはインストール後に SiteScope のライセンス情報を入力できます。ライセンスの詳細については，「SiteScope ライセンス」(27ページ)を参照してください。
	SiteScope 管理者アカウント用のユーザ名およびパスワードを作成します。これは標準のアカウントで，製品がインストールされると有効になります。このアカウントは SiteScope を管理するすべての権限を持ち，アカウントを制限しなければ，製品にアクセスするすべてのユーザが使用します。 組織の要件に基づいて，その他のユーザ・アカウントを作成して設定します。詳細については，SiteScope ヘルプの「SiteScope の使用」にある「ユーザ管理プリファレンス」セクションを参照してください。管理者ユーザにユーザ名とパスワードが定義されていない場合は，SiteScope はログイン・ページをスキップして自動的にログインします。
	SiteScope 電子メールのプリファレンスの電子メール・サーバに管理者の電子メール・アドレスを設定し，SiteScope が使用できるメール・サーバを指定して，電子メール・メッセージや警告をユーザに転送します。詳細については，SiteScope へ

✓	ステップ
	ルプの「SiteScope の使用」にある「電子メール・プリファレンス」セクションを参照してください。
	監視を可能にするリモート・サーバの接続プロファイルを設定します。セキュリティ要件に応じて，使用する接続方法を指定します。詳細については，SiteScope ヘルプの「SiteScope の使用」にある「リモート・サーバ」セクションを参照してください。
	必要に応じて，ログのプリファレンスを調整して，監視データを SiteScope サーバ上に保持する日数を設定します。標準では，SiteScope は 40 日以上経過したログを削除します。監視データを外部データベースにエクスポートする場合は，データベースと必要なドライバを準備し，ログのプリファレンスを適切に設定します。詳細については，SiteScope ヘルプの「SiteScope の使用」にある「ログ・プリファレンス」セクションを参照してください。
	リモート・データベースとの接続用のミドルウェア・ドライバと，ドライバを必要とするモニタ用のアプリケーションをインストールします。
	SiteScope を Business Service Management（BSM）のデータ・コレクタとして使用する場合は，BSM 統合を設定します。詳細については，SiteScope ヘルプの「SiteScope の使用」にある「BSM の操作」セクションを参照してください。
	SiteScope を使用して，BSM で HP Operations Manager（HPOM）または 操作管理で使用するためにイベントを送信，またはメトリクスをレポートするとき，HP Operations Manager 統合を設定します。詳細については，HP ソフトウェア統合サイトの「HP Operations Manager 製品との統合」を参照してください。 • HPOM for Windows の場合 : http://support.openview.hp.com/sc/solutions/integrations.jsp?intid=39 • HPOM for UNIX の場合 : http://support.openview.hp.com/sc/solutions/integrations.jsp?intid=628
	ビジネス・システム・インフラストラクチャを評価して特定した要件と制約に基づき，グループおよびモニタ構成の枠組みを設定します。
	テンプレートを作成します。これによりグループ構造，命名規則，設定が標準化され，迅速にモニタをデプロイできるようになります。詳細については，SiteScope ヘルプの「SiteScope の使用」にある「ユーザ定義のテンプレートおよびソリューション・テンプレート」セクションを参照してください。
	グループと主要なモニタの依存関係を作成し，過剰な警告を制御できるようにします。詳細については，SiteScope ヘルプの「SiteScope の使用」にある「SiteScope グループを使った作業」セクションを参照してください。
	SiteScope をビジネスの関係者およびシステム管理者に公開します。

SiteScope のユーザが定義され，監視データの受信が可能な状態で運用が開始されたら，ビジネス・ユーザおよびシステム・ユーザに対して，SiteScope のレポート機能および警告機能にアクセスして利用する方法を説明するプロセスを開始します。

第26章: Microsoft ホットフィックスのインストール

SiteScope の拡張性およびパフォーマンスを向上させるため，SiteScope のインストール後に次の Microsoft ホットフィックスをインストールすることをお勧めします。

ホットフィックスのダウンロード	説明
http://support.microsoft.com/kb/2847018 http://support.microsoft.com/kb/2775511	最新の Microsoft mrxsmb.sys および mrxsmb10.sys または mrxsmb20.sys パッチ・ファイルを SiteScope サーバにインストールして，同一のホストに対して複数の perfex ベースのモニタを実行するときのパフォーマンスの問題およびモニタの省略を回避します。
http://support.microsoft.com/?scid=kb;en-us;942589	64 ビット・バージョンの Windows 2003，Windows 2008，または Windows XP 上で Microsoft Exchange モニタを使用するには，この Microsoft ホットフィックスをインストールします（32 ビット・アプリケーションは 64 ビット・バージョンの Windows Server 2003 または 2008 を動作しているコンピュータ上で system32 フォルダにアクセスできないため）。
http://support.microsoft.com/kb/961435	WMI を使用して Windows Server 2008 を監視できるようにするには，対象の Windows システムにこの Microsoft ホットフィックスをインストールします。

さらに，次のサポート技術情報（Microsoft Knowledge Base）の記事に記載される手順を実行して，権限の問題および不足/破損したカウンタ値の問題を回避することをお勧めします。

サポート技術情報（Microsoft Knowledge Base）の記事	問題 / 詳細
http://support.microsoft.com/kb/300702/en-us http://support.microsoft.com/kb/164018/en-us	**マシンに接続できない** :Windows リモート・サーバ上でパフォーマンス・オブジェクトを監視するには，ユーザは特定のアクセス権限が必要です。サポート技術情報（Microsoft Knowledge Base）の記事 300702 および記事 164018 を参照してください。
http://support.microsoft.com/kb/295292	**WMI 権限** :リモート監視用に WMI サービスを設定するには，WMI リモート・サーバで入力したユーザ

サポート技術情報（Microsoft Knowledge Base）の記事	問題 / 詳細
	に，WMI namespace root\CIMV2 からリモートで統計を読み取ることのできる権限が必要です。
http://support.microsoft.com/kb/300956/en-us	**不足 / 破損したパフォーマンス・カウンタ・ライブラリ値**: 必要なパフォーマンス・カウンタ・ライブラリ値が見つからない場合や破損している場合は，Microsoft サポート技術情報（Microsoft Knowledge Base）の記事 KB300956 の手順に従って，それらの値を手動で再構築します。

第27章: SiteScope を使った作業の開始

本章の内容

- 「SiteScope サービスの開始の概要」(197ページ)
- 「Windows プラットフォームでの SiteScope サービスの開始と停止」(197ページ)
- 「Linux プラットフォームでの SiteScope プロセスの開始と停止」(198ページ)
- 「SiteScope への接続」(199ページ)
- 「SiteScope クラシック・インタフェース」(200ページ)
- 「トラブルシューティングおよび制限事項」(200ページ)

SiteScope サービスの開始の概要

SiteScope のプロセスは，インストール中にすべてのプラットフォームで起動されます。

- Windows プラットフォームでは，SiteScope は，サーバが再起動された場合に自動的に再起動するよう設定されたサービスとして追加されます。
- Linux プラットフォームでは，SiteScope がインストールされたサーバを再起動する場合は常に，SiteScope のプロセスを再起動する必要があります。

本項で説明する手順を使用して，必要に応じて SiteScope のプロセスの開始と停止を手動で行うことができます。

Windows プラットフォームでの SiteScope サービスの開始と停止

SiteScope は，Microsoft Windows プラットフォーム上のサービスとしてインストールされます。標準設定では，サーバが再起動されるときには常に，SiteScope サービスが自動的に再起動されるよう設定されています。［サービス］コントロール・パネルを使用して，SiteScope サービスの開始と停止を手動で行うことができます。

［サービス］コントロール・パネルを使用して SiteScope サービスの開始または停止を行うには，次の手順で行います。

1. ［**スタート**］>［**設定**］>［**コントロール パネル**］>［**管理ツール**］>［**サービス**］を選択し，［**サービス**］コントロール・パネルを開きます。
2. サービスのリストで［**SiteScope**］を選択し，右クリックしてショートカット・メニューを表示します。
3. ショートカット・メニューから必要に応じて［**開始**］または［**停止**］を選択します。

net start コマンドおよび net stop コマンド

net start コマンドおよび net stop コマンドを使用して SiteScope サービスの開始と停止を行うこともできます。

net start コマンドを使用して SiteScope サービスを開始するには，次の手順で行います。

1. SiteScope がインストールされているサーバのコマンド・ライン・ウィンドウを開きます。
2. 次の構文を使用して netstart ユーティリティを実行します。

   net start SiteScope

net stop コマンドを使用して SiteScope サービスを停止するには，次の手順で行います。

1. SiteScope を実行しているサーバのコマンド・ライン・ウィンドウを開きます。
2. 次の構文を使用して netstop ユーティリティを実行します。

   net stop SiteScope

Linux プラットフォームでの SiteScope プロセスの開始と停止

SiteScope は自動開始プロセスを備えており，システムが起動または停止すると，SiteScope が自動的に開始または停止するようになっています。SiteScope 実行ファイルに対する権限（開始，停止）を変更する場合は，**/etc/init.d/sitescope** ファイルの権限も変更する必要があります。

製品に付属のシェル・スクリプトを使用すれば，SiteScope の開始と停止を手動で行うこともできます。init.d スクリプトを使用して，サーバが再起動されるときに SiteScope を自動的に再起動することもできます。

注: SiteScope を Linux にインストールするときは root ユーザ・アカウントを使用する必要がありますが，インストールを行った後は，非 root ユーザ・アカウントから実行できます。詳細については，「SiteScope を実行する権限のある非 root ユーザ・アカウントの設定」(44ページ)を参照してください。

Linux 上の SiteScope プロセスを手動で開始するには，次の手順を実行します。

1. SiteScope がインストールされているサーバのターミナル・ウィンドウを開きます。
2. 次の構文を使用して，start コマンド・シェル・スクリプトを実行します。

   <installpath>/SiteScope/start

   （Linux/UNIX マシンの場合は，service sitescope start を任意のディレクトリで実行してもかまいません）。

Linux 上の SiteScope プロセスを手動で停止するには，次の手順を実行します。

1. SiteScope を実行しているサーバのターミナル・ウィンドウを開きます。
2. 次の構文を使用して，stop コマンド・シェル・スクリプトを実行します。

   <installpath>/SiteScope/stop

   （Linux/UNIX マシンの場合は，service sitescope stop を任意のディレクトリで実行してもかまいません）。

前述のコマンドの <installpath> を SiteScope がインストールされている場所のパスに置き換えます。たとえば，SiteScope が /usr ディレクトリにインストールされている場合には，SiteScope を停止するコマンドは，次のようになります。

/usr/SiteScope/stop

SiteScope への接続

SiteScope は，Web アプリケーションとして設計されています。このため，SiteScope の参照と管理には，SiteScope サーバにアクセスできる Web ブラウザを使用します。

SiteScope は，2 つのポート（8080 および 8888）で応答するようにインストールされます。このポートを使用するように設定されているサービスがほかにある場合は，インストール・プロセスによって別のポートで SiteScope が応答するように設定されます。

Windows プラットフォームでは，インストール・プロセスによって，［**スタート**］ > ［**すべてのプログラム**］メニューの SiteScope 用にメニューに SiteScope へのリンクが追加されます。［スタート］メニュー・フォルダはインストール時に選択します。

SiteScope にアクセスするには，次の手順を実行します。

Web ブラウザで SiteScope のアドレスを入力します。標準アドレスは，http://localhost:8080/SiteScope です。

Windows プラットフォームでは，［スタート］メニューから SiteScope にアクセスすることもできます。**［スタート］ > ［すべてのプログラム］ > ［HP SiteScope**］ > **［HP SiteScope を開く］**をクリックします。SiteScope ポートを SiteScope のインストール後に変更した場合，ポートは「**HP SiteScope を開く**」リンクで更新されます。

SiteScope が初めてデプロイされた場合は，インタフェース要素の初期化のために遅延が生じます。SiteScope が［ダッシュボード］ビューで開きます。

注:

- このアカウントとその権限の使用を制限するには，管理者アカウント・プロファイルを編集して，ユーザ名とログイン・パスワードを含める必要があります。これにより，SiteScope にアクセスする前に SiteScope によってログイン・ダイアログが表示されます。管理者アカウント・プロファイルの編集に関する情報については，SiteScope ヘルプで『SiteScope の使用』の「ユーザ管理プリファレンス」セクションを参照してください。

- SiteScope を別のマシンから表示する場合は，最新のサポートされている JRE（Java Runtime Environment）がインストールされているマシンを使用することをお勧めします。

SiteScope クラシック・インタフェース

SiteScope の以前のバージョンで利用できた SiteScope クラシック・インタフェース（URL は http://<sitescope_host>:8888）は，SiteScope の管理には使用できなくなりました。

master.config ファイルの **_serverFilter** プロパティにクラシック・インタフェースの特定のページが一覧表示されている場合は，引き続きこれらのページにアクセスできます。標準設定で一覧表示されているページには，［Monitor Summary］ページと［Alert Report］ページがあります。

注: 標準設定で有効になっている SiteScope クラシック・インタフェースのページは削除しないでください。何らかの機能に影響を及ぼす可能性があります。

トラブルシューティングおよび制限事項

この項では，SiteScope へのログオン時の次の問題に対する注意事項と制限事項について説明します。

起動に関する特定の問題：

- 「SiteScope が起動せず，エラー・メッセージが表示される」(200ページ)
- 「SiteScope アプレットの読み込みが失敗して「NoClassDefFound」例外が表示される」(201ページ)
- 「64 ビットのコンピュータからアプレットをロードする場合の問題」(201ページ)
- 「ブラウザ・ウィンドウの複数のタブで同じ SiteScope サーバを開くと，SiteScope がハングする」(201ページ)
- 「SiteScope メニュー・バーが開くが，アプレットの起動に失敗し，空の画面，エラー，または「x」の画像が表示される」(202ページ)
- 「SiteScope を起動できない場合に SiteScope インストールのバックアップとリカバリを行う」(202ページ)
- 「SiteScope が Firefox で開かない」(204ページ)

SiteScope が起動せず，エラー・メッセージが表示される

SiteScope アプレットの起動時に「Java Runtime Environmentがロードできません」というエラー・メッセージや，ほかの未知のエラーが発生した場合は，次の手順を実行します。

各手順の後で，SiteScope を再度開いてみてください。それでも SiteScope でエラーが発生する場合は，次の手順に進んでください。

1. すべてのブラウザ・ウィンドウを閉じます。
2. Windows タスク・マネージャを使用して，実行中のブラウザ・プロセスがあればすべて終了します。
3. ローカルの Java アプレット・キャッシュを消去します。**［スタート］>［コントロール パネル］>［Java］**を選択します。［**基本**］タブで，**［設定］>［ファイルの削除**］をクリックし，［**OK**］をクリックします。
4. 次のフォルダの内容を削除して，ローカルの Java アプレット・キャッシュを消去します。
C:\Documents and Settings\<ユーザ名>\Application Data\Sun\Java\Deployment\cache

SiteScope アプレットの読み込みが失敗して「NoClassDefFound」例外が表示される

アプレットの読み込みが失敗して「NoClassDefFound」例外が表示される場合は，クライアント Java 設定（**［コントロール パネル］>［Java］>［基本］タブ>［インターネット一時ファイル］>［設定］**）で［**コンピュータに一時ファイルを保持します**］オプションを選択します。

セキュリティ上必要な場合は，SiteScope アプレットの使用が完了した時点でこれらの一時ファイルを手動で削除してください。

1. SiteScope アプレットを終了します。
2. **［スタート］>［コントロール パネル］>［Java］>［一般］タブ**を選択します。
3. ［**インターネット一時ファイル**］セクションで，［**設定**］ > ［**ファイルの削除**］をクリックします。

64 ビットのコンピュータからアプレットをロードする場合の問題

64 ビットのコンピュータで SiteScope を実行している場合，JRE に一致するブラウザのバージョンを使用してください。

JRE	［参照］
64 ビット JRE	Internet Explorer（64 ビット）
32 ビット JRE	Internet Explorer（32 ビット）

ブラウザ・ウィンドウの複数のタブで同じ SiteScope サーバを開くと，SiteScope がハングする

ブラウザ・ウィンドウの複数のタブで同じ SiteScope サーバ・ユーザ・インタフェースを開いた場合，SiteScope サーバ・タブ間で移動を試みると SiteScope がハングします。

考えられる解決策 :

- 重複しているタブを閉じ，同一の SiteScope サーバ・ユーザ・インタフェースに対してタブが 1 つだけ開かれた状態にします。
- または，新しいブラウザ・ウィンドウを開きます。

SiteScope メニュー・バーが開くが，アプレットの起動に失敗し，空の画面，エラー，または「x」の画像が表示される

これは，Java コントロール・パネルが Web ブラウザを使用するように設定されていないために発生します。

考えられる解決策 :

1. ［**スタート**］ > ［**コントロール パネル**］ > ［**Java**］をクリックします。［**基本**］タブで［**ネットワーク設定**］をクリックし，［**直接接続**］オプションを選択し，［**OK**］をクリックします。
2. ［**詳細**］タブで，［**ブラウザの標準設定の Java**］フォルダ（または Java 5 を使用している場合は［**<APPLET> タグのサポート**］）を展開します。［**Microsoft Internet Explorer**］と［**Mozilla ファミリ**］が選択されていることを確認します。［**適用**］をクリックしてから［**OK**］をクリックします。
3. ブラウザを再起動します。

SiteScope を起動できない場合に SiteScope インストールのバックアップとリカバリを行う

SiteScope が停止し，再起動ができなくなったために SiteScope 設定データをリカバリするには，現在の SiteScope インストール・ディレクトリとこのディレクトリ内に含まれるすべてのサブディレクトリのバックアップを作成し，その後で新しいバージョンの SiteScope をインストールします。現在の SiteScope インストールをバックアップするには，設定ツールを使用して SiteScope データを **.zip** ファイルにエクスポートするか，あるいは必要なファイルを手動でバックアップします。

SiteScope の再インストールが完了した時点で，モニタ設定データを SiteScope にコピーできます。設定ツールを使用してインストール・ディレクトリのバックアップを作成した場合は，設定ツールを使用してこのコピー作業が行えます。設定ツールを使用しなかった場合は，バックアップしたすべてのフォルダとファイルを新しいインストール・ディレクトリから削除してから，バックアップしたフォルダとファイルをこのインストール・ディレクトリにコピーします。

SiteScope インストールをバックアップするには，次の手順で行います。

1. SiteScope を停止します。

   注: 必ずしも必要ではありませんが，バックアップを作成する前に SiteScope を停止することをお勧めします。

2. 次のいずれかの方法で，現在の SiteScope インストールのバックアップを作成します。
   - 設定ツールを使用して，設定を **.zip** ファイルにエクスポートする。詳細については，「SiteScope 設定ツールの使用」(124ページ)を参照してください。
   - 次のフォルダとファイルを，SiteScope インストールからバックアップ先にコピーします。

ディレクトリ	説明
\cache	Business Service Management が停止していた場合に Business Service Management に報告されなかったデータ・サンプルが含まれています。
\conf\ems	統合モニタ・タイプとともに使用される重要な設定ファイルおよび制御ファイルが含まれています。これは，別の Business Service Management アプリケーションに報告するエージェントとして SiteScope を使用する場合にのみ適用されます。
\conf\integration	Business Service Management との統合に使用されるトポロジ・ファイルが含まれています。
\discovery\scripts\custom	カスタム・ディスカバリ・スクリプトが含まれています。
\groups	SiteScope の運用に必要な，モニタ，警告，レポート，およびその他の重要な設定データが含まれています。
\htdocs	定期レポートとユーザがカスタマイズした SiteScope インタフェースのスタイル・シートが含まれています。レポート・ページの損傷を防ぎ，古いレポートを表示するためには，このディレクトリをバックアップして SiteScope ディレクトリ（同じ SiteScope バージョンにあるディレクトリ）にコピーします。このフォルダは，設定を新しい SiteScope バージョンにインポートする際にバックアップできません。
\logs	日付が記述された監視データのログなど，多くのログが含まれています。最新の監視データのログ・ファイルと，このディレクトリに含まれるほかのタイプのログを選択的にバックアップしてください。また，履歴の継続性を保つために，**error.log**，**RunMonitor.log**，**access.log, alert.log**，**monitorCount.log** ログをバックアップすることもできます。
\persistency	これは，この製品の中心的な永続ディレクトリです。このディレクトリには，モニタ，グループ，警告，テンプレートなど，定義されているすべての SiteScope エントリが含まれています。
\scripts	スクリプト・モニタが使用するスクリプトが含まれています。

ディレクトリ	説明
\scripts.remote	スクリプト・モニタがリモート・サーバ上のほかのスクリプトをトリガするために使用するコマンド・スクリプトが含まれています。
\templates.*	モニタの機能，アラートの内容，その他の機能をカスタマイズするために使用されるデータとテンプレートが含まれています。すべて templates という名前で始まるサブディレクトリのグループです。 **例：** templates.mail，templates.os，templates.webscripts
\WEB-INF\lib\peregrine.jar	HP Service Manager 統合を設定した際に変更（再生成）された可能性があるファイルです。

SiteScope インストールをリカバリするには，次の手順で行います。

1. SiteScope の新規インストールを実行します。詳細については，「インストール・ワークフロー」(85ページ)を参照してください。
2. SiteScope のインストールが完了した後で，次の処理を行います。
   - 現在の SiteScope インストール・ディレクトリのバックアップを作成するために設定ツールを使用した場合は，作成済みの **.zip** ファイルを設定ツールを使用してインポートします。詳細については，「SiteScope 設定ツールの使用」(124ページ)を参照してください。
   - バックアップを手動で作成した場合は，前述のフォルダとファイルをすべて新しいインストール・ディレクトリから削除してから，バックアップしたフォルダとファイルをこのインストール・ディレクトリにコピーします。

SiteScope が Firefox で開かない

問題：スマート・カードの実施が無効化されているのにクライアント証明書認証が有効な場合，SiteScope が Firefox ブラウザで開きません。

解決方法：スマート・カードの実施が無効化されているのにクライアント証明書認証が有効な場合に SiteScope を Firefox ブラウザで開く方法については，「クライアント証明書が有効な場合の Firefox の使用」(158ページ)を参照してください。

付録

付録A: SiteScope のTomcat サーバとの IIS の統合

Internet Information Server（IIS）を SiteScope に付属の Apache Tomcat サーバと統合するには，Apache Tomcat サーバが使用する設定ファイルに変更を行い，IIS 設定の対応する Web サイト・オブジェクトに仮想ディレクトリを作成します。

本項の内容

- 「Apache Tomcat サーバ・ファイルの設定」(206ページ)
- 「IIS の設定」(209ページ)

Apache Tomcat サーバ・ファイルの設定

IIS を Apache Tomcat サーバと統合できるようにするには，SiteScope に付属の Apache Tomcat サーバの設定ファイルを編集しなければなりません。

Apache Tomcat サーバ・ファイルの設定を設定するには，次の手順で行います。

1. Apache のコネクタ・ファイルのダウンロード・サイトから最新の Java Connector jk をダウンロードします

   http://tomcat.apache.org/download-connectors.cgi
2. **isapi_redirect.dll** ファイルを**<Tomcat インストール・ディレクトリ>\bin\win32** ディレクトリにコピーします。標準設定では，Tomcat サーバは SiteScope のインストール時に **C:\SiteScope\Tomcat** にインストールされます。このディレクトリが存在しなければ，**win32** ディレクトリを作成します。
3. 次のいずれかを実行します。
   - **isapi_redirect.dll** ファイルと同じディレクトリに設定ファイルを作成し，**isapi_redirect.properties** という名前を付けます。

     isapi_redirect.properties ファイルの例：

     ```
     # Configuration file for the Jakarta ISAPI Redirector

     # The path to the ISAPI Redirector Extension, relative to the website
     # This must be in a virtual directory with execute privileges
     extension_uri=/jakarta/isapi_redirect.dll

     # Full path to the log file for the ISAPI Redirector
     log_file=C:\SiteScope\Tomcat\logs\isapi.log
     ```

```
# Log level (debug, info, warn, error or trace)
log_level=info

# Full path to the workers.properties file
worker_file=C:\SiteScope\Tomcat\conf\workers.properties.minimal

# Full path to the uriworkermap.properties file
worker_mount_file=C:\SiteScope\Tomcat\conf\uriworkermap.properties
```

この設定はログ・ファイル（**<SiteScope のルート・ディレクトリ>\Tomcat\logs** ディレクトリに含めることをお勧めします）とワーカ・ファイルおよびワーカのマウント・ファイル（**<SiteScope のルート・ディレクトリ>\Tomcat\conf** ディレクトリに格納しなければなりません）を指します。

- 同じ設定エントリ（上記を参照）を次のパスのレジストリに追加します。HKEY_LOCAL_MACHINE\SOFTWARE\Apache Software Foundation\Jakarta Isapi Redirector\1.0

4. **<SiteScope のルート・ディレクトリ>\Tomcat\conf** ディレクトリに **workers.properties.minimal** という名前の SiteScope ワーカ・ファイルを作成します。

SiteScope ワーカ・ファイルの例 :

```
# workers.properties.minimal -
#
# This file provides minimal jk configuration
# properties needed to
# connect to Tomcat.
#
# Defining a worker named ajp13w and of type ajp13
# Note that the name and the type do not have to
# match.
worker.list=ajp13w
worker.ajp13w.type=ajp13
worker.ajp13w.host=localhost
worker.ajp13w.port=8009
#END
```

注 :

- **worker.ajp13w.port** は使用されている Tomcat のバージョンによって異なります。**<SiteScope のルート・ディレクトリ>\Tomcat\conf\server.xml** を開いて文字列 <Connector port= を検索し，このバージョンの Tomcat が使用しているポートを判別します。

- SiteScope を SiteMinder と統合するように設定する場合，**server.xml** ファイルの <!-- Define an AJP 1.3 Connector on port 8009 --> セクションで，次のようにリダイレクト・ポートを変更します。

  <!-- <Connector port="18009"

URIEncoding="UTF-8" enableLookups="false" redirectPort="8443" protocol="AJP/1.3" /> -->

から次へ変更

<Connector port="18009"
URIEncoding="UTF-8" enableLookups="false" redirectPort="80" protocol="AJP/1.3" />

- IIS と Tomcat が同じマシン上にない場合は，**workers.properties.minimal** のホスト属性をほかのマシンを指すよう変更します。

5. **<SiteScope のルート・ディレクトリ>\Tomcat\conf** ディレクトリに SiteScope ワーカのマウント・ファイルを作成します。

上記の設定例にような，uriworkermap.properties という名前のSiteScope ワーカ・ファイルの例：

```
# uriworkermap.properties - IIS
#
# This file provides sample mappings for example:
# ajp13w worker defined in workermap.properties.minimal
# The general syntax for this file is:
# [URL]=[Worker name]
/SiteScope=ajp13w
/SiteScope/*=ajp13w
#END
```

新しい構文は，SiteScope の 2 つのルールを次の 1 つに結合します。/SiteScope/*=ajp13w

Tomcat ログ出力は，**<SiteScope のルート・ディレクトリ>\logs\tomcat.log** ファイルに書き込まれます。ログ・ファイルの設定は，**<SiteScope のルート・ディレクトリ>\Tomcat\common\classes\log4j.properties** ファイルで実行できます。

トラブルシューティング

問題：SiteScope の以前のバージョンからアップグレードするとき， **<SiteScope のルート・ディレクトリ>\Tomcat\conf** ディレクトリの Tomcat 設定 **server.xml** ファイルが上書きされ，そのファイルへの変更がすべて削除されてしまう（たとえば，SiteScope が SSL を使用するよう設定したときに行われた設定など)。

解決方法：これらの変更を復元するには，アップグレードの実行後に **server.xml** ファイルに変更を再適用する必要があります。

a. SiteScope を停止します。

b. 次のファイルを置き換えます。

置換前ファイル	置換後のファイル
<SiteScope のルート・ディレクトリ	**<SiteScope のルート・ディレクトリ >\installation\HPSiS1122\backup\java\lib\security\cacert**

置換前ファイル	置換後のファイル
>\java\lib\security\cacerts	**s**
<SiteScope のルート・ディレクトリ >\java\lib\security\java.security	**<SiteScope のルート・ディレクトリ >\installation\HPSiS1122\backup\java\lib\security\java.security**
<SiteScope のルート・ディレクトリ >\java\lib\security\javaws.policy	**<SiteScope のルート・ディレクトリ >\installation\HPSiS1122\backup\java\lib\security\javaws.policy**
<SiteScope のルート・ディレクトリ >\java\lib\security\java.policy	**<SiteScope のルート・ディレクトリ >\installation\HPSiS1122\backup\java\lib\security\java.policy**

c. すべての強化およびその他の変更を，**<SiteScope のルート・ディレクトリ >\installation\HPSiS1122\backup\Tomcat\conf\server.xml** から **<SiteScope のルート・ディレクトリ>\Tomcat\conf\server.xml** に手動で再適用します。

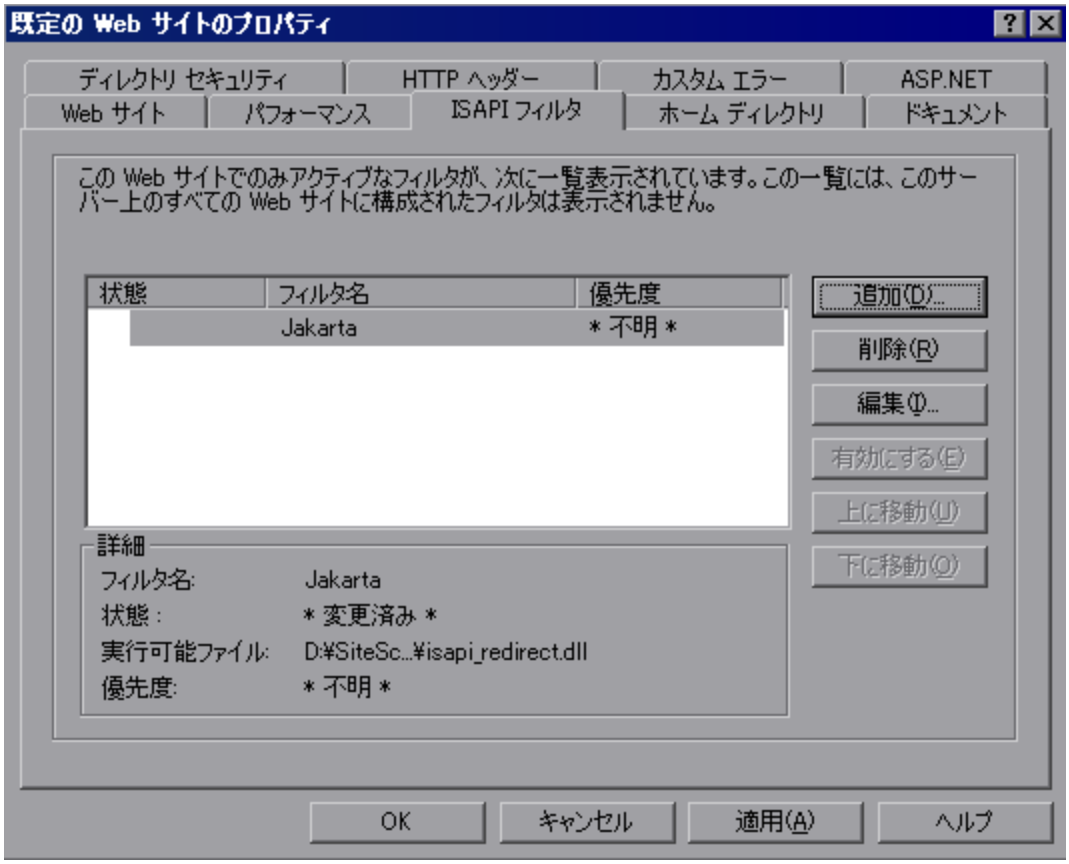
IIS の設定

Tomcat サーバが使用する設定ファイルに変更を行ったら，IIS 設定の対応する Web サイト・オブジェクトに仮想ディレクトリを作成する必要があります。

IIS を設定するには，次の手順で行います。

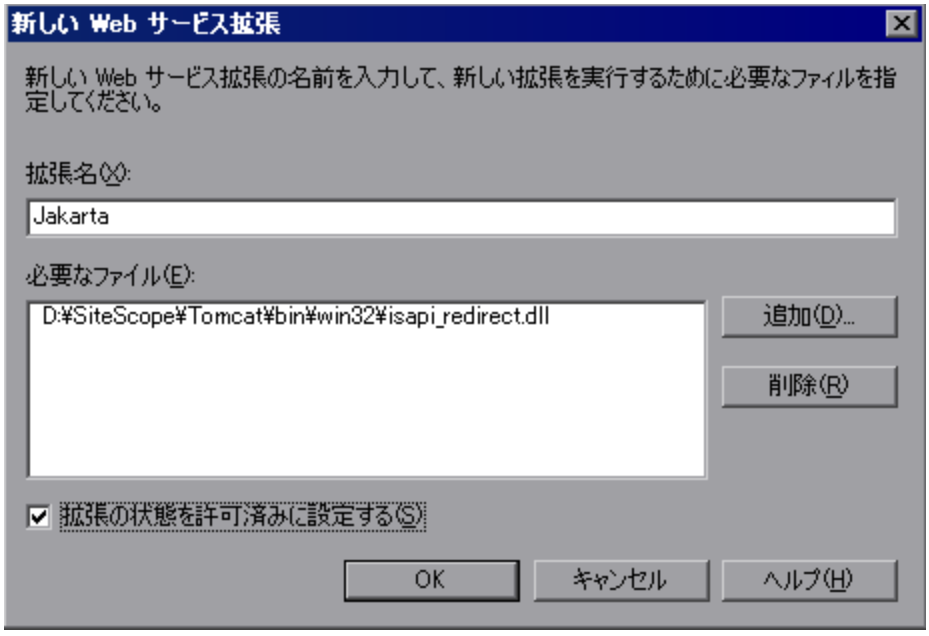
1. Windows で，［**スタート**］ > ［**設定**］ > ［**コントロール パネル**］ > ［**管理ツール**］ > ［**インターネット インフォメーション サービス（IIS）マネージャ**］をクリックします。
2. 右側の表示枠で，「< **ローカル コンピュータ名** > \Web Sites\ < **Web サイト名** > 」を右クリックし，［**新規作成**］ > ［**仮想ディレクトリ**］をクリックします。この名前を **Jakarta** に変更し，**isapi_redirect.dll** が含まれるディレクトリに**ローカル・パス**を設定します。

3. <**Web サイト名**> を右クリックし，［**プロパティ**］をクリックします。
4. ［**ISAPI フィルタ**］タブをクリックしてから，［**追加**］をクリックします。［**フィルタ名**］カラムで，「**Jakarta**」を選択し，**isapi_redirect.dll** を参照します。フィルタが追加されますが，この段階ではまだアクティブではありません。



［**適用**］をクリックします。

5. ［**<ローカル マシン名>**］ **>** ［**Web サービス拡張**］を右クリックし，［**新しい Web サービス拡張を追加**］をクリックします。［新しい Web サービス拡張］ダイアログ・ボックスが開きます。
6. ［**拡張名**］ボックスに「Jakarta」という名前を入力し，［**必要なファイル**］で **isapi_redirect.dll** ファイルを参照します。［**拡張の状態を許可済みに設定する**］を選択します。



［**OK**］をクリックします。

7. IIS Web サーバを再起動し，Web サービス経由でアプリケーションにアクセスしてみてください。

付録B: SiteScope と SiteMinder との統合

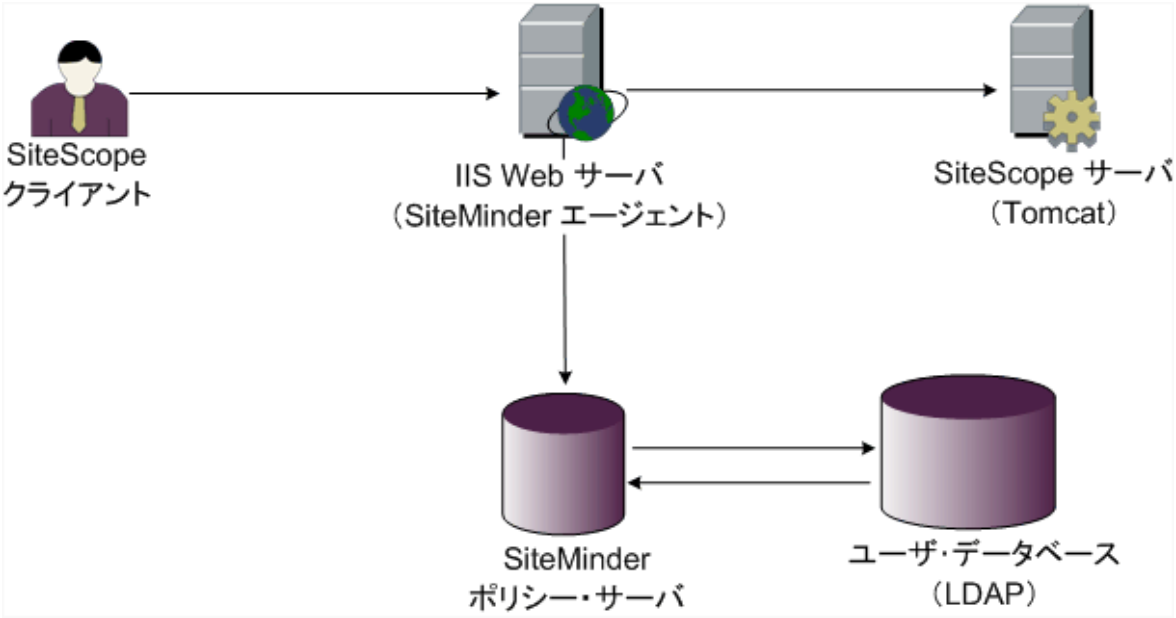
SiteScope は，セキュリティ・アクセス管理ソリューションである SiteMinder と統合でき，顧客のユーザとアクセス管理設定を活用できます。

本項の内容

- 「SiteMinder との統合について」(213ページ)
- 「統合の要件」(214ページ)
- 「統合のプロセス」(214ページ)
- 「SiteMinder ポリシー・サーバの設定」(215ページ)
- 「SiteMinder を使用するための SiteScope の設定」(216ページ)
- 「IIS の設定」(216ページ)
- 「さまざまな SiteScope ロールの権限の定義」(217ページ)
- 「SiteScope へのログオン」(217ページ)
- 「注意事項とガイドライン」(217ページ)

SiteMinder との統合について

次の図で，SiteScope を SiteMinder と統合して，SiteScope ユーザを認証して権限を与える方法について説明します。



このアーキテクチャでは，SiteMinder エージェントは，SiteScope の Tomcat アプリケーション・サーバの前に配置された IIS Web サーバ上に構成されています。SiteMinder エージェントは Web サー

バ上になければなりません。IIS Web サーバは，すべての SiteScope ユーザを（LDAP 上または任意のほかの同様のリポジトリ上で）管理する SiteMinder ポリシー・サーバに接続されます。

SiteMinder エージェントはすべての SiteScope の関連トラフィックを傍受し，ユーザの資格情報を確認します。ユーザの資格情報は，認証と権限付与のため SiteMinder ポリシー・サーバに送信されます。SiteMinder はユーザを認証すると，ログインして SiteMinder の認証を渡そうとした正確なユーザを示すトークンを（特別な HTTP ヘッダを付けて）SiteScope に送ります。

注: SiteScope クライアント，IIS Web サーバ，SiteScope Tomcat アプリケーション・サーバは，同じマシン上で設定することをお勧めします。

統合の要件

本項では，SiteScope と SiteMinder を統合するための最小システム要件について説明します。

オペレーティング・システム	Windows 2003 Standard/Enterprise SP1
Web サーバ	IIS 5.0，IIS 6.0
アプリケーション・サーバ	Tomcat 5.0.x
Java コネクタ	Java Connector jk-1.2.21

統合のプロセス

この節では，SiteMinder との統合のプロセスについて説明します。

SiteScope を SiteMinder と統合するには，次の手順で行います。

1. **SiteMinder ポリシー・サーバを準備して設定します。**

   SiteMinder 管理者は，Web エージェントのインストール，IIS Web サーバへの Web エージェントのインストール，および Web エージェントの設定のために，SiteMinder ポリシー・サーバを準備する必要があります。

   さらに，SiteMinder 管理者は SiteMinder ポリシー・サーバを設定する必要があります。SiteMinder の推奨設定の詳細については，「SiteMinder ポリシー・サーバの設定」(215ページ)を参照してください。

2. **SiteMinder を使用するために SiteScope を設定します。**

   SiteScope を SiteMinderと統合できるようにするには，Tomcat サーバが使用する設定ファイルを変更する必要があります。詳細については，「Apache Tomcat サーバ・ファイルの設定」(206ページ)を参照してください。

3. **IIS を設定します。**

IIS 設定の対応する Web サイト・オブジェクトに仮想ディレクトリを作成する必要があります。詳細については，「IIS の設定」(209ページ)を参照してください。

4. **SiteScope のロールごとに権限を定義します。**

   SiteMinder との統合が有効になったら，SiteScope のロールごとに権限を定義しなければなりません。詳細については，「さまざまな SiteScope ロールの権限の定義」(217ページ)を参照してください。

SiteMinder ポリシー・サーバの設定

SiteScope 領域オブジェクト，認証用と追加属性を持つクッキーの送信用の 2 つの SiteScope ルール・オブジェクト，追加の LDAP 属性を SiteScope に転送する SiteScope 応答オブジェクトを生成することによって，また SiteScope ルールと応答をセキュリティ・ポリシー・オブジェクトに追加することによって SiteMinder ポリシー・サーバを設定します。

ポリシー・サーバで SiteScope 領域オブジェクトを作成する前に，次のことを確認します。

- ドメイン上に特別な管理者（1 つ以上のユーザ・ディレクトリ）が設定されていること。
- 1 つ以上のユーザ・ディレクトリ・オブジェクトが設定されていること。これらのオブジェクトは，LDAP ディレクトリまたはほかの任意のリポジトリに含まれるユーザを表します。
- 認証スキームを定義していること。

  ドメインが 1 つ以上のユーザ・ディレクトリ・オブジェクトに接続されていること。領域用に特別なドメインを作成する必要はありません。既存のドメインを使用できます。

SiteMinder ポリシー・サーバを設定するには，次の手順で行います。

1. SiteMinder 管理にログインします。
2. 領域を作成し，次の情報を入力します。
   - **名前：**領域に名前を入力します。例：**SiteScope realm**。
   - **リソース・フィルタ：/SiteScope** と入力します。SiteScope 次のすべてが領域に含まれます。
3. 新規領域を右クリックして，［**Create rule under realm**］をクリックします。
   - 認証用に新しいルールを作成します。ルールに分かりやすい名前を入力します（**SiteScope rule** など）。［**Action**］セクションで，［**Web Agent Action**］オプションを選択し，すべての HTTP 要求スキーム（**Get**，**Post** ，および**Put**）を選択します。
   - クッキーおよびその他の属性の SiteScope への転送用に 2 番目のルールを作成します。ルールに分かりやすい名前を入力します（例：**Users role**）。［**Action**］セクションで［**Authentication events**］オプションを選択し，ドロップダウン・リストから［**OnAuthAccept**］を選択します。
4. SiteScope 応答オブジェクトを作成して，追加の LDAP 属性を関連する認証情報とともに SiteScope に転送します。

a. ［**Responses**］を右クリックして，［Response Properties］ウィンドウを開きます。
b. 応答に分かりやすい名前を入力します。例：**SiteScope Role**。
c. ［**Attribute List**］セクションで［**Create**］ボタンをクリックして，属性リストを設定するための新規ウィンドウを開きます。
d. ［**Attribute Kind**］セクションで，［**User Attribute**］オプションを選択します。
e. ［**Attribute Fields**］セクションで，変数名として **SITESCOPE_ROLE** を選択し，SiteScope へのヘッダで送信されるあらかじめ設定されていたユーザ・ディレクトリから選択されたフィールドに属性名を選択します。これは認証用に送信されるユーザ・ディレクトリ属性です。

注: LDAP グループ・オブジェクトまたはネストされたグループ・オブジェクトを使用して SiteScope のロールを定義している場合は，［**変数名**］フィールドに特別な SiteMinder 変数が使用されます。通常のグループには **SM_USERGROUPS** 変数を使用し，ネストされたグループの情報を **SITESCOPE_ROLE** HTTP ヘッダに含める場合は，**SM_USERNESTEDGROUPS**を使用する必要があります。

5. SiteScope ルールと応答をセキュリティ・ポリシー・オブジェクトへ追加します。
   a. ［**Policies**］オプションをクリックして，新規セキュリティ・ポリシーを作成します。
   b. ポリシーに分かりやすい名前を入力します。例：**SiteScope Policy**。
   c. ［**Users**］タブをクリックして，ポリシーを適用するエンティティを追加または削除します（領域の同じドメインの一部であるユーザ・ディレクトリからのみエンティティを選択できます）。
   d. ［**Rules**］タブをクリックして，手順 3 で説明した 2 つのルール，**Users Role** と **SiteScopeSiteScope Rule** を選択します。さらに，手順 4 のユーザ・ロールの応答として以前に定義された **SiteScope Role** 応答を追加します。

SiteMinder を使用するための SiteScope の設定

SiteScope を SiteMinderと統合できるようにするには，Tomcat サーバが使用する設定ファイルを変更する必要があります。Tomcat サーバ・ファイルの設定の詳細については，「Apache Tomcat サーバ・ファイルの設定」(206ページ)を参照してください。

IIS の設定

Tomcat サーバが使用する設定ファイルに変更を行ったら，IIS を設定する必要があります。IIS 設定の詳細については，「IIS の設定」(209ページ)を参照してください。

さまざまな SiteScope ロールの権限の定義

SiteMinder との統合が有効になったら，（SiteScope の通常ユーザの権限モデルを使用して）SiteScope のロールごとに権限を定義しなければなりません。このロールへのユーザの関連付けは，LDAP グループ内など，SiteScope 外で行われます。新規 SiteScope ユーザが追加されたら，これは SiteMinder でのみ定義されなければなりません。ユーザは自動的に関連する SiteScope ロールから権限を継承するためです。

注: SiteMinder が使用する SiteScope ユーザ・アカウントにはパスワードが必要ないことを確認してください。パスワードがあると SiteMinder はログオンできなくなります。ユーザ・アカウントの作成の詳細については，SiteScope ヘルプで『SiteScope の使用』の「ユーザ管理プリファレンス」セクションを参照してください。

SiteScope へのログオン

ユーザが SiteScope にログオンを試みると，SiteMinder が要求を傍受します。SiteMinder がユーザの資格情報を認証すると，SiteScope ユーザ名とロール（グループ）が SiteScope に割り当てられます（例: ユーザ :Fred，ロール :Accounting）。SiteScopeでユーザ名が有効なユーザ名として認識されなくてもロールが認識されれば，そのロールで SiteScope にログインできます（先の例では，ユーザ :Accounting）。

SiteScope にログオンするには，次の手順で行います。

Web ブラウザを開き，次の URL を入力します。

http://<IIS マシン名>/SiteScope

注: IIS と SiteScope が同じマシンにある場合は，ポート 8080 ではなく標準設定のポート 80 に接続しなければなりません。

SiteMinder がユーザの認証に成功し，SiteScope にログオンすると，直接 SiteScope がダッシュボード・ビューを開きます。

注意事項とガイドライン

- SiteScope にログインしたすべてのユーザ名は監査ログに一覧表示されます。監査ログは，**<SiteScope のルート・ディレクトリ>\logs** ディレクトリにあります。これは，ユーザがロール名でログインした場合も同様です。たとえば，Fred というユーザが，SiteScope によって Fred が有効なユーザとして認識されないがロールは認識されたため，ロールでログインした場合でも，すべての操作は監査ログでユーザ名 Fred で一覧表示されます。
- SiteMinder 環境からログアウトした後でブラウザがリダイレクトされるページを指定できます（これは，SiteScope で［**ログアウト**］ボタンをクリックすると開くページです）。ログアウト・

ページを有効にするには，**<SiteScope のルート・ディレクトリ>\groups** にある **master.config** ファイルを開いて次の行を追加します。

_siteMinderRedirectPageLogout=<url_to_go_to_after_logout>

- SiteMinder が SiteScope にログオンするときに使用するユーザ・アカウントにはパスワードを設定してはなりません。さもないと SiteMinderがログオンできなくなります。SiteScope でのユーザ・アカウントの設定の詳細については，SiteScope ヘルプにある『SiteScope の使用』の「ユーザ管理プリファレンス」セクションを参照してください。
- ユーザが SiteScope URL を使用して SiteScope に直接アクセスするのを防ぐため，SiteScope のインストール時に Tomcat サーバで HTTP ポート 8080 および 8888 を無効にすることを検討してください。
- Web ブラウザが無効になってから 30 分後にユーザが SiteScope からログアウトされないようにするため，**master.config** ファイルの "_keepAliveFromJSP=" プロパティを "=true" に変更してください。

付録C: セキュア接続を使用するための SiteScope の手動による設定

セキュア接続を使用して SiteScope インタフェースへのアクセスを制限するよう，SiteScope を手動で設定できます。

強化ツールを使用して，SSL を使用するために SiteScope を設定することを推奨します。詳細については，「強化ツールの使用」(176ページ)を参照してください。

本項の内容

- 「TLS の使用に向けた SiteScope の準備」(219ページ)
- 「Tomcat 上の TLS 用の SiteScope の設定」(223ページ)
- 「相互 TLS 構成用の SiteScope の設定」(225ページ)
- 「SiteScope を TLS デプロイメントの BSM サーバに接続するための設定」(226ページ)
- 「クライアント証明書が必要な BSM サーバに SiteScope を接続する設定」(226ページ)
- 「BSM サーバがクライアント証明書を必要とするときの SiteScope でのトポロジ・ディスカバリ・エージェントの設定方法」(229ページ)

TLS の使用に向けた SiteScope の準備

SiteScope には **Keytool.exe** が付属しています。Keytool は，鍵および証明書管理ユーティリティです。Keytool により，ユーザは，デジタル署名を使用した認証のための自分の公開鍵/秘密鍵ペアおよび関連する証明書を管理できます。また，通信するほかのユーザおよび組織の公開鍵をキャッシュすることもできます。これは，**<SiteScope インストール・パス>\SiteScope\java\bin** ディレクトリにインストールされています。

注意: デジタル証明書を作成，要求，およびインストールする場合には，各手順で使用するパラメータおよびコマンド・ライン引数は非常に重要であり，繰り返し使用するものなので，必ずメモを取っておいてください。

注:

- SiteScope はキーストアとトラストストアを JKS フォーマットでのみ使用します。
- TLS で使用するために SiteScope クラシックのインタフェースを準備するには，Tomcat サーバ（「Tomcat 上の TLS 用の SiteScope の設定」(223ページ)を参照）および，クラシック・インタフェース・エンジン（「HTTPS を使用した SiteScope レポートおよびクラシック・ユーザ・インタフェースへのアクセス」(233ページ)の説明を参照）の両方を設定する必要があります。

詳細については，Oracle の Web サイト（http://docs.oracle.com/javase/7/docs/technotes/tools/windows/keytool.html）を参照してください。

本項の内容

- 「認証局からの証明書の使用」(220ページ)
- 「自己署名証明書の使用」(222ページ)

認証局からの証明書の使用

認証局が発行するデジタル証明書を使用できます。このオプションを使用するには，Keytool で使用されるキー・ストア・ファイルにインポート可能なデジタル証明書が必要です。自分の組織がこれに該当するデジタル証明書を持っていない場合は，認証局に証明書の発行を要求する必要があります。

キー・ストア・ファイルおよびデジタル証明書要求を作成するには，次の手順に従います。

認証局からの証明書を使用するには，次の手順を実行します。

1. 認証局からルート証明書とその他の中間証明書（存在する場合）を取得します。
2. ルート証明書とその他の中間証明書（存在する場合）を **<SiteScope ルート・ディレクトリ>\java\lib\security\cacerts** にインポートします。この操作は，ユーザ・インタフェースを使用するか，次のコマンドを実行することにより行います。

   keytool -import -alias yourCA -file C:\CAcertificate.cer -keystore ..\lib\security\cacerts -storepass changeit
3. **<SiteScope ルート・ディレクトリ>\groups** ディレクトリにある **serverKeystore** ファイルを削除します。このファイルは削除しても，単にほかのディレクトリに移動してもかまいません。
4. **<SiteScope ルート・ディレクトリ>\java\bin** ディレクトリから次のコマンドを実行し，鍵ペアを作成します。

   keytool -genkey -dname "CN=www.yourDomain.com, OU=yourDepartment, O=yourCompanyName, L=yourLocation, ST=yourState, C=yourCountryCode" -alias yourAlias -keypass keypass -keystore ..\..\groups\serverKeystore -storepass keypass -keyalg "RSA" -validity valdays

   注:
   - このコマンドおよびその他のコマンドはすべて，1 行で入力する必要があります。ここでは，ページに収まるようにコマンド・ラインを分割しています。
   - 証明書を生成するときに使用する serverKeystore 文字列は，本書に記載されているとおりに，大文字と小文字を区別して入力する必要があります。そうしないと、SiteScope Failover の使用時に失敗します。
   - IOException: Cannot recover key エラーを回避するため，プライベート・キー・パスワードとキーストア・パスワードは同一でなければなりません。

このコマンドにより，**<SiteScope ルート・ディレクトリ>\groups ディレクトリ**に**serverKeystore** というファイルが作成されます。SiteScope はこのファイルを使用して，セキュア・セッションで使用される証明書を格納します。このファイルのバックアップ・コピーを別の場所に保存しておいてください。

ガイドラインと制限事項

- -dname オプションの値は，ここに示す順に指定する必要があります。イタリック体で示されている部分には，各自の環境に合わせた値を指定します。キーワードは，次に示す項目の略語です。

  CN = commonName : 人名（例 : Warren Pease）

  OU = organizationUnit : 組織の小区分（例 : NetAdmin）

  O = organizationName : 組織の大区分（例 : ACMe-Systems, Inc.）

  L = localityName : 地域（都市）名（例 : Palo Alto）

  ST = stateName : 州名（例 : California）

  C = country : 2 文字の国コード（例 : US）

- -dname（識別名文字列）変数内のサブコンポーネントの大文字/小文字は区別されませんが，その順序は意味を持ちます（ただし，すべてのサブコンポーネントを指定する必要はありません）。-dname 変数は会社を表し，CN は SiteScope がインストールされている Web サーバのドメイン名です。

- -storepass の値は，キー・ストア・ファイルの保護に使用するパスワードです。パスワードは 6 文字以上で指定しなければなりません。キー・ストア・ファイルの証明書データのインポートや削除を行うには，このパスワードを使用する必要があります。

- -alias 変数は，キー・ストア内のエントリを識別するための別名またはニックネームです。

5. **<SiteScope のルート・ディレクトリ>\java\bin** ディレクトリで次のコマンドを実行して，このキーストアに対する証明書要求を作成します。

   keytool -certreq -alias yourAlias -file ..\..\groups\sis.csr -keystore ..\..\groups\serverKeystore -storepass passphrase

   このコマンドにより，**<SiteScope のルート・ディレクトリ>\groups** ディレクトリに「**sis.csr**」というファイルが作成されます。このファイルを使用して，認証局からの証明書を要求します。

   認証局から証明書を受け取ったら（応答メッセージに **cert.cer** という名前のファイルが含まれています），前述の手順で作成したキー・ストア・ファイルにこの証明書をインポートする必要があります。キー・ストア・ファイルの名前は **serverKeystore** になっています。SiteScope で使用するために証明書をインポートするには，次の手順を使用します。

6. **<SiteScope ルート・ディレクトリ>\java\bin** ディレクトリで次のコマンドを実行して，証明書データをキー・ストア・ファイルにインポートします。

   keytool -import -trustcacerts -alias yourAlias -file cert.cer -keystore ..\..\groups\serverKeystore

注: 認証局から証明書をインポートするときに keytool error: java.lang.Exception: Failed to establish chain from reply を回避するには，認証局から **<SiteScope ルート・ディレクトリ>\java\lib\security\cacerts** にルート証明書とその他の中間証明書（存在する場合）をインポートします。この操作を行うには，ユーザ・インタフェースから証明書管理を使用するか，次のコマンドを実行します。

keytool -import -alias yourCA -file C:\CAcertificate.cer -keystore ..\lib\security\cacerts -storepass changeit

7. 安全な接続を使用するように **SiteScope** を変更するには，**SiteScope** の特定の設定または設定ファイルを追加あるいは変更する必要があります。詳細については，「Tomcat 上の TLS 用の SiteScope の設定」(223ページ)を参照してください。

自己署名証明書の使用

自己署名証明書を生成して SiteScope を設定するときは，次のいずれかの方法を使用することもできます。

- **SSL ツール：** 詳細については，「SSL ツールを使用するには，次の手順を実行します。」(222ページ)を参照してください。
- **手動設定：** -selfcert オプションを使用して，Keytool ユーティリティで自己署名証明書を生成します。詳細については，「自己署名証明書を手動で生成するには，次の手順を実行します。」(222ページ)を参照してください。

注: ほとんどの場合は，SSL ツールを使用することをお勧めします。ただし，手動設定を使用する場合もあります。手動設定を使用するのは，Windows プラットフォーム上で SSL を使用するように SiteScope を設定し，%SITESCOPE_HOME% 変数を使用していない場合（たとえば，**go.bat** コマンドを使用して，SiteScope がすでに別の場所から起動されている場合），または Linux プラットフォーム上で SiteScope を **/opt/HP/SiteScope/** ディレクトリ以外にインストールしている場合です。

SSL ツールを使用するには，次の手順を実行します。

1. 次のコマンドを入力して SiteScope サービスを停止します。

   cd /opt/HP/SiteScope/
   ./stop

2. 次のコマンドを入力して SSL ツールを実行します。

   cd /opt/HP/SiteScope/tools/SSL/
   ./ssl_tool.sh

3. SSL ツールの指示に従います。

自己署名証明書を手動で生成するには，次の手順を実行します。

1. **<SiteScope ルート・ディレクトリ>\groups** ディレクトリにある **serverKeystore** ファイルを削除します。このファイルは削除しても，単にほかのディレクトリに移動してもかまいません。

2. **<SiteScope ルート・ディレクトリ>\java\bin** ディレクトリから次のコマンドを実行します。変数には，自分の組織に固有な情報を指定します。

   keytool -genkey -dname "CN=www.yourDomain.com, OU=yourDepartment, O=yourCompanyName, L=yourLocation, ST=yourState, C=yourCountryCode" -alias yourAlias -keypass keypass -keystore ..\..\groups\serverKeystore -storepass passphrase -keyalg "RSA" -validity valdays

   注:

   - このコマンドおよびその他のコマンドはすべて，1 行で入力する必要があります。ここでは，ページに収まるようにコマンド・ラインを分割しています。
   - 証明書を生成するときに使用する serverKeystore 文字列は，本書に記載されているとおりに，大文字と小文字を区別して入力する必要があります。そうしないと、SiteScope Failover の使用時に失敗します。

3. **<SiteScope ルート・ディレクトリ>\java\bin** ディレクトリから次のコマンドも実行します。

   keytool -selfcert -alias yourAlias -sigalg "MD5withRSA" -keypass password -dname "CN=www.yourDomain.com, OU=yourDepartment, O=yourCompanyName, L=yourLocation, ST=yourState, C=yourCountryCode" -keystore ..\..\groups\serverKeystore

4. 安全な接続を使用するように SiteScope を変更するには，SiteScope の特定の設定または設定ファイルを追加あるいは変更する必要があります。詳細については，「Tomcat 上の TLS 用の SiteScope の設定」(223ページ)を参照してください。
5. 必要に応じて，次のコマンドを実行することで，BSM で使用する証明書をエクスポートできます。

   keytool -exportcert -alias yourAlias -file <SiteScope root directory>\certificate_name.cer -keystore ..\..\groups\serverKeystore

   入力を促すメッセージが表示されたら，キーストア・パスワードを入力します。

Tomcat 上の TLS 用の SiteScope の設定

Tomcat で TLS を有効にするには，Tomcat サーバが使用する設定ファイルを変更する必要があります。

1. **< SiteScope のルート・ディレクトリ > \Tomcat\conf** ディレクトリにある **server.xml** ファイルを開きます。
2. 設定ファイルの次のようなセクションを探します。

```
<!-- Define a SSL Coyote HTTP/1.1 Connector on port 8443 -->
<!--
Connector port="8443" maxHttpHeaderSize="8192"
maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
enableLookups="false" disableUploadTimeout="true"
acceptCount="100" scheme="https" secure="true"
```

```
clientAuth="false" sslProtocol="TLS"
compression="on" compressionMinSize="2048" noCompressionUserAgents="gozilla, traviata"
compressableMimeType="text/html,text/xml,text/javascript,text/css,image/x-icon,application/json" />
-->
```

3. このセクションを次のように変更します。

```
<!-- Define a SSL Coyote HTTP/1.1 Connector on port 8443 -->

<Connector port="8443"
maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
enableLookups="false" disableUploadTimeout="true"
acceptCount="100" debug="0" scheme="https" secure="true"
clientAuth="false" sslEnabledProtocols="TLSv1,TLSv1.1,SSLv2Hello"
keystoreFile="<SiteScope のインストール・パス>\SiteScope\groups\serverKeystore"
keystorePass="testing"
/>
```

<SiteScope のインストール・パス> は，SiteScope のインストール先のパスです。

注:

- SiteScope と同じサーバにほかの HP 製品がインストールされている場合は，競合を回避するために，ポート 8443 を別のポートに変更しなければならない場合があります。
- Tomcat ログ出力は，**<SiteScope のルート・ディレクトリ>\logs\tomcat.log** ファイルに書き込まれます。ログ・ファイルの設定は，**<SiteScope のルート・ディレクトリ>\Tomcat\common\classes\log4j.properties** ファイルで実行できます。
- 弱い Cipher を無効化することで，Tomcat サーバのセキュリティを強化できます。このためには，**<SiteScope のルート・ディレクトリ>\Tomcat\conf\server.xml** を開いて，既存のリストを次のように変更します。

  <Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
  maxThreads="150" scheme="https" secure="true" clientAuth="false"
  sslEnabledProtocols="TLSv1,TLSv1.1,SSLv2Hello" ciphers="SSL_RSA_WITH_RC4_128_SHA,
  TLS_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_
  DSS_WITH_AES_128_CBC_SHA, SSL_RSA_WITH_3DES_EDE_CBC_SHA, SSL_DHE_RSA_WITH_
  3DES_EDE_CBC_SHA, SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA"/>]

標準設定では，Tomcat は SiteScope ユーザのホーム・ディレクトリにある **.keystore** ファイルを探します。

Tomcat サーバ用に TLS を有効にする方法については，http://tomcat.apache.org/tomcat-5.5-doc/ssl-howto.html を参照してください。

4. この例を使用して Tomcat で TLS を有効にしたら，次の URL で，SiteScope インタフェースを利用できるようになります。

   https://<SiteScope サーバ>:8443/SiteScope（リンクは大文字と小文字が区別されます）

相互 TLS 構成用の SiteScope の設定

SiteScope サーバがクライアントからのクライアント証明書を要求する場合，次の手順を実行します。

1. SiteScope は TLS で設定する必要があります。詳細については，「Tomcat 上の TLS 用の SiteScope の設定」(223ページ)を参照してください。
2. **<SiteScope のルート・ディレクトリ>\Tomcat\conf\server.xml** 設定ファイルの次のセクションを見つけて，クライアント証明書を要求するように Tomcat サーバを設定します。

```
<Connector port="8443"
    maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
    enableLookups="false" disableUploadTimeout="true"
    acceptCount="100" debug="0" scheme="https" secure="true"
    sslEnabledProtocols="TLSv1,TLSv1.1,SSLv2Hello"
    keystoreFile="..\groups\serverKeystore"
    keystorePass="changeit"
```

そして次の属性を追加して，clientAuth="true" を変更します：

```
     truststoreFile="..\java\lib\security\cacerts"
    truststorePass="changeit"
    truststoreType="JKS"
    clientAuth="true"
/>
```

3. 次のコマンドを実行して，クライアント証明書を所属する組織に対して発行する認証局のルート証明書を SiteScope トラストストアにインポートします（**<SiteScope のルート・ディレクトリ>\java\lib\security\cacerts**）。

```
C:\SiteScope\java\>keytool -import -trustcacerts -alias <別名> -keystore ..\lib\security\
  cacerts -file <証明書ファイル>
```

4. クライアント証明書を作成するか，既存のものをブラウザにインポートします。
5. SiteScope を再起動して，次のリンクを使用してそれにアクセスします。

   https://<サーバ>:8443/SiteScope（リンクは大文字と小文字が区別されます）

注:

SiteScope SOAP API の呼び出しも証明書が必要です。次を Java コードに追加してクライアント証明書に対応します。

System.setProperty("javax.net.ssl.keyStore",<JKS 形式のクライアント証明書キーストアへのパス名>);

System.setProperty("javax.net.ssl.keyStorePassword", <クライアント証明書キーストアのパスワード>);

（任意指定）System.setProperty（"javax.net.ssl.trustStore"，<JKS 形式のトラストストアへのパス名>）；

または次の JVM 引数を使用します。

-Djavax.net.ssl.keyStore=<JKS 形式のクライアント証明書キーストアへのパス名>

-Djavax.net.ssl.keyStorePassword=<クライアント証明書キーストアのパスワード>

（任意指定）-Djavax.net.ssl.trustStore=<JKS 形式のトラストストアへのパス名>

SiteScope を TLS デプロイメントの BSM サーバに接続するための設定

TLS デプロイメントを使用する BSM サーバに SiteScope を接続するには，次の手順で行います。

1. SiteScope サーバに接続します。
2. SiteScope のユーザ・インタフェースで［証明書管理］を使用して，CA ルート証明書または BSM サーバ証明書を SiteScope にインポートします。詳細については，SiteScopeヘルプで『SiteScope の使用ガイド』の「証明書管理」セクションを参照してください。
3. BSM がロード・バランサを使用して設定されている場合，SiteScope のユーザ・インタフェースで［証明書管理］を使用して，Load Balance Core および Center URL の証明書を SiteScope にインポートします。詳細については，SiteScopeヘルプで『SiteScope の使用ガイド』の「証明書管理」セクションを参照してください。
4. 証明書を BSM にインポートする方法の詳細については，BSM 文書ライブラリで『BSM Hardening Guide』の「SiteScope」セクションを参照してください。

クライアント証明書が必要な BSM サーバに SiteScope を接続する設定

クライアント証明書を要求する BSM サーバに SiteScope を接続するには，次の手順で行います。

1. SiteScope サーバに接続します。
2. SiteScope のユーザ・インタフェースで［証明書管理］を使用して，CA ルート証明書または BSM サーバ証明書を SiteScope にインポートします。詳細については，SiteScopeヘルプで『SiteScope の使用ガイド』の「証明書管理」セクションを参照してください。
3. JKS 形式でクライアント証明書を取得した場合は，**<SiteScope のルート・ディレクトリ>\templates.certificates** フォルダにそれをコピーして，手順 11 から続行します。

注:

- プライベート・キー・パスワードが少なくとも 6 文字であること，またプライベート・キーとキーストア・パスワードが同一であることを確認します。
- さらに，上記のキーストアにキーストアを発行した CA 証明書が含まれていることを確認します。

ほかの形式でクライアント証明書を取得した場合は，次の手順を実行してください。

4. **<SiteScope のルート・ディレクトリ>\java\bin** ディレクトリで次のコマンドを実行して，**<SiteScope のルート・ディレクトリ>/templates.certificates** の下にキーストアを作成します。

   keytool -genkey -keyalg RSA -alias sis -keystore
   <SiteScope root directory>\templates.certificates\.ks -storepass
   <your_keystore_password>

   例：

   keytool -genkey -keyalg RSA -alias sis -keystore C:\SiteScope\templates.certificates\.ks -storepass changeit
   What is your first and last name?
   [Unknown]:domain.name
   What is the name of your organizational unit?
   [Unknown]:dept
   What is the name of your organization?
   [Unknown]:XYZ Ltd
   What is the name of your City or Locality?
   [Unknown]:New York
   What is the name of your State or Province?
   [Unknown]:USA
   What is the two-letter country code for this unit?
   [Unknown]:US
   Is CN=domain.name, OU=dept, O=XYZ Ltd, L=New York, ST=USA, C=US correct?
   [no]:yes

   Enter key password for <SiteScope>

   キーストアのパスワードと同じパスワードを使用するには，ENTER キーを押します。

5. **<SiteScope のルート・ディレクトリ>\java\bin** ディレクトリで次のコマンドを実行して，このキーストアに対する証明書要求を作成します。

   keytool -certreq -alias sis -file c:\sis.csr -keystore
   <SiteScope root directory>\templates.certificates\.ks -storepass
   <your_keystore_password>

   例：

   keytool -certreq -alias sis -file c:\sis.csr -keystore
   C:\SiteScope\templates.certificates\.ks -storepass changeit

6. 認証局から証明書要求に対する署名を受けます。**.csr** ファイルの内容をコピーして，証明局の Web フォームに貼り付けます。
7. 署名付きのクライアント証明書を BASE-64 形式で **<SiteScope のルート・ディレクトリ>\templates.certificates\clientcert.cer** にダウンロードします。
8. BASE-64 形式で認証局の証明書を c:\ にダウンロードします。
9. 次のコマンドを実行して，認証局の証明書を JKS キーストアにインポートします。

   keytool -import -alias ca -file c:\ca.cer -keystore
   <SiteScope root directory>\templates.certificates\.ks -storepass
   <your_keystore_password>

   例：

   keytool -import -alias ca -file c:\ca.cer -keystore C:\SiteScope\templates.certificates\.ks -storepass changeit
   Owner:CN=dept-CA, DC=domain.name
   Issuer:CN=dept-CA, DC=domain.name
   Serial number:2c2721eb293d60b4424fe82e37794d2c
   Valid from:Tue Jun 17 11:49:31 IDT 2008 until:Mon Jun 17 11:57:06 IDT 2013
   Certificate fingerprints:
   MD5:14:59:8F:47:00:E8:10:93:23:1C:C6:22:6F:A6:6C:5B
   SHA1:17:2F:4E:76:83:5F:03:BB:A4:B9:96:D4:80:E3:08:94:8C:D5:4A:D5
   Trust this certificate?[no]:yes
   Certificate was added to keystore

10. 次のコマンドを実行して，クライアント証明書をキーストアにインポートします。

    keytool -import -alias sis -file
    <SiteScope root directory>\templates.certificates\certnew.cer -keystore
    <SiteScope root directory>\templates.certificates\.ks -storepass
    <your_keystore_password>

    例：

    keytool -import -alias sis -fil c:\SiteScope\templates.certificates\certnew.cer -keystore C:\SiteScope\templates.certificates\.ks -storepass changeit

    証明書の応答は，**<SiteScope のルート・ディレクトリ>\java\bin** ディレクトリのキーストアにインストールされます。

11. **<SiteScope のルート・ディレクトリ>\java\bin** ディレクトリから次のコマンドを実行してキーストアの内容を確認し，キーストアのパスワードを入力します。

    keytool -list -keystore <SiteScope root directory>\templates.certificates\.ks

    例：

    keytool -list -keystore C:\SiteScope\templates.certificates\.ks
    Enter keystore password:changeit

```
Keystore type:jks
Keystore provider:SUN

Your keystore contains 2 entries
ca, Mar 8, 2009, trustedCertEntry,
Certificate fingerprint (MD5):14:59:8F:47:00:E8:10:93:23:1C:C6:22:6F:A6:6C:5B
sis, Mar 8, 2009, keyEntry,
Certificate fingerprint (MD5):C7:70:8B:3C:2D:A9:48:EB:24:8A:46:77:B0:A3:42:E1

C:\SiteScope\java\bin>
```

12. クライアント証明書にこのキーストアを使用するには，**<SiteScope のルート・ディレクトリ>\groups\master.config** ファイルに次の行を追加します。

    _urlClientCert=<keystoreName>

    _urlClientCertPassword=<keystorePassword>

    例：

    _urlClientCert=.ks
    _urlClientCertPassword=changeit

13. 変更点をファイルに保存します。
14. ［**SiteScope プリファレンス**］ > ［**統合プリファレンス**］ > ［**BSM プリファレンス利用可能操作**］を選択し，［**リセット**］をクリックして，SiteScope サーバからすべての BSM 関連設定を削除し，BSM からすべての SiteScope 設定を削除します。
15. SiteScope サーバを再起動します。
16. BSM で，［**管理**］ > ［**システム可用性管理**］を選択し，［**新規 SiteScope**］ボタンをクリックして，SiteScope インスタンスを追加します。

    注: SiteScope と BSM 間の接続に失敗した場合は，**<SiteScope のルート・ディレクトリ>\log\bac_integration.log** にエラーがないか調べます。

BSM サーバがクライアント証明書を必要とするときの SiteScope でのトポロジ・ディスカバリ・エージェントの設定方法

クライアント証明書を使用して BSM ゲートウェイ・サーバに接続するように SiteScope を設定した後で（「クライアント証明書が必要な BSM サーバに SiteScope を接続する設定」(226ページ)を参照），ディスカバリが BSM サーバにトポロジをレポートするように次の手順を実行する必要があります。

1. **<SiteScope のルート・ディレクトリ>\WEB-INF\classes** で **security** という名前のフォルダを（存在しない場合）作成します。
2. **MAMTrustStoreExp.jks** と **ssl.properties** を **<SiteScope のルート・ディレクトリ>\WEB-INF\classes** から**<SiteScope のルート・ディレクトリ>\WEB-INF\classes\security** フォルダに移動します。
3. CA ルート証明書（または BSM サーバ証明書）をディスカバリ・トラストストア（**MAMTrustStoreExp.jks**）にパスワードとともにインポートします（ディスカバリ・トラストストアの標準設定のパスワードは **logomania** で，次のように暗号化されます。 [22,-8,116,-119,-107,64,49,93,-69,57,-13,-123,-32,-114,-88,-61]):

   keytool -import -alias <your_CA> -keystore <SiteScope のルート・ディレクトリ>\WEB-INF\classes\security\MAMTrustStoreExp.jks -storepass <your_keystore_password>

   例：

   keytool -import -alias AMQA_CA -file c:\ca.cer -keystore C:\SiteScope\WEB-INF\classes\security\MAMTrustStoreExp.jks -storepass logomania

   注: プライベート・キー・パスワードは少なくとも 6 文字でなければなりません。またプライベート・キーとキーストアのパスワードは同一でなければなりません。

4. 次のコマンドを使用してトラストストアのコンテンツを確認します。

   <SiteScope のルート・ディレクトリ>\java\bin>keytool -list -keystore <SiteScope のルート・ディレクトリ>\WEB-INF\classes\security\MAMTrustStoreExp.jks -storepass <your_keystore_password>
   Keystore type:<Keystore_type>
   Keystore provider:<Keystore_provider>
   Your keystore contains 2 entries mam, Nov 4, 2004, trustedCertEntry,Certificate fingerprint (MD5): <Certificate_fingerprint> amqa_ca, Dec 30, 2010, trustedCertEntry,Certificate fingerprint (MD5): <Certificate_fingerprint>

   例：

   C:\SiteScope\java\bin>keytool -list -keystore C:\SiteScope\WEB-INF\classes\security\MAMTrustStoreExp.jks -storepass logomania

   Keystore type:JKS
   Keystore provider:SUN

   Your keystore contains 2 entries

   mam, Nov 4, 2004, trustedCertEntry,
   Certificate fingerprint (MD5):C6:78:0F:58:32:04:DF:87:5C:8C:60:BC:58:75:6E:F7
   amqa_ca, Dec 30, 2010, trustedCertEntry,
   Certificate fingerprint (MD5):5D:47:4B:52:14:66:9A:6A:0A:90:8F:6D:7A:94:76:AB

5. SiteScope クライアント・キーストア（.ks）を**<SiteScope のルート・ディレクトリ>\templates.certificates** から **<SiteScope のルート・ディレクトリ>SiteScope\WEB-INF\classes\security** にコピーします。
6. **ssl.properties** ファイルで，**javax.net.ssl.keyStore** プロパティをキーストア名に更新します。たとえば，javax.net.ssl.keyStore=.ks です。
7. キーストアのディスカバリ・パスワード（標準設定は logomania）を一致させるために SiteScope クライアント・キーストア・パスワードを変更します。

   keytool -storepasswd -new <Discovery_keystore_password> -keystore <SiteScope のルート・ディレクトリ>\WEB-INF\classes\security\.ks -storepass <your_keystore_password>

   例：

   keytool -storepasswd -new logomania -keystore C:\SiteScope\WEB-INF\classes\security\.ks -storepass changeit

8. キーストアのディスカバリ・パスワードを一致させるためにプライベート・キー・パスワードを変更します。

   keytool -keypasswd -alias sis -keypass <your_keystore_password> -new <Discovery_keystore_password> -keystore <SiteScope のルート・ディレクトリ>\WEB-INF\classes\security\.ks -storepass <your_keystore_password>

   例：

   keytool -keypasswd -alias sis -keypass changeit -new logomania -keystore C:\SiteScope\WEB-INF\classes\security\.ks -storepass logomania

9. 新しいパスワードを使用してキーストアを確認します。

   keytool -list -v -keystore <SiteScope のルート・ディレクトリ>\WEB-INF\classes\security\.ks -storepass <your_keystore_password>

   例：

   keytool -list -v -keystore C:\SiteScope\WEB-INF\classes\security\.ks -storepass logomania

10. SiteScope サーバを再起動します。
11. BSM で，［**管理**］ > ［**システム可用性管理**］を選択し，［**新規 SiteScope**］ボタンをクリックして，SiteScope インスタンスを追加します。［プロファイル設定］ペインで，［**BSM フロントエンドは HTTPS を使用します**］チェック・ボックスを必ず選択します。
12. **［BSM］ > ［管理］ >** ［**RTSM** 管理］ > **［IT ユニバース マネージャ］ > ［システム モニタ］** ビューにトポロジが表示されていることをチェックします。

トラブルシューティング

- 次のエラーについては，**<SiteScope のルート・ディレクトリ>\logs\bac_integration** に配置されている **bac-integration.log** を確認します。

```
2010-12-30 11:03:06,399 [TopologyReporterSender] (TopologyReporterSender.java:364)
 ERROR - failed to run main topology agent. topologyCommand=TopologyCommand
{commandType=RUN_SCRIPT, …
java.lang.IllegalArgumentException:cannot find script with name=create_monitor.py
at com.mercury.sitescope.integrations.bac.topology.dependencies.DependenciesCrawler.
findDependencies(DependenciesCrawler.java:60)
at com.mercury.sitescope.integrations.bac.topology.dependencies.
ScriptDependenciesFinder.find(ScriptDependenciesFinder.java:80)
at com.mercury.sitescope.integrations.bac.topology.TopologyReporterSender.
getDependencies(TopologyReporterSender.java:552)
at com.mercury.sitescope.integrations.bac.topology.TopologyReporterSender.
send(TopologyReporterSender.java:347)
at com.mercury.sitescope.integrations.bac.topology.TopologyReporterSender.
run(TopologyReporterSender.java:304)
at java.lang.Thread.run(Thread.java:619)
```

- 証明書およびキーストアのパスワードが同一であることを確認します。

付録D: HTTPS を使用した SiteScope レポートおよびクラシック・ユーザ・インタフェースへのアクセス

https プロトコルを経由したアクセスでの SSL 接続を使用するよう SiteScope Web サーバをセットアップできます。本項では，これを行うために必要な手順について説明します。

本項では次について説明します。

- 「SiteScope の証明書を使った作業について」(233ページ)
- 「認証局からの証明書の使用」(233ページ)
- 「自己署名証明書の使用」(235ページ)

SiteScope の証明書を使った作業について

SiteScope には **Keytool.exe** が付属しています。Keytool は，鍵および証明書管理ユーティリティです。Keytool により，ユーザは，デジタル署名を使用した認証のための自分の公開鍵/秘密鍵ペアおよび関連する証明書を管理できます。また，通信対象の当事者の公開鍵をキャッシュすることもできます。Keytool は，**<SiteScope インストール・パス>\SiteScope\java\bin** ディレクトリにインストールされています。

注: デジタル証明書を作成，要求，およびインストールするプロセスは，細かい注意が必要です。各手順で使用するパラメータおよびコマンド・ライン引数は，手順全体をとおして同じ値を使用する非常に重要なものなので，必ずメモを取っておいてください。

Keytool の詳細については，次の Sun Microsystems の Web サイトを参照してください。

http://java.sun.com/j2se/1.3/docs/tooldocs/win32/keytool.html

認証局からの証明書の使用

認証局によって発行されたデジタル証明書を使用するには，次の手順を実行します。このオプションを使用するには，Keytool で使用されるキー・ストア・ファイルにインポート可能なデジタル証明書が必要です。所属する組織がこれに該当するデジタル証明書を持っていない場合は，認証局に証明書の発行を要求する必要があります。

認証局からの証明書を使用するには，次の手順を実行します。

1. **<SiteScope のルート>\groups** ディレクトリにある **serverKeystore** ファイルを削除します。このファイルは削除しても，単にほかのディレクトリに移動してもかまいません。

注: 下記に示されている手順を実行する前にこのファイルを削除する必要があります。

2. 次に鍵のペアを作成する必要があります。これを行うには，**<SiteScope ルート>\java\bin** ディレクトリから下記のコマンド・ラインを実行する必要があります。

   注: 変数には，所属する組織に固有の情報を指定します。

   このコマンドおよびその他のコマンドはすべて，1 行で入力する必要があります。ここでは，ページに収まるようにコマンド・ラインを分割しています。

   keytool -genkey -dname "CN=www.yourDomain.com, OU=yourDepartment, O=yourCompanyName, L=yourLocation, S=yourState, C=yourCountryCode" -alias yourAlias -keypass keypass -keystore ..\..\groups\serverKeystore -storepass passphrase -keyalg "RSA" -validity valdays

   このコマンドにより，**SiteScope\groups ディレクトリ**に「**serverKeystore**」というファイルが作成されます。SiteScope はこの KeyStore ファイルを使用して，セキュア・セッションで使用される証明書を格納します。このファイルのバックアップ・コピーを別の場所に保存しておいてください。

   -dname オプションの値は，ここに示す順に指定する必要があります。イタリック体で示されている部分には，各自の環境に合わせた値を指定します。キーワードは，次に示す項目の略語です。

   CN = commonName : 人名（例 : 「Warren Pease」）

   OU = organizationUnit : 組織の小区分（例 : 「NetAdmin」）

   O = organizationName : 組織の大区分（例 : 「ACMe-Systems, Inc.」）

   L = localityName : 地域（都市）名（例 : 「Palo Alto」）

   ST = stateName : 州名（例 : 「California」）

   C = country : 2 文字の国コード（例 : 「US」）

   - **-dname**（識別名文字列）変数内のサブコンポーネントの大文字/小文字は区別されませんが，その順序は意味を持ちます（ただし，すべてのサブコンポーネントを指定する必要はありません）。-dname 変数は会社を表し，CN は SiteScope がインストールされている Web サーバのドメイン名です。
   - -storepass には，キー・ストア・ファイルを保護するためのパスワードを指定します。パスワードは 6 文字以上で指定しなければなりません。キー・ストア・ファイルとの間で証明書のインポートや削除を行うには，このパスワードを使用する必要があります。
   - -alias 変数は，キー・ストア内のエントリを識別するための別名またはニックネームです。

3. 証明書要求ファイルを作成します。これを行うには，**<SiteScope ルート>\java\bin** ディレクトリで次のコマンドを実行します。

   keytool -certreq -alias yourAlias -file ..\..\groups\filename.csr -keypass keypass -keystore ..\..\groups\serverKeystore -storepass passphrase -keyalg "RSA"

このコマンドにより要求ファイルとして使用される .csr が生成されます。このファイルを証明書に対する要求とともに認証局（CA）に送信する必要があります。認証局から証明書を受け取ったら（応答に **cert.cer** という名前のファイルが含まれています），前述の手順で作成したキー・ストア・ファイルにこの証明書をインポートする必要があります。キー・ストア・ファイルの名前は **serverKeystore** になっています。次の手順を実行して証明書をインポートします。

4. 証明書データをキー・ストア・ファイルにインポートするには，**SiteScope\java\bin** ディレクトリから次のコマンドも実行します。

   keytool -import -trustcacerts -alias yourAlias -file cert.cer -keystore ..\..\groups\serverKeystore

5. セキュアな接続を使用するように SiteScope を変更するには，**<SiteScope ルート >\groups\master.config** ファイル内の次のパラメータを追加または変更する必要があります。

   _httpSecurePort=8899

   _httpSecurePort パラメータで使用する数は，使用可能な任意のポート番号に設定できます。ポート番号は，HTTP（セキュアでない）を使用して SiteScope にアクセスするための標準設定ポートである 8888 以外を使用することを推奨します。

   HTTPS のみを使用して SiteScope にアクセスするには，**master.config** ファイル内の次のパラメータを以下に示すように，各項目の該当する値を代入して，変更する必要があります。

   _httpPort=

   _httpSecurePort=8899

   _httpSecureKeyPassword=passphrase

   _httpSecureKeystorePassword=keypass

   注: master.config ファイルのすべてのパラメータは大文字と小文字を区別し，構文に依存します。ファイルに余分なスペースや行を追加しないようにします。

6. **master.config** ファイルへの変更を保存します。
7. 変更を有効にするには SiteScope サービスを停止して再起動します。

これで，HTTP を使用して SiteScope にアクセスできるようになります。たとえば，ファイアウォールの内側からアクセスする場合の標準設定のアドレスは次のとおりです。

http://server_IP_address:8888

上記で説明した手順に基づき，次のアドレスで，HTTPS を使用して SiteScope にアクセスすることも可能です。

https://server_IP_address:8899

自己署名証明書の使用

自己署名証明書を生成することもできます。これを行うには，Keytool ユーティリティで -selfcert オプションを使用して自己署名証明書を生成します。

自己署名証明書を使用するには，次の手順で行います。

1. **<SiteScope のルート>\groups** ディレクトリにある **serverKeystore** ファイルを削除します。このファイルは削除しても，単にほかのディレクトリに移動してもかまいません。

   注: 下記に示されている手順を実行する前にこのファイルを削除する必要があります。

2. 次に，**<SiteScope ルート>\java\bin** ディレクトリで次のコマンドを実行します。

   注: 変数には，所属する組織に固有の情報を指定します。

   このコマンドおよびその他のコマンドはすべて，1 行で入力する必要があります。ここでは，ページに収まるようにコマンド・ラインを分割しています。

   keytool -genkey -dname "CN=www.yourDomain.com, OU=yourDepartment, O=yourCompanyName, L=yourLocation, S=yourState, C=yourCountryCode" -alias yourAlias -keypass keypass -keystore ..\..\groups\serverKeystore -storepass passphrase -keyalg "RSA" -validity valdays

3. 次に，**SiteScope\java\bin** ディレクトリで次のコマンドを実行します。

   keytool -selfcert -alias yourAlias -sigalg "MD5withRSA" -keypass password -dname "CN=www.yourDomain.com, OU=yourDepartment, O=yourCompanyName, L=yourLocation, S=yourState, C=yourCountryCode" -keystore ..\..\groups\serverKeystore

4. セキュアな接続を使用するように SiteScope を変更するには，**<SiteScope ルート>\groups\master.config** ファイル内の次のパラメータを追加または変更する必要があります。

   _httpSecurePort=8899

   _httpSecurePort パラメータで使用する数は，使用可能な任意のポート番号に設定できます。ポート番号は，HTTP（セキュアでない）を使用して SiteScope にアクセスするための標準設定ポートである 8888 以外を使用することを推奨します。

   HTTPS のみを使用して SiteScope にアクセスするには，master.config ファイル内の次のパラメータを以下に示すように，各項目の該当する値を代入して，変更する必要があります。

   _httpPort=

   _httpSecurePort=8899

   _httpSecureKeyPassword=passphrase

   _httpSecureKeystorePassword=keypass

   注: master.config ファイルのすべてのパラメータは大文字と小文字を区別し，構文に依存します。ファイルに余分なスペースや行を追加しないようにします。

5. **master.config** ファイルへの変更を保存します。
6. 変更を有効にするには SiteScope サービスを停止して再起動します。

これで，HTTP を使用して SiteScope にアクセスできるようになります。たとえば，ファイアウォールの内側からアクセスする場合の標準設定のアドレスは次のとおりです。

http://server_IP_address:8888

上記で説明した手順に基づき，次のアドレスで，HTTPS を使用して SiteScope にアクセスすることも可能です。

https://server_IP_address:8899

ドキュメントに関するフィードバックの送信

本書に関してコメントがある場合は，電子メールでドキュメント・チームにご連絡ください。電子メール・クライアントがこのシステム上で設定されている場合は，上にあるリンクをクリックすると，件名の行に以下の情報が付いた電子メールのウィンドウが開きます。

デプロイメント・ガイド に関するフィードバック（SiteScope 11.30）

電子メールにお客様のフィードバックを追加し，送信をクリックしてください。

使用できる電子メール・クライアントがない場合は，上記の情報を Web メール・クライアントの新しいメッセージにコピーして，フィードバックを SW-doc@hp.com に送信してください。

お客様のフィードバックをお待ちしております。