HP Business Availability Center

Windows および Solaris オペレーティング・システム用

ソフトウェア・バージョン : 7.50

HP SiteScope デプロイメント・ガイド

文書番号 :BACSIS7.50JP/01
文書発行日 : 2008 年 5 月 （英語版）
ソフトウェア・リリース日 : 2008 年 5 月（英語版）

invent

利用条件

保証

HP の製品およびサービスの保証は，かかる製品およびサービスに付属する明示的な保証の声明において定められている保証に限ります。本文書の内容は，追加の保証を構成するものではありません。HP は，本文書に技術的な間違いまたは編集上の間違い，あるいは欠落があった場合でも責任を負わないものとします。

本文書に含まれる情報は，事前の予告なく変更されることがあります。

制限事項

本コンピュータ・ソフトウェアは，機密性があります。これらを所有，使用，または複製するには，HP からの有効なライセンスが必要です。FAR 12.211 および 12.212 に従って，商用コンピュータ ソフトウェア，コンピュータ ソフトウェアのドキュメント，および商用アイテムの技術データは，HP の標準商用ライセンス条件に基づいて米国政府にライセンスされています。

サードパーティ Web サイト

HP は，補足情報の検索に役立つ外部サードパーティ Web サイトへのリンクを提供します。サイトの内容と利用の可否は予告なしに変更される場合があります。HP は，サイトの内容または利用の可否について，いかなる表明も保証も行いません。

著作権

商標

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 またはその子会社の商標または登録商標です。

Java™ は，Sun Microsystems, Inc. の米国商標です。

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

Oracle® は，カリフォルニア州レッドウッド市の Oracle Corporation の米国登録商標です。

Unix® は，The Open Group の登録商標です。

文書の更新

本書のタイトル・ページには，次の識別情報が含まれています。

- ソフトウェアのバージョンを示すソフトウェア・バージョン番号
- 文書が更新されるたびに更新される文書発行日
- 本バージョンのソフトウェアをリリースした日付を示す，ソフトウェア・リリース日付

最新のアップデートまたは文書の最新版を使用していることを確認するには，
http://h20230.www2.hp.com/selfsolve/manuals を参照します。

サポート

HP Software のサポート Web サイトは，次の場所にあります。
http://support.openview.hp.com

HP Software のオンライン・サポートは，インタラクティブな技術サポート・ツールにアクセスするための効率的な手段を提供します。サポート・サイトを利用することで，次のようなことができるメリットがあります。

- 関心のある内容のナレッジ文書の検索
- サポート・ケースおよび機能強化要求の提出および追跡
- 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 サポートの連絡先の表示
- 利用可能なサービスに関する情報の確認
- ほかのソフトウェア顧客との議論の開始
- ソフトウェアのトレーニングに関する調査と登録

ほとんどのサポート・エリアは，HP Passport ユーザとしての登録およびサインインが必要です。また多くは，サポート契約も必要です。アクセス・レベルの詳細情報については，
http://h20230.www2.hp.com/new_access_levels.jsp を参照してください。

HP Passport ID の登録は，次の場所で行います。
http://h20229.www2.hp.com/passport-registration.html

目次

第 II 部：SITESCOPE をインストールする前に

第 III 部：SITESCOPE のインストール

第 IV 部：SITESCOPE の安全な稼働

目次

はじめに

HP SiteScope デプロイメント・ガイドへようこそ。本書では SiteScope について紹介し，開始方法，サーバのインストール，およびアップグレード・プロセスの詳細について説明します。

本章の内容

本書の構成

本書は，次の部で構成されています。

第 I 部　SiteScope の紹介

SiteScope について紹介し，スタートアップ・ロードマップを示します。また，デプロイメント計画，エージェントレス監視，および SiteScope ライセンスに関する情報も提供します。

第 II 部　SiteScope をインストールする前に

インストールの概要と，システム要件，推奨サーバ設定について説明します。既存の SiteScope のアップグレード方法についても説明します。

第 III 部　SiteScope のインストール

Windows，Linux，および Solaris の各プラットフォームでの SiteScope のインストールとアンインストールの方法について説明します。また，設定ツールを使用した SiteScope の設定方法，オペレーティング・システムと SiteScope のサイズ設定方法，および多くのインスタンスを監視する場合に最適なパフォーマンスを得る方法についても説明します。

第 IV 部　SiteScope の安全な稼働

SiteScope プラットフォームを強化するためのオプションの設定方法，モニタにアクセスするのに必要なユーザ権限と資格情報の設定方法，および Secure Sockets Layer（SSL）を使用するための SiteScope の設定方法について説明します。

第 V 部　作業の開始と SiteScope へのアクセス

SiteScope サービスの開始と停止方法と，初めて SiteScope にログインする方法について説明します。また，SiteScope のインストールの後に実行しなければならない推奨管理手順についても説明します。

第 VI 部　付録

IIS の設定方法，SiteScope と SiteSeer ホスティング型サービスのアカウントの統合方法，SiteScope と SiteMinder ポリシー・ベース認証との統合方法，およびモニタ設定コピー・ユーティリティを使用した現在の SiteScope バージョンのアップグレード方法について説明します。

対象読者

本書は，次の SiteScope 利用者を対象としています。

- SiteScope 管理者
- HP Business Availability Center 管理者

本書の読者は，エンタープライズ・システムの管理および HP Business Availability Center データ・コレクタに精通しているものとします。

HP SiteScope ドキュメント

HP SiteScope ドキュメントは，SiteScope のデプロイメント，管理，および使用に関する包括的な情報を提供します。

SiteScope には，次のドキュメントが付属しています。

リリース・ノート（新機能紹介を含む）：新機能，バージョンの制限事項，最新アップデートのリストが収められています。SiteScope では，［**ヘルプ**］＞［**新機能**］を選択します。リリース・ノートは，SiteScope ダウンロード・ページからも入手できます。

オンライン・ヘルプ：SiteScope ヘルプには，SiteScope で［**ヘルプ**］＞［**SiteScope ヘルプ**］を選択してアクセスできます。コンテキスト・センシティブ・ヘルプは，特定の SiteScope ページから［**ヘルプ**］＞［**このページのヘルプ**］を選択するか，特定のウィンドウで［**ヘルプ**］ボタンをクリックします。

SiteScope ヘルプには，以下のオンライン・リソースがあります。

- Documentation Updates：SiteScope ヘルプに対する更新の詳細の一覧を示します。
- Glossary：SiteScope で使用される主要な用語を定義します。
- Using SiteScope：SiteScope アプリケーションの管理方法と作業方法について説明します。

オンライン文書と印刷用マニュアル：すべての SiteScope マニュアルは，PDF または他の印刷形式で入手できます。PDF ファイルにアクセスするには，SiteScope で［**ヘルプ**］＞［**SiteScope ヘルプ**］を選択し，PDF タブを選択します。

次のオンライン文書は，PDF 形式でのみ入手できます。SiteScope ヘルプの［**Main Topics**］タブからアクセスすることもできます。

- 『**HP SiteScope デプロイメント・ガイド**』：SiteScope について紹介し，開始方法，サーバのインストール，およびアップグレード手順，および統合を使った作業の詳細について説明します。
- 『**HP SiteScope Failover Guide**』（英語版）：インフラストラクチャ監視にフェールオーバ機能を実装できる SiteScope の特別なバージョンである SiteScope Failover のインストール方法と作業方法について説明します。

SiteScope モニタ・メトリックスおよび測定値に関するマニュアルは，Word 形式で SiteScope ヘルプの［**Main Topics**］タブから入手できます。このマニュアルはすべての SiteScope モニタと関連カウンタまたはメトリックスに関する情報を集めたものです。このマニュアルには，モニタごとに設定可能なすべてのメトリックスと，サポートされるアプリケーションやオペレーティング・システムのバージョンが一覧表示されています。このマニュアルの最新版は，HP ソフトウェア・サポート担当者にお問い合わせください。

オンライン文書の閲覧と印刷には，Adobe Reader 4.0 以降を使用します。Adobe Reader は，Adobe Web サイト（www.adobe.com/jp/）からダウンロードできます。

その他のオンライン・リソース

［**トラブルシューティング&ナレッジ ベース**］から，セルフソルブ・ナレッジ・ベースを検索できる HP ソフトウェア・サポート Web サイトのトラブルシューティング・ページにアクセスできます。［**ヘルプ**］＞［**トラブルシューティング&ナレッジ ベース**］を選択します。この Web サイトの URL は，http://support.openview.hp.com/troubleshooting.jsp です。

HP ソフトウェア サポート：HP ソフトウェア・サポート Web サイトにアクセスします。このサイトで，セルフソルブ・ナレッジ・ベースを参照できます。また，ユーザ・ディスカッション・フォーラムへの投稿や検索，サポート依頼の送信，パッチや更新された文書のダウンロードなども行えます。［**ヘルプ**］＞［**HP Software サポート**］を選択します。この Web サイトの URL は，http://support.openview.hp.com です。

ほとんどのサポート・エリアは，HP Passport ユーザとしての登録およびサインインが必要です。また多くは，サポート契約も必要です。

アクセス・レベルの詳細情報については，
http://h20230.www2.hp.com/new_access_levels.jsp を参照してください。

HP Passport ユーザ ID の登録は，次の場所で行います。
http://h20229.www2.hp.com/passport-registration.html

HP ソフトウェア Web サイト：HP ソフトウェア Web サイトにアクセスします。このサイトでは，HP ソフトウェアの製品に関する最新情報を提供します。新しいソフトウェアのリリース，セミナー，展示会，HP ソフトウェア・サポートなどの情報も含まれています。［**ヘルプ**］＞［**HP ソフトウェア Web サイト**］を選択します。この Web サイトの URL は，http://www.hp.com/jp/software です。

表記規則

本書では次の表記規則に従います。

UI 要素と**関数名**	アクションの実行対象となるインタフェース要素の名前，ファイルの名前またはパス，強調を必要とするその他の項目を示します（例：［**保存**］ボタンをクリックします）。メソッド名や関数名もこのスタイルで示します（例：**wait_window** ステートメントには次のパラメータがあります）。
引数	メソッド，プロパティ，関数の引数，書名を示します（例：詳細については，『**HP ユーザーズ・ガイド**』を参照してください）。
< **置き換える値** >	ファイル・パスまたは URL アドレスの中で，実際の値に置き換える必要がある部分は山括弧で囲んで示します（例：＜ **MyProduct のインストール・フォルダ**＞ **¥bin**）。
例	使用例やユーザがそのまま入力しなければならない文字列に使用します（例：エディット・ボックスに「Hello」と入力します）。
CTRL+C	キーボードのキーを示します（例：ENTER キーを押します）。
[ ]	省略可能な引数は，半角の大括弧で囲んで示します。
{ }	引数に割り当てる値の候補は，中括弧で囲んで示します。値をいずれか 1 つ割り当てる必要があります。
...	構文内の省略記号は，同じ形式で項目をさらに組み入れることができることを意味します。プログラミング例に含まれる場合は，何行かが意図的に省略されていることを示します。
|	垂直バー（パイプ記号）は，バーで区切られているオプションのいずれかを指定しなければならないことを示します。

第 I 部

SiteScope の紹介

第 1 章

SiteScope の紹介

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認を目的とする，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。また，SiteScope は，Business Availability Center，HP Software-as-a-Service，HP LoadRunner など，ほかの HP 製品の監視の基盤としても機能します。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 にはまた，標準化された監視組織の開発および監視デプロイメントの迅速化のためのツールと，さまざまなメディアでイベント情報の通信と記録に使用できる警告タイプを提供するテンプレート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，SiteScope が実行されるサーバの数ではなく，監視される測定値の数に基づいてライセンスされます。測定値とは，システム・リソースの値，パフォーマンス・パラメータ，URL，または同様のシステム応答のことです。つまり，SiteScope のデプロイメントは，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柔軟に規模を変更できます。SiteScope は，HP から提供される永続ライセンス，または新しい SiteScope に含まれる評価ライセンスのどちらかを使用してインストールできます。必要に応じてライセンスをアップグレードして，初期デプロイメントの監視機能を拡張したり，インフラストラクチャ内でデプロイメントを拡張したりできます。

SiteScope は，業界初のエージェントレス監視ソリューションとして開発されました。それ以来，SiteScope のユーザは，業界で定評のあるエージェントレス監視アーキテクチャを活用してきました。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 TCO（Total Cost of Ownership）が削減されます。

- 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 を配備し，Business Availability Center や Service Level Management などのその他の HP のソリューションを追加することで，確実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・レベルを管理することができます。

第 2 章

スタートアップ・ロードマップ

本章では，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提供します。

1 お使いの SiteScope を登録します。

お使いの SiteScope を登録すると，HP の全製品に関するテクニカル・サポートおよび情報へ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 ソフトェア・サポート Web サイト（http://support.openview.hp.com/）で SiteScope の登録を行うことができます。

2 ヘルプの入手先について参照します。

HP サービス，HP ソフトェア・サポート，および SiteScope ヘルプをはじめとする，さまざまなサポートについての情報を得ます。詳細については，11 ページ「HP SiteScope ドキュメント」を参照してください。

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。21 ページ「デプロイメントの方法と計画」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 をインストールします。

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，53 ページ「インストールの概要」を参照してください。SiteScope に安全にアクセスする方法の詳細については，141 ページ「SiteScope プラットフォームのセキュリティ強化」を参照してください。

5 SiteScope にログインし，システム管理を開始します。

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，175 ページ「インストール後の管理」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 のヘルプを参照してください。

第 3 章

デプロイメントの方法と計画

SiteScope をデプロイすることは，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：以下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。

本章の内容

エンタープライズ・システム監視の方法

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以下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 には監視を行うツールが実装されています。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。警告アクションとして電子メール通知が一般的に使用されます。SiteScope には，ほかのシステムと統合が可能なその他の警告タイプも用意されています。

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 SiteScope モニタの依存オプションを使用します。

➤ **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べき制約を理解します。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 が稼動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 上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
- レポーティングのため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，118 ページ「Windows プラットフォーム上の SiteScope のサイズ設定」または 123 ページ「Solaris および Linux プラットフォーム上での SiteScope のサイズ設定」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。

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 のライセンスはサーバ・ベースではありません。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 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べき事項

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。

Microsoft Windows ネットワーク環境で SiteScope を使用する場合にさらに考慮すべき事項を次に示します。

- **リモート・レジストリ・サービス**：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。
- **Windows 2000 Service Pack 2**：Windows 2000 Service Pack 2 には既知の問題があります。リモート・レジストリ・サービスではメモリ・リークが発生します。この問題により，Service Pack 2 を使用しているリモート Windows 2000 サーバの SiteScope モニタは，動きを止めることがしばしばあります。メモリ・リークの問題は，Windows 2000 Service Pack 3 で修正されました。この問題を避けるには，SiteScope で監視する予定のすべての Windows 2000 サーバに Service Pack 3 をインストールすることをお勧めします。

UNIX 環境の場合に考慮すべき事項

SiteScope Web サーバが特権ポート上で実行されない限り，SiteScope のインストールや実行を root ユーザが行う必要はありません。

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。

第 4 章

エージェントレス監視について

本章では，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，パフォーマンスや運用を監視するほかのソリューションに比べてかなり簡単です。

本章の内容

SiteScope 監視機能について

SiteScope は，システムやサービスをさまざまなレベルで監視するため，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。

本章は，次の項目で構成されています。

➤ 30 ページ「SiteScope の監視の方法」

➤ 33 ページ「ファイアウォールと SiteScope のデプロイメント」

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。

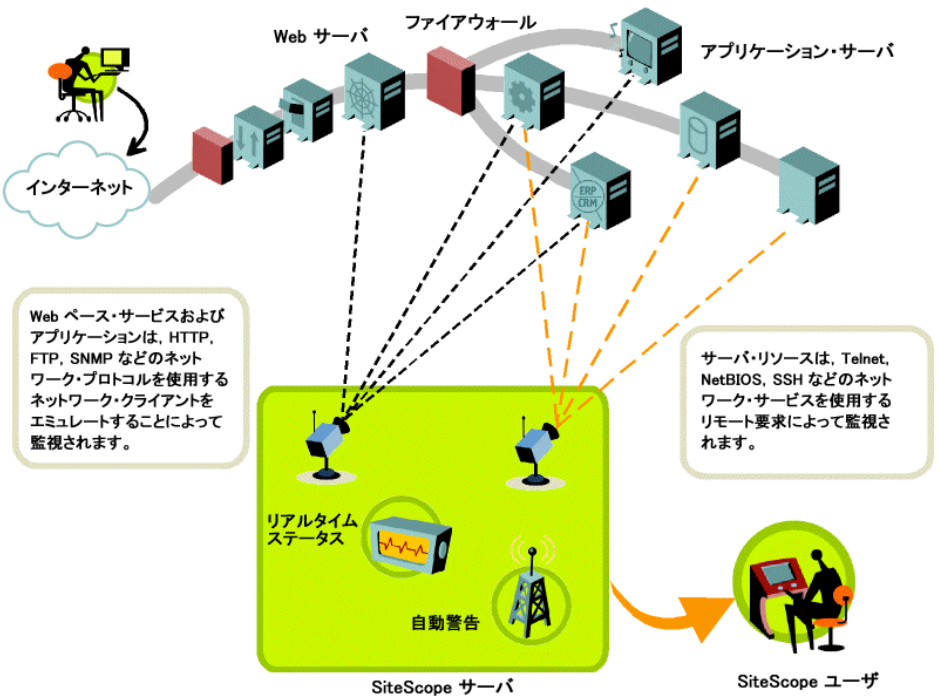
➤ **標準ベースのネットワーク・プロトコル**

このカテゴリには，HTTP，HTTPS，FTP，SMTP，SNMP，および UDP 経由の監視が含まれます。これらの種類のモニタは，一般に SiteScope が実行されているプラットフォームまたはオペレーティング・システムに依存しません。たとえば，Linux にインストールされた SiteScope は，Windows 2000，HP-UX，Solaris UNIX 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。たとえば，Windows パフォーマンス・カウンタは，Windows 用の SiteScope には含まれていますが，Solaris 用の SiteScope には含まれていません。

次の図に，SiteScope を使用したエージェントレス監視の概要を示します。SiteScope モニタはリモート・マシン上でサービスの要求を行い，パフォーマンスおよび可用性に関するデータを収集します。



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 NT/2000/2003（x86 および Alpha については，次の注を参照）
- Sun Solaris（Sparc および x86）
- Linux
- AIX
- HP/UX
- Digital Unix
- SGI IRIX
- SCO
- FreeBSD

注：UNIX で実行されている SiteScope から Windows マシン上のサーバ・リソース（たとえば，CPU 利用率，メモリ）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，セキュア・シェル・クライアントをインストールする必要があります。詳細については，SiteScope ヘルプの「SiteScope Monitoring Using Secure Shell (SSH)」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あり，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 Operating System Adapters」を参照してください。

SiteScope がリモートでシステム・データにアクセスする各サーバのログイン・アカウントを有効にする必要があります。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 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** ユーザに対して設定されたユーザ・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 の機能	使用される標準ポート
SiteScope Web サーバ	ポート 8080
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
電子メールによる警告	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

第 5 章

SiteScope のライセンス

SiteScope のライセンスは，実行可能なモニタの数と，（場合によっては）使用可能なモニタのタイプを制御します。サイト，シート，またはユーザの数に基づいて販売されるソフトウェアとは異なり，SiteScope のライセンスは監視の要件に基づいています。このため，SiteScope の規模を環境に合わせて効率良く柔軟に調整できます。

本章の内容

SiteScope のライセンスの概要

SiteScope ライセンスの購入と登録を行うことによって，重要な権利および権限を得ることができます。登録ユーザは，HP のすべての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，無料のアップデートやアップグレードを受ける資格を得ます。また，HP ソフトウェア・サポート Web 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，HP Software セルフ・ソルブ技術情報での技術情報の検索や，SiteScope マニュアルのアップデートのダウンロードを行うことができます。

SiteScope ライセンスの種類について

SiteScope を使用するには，有効なライセンスが必要です。評価ライセンスは，SiteScope を新規にインストールまたはダウンロードするたびに取得できます。SiteScope をインストールするには，永続ライセンスまたは評価ライセンスを使用します。

注：SiteScope 7.x から SiteScope 8.x または 9.x バージョンにアップグレードする場合には，新しい一般ライセンス番号が必要です。

SiteScope ライセンスのアップグレードが必要な場合は，HP の営業担当にお問い合わせください。

SiteScope のライセンスには，次の 2 つのカテゴリがあります。

- **一般**：SiteScope アプリケーションを有効にするために必要なライセンスの種類
- **オプション**：オプションの監視機能を有効にするためのライセンス

これら 2 つのカテゴリに，合わせて 4 つのライセンスの種類があります。次の表に，SiteScope のライセンスの種類について説明します。

一般ライセンスの種類

次の表は，一般ライセンスの種類を示します。

ライセンスの種類	説明
評価ライセンス	ダウンロードした SiteScope に付属する標準のライセンスで，評価期間中に製品の標準的な使用が可能になります。
拡張ライセンス	HP が発行する一時的なライセンスで，評価期間を一定の期間延長します。

ライセンスの種類	説明
永続ライセンス	標準のライセンスで，ライセンスの一部として含まれているモニタ・ポイントの数に基づいて，製品の継続的な使用が可能になります。
フェイルオーバ・ライセンス	HP が発行する特別なライセンスで，SiteScope インスタンスを別の SiteScope のフェイルオーバとして機能させることができます。

オプション・ライセンスの種類

次の表は，オプション・ライセンスの種類を示します。

ライセンスの種類	説明
エンタープライズ・アプリケーション・オプション・ライセンス	HP が発行する特別なライセンスで，オプションの SiteScope モニタが使用可能になります。
ソリューション・テンプレート・オプション・ライセンス	HP が発行する特別なライセンスで，ソリューション・テンプレートが利用可能になります。通常，ソリューション・テンプレートごとにライセンスが異なります。
Enterprise Management Systems（EMS）オプション・ライセンス	HP が発行する特別なライセンスで，Enterprise Management Systems 統合モニタ群が使用可能になります。
Web スクリプト・モニタ・オプション・ライセンス	HP が発行する特別なライセンスで，Web スクリプト・モニタによる監視が利用可能になります。

注：拡張ライセンスは，評価ライセンスとオプション・ライセンスのどちらかに発行されます。

インストールされた個々の SiteScope には，固有のモニタ・ライセンスが必要です。現在の SiteScope には，1 つのライセンスを複数の SiteScope で共有するためのライセンス・サーバ機能はありません。

次の表に，評価および永続ライセンスとオプション・ライセンスの違いの概要を示します。

トピック	永続および評価ライセンス	オプション・ライセンス
概要	SiteScope 製品の標準機能を使用可能にします。	個々のライセンスは，オプションの特定のモニタ・タイプを使用可能にします。
ライセンス・キーあたりのインストール数	インストールされた個々の SiteScope には，個別の永続または評価ライセンス・キーが必要です。	インストールされた個々の SiteScope に個別のオプション・ライセンスを適用して，SiteScope サーバのオプション機能を使用可能にする必要があります。
モニタ・ポイント	ライセンス・キーには，事前に設定された「モニタ・ポイント」の数が含まれています。モニタ・ポイントによって，作成できるモニタ・インスタンスの数と，個々の SiteScope サーバで測定できる測定値の数が決まります。	オプション・ライセンス・キーは，SiteScope が使用するオプションのモニタ・タイプを使用可能にします。永続ライセンス・キーによって管理されているモニタ・ポイントの総数が，オプション・ライセンス・キーによって増えることはありません。
その他		オプションのモニタ・タイプを作成するために使用されるモニタ・ポイントは，永続ライセンス・キーに含まれるモニタ・ポイントの総数から差し引かれます。
ライセンス・キーの入力	永続ライセンス・キーは，SiteScope のインストール後に初めて実行したときの初期起動画面で入力するか，評価期間内であれば［General Preferences（一般のプリファレンス)］ページを使用していつでも入力できます。	オプション・ライセンス・キーは，SiteScope のインストール後に初めて実行したときの初期起動画面の入力フィールドを使用して入力するか，［General Preferences（一般のプリファレンス)］ページを使用して入力します。

試用期間中に SiteScope を使用する場合は，ライセンス・キーの入力は必須ではありません。

モニタ・ライセンスの概要

SiteScope のライセンスは，柔軟なスケーリングとデプロイメントを可能にするポイント・システムに基づいています。SiteScope の永続ライセンスは，モニタ・タイプの組み合わせをアクティブにするために使用されるポイントをいくつか提供します。

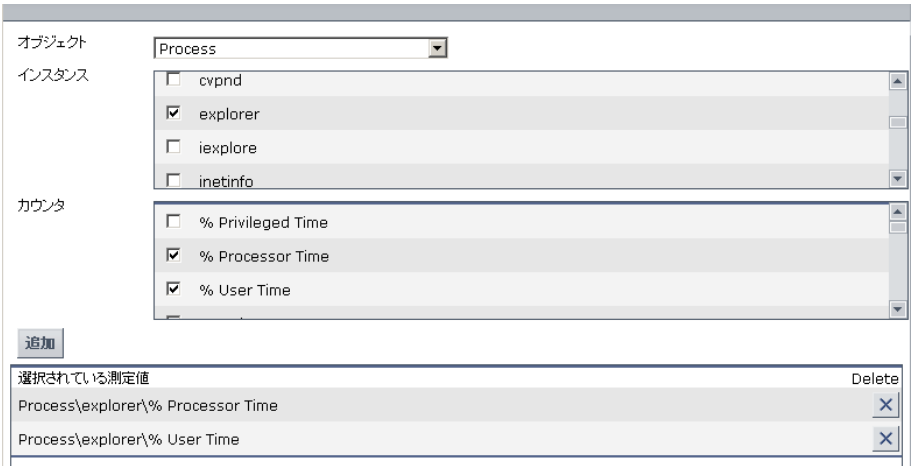
注：SiteScope には，ユーザ・ベースのアクセス権のライセンスはありません。SiteScope アプリケーション・サーバにアクセスできるユーザの数には制限がありません。

作成できる SiteScope モニタの数は，次の 2 つの要因によって決まります。

- 購入したモニタ・ポイントの総数
- 使用する SiteScope モニタのタイプ

モニタ・タイプは，アクティブにする必要があるポイントの数によって 3 つのカテゴリに分かれます。たとえば，Web ページに 1 つの URL モニタを設定する場合は，モニタ・インスタンスごとに 1 つのモニタ・ポイントが必要です。Apache Server モニタを設定する場合は，監視するサーバ・パフォーマンス測定値ごとに 1 つのモニタ・ポイントが必要です。

Microsoft Windows リソース・モニタまたは UNIX リソース・モニタを設定する場合は，モニタ・インスタンスごとに 1 つのモニタ・ポイントが必要です。これらのモニタを設定するには，最初にオブジェクト，次にそのオブジェクトに関連するインスタンス，そして各インスタンスに関連するカウンタを選択します。次の Microsoft Windows リソース・モニタの例では，選択されたオブジェクトが Process，選択されたインスタンスが explorer，そして選択されたカウンタが % Processor Time と % User Time です。この場合は，explorer インスタンスに 1 ポイント必要となります。監視する別のインスタンスを選択すると，2 ポイント必要というようになります。



次の節は，さまざまな SiteScope モニタ・タイプのインスタンスごとに使用されるポイントの一覧です。

- 41 ページ「システム・モニタ」
- 42 ページ「アプリケーション・モニタ」
- 43 ページ「Web/URL モニタ」
- 43 ページ「Web スクリプト・モニタ」
- 44 ページ「ネットワーク・サービス・モニタ」
- 44 ページ「コンテナ・モニタ・タイプ」
- 45 ページ「エンタープライズ・アプリケーション・モニタ」
- 45 ページ「ソリューション・テンプレート」

システム・モニタ

システム・モニタは，インフラストラクチャ・リソースの可用性を確認するために使用します。次のモニタ・タイプでは，モニタ・インスタンスあたり 1 ポイントでライセンスが供与されます。

- コンポジット
- CPU 使用率
- データベース
- DHCP
- ディレクトリ
- ディスク領域
- ファイル
- LDAP
- ログ・ファイル
- メモリ
- Microsoft Windows ダイアルアップ
- Microsoft Windows イベント・ログ
- Microsoft Windows リソース
- ニュース
- ネットワーク
- Radius
- スクリプト
- サービス
- UNIX リソース

アプリケーション・モニタ

アプリケーション・モニタは，特定のインフラストラクチャ・アプリケーションの可用性とパフォーマンスのパラメータを確認するために使用します。これらのモニタ・タイプでは，モニタ・インスタンスあたり最大で 10 のパフォーマンス測定値を監視することが可能であり，測定値または測定項目あたり 1 ポイントでライセンスが供与されます。

- Apache Web サーバ
- ATG Dynamo アプリケーション・サーバ
- BEA Tuxedo
- BEA WebLogic アプリケーション・サーバ
- BroadVision アプリケーション・サーバ
- CheckPoint Firewall-1
- Cisco Works
- Citrix MetaFrame
- IBM DB2
- IBM WebSphere アプリケーション・サーバ
- F5 Big-IP
- MacroMedia ColdFusion サーバ
- MAPI
- NetScape Enterprise/iPlanet サーバ
- Microsoft Windows パフォーマンス・カウンタ（Microsoft Windows プラットフォーム）
- Novell SilverStream
- Oracle9i アプリケーション・サーバ
- Oracle JDBC
- Real One/Real Media Player と Server
- SunONE サーバ
- Sybase データベース

Web/URL モニタ

URL モニタ・タイプは，Web ページの可用性とコンテンツをチェックするために使用します。次のモニタ・タイプでは，複数ステップによるトランザクションの場合，インスタンスまたはステップあたり 1 ポイントでライセンスが供与されます。

- e ビジネス・トランザクション
- リンク・チェック
- URL
- URL コンテンツ
- URL のリスト（URL あたり 1 ポイント）
- URL シーケンス（ステップあたり 1 ポイント）
- Web サーバ
- Web サービス

Web スクリプト・モニタ

Web スクリプト・モニタを使用して，仮想エンド・ユーザとターゲット Web サイトの間のトランザクションを監視します。次のモニタ・タイプでは，モニタによって実行されるトランザクションあたり 4 ポイントでライセンスが供与されます。トランザクションには，URL を必要な数だけ含めることができます。モニタには，トランザクションごとに 12 までの測定値を含めることができます。

- Web スクリプト・モニタ

ネットワーク・サービス・モニタ

ネットワーク・サービス・モニタは，インフラストラクチャに存在する可能性がある各種サービスの可用性を確認するために使用します。これらのモニタ・タイプでは，モニタ・インスタンスあたり 1 ポイントでライセンスが供与されます。

- DNS
- フォーミュラ（帯域幅）コンポジット
- FTP
- メール
- ネットワーク帯域幅（インタフェースあたり 1 ポイント）
- Ping
- ポート
- RTSP（Real Time Streaming Protocol）
- SNMP
- MIB による SNMP
- SNMP トラップ

コンテナ・モニタ・タイプ

コンポジット・モニタと e ビジネス・トランザクション・モニタによって提供されるシーケンス・チェック機能と複合監視機能は，引き続き使用可能です。これらのモニタ・タイプは，メンバ・モニタをグループ化して適切なモニタ・ポイントの比率でカウントするために使用されます。これらのモニタは，その中に含まれるメンバ・モニタのモニタ・ポイントを加算せずに設定できます。

エンタープライズ・アプリケーション・モニタ

これらのオプションのモニタでは，アプリケーションの種類ごとにライセンスが供与されます。次のアプリケーションのどれを監視可能にするかに基づいて，オプション・ライセンスを購入します。

- COM+
- SAP CCMS
- Siebel
- WebSphere MQ Status

ソリューション・テンプレート

ソリューション・テンプレートは，オプションと標準の両方のモニタ・タイプに含まれる，最適化されたモニタ・テンプレートです。テンプレートとテンプレート固有のモニタ・タイプにアクセスするには，オプション・ライセンスが必要です。オプション・ライセンスを購入すると，特定のソリューション向けの『Best Practices』（英語版）のマニュアルも入手できます。SiteScope には，次のソリューション・テンプレートが用意されています。

- Active Directory
- JBoss アプリケーション・サーバ
- Microsoft Exchange（Microsoft Exchange 5.5，2000，2003，および 2007 をサポート）
- Microsoft IIS 6
- Microsoft SQL サーバ
- .NET（.NET CLR Data，ASP.NET，および ASP.NET アプリケーションをサポート）
- Oracle データベース
- Operating System Host（Microsoft Windows，AIX，Linux，および Solaris をサポート）
- SAP（SAP R/3 および SAP J2EE をサポート）
- Siebel
- WebLogic
- WebSphere

ライセンス・ポイント数の見積もり

購入するライセンス・ポイントの数は，予定している SiteScope のデプロイの方法と，監視するシステムやサービスのレベルによって異なります。次に，必要なライセンス・ポイント数の見積もりに関するガイドラインを示します。

サーバの状態の監視

サーバの状態の監視に必要なポイント数は，主に監視するサーバ・マシンの数によって決まります。監視対象の各サーバで，次の各項目について 1 つのポイントが必要です。

- CPU の監視
- 個々のハード・ディスクまたは主要なディスク・パーティション
- メモリ
- 個々の主要なサーバ・プロセスまたはサービス
- 個々の主要なファイル，ログ，またはディレクトリ

Web プロセスとコンテンツの監視

Web プロセスとコンテンツの監視に必要なポイント数は，監視する Web ベースのプロセスとページの数によって決まります。Web ベースのプロセスには，Web ページのシーケンスが含まれます。たとえば，セキュア・サーバにログインして勘定残高を確認し，ログアウトするとします。多くの場合，URL のシーケンスには異なる宛先ページを持つ同じパスが含まれます。オンライン・サービスの場合は，バックエンド・データベースをチェックして，Web インタフェース経由で修正したデータが正しく更新されているかどうか確認することも必要です。また，ファイルのダウンロードや，自動化された電子メール・メッセージの送受信が含まれるプロセスも考えられます。

- 個々の Web ベースの URL シーケンスを監視する場合は，監視する Web ベースのプロセスごとに 1 つのシーケンス・モニタ・インスタンスと，そのシーケンス内の URL またはステップごとに 1 つのポイントが必要です。
- ほかのインターネット・ページまたはプロセスを監視する場合は，監視するファイルのダウンロード，電子メールによる確認，または個々の Web ページ・コンテンツごとに 1 つのポイントが必要です。

アプリケーション・パフォーマンスの監視

アプリケーション・パフォーマンスの監視は，ネットワーク・ベースのサービスの可用性を確保し，パフォーマンスの問題を検出するための重要な手段です。また，アプリケーションやシステムの多くは複雑であるため，必要なモニタ・ポイント数を見積もるのは非常に困難です。SiteScope の柔軟なライセンス・モデルでは，監視機能をニーズに合わせて簡単に変更できます。

- アプリケーション・パフォーマンスの監視に必要なポイント数は，次の要因によって決まります。
- デプロイされるアプリケーションの数
- アプリケーションの種類
- 監視するパフォーマンス測定値の数

一部のアプリケーション（一部の Web サーバなど）のパフォーマンス測定値は，1 つのモニタ・インスタンスと，10 測定値ポイント未満の測定値数によって使用可能となる場合があります。たとえば，Apache Web サーバは，1 つの URL について，アクセス総数，サーバ使用可能時間，および 1 秒あたりの要求数を含むパフォーマンス測定値を提供します。ほかのアプリケーションやシステムでは，複数のサーバ・アドレス，モジュール，および複数のモニタ・インスタンスを必要とする測定値が含まれる場合があります。アプリケーションによっては，監視するデータベース・アプリケーションと統合されている場合もあります。

次に，データのアクセス方法に応じて，アプリケーションの監視に必要なポイントを見積もるためのガイドラインを示します。

- アプリケーションごとに 1 つのアプリケーション・モニタ・インスタンスと，監視するパフォーマンス測定値ごとに 1 つのポイント
- アプリケーション・ステータス URL ごとに 1 つのモニタ・インスタンスと，監視するパフォーマンス測定値ごとに 1 つのポイント

ネットワークの監視

ネットワークの監視には，ユーザがネットワークにアクセスして使用するために必要な，ネットワーク・サービスの接続と可用性の両方の確認が含まれます。これには，DNS，DHCP，LDAP，および RADIUS などのサービスの監視が含まれます。ネットワークのハードウェアや設定によっては，SiteScope の SNMP モニタ・タイプを使用して SNMP 経由でネットワーク・インフラストラクチャにクエリすることで，ネットワークのパフォーマンス統計情報にアクセスできる場合もあります。

次に，ネットワークの監視に必要なポイント数の見積もりに関するガイドラインを示します。

- 主要なネットワークの接続先ごとに 1 つのポイント
- 主要なネットワーク・サービス（DNS や LDAP など）ごとに 1 つのポイント
- SNMP 経由で監視する測定値ごとに 1 つのポイント

モニタ・ポイントの購入

SiteScope のモニタ・ポイントは，モニタを柔軟にデプロイできるように，50，100，500，および 2,000 ポイントのブロック単位で販売されています。たとえば，100 ポイントのブロックを購入すれば，次のようにさまざまな監視オプションを設定できます。

- それぞれ 5 つのパフォーマンス測定値を監視する 10 のアプリケーション・モニタ（5 x 10 = 50 ポイント）
- それぞれ 10 のトランザクション・ステップを横断する 2 つのシーケンス・モニタの組み合わせ（10 x 2 = 20 ポイント）
- 1 ポイントのネットワーク・サービス・モニタまたはサーバ・モニタを 30（1 x 30 = 30 ポイント）

同じ 100 ポイントのブロックを使用して，次のように設定することもできます。

- それぞれ 1 つの測定値を監視する 10 のアプリケーション・モニタ（1 x 10 = 10 ポイント）
- 5 つのステップを持つ シーケンス・モニタ（5 ポイント）
- 85 のネットワーク・サービス・モニタまたはサーバ・モニタ（85 ポイント）

SiteScope のインストールには，無料の評価ライセンスが含まれています。評価期間以後も SiteScope を使用するには，お使いの SiteScope 用の永続ライセンス・キーを要求してアクティブにする必要があります。モニタ・ポイントの購入の詳細については，HP の営業担当にお問い合わせください。

SiteScope ライセンス情報の変更

SiteScope をインストールした後は，いつでもライセンスを変更または追加できます。電話または電子メールで HP SiteScope の営業スタッフにライセンスを要求することができます。営業担当者への連絡方法の詳細については，HP の Web サイト（http://www.hp.com/jp/software）を参照してください。

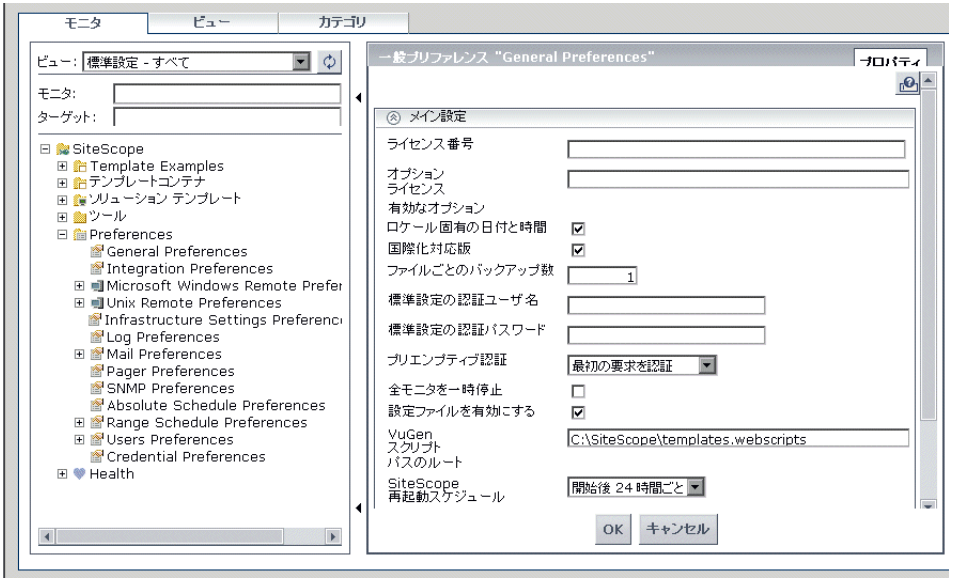
HP からライセンス・キーを受け取ったら，ブラウザ・インタフェース経由で SiteScope にライセンス・キーを入力します。

SiteScope でライセンス情報を入力または変更するには，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動している必要があります。

2 左側のモニタ・ツリーで，［**Preferences**］を展開し，［**General Preferences**］をクリックします。画面の右側の内容領域に，［一般のプリファレンス（General Preferences）］プロパティが表示されます。

3 ページ下部にある，［**編集**］ボタンをクリックします。［一般のプリファレンスの編集（General Preferences)］ページが表示されます。



4 ［**ライセンス番号**］ボックスで，ライセンス・キーの番号を入力または変更します。オプション・ライセンスを受け取った場合は，ライセンス情報を［**オプション ライセンス**］ボックスに入力します。ボックスに複数のオプション・ライセンスを入力するには，オプション・ライセンスをカンマ（,）で区切ります。

5 ［**OK**］ボタンをクリックし，変更を保存します。更新された情報で［一般のプリファレンス（General Preferences)］プロパティが表示されます。［**有効なオプション**］の右側に有効なオプション・ライセンスが表示されます。

第 II 部

SiteScope をインストールする前に

第 6 章

SiteScope をインストールする前に

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べき計画の手順とアクションがいくつかあります。

本章の内容

インストールの概要

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。**

2 **SiteScope のインストール実行ファイルを入手します。**

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 9.50 をインストールするためには，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 9.50 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，65 ページ「Windows 用の SiteScope のインストール」および 91 ページ「Solaris または Linux への SiteScope のインストール」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，179 ページ「SiteScope を使った作業の開始」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，175 ページ「インストール後の管理」を参照してください。

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 は，サポートされている 64- ビット環境の Windows および UNIX オペレーティング・システムに 32- ビットのアプリケーションとしてインストールできます。

本章は，次の項目で構成されています。

Windows の場合のシステム要件

Windows プラットフォームに SiteScope をインストールする場合は，次のシステム要件を使用します。

コンピュータおよびプロセッサ	Pentium III 800 MHZ 以上
オペレーティング・システム	➤ Microsoft Windows 2000 Server/Advanced Server SP4 ➤ Microsoft Windows 2003 Standard/Enterprise SP1， SP2 ➤ Microsoft Windows Server 2003 R2 SP1
メモリ	512 MB 以上（2 GB 以上を推奨）
ハード・ディスクの空き容量	2 GB 以上（10 GB 以上を推奨）
Web ブラウザ	Microsoft Internet Explorer 6.0 SP1 以降 ; Firefox 1.0 以降

Solaris の場合のシステム要件

Solaris プラットフォームに SiteScope をインストールする場合は，次のシステム要件を使用します。

コンピュータおよびプロセッサ	Sun 400 MHz UltraSparc II プロセッサ以上
オペレーティング・システム	Sun Solaris 9 または 10（最新のパッチ・クラスタを使用）
メモリ	512 MB 以上（2 GB 以上を推奨）
ハード・ディスクの空き容量	2 GB 以上（10 GB 以上を推奨）
Web ブラウザ	Firefox 1.0 以降

注：Solaris プラットフォームで SiteScope 管理レポートを表示するには，SiteScope サーバ上で X Window システムが稼働している必要があります。

RedHat Linux の場合のシステム要件

RedHat Linux プラットフォームに SiteScope をインストールする場合は，次のシステム要件を使用します。

コンピュータおよびプロセッサ	Pentium III 800 MHZ 以上
オペレーティング・システム	RedHat ES/AS Linux 3，4 **注**：NPTL（Native POSIX Threading Library）搭載の RedHat Linux 9 は，SiteScope の現在のバージョン以降はサポートされません。
メモリ	512 MB 以上（2 GB 以上を推奨）
ハード・ディスクの空き容量	2 GB 以上（10 GB 以上を推奨）
Web ブラウザ	Firefox 1.0 以降

VMware のシステム要件

SiteScope では，下記のテスト済みの設定に従って，次の VMware 環境がサポートされています。

サポート対象環境とテスト済み環境	➤ VMware ESX 3.0 ➤ VMware VirtualCenter 3.0
サポート対象環境のみ	➤ VMware VirtualCenter 2.x ➤ VMware ESX 3.x ➤ VMware ESX 2.5 via VirtualCenter 2.x ➤ VMware ESX 3.x via VirtualCenter 3.x

テスト済みの VMWare 設定	➤ 1 つの物理サーバ上の 2 VMWare 仮想マシン（VM） ➤ 各 VM に 2 つの CPU，2Ghz，2 GB のメモリ，および 10 GB のディスク空き領域 ➤ 同じ物理サーバにほかの VM は存在していない ➤ VMTools をインストール済み
テスト済みの SiteScope 設定	➤ 各 VM に 1 つの SiteScope（この VM にほかのアプリケーションが存在していない） ➤ 各 VM に同じバージョンの SiteScope ➤ 1 分間に各 VM で 650 モニタを実行，合計 6500 モニタ

VMware 環境に SiteScope をインストールする場合は，この最低システム要件を使用します。

コンピュータおよびプロセッサ	4 Intel Xeon 物理プロセッサ（各 2 GHz）
オペレーティング・システム	Microsoft Windows 2003 Standard/Enterprise SP1
メモリ（RAM）	4 GB
ハード・ディスクの空き容量	20 GB（ハード・ディスク速度 7200 rpm）
ネットワーク・カード	1 物理ギガビット・ネットワーク・インタフェース・カード
その他のソフトウェア	VMTools がインストールされている必要があります。

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，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 Availability Center 統合，およびデータベースのログ記録。提示されている最高値はすべての環境に当てはまるものではありません。

---

64 ビット環境の監視のサポート

SiteScope は，次の 64 ビット環境での監視をサポートします。

オペレーティング・システム	➤ Windows 2003 Server 64 ビット ➤ Windows 2008 Server 64 ビット ➤ Solaris 64 ビット ➤ HP-UX 64 ビット ➤ Linux 64 ビット
サポートされている SiteScope モニタ	➤ CPU モニタ ➤ ディスク容量モニタ ➤ メモリ・モニタ ➤ Microsoft Windows リソース・モニタ ➤ Microsoft Windows イベント・ログ・モニタ ➤ サービス・モニタ ➤ UNIX リソース・モニタ

推奨サーバ構成

次の表に，SiteScope をデプロイするための推奨サーバ構成を示します。これらは，設定されたモニタ・インスタンスの数と SiteScope サーバ上で 1 分間に稼働するモニタの数に基づく，一般的な推奨事項です。

レベル	サーバの詳細	Intel プラットフォーム	Solaris プラットフォーム
1	モニタ数が 1,000 未満で，1 分間に稼働するモニタ数が 300 未満の SiteScope サーバ	シングル・プロセッサ（Pentium III 1.0 GHz 以上）*，512 MB のシステム・メモリ，1 つのネットワーク・コントローラ，2 GB のディスク領域	シングル・プロセッサ（Ultra 10，Netra T1 など），512 MB のシステム・メモリ，1 つのネットワーク・コントローラ，2 GB のディスク領域
2	稼働するモニタ数が 1,000 ～ 2,000 で，1 分間に稼働するモニタ数が 500 未満の SiteScope サーバ	デュアル・プロセッサ（Pentium III 1.0 GHz 以上または Pentium III Xeon 700 MHz 以上）*，1,024 MB のシステム・メモリ，2 つの Fast Ethernet ネットワーク・コントローラ，4 GB のディスク領域	デュアル・プロセッサ（Ultra 2/E220/E250 400 MHz 以上），784 MB のシステム・メモリ，2 つの Fast Ethernet ネットワーク・コントローラ，4 GB のディスク領域
3	モニタ数が 2,001 ～ 3,999 で，1 分間に稼働するモニタ数が 500 超の SiteScope サーバ	クアッド・プロセッサ（Pentium III Xeon 700 MHz 以上）*，1,024 ～ 1,536 MB のシステム・メモリ，少なくとも 2 つの Fast Ethernet ネットワーク・コントローラ，8 GB のディスク領域	デュアル・プロセッサ（E280R）またはクアッド・プロセッサ（Ultra2/E220/E250），1,024 MB のシステム・メモリ，2 つの Fast Ethernet ネットワーク・コントローラ，8 GB のディスク領域

***** SiteScope のパフォーマンスに関して，デュアルまたはマルチ・プロセッサ・システムは，プロセッサの速度を上げるより効果的です。レベル 2 およびレベル 3 を実装する場合は，Intel Xeon プロセッサをお勧めします。

注： 4,000 を超えるモニタ・インスタンスを持つ SiteScope の実装は，別々のサーバにインストールされた複数の SiteScope に分割して行うことをお勧めします。

既存の SiteScope のアップグレードの準備

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，監視機能への影響を最小限に抑えながら，新しいバージョンの SiteScope をインストールし，既存の SiteScope からモニタ設定を転送することができます。しかし，SiteScope はさまざまな方法でカスタマイズできるため，新しいバージョンの SiteScope をクリーンなディレクトリ構造にインストールし，アップグレードの前に SiteScope の主要なデータのバックアップ・コピーを取っておくことをお勧めします。

SiteScope のインストール用に作成する新しいディレクトリの名前は **SiteScope** にし，別のディレクトリ・パスに置く必要があります。たとえば，元の SiteScope ディレクトリが C:¥SiteScope であれば，新しいディレクトリは C:¥9.5¥SiteScope にします。

インストール後，設定ツールを使用して，モニタ設定データを以前のバージョンの SiteScope からコピーできます。詳細については，79 ページ「設定ツールの実行」（Windows の場合）または 109 ページ「設定ツールの実行」（UNIX の場合）を参照してください。

SiteScope のアップグレードに備える最も簡単な方法は，現在の SiteScope のインストール・ディレクトリと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。

重要：SiteScope では，バイナリ設定ストレージ方式が採用されています。8.0.0.0 より前のバージョンからアップグレードする場合は，モニタ・グループ・ファイルの設定データが読み取られ，新しい設定データ・ストレージにコピーされます。以前のバージョンの SiteScope からアップグレードする場合は，ファイルを新しい SiteScope にコピーする前に，モニタ・グループおよびマスタ設定ファイルのエラーを解決しておく必要があります。設定ファイルのエラーを確認するには，以前のバージョンの SiteScope の SiteScope 状況の監視機能を使用できます。

SiteScope の毎日のモニタ・ログは，設定されたモニタの数，モニタの実行頻度，およびデータ・ログを保持する日数に応じて，バックアップ用の格納領域を大量に必要とする場合があります。SiteScope のインストール・ディレクトリを完全にバックアップすることが現実的でない場合は，現在の SiteScope から次のディレクトリの内容をバックアップすることを強くお勧めします。

ディレクトリ	説明
SiteScope¥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。
SiteScope¥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。
SiteScope¥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。
SiteScope¥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。 **例**：templates.mail，templates.os，templates.page

ディレクトリ	説明
SiteScope¥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。 **注**：このディレクトリのバックアップをとり，アップグレード後に SiteScope 9.50 ディレクトリにコピーする必要があります。これにより，レポート・ページに損害を与える原因を取り除くことができます。
SiteScope¥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 HP Business Availability Center 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。

SiteScope¥logs ディレクトリには，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。これらのログ・ファイルによって使用される格納領域の合計は，場合によっては SiteScope ソフトウェアを構成するファイルよりもかなり大きくなります。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することもできます。たとえば，直前の 7 日間の監視データのログをバックアップできます。モニタの測定値を含むログ・ファイルは，次のような形式のファイル名を持つ日付が記述されたファイルです。

SiteScopeyyyy_mm_dd.log

これらのログ・ファイルは，最も新しく作成されたファイルから順に選択的にバックアップできます。また，履歴の継続性を保つために次のログをバックアップすることもできます。

- **error.log**
- **RunMonitor.log**
- **access.log**
- **alert.log**
- **monitorCount.log**

第 III 部

SiteScope のインストール

第 7 章

Windows 用の SiteScope のインストール

Windows 用の SiteScope は，1 つの自己解凍型実行ファイルとして提供され，HP の Web サイトからダウンロードできるほか，CD-ROM で入手することもできます。SiteScope は，1 つのサーバにインストールされ，Windows プラットフォーム上の 1 つのアプリケーションとして稼働します。

本章の内容

インストールのワークフロー

SiteScope バージョン 9.50 のインストールは，初めてインストールする場合の手順と，以前のバージョンの SiteScope をすでにインストールしているユーザの手順が異なります。

新規ユーザ

SiteScope をインストールしていないユーザは，次の手順に従います。

1 **SiteScope 9.50 をインストールします。**

詳細については，67 ページ「完全インストールの実行」を参照してください。

2 **SiteScope に接続します。**

詳細については，182 ページ「SiteScope への接続」を参照してください。

以前のバージョンの SiteScope をインストール済みのユーザ

以前のバージョンの SiteScope から SiteScope バージョン 9.50 へのアップグレードは自動的には行われません。ユーザは次の手順に従います。

1 SiteScope 9.50 をインストールします。

SiteScope バージョン 9.50 は，現在 SiteScope がインストールされているのと同じマシンにでも，別のマシンにでもインストールできます。SiteScope を同じマシンにインストールする場合は，異なるディレクトリにインストールしなければなりません。インストールの詳細については，67 ページ「完全インストールの実行」を参照してください。

インストール・プロセスの一部として，後で SiteScope バージョン 9.50 にインポートできるよう，現在の SiteScope からデータをエクスポートできます。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。詳細については，85 ページ「ユーザ・データのエクスポート」を参照してください。

2（オプション）SiteScope データを以前のバージョンから SiteScope 9.50 へインポートします。

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。詳細については，88 ページ「ユーザ・データのインポート」を参照してください。

3 以前のバージョンから SiteScope 9.50 へモニタ設定をコピーします。

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，それらを 9.50 ディレクトリにコピーする必要があります。また，モニタ設定ファイルが 9.50 ディレクトリを指定していることを確認する必要があります。詳細については，85 ページ「ユーザ・データのエクスポート」を参照してください。

注：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する必要があります。

---

4 SiteScope に接続します。

詳細については，182 ページ「SiteScope への接続」を参照してください。

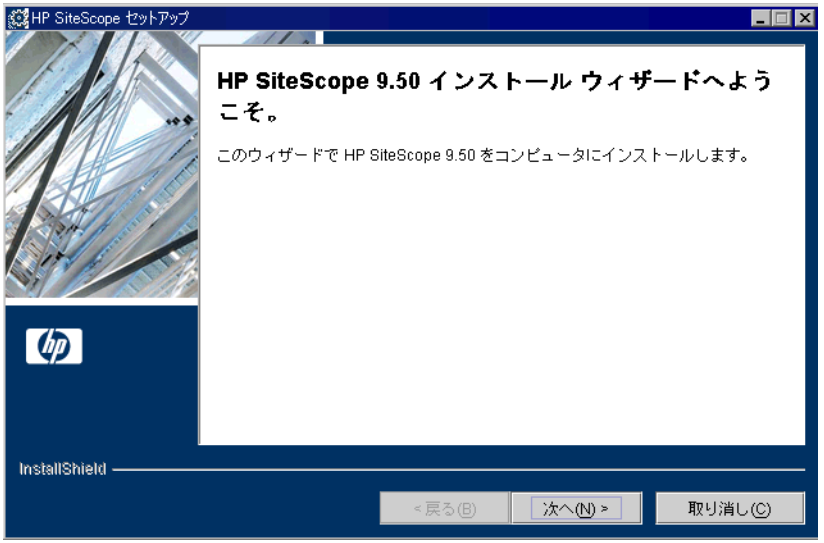
完全インストールの実行

Windows 2000 または Windows Server 2003 に SiteScope をインストールするには，次の手順を使用します。

SiteScope をインストールするには，次の手順を実行します。

1 SiteScope セットアップ・ファイルをダウンロードするか，SiteScope をインストールするマシンの CD-ROM ドライブに SiteScope ソフトウェアを含む CD-ROM を挿入します。

2 **HPSiteScope_v9.5_win.exe** プログラムを実行します。InstallShield ウィザードが開きます。



［**次へ**］をクリックしてインストールを開始します。

注：

- 別のシステムが動作しているためにサーバの再起動が必要な場合，InstallShield ウィザードにより，マシンを再起動した後でインストールを終了するよう指示されます。
- サーバで Microsoft ターミナル・サーバー・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，InstallShield 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終了します。

3 使用許諾契約画面が開きます。

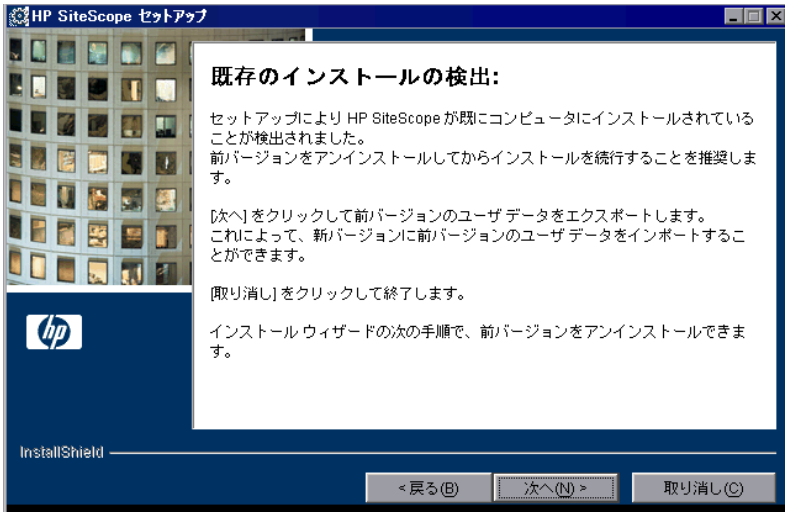
SiteScope の使用許諾契約を確認します。

SiteScope をインストールするには，［**使用条件の条項に同意します。**］をクリックして使用許諾契約の内容に同意する必要があります。その後［**次へ**］をクリックして次に進みます。

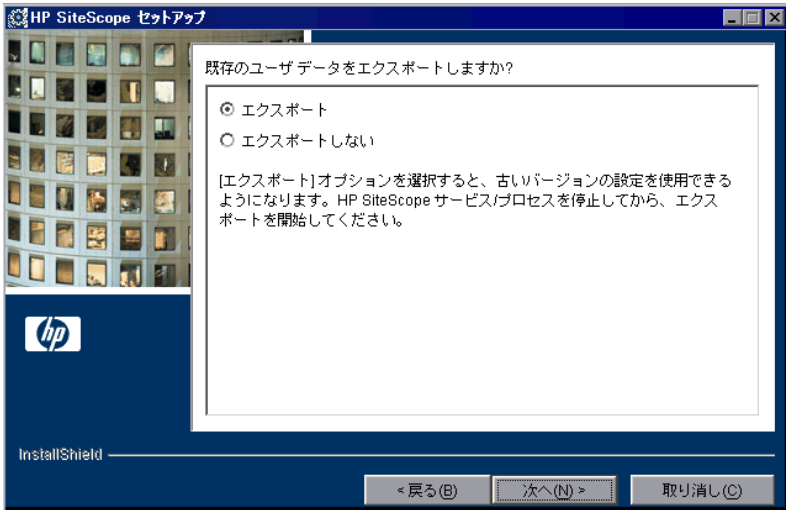
［**使用条件の条項に同意しません。**］をクリックした場合は，InstallShield ウィザードが終了します。

SiteScope をインストールした後でも，SiteScope の使用許諾契約のテキストは＜ **SiteScope のルート・フォルダ**＞ **¥license.html** で確認できます。

4 インストール・プロセスで以前のバージョンの SiteScope が検出された場合は，既存の SiteScope の画面が開きます。



［**次へ**］をクリックして次に進みます。既存のユーザ・データのエクスポート用の画面が開きます。この画面で現在の SiteScope のデータをエクスポートし，後で新しい SiteScope バージョンにインポートできます。



オプションを選択し，［**次へ**］をクリックして次に進みます。

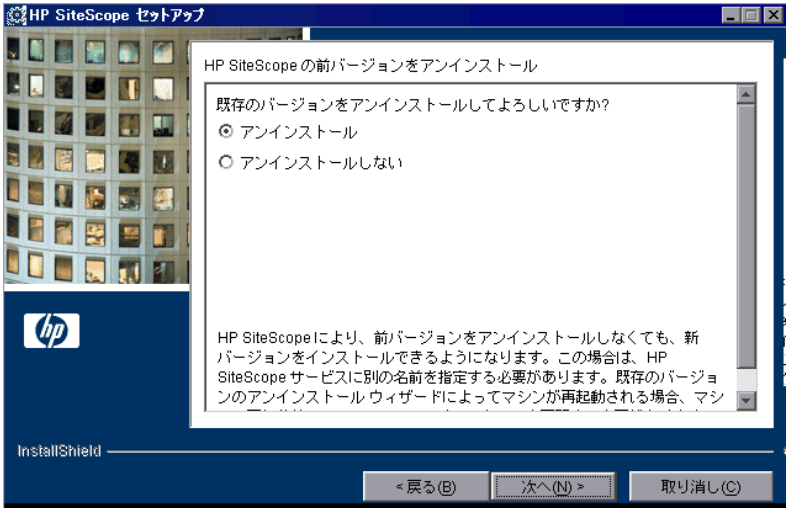
エクスポート・オプションを選択した場合は，次のことを行います。

➤ データをエクスポートする前に，SiteScope サービスまたはプロセスを停止します。

➤ エクスポートするユーザ・データの設定を入力します。85 ページ「ユーザ・データのエクスポート」の手順 4 を参照してください。

➤ データのエクスポート後に SiteScope サービスまたはプロセスを再起動します。

既存の SiteScope バージョンをアンインストールするようメッセージが表示されます。

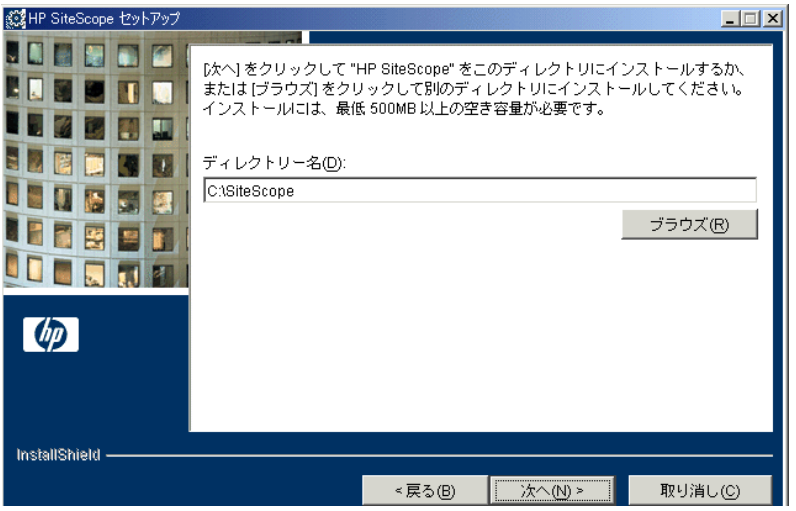


アンインストール・オプションを選択し，［**次へ**］をクリックして次に進みます。

注：既存の SiteScope をアンインストールした場合は，新しいバージョンをインストールする前にマシンを再起動する必要があります。マシンを再起動したら，最初からインストール・ウィザードが開始されます。

---

5 インストール・ディレクトリの画面が開きます。



標準設定のディレクトリを受け入れるか，［**ブラウズ**］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。

新しいディレクトリ名を入力したら，［**次へ**］をクリックして次に進みます。

注：インストール・パスが **SiteScope** というフォルダ名で終了していない場合はエラー・メッセージが表示されます。大文字と小文字が正しく使用しなかった場合（つまり sitescope と入力した場合は），まずインストール先フォルダを無効なフォルダ名に変更してから InstallShield のインストール先フォルダ・メカニズムをリセットし，正しいフォルダ名を入力します。

1. 無効なフォルダ名を入力します。たとえば，SiteScope1 と入力します。
2. ［**次へ**］をクリックしてから［**戻る**］をクリックします。
3. 正しいフォルダ名で終了するパスを入力します。たとえば，C:¥Apps¥SiteScope と入力します。

インストール・パスには空白を含めることはできません。

---

6 SiteScope のセットアップの種類を選択する画面が開きます。

- ［**HP SiteScope**］：標準の SiteScope です。
- ［**HP Sitescope Failover**］：このセットアップ・タイプは，SiteScope サーバが失敗した後に可用性の監視を行えるよう，バックアップの SiteScope サーバを提供します。
- ［**HP SiteScope for LoadRunner**］：このセットアップ・タイプは，LoadRunner ユーザが LoadRunner のアプリケーションで SiteScope モニタを定義し使用できるようにします。
- ［**HP System Health**］：このセットアップ・タイプは設定をチェックし，HP Business Availability Center の状況を確認する SiteScope のバージョンをインストールします。

使用に適した種類を選択します。

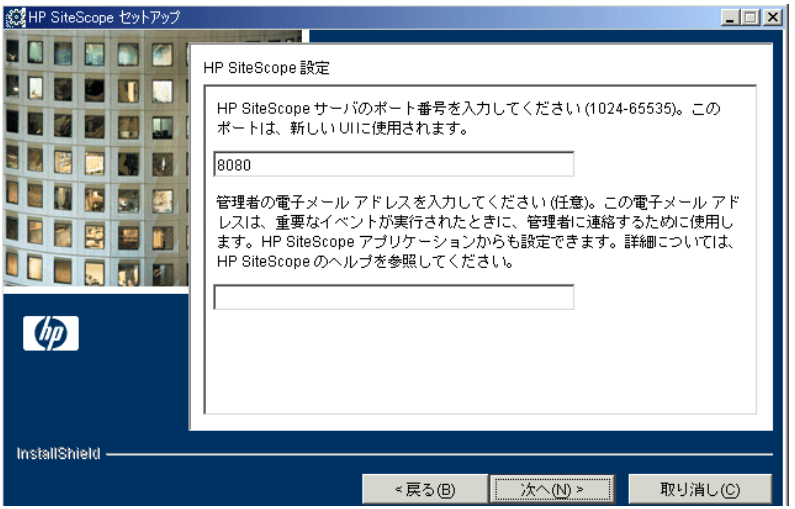
［**次へ**］をクリックして次に進みます。

7 SiteScope を以前のバージョンの SiteScope がインストールされているマシンにインストールする場合は，SiteScope サービス名画面が開きます。

SiteScope サービスに別の名前を入力します。

［**次へ**］をクリックして次に進みます。

8 ポートおよび電子メールの定義画面が開きます。



希望のポート番号を入力するか，標準設定のポート番号「8080」を受け入れます。

- ポートは，後で設定ツールを実行する時に変更できます。
- 入力したポート番号がすでに使用されている場合，エラー・メッセージが表示されます。その場合は別のポートを入力します。

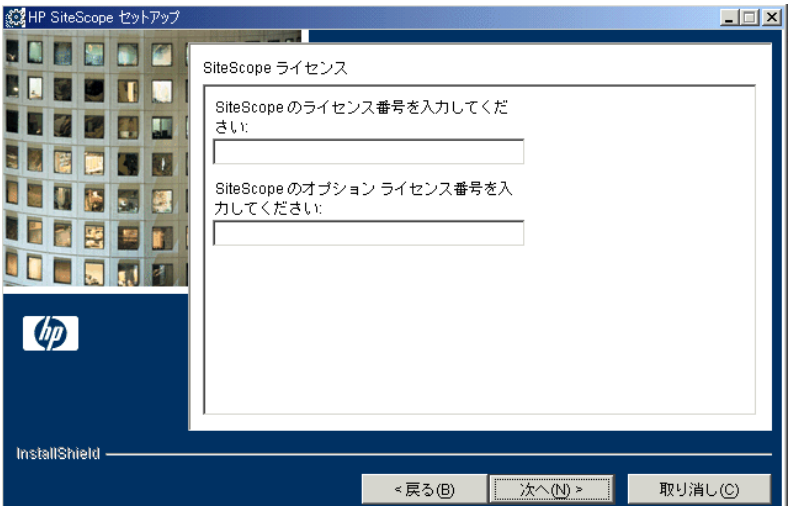
SiteScope が電子メールでの警告を SiteScope 管理者へ送信するために使用する，電子メール・アドレスを入力します。

注：

- この時点での電子メール・アドレスの入力は，SiteScope のインストールに必須ではありません。この情報は，後で SiteScope の［Mail Preferences（電子メールのプリファレンス)］設定を使用して入力できます。
- 電子メール・サーバが NTLM 認証を使用する場合，管理者の電子メール・アドレスは正規の電子メール・アドレスでなければなりません。

［**次へ**］をクリックして次に進みます。

9 ライセンス画面が開きます。



SiteScope のライセンス番号を入力します。

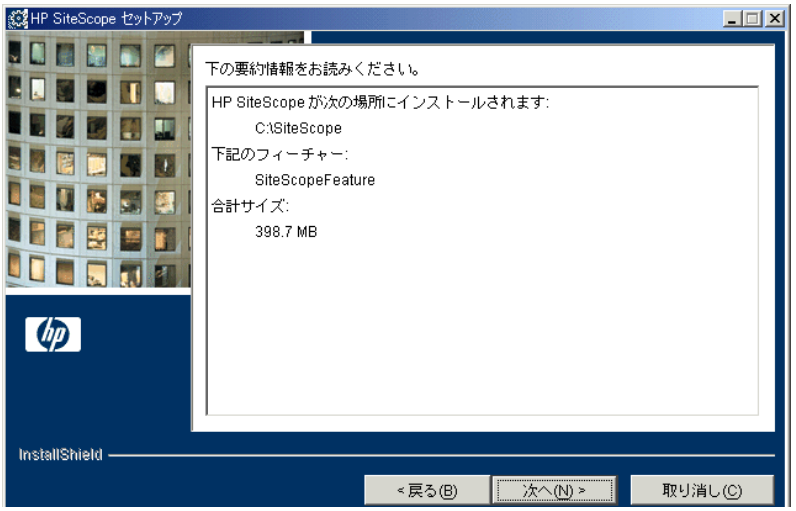
オプション・ライセンスがある場合は，その番号を 2 つ目のテキスト・ボックスに入力します。

注：

- 試用期間中に SiteScope を使用する場合は，この時点でライセンス情報を入力する必要はありません。
- **SiteScope Failover** のインストールではライセンス画面が表示されません。SiteScope Failover のライセンス番号は，SiteScope のインストール後に［**General Preferences**］に入力します。

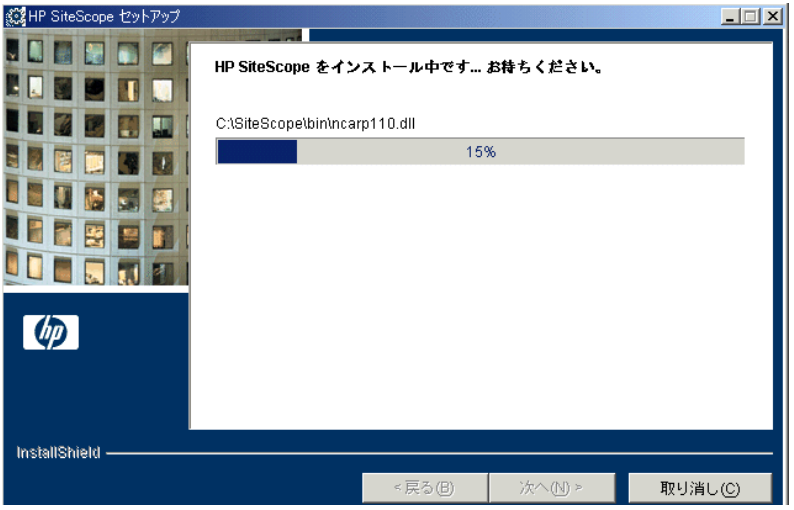
［**次へ**］をクリックして次に進みます。

10 要約情報画面が開きます。

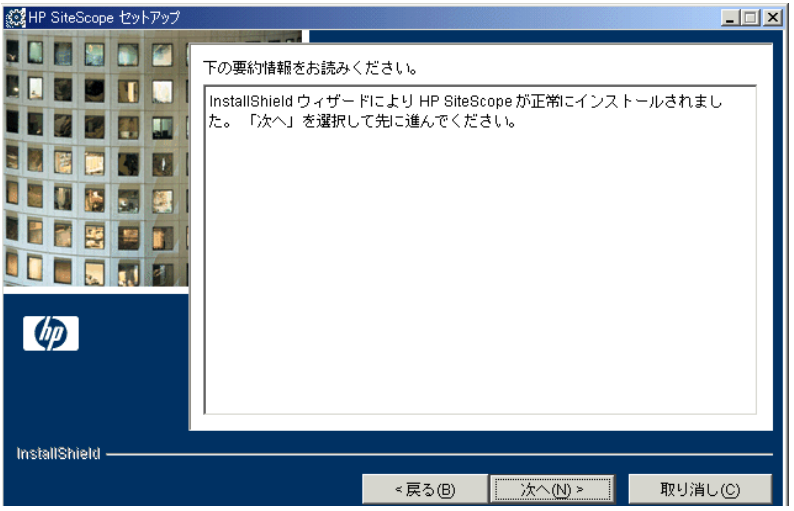


情報が正しいことを確認し，［**次へ**］をクリックして次に進みます。選択内容を変更するには，［**戻る**］をクリックして前の画面に戻ります。

11 SiteScope のインストール・プロセスが起動し，インストールの進行を示す画面が開きます。

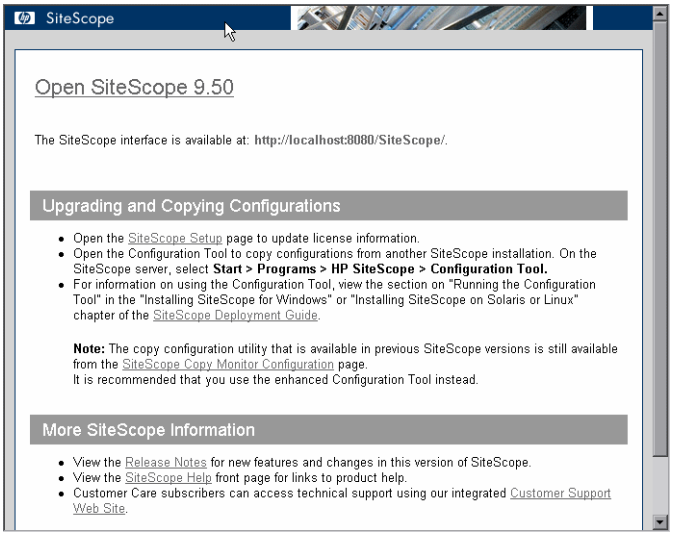


インストール・プロセスが完了すると，インストールが成功したことを示すメッセージが表示されます。



［**次へ**］をクリックしてウィザードを続行します。

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，再起動が実行されます。サーバを再起動し，ログインすると，インストール・ウィザードが必要なその他のセットアップ処理を実行し，SiteScope サーバを起動します。［Open SiteScope］ページが開きます。



［Open SiteScope］ページには，インストールした SiteScope への接続アドレスや，SiteScope のドキュメントやサポート情報などへのリンクがいくつか表示されます。これは静的な HTML ページです。

Windows プラットフォームでは，［スタート］メニューの［SiteScope］プログラム・フォルダに，このページへのショートカットが追加されます。SiteScope が稼働している場合は，このページを使用して SiteScope にアクセスできます。

12 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 サービス・パック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，182 ページ「SiteScope への接続」を参照してください。

設定ツールの実行

設定ツールはインストール・プロセスの一部として，または独立して実行できます。インストール・プロセス中にサイズ設定はできません。

インストール・プロセスが以前のバージョンの SiteScope を検出した場合，ユーザ・データをエクスポートするかどうか確認されます。データをエクスポートすると，後でそのデータをインポートできます。

本項は，次の項目で構成されています。

SiteScope のポート番号の変更

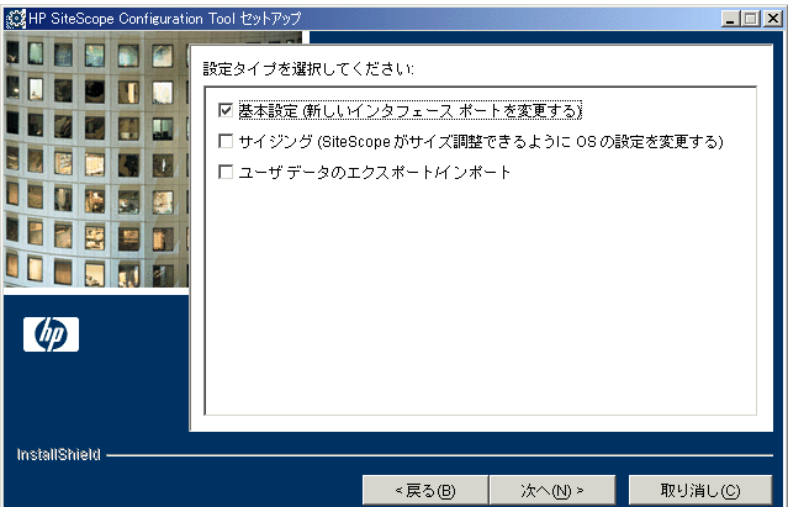
標準設定のポート 8080 を使用しない場合，SiteScope のポート番号を変更できます。

SiteScope のポート番号を変更するには，次の手順を実行します。

1 SiteScope サーバで，［**スタート**］＞［**プログラム**］＞［**HP SiteScope**］＞［**Configuration Tool**］を選択します。［Configuration Tool］が開きます。

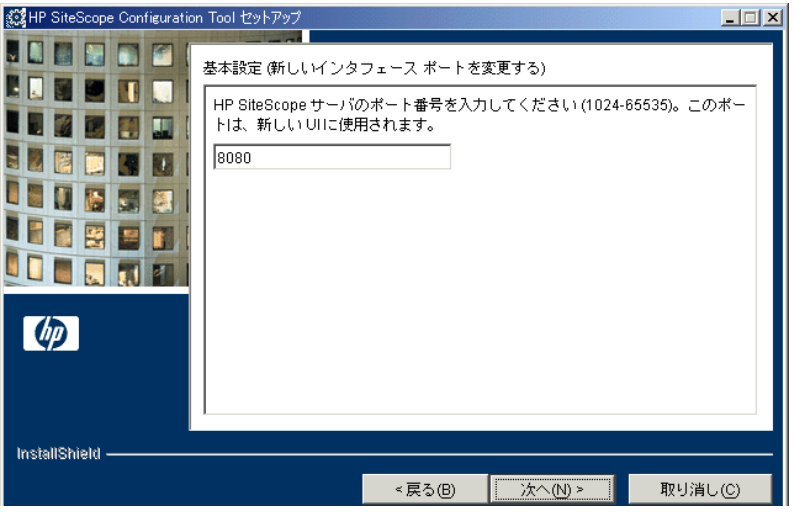
［**次へ**］をクリックしてウィザードを開始します。

2 ［**基本設定**］を選択します。



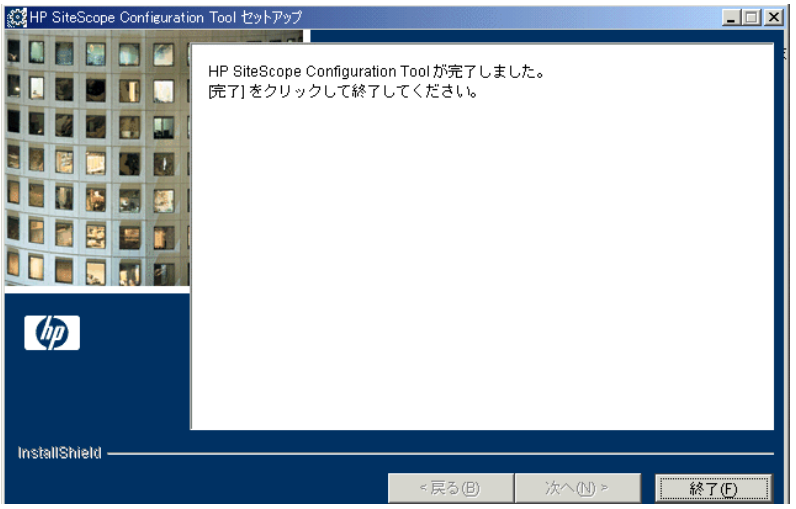
［**次へ**］をクリックします。

3 テキスト・ボックスにポート番号を入力します。



［**次へ**］をクリックします。

4 最後のダイアログ・ボックスが開き，ポート変更のステータスが表示されます。



［**終了**］をクリックして変更を保存し，終了します。

SiteScope のサイズ設定

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。

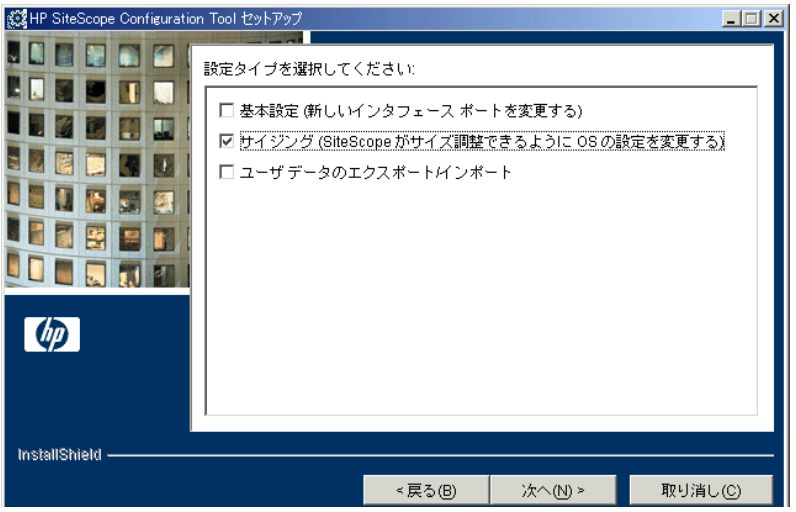
- **JVM ヒープ・サイズ**：値が 256 MB から 768 MB に変更されます。
- **デスクトップ・ヒープ・サイズ**：値が 512 MB から 2048 MB に変更されます。
- **ポップアップ警告**：メッセージが無効になります。

最適化を行うには，次の手順を実行します。

1 SiteScope サーバで，［**スタート**］＞［**プログラム**］＞［**HP SiteScope**］＞［**Configuration Tool**］を選択します。［Configuration Tool］が開きます。

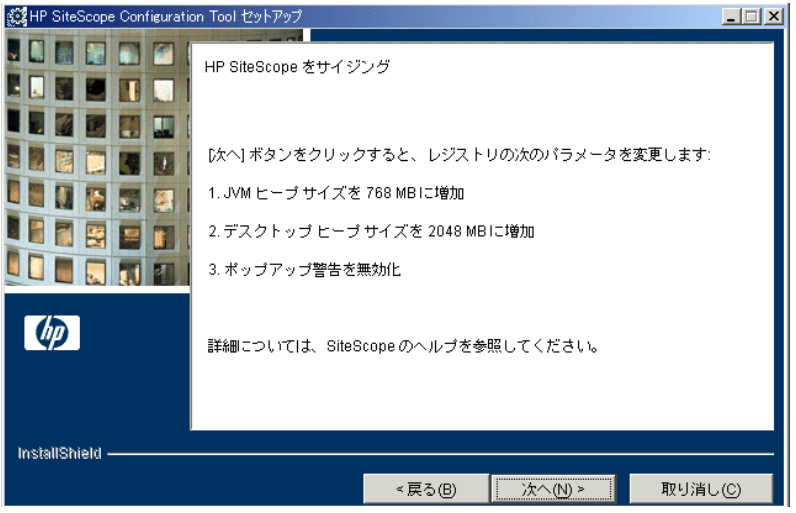
［**次へ**］をクリックしてウィザードを開始します。

2 [**サイジング**] を選択します。



[**次へ**] をクリックします。

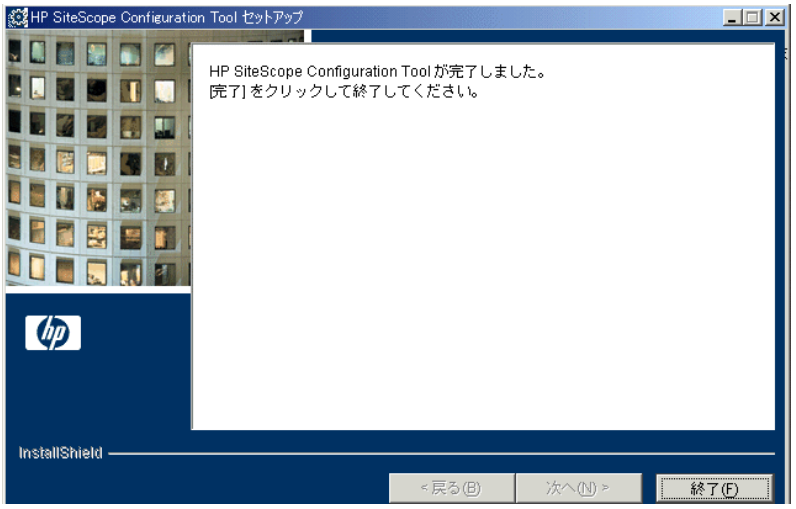
3 Windows レジストリのパラメータ一覧を表示する画面が開きます。



Windows レジストリ・キーが自動的に変更され，オペレーティング・システムのパフォーマンスが最適化されます。

[**次へ**] をクリックします。

4 最後のダイアログ・ボックスが開きます。



［**終了**］をクリックして変更を保存します。

ユーザ・データのエクスポート

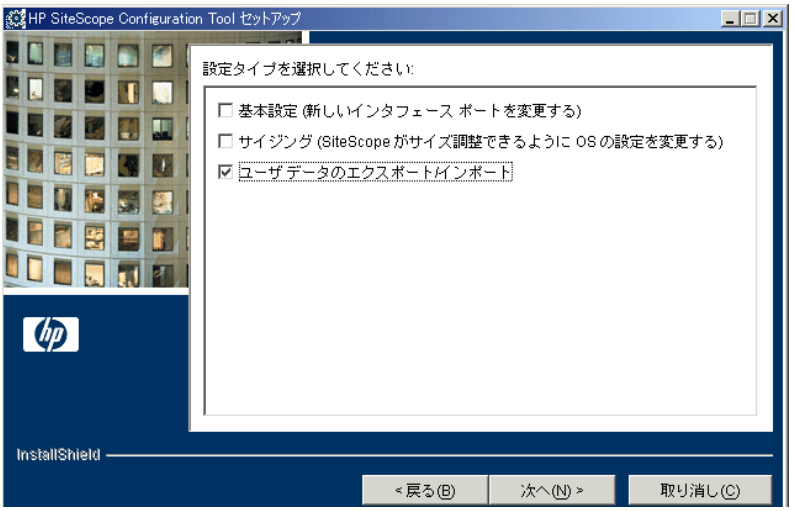
後でインポートするためにテンプレート，ログなどの SiteScope データをエクスポートできます。

ユーザ・データをエクスポートするには，次の手順を実行します。

1 SiteScope サーバで，［**スタート**］＞［**プログラム**］＞［**HP SiteScope**］＞［**Configuration Tool**］を選択します。［Configuration Tool］が開きます。

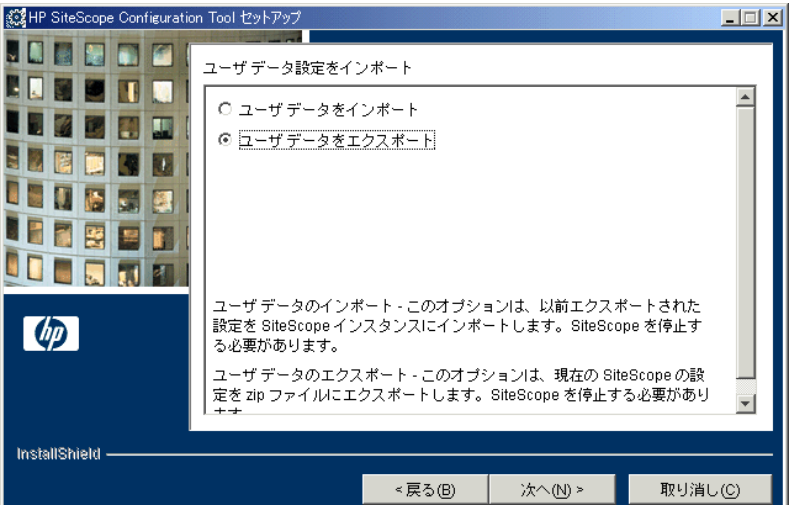
［**次へ**］をクリックしてウィザードを開始します。

2 [**ユーザ データのエクスポート / インポート**] を選択します。



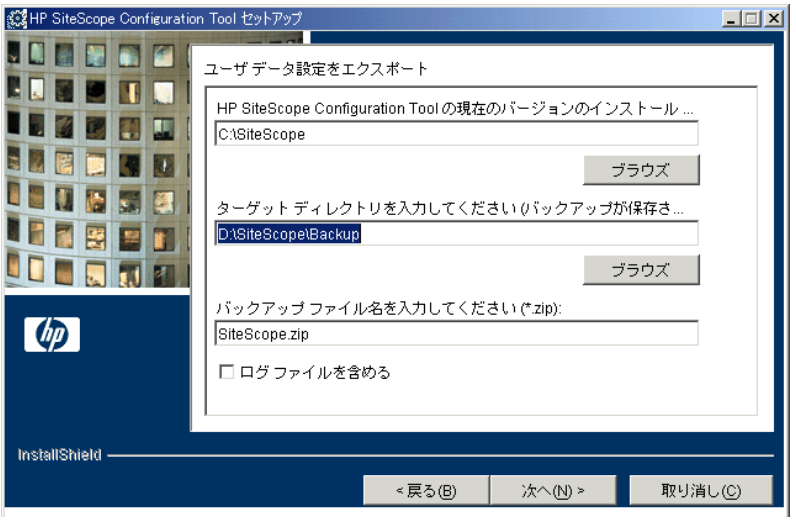
[**次へ**] をクリックします。

3 [**ユーザ データをエクスポート**] を選択します。



[**次へ**] をクリックします。

4 ［ユーザ データ設定をエクスポート］ダイアログ・ボックスが開きます。



- ［**ユーザ データ設定をエクスポート**］に，SiteScope インストール・ディレクトリまでのパスを入力します。たとえば，表示されたディレクトリ・パスを受け入れたくなく，インストール・ディレクトリのパスが D:¥SS9_0¥SiteScope である場合は，D:¥SS9_0¥SiteScope と入力します。
- ［**ターゲット ディレクトリを入力してください（バックアップが保存される場所）**］に，エクスポートされるユーザ・データ・ファイルを保存するディレクトリを入力します。すでに存在しているディレクトリを入力します。
- ［**バックアップ ファイル名を入力してください**］に，エクスポートしたユーザ・データ・ファイルに付ける名前を入力します。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。

［**次へ**］をクリックして［**終了**］をクリックし，エクスポート操作を完了します。

ユーザ・データのインポート

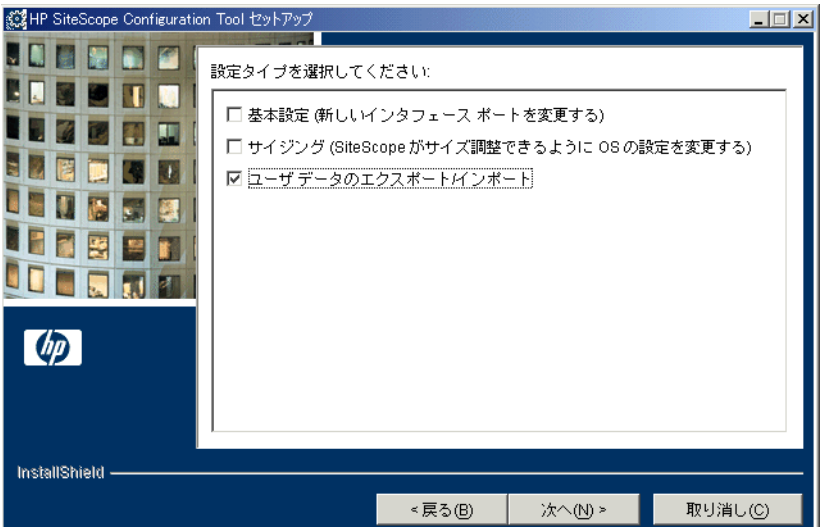
テンプレート，ログなどの SiteScope データをインポートできます。

ユーザ・データをインポートするには，次の手順を実行します。

1 SiteScope サーバで，［**スタート**］＞［**プログラム**］＞［**HP SiteScope**］＞［**Configuration Tool**］を選択します。［Configuration Tool］が開きます。

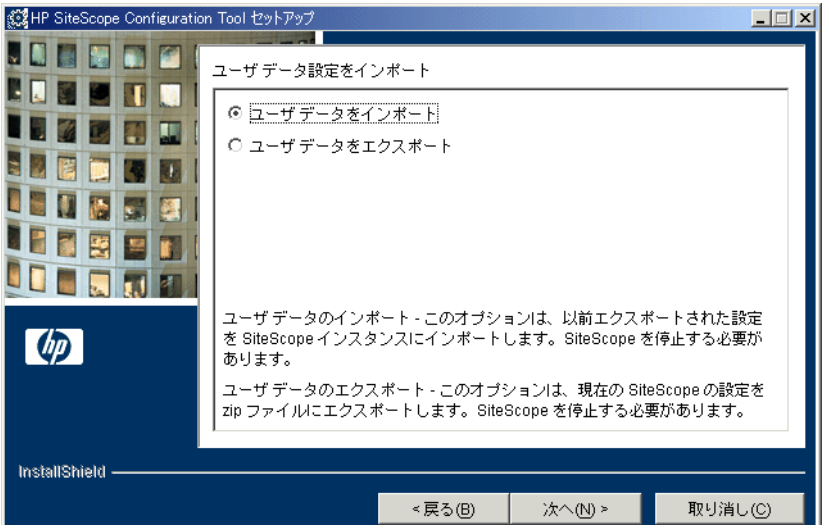
［**次へ**］をクリックしてウィザードを開始します。

2 [**ユーザ データのエクスポート / インポート**] を選択します。



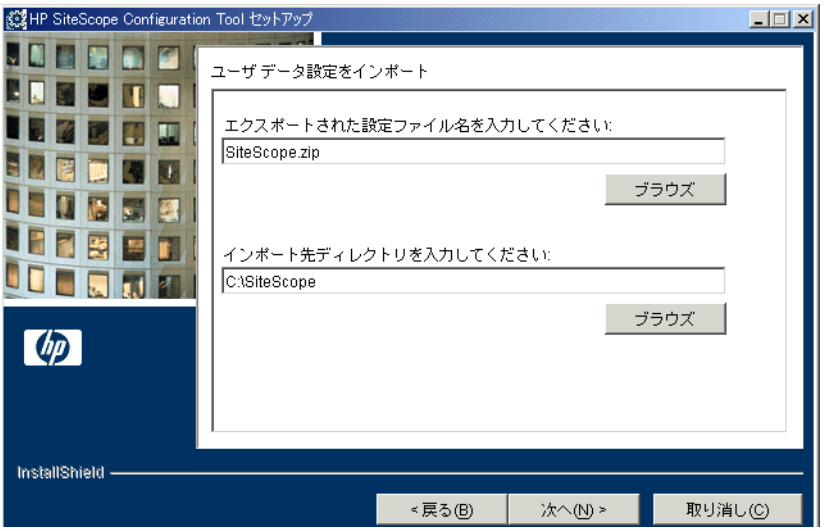
[**次へ**] をクリックします。

3 [**ユーザ データをインポート**] を選択します。



[**次へ**] をクリックします。

4 ［ユーザ データ設定をインポート］ダイアログ・ボックスが開きます。



- ［**エクスポートされた設定ファイル名を入力してください**］に，インポートするユーザ・データ・ファイルの名前を入力します。
- ［**インポート先ディレクトリを入力してください**］に，ユーザ・データ・ファイルを送信するディレクトリを入力します。

［**次へ**］をクリックして［**終了**］をクリックし，インポート操作を完了します。

第 8 章

Solaris または Linux への SiteScope のインストール

Solaris 用の SiteScope および Linux 用の SiteScope は，1 つの圧縮アーカイブ・ファイルとして提供され，HP の Web サイトからダウンロードできるほか，CD-ROM で入手することもできます。SiteScope は，1 つのサーバにインストールされ，1 つのアプリケーションまたはプロセスとして稼働します。

本章の内容

インストールのワークフロー

SiteScope バージョン 9.50 のインストールは，初めてインストールする場合の手順と，以前のバージョンの SiteScope をすでにインストールしているユーザの手順が異なります。

新規ユーザ

SiteScope をインストールしていないユーザは，次の手順に従います。

1 **SiteScope 9.50 のインストールの準備を整えます。**

詳細については，93 ページ「インストールの準備」を参照してください。

2 **SiteScope 9.50 をインストールします。**

詳細については，94 ページ「完全インストールの実行」を参照してください。

3 SiteScope に接続します。

詳細については，182 ページ「SiteScope への接続」を参照してください。

以前のバージョンの SiteScope をインストール済みのユーザ

以前のバージョンの SiteScope から SiteScope バージョン 9.50 へのアップグレードは自動的には行われません。ユーザは次の手順に従います。

1 SiteScope 9.50 のインストールの準備を整えます。

詳細については，93 ページ「インストールの準備」を参照してください。

2 SiteScope 9.50 をインストールします。

SiteScope バージョン 9.50 は，現在 SiteScope がインストールされているのと同じマシンにでも，別のマシンにでもインストールできます。SiteScope を同じマシンにインストールする場合は，同じディレクトリにでも，別のディレクトリにでもインストールできます。詳細については，94 ページ「完全インストールの実行」を参照してください。

インストール・プロセスの一部として，後で SiteScope バージョン 9.50 にインポートできるよう，現在の SiteScope からデータをエクスポートできます。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。詳細については，112 ページ「ユーザ・データのエクスポート」を参照してください。

3（オプション）SiteScope データを以前のバージョンから SiteScope 9.50 へインポートします。

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。詳細については，114 ページ「ユーザ・データのインポート」を参照してください。

4 以前のバージョンから SiteScope 9.50 へモニタ設定をコピーします。

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，それらを 9.50 ディレクトリにコピーする必要があります。また，モニタ設定ファイルが 9.50 ディレクトリを指定していることを確認する必要があります。詳細については，112 ページ「ユーザ・データのエクスポート」を参照してください。

5 SiteScope に接続します。

詳細については，182 ページ「SiteScope への接続」を参照してください。

インストールの準備

お使いの環境によっては，Solaris または Linux に SiteScope をインストールするための準備に，ユーザ・ログイン・アカウントの作成，適切なインストール先の場所の選択，アカウント権限の設定が必要になります。

UNIX または 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実行するユーザ・アカウントを作成します。そのアカウントの標準のシェルを設定します。

2 SiteScope アプリケーションをインストールする場所（/opt/, /usr/local/SiteScope，/home/monitoring/SiteScope など）を選択または作成します。インストールする場所で，SiteScope のインストールと運用を行うために十分なディスク領域が使用できることを確認します。

注：SiteScope 9.50 をインストールするための新しいディレクトリを作成します。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 9.50 をインストールしないでください。

---

3 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。

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。

完全インストールの実行

Solaris 用の SiteScope および Linux 用の SiteScope には，いくつかのインストール・オプションが用意されています。オプションは次のとおりです。

- 対話形式のグラフィカル・ユーザ・インタフェースを持つマルチプラットフォームのインストール実行ファイル（詳細については，94 ページ「インストール実行ファイルを使用した SiteScope のインストール」を参照）
- コマンド・ライン入力を使用するコンソール・モードのインストール・スクリプト（詳細については，104 ページ「コンソール・モードを使用した SiteScope のインストール」を参照）

インストール実行ファイルを使用した SiteScope のインストール

マルチプラットフォームの InstallShield ウィザードを使用して，Solaris または Linux に SiteScope をインストールできます。

注：X11 ライブラリが既にサーバにインストールされている場合には，マルチプラットフォームの InstallShield 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には，コンソール・モードで SiteScope をインストールします。詳細については，104 ページ「コンソール・モードを使用した SiteScope のインストール」を参照してください。

マルチプラットフォームのインストーラを使用して Solaris または Linux に SiteScope をインストールするには，次の手順を実行します。

1 SiteScope をインストールするマシンに SiteScope セットアップ・ファイル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・アカウントで，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。

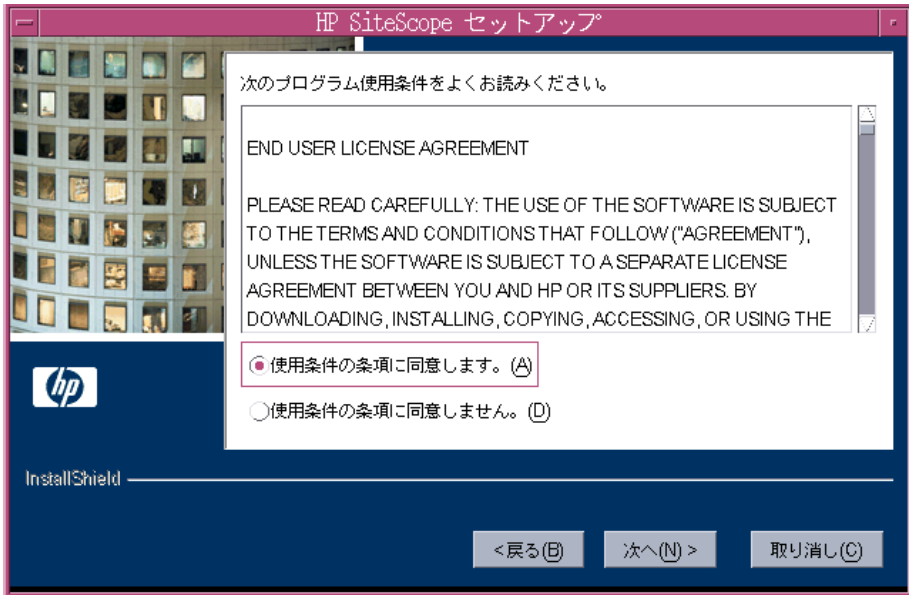
2 次のコマンドを使用して，インストール・スクリプトを実行します。

```
SiteScopeSetup/HPSiteScope_v9.5_solaris.bin
```

インストール実行ファイルによって，InstallShield ウィザードと HP SiteScope が初期化されます。InstallShield ウィザードのようこそウィンドウが開きます。

［**次へ**］をクリックして次に進みます。

3 使用許諾契約画面が開きます。



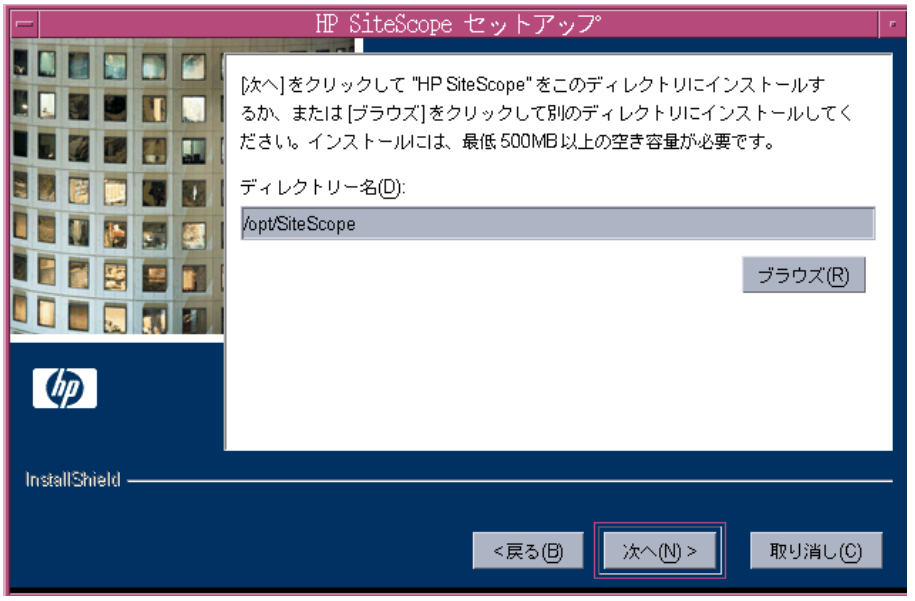
SiteScope の使用許諾契約を確認します。

SiteScope をインストールするには，［**使用条件の条項に同意します。**］をクリックして使用許諾契約の内容に同意する必要があります。その後［**次へ**］をクリックして次に進みます。

［**使用条件の条項に同意しません。**］をクリックした場合は，InstallShield ウィザードが終了します。

SiteScope をインストールした後でも，SiteScope の使用許諾契約のテキストは＜ **SiteScope のルート・フォルダ**＞ **¥license.html** で確認できます。

4 インストール・ディレクトリの画面が開きます。



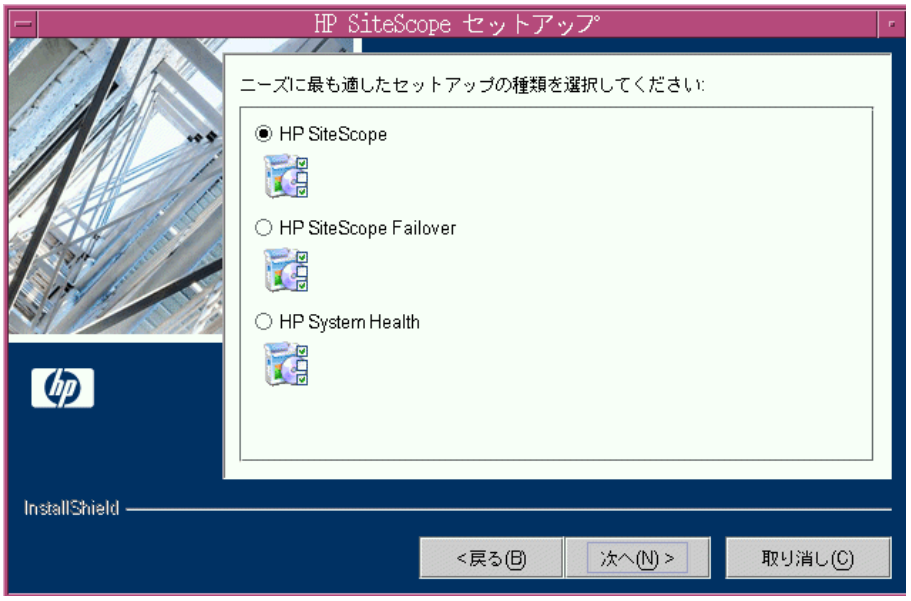
標準設定のディレクトリを受け入れるか，［**ブラウズ**］をクリックして別のディレクトリを選択します。

新しいディレクトリ名を入力したら，［**次へ**］をクリックして次に進みます。

注：インストール・パスは，「**SiteScope**」という名前のフォルダで終わる必要があります。インストール・パスには空白を含めることはできません。

---

5 SiteScope のセットアップの種類を選択する画面が開きます。

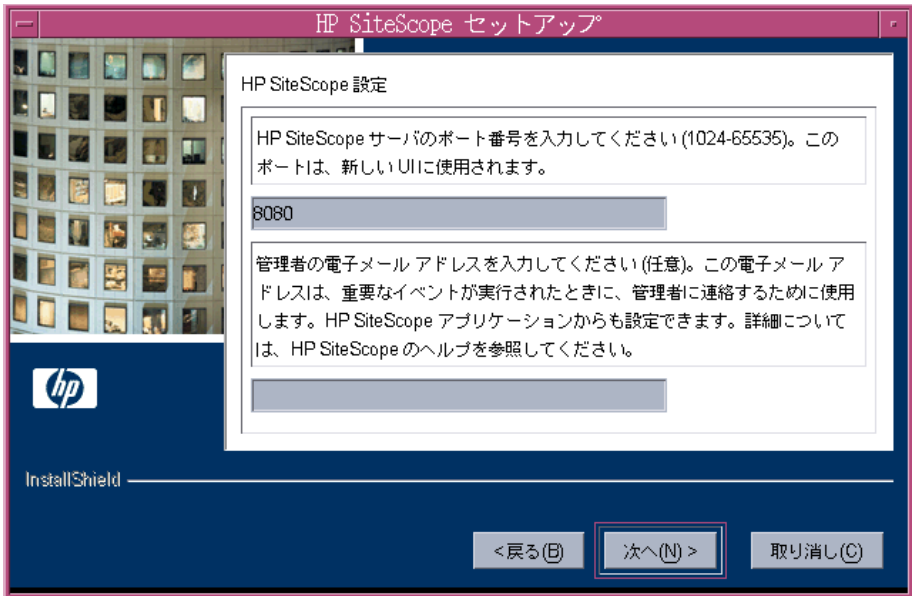


- ［**HP SiteScope**］：標準の SiteScope です。
- ［**HP Sitescope Failover**］：このセットアップ・タイプは，SiteScope サーバが失敗した後に可用性の監視を行えるよう，バックアップの SiteScope サーバを提供します。
- ［**HP System Health**］：このセットアップ・タイプは設定をチェックし，HP Business Availability Center の状況を確認する SiteScope のバージョンをインストールします。

使用に適した種類を選択します。

［**次へ**］をクリックして次に進みます。

6 ポートおよび電子メールの定義画面が開きます。



希望のポート番号を入力するか，標準設定のポート番号「8080」を受け入れます。

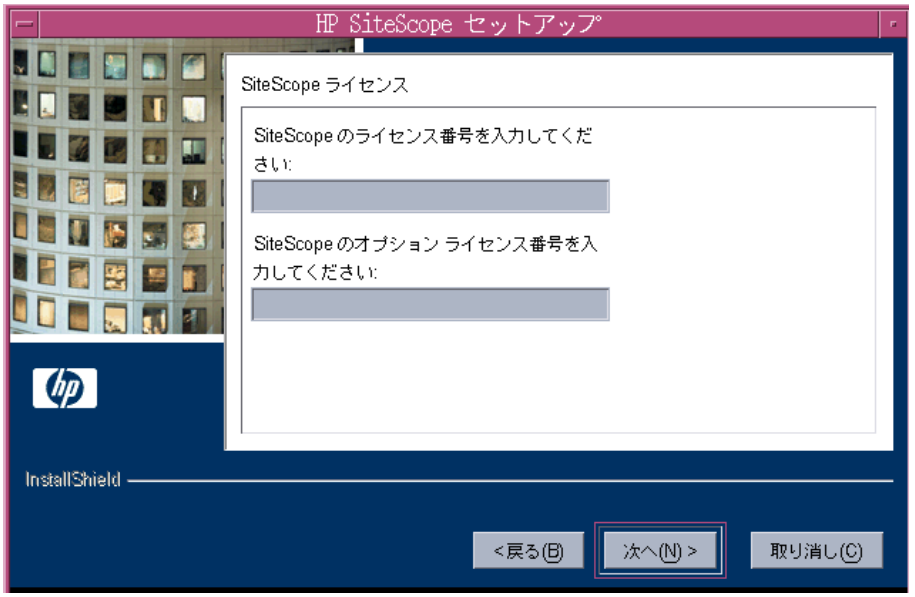
- ポートは，後で 設定ツール・ユーティリティを実行する時に変更できます。
- 入力したポート番号がすでに使用されている場合，エラー・メッセージが表示されます。その場合は別のポートを入力します。

SiteScope が電子メールでの警告を SiteScope 管理者へ送信するために使用する，電子メール・アドレスを入力します。

注：電子メール・アドレスの入力は，SiteScope のインストールに必須ではありません。この情報は，後で SiteScope の［Mail Preferences（電子メールのプリファレンス)］ページを使用して入力できます。

［**次へ**］をクリックして次に進みます。

7 ライセンス番号の画面が開きます。



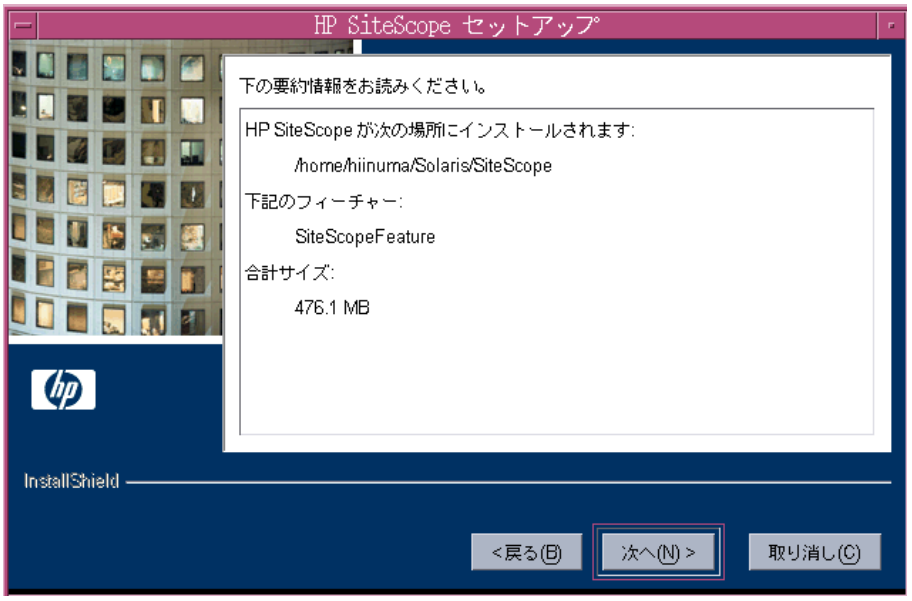
SiteScope のライセンス番号を入力します。

オプション・ライセンスがある場合は，その番号を 2 つ目のテキスト・ボックスに入力します。

注：試用期間中に SiteScope を使用する場合は，この時点でライセンス情報を入力する必要はありません。

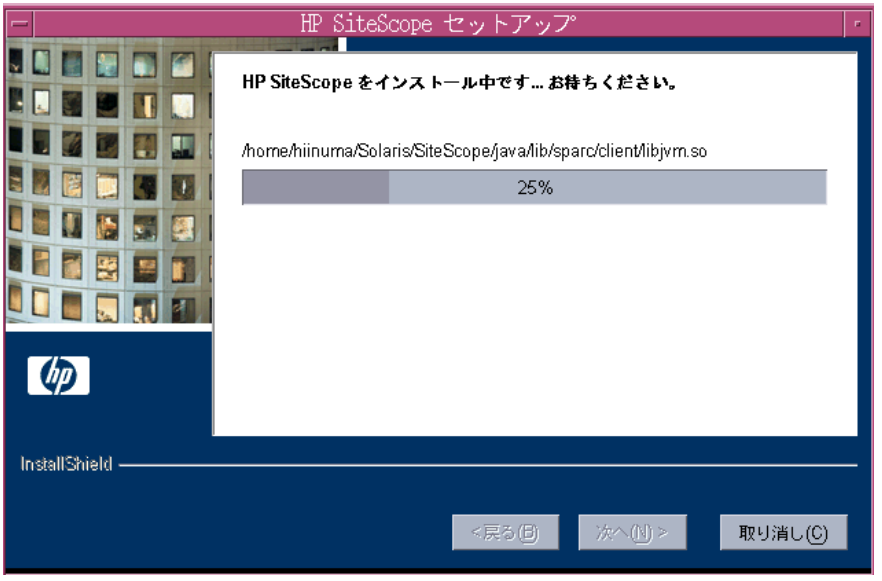
［**次へ**］をクリックして次に進みます。

8 要約情報画面が開きます。

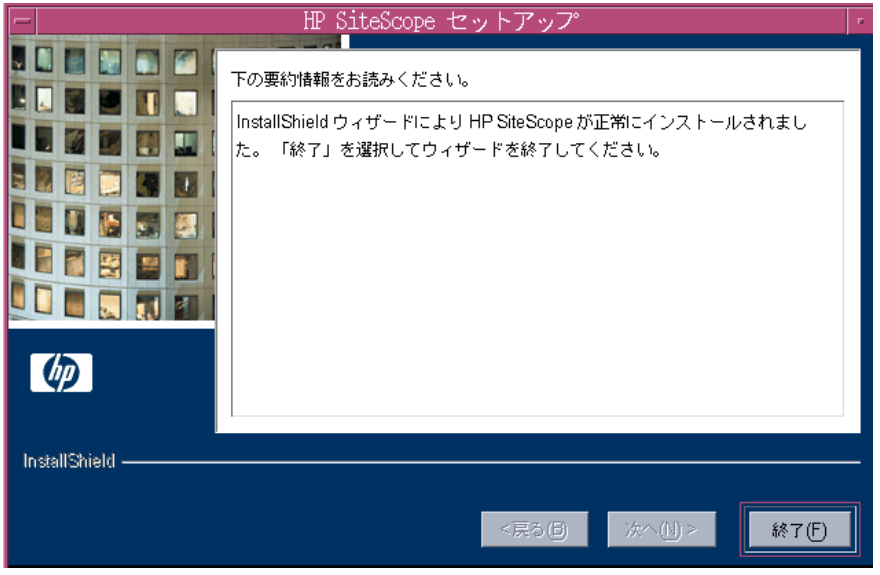


情報が正しいことを確認し，［**次へ**］をクリックして次に進みます。選択内容を変更するには，［**戻る**］をクリックして前の画面に戻ります。

9 SiteScope のインストール・プロセスが起動し，インストールの進行を示す画面が開きます。

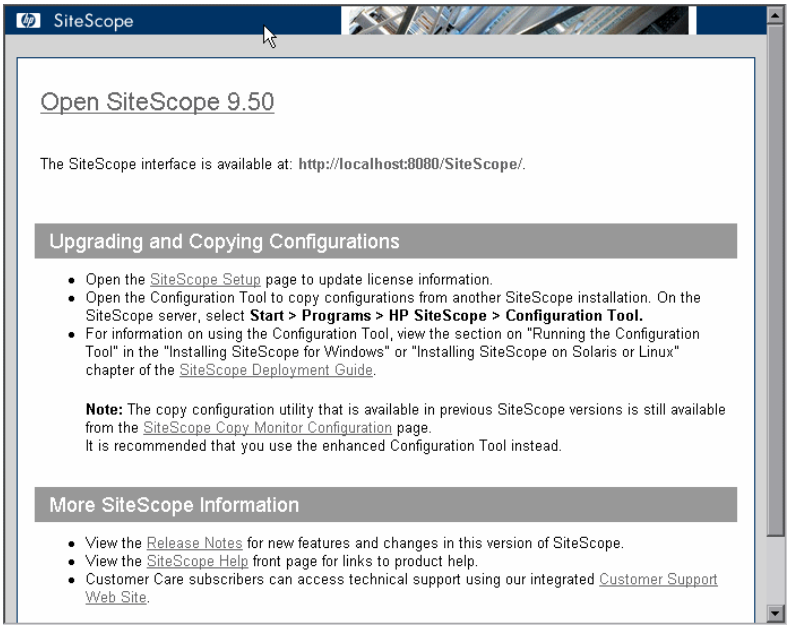


インストール・プロセスが完了すると，インストールが成功したことを示すメッセージが表示されます。[**終了**] をクリックします。



10 SiteScope サーバからログアウトし，再度ログインします。

インストール・ウィザードにより，必要なその他のセットアップ処理が実行され，SiteScope サーバが起動します。［Open SiteScope］ページが開きます（自動的に開かない場合は、＜ SiteScope インストール・ディレクトリ＞ /docs /Open_SiteScope.htm をブラウザで表示します）。



［Open SiteScope］ページには，インストールした SiteScope への接続アドレスや，SiteScope のドキュメントやサポート情報などへのリンクがいくつか表示されます。これは静的な HTML ページです。

11 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 サービス・パック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，182 ページ「SiteScope への接続」を参照してください。

コンソール・モードを使用した SiteScope 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・インタフェースを介してインストール・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。

コンソール・モードを使用して Solaris または Linux に SiteScope をインストールするには，次の手順を実行します。

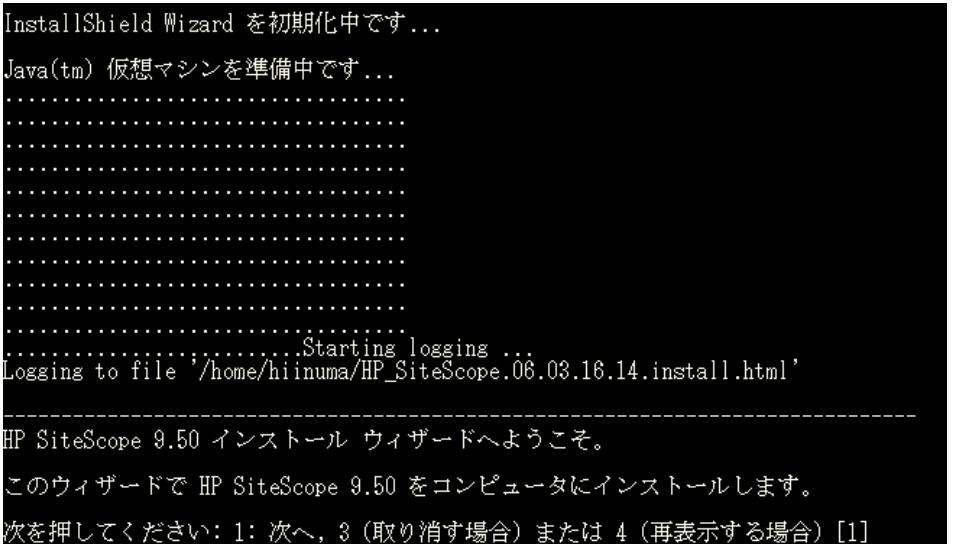
1 SiteScope をインストールするマシンに SiteScope セットアップ・ファイルをダウンロードします。

または，SiteScope のインストールに使用するユーザ・アカウントで，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。

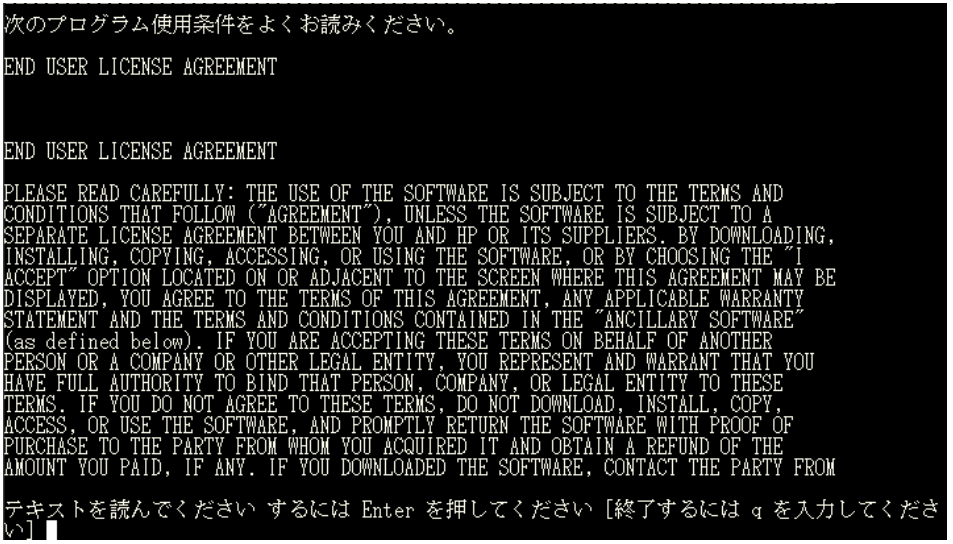
2 次のコマンドを実行します。

```
/bin/sh SiteScopeInstall/HPSiteScope_v9.5_solaris.bin – console
```

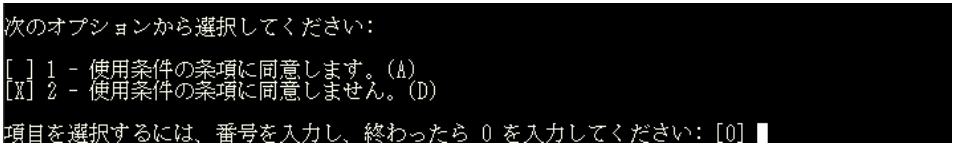
インストール・スクリプトによって，Java 仮想マシンが初期化されて，インストールが開始されます。確認画面が表示されます。



3 インストールを続行するには，1 を入力します。使用許諾契約のテキストが表示されます。使用許諾契約を読む前にインストールをキャンセルするには，3 を入力し，次にインストールのキャンセルを確認します。



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。



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には，1 を入力し，次に 0 を入力します。継続プロンプトが表示されます。

注：SiteScope 使用許諾契約の確認後にインストールをキャンセルするには，1 を入力し，0 を入力して，次の継続プロンプトで 3 を入力します。

---

4 インストール場所の選択プロンプトが表示されます。

```
HP SiteScope インストール・ロケーション
ディレクトリーを指定してください。このままでよい場合には、Enter を押してください。.
ディレクトリー名(D): [/opt/SiteScope]
次を押してください: 1: 次へ, 2: 前へ, 3 (取り消す場合) または 4 (再表示する場合) [1]
```

SiteScope をインストールする場所を入力します。標準設定の場所が角括弧で囲んで表示されます。これはインストール実行ファイルの場所に相対的なパスです。

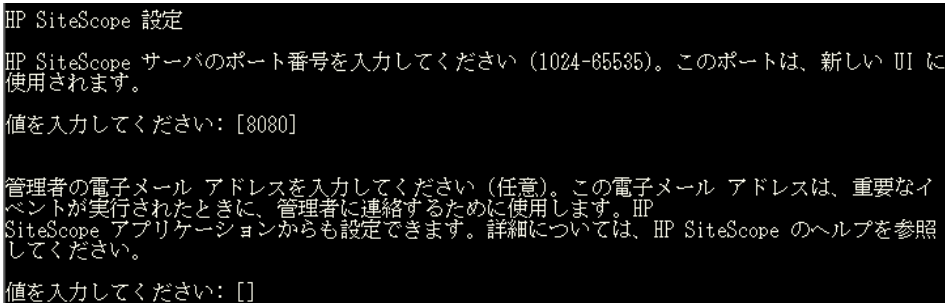
インストール先を変更するには，角括弧を使用せずに，コマンド・ライン・エントリとしてインストール先のパスを入力します。インストール先は，**SiteScope** というディレクトリで終わる必要があります。1 を入力して，次の手順に進みます。

5 SiteScope のセットアップの種類を選択する画面が開きます。

```
ニーズに最も適したセットアップの種類を選択してください:
[X] 1 - SiteScope Typical
[ ] 2 - SiteScope High Availability
[ ] 3 - System Health
項目を選択するには、番号を入力し、終わったら 0 を入力してください: [0]
```

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するか，標準設定の［**SiteScope Typical**］を受け入れます。0 を入力して次に進みます。

6 ポートと電子メール・アドレスのプロンプトが表示されます。



希望のポート番号を入力するか，標準設定のポート番号「8080」を受け入れます。

SiteScope 管理者の電子メール・アドレスを入力します。たとえば，sitescopeadmin@thiscompany.com を入力します。

この時点で電子メール・アドレスを入力しない場合は，ENTER キーを押して，この部分を空白のままにし，次の手順に進みます。

電子メールの情報は，SiteScope の実行後，［Mail Preferences（電子メールのプリファレンス)］ページを使用して入力できます。

7 1 を入力して，次の手順に進みます。ライセンス番号のプロンプトが表示されます。

8 SiteScope のライセンス番号を入力します。オプション・ライセンスがある場合は，その番号を 2 つ目のテキスト・ボックスに入力します。

試用期間中に SiteScope を使用する場合は，この時点でライセンス情報を入力する必要はありません。

9 1 を入力して，インストールを続けます。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。

```
HP SiteScope が次の場所にインストールされます:

/home/hiinuma/Solaris/SiteScope

下記のフィーチャー:

SiteScopeFeature

合計サイズ:

 476.1 MB

次を押してください: 1: 次へ, 2: 前へ, 3 (取り消す場合) または 4 (再表示する場合) [1]
```

10 指定したインストール場所を変更せずに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 を入力します。インストール・プロセスが開始されます。

11 画面に表示された SiteScope のアドレスとポート番号を書き留めます。標準設定では，SiteScope はポート番号 8080 で応答しようとします。ほかのアプリケーションがこのポート番号を使用している場合，SiteScope は別のポート番号（ポート 8889 など）の使用を試みます。

SiteScope へ接続するには，182 ページ「SiteScope への接続」の手順に従います。

12 1 を入力して，次の手順に進みます。インストールのステータス・メッセージが表示されます。

```
InstallShield ウィザードにより HP SiteScope が正常にインストールされました。 「終了」を選
択してウィザードを終了してください。

次を押してください: 3 (完了する場合) または 4 (再表示する場合) [3]
```

13 1 を入力して，インストール・スクリプトを終了します。

設定ツールの実行

設定ツールはインストール・プロセスの一部として，または独立して実行できます。

インストール・プロセスが以前のバージョンの SiteScope を検出した場合，ユーザ・データをエクスポートするかどうか確認されます。データをエクスポートすると，後でそのデータをインポートできます。

本項は，次の項目で構成されています。

- 109 ページ「SiteScope のポート番号の変更」
- 112 ページ「ユーザ・データのエクスポート」
- 114 ページ「ユーザ・データのインポート」

SiteScope のポート番号の変更

標準設定のポート 8080 を使用しない場合，SiteScope のポート番号を変更できます。

SiteScope のポート番号を変更するには，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。

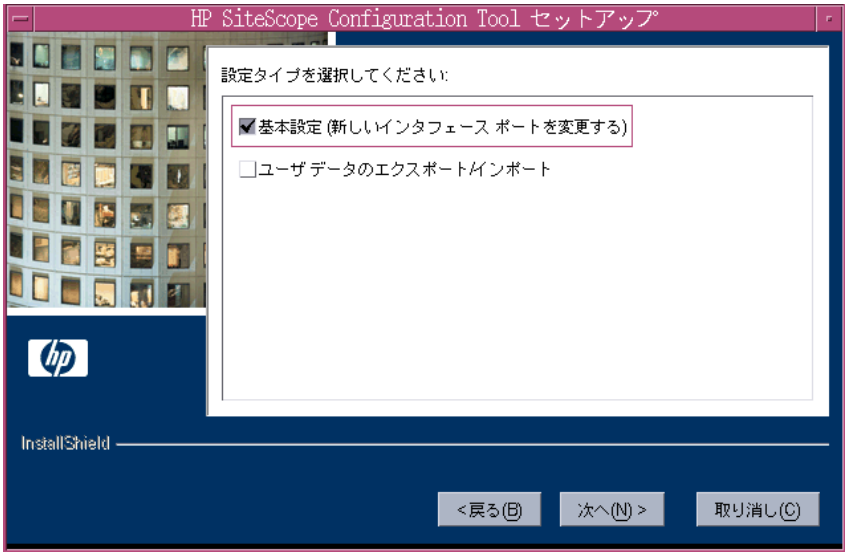
a グラフィック・モードで，
＜ SiteScope インストール・ディレクトリ＞ /bin/configTool.sh を実行します。

b コンソール・モードで，
＜ SiteScope インストール・ディレクトリ＞ /bin/configTool.sh -console を実行します。

［Configuration Tool］が開きます。

［**次へ**］をクリックします。

2 ［**基本設定**］を選択します。

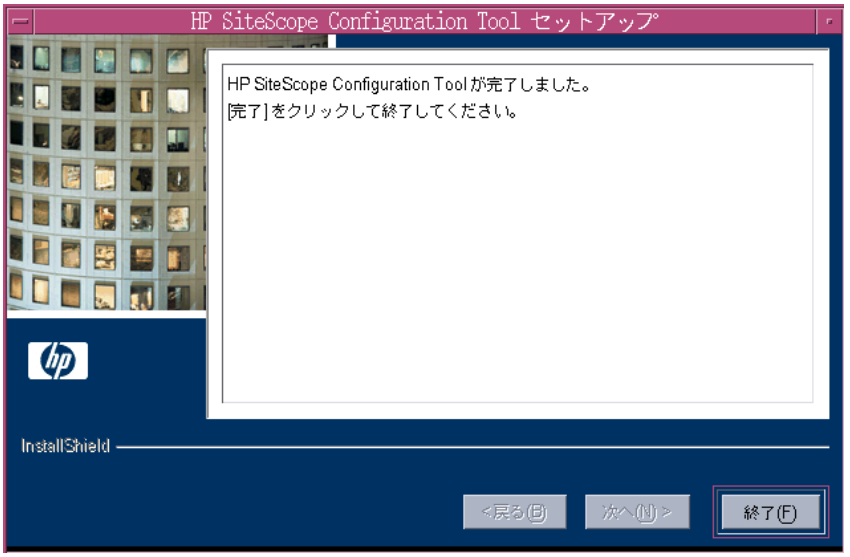


［**次へ**］をクリックします。

3 テキスト・ボックスにポート番号を入力します。

［**次へ**］をクリックします。

4 最後のダイアログ・ボックスが開き，ステータスが表示されます。



［**終了**］をクリックして変更を保存し，終了します。

ユーザ・データのエクスポート

後でインポートするためにテンプレート，ログなどの SiteScope データをエクスポートできます。

ユーザ・データをエクスポートするには，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。

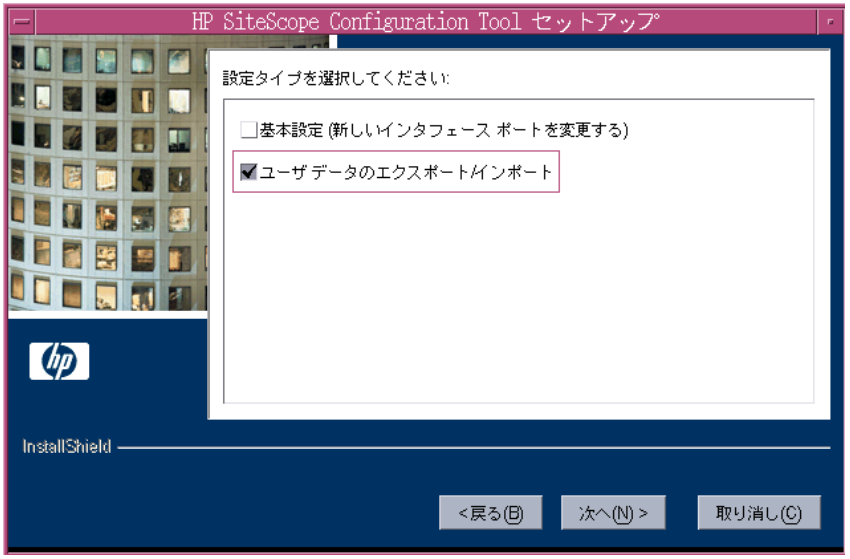
a グラフィック・モードで，
＜ SiteScope インストール・ディレクトリ＞ /bin/configTool.sh を実行します。

b コンソール・モードで，
＜ SiteScope インストール・ディレクトリ＞ /bin/configTool.sh -console を実行します。

［Configuration Tool］が開きます。

［**次へ**］をクリックします。

2 ［**ユーザ データのエクスポート / インポート**］を選択します。



［**次へ**］をクリックします。

3 ［ファイルへのデータのエクスポート］ダイアログ・ボックスが開きます。

- ［**ユーザ データ設定をエクスポート**］に，SiteScope インストール・ディレクトリまでのパスを入力します。例えば，表示されたディレクトリ・パスを受け入れたくなく，インストール・ディレクトリのパスが /opt/9_0/SiteScope である場合は，/opt/9_0/SiteScope と入力します。
- ［**ターゲット ディレクトリを入力してください（バックアップが保存される場所）**］に，エクスポートされるユーザ・データ・ファイルを保存するディレクトリを入力します。すでに存在しているディレクトリを入力します。
- ［**バックアップ ファイル名を入力してください**］に，エクスポートしたユーザ・データ・ファイルに付ける名前を入力します。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。

［**次へ**］をクリックして［**終了**］をクリックし，エクスポート操作を完了します。

ユーザ・データのインポート

テンプレート，ログなどの SiteScope データをインポートできます。

ユーザ・データをインポートするには，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。

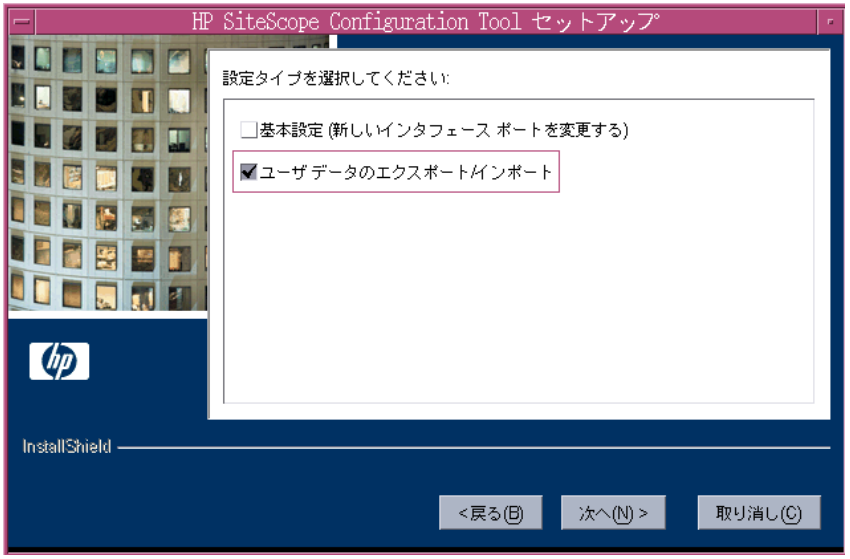
a グラフィック・モードで，
＜ SiteScope インストール・ディレクトリ＞ /bin/configTool.sh を実行します。

b コンソール・モードで，
＜ SiteScope インストール・ディレクトリ＞ /bin/configTool.sh -console を実行します。

［Configuration Tool］が開きます。

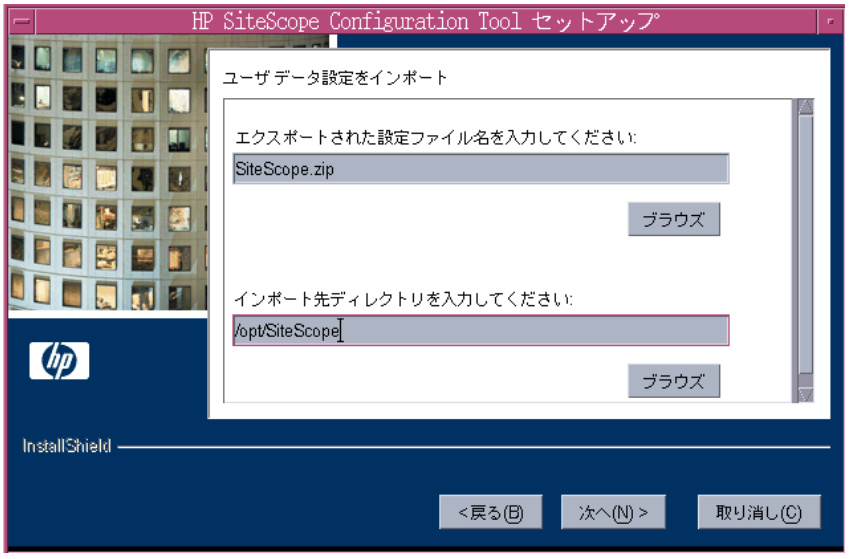
［**次へ**］をクリックします。

2 ［**ユーザ データのエクスポート / インポート**］を選択します。



［**次へ**］をクリックします。

3 ［ユーザ データ設定をインポート］ダイアログ・ボックスが開きます。



- ［**エクスポートされた設定ファイル名を入力してください**］に，インポートするユーザ・データ・ファイルの名前を入力します。
- ［**インポート先ディレクトリを入力してください**］に，ユーザ・データ・ファイルを送信するディレクトリを入力します。

［**次へ**］をクリックして［**終了**］をクリックし，インポート操作を完了します。

第 9 章

SiteScope のサイズ設定

大量のインスタンス（2,000 を超えるモニタまたは 1 分あたり 200 を超えるモニタ，あるいはその両方）で最適なパフォーマンスを得るには，SiteScope を稼動しているサーバでチューニングを行う必要があります。

本章の内容

SiteScope のサイズ設定について

SiteScope が稼動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。最適なチューニングを行うために，HP 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。Business Availability Center，BMC，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。
- 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。

Windows プラットフォーム上の 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・システムで次のチューニング手順を実行する必要があります。

1 SiteScope をサイズ設定します。

最初に SiteScope をサイズ設定し，次の手順に進む前に少なくとも 24 時間 SiteScope を実行することを強くお勧めします。詳細については，119 ページ「SiteScope のサイズ設定」の手順を参照してください。

2 Windows をサイズ設定します。

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・システムをサイズ設定し，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，119 ページ「Windows オペレーティング・システムのサイズ設定」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，122 ページ「一般的な保守の推奨事項」を参照してください。

重要：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強くお勧めします。

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［**エラーを検証する**］オプションを使用することを確認する必要があります。［エラーを検証する］オプションは，ごくわずかのモニタにのみ使用されるべきであり，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。

SiteScope にはスケジュールされたモニタのキューがあります。スケジュールされたモニタはこのキューに基づいて順番に実行されます。有効な［**エラーを検証する**］オプションが設定されているモニタでエラーが発生すると，そのモニタはキューの最後で再実行するようにはスケジューリングされません。その代わりに，このモニタは，スケジュールされているほかのすべてのモニタに取って代わって，キューの先頭に移動します。［**エラーを検証する**］オプションを使用するモニタがごくわずかの場合，これは問題になりません。モニタ数が大量の場合，この動作によりキューが混乱し，SiteScope プログラムの重大なパフォーマンス問題が発生します。

SiteScope をサイズ設定するには，次の手順を実行します。

1 各モニタの［詳細設定］を開き，［**エラーを検証する**］がチェックされているかどうか調べます。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。

2 Windows オペレーティング・システムをサイズ設定する前に，少なくとも 24 時間 SiteScope を実行します。

Windows オペレーティング・システムのサイズ設定

Windows オペレーティング・システムのサイズ設定では，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。

注：これらは推奨設定です。値の増減を行う必要がある場合は，まず HP ソフトウェア・サポートにお問い合わせください。

Windows をサイズ設定するには，次の手順を実行します。

1 設定ツール・ユーティリティを実行します。

このツールにより，JVM ヒープ・サイズとデスクトップ・ヒープ・サイズを増加します。また，SiteScope の実行可能ファイルに対する警告ポップアップを無効にします。詳細については，79 ページ「設定ツールの実行」を参照してください。

2 SiteScope が利用可能なメモリ量を増やします。

a ［レジストリ エディタ］を起動し，［**HKEY_LOCAL_MACHINE**］ウィンドウで，［**SYSTEM**］＞［**CurrentControlSet**］＞［**Services**］＞［**SiteScope**］＞［**serviceParam**］を選択します。

b 複数の CPU を搭載している場合は，値を次のように変更します（すべて単一行）。

-XX:+UseParallelGC -Xmx512m -Dsun.net.inetaddr.ttl=0 -cp C:¥SiteScope¥classes SiteScope x

この値は，パラレル・ガベージ・コレクションを利用します。

重要：

- 前述の説明に従ってメモリ量を増やすまで，パラレル・ガベージ・コレクション・オプションを設定しないことを強くお勧めします。
- パラレル・ガベージ・コレクション・オプションの設定で問題が発生した場合は，すぐに削除してください。
- 特にハイパースレッドが有効な 4-CPU サーバなど，マシンによってはこのオプションによりパフォーマンスが低下します。この問題を防ぐには，4-CPU マシンでハイパースレッドを**無効**にします。

---

3 SiteScope プログラムで利用可能なファイル・ハンドルの数を増やします。

a 適切な Windows Service Pack または Hotfix が SiteScope サーバにインストールされていることを確認します。

- Windows 2000 の場合，Service Pack 4 がインストールされている必要があります。Windows 2000 でのファイル・ハンドルの増加と Service Pack のダウンロードに関する詳細については，http://support.microsoft.com/kb/326591/ja-jp を参照してください。
- Windows XP の場合，Hotfix 327699 がインストールされている必要があります。Windows XP でのファイル・ハンドルの増加と Hotfix のダウンロードに関する詳細については，http://support.microsoft.com/kb/327699/ja-jp を参照してください。

b［**スタート**］＞［**ファイル名を指定して実行**］を選択します。［名前］テキスト・ボックスに **regedt32.exe** と入力します。［レジストリ エディタ］ダイアログ・ボックスが開きます。

c［**HKEY_LOCAL_MACHINE**］ウィンドウで，［**SOFTWARE**］＞［**Microsoft**］＞［**Windows NT**］＞［**CurrentVersion**］＞［**Windows**］を選択します。右側の表示枠に，現在の Windows のパラメータと値が表示されます。

d 右側の表示枠で，［**USERProcessHandleQuota**］をダブルクリックします。［DWORD 値の編集］ダイアログ・ボックスが開きます。

e［データ］テキスト・ボックスに 18000 と入力します。

f［基数］表示枠で［**バイナリ**］をクリックします。

g［**OK**］をクリックして設定を保存し，ダイアログ・ボックスを閉じます。

4［レジストリ エディタ］ダイアログ・ボックスで，［**レジストリ**］を選択して［**終了**］をクリックします。レジストリの変更が保存され，ダイアログ・ボックスが閉じます。

5 SiteScope サーバを再起動します。

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。

➤ **エラーを検証する機能の使用を最小限に抑える。**

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。接続の問題によるモニタの失敗では，そのモニタが終了する前，エラーの検証には［**接続タイムアウト**］に設定されている時間がかかる場合があります。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。

➤ **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 分間に稼動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。

➤ **グループのファイル・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 サーバは監視対象マシンのできるだけ近く，つまりローカル・ネットワーク上に，物理的に設置します。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。

Solaris および Linux プラットフォーム上での SiteScope のサイズ設定

Solaris および 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と，いくつかのパラメータが変更されます。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数のスレッドを設定し，Solaris または 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，123 ページ「オペレーティング・システムのチューニング」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，126 ページ「Java Virtual Machine のチューニング」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，129 ページ「一般的な保守の推奨事項」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スレッドと，Solaris または 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。

スレッドの設定

SiteScope では，通常の運用時に大量のスレッドが消費されます。たとえば，SSH リモート接続を使用して 500 のサーバを監視する 5000 の SiteScope モニタ・インスタンスを実行する場合，インスタンスあたり 3000 以上のスレッドが必要です。

スレッドの種類	必要なスレッド数
SiteScope の一般的な使用量 （例：HTTP サーバ，レポートなど）	100
モニタ・スレッド （モニタ・スレッド = _maxMonitorsRunning の値）	500
SSH スレッド （標準設定では，リモート SSH ごとに 3 スレッド）	1500
スクリプト警告スレッド （スクリプト警告スレッド = _maxMonitorsRunning * .25）	125
スクリプト・モニタ・スレッド （スクリプト・モニタ・スレッド = モニタ数 * .20）	1000
スレッドの合計数	3225

［Infrastructure Settings Preferences］の［**サーバ設定**］領域で，**_maxMonitorsRunning** パラメータを設定できます。詳細については，SiteScope ヘルプの「Infrastructure Settings Preferences」を参照してください。

Solaris または Linux オペレーティング・システム・パラメータの設定

Solaris または 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 サーバで次の手順を実行します。

Solaris または Linux オペレーティング・システム・パラメータを設定するには，次の手順を実行します。

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
```

標準設定は 1024 です（この制限はユーザの**ルート**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 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** および **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。

- コア・ファイル・サイズ（ブロック）「unlimited」
- データ・セグメント・サイズ（キロバイト）「unlimited」
- ファイル・サイズ（ブロック）「unlimited」
- 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）「unlimited」
- 最大ユーザ・プロセス数「8192」
- 仮想メモリ（キロバイト）「unlimited」

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。

3 プロセッサ・セット，動的システム・ドメイン，およびコンテナを変更します。

5 つ以上の CPU を搭載するサーバで SiteScope を実行すると，パフォーマンスに悪影響を与える可能性があります。CPU 数が増加すると，JVM でのガベージ・コレクションのオーバーヘッドも増加します。このオーバーヘッドは，Java 1.4 固有の制限事項と，SiteScope が操作のためにヒープ領域を集中的に使用することによります。

たとえば，4 CPU プロセッサ・セット上で稼動している SiteScope インスタンスの CPU 使用率は約 12% です。同じ SiteScope インスタンスが 24 の CPU 上で稼動すると，24 の CPU すべてに対して CPU 使用率が 80% となります。

使用している SiteScope サーバに 5 つ以上の CPU が搭載されている場合，4 CPU プロセッサ・セット，動的システム・ドメイン，または 4 CPU コンテナ（Solaris 10）を作成して，SiteScope アプリケーションを実行することをお勧めします。

Java Virtual Machine 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，次の手順を実行します。

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 256 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。

ヒープ領域は，＜ **SiteScope 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，1526 MB まで増やせる場合があります。

通常，768 MB あればほとんどの大量インスタンスに対応します。

2 スレッド・スタック・サイズ（-Xss）を増やします。

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，-VXss は，スレッドごとに 512 KB メモリです。

＜ **SiteScope 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（-VXmx - (threads * -Xss)）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 を超えるモニタなどインスタンスが非常に大量の場合，128 KB の -VXss を利用できます。

SiteScope バージョン 7.8.1.2 からは，-VXss は 256 KB に設定されていました。SiteScope を完全インストールではなくアップグレードした場合，スレッド・スタック・サイズは更新されない可能性があります。このパラメータが正しく定義されていることを確認してください。

3 パラレル・ガベージ・コレクションを実装します。

ガベージ・コレクションは，他のスレッドのメモリを解放するために，ヒープ・リソースの割り当てを解除する JVM プロセスです。SiteScope のインスタンスが大量な場合，JVM の標準のガベージ・コレクション・アルゴリズムでは不十分で，パラレル・ガベージ・コレクションが必要な場合があります。これにより，アプリケーション・スレッドを不安定にしたり，システムのパフォーマンスを妨げたりすることなく，コレクタ・スレッドを複数の CPU に渡って実行できます。

Java バージョン 1.4.2 以降では，SiteScope サーバにパラレル・ガベージ・コレクションを実装する方法は 2 つあります。次のいずれかの方法を使用します。

- ＜ **SiteScope ルート・ディレクトリ**＞ **¥bin¥start-monitor** スクリプトを編集し，exec ../java/bin/java で始まる行までスクロールします。その行に次のパラメータを追加します。

  -XX:+UseParallelGC

  たとえば，元の行が次のような場合，
  exec ../java/bin/java -Xmx256m -Xss256k

  次のように変更します。

  exec ../java/bin/java -Xmx256m -Xss256k -XX:+UseParallelGC

  UseParallelGC パラメータを使用する方法をお勧めします。これにより，パラレル・スカビンジング・ガベージ・コレクションが有効になります。

- ＜ **SiteScope ルート・ディレクトリ**＞ **¥bin¥start-monitor** スクリプトを編集し，exec ../java/bin/java で始まる行までスクロールします。その行に次のパラメータを 1 行で追加します。

  -XX:+UseParNewGC -XX:ParallelGCThreads-XX:+UseConcMarkSweepGC

  たとえば，元の行が次のような場合，
  exec ../java/bin/java -Xmx256m -Xss256k

  次のように変更します（1 行）。

  exec ../java/bin/java -Xmx256m -Xss256k -XX:+UseParNewGC -XX:ParallelGCThreads -XX:+UseConcMarkSweepGC

UseParNewGC により，新たなヒープ領域，つまり直近に割り当てられたリソースのある領域でパラレル・ガベージ・コレクションが有効になります。UseConcMarkSweepGC により，古いヒープ領域，つまり長期間割り当てられているリソースのある領域でパラレル・ガベージ・コレクションが有効になります。

この方法では，システム・プロセッサの数に応じて，適切なガベージ・コレクションのスレッド数も決定します。

パラレル・ガベージ・コレクションでは，SiteScope の JVM に 5 つ以上の CPU が割り当てられたインスタンスで有効にしないでください。詳細については，125 ページ「プロセッサ・セット，動的システム・ドメイン，およびコンテナを変更します。」を参照してください。

ガベージ・コレクションのログ記録は，パフォーマンス分析でも有効にできます。

➤ ＜ **SiteScope ルート・ディレクトリ**＞ **¥bin¥start-monitor** スクリプトを編集し，exec ../java/bin/java で始まる行までスクロールします。その行に次のパラメータを 1 行で追加します。

-verbose:gc -Xloggc:..¥logs¥MonitorGC.log -XX:+PrintGCTimeStamps-XX:+PrintGCDetails -XX:+PrintTenuringDistribution

たとえば，元の行が次のような場合，
exec ../java/bin/java -Xmx256m -Xss256k

次のように変更します（1 行）。

exec ../java/bin/java -Xmx256m -Xss256k -verbose:gc -Xloggc:..¥logs¥MonitorGC.log -XX:+PrintGCTimeStamps-XX:+PrintGCDetails -XX:+PrintTenuringDistribution

ガベージ・コレクションのログ記録を継続して行うことはお勧めしません。ログの解釈の詳細については，HP ソフトウェア・サポートにお問い合わせください。

一般的な保守の推奨事項

Solaris および 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。

➤ **状況モニタを利用する。**

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，［**依存の対象**］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。**

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。接続の問題によるモニタの失敗では，そのモニタが終了する前，エラーの検証には［**接続タイムアウト**］に設定されている時間がかかる場合があります。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。

SSH で，**接続キャッシュの有効化**を設定します。［**最大接続数**］を調整して，特定のサーバに対して稼動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，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 分間に稼動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。

➤ **グループのファイル・エラーを解決する。**

SiteScope バージョン 7.9.0.0 以降の状況モニタ，または以前のバージョンの SiteScope の MgAnalyzer.exe を使用して，モニタの設定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 サーバは監視対象マシンのできるだけ近く，つまりローカル・ネットワーク上に，物理的に設置します。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。

➤ **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。このサーバを監視対象サーバに物理的に近づけ，サーバの負荷の影響を最小にすることをお勧めします。

SiteScope サーバのサイズ設定に関するその他の注意事項

次に，SiteScope のデプロイメントとパフォーマンスのための，サーバのサイズ設定に関するその他の注意事項と推奨事項を示します。

- 高速な（10 KB rpm から 15 KB rpm）SCSI ディスク・ドライブを使用すると，SiteScope のシステム I/O の向上に役立ちます。
- 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。
- SiteScope のデータベース・ログ記録または HP Business Availability Center のログ記録を有効にしたときに（たとえば，SiteScope をエージェントとして，HP Business Availability Center または HP Software-as-a-Service に報告させたときに），モニタ・インスタンスの総数が 700 前後になる場合は，デュアル・プロセッサのサポートを追加します。
- Ping，Windows NT または UNIX の Telnet（サーバ監視の場合）を使用して高頻度監視（毎分 1 回を超える頻度の監視）を行う場合は，プロセッサのサポート（追加のプロセッサや高速なプロセッサなど）を追加します。これは，I/O の増加やプロセスのフォークに対応するために必要です。

第 10 章

SiteScope のアンインストール

サーバ・マシンから SiteScope をアンインストールできます。

本章の内容

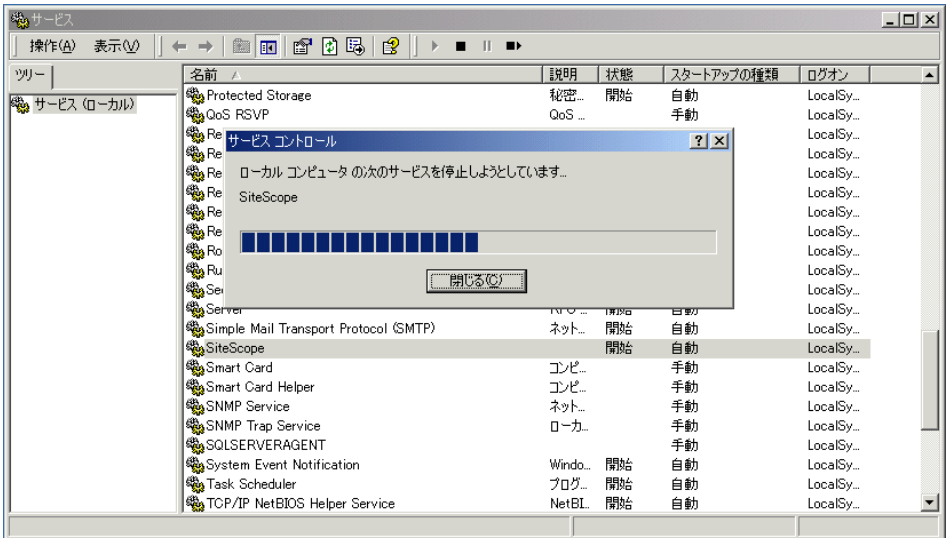
Windows プラットフォームの SiteScope のアンインストール

Windows プラットフォーム上で稼動している 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。

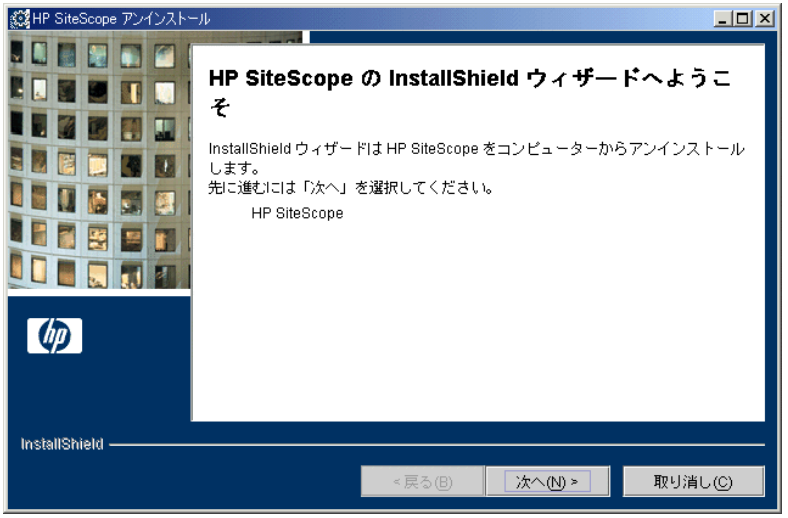
Windows プラットフォームの SiteScope をアンインストールするには，次の手順を実行します。

1 ［**スタート**］＞［**プログラム**］＞［**管理ツール**］＞［**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。

2 サービスの一覧から **SiteScope** サービスを選択します。SiteScope が稼動している場合は，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。

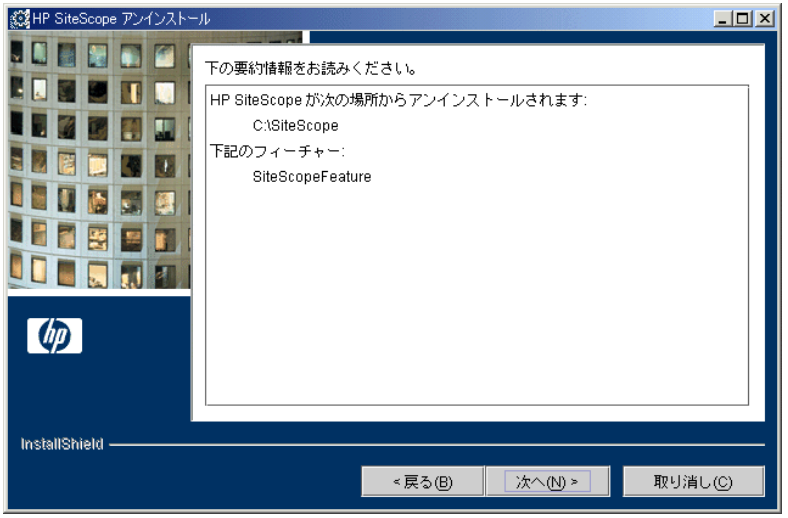


3 ［**スタート**］＞［**プログラム**］＞［**HP SiteScope**］＞［**Uninstall HP SiteScope**］を選択します。HP SiteScope の InstallShield ウィザードが開始されます。



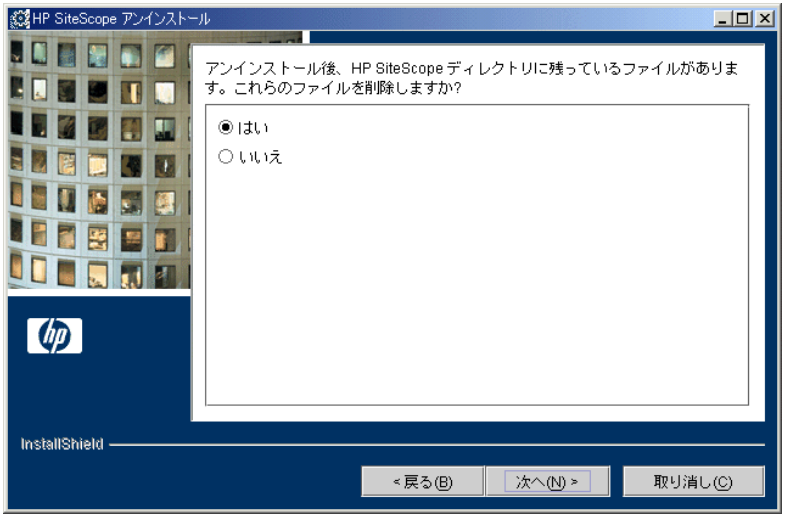
［**次へ**］をクリックし，SiteScope をアンインストールすることを確認します。

4 要約情報画面が開きます。



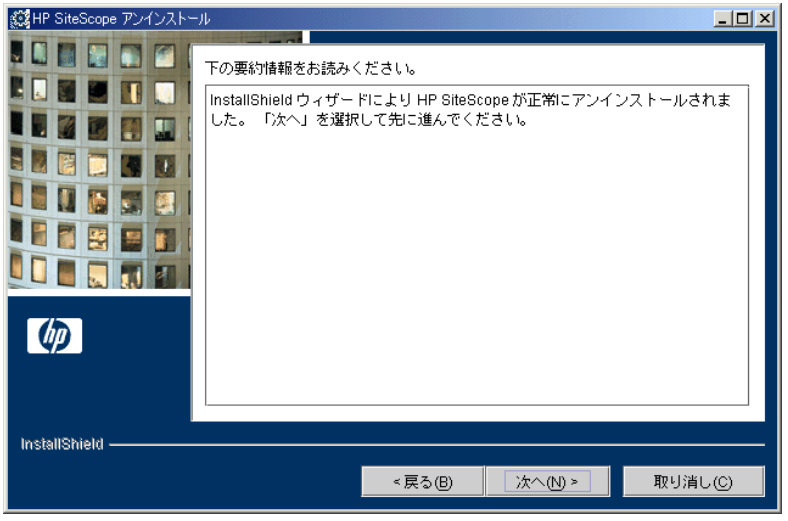
［**次へ**］をクリックして次に進みます。

5 アンインストール手順の中で，HP SiteScope ディレクトリ・ファイル（< **HP SiteScope ルート・ディレクトリ** >の下のすべてのファイルとサブディレクトリ。ルート・ディレクトリ自体は含まれません）を削除するためのオプションも提示されます。



オプションを選択し，［**次へ**］をクリックして次に進みます。

6 SiteScope が正しくアンインストールされたことを示す画面が開きます。



［**次へ**］をクリックしてアンインストール手順を完了します。

7 サーバを再起動します。サーバを再起動しないと，ほかのアプリケーションで予期しない問題が発生することがあります。

Solaris または Linux プラットフォームの SiteScope のアンインストール

Solaris または Linux プラットフォーム上で稼動している 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。

Solaris または Linux プラットフォームの SiteScope をアンインストールするには，次の手順を実行します。

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 が稼動しているマシンにログインします。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。このスクリプトを実行するコマンド・ラインの例を次に示します。

SiteScope/stop

SiteScope が停止したことを示すメッセージが表示されます。

3 ＜**インストール・パス**＞ **/SiteScope/_uninst** ディレクトリの uninstall スクリプトを実行します。このスクリプトを実行するコマンド・ラインの例を次に示します。

SiteScope/_uninst/uninstall

アンインストール手順のどの時点でも，［**戻る**］をクリックして前の画面に戻り，応答内容の確認や変更ができます。

4 HP SiteScope の InstallShield ウィザードが開始されます。［**次へ**］をクリックし，SiteScope をアンインストールすることを確認します。

5 133 ページ「Windows プラットフォームの SiteScope のアンインストール」の 4 から 7 の手順を完了します。

第 IV 部

SiteScope の安全な稼働

第 11 章

SiteScope プラットフォームのセキュリティ強化

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。

本章の内容

SiteScope プラットフォームのセキュリティ強化

ネットワークおよびシステムのセキュリティは，ますます重要になっています。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。

重要：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 へのすべてのアクセスを制限するには，SiteScope が提供する SiteScope Web サーバおよび Apache Tomcat サーバの両方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「User Preferences」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。結果として，現実的に妥当な時間内には，元のパスワードの復元はできなくなります。

IP アドレスによる SiteScope へのアクセス制限

アプリケーションへのアクセスを要求するクライアントの IP アドレスに基づいて，SiteScope へのアクセスを制限できます。これはアクセス制御リストの形になります。前述のように，SiteScope には 2 つの製品インタフェースと 2 つの Web サーバが含まれます。変更を有効にするには，両方のインタフェースに変更を適用する必要があります。

SiteScope Web サーバへのアクセスを制限するには，［General Preferences］設定を使用して，許可する IP アドレスを入力します。このアクセス制御は，ユーザ名およびパスワードも使用するように要求することでさらに強化できます。詳細については，SiteScope ヘルプの「General Preferences」を参照してください。

IP アクセス制御リストを使用して SiteScope インタフェースへのアクセスを制限するには，SiteScope に含まれる Tomcat サーバの設定ファイルを編集する必要があります。Tomcat サーバ設定ファイルの適切なセクションに Valve コンポーネントを追加して，アクセス制御リストを有効にすることができます。ドキュメントは，Apache Jakarta の Web サイト（http://jakarta.apache.org/tomcat/tomcat-5.5-doc/config/valve.html）を参照してください。

SSL（Secure Socket Layer）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 SSL を使用するように設定できます。このオプションを有効にすると，証明書を使用してユーザを認証することが必要となります。詳細については，167 ページ「SSL を使用するための SiteScope の設定」を参照してください。

第 12 章

権限と資格情報

本章では SiteScope モニタの表を示します。各モニタは，対応するプロトコル，モニタへのアクセスに必要なユーザ権限と資格情報，およびその他の注意事項とともに一覧します。

この章の目的は，SiteScope モニタを保護するために必要な権限に関する基本的な情報を提供することです。

モニタ名	プロトコル	ユーザ権限と資格情報	注意事項
Apache サーバ	HTTP/ HTTPS	サーバ統計情報ページへのアクセスに必要ない限り，必要ありません。	
ASP サーバ	Perfex	Windows 上でパフォーマンス・オブジェクトを監視するために，ユーザには特定のアクセス権限が必要です。詳細については，Microsoft サポート技術情報の記事 http://support.microsoft.com/kb/300702/ja および記事 http://support.microsoft.com/kb/164018/ja-jp を参照してください。これらの記事には，監視対象サーバ上のユーザに許可する必要がある権限とセキュリティ・ポリシーが記述されています。	**Perfmon User**：Windows サーバ上でパフォーマンス・オブジェクトを監視するために必要な権限が与えられたユーザです。 **注：**Windows サーバの **Performance Monitor Users**（Windows 2000 および Windows 2003），**Power Users**，および **Administrators** グループは，Perfmon User に必要な権限とセキュリティ・ポリシーのセットにすでに関連付けられています。言い換えると，これらのグループに属するすべてのユーザは，パフォーマンス・オブジェクトの監視に必要な権限をすべて持っており，自動的に Perfmon User となります。**Performance Monitor Users** グループには正確な権限セットがありますが，**Power Users** と **Administrators** グループには，パフォーマンスの監視に必要のない追加の権限がいくつか関連付けられています。

モニタ名	プロトコル	ユーザ権限と資格情報	注意事項
ASP サーバ（続き）	Perfex（続き）		**SiteScope ユーザ**：SiteScope サービスにログオンするユーザです。SiteScope モニタがリモート・サーバから perfmon データを収集できるようにするために，Perfmon User として定義されたユーザの資格情報を使用して，リモート・サーバへの接続を確立する必要があります。これらの接続は次のオプションを使用して確立できます。 SiteScope ユーザを，リモート・マシン上のユーザでもあるドメイン・ユーザとして設定します。 リモート・マシン上で SiteScope ユーザが Perfmon User として定義されていない場合，リモート・マシン上で Perfmon User として定義されているユーザの資格情報を使用して，SiteScope で **リモート NT** オブジェクトを設定する必要があります。その後，モニタはリモート NT オブジェクトを使用するように設定されます。
BroadVision	独自開発		

モニタ名	プロトコル	ユーザ権限と資格情報	注意事項
CheckPoint Firewall-1	SNMP	コミュニティ文字列。	このモニタは SNMP V3 をサポートしないため，コミュニティ文字列はネットワーク経由でプレーン・テキストとして渡されます。対象の SNMP エージェントは，コミュニティ文字列が MIB のサブセットの読み取りのみに使用できるように設定されます。そのような設定を行うと，未承認の人物がコミュニティ文字列を取得した場合，その人物が行えるのはエージェントの OID を読み取ることだけになります（設定はできません）。

モニタ名	プロトコル	ユーザ権限と資格情報	注意事項
Cisco Works	SNMP	SNMP のバージョンに応じて，コミュニティ文字列またはユーザ名とパスワード。	このモニタに対する最も安全な設定は，認証（SHA または MD5）と DES の非公開暗号を使う，SNMP V3 の使用が設定されているエージェントに対して実行することです。この設定では，暗号化されていない SNMP データはネットワーク経由では渡されません。これにより，悪意のあるユーザが監視対象のデバイスを危険にさらす可能性を大きく低減します。監視対象デバイスの SNMP エージェントの実装バグによるセキュリティ上の脆弱性は考慮されていません。 このモニタに対する最も危険な設定は，監視対象デバイスのエージェントによって実装された MIB 全体に対する読み取りおよび書き込みの両方のアクセス権を持つコミュニティ文字列を使う SNMP V1 を使用することです。この設定では，悪意のあるユーザがネットワーク上で盗聴することによってコミュニティ文字列を取得し，それを使用してデバイスを再設定することができます。
Citrix サーバ	PDH	ASP サーバ・モニタと同じ。	
ColdFusion	Perfex	ASP サーバ・モニタと同じ。	
COM+	HTTP/ HTTPS		

モニタ名	プロトコル	ユーザ権限と資格情報	注意事項
CPU（Windows）	Perfex	ASP サーバ・モニタと同じ。	SiteScope が動作するサーバを Active Directory の Domain Admin グループに追加します（Windows 2000 以降の場合）。このオプションでは，SiteScope サービスは，ローカル・システム・アカウントとしてログインするように設定されますが，SiteScope が実行されているマシンは，ドメイン管理権限のあるグループに追加されます。 非管理者アクセスを許可するように，ドメイン内のすべてのマシンのレジストリ・アクセス権を編集します。非管理者ユーザが perfmon を使用してリモートでマシンを監視できるようにする方法については，Microsoft サポート技術情報の記事 http://support.microsoft.com/kb/164018/ja-jp を参照してください。このオプションを使用するには，監視する各リモート・マシンでレジストリを変更する必要があります。したがって，ドメインのサーバ・リストにドメインのすべてのマシンが含まれていても，接続プロファイルなしで監視できるのは，レジストリが変更されたリモート・マシンのみです。

モニタ名	プロトコル	ユーザ権限と資格情報	注意事項
CPU（Solaris/ Linux）	UNIX/ Linux Shell	リモート・サーバにはシェル・アクセスが必要です。サポートされているアクセス・プロトコルは，telnet, SSH，および rlogin です。また，ログイン・ユーザには，さまざまな実行ファイル・プログラムを実行する権限も必要です。	SiteScope が実行するさまざまなコマンドに UNIX グループ権限を使用することにより，ログイン・ユーザのアクセスを制限できます。個々のオペレーティング・システムに関連するコマンドの一覧は，**templates.os** ファイルにあります。
データベース	JDBC	特定のデータベースへのアクセスを認証するためにユーザの資格情報が必要です。各データベースには，アクセスが必要な個々のテーブルへのアクセス制御を提供するための特定の方法があります。	ユーザには，指定されたあらゆる SQL ステートメントを実行できる権限が必要です。
DB2	独自開発	管理者権限を持つユーザとパスワード。	
ディレクトリ	Shell	リモート・サーバにはシェル・アクセスが必要です。サポートされているアクセス・プロトコルは，telnet, SSH，および rlogin です。また，ログイン・ユーザには，さまざまな実行ファイル・プログラムを実行する権限も必要です。	SiteScope が実行するさまざまなコマンドに UNIX グループ権限を使用することにより，ログイン・ユーザのアクセスを制限できます。個々のオペレーティング・システムに関連するコマンドの一覧は，**templates.os** ファイルにあります。
ディレクトリ（Windows）	Netbios	読み取り専用ファイル・システム・アクセス。	特定のファイルに対する権限は，オペレーティング・システム・レベルで制御できます。
ディレクトリ（Solaris/ Linux）	ファイル・システム・アクセス	個々のファイルに対する読み取り専用ファイル・システム・アクセス。	特定のファイルに対する権限は，オペレーティング・システム・レベルで制御できます。

モニタ名	プロトコル	ユーザ権限と資格情報	注意事項
ディスク領域（Windows）	Perfex	ASP サーバ・モニタと同じ。	Windows 2000 の場合，ディスク・カウンタは perfex で有効になっている必要があります。
ディスク領域（Solaris/ Linux）	Shell	リモート・サーバにはシェル・アクセスが必要です。サポートされているアクセス・プロトコルは，telnet, SSH，および rlogin です。また，ログイン・ユーザには，さまざまな実行可能プログラムを実行する権限も必要です。	SiteScope が実行するさまざまなコマンドに UNIX グループ権限を使用することにより，ログイン・ユーザのアクセスを制限できます。個々のオペレーティング・システムに関連するコマンドの一覧は，**templates.os** ファイルにあります。
Dynamo	SNMP	コミュニティ文字列。	このモニタは SNMP V3 をサポートしないため，コミュニティ文字列はネットワーク経由でプレーン・テキストとして渡されます。対象の SNMP エージェントは，コミュニティ文字列が MIB のサブセットの読み取りのみに使用できるように設定されます。そのような設定を行うと，未承認の人物がコミュニティ文字列を取得した場合，その人物が行えるのはエージェントの OID を読み取ることだけになります（設定はできません）。

モニタ名	プロトコル	ユーザ権限と資格情報	注意事項
F5 Big-IP	SNMP	SNMP のバージョンに応じて，コミュニティ文字列またはユーザ名とパスワード。	このモニタに対する最も安全な設定は，認証（SHA または MD5）と DES の非公開暗号を使う，SNMP V3 の使用が設定されているエージェントに対して実行することです。この設定では，暗号化されていない SNMP データはネットワーク経由では渡されません。これにより，悪意のあるユーザが監視対象のデバイスを危険にさらす可能性を大きく低減します。監視対象デバイスの SNMP エージェントの実装バグによるセキュリティ上の脆弱性は考慮されていません。 このモニタに対する最も危険な設定は，監視対象デバイスのエージェントによって実装された MIB 全体に対する読み取りおよび書き込みの両方のアクセス権を持つコミュニティ文字列を使う SNMP V1 を使用することです。この設定では，悪意のあるユーザがネットワーク上で盗聴することによってコミュニティ文字列を取得し，それを使用してデバイスを再設定することができます。
ファイル（Windows）	Netbios	ログ・ファイルへの読み取り専用アクセスのための Windows 権限。	
ファイル（Solaris/ Linux）	ファイル・システム・アクセス	対象のファイル・システムに対するファイルの読み取り専用権限。	

モニタ名	プロトコル	ユーザ権限と資格情報	注意事項
FTP	FTP	ユーザ固有のファイルをコピーするための読み取り専用権限を持つ，FTP サイト用の有効なユーザ名とパスワード。カスタマー・サイトは匿名ログインを許可します。	
IIS	Perfex	ASP サーバ・モニタと同じ。	
iPlanet アプリケーション・サーバ	SNMP	SNMP のバージョンに応じて，コミュニティ文字列またはユーザ名とパスワード。	このモニタに対する最も安全な設定は，認証（SHA または MD5）と DES の非公開暗号を使う，SNMP V3 の使用が設定されているエージェントに対して実行することです。この設定では，暗号化されていない SNMP データはネットワーク経由では渡されません。これにより，悪意のあるユーザが監視対象のデバイスを危険にさらす可能性を大きく低減します。監視対象デバイスの SNMP エージェントの実装バグによるセキュリティ上の脆弱性は考慮されていません。 このモニタに対する最も危険な設定は，監視対象デバイスのエージェントによって実装された MIB 全体に対する読み取りおよび書き込みの両方のアクセス権を持つコミュニティ文字列を使う SNMP V1 を使用することです。この設定では，悪意のあるユーザがネットワーク上で盗聴することによってコミュニティ文字列を取得し，それを使用してデバイスを再設定することができます。

モニタ名	プロトコル	ユーザ権限と資格情報	注意事項
iPlanet Web サーバ	SNMP	SNMP のバージョンに応じて，コミュニティ文字列またはユーザ名とパスワード。	このモニタに対する最も安全な設定は，認証（SHA または MD5）と DES の非公開暗号を使う，SNMP V3 の使用が設定されているエージェントに対して実行することです。この設定では，暗号化されていない SNMP データはネットワーク経由では渡されません。これにより，悪意のあるユーザが監視対象のデバイスを危険にさらす可能性を大きく低減します。監視対象デバイスの SNMP エージェントの実装バグによるセキュリティ上の脆弱性は考慮されていません。 このモニタに対する最も危険な設定は，監視対象デバイスのエージェントによって実装された MIB 全体に対する読み取りおよび書き込みの両方のアクセス権を持つコミュニティ文字列を使う SNMP V1 を使用することです。この設定では，悪意のあるユーザがネットワーク上で盗聴することによってコミュニティ文字列を取得し，それを使用してデバイスを再設定することができます。
LDAP	LDAP	単純な認証を行う LDAP サーバでの有効なユーザ名とパスワード。クエリまたは検索操作には適切な権限が必要です。バージョン 7.9 では，匿名認証もサポートされています。	

モニタ名	プロトコル	ユーザ権限と資格情報	注意事項
リンク・チェック	HTTP/HTTPS	HTTP/HTTPS サイトでユーザ名とパスワードが必要ない限り，必要ありません。	ユーザにはリンクをクリックできる権限が必要です。
ログ・ファイル（Windows）	Netbios	ログ・ファイルへの読み取り専用アクセスのための Windows 権限。	
ログ・ファイル（Solaris/Linux）	Shell	リモート・サーバにはシェル・アクセスが必要です。サポートされているアクセス・プロトコルは，telnet，SSH，および rlogin です。また，ログイン・ユーザには，さまざまな実行ファイル・プログラムを実行する権限も必要です。対象のファイル・システムに対するファイルの読み取り専用権限。	SiteScope が実行するさまざまなコマンドに UNIX グループ権限を使用することにより，ログイン・ユーザのアクセスを制限できます。個々のオペレーティング・システムに関連するコマンドの一覧は，**templates.os** ファイルにあります。
メール	SMTP	有効な電子メール・アカウントとパスワード。	
MAPI	MAPI	テスト電子メールを送受信するための 1 つまたは 2 つの電子メール・アカウントのユーザ名とパスワード。	SiteScope は SiteScope サーバ上で Local Administrator として実行する必要があります。テスト電子メールアカウントには，SiteScope サーバでの Local Administrator 権限が必要です。
メモリ（Windows）	Perfex	ASP サーバ・モニタと同じ。	

モニタ名	プロトコル	ユーザ権限と資格情報	注意事項
メモリ（Solaris/ Linux）	Shell	リモート・サーバにはシェル・アクセスが必要です。サポートされているアクセス・プロトコルは，telnet, SSH，および rlogin です。また，ログイン・ユーザには，さまざまな実行ファイル・プログラムを実行する権限も必要です。	SiteScope が実行するさまざまなコマンドに UNIX グループ権限を使用することにより，ログイン・ユーザのアクセスを制限できます。個々のオペレーティング・システムに関連するコマンドの一覧は，**templates.os** ファイルにあります。
Microsoft Windows イベント・ログ	Perfex	ASP サーバ・モニタと同じ。	
Microsoft Windows Performance Counter	Perfex	ASP サーバ・モニタと同じ。	
Microsoft SQL サーバ	Perfex	ASP サーバ・モニタと同じ。	
Microsoft Windows Dialup	MODEM	接続されている ISP アカウントに対するユーザ名とパスワード。アカウントには，指定されたテスト・モニタを実行できる権限が必要です。	
Microsoft Windows Media Player	ファイル・システム・アクセス	対象のファイル・システムに対するファイルの読み取り専用権限。	
Microsoft Windows Media Server	Perfex	ASP サーバ・モニタと同じ。	
Microsoft Windows リソース	PDH	ASP サーバ・モニタと同じ。	
ネットワーク	Perfex	ASP サーバ・モニタと同じ。	

モニタ名	プロトコル	ユーザ権限と資格情報	注意事項
ネットワーク帯域幅	SNMP	SNMP のバージョンに応じて，コミュニティ文字列またはユーザ名とパスワード。	このモニタに対する最も安全な設定は，認証（SHA または MD5）と DES の非公開暗号を使う，SNMP V3 の使用が設定されているエージェントに対して実行することです。この設定では，暗号化されていない SNMP データはネットワーク経由では渡されません。これにより，悪意のあるユーザが監視対象のデバイスを危険にさらす可能性を大きく低減します。監視対象デバイスの SNMP エージェントの実装バグによるセキュリティ上の脆弱性は考慮されていません。 このモニタに対する最も危険な設定は，監視対象デバイスのエージェントによって実装された MIB 全体に対する読み取りおよび書き込みの両方のアクセス権を持つコミュニティ文字列を使う SNMP V1 を使用することです。この設定では，悪意のあるユーザがネットワーク上で盗聴することによってコミュニティ文字列を取得し，それを使用してデバイスを再設定することができます。
ニュース	NNTP	ニュース・サーバに必要な場合，ニュース・グループ内のメッセージの総数をクエリする読み取り専用の権限を持つ，有効なユーザ名とパスワード。	
Oracle 9iAS	HTTP/ HTTPS		

モニタ名	プロトコル	ユーザ権限と資格情報	注意事項
Oracle データベース	JDBC	Oracle ユーザは，＜ **SiteScope ルート・ディレクトリ＞¥ templates.applications¥ commands.oraclejdbc** にあるすべての SQL ステートメントを実行できる権限を持ってログインします。	
Ping	ICMP	N/A	
ポート	TCP	N/A	
Radius	Radius	Radius サーバでの有効なユーザ名とパスワード。ほかの権限は必要ありません。	SiteScope の IP を Radius サーバと通信可能なサーバのリストに追加する必要があります。また，PAP 認証を行うように設定する必要があります。
Real Media Player	ファイル・システム・アクセス	対象のファイル・システムでのファイルの読み取り専用権限。	
Real Media Server	Perfex	ASP サーバ・モニタと同じ。	
RTSP	ファイル・システム・アクセス	対象のファイル・システムでのファイルの読み取り専用権限。	
SAP CCMS	独自開発	XMI 認証。	XMI 認証を持つプロファイルは，S_A.SYSTEM, PD_CHICAGO, S_WF_RWTEST，および SAP_ALL です。
SAP CCMS Alert			
SAP パフォーマンスまたは Work Processes	SAPGUI	現在調査中です。	

モニタ名	プロトコル	ユーザ権限と資格情報	注意事項
SAP Portal	HTTP/ HTTPS	http:// ＜ユーザの Portal サーバ＞ /sapportal にログインして［Portal Monitoring］ページにアクセスする権限が必要です。	
スクリプト（Windows）	Remote Shell	ASP サーバ・モニタと同じ。	
スクリプト（Solaris/ Linux）	Shell	リモート・サーバにはシェル・アクセスが必要です。サポートされているアクセス・プロトコルは，telnet, SSH，および rlogin です。また，ログイン・ユーザには，さまざまな実行ファイル・プログラムを実行する権限も必要です。	SiteScope が実行するさまざまなコマンドに UNIX グループ権限を使用することにより，ログイン・ユーザのアクセスを制限できます。個々のオペレーティング・システムに関連するコマンドの一覧は，**templates.os** ファイルにあります。
ローカル・マシン上のスクリプト（Solaris, Linux，および Windows）	ファイル・システム・アクセス	対象のファイル・システムに対するファイルの読み取り専用権限。	
サービス（Windows）	Perfex	ASP サーバ・モニタと同じ。	
サービス（Solaris/ Linux）	Shell	リモート・サーバにはシェル・アクセスが必要です。サポートされているアクセス・プロトコルは，telnet, SSH，および rlogin です。また，ログイン・ユーザには，さまざまな実行ファイル・プログラムを実行する権限も必要です。	SiteScope が実行するさまざまなコマンドに UNIX グループ権限を使用することにより，ログイン・ユーザのアクセスを制限できます。個々のオペレーティング・システムに関連するコマンドの一覧は，**templates.os** ファイルにあります。
Siebel ログ	ファイル・システム・アクセス	対象の Siebel サーバ・ファイル・システムに対するファイルの読み取り専用権限。	

モニタ名	プロトコル	ユーザ権限と資格情報	注意事項
Siebel サーバ・マネージャ	CmdLine	ユーザ・アカウントには，Siebel サーバ・マネージャ（srvrmgr）・コマンドを発行する Siebel 管理者権限が必要です。	srvrmgr クライアントがリモートの場合，リモート srvrmgr コマンドを実行するための適切なユーザ名およびパスワードの資格情報を使用して，リモート Windows またはリモート UNIX をセットアップする必要があります。
Siebel Web サーバ	HTTP/ HTTPS	対象の Siebel Extensions ページがサードパーティー製の HTML フォーム・ベースの認証ソフトウェアの背後にある場合，ユーザ名とパスワードが必要です。	ユーザには，Siebel SWE ページを取得する権限が必要です。
SilverStream	HTTP/ HTTPS	サーバ管理 Web ページ http://servername:port/SilverStream/Statistics を取得する権限を持つユーザ名とパスワード。	

モニタ名	プロトコル	ユーザ権限と資格情報	注意事項
SNMP	SNMP	SNMP のバージョンに応じて，コミュニティ文字列またはユーザ名とパスワード。	このモニタに対する最も安全な設定は，認証（SHA または MD5）と DES の非公開暗号を使う，SNMP V3 の使用が設定されているエージェントに対して実行することです。この設定では，暗号化されていない SNMP データはネットワーク経由では渡されません。これにより，悪意のあるユーザが監視対象のデバイスを危険にさらす可能性を大きく低減します。監視対象デバイスの SNMP エージェントの実装バグによるセキュリティ上の脆弱性は考慮されていません。 このモニタに対する最も危険な設定は，監視対象デバイスのエージェントによって実装された MIB 全体に対する読み取りおよび書き込みの両方のアクセス権を持つコミュニティ文字列を使う SNMP V1 を使用することです。この設定では，悪意のあるユーザがネットワーク上で盗聴することによってコミュニティ文字列を取得し，それを使用してデバイスを再設定することができます。

モニタ名	プロトコル	ユーザ権限と資格情報	注意事項
MIB による SNMP	SNMP	SNMP のバージョンに応じて，コミュニティ文字列またはユーザ名とパスワード。	このモニタに対する最も安全な設定は，認証（SHA または MD5）と DES の非公開暗号を使う，SNMP V3 の使用が設定されているエージェントに対して実行することです。この設定では，暗号化されていない SNMP データはネットワーク経由では渡されません。これにより，悪意のあるユーザが監視対象のデバイスを危険にさらす可能性を大きく低減します。監視対象デバイスの SNMP エージェントの実装バグによるセキュリティ上の脆弱性は考慮されていません。 このモニタに対する最も危険な設定は，監視対象デバイスのエージェントによって実装された MIB 全体に対する読み取りおよび書き込みの両方のアクセス権を持つコミュニティ文字列を使う SNMP V1 を使用することです。この設定では，悪意のあるユーザがネットワーク上で盗聴することによってコミュニティ文字列を取得し，それを使用してデバイスを再設定することができます。

モニタ名	プロトコル	ユーザ権限と資格情報	注意事項
SNMP トラップ	SNMP	不要ですが，SiteScope にトラップを送信するためにネットワーク上でエージェントを設定する権限は必要です。予約済みのポートであるポート 162 にバインドできるように，SiteScope は権限を持つユーザとして実行する必要があります。	SNMP V1 および V2 トラップに関するセキュリティ・リスクとして，悪意のあるユーザがトラップで渡されたデータを盗聴する可能性があります。 認証と非公開暗号を使用する V3 トラップを使用することにより，盗聴者によってデータが悪用される可能性が大幅に削減されます。
SunOne	HTTP/ HTTPS	認証を必要とするプロキシを使用しない限り，不要。	
Tuxedo	独自開発	PeopleSoft Tuxedo には，あらかじめ設定されている 2 つのユーザ，**PS** および **VP** が含まれています。これらは監視専用アカウントです。SiteScope の監視では，ほかのユーザの作成や使用を行うことはできません。	
URL	HTTP/ HTTPS	SiteScope には何も必要ありません。サーバには有効なユーザ名とパスワードが必要です。	
URL 内容	HTTP/ HTTPS	SiteScope には何も必要ありません。サーバには有効なユーザ名とパスワードが必要です。	
URL リスト	HTTP/ HTTPS	SiteScope には何も必要ありません。サーバには有効なユーザ名とパスワードが必要です。	
URL シーケンス	HTTP/ HTTPS	SiteScope には何も必要ありません。サーバには有効なユーザ名とパスワードが必要です。	

モニタ名	プロトコル	ユーザ権限と資格情報	注意事項
Web サーバ	Perfex	ASP サーバ・モニタと同じ。	
Web サーバ（Solaris, Linux，および Windows）	ファイル・システム・アクセス	対象のファイル・システムに対するファイルの読み取り専用権限。	
Web サービス	HTTP/ HTTPS	対象の Web サービスが必要とする場合，基本認証，ダイジェスト認証，および NTLM 認証をサポートします。	
WebLogic 5.x	SNMP	コミュニティ文字列の資格情報が SNMP エージェントの文字列と一致する必要があります。	
WebLogic 6.x 以降	RMI	少なくともモニタ・ロールの権限を持つグループに属するユーザが必要です。	
WebSphere パフォーマンス・サーブレット	HTTP/ HTTPS	サーブレットの URL のユーザ名およびパスワードによる HTTP 認証。ユーザは資格情報をカスタマイズできます。	
WebSphere 3.5x	RMI		
WebSphere 4.5	RMI	少なくともモニタ・ロールの権限を持つグループに属するユーザが必要です。	

モニタ名	プロトコル	ユーザ権限と資格情報	注意事項
WebSphere 5.x（HTTP 経由の SOAP）	HTTP/ HTTPS	少なくともモニタ・ロールの権限を持つグループに属するユーザが必要です。	
WebSphere MQ	独自開発	SiteScope アカウントは，MQ Windows サーバ内の mqm グループのメンバーである必要があります。 MQ UNIX では，使用されるサーバ接続チャネルは SSL 認証を要求できません。	

第 13 章

SSL を使用するための SiteScope の設定

SiteScope は，SiteScope インタフェースへのアクセスを制限するために SSL（Secure Sockets Layer）を使用するように設定できます。

本章の内容

SiteScope での SSL の使用について

SiteScope サーバで SSL をサポートするには，SiteScope インタフェースを提供する Web サーバを SSL に対応するように設定します。このためには，デジタル証明書をキー・ストア・ファイルにインポートし，SiteScope が HTTPS 要求にのみ応答するようにサーバの設定を変更します。

重要：SiteScope へのすべてのアクセスを HTTPS クライアント接続に制限するには，本項の手順に従って，SiteScope が提供する SiteScope Web サーバおよび Tomcat サーバの両方で SSL を使用するように設定する必要があります。

SSL を使用するための 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。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。

重要：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。

Keytool の詳細については，
http://java.sun.com/j2se/1.3/docs/tooldocs/win32/keytool.html を参照してください。

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，次の手順を使用します。

認証局に対する証明書要求ファイルを作成するには，次の手順を実行します。

1 ＜ **SiteScope のルート・ディレクトリ**＞ **¥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 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・ラインを実行して鍵ペアを作成します。

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。

---

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 のルート・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）
  S = 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エイリアスまたはニックネームです。

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。証明書を SiteScope で使用するためにインポートするには，次の手順を使用します。

認証局からの証明書をインポートするには，次の手順を実行します。

1 ＜ **SiteScope のルート・ディレクトリ**＞ **¥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

2 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，171 ページ「SSL 用の SiteScope の設定」を参照してください。

自己署名証明書の使用

SiteScope で使用するための自己署名証明書を生成することもできます。このためには，次の手順に従って，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，次の手順を実行します。

1 ＜ **SiteScope のルート・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 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ます。変数には，自分の組織に固有な情報を指定します。

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。

---

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 ＜ **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 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，171 ページ「SSL 用の SiteScope の設定」を参照してください。

SSL 用の SiteScope の設定

Tomcat で SSL 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"
maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
enableLookups="false" disableUploadTimeout="true"
acceptCount="100" debug="0" scheme="https" secure="true"
clientAuth="false" sslProtocol="TLS" />
-->
```

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" sslProtocol="TLS"
keystoreFile=" ＜ SiteScope インストール・パス＞ ¥SiteScope¥groups¥serverKeystore"
keystorePass="testing"
/>
```

＜ SiteScope **インストール・パス**＞ は，SiteScope のインストール先のパスです。

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 SSL 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。

この例を使用して Tomcat で SSL 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

第 V 部

作業の開始と SiteScope へのアクセス

第 14 章

インストール後の管理

この項では，SiteScope のインストール後に実行すべき推奨手順を説明します。

本章の内容

インストール後の管理チェックリスト

このチェックリストを使用して，SiteScope のインストール後に実行すべき管理作業を確認してください。

✔	ステップ
	SiteScope サポートの登録。詳細については，17 ページ「スタートアップ・ロードマップ」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インします。詳細については，183 ページ「SiteScope への接続」を参照してください。
	SiteScope の以前のバージョンから SiteScope 9.50 に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 から新しい SiteScope に転送します。設定ツールの使い方については，77 ページ「設定ツールの実行」（Windows）または 107 ページ「設定ツールの実行」（Solaris または Linux）を参照してください。
	SiteScope ライセンス情報をインストール中に入力しなかった場合は，[General Preferences（一般のプリファレンス）] ページに入力してください。詳細については，SiteScope ヘルプの「General Preferences」を参照してください。新しい SiteScope は 評価ライセンスで 10 日間操作できます。ライセンスの詳細については，33 ページ「SiteScope のライセンス」を参照してください。

✔	ステップ
	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「User Preferences」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 ヘルプの「E-mail Preferences」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「Microsoft Windows Remote Preferences」および「UNIX Remote Preferences」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「Log Preferences」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。
	HP Business Availability Center に報告するよう SiteScope を設定します。詳細については，SiteScope ヘルプの「Integration Preferences」を参照してください。
	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 Templates」を参照してください。

✔	ステップ
	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「Manage a Group – Workflow」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 15 章

SiteScope を使った作業の開始

本章では，SiteScope サービスの開始方法と停止方法，および最初に SiteScope にログインする方法について説明します。

本章の内容

SiteScope サービスの開始

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。

➤ Solaris および 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。

本項で説明するステップを使用して，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，次の手順を実行します。

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，次の手順を実行します。

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，次の手順を実行します。

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
```

Solaris および Linux プラットフォームでの SiteScope サービスの開始と停止

製品に付属するシェル・スクリプトを使用して，SiteScope 開始と停止を手動で行うことができます。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。

Solaris および Linux 上で SiteScope のプロセスを開始するには，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。

＜インストール・パス＞ /SiteScope/start

Solaris および Linux 上で SiteScope のプロセスを停止するには，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。

＜インストール・パス＞ /SiteScope/stop

前述のコマンドの**＜インストール・パス＞**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 の stop 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。SiteScope は，**Open_SiteScope.htm** ファイルのポート番号情報を更新します。このファイルは，SiteScope のインストール・ディレクトリにある HTML ページです。

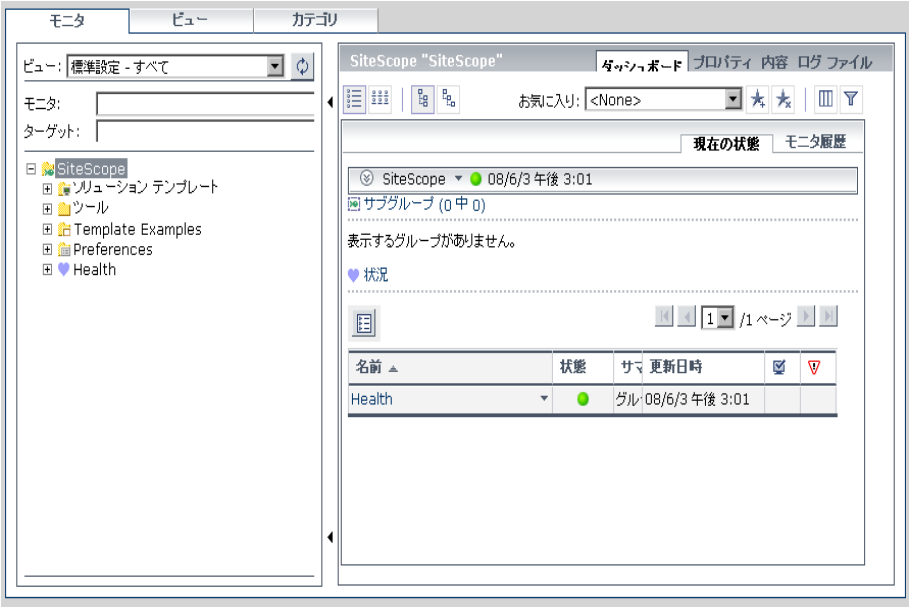
Windows プラットフォームでは，インストール・プロセスによって，［**スタート**］＞［**プログラム**］の SiteScope 用のメニューに，このファイルへのリンクが追加されます。［スタート］メニュー・フォルダはインストール時に選択します。

SiteScope へのアクセス

SiteScope にアクセスするには，Web ブラウザで SiteScope のアドレスを入力します。標準設定のアドレスは 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**］＞［**プログラム**］＞［**HP SiteScope**］＞［**Open HP SiteScope**］をクリックします。

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。次に示すように，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ログイン・ダイアログ・ボックスが表示されるようになります。管理者アカウント・プロファイルの編集方法の詳細については，SiteScope ヘルプの「User Preferences」を参照してください。

第 VI 部

付録

付録 A

IIS の SiteScope の Tomcat サーバとの統合

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。

本章の内容

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，次の手順を実行します。

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。以下にこのファイルの例を示します。

```
# 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 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 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。以下に SiteScope ワーカ・ファイルの例を示します。

```
# 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：IIS と Tomcat が同じマシン上にない場合は，**workers.properties.minimal** のホスト属性を他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。次に，前述の設定例と同じように，**uriworkermap.properties** という名前の SiteScope ワーカのマウント・ファイルの例を示します。

```
# 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
```

注：次の新しい構文は，SiteScope の 2 つのルールを 1 つに結合します。
/SiteScope/*=ajp13w

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。

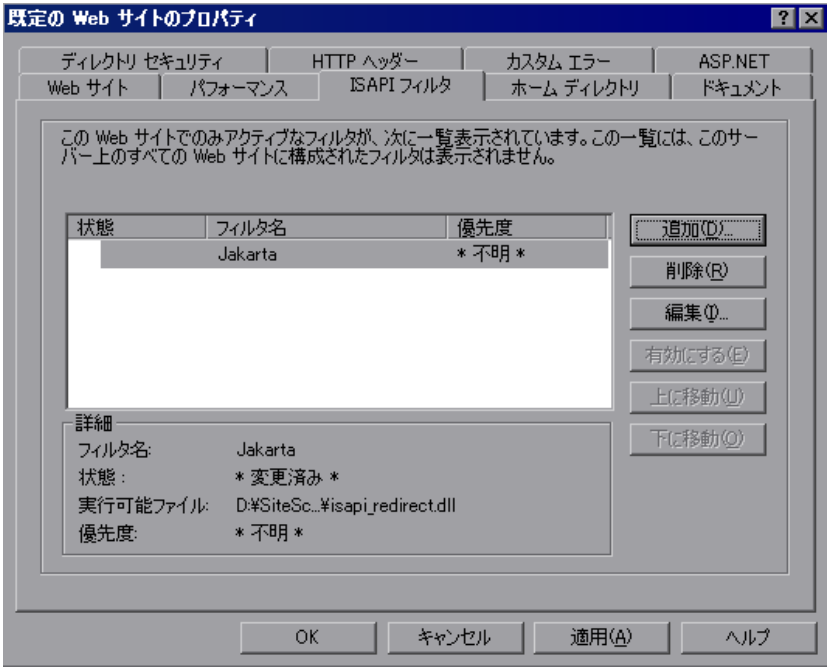
IIS を設定するには，次の手順を実行します。

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。

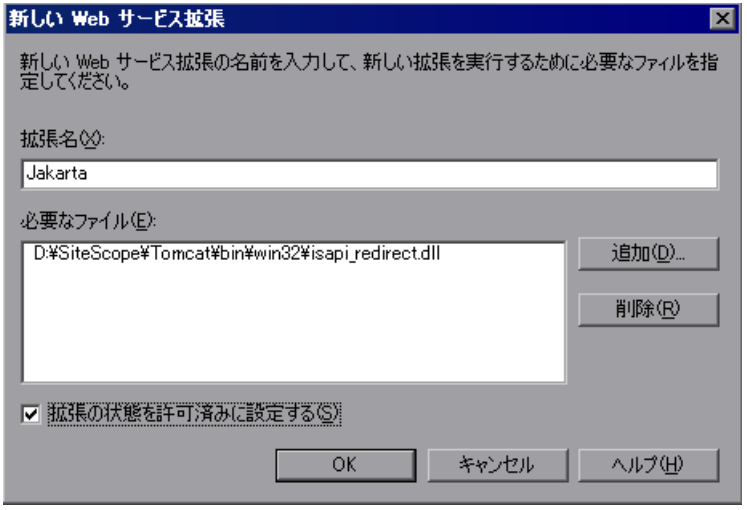
4［**ISAPI フィルタ**］タブをクリックしてから，［**追加**］をクリックします。［**フィルタ名**］カラムで，「**Jakarta**」を選択し，**isapi_redirect.dll** を参照します。フィルタが追加されますが，この段階ではまだアクティブではありません。



［**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 SiteSeer との統合

SiteScope は，SiteSeer ホスティング型サービスのアカウントと統合できます。こうすることにより，ファイアウォールの内部および外部から単一のインタフェースでシステムの可用性データを表示できます。

注：SiteScope 8.0 以降では，SiteScope への SiteSeer の統合は，SiteScope クラシック・インタフェースでのみ利用できます。この機能は，新しい SiteScope 9.50 インタフェースではサポートされていません。

本章の内容

SiteSeer との統合について

SiteSeer は，ファイアウォールの外部からシステムの可用性を監視するためのリモート・サービスです。SiteSeer は SiteScope テクノロジに基づいて構築されています。このため，SiteSeer によって収集されたデータは，SiteScope データと直接の互換性があります。

SiteSeer リモート監視アカウントからの監視情報は，SiteScope のメイン・パネルにグループとして表示されます。SiteSeer グループ名をクリックすると，SiteSeer アカウント画面が開きます。SiteScope パネルに戻るには，ブラウザの［**戻る**］ボタンをクリックします。

注：1 つの SiteScope に，1 つの SiteSeer アカウントしか追加できません。

SiteSeer 接続情報およびログイン情報を指定し，SiteSeer サービスとの接続をテストするには，［SiteSeer Preferences］フォームを使用します。これを行うには，現在の SiteSeer アカウントが必要です。また，SiteSeer と統合する SiteScope サーバには，アカウントが実行されている SiteSeer ホスティング型サービス・サーバとの HTTP または HTTPS アクセスが必要です。

注：［SiteSeer Preferences］フォームにアクセスし，SiteSeer データを表示するには，SiteScope クラシック・インタフェースを介して SiteScope にアクセスする必要があります。［SiteSeer Preferences］フォームの URL の例は次のとおりです。
http:// ＜ SiteScope サーバ＞ :8888/SiteScope/cgi/go.exe/SiteScope?page=siteseerPrefs&account=administrator
このフォームは，SiteScope クラシック・インタフェースの［**Preferences**］＞［**SiteSeer**］リンクにあります。

SiteSeer 統合用の設定

［SiteSeer Preferences］フォームは，2 つのセクション（［Required Settings］および［Advanced Options］）に分かれています。本項では，この 2 つのセクションの設定，およびこの 2 つのセクションを使用して SiteSeer アカウントと通信するように SiteScope を設定する方法について説明します。

［Required Settings］

［Required Settings］セクションには，リモート SiteSeer サービス・アカウントに接続するために SiteScope が必要とする情報が含まれます。

［SiteSeer Account］

SiteSeer アカウントの名前を入力します。このアカウント名は，通常電子メール・アドレスに指定されているドメイン名です。アカウント名は，SiteSeer アカウントの URL を調べると確認できます。たとえば，次の SiteSeer URL があるとします。

http://siteseer.mercuryinteractive.com/SiteScope?account=mycompany.com

この場合，アカウント名は mycompany.com です。

［SiteSeer Username］

SiteSeer アカウントへのログインに使用するユーザ名を入力します。これは，SiteSeer アカウントのメイン画面に表示されるユーザ名と同じです。

［SiteSeer Password］

SiteSeer アカウントへのログインに使用するパスワードを入力します。

［SiteSeer Host Name］

SiteSeer サービスのホスト名を入力します。一般には，siteseer2.mercuryinteractive.com または siteseer.mercuryinteractive.com です。SiteSeer アカウントの URL を調べ，これと異なるかどうかを確認してください。たとえば，次の URL があるとします。

http://siteseer2.mercuryinteractive.com/SiteScope?account=mydot.com

この場合，ホスト名は siteseer2.mercuryinteractive.com です。

［Advanced Options］

［Advanced Options］セクションでは，SiteScope インターフェイスでの SiteSteer アカウント情報のアクセスと表示をさらに制御できます。適切に項目を指定し，［**Save Changes**］ボタンをクリックします。

［Disabled］

このチェック・ボックスをオンにすると，SiteScope メイン・パネルに SiteSeer グループが表示されなくなります。ただし，対象の SiteSeer アカウントで現在有効なモニタは無効にされません。

［SiteSeer Title］

SiteScope パネルで SiteSeer アカウント・グループのラベルに使用するオプションのタイトルを入力します。標準設定では，グループ名として SiteSeer が使用されます。

［SiteSeer Proxy］

SiteSeer アカウントへのアクセスにプロキシ・サーバを使用する必要がある場合，ここにプロキシ・アドレスまたはドメイン名を入力します。

［SiteSeer Proxy Username］

プロキシを使用する場合，プロキシ・ユーザ名を入力します。

［SiteSeer Proxy Password］

プロキシを使用する場合，プロキシ・パスワードを入力します。

［Hide SiteSeer Group］

このオプションを選択すると，SiteScope パネルに SiteSeer グループが表示されなくなります。

［Automatic SiteSeer Login］

このチェックボックスをオンにすると，SiteSeer アカウントに自動ログインできるようになります。

[SiteSeer Read Only Username]

SiteSeer アカウントへの読み取り専用アクセスのログインに使用するユーザ名を入力します。これは，標準設定の管理者アカウント以外の SiteSeer ログイン・アカウントを定義している場合に使用します。通常は，「user」アカウントです。

[SiteSeer Read Only Password]

SiteSeer アカウントへの読み取り専用アクセスのログインに使用するパスワードを入力します。

付録 C

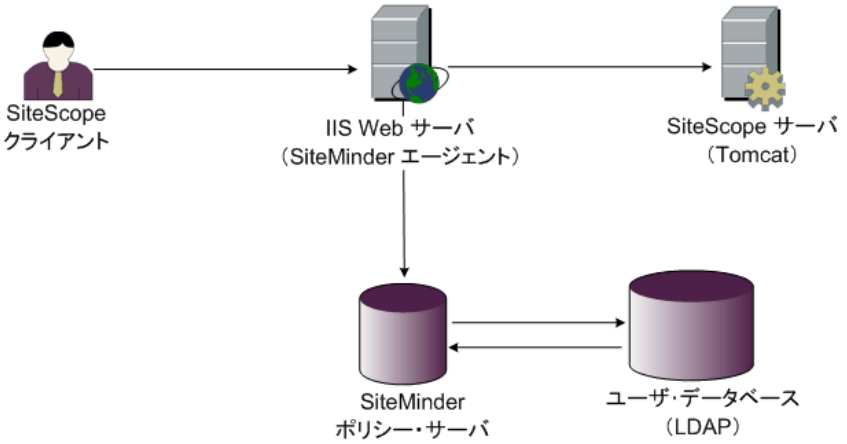
SiteScope と SiteMinder との統合

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。

本章の内容

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 上または任意の他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，および SiteScope Tomcat アプリケーション・サーバは同じマシンで構成することを推奨します。

統合の要件

この節では，SiteScope と SiteMinder を統合するための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 2000，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 以降

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，次の手順を実行します。

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，204 ページ「SiteMinder ポリシー・サーバの設定」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，187 ページ「Apache Tomcat サーバ・ファイルの設定」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，191 ページ「IIS の設定」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，206 ページ「さまざまな SiteScope ロールの権限の定義」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設定することによって，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他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，次の手順を実行します。

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 以下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（例：**SiteScope rule**）。［**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共に 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，［**Attribute Name**］フィールドに特別な SiteMinder 変数が使用されます。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，通常のグループには **SM_USERGROUPS** 変数を使用しなければなりません。

5 SiteScope ルールとセキュリティ・ポリシー・オブジェクトへの応答を追加します。

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，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（エンティティは，領域の同じドメインに含まれるユーザ・ディレクトリからのみ選択できます）。

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 **SiteScope 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，187 ページ「Apache Tomcat サーバ・ファイルの設定」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，191 ページ「IIS の設定」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。さもないと SiteMinder はログイ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 ヘルプの「User Preferences」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」）。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，次の手順を実行します。

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 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 によって有効なユーザとしては認識されないけれどもロールは認識されたために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［**LOGOUT**］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 にログイ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 がログイ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 ヘルプの SiteScope 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。

付録 D

SiteScope 設定のコピー

注：この機能はまだ使用できますが，設定ツールに置き換えられました。設定ツールの使い方については，79 ページ「設定ツールの実行」（Windows）または 109 ページ「設定ツールの実行」（Solaris および Linux）を参照してください。

お使いの環境で 9.0 以前のバージョンの SiteScope が稼働していて，それを SiteScope の最新バージョンにアップグレードする場合は，モニタ設定コピー・ユーティリティを使用して既存のモニタ設定を転送します。このユーティリティにより，ある SiteScope から別の SiteScope に設定データを移動するのに便利なツールが提供されます。

モニタ設定コピー・ユーティリティには，SiteScope クラシック・インタフェースからアクセスします。新しいインタフェースからはアクセスできません。このユーティリティへのアクセス方法の詳細については，212 ページ「設定データのコピー」を参照してください。

注：ただし，コピー・ユーティリティではコピーされない SiteScope 設定データもあります。このユーティリティでコピーされないデータの詳細については，210 ページ「注意事項と制限事項」を参照してください。

使用法

このユーティリティは，以前のバージョンの SiteScope からアップグレードしている場合に使用します。このコピー操作は，新しい SiteScope にほかの設定を行う前に，設定データをコピーするために使用できます。またこのユーティリティを使用すると，ある SiteScope から別の SiteScope に，既存の SiteScope 設定をコピーできます。

注：設定データ・ファイルは，既存の SiteScope から新しい SiteScope に手作業でコピーすることができます。新しい SiteScope の対応するディレクトリに設定ファイルを移動するときに，コピー先の SiteScope が稼働していてはいけません。これは，SiteScope 9.50 の設定メカニズムとの設定の競合が発生する可能性を避けるためです。

要件

コピー操作では，設定データを転送するために HTTP 要求を使用します。SiteScope には，設定ファイルを転送する機能が含まれています。この機能を使用するには，最新バージョンの SiteScope（設定のコピー先）のインストールが稼働していて，旧バージョンの SiteScope（設定のコピー元）から HTTP（または場合によっては HTTPS）を使用してアクセスできる必要があります。

注意事項と制限事項

モニタ設定コピー・ユーティリティの使用における重要な注意事項と制限事項を次に示します。

- **SiteScope 9.50 のライセンス**：SiteScope 7.9.x から SiteScope 9.50 にアップグレードする場合，ライセンス・キーはコピーされません。このアップグレードのシナリオでは，SiteScope 9.50 には新しいライセンス・キーが必要であり，以前のバージョンの SiteScope のライセンス・キーでは操作できません。既存のライセンスを置き換えて SiteScope 9.50 ライセンスを取得するには，HP の営業担当者にご連絡ください。

  SiteScope 8.x から SiteScope 9.50 にアップブレードする場合，新しいライセンス・キーは必要ありません。SiteScope 8. x のライセンスは有効であり，アップグレード・プロセス中にコピーされます。

➤ **統合（EMS）モニタ設定ファイル：**

あるディレクトリに SiteScope 7.9.5.0 がインストールされていて，別のディレクトリに 9.50 がインストールされている場合，SiteScope 7.9.5.0 の ems ディレクトリを 9.50 のディレクトリにコピーする必要があります。たとえば，SiteScope 7.9.5.0 が C:¥SiteScope にインストールされていて，SiteScope 9.50 が D:¥SiteScope にインストールされているとします。この場合，7.9.5.0 の C:¥SiteScope¥ems ディレクトリを，9.50 の D:¥SiteScope¥ems ディレクトリにコピーする必要があります。

SiteScope 8.x から 9.50 にアップグレードする場合，コピーする必要があるのは，作成または変更した **SiteScope¥conf¥ems** ディレクトリのファイルだけです。

各統合モニタを編集して，［**EMS 設定ファイル パス**］が 9.50 ディレクトリを指定していることを確認します。

➤ **その他のモニタ設定ファイル：**

次のモニタについて，さまざまなモニタ設定ファイルが 9.50 ディレクトリを指定していることを確認し，必要に応じて変更します。

- ➤ スクリプト
- ➤ SNMP
- ➤ MIB による SNMP
- ➤ SNMP トラップ
- ➤ テクノロジ統合（すべてのタイプ）
- ➤ WebScript
- ➤ Windows Performance Counter

➤ **ミドルウェアおよびドライバ**：外部データベースに対する接続，監視，SiteScope データのログ記録に使用されるデータベース・ドライバなどのミドルウェアは，コピー・ユーティリティではコピーされません。これらのライブラリまたはパッケージは，新しい SiteScope に手作業で再インストールする必要があります。

➤ **カスタム・モニタ**：コピー・ユーティリティでは，カスタム・モニタ・ファイルはコピーされません。必要に応じて，適切なファイルを新しい SiteScope にコピーする必要があります。

設定データのコピー

ある SiteScope から別の SiteScope に SiteScope モニタ設定をコピーするには，次の手順を使用します。

SiteScope 設定をコピーするには，次の手順を実行します。

1 SiteScope クラシック・インタフェースで最新のバージョンの SiteScope セットアップ・ページにアクセスします。このページは，インストール後，グループまたはモニタが作成される前に，クラシック・インタフェース・ポート番号を使用して初めて SiteScope を開いたときに表示されます。

次の構文を使用してセットアップ・ページの URL を開くことができます。

http:// ＜ SiteScope のホスト＞ :8888/SiteScope/cgi/go.exe/SiteScope?page=setup

2 セットアップ・ページで必要なフィールドを入力して，ページの下部にある［**Copy**］をクリックします。［Copy Monitor Configurations］ページが開きます。

3［**Remote SiteScope Server Address and Port**］フィールドに，旧バージョンの SiteScope が稼働しているサーバのホスト名またはアドレスを入力します。コピー元の SiteScope がリッスンするポート番号を含めます。

標準設定では，SiteScope はポート 8888 でリッスンします。

4［**SiteScope Administrator User Name**］フィールドに旧バージョンの SiteScope の管理者のユーザ名を入力し，［**SiteScope Administrator Password**］フィールドにその管理者のパスワードを入力します。

注：入力するのは，リモート SiteScope の［Users Preferences（ユーザ プリファレンス)］で設定されているユーザ名とパスワードであり，ファイル・システムを介してリモート・サーバにログインするためのユーザ名とパスワードではありません。コピー元の SiteScope に管理者ユーザを定義していない場合は，これらのフィールドには何も入力しません。

---

5 データ転送に HTTPS セキュア・プロトコルを使用する場合は，［**Use HTTPS**］チェック・ボックスを選択します。

6 コピー元の SiteScope との通信にプロキシ・サーバを使用する必要がある場合は，［**Proxy Server**］フィールド，［**Proxy Server User Name**］フィールド，［**Proxy Server Password**］フィールドに適切な接続情報を入力します。

7 コピー元の SiteScope で［International Version］オプションが有効な場合は（［General Preferences（一般のプリファレンス）］ページを参照），［Copy Monitor Configurations］画面の［**International Version**］チェック・ボックスを選択します。

8［**Copy**］ボタンをクリックして次に進みます。コピーの確認画面が開きます。

9［**Copy**］ボタンをクリックして，コピー操作を開始します。進行を示す画面が開きます。

コピー操作が正常に終了すると，新しい SiteScope が自動的に再起動され，コピーされた設定が処理されます。

10 SiteScope の再起動後，適切なアドレスとポート番号を入力して，SiteScope インタフェースに対する新しい Web ブラウザ要求を行います。

たとえば，新しい SiteScope 8.0 インタフェースは
http:// ＜ SiteScope のホスト＞ :8080/SiteScope/ で利用できます。

SiteScope クラシック・インタフェースは
http:// ＜ SiteScope のホスト＞ :8888/SiteScope で利用できます。

索引