IBM Security

IBM Security SiteProtector System
インストール・ガイド

バージョン 3.0

お願い

本書および本書で紹介する製品をご使用になる前に、 73 ページの『特記事項』に記載されている情報をお読みください。

本製品およびオプションに電源コード・セットが付属する場合は、それぞれ専用のものになっていますので他の電気機器には使用しないでください。

本書は、IBM Security SiteProtector System バージョン 3.0、および新しい版で明記されていない限り、以降のすべてのリリースおよびモディフィケーションに適用されます。

お客様の環境によっては、資料中の円記号がバックスラッシュと表示されたり、バックスラッシュが円記号と表示されたりする場合があります。

原典： IBM Security
IBM Security SiteProtector System
Installation Guide
Version 3.0

発行： 日本アイ・ビー・エム株式会社

担当： トランスレーション・サービス・センター

第1刷 2013.8

© Copyright IBM Corporation 1994, 2013.

目次

本書について v

第 1 章 SiteProtector の概要. 1
SiteProtector の用語 1
SiteProtector のアーキテクチャー. 1
SiteProtector コンポーネント 3
アドオン・コンポーネント. 4

第 2 章 ハードウェア要件とソフトウェア要件 5
仮想化 (VMware) をサポートするためのシステム要件 5
厳重 (SP800-131A) 暗号化の要件 5
SiteProtector Express インストールのシステム要件 . . 6
SiteProtector Database のシステム要件 8
Application Server のシステム要件 10
Console のシステム要件 13
Event Viewer のシステム要件 15
Event Archiver のシステム要件 16
Event Collector および Agent Manager のシステム要件 18
X-Press Update Server のシステム要件 20

第 3 章 SiteProtector のインストールの計画 23
スケーラビリティー・ガイドライン 23
デプロイメント・シナリオ 23
パフォーマンスに関する考慮事項 24
推奨事項 25
最小デプロイメント 26
小規模デプロイメント 27
中規模デプロイメント 28
大規模デプロイメント 29
複数サイトのデプロイメント 31
インストールに関する考慮事項 31
インストール・オプション 31
インストール・プログラムの場所 32
インストールに関するその他の注意点 32
インストール・プログラムによって生成される情報 34
SiteProtector のインストールの準備 34
セキュリティーに関する考慮事項 34
厳重な (SP800-131A) 暗号セキュリティーに関する考慮事項 35
Internet Explorer での TLS v1.2 の設定 36
セキュア通信を行うための SiteProtector データベースの IPsec の構成 37
Site Database システムの準備 37
SiteProtector コンポーネントのインストール先となるシステムの準備 37
Microsoft 更新のインストール 38
Microsoft 更新 38
Microsoft 更新のダウンロード 38
Microsoft 更新の管理 38
インストールのチェックリスト 39
インストール前のチェックリスト 39
必要な情報のチェックリスト 40
Express オプションのインストール・タスク・リスト 40
SiteProtector パッケージのインストール・タスク・リスト 41
インストール後のタスク 41

第 4 章 SiteProtector のインストール 43
Express インストールを使用した最小デプロイメントまたは小規模デプロイメントのインストール . . . 43
Express インストール実行の準備 43
TCP/IP 経由の SQL Server Express 通信の有効化 43
Express インストールの実行 44
中規模 SiteProtector デプロイメントのインストール 45
大規模 SiteProtector デプロイメントのインストール 47
SQL Server クラスターでの SiteProtector のインストール 49
64 ビット・プラットフォームでの SiteProtector のインストール 51
Windows NT 認証を使用する場合の SiteProtector のインストール 51

第 5 章 追加コンポーネントのインストール 53
追加コンポーネントの概要 53
追加の Console のインストール 55
追加の Event Collector のインストール 55
追加の Agent Manager のインストール 56
追加の Event Viewer のインストール. 57
追加 XPU Server のインストール 57
Event Archiver のインストール 59

第 6 章 インストールの問題のトラブルシューティング 61
失敗したインストールのトラブルシューティング . . 61
インストールの問題 61
issApp ログインが既に存在する 61
Event Collector ログインを削除できない 62
Event Collector を停止できない 62
データベースが使用中である 62

第 7 章 アンインストール. 63
SiteProtector コンポーネントのアンインストール . . 63
SiteProtector のアンインストール 63

© Copyright IBM Corp. 1994, 2013

第 8 章 データベース通信の保護 65
暗号化プロトコル 65
SSL 暗号化の有効化 65
SSL 暗号化に関する考慮事項 65
Event Collector での SSL の有効化 65
Application Server での SSL の有効化 66
Agent Manager での SSL の有効化 67
SecurityFusion Module での SSL の有効化 . . . 67

付録 A. サポートされるエージェントとアプライアンス 69

付録 B. IBM サポートへの連絡. 71

特記事項 73
商標 74
通信規制の注記 74
プライバシー・ポリシーに関する考慮事項 74
適切なセキュリティーの実践に関する注意事項 . . 75

索引 77

本書について

本書では、IBM® Security SiteProtector™ System をインストールする際に必要な情報を提供します。

対象読者

本書は、ネットワークまたはセキュリティー管理者、あるいは SiteProtector System のインストールとネットワーク・セキュリティーの管理を行う他の担当者を対象としています。本書では、ファイアウォールやプロキシーの構成、および Microsoft SQL データベースの構成など、ネットワーク・デバイスについて読者がよく理解していることを前提とします。

前提条件および関連情報

以下の表で、SiteProtector System をインストールしてから構成する際に使用する SiteProtector 資料について説明します。

資料	内容
IBM Security SiteProtector System 構成ガイド	SiteProtector の構成、更新、および保守に関する情報が記載されています。
IBM Security SiteProtector System ポリシーおよびレスポンス構成ガイド	Central Responses を含むポリシーとレスポンスの構成についての情報が記載されています。
IBM Security SiteProtector System SiteProtector Traffic のファイアウォールの構成	ネットワーク・デバイスと SiteProtector System コンポーネントが相互に通信できるようにするために、セキュリティー・マネージャーがファイアウォールを構成するための情報が記載されています。
IBM Security SiteProtector System セキュリティー・アナリスト向けユーザー・ガイド	セキュリティー・アナリストが SiteProtector System 用のポリシーおよびレスポンスを管理するための情報が記載されています。
IBM Security SiteProtector インフォメーション・センター (ヘルプ)	印刷されたユーザー文書には記載されていない可能性がある詳細な手順を含む、SiteProtector を使用するために必要なすべての手順が含まれています。

次の場所で、PDF 形式のすべての SiteProtector 資料を見つけてください。

- IBM Security 製品インフォメーション・センター。

© Copyright IBM Corp. 1994, 2013

第 1 章 SiteProtector の概要

IBM Security SiteProtector System は、ネットワーク、サーバー、および Desktop Endpoint Security エージェントと小規模ネットワークまたはアプライアンスの管理と分析を統合して行う中央管理システムです。大きな企業規模の環境に対応してセキュリティーを提供するために、SiteProtector を簡単に拡大することができます。

SiteProtector は、すべての IBM Security 製品のコマンド、制御、およびモニター機能を提供します。

SiteProtector の用語

SiteProtector の資料では、特別な用語が使用されます。

本書では、セキュリティー製品に関する以下の用語が使用されます。

用語	説明
エージェント (agent)	すべてのアプライアンスとスキャナー、および Network Sensor、Server Sensor、Desktop Sensor を表す一般用語。
アプライアンス (appliance)	ネットワークまたはゲートウェイ上のインラインのセキュリティー・デバイス。 アプライアンスはそのタイプに応じて、不正侵入の検出と防御、アンチウィルス、アンチスパム、仮想プライベート・ネットワーキング (VPN)、Web フィルタリング、およびファイアウォール機能を任意に組み合わせて提供できる。
スキャナー (scanner)	アセットをスキャンして脆弱性やその他のセキュリティー・リスクの有無を調べるエージェント。
センサー (sensor)	ネットワークおよびサーバーのネットワーク・トラフィックをモニターして攻撃を識別し、場合によっては攻撃を停止するエージェント。

SiteProtector のアーキテクチャー

SiteProtector のアーキテクチャーは、複数のコンピューターへのインストールに役立ちます。

SiteProtector サイトのコンポーネントの概要。

© Copyright IBM Corp. 1994, 2013

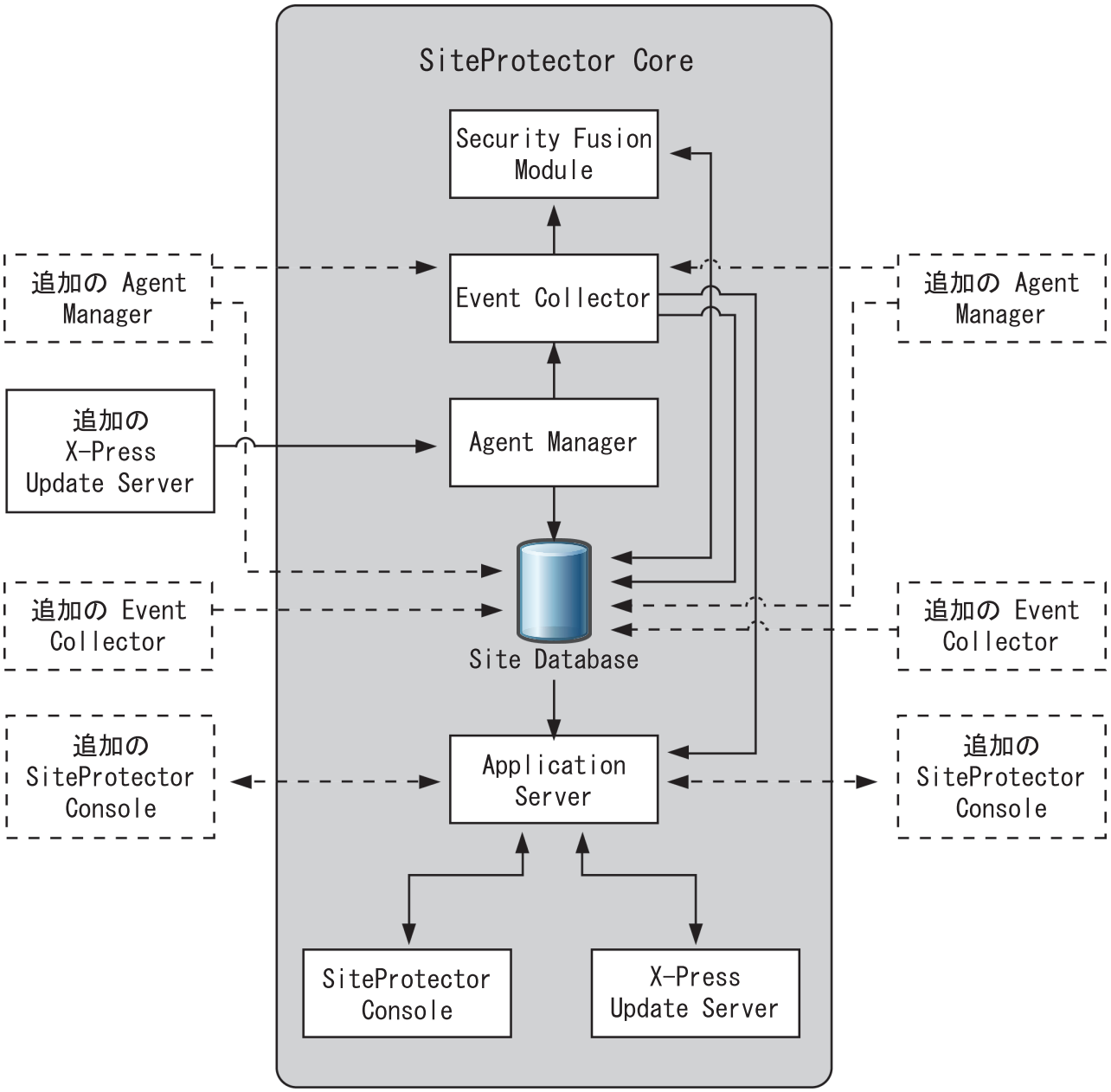

図 1. 標準的なサイトにおけるコンポーネント

通信チャネル

SiteProtector System コンポーネントは特定のチャネルを使用して相互に通信し、他の IBM Security 製品とも通信を行います。通信に使用されるポートの完全なリストについては、「*SiteProtector Traffic のファイアウォールの構成*」の資料 (http://pic.dhe.ibm.com/infocenter/sprotect/v2r8m0/index.jsp?topic=%2Fcom.ibm.siteprotector.doc%2Fpdfs%2Fsp_printable_pdfs.htmで入手可) を参照してください

SiteProtector コンポーネント

SiteProtector System は多数のコンポーネントで構成されています。

SiteProtector コンポーネント	説明
Agent Manager	Agent Manager は、Desktop Endpoint Security エージェントと IBM Security アプライアンスのコマンドと制御アクティビティーを管理します。また、エージェントから Event Collector へのデータ転送を容易にします。 Agent Manager を使用することで、SiteProtector でのエージェントとコンポーネントからのデータの収集および管理が可能になります。Agent Manager は Express オプションと Recommended オプションと共にインストールされます。
Console	SiteProtector Console は SiteProtector に対するメインのユーザー・インターフェースです。ユーザーは、イベントのモニター、スキャンのスケジューリング、レポートの生成、およびエージェントの構成など、ほとんどの SiteProtector 機能をこの Console から実行します。
Event Archiver	Event Archiver はイベント・データを保管し、Site Database で保管する必要があるイベントの数を減らしてパフォーマンスを向上させます。
Event Collector	Event Collector は、センサーからのリアルタイム・イベントと、スキャナーからのぜい弱性データを管理します。
Event Viewer (オプション)	SiteProtector Event Viewer は Event Collector から未処理のイベントを受け取り、トラブルシューティング用に、セキュリティー・データに対するほぼリアルタイムでのアクセスを提供します。
SecurityFusion™ Module	SecurityFusion Module は、サイトにおける重大な脅威を素早く識別して対応する機能を高めます。高度な分析技法を使用して、SecurityFusion Module は影響が大きい攻撃をエスカレートします。これは、最も重要な攻撃アクティビティーに焦点を当てるのに役立ちます。
Site Database	SiteProtector データベース (Site Database) にはエージェントの未加工データ、発生メトリック (エージェントによってトリガーされたセキュリティー・イベントの統計)、グループ情報、コマンド・データと制御データ、および X-Press Update (XPU) のステータスが格納されます。
SiteProtector Reporting	グラフィカルな要約とコンプライアンスのレポートは、管理者がセキュリティーの状態を評価するために必要な情報を提供します。レポートは、ぜい弱性アセスメント、攻撃アクティビティー、監査、コンテンツ・フィルタリング、 Desktop Endpoint Security、SecurityFusion およびウィルス・アクティビティーに関する情報を示します。
SP Core	SP Core には以下のコンポーネントが含まれます。 • Application Server。SiteProtector Console と Site Database の間の通信を可能にします。 • Agent Controller。イベント収集を開始または停止するコマンドなど、エージェントのコマンドと制御アクティビティーを管理します。 • X-Press Update Server。IBM ダウンロード・センターからダウンロードされた X-Press Update (XPU) を保管し、ネットワーク上のエージェントとコンポーネントで XPU を使用できるようにする Web サーバーです。Update Server を使用することで、類似製品の更新を何度もダウンロードする必要がなくなるため、ユーザーは更新プロセスをより効率的に管理できるようになります。 • SiteProtector Web Access。SiteProtector のイベント・アセットとセキュリティー・イベントをモニターするために SiteProtector に簡単にアクセスできるようにする読み取り専用のインターフェースです。

SiteProtector コンポーネント	説明
X-Press Update Server	X-Press Update Server は、IBM ダウンロード・センターからダウンロードされた X-Press Update (XPU) を保管し、ネットワーク上のエージェントとコンポーネントで XPU を使用できるようにする Web サーバーです。Update Server を使用することで、類似製品の更新を何度もダウンロードする必要がなくなるため、ユーザーは更新プロセスをより効率的に管理できるようになります。

アドオン・コンポーネント

SiteProtectorのアドオン・コンポーネントは、追加の保護および機能を提供します。

注: ここで示すアドオン・コンポーネントは、SiteProtector で使用可能な別途使用許諾された機能です。

SiteProtector SecureSync Failover

SiteProtector SecureSync Failover 機能は、SiteProtector をフェイルオーバー用に構成する方法と、完全に失敗した後に SiteProtector を復旧する方法に関する情報をユーザーに提供します。

第 2 章 ハードウェア要件とソフトウェア要件

IBM Security SiteProtector System の各コンポーネントには特定のハードウェア要件とソフトウェア要件があります。

このセクションのシステム要件に関するトピックの表には、以下の構成の項目が含まれています。

- **SiteProtector ベースライン**は、メイン SiteProtector System の要件を指します。
- **XGS サポート**は、 IBM Security Network Protection アプライアンスのポリシー編集に関する要件を指します。このポリシー編集には、一部の Microsoft オペレーティング・システムでのみサポートされている Internet Explorer v9 以上が必要です。
- **SP800-131A サポート**は、米国連邦情報・技術局 (NIST) が定義した厳重 (SP800-131A) 暗号化の要件を指します。厳重暗号化には、Internet Explorer v8 以上でのみサポートされている Transport Layer Security (TLS) v1.2 が必要です。Internet Explorer v8 以上は、一部の Microsoft オペレーティング・システムでのみサポートされています。

重要: 一部の SiteProtector コンポーネントのインストールでは、Windows ファイル・システム・レジストリー設定で 8.3 形式のショート・ネーミングが必要になります。SiteProtector コンポーネントのインストールを計画しているサーバーのレジストリー設定でショート・ネームを無効にした場合は、SiteProtector をインストールする前に、ショート・ネームを再度有効にする必要があります。

注: SiteProtector System では、Windows Server 2012 Standard で使用可能な Resilient File System (ReFS) はサポートされていません。

仮想化 (VMware) をサポートするためのシステム要件

以下の表で、仮想化のシステム要件について説明します。

コンポーネント	最小要件
仮想化	• VMware ESX 4.x または ESXi 4.x または 5.x • Microsoft Windows Server 2008 Hyper-V • Microsoft Virtual Server 2005

注: 仮想マシンが 6 ページの『SiteProtector Express インストールのシステム要件』に記載されている要件を満たしている場合は、仮想環境にすべての SiteProtector コンポーネントをインストールすることができます。

厳重 (SP800-131A) 暗号化の要件

厳重 (SP800-131A) 暗号化には Transport Layer Security (TLS) v1.2 が必要です。TLS v1.2 は Internet Explorer v8 以上でのみサポートされています。Internet Explorer v8 以上は、一部の Microsoft オペレーティング・システムでのみサポートされています。

厳重暗号化を使用するには、Internet Explorer が TLS 1.2 をサポートするように構成されている必要があります。

© Copyright IBM Corp. 1994, 2013

厳重暗号化を使用するには、SiteProtector Database に対して IPsec を構成する必要があります。詳しくは、以下に示す関連タスクを参照してください。

特定の要件については、このセクションのシステム要件に関するトピックの表の「**SP800-131A サポート**」列を参照してください。

SiteProtector Express インストールのシステム要件

SiteProtector Express インストールは、SiteProtector System でサポートされている最小デプロイメント構成です。1 台のコンピューターにすべての SiteProtector コンポーネントをインストールします。これは、小規模ネットワークやテスト環境に最も適しています。

以下の表で、Express インストールのシステム要件について説明します。この表には次の構成の項目が含まれています。

- **SiteProtector ベースライン**は、メイン SiteProtector System の要件を指します。
- **XGS サポート**は、 IBM Security Network Protection アプライアンスのポリシー編集に関する要件を指します。このポリシー編集には、一部の Microsoft オペレーティング・システムでのみサポートされている Internet Explorer v9 以上が必要です。
- **SP800-131A サポート**は、米国連邦情報・技術局 (NIST) が定義した厳重 (SP800-131A) 暗号化の要件を指します。厳重暗号化には、Internet Explorer v8 以上でのみサポートされている Transport Layer Security (TLS) v1.2 が必要です。Internet Explorer v8 以上は、一部の Microsoft オペレーティング・システムでのみサポートされています。

コンポーネント	最小要件	SP ベースライン	XGS サポート	SP800-131A サポート*
プロセッサー	Xeon 3000 シリーズまたは Core 2 Duo (最小) 2.53 GHz Intel Xeon E5540 (推奨)	✓	✓	✓
オペレーティング・システム SiteProtector は、Windows オペレーティング・システムの 32 ビット・バージョンと 64 ビット・バージョンの両方に対応しています。64 ビットのみのシステムには注が付いています。 **注:** SiteProtector とそのコンポーネントは、NTFS でフォーマットされたパーティションで実行する必要があります。FAT および FAT32 パーティションでは、システムを適切に強化できません。	Windows Server 2012 Standard[1] (64 ビットのみ)	✓	✓	✓
	Windows Server 2008 R2 Standard (64 ビットのみ)	✓	✓	✓

コンポーネント	最小要件	SP ベースライン	XGS サポート	SP800-131A サポート*
	Windows Server 2008 R2 Enterprise (64 ビットのみ)	✓	✓	✓
	Windows Server 2008 Standard	✓	✓	
	Windows Server 2008 Enterprise	✓	✓	
	Windows Server 2003 R2 Standard	✓		
	Windows Server 2003 R2 Enterprise	✓		
	Windows Server 2003 SP2 Standard	✓		
	Windows Server 2003 SP2 Enterprise	✓		
RAM	2 GB (最小) 8 GB (推奨)	✓	✓	✓
OS および DBMS の空きハード・ディスク・スペース	18 GB (最小) 36 GB (推奨)	✓	✓	✓
30 日分の追加データの空きハード・ディスク・スペース	20 GB (最小) 38 GB (推奨)	✓	✓	✓
90 日分の追加データの空きハード・ディスク・スペース	23 GB (最小) 41 GB (推奨)	✓	✓	✓
画面解像度	1024 x 768 ピクセル	✓	✓	✓
サード・パーティー・ソフトウェア (付属しています)	IBM Java Runtime Environment (JRE) バージョン 1.7.0 SR2	✓	✓	✓
サード・パーティー・ソフトウェア (付属していません)	• SQL Server 2012 Express Edition (テスト・システムとしてのみ推奨) **注:** SQL Server 2012 Express ではデータベースのサイズが 10 GB に制限されています。 • SQL Server 2012 Standard Edition • SQL Server 2012 Enterprise Edition • SQL Server 2008 Standard Edition • SQL Server 2008 R2 Standard Edition • SQL Server 2008 Enterprise Edition • SQL Server 2008 R2 Enterprise Edition • SQL Server 2008 (64 ビット) • SQL Server 2005 Enterprise Edition • SQL Server 2005 Standard Edition • SQL Server 2005 (64 ビット)	✓	✓	✓
	Internet Explorer 8.0 以降 http://www.microsoft.com/windows/internet-explorer/default.aspx	✓		✓ (TLS 1.2 を使用)

コンポーネント	最小要件	SP ベースライン	XGS サポート	SP800-131A サポート*
	Internet Explorer 9.0 以降 http://www.microsoft.com/windows/internet-explorer/default.aspx	✓	✓	✓ (TLS 1.2 を使用)
	• Adobe Reader 8.0 以降http://get.adobe.com/reader/ • Windows オペレーティング・システムのソフトウェアと Windows ベースのハードウェアの最新の更新については、Microsoft Update Web サイトhttp://www.windowsupdate.com	✓	✓	✓
固定 IP アドレスか	はい	✓	✓	✓
その他の要件	以下の項目などのさまざまな要因に応じて追加されるメモリーおよびディスク・スペース。 • ビューの数 • アセットの数 • エージェントの数 • 同時ユーザーの数 • エージェントに実装されるポリシーのタイプ • サーバーに保管されるデータの量	✓	✓	✓

[1]Windows Server 2012 は、通常モードでインストールする必要があります。SiteProtector は、「コアのみ」のモードでインストールされた Windows Server 2012 をサポートしていません。

* 詳しくは 5 ページの『厳重 (SP800-131A) 暗号化の要件』を参照してください。

SiteProtector Database のシステム要件

以下の表で、SiteProtector Database のシステム要件について説明します。この表には次の構成の項目が含まれています。

- **SiteProtector ベースライン**は、メイン SiteProtector System の要件を指します。
- **XGS サポート**は、 IBM Security Network Protection アプライアンスのポリシー編集に関する要件を指します。このポリシー編集には、一部の Microsoft オペレーティング・システムでのみサポートされている Internet Explorer v9 以上が必要です。
- **SP800-131A サポート**は、米国連邦情報・技術局 (NIST) が定義した厳重 (SP800-131A) 暗号化の要件を指します。厳重暗号化には、Internet Explorer v8 以上でのみサポートされている Transport Layer Security (TLS) v1.2 が必要です。Internet Explorer v8 以上は、一部の Microsoft オペレーティング・システムでのみサポートされています。

SiteProtector Database で厳重 (SP800-131A) 暗号化を使用する場合は、 37 ページの『セキュア通信を行うための SiteProtector データベースの IPsec の構成』を参照してください。

コンポーネント	最小要件	SP ベースライン	XGS サポート	SP800-131A サポート*
プロセッサー	Xeon 3000 シリーズまたは Core 2 Duo (最小) 3.00 GHz Intel Xeon E5450 (推奨)	✓	✓	✓
オペレーティング・システム SiteProtector は、Windows オペレーティング・システムの 32 ビット・バージョンと 64 ビット・バージョンの両方に対応しています。64 ビットのみのシステムには注が付いています。 **注:** SiteProtector とそのコンポーネントは、NTFS でフォーマットされたパーティションで実行する必要があります。FAT および FAT32 パーティションでは、システムを適切に強化できません。	Windows Server 2012 Standard[1] (64 ビットのみ)	✓	✓	✓
	Windows Server 2008 R2 Standard (64 ビットのみ)	✓	✓	✓
	Windows Server 2008 R2 Enterprise (64 ビットのみ)	✓	✓	✓
	Windows Server 2008 Standard	✓	✓	
	Windows Server 2008 Enterprise	✓	✓	
	Windows Server 2003 R2 Standard	✓		
	Windows Server 2003 R2 Enterprise	✓		
	Windows Server 2003 SP2 Standard	✓		
	Windows Server 2003 SP2 Enterprise	✓		
RAM	2 GB (最小) 4 GB (推奨)	✓	✓	✓
空きハード・ディスク・スペース	18 GB (最小) 36 GB (推奨)	✓	✓	✓
サード・パーティー・ソフトウェア (付属しています)	IBM Java Runtime Environment (JRE) バージョン 1.7.0 SR2	✓	✓	✓

コンポーネント	最小要件	SP ベースライン	XGS サポート	SP800-131A サポート*
サード・パーティー・ソフトウェア (付属していません)	• SQL Server 2012 Express Edition (テスト・システムとしてのみ推奨) **注:** SQL Server 2012 Express ではデータベースのサイズが 10 GB に制限されています。 • SQL Server 2012 Standard Edition • SQL Server 2012 Enterprise Edition • SQL Server 2008 Standard Edition • SQL Server 2008 R2 Standard Edition • SQL Server 2008 Enterprise Edition • SQL Server 2008 R2 Enterprise Edition • SQL Server 2008 (64 ビット) • SQL Server 2005 Enterprise Edition • SQL Server 2005 Standard Edition • SQL Server 2005 (64 ビット)	✓	✓	✓
	Internet Explorer 8.0 以降 http://www.microsoft.com/windows/internet-explorer/default.aspx	✓		✓ (TLS 1.2 を使用)
	Internet Explorer 9.0 以降 http://www.microsoft.com/windows/internet-explorer/default.aspx	✓	✓	✓ (TLS 1.2 を使用)
	• Windows オペレーティング・システムのソフトウェアと Windows ベースのハードウェアの最新の更新については、Microsoft Update Web サイトhttp://www.windowsupdate.com	✓	✓	✓
固定 IP アドレスか	はい	✓	✓	✓
その他の要件	以下の項目などのさまざまな要因に応じて追加されるメモリーおよびディスク・スペース。 • ビューの数 • アセットの数 • エージェントの数 • 同時ユーザーの数 • エージェントに実装されるポリシーのタイプ • サーバーに保管されるデータの量	✓	✓	✓

[1]Windows Server 2012 は、通常モードでインストールする必要があります。SiteProtector は、「コアのみ」のモードでインストールされた Windows Server 2012 をサポートしていません。

* 詳しくは 5 ページの『厳重 (SP800-131A) 暗号化の要件』を参照してください。

Application Server のシステム要件

Application Server のインストール・パッケージには、X-Press Update Server と Web Console も含まれています。

以下の表で、Application Server のシステム要件を説明します。この表には次の構成の項目が含まれています。

- **SiteProtector ベースライン**は、メイン SiteProtector System の要件を指します。
- **XGS サポート**は、 IBM Security Network Protection アプライアンスのポリシー編集に関する要件を指します。このポリシー編集には、一部の Microsoft オペレーティング・システムでのみサポートされている Internet Explorer v9 以上が必要です。
- **SP800-131A サポート**は、米国連邦情報・技術局 (NIST) が定義した厳重 (SP800-131A) 暗号化の要件を指します。厳重暗号化には、Internet Explorer v8 以上でのみサポートされている Transport Layer Security (TLS) v1.2 が必要です。Internet Explorer v8 以上は、一部の Microsoft オペレーティング・システムでのみサポートされています。

コンポーネント	最小要件	SP ベースライン	XGS サポート	SP800-131A サポート*
プロセッサー	Xeon 3000 シリーズまたは Core 2 Duo (最小) 3.00 GHz Intel Xeon E5450 (推奨)	✓	✓	✓
オペレーティング・システム SiteProtector は、Windows オペレーティング・システムの 32 ビット・バージョンと 64 ビット・バージョンの両方に対応しています。64 ビットのみのシステムには注が付いています。 **注:** SiteProtector とそのコンポーネントは、NTFS でフォーマットされたパーティションで実行する必要があります。FAT および FAT32 パーティションでは、システムを適切に強化できません。	Windows Server 2012 Standard[1] (64 ビットのみ)	✓	✓	✓
	Windows Server 2008 R2 Standard (64 ビットのみ)	✓	✓	✓
	Windows Server 2008 R2 Enterprise (64 ビットのみ)	✓	✓	✓
	Windows Server 2008 Standard	✓	✓	
	Windows Server 2008 Enterprise	✓	✓	
	Windows Server 2003 R2 Standard	✓		
	Windows Server 2003 R2 Enterprise	✓		
	Windows Server 2003 SP2 Standard	✓		
	Windows Server 2003 SP2 Enterprise	✓		
RAM	2 GB (最小) 4 GB (推奨)	✓	✓	✓

コンポーネント	最小要件	SP ベースライン	XGS サポート	SP800-131A サポート*
空きハード・ディスク・スペース	18 GB (最小) 40 GB (推奨)	✓	✓	✓
画面解像度	1024 x 768 ピクセル	✓	✓	✓
サード・パーティー・ソフトウェア (付属しています)	IBM Java Runtime Environment (JRE) バージョン 1.7.0 SR2	✓	✓	✓
サード・パーティー・ソフトウェア (付属していません)	Internet Explorer 8.0 以降 http://www.microsoft.com/windows/internet-explorer/default.aspx	✓		✓ (TLS 1.2 を使用)
	Internet Explorer 9.0 以降 http://www.microsoft.com/windows/internet-explorer/default.aspx	✓	✓	✓ (TLS 1.2 を使用)
	• Java J2SE Runtime Environment 5.0 (1.5.0) 以降 • Adobe Reader 8.0 以降http://get.adobe.com/reader/ • Windows オペレーティング・システムのソフトウェアと Windows ベースのハードウェアの最新の更新については、Microsoft Update Web サイトhttp://www.windowsupdate.com	✓	✓	✓
固定 IP アドレスか	はい	✓	✓	✓
仮想化	• VMware ESX 4.x または ESXi 4.x または 5.x • Microsoft Windows Server 2008 Hyper-V • Microsoft Virtual Server 2005	✓	✓	✓
その他の要件	以下の項目などのさまざまな要因に応じて追加されるメモリーおよびディスク・スペース。 • ビューの数 • アセットの数 • エージェントまたはアプライアンスの数 • 同時ユーザーの数 • エージェントまたはアプライアンスに実装されるポリシーのタイプ	✓	✓	✓

[1]Windows Server 2012 は、通常モードでインストールする必要があります。SiteProtector は、「コアのみ」のモードでインストールされた Windows Server 2012 をサポートしていません。

* 詳しくは 5 ページの『厳重 (SP800-131A) 暗号化の要件』を参照してください。

注: リソースの割り振りによる SiteProtector のパフォーマンス全体への影響が、Microsoft Virtual Server 2005 を使用していない場合よりも使用している場合の方がより大きいことがテストで明らかになりました。例えば、基本オペレーティング・システムとある仮想インスタンスがシングル・プロセッサー・ユニットで稼働していた場合、仮想インスタンスのみの仕様を満たすハードウェア・インスタンスで稼働していた場合よりも、SiteProtector の実行が遅くなります。そのため、Virtual Server 2005 を使用する場合には追加リソースの提供を検討してください。

Console のシステム要件

注: SiteProtector Console で「**ヘルプ**」を初めてクリックしたときに、Internet Explorer に「証明書のエラー」と表示される場合があります。今後このエラーが発生しないようにするには、Application Server で生成されるセキュリティー証明書をインストールします。詳しくは、Microsoft サポート Web サイト (http://support.microsoft.com/kb/931850) を参照してください。

以下の表で、単一 Console のシステム要件について説明します。この表には次の構成の項目が含まれています。

- **SiteProtector ベースライン**は、メイン SiteProtector System の要件を指します。
- **XGS サポート**は、 IBM Security Network Protection アプライアンスのポリシー編集に関する要件を指します。このポリシー編集には、一部の Microsoft オペレーティング・システムでのみサポートされている Internet Explorer v9 以上が必要です。
- **SP800-131A サポート**は、米国連邦情報・技術局 (NIST) が定義した厳重 (SP800-131A) 暗号化の要件を指します。厳重暗号化には、Internet Explorer v8 以上でのみサポートされている Transport Layer Security (TLS) v1.2 が必要です。Internet Explorer v8 以上は、一部の Microsoft オペレーティング・システムでのみサポートされています。

コンポーネント	最小要件	SP ベースライン	XGS サポート	SP800-131A サポート*
プロセッサー	Xeon 3000 シリーズまたは Core 2 Duo (最小) 3.00 GHz Intel Xeon E5450 (推奨)	✓	✓	✓
オペレーティング・システム SiteProtector は、Windows オペレーティング・システムの 32 ビット・バージョンと 64 ビット・バージョンの両方に対応しています。64 ビットのみのシステムには注が付いています。 **注:** SiteProtector とそのコンポーネントは、NTFS でフォーマットされたパーティションで実行する必要があります。FAT および FAT32 パーティションでは、システムを適切に強化できません。	Windows 8	✓	✓	✓
	Windows 7	✓	✓	✓
	Windows 7 Enterprise	✓	✓	✓
	Windows 7 Ultimate	✓	✓	✓
	Windows Server 2012 Standard[1] (64 ビットのみ)	✓	✓	✓
	Windows Server 2008 R2 Standard (64 ビットのみ)	✓	✓	✓

コンポーネント	最小要件	SP ベースライン	XGS サポート	SP800-131A サポート*
	Windows Server 2008 R2 Enterprise (64 ビットのみ)	✓	✓	✓
	Windows Vista Business	✓	✓	
	Windows Vista Enterprise	✓	✓	
	Windows Server 2008 Standard	✓	✓	
	Windows Server 2008 Enterprise	✓	✓	
	SQL Server 2008 R2 Standard Edition	✓		
	SQL Server 2008 R2 Enterprise Edition	✓		
	Windows Server 2003 R2 Standard	✓		
	Windows Server 2003 R2 Enterprise	✓		
	Windows Server 2003 SP2 Standard	✓		
	Windows Server 2003 SP2 Enterprise	✓		
RAM	512 MB (最小) 1 GB (推奨)	✓	✓	✓
空きハード・ディスク・スペース	4 GB (最小) 20 GB (推奨)	✓	✓	✓
画面解像度	1024 x 768 ピクセル	✓	✓	✓
色の設定	High Color (16 ビット)			
固定 IP アドレスか	いいえ			
サード・パーティー・ソフトウェア (付属しています)	IBM Java Runtime Environment (JRE) バージョン 1.7.0 SR2	✓	✓	✓
サード・パーティー・ソフトウェア (付属していません)	Internet Explorer 8.0 以降 http://www.microsoft.com/windows/internet-explorer/default.aspx	✓		✓ (TLS 1.2 を使用)
	Internet Explorer 9.0 以降 http://www.microsoft.com/windows/internet-explorer/default.aspx	✓	✓	✓ (TLS 1.2 を使用)
	• Adobe Reader 8.0 以降http://get.adobe.com/reader/ • Windows オペレーティング・システムのソフトウェアと Windows ベースのハードウェアの最新の更新については、Microsoft Update Web サイトhttp://www.windowsupdate.com	✓	✓	✓

[1]Windows Server 2012 は、通常モードでインストールする必要があります。SiteProtector は、「コアのみ」のモードでインストールされた Windows Server 2012 をサポートしていません。

* 詳しくは 5 ページの『厳重 (SP800-131A) 暗号化の要件』を参照してください。

Event Viewer のシステム要件

以下の表で、Event Viewer のシステム要件について説明します。この表には次の構成の項目が含まれています。

- **SiteProtector ベースライン**は、メイン SiteProtector System の要件を指します。
- **XGS サポート**は、 IBM Security Network Protection アプライアンスのポリシー編集に関する要件を指します。このポリシー編集には、一部の Microsoft オペレーティング・システムでのみサポートされている Internet Explorer v9 以上が必要です。
- **SP800-131A サポート**は、米国連邦情報・技術局 (NIST) が定義した厳重 (SP800-131A) 暗号化の要件を指します。厳重暗号化には、Internet Explorer v8 以上でのみサポートされている Transport Layer Security (TLS) v1.2 が必要です。Internet Explorer v8 以上は、一部の Microsoft オペレーティング・システムでのみサポートされています。

コンポーネント	最小要件	SP ベースライン	XGS サポート	SP800-131A サポート
プロセッサー	Xeon 3000 シリーズまたは Core 2 Duo (最小) 3.00 GHz Intel Xeon E5450 (推奨)	✓	✓	✓
オペレーティング・システム SiteProtector は、Windows オペレーティング・システムの 32 ビット・バージョンと 64 ビット・バージョンの両方に対応しています。64 ビットのみのシステムには注が付いています。 **注:** SiteProtector とそのコンポーネントは、NTFS でフォーマットされたパーティションで実行する必要があります。FAT および FAT32 パーティションでは、システムを適切に強化できません。	Windows 8	✓	✓	✓
	Windows 7	✓	✓	✓
	Windows 7 Enterprise	✓	✓	✓
	Windows 7 Ultimate	✓	✓	✓
	Windows Server 2012 Standard[1] (64 ビットのみ)	✓	✓	✓
	Windows Server 2008 R2 Standard (64 ビットのみ)	✓	✓	✓
	Windows Server 2008 R2 Enterprise (64 ビットのみ)	✓	✓	✓
	Windows Vista Business	✓	✓	
	Windows Vista Enterprise	✓	✓	
	Windows Server 2008 Standard	✓	✓	

コンポーネント	最小要件	SP ベースライン	XGS サポート	SP800-131A サポート
	Windows Server 2008 Enterprise	✓	✓	
	SQL Server 2008 R2 Standard Edition	✓		
	SQL Server 2008 R2 Enterprise Edition	✓		
	Windows Server 2003 R2 Standard	✓		
	Windows Server 2003 R2 Enterprise	✓		
	Windows Server 2003 SP2 Standard	✓		
	Windows Server 2003 SP2 Enterprise	✓		
RAM	512 MB (最小) 1 GB (推奨)	✓	✓	✓
空きハード・ディスク・スペース	4 GB (最小) 20 GB (推奨)	✓	✓	✓
画面解像度	1024 x 768 ピクセル	✓	✓	✓
色の設定	High Color (16 ビット)	✓	✓	✓
固定 IP アドレスか	いいえ	✓	✓	✓
サード・パーティー・ソフトウェア (付属しています)	IBM Java Runtime Environment (JRE) バージョン 1.7.0 SR2	✓	✓	✓

[1]Windows Server 2012 は、通常モードでインストールする必要があります。SiteProtector は、「コアのみ」のモードでインストールされた Windows Server 2012 をサポートしていません。

Event Archiver のシステム要件

以下の表で、Event Archiver のシステム要件について説明します。この表には次の構成の項目が含まれています。

- **SiteProtector ベースライン**は、メイン SiteProtector System の要件を指します。
- **XGS サポート**は、 IBM Security Network Protection アプライアンスのポリシー編集に関する要件を指します。このポリシー編集には、一部の Microsoft オペレーティング・システムでのみサポートされている Internet Explorer v9 以上が必要です。
- **SP800-131A サポート**は、米国連邦情報・技術局 (NIST) が定義した厳重 (SP800-131A) 暗号化の要件を指します。厳重暗号化には、Internet Explorer v8 以上でのみサポートされている Transport Layer Security (TLS) v1.2 が必要です。Internet Explorer v8 以上は、一部の Microsoft オペレーティング・システムでのみサポートされています。

コンポーネント	最小要件	SP ベースライン	XGS サポート	SP800-131A サポート
プロセッサー	Xeon 3000 シリーズまたは Core 2 Duo (最小) 3.00 GHz Intel Xeon E5450 (推奨)	✓	✓	✓

コンポーネント	最小要件	SP ベースライン	XGS サポート	SP800-131A サポート
オペレーティング・システム SiteProtector は、Windows オペレーティング・システムの 32 ビット・バージョンと 64 ビット・バージョンの両方に対応しています。64 ビットのみのシステムには注が付いています。 **注:** SiteProtector とそのコンポーネントは、NTFS でフォーマットされたパーティションで実行する必要があります。FAT および FAT32 パーティションでは、システムを適切に強化できません。	Windows Server 2012 Standard[1] (64 ビットのみ)	✓	✓	✓
	Windows Server 2008 R2 Standard (64 ビットのみ)	✓	✓	✓
	Windows Server 2008 R2 Enterprise (64 ビットのみ)	✓	✓	✓
	Windows Server 2008 Standard	✓	✓	
	Windows Server 2008 Enterprise	✓	✓	
	Windows Server 2003 R2 Standard	✓		
	Windows Server 2003 R2 Enterprise	✓		
	Windows Server 2003 SP2 Standard	✓		
	Windows Server 2003 SP2 Enterprise	✓		
RAM	512 MB (最小) 1 GB (推奨)	✓	✓	✓
空きハード・ディスク・スペース	9 GB (最小) 20 GB (推奨)	✓	✓	✓
サード・パーティー・ソフトウェア (付属していません)	• Windows オペレーティング・システムのソフトウェアと Windows ベースのハードウェアの最新の更新については、Microsoft Update Web サイトhttp://www.windowsupdate.com	✓	✓	✓
固定 IP アドレスか	はい	✓	✓	✓

コンポーネント	最小要件	SP ベースライン	XGS サポート	SP800-131A サポート
その他の要件	以下の項目などのさまざまな要因に応じて追加されるメモリーおよびディスク・スペース。 • エージェントまたはアプライアンスの数 • 同時ユーザーの数 • エージェントまたはアプライアンスに実装されるポリシーのタイプ • イベント・ログ	✓	✓	✓

[1]Windows Server 2012 は、通常モードでインストールする必要があります。SiteProtector は、「コアのみ」のモードでインストールされた Windows Server 2012 をサポートしていません。

Event Collector および Agent Manager のシステム要件

以下の表で、単一の Event Collector または単一の Agent Manager のシステム要件について説明します。この表には次の構成の項目が含まれています。

- **SiteProtector ベースライン**は、メイン SiteProtector System の要件を指します。
- **XGS サポート**は、 IBM Security Network Protection アプライアンスのポリシー編集に関する要件を指します。このポリシー編集には、一部の Microsoft オペレーティング・システムでのみサポートされている Internet Explorer v9 以上が必要です。
- **SP800-131A サポート**は、米国連邦情報・技術局 (NIST) が定義した厳重 (SP800-131A) 暗号化の要件を指します。厳重暗号化には、Internet Explorer v8 以上でのみサポートされている Transport Layer Security (TLS) v1.2 が必要です。Internet Explorer v8 以上は、一部の Microsoft オペレーティング・システムでのみサポートされています。

コンポーネント	最小要件	SP ベースライン	XGS サポート	SP800-131A サポート*
プロセッサー	Xeon 3000 シリーズまたは Core 2 Duo (最小) 3.00 GHz Intel Xeon E5450 (推奨)	✓	✓	✓

コンポーネント	最小要件	SP ベースライン	XGS サポート	SP800-131A サポート*
オペレーティング・システム SiteProtector は、Windows オペレーティング・システムの 32 ビット・バージョンと 64 ビット・バージョンの両方に対応しています。64 ビットのみのシステムには注が付いています。 **注:** SiteProtector とそのコンポーネントは、NTFS でフォーマットされたパーティションで実行する必要があります。FAT および FAT32 パーティションでは、システムを適切に強化できません。	Windows Server 2012 Standard[1] (64 ビットのみ)	✓	✓	✓
	Windows Server 2008 Standard	✓	✓	✓
	Windows Server 2008 R2 Standard (64 ビットのみ)	✓	✓	✓
	Windows Server 2008 Enterprise	✓	✓	✓
	Windows Server 2008 R2 Enterprise (64 ビットのみ)	✓	✓	✓
	Windows Server 2003 R2 Standard	✓	✓	
	Windows Server 2003 R2 Enterprise	✓	✓	
	Windows Server 2003 SP2 Standard	✓	✓	
	Windows Server 2003 SP2 Enterprise	✓	✓	
RAM	2 GB (最小) 4 GB (推奨)	✓	✓	✓
空きハード・ディスク・スペース	4 GB (最小) 20 GB (推奨)	✓	✓	✓
固定 IP アドレスか	はい	✓	✓	✓
サード・パーティー・ソフトウェア (付属しています)	IBM Java Runtime Environment (JRE) バージョン 1.7.0 SR2	✓	✓	✓
サード・パーティー・ソフトウェア (付属していません)	• Windows オペレーティング・システムのソフトウェアと Windows ベースのハードウェアの最新の更新については、Microsoft Update Web サイトhttp://www.windowsupdate.com	✓	✓	✓
専用システムか	はい	✓	✓	✓

コンポーネント	最小要件	SP ベースライン	XGS サポート	SP800-131A サポート*
その他の要件	以下の項目などのさまざまな要因に応じて追加されるメモリーおよびディスク・スペース。 • エージェントまたはアプライアンスの数 • 同時ユーザーの数 • エージェントまたはアプライアンスに実装されるポリシーのタイプ • イベント・ログ	✓	✓	✓

[1]Windows Server 2012 は、通常モードでインストールする必要があります。SiteProtector は、「コアのみ」のモードでインストールされた Windows Server 2012 をサポートしていません。

* 詳しくは 5 ページの『厳重 (SP800-131A) 暗号化の要件』を参照してください。

X-Press Update Server のシステム要件

以下の表で、X-Press Update Server のシステム要件について説明します。この表には次の構成の項目が含まれています。

- **SiteProtector ベースライン**は、メイン SiteProtector System の要件を指します。
- **XGS サポート**は、 IBM Security Network Protection アプライアンスのポリシー編集に関する要件を指します。このポリシー編集には、一部の Microsoft オペレーティング・システムでのみサポートされている Internet Explorer v9 以上が必要です。
- **SP800-131A サポート**は、米国連邦情報・技術局 (NIST) が定義した厳重 (SP800-131A) 暗号化の要件を指します。厳重暗号化には、Internet Explorer v8 以上でのみサポートされている Transport Layer Security (TLS) v1.2 が必要です。Internet Explorer v8 以上は、一部の Microsoft オペレーティング・システムでのみサポートされています。

コンポーネント	最小要件	SP ベースライン	XGS サポート	SP800-131A サポート
プロセッサー	Xeon 3000 シリーズまたは Core 2 Duo (最小) 3.00 GHz Intel Xeon E5450 (推奨)	✓	✓	✓

コンポーネント	最小要件	SP ベースライン	XGS サポート	SP800-131A サポート
オペレーティング・システム SiteProtector は、Windows オペレーティング・システムの 32 ビット・バージョンと 64 ビット・バージョンの両方に対応しています。64 ビットのみのシステムには注が付いています。 **注:** SiteProtector とそのコンポーネントは、NTFS でフォーマットされたパーティションで実行する必要があります。FAT および FAT32 パーティションでは、システムを適切に強化できません。	Windows Server 2012 Standard[1] (64 ビットのみ)	✓	✓	✓
	Windows Server 2008 R2 Standard (64 ビットのみ)	✓	✓	✓
	Windows Server 2008 R2 Enterprise (64 ビットのみ)	✓	✓	✓
	Windows Server 2008 Standard	✓	✓	
	Windows Server 2008 Enterprise	✓	✓	
	Windows Server 2003 R2 Standard	✓		
	Windows Server 2003 R2 Enterprise	✓		
	Windows Server 2003 SP2 Standard	✓		
	Windows Server 2003 SP2 Enterprise	✓		
RAM	512 MB (最小) 1 GB (推奨)	✓	✓	✓
空きハード・ディスク・スペース	9 GB (最小) 20 GB (推奨)	✓	✓	✓
固定 IP アドレスか	はい	✓	✓	✓
サード・パーティー・ソフトウェア (付属していません)	• Windows オペレーティング・システムのソフトウェアと Windows ベースのハードウェアの最新の更新については、Microsoft Update Web サイトhttp://www.windowsupdate.com	✓	✓	✓

[1]Windows Server 2012 は、通常モードでインストールする必要があります。SiteProtector は、「コアのみ」のモードでインストールされた Windows Server 2012 をサポートしていません。

第 3 章 SiteProtector のインストールの計画

スケーラビリティー・ガイドライン

この情報は、SiteProtector の初期デプロイメントを計画するとき、あるいは拡大するパフォーマンス要求に対応するために既存構成の拡張を計画するときに役立ちます。

デプロイメント・シナリオ

1 つのコンピューターからなる最小構成で SiteProtector System をデプロイするか、中規模または大規模ネットワーク向けに複数コンピューターからなる大型のデプロイメントを使用することができます。各デプロイメント・シナリオにはさまざまなハードウェアとソフトウェアの要件があります。SiteProtector のインストールおよび構成の方法を計画する際には、これらのシナリオを考慮してください。

最小デプロイメント

このシナリオは、実施できる最小の SiteProtector デプロイメントであり、必要なコンピューターは 1 台です。このデプロイメントは、小規模ネットワークやテスト環境に最も適しています。

アプローチ

SiteProtector の Express インストールを実行します。これにより、Application Server と SiteProtector Database が 1 台のコンピューターにインストールされます。

小規模デプロイメント

このシナリオで必要なコンピューターは 1 台のみですが、最小デプロイメントよりも高い性能を備えたコンピューターが必要です。

アプローチ

SiteProtector の Express インストールを実行します。これにより、Application Server と SiteProtector Database が 1 台のコンピューターにインストールされます。

中規模デプロイメント

このシナリオでは 3 台から 4 台のコンピューターが必要になります。

コンピューター 1

1 番目のコンピューターに SiteProtector Database をインストールします。

コンピューター 2

2 番目のコンピューターに Application Server をインストールします。Application Server のインストールでは、X-Press Update Server と Web コンソールもインストールされます。

また、2 番目のコンピューターには SiteProtector Console もインストールします。 SiteProtector Console のインストールでは、Event Viewer もインストールされます。

コンピューター 3 および 4

3 番目のコンピューターに Agent Manager コンポーネントと Event Collector コンポーネントをインストールし、4 番目のコンピューターには Agent Manager と Event Collector のペアを任意で追加インストールします。

© Copyright IBM Corp. 1994, 2013

大規模ネットワーク

このシナリオでは 4 台から 5 台のコンピューターが必要になります。

コンピューター 1
: 1 番目のコンピューターに SiteProtector Database をインストールします。

コンピューター 2
: 2 番目のコンピューターに Application Server をインストールします。Application Server のインストールでは、X-Press Update Server と Web コンソールもインストールされます。

  また、2 番目のコンピューターには SiteProtector Console もインストールします。 SiteProtector Console のインストールでは、Event Viewer もインストールされます。

コンピューター3、4、および 5
: 3 番目のコンピューターに Agent Manager コンポーネントと Event Collector コンポーネントをインストールし、4 番目と 5 番目のコンピューターには Agent Manager と Event Collector のペアを任意で追加インストールします。

パフォーマンスに関する考慮事項

SiteProtector System のパフォーマンスは、イベントのロード、複数のコンソール操作、長期にわたる分析照会、レポート生成など、多くの要因の影響を受けます。

サイトにおける 1 日当たりの平均イベント数と最大ハートビート数がここに示すガイドラインより常に多い場合、使用するエージェントの数に関係なく、サイトでパフォーマンス上の問題が発生している可能性があります。考えられる問題には以下のようなものがあります。

- コンソールの速度が遅くなるか、レスポンスしなくなる可能性がある。
- アクティビティーが構成の制約範囲内に収まるまで、データベースが新規イベントを一時的に受け入れられなくなる可能性がある。
- アクティビティーが構成の制約範囲内に収まるまで、データベースが非常に遅い速度でイベントを処理する可能性がある。

使用環境でのアクティビティーがデプロイメント・サイズの制約を超えている場合は、以下のガイドラインに従って、デプロイメントのサイズを調節することを検討してください。

パフォーマンスに影響する要因

次のいくつかの要因が SiteProtector の全体的なパフォーマンスとレスポンスに影響する場合があります。

- 複数のコンソール操作
- 長期にわたる分析照会
- レポートの生成
- フュージョン分析
- メンテナンス操作

Event Collector と Agent Manager のセットアップ

中規模および大規模のデプロイメントの場合、IBM Security では、Event Collector と Agent Manager を同じコンピューターにインストールすることを推奨しています。専用システムに Agent Manager をインストールする場合のシステム要件は、同じコンピューターを共有する Event Collector と Agent Manager にも適用されます。 Agent Manager の要件について詳しくは、5 ページの『第 2 章 ハードウェア要件とソフトウェア要件』を参照してください。

複数の Agent Manager と Event Collector を使用する場合

冗長性の確保など、エージェントの更新中に必要な帯域幅を増やすには、複数の Event Collector と Agent Manager のペアが必要になります。ただし、Agent Manager または Event Collector の数を増やしても、本書に示されているイベントとハートビートの限度は増えません。

中規模および大規模のデプロイメントの場合

パフォーマンスを最適化するには、データベース・サーバー上にインストールした Event Collector を冗長性確保の目的でのみ使用する必要があります。これにより、サーバー・リソースをデータベース・サービス専用にすることができ、パフォーマンスが向上する可能性があります。

パフォーマンスを最適化するには、Application Server 上の Agent Manager を冗長性確保の目的でのみ使用する必要があります。これにより、サーバー・リソースを Application Server サービス専用にすることができ、パフォーマンスが向上する可能性があります。

Proventia® Desktop Endpoint Security の Update Server

バージョン 9.0 以降の Proventia Desktop Endpoint Security には、ウィルス定義を頻繁に更新する必要がある、シグニチャー・ベースのアンチウィルスおよびアンチスパイウェア・スキャンが含まれます。このような更新に確実に対応できるようにするには、技術情報記事 (英語) の「*Number of Update Servers to Support AntiVirus Capability for Proventia Desktop 9.0 Agents*」(Technote 1435588) (https://www-304.ibm.com/support/docview.wss?uid=swg21435588) を参照してください。

推奨事項

ハードウェア、ソフトウェア、および空きディスク・スペースに関する推奨事項を示します。ここで示す推奨事項は標準的なお客様の環境に基づくものであり、環境によっては当てはまらない場合があります。

重要: 本書では、アクティブ・エージェント、イベント、ハートビート、およびその他の要因に関するサイジング基準について説明します。構成内のセンサーの数に関係なく、1 日当たりの平均イベント数および 1 日当たりの最大ハートビート数を超過しないようにしてください。

ハードウェアおよびソフトウェア

ハードウェアおよびソフトウェアに関する推奨事項は、以下の項目に基づいています。

項目	説明
サイトの最大アクティブ・エージェント数	この数は、サイト全体のアクティブ・エージェントの最大数を表しています。ここに示す推奨事項は、サイト全体のアクティブ・エージェントの総数がこの列の数を継続的に超過することはないことを前提としています。
サイトの 1 日当たりの最大イベント数	この数は、サイト全体の 1 日当たりの処理イベントの最大数を表しています。ここに示す推奨事項は、サイト全体の 1 日当たりのイベントの総数がこの列の数を継続的に超過することはないことを前提としています。
1 日当たりの最大ハートビート数	この数は、サイト全体のデータベースで処理される 1 日当たりのハートビートの最大数を表しています。ここに示す推奨事項は、サイト全体の 1 日当たりのハートビートの総数がこの列の数を継続的に超過することはないことを前提としています。

項目	説明
エージェントごとの 1 日当たりの最大推奨ハートビート数	この数は、サイト全体のエージェントごとの 1 日当たりのハートビートの最大数を表しています。ここに示す推奨事項は、サイト全体のエージェントごとの 1 日当たりの最大推奨ハートビート数がこの列の数を継続的に超過することはないことを前提としています。
最小ハートビート間隔 (秒 (時) 単位)	この数は、秒と時の両方の単位で示されるエージェントごとの最短ハートビート間隔を表しています。ここに示す推奨事項は、サイト全体のエージェントごとの最小ハートビート間隔がこの列の数より常に下回らないことを前提としています。
レスポンスのないエージェント・グループのしきい値 (分 (時) 単位)	この数は、ハートビートが受信されない場合に、エージェントがレスポンスなしと見なされるまでの時間のしきい値を分と時で指定します。
Event Collector と Agent Manager のペアの推奨追加数	この数は、特定のデプロイメント・シナリオにおける Event Collector と Agent Manager のペアの推奨追加数を指定します。

空きハード・ディスク・スペース

空きハード・ディスク・スペースに関する推奨事項は以下の項目に基づいています。

- 予期されるイベント・ボリューム
- 30 日間のイベント・データの保管に必要なスペース
- 90 日間のイベント・データの保管に必要なスペース
- 定期的なデータベース・メンテナンスの実行に必要なスペース

データベース・レイアウト

データベース・ファイルのレイアウトについては、Microsoft SQL Web サイト (英語) (http://www.microsoft.com/sql/) にアクセスしてください。

最小デプロイメント

SiteProtector System の最小規模デプロイメントは単一のコンピューターにインストールすることができます。これはテスト環境に最適です。このタスクは、Express インストールで実行できます。

環境

単一のコンピューターでの最小デプロイメントは、次の環境に適しています。

サイトの最大アクティブ・エージェント数	サイトの 1 日当たりの最大イベント数	1 日当たりの最大ハートビート数	エージェントごとの 1 日当たりの最大推奨ハートビート数	最小ハートビート間隔 (秒 (時) 単位)	レスポンスのないエージェント・グループのしきい値 (分 (時) 単位)	Event Collector と Agent Manager のペアの推奨追加数
500	50,000	1,000	2	43,200 (12)	720 (12)	0[a]

24 ページの『パフォーマンスに関する考慮事項』[a] トピックを参照してください。

ハードウェアおよびソフトウェア

以下の表に、最小デプロイメント向けのハードウェアおよびソフトウェアの推奨事項を示します。

項目	最小	推奨
プロセッサー	Xeon 3000 シリーズまたは Core 2 Duo	(1) 2.53 GHz Intel Xeon E5540
オペレーティング・システム	Windows Server 2003	Windows Server 2012[1]
SQL Server	SQL Server 2005	SQL Server 2012
RAM	1 GB	2 GB
OS および DBMS の空きハード・ディスク・スペース	18 GB	36 GB
30 日分の追加データの空きハード・ディスク・スペース	20 GB	38 GB
90 日分の追加データの空きハード・ディスク・スペース	23 GB	41 GB

[1]Windows Server 2012 は、通常モードでインストールする必要があります。SiteProtector は、「コアのみ」のモードでインストールされた Windows Server 2012 をサポートしていません。

注: 最小要件およびサポートされているすべてのオペレーティング・システムとデータベース・サーバーのリストについては、5 ページの『第 2 章 ハードウェア要件とソフトウェア要件』を参照してください。

小規模デプロイメント

SiteProtector System の小規模デプロイメントは単一のコンピューターにインストールすることができます。このタスクは、Express インストールで実行できます。

ここに示す小規模デプロイメントのハードウェアとソフトウェアの要件は、IBM Security SiteProtector System SP3001 アプライアンスと同等であることに注意してください。

SiteProtector System SP3001 アプライアンスの仕様については、IBM Security SiteProtector System データ・シート (http://www.ibm.com/common/ssi/cgi-bin/ssialias?subtype=SP&infotype=PM&appname=SWGE_WG_WG_USEN&htmlfid=WGD03013USEN&attachment=WGD03013USEN.PDF)を参照してください。

環境

小規模デプロイメントは次の環境に適しています。

サイトの最大アクティブ・エージェント数	サイトの 1 日当たりの最大イベント数	1 日当たりの最大ハートビート数	エージェントごとの 1 日当たりの最大推奨ハートビート数	最小ハートビート間隔 (秒 (時) 単位)	レスポンスのないエージェント・グループのしきい値 (分 (時) 単位)	Event Collector と Agent Manager のペアの推奨追加数
25,000	1,250,000	150,000	6	14,400 (4)	240 (4)	0[a]

[a] 24 ページの『パフォーマンスに関する考慮事項』のトピック『複数の Agent Manager と Event Collector を使用する場合』を参照してください。

ハードウェアおよびソフトウェア

以下の表に、小規模デプロイメント向けのハードウェアおよびソフトウェアの推奨事項を示します。

項目	推奨
プロセッサー	(1) 2.53 GHz Intel Xeon E5540 (8 MB キャッシュ搭載)
オペレーティング・システム	Windows Server 2012[1]
SQL Server	SQL Server 2012
RAM	12 GB
ハード・ディスク・ドライブ速度	10.5K RPM SAS
ハード・ディスク・ドライブ構成	RAID 1+0
OS および DBMS の空きハード・ディスク・スペース	36 GB
30 日分の追加データの空きハード・ディスク・スペース	52 GB
90 日分の追加データの空きハード・ディスク・スペース	157 GB

[1]Windows Server 2012 は、通常モードでインストールする必要があります。SiteProtector は、「コアのみ」のモードでインストールされた Windows Server 2012 をサポートしていません。

注: 最小要件およびサポートされているすべてのオペレーティング・システムとデータベース・サーバーのリストについては、5 ページの『第 2 章 ハードウェア要件とソフトウェア要件』を参照してください。

中規模デプロイメント

SiteProtector System の中規模デプロイメントでは、最低でも 3 台のコンピューターが必要になります。

中規模デプロイメントでは、SiteProtector System の機能を 3 台または 4 台のコンピューターに分割できます。

コンピューター	コンポーネント
1	Database
2	Application Server (Application Server のインストール済み環境には、 X-Press Update Server と Web コンソールが含まれます。)
3 と 4	Event Collector Agent Manager

環境

中規模デプロイメントは次の環境に適しています。

サイトの最大アクティブ・エージェント数	サイトの 1 日当たりの最大イベント数	1 日当たりの最大ハートビート数	エージェントごとの 1 日当たりの最大推奨ハートビート数	最小ハートビート間隔 (秒 (時) 単位)	レスポンスのないエージェント・グループのしきい値 (分 (時) 単位)	Event Collector と Agent Manager のペアの推奨追加数
50,000	5,000,000	300,000	6	14,400 (4)	240 (4)	2[a]

24 ページの『パフォーマンスに関する考慮事項』[a] トピックを参照してください。

ハードウェアおよびソフトウェア

以下の表に、中規模デプロイメント向けのハードウェアおよびソフトウェアの推奨事項を示します。

コンピューター	項目	推奨
1 (Database)	プロセッサー	(1) 3.00 GHz Intel Xeon E5450 (8 MB キャッシュ搭載)
	オペレーティング・システム	Windows Server 2012[1]
	SQL Server	SQL Server 2012
	RAM	8 GB
	データベース・ハード・ディスク構成	
	30 日間のデータベース使用量 (GB 単位)	176 GB
	90 日間のデータベース使用量 (GB 単位)	528 GB
	データベース・ハード・ディスク・ドライブ速度	15K RPM SCSI ディスク
	データベース・ハード・ディスク・ドライブ構成	RAID 5 / RAID 1+0
	データベース・ハード・ディスク・ドライブ・アクセス	2G+ ファイバー・チャネル SAN
2 (アプリケーション・サーバー)	プロセッサー	(1) 3.00 GHz Intel Xeon E5450 (8 MB キャッシュ搭載)
	オペレーティング・システム	Windows Server 2012[1]
	RAM	4 GB
	空きハード・ディスク・スペース	36 GB
	OS ハード・ディスク・ドライブ速度	10K RPM ディスク
	OS ハード・ディスク・ドライブ構成	RAID 1+0
3 および 4 (Event Collector/Agent Manager)	プロセッサー	(1) 3.00 GHz Intel Xeon E5450 (8 MB キャッシュ搭載)
	オペレーティング・システム	Windows Server 2012[1]
	RAM	2 GB
	空きハード・ディスク・スペース	36 GB

[1]Windows Server 2012 は、通常モードでインストールする必要があります。SiteProtector は、「コアのみ」のモードでインストールされた Windows Server 2012 をサポートしていません。

注: 最小要件およびサポートされているすべてのオペレーティング・システムとデータベース・サーバーのリストについては、5 ページの『第 2 章 ハードウェア要件とソフトウェア要件』を参照してください。

大規模デプロイメント

SiteProtector System の大規模デプロイメントでは、最低でも 4 台のコンピューターが必要になります。

大規模デプロイメントでは、SiteProtector System の機能を 5 台以上のコンピューターに分割できます。

コンピューター	コンポーネント
1	Database

コンピューター	コンポーネント
2	Application Server (Application Server のインストール済み環境には、 X-Press Update Server と Web コンソールが含まれます。)
3、4、および 5	Event Collector Agent Manager

環境

大規模デプロイメントは次の環境に適しています。

サイトの最大アクティブ・エージェント数	サイトの 1 日当たりの最大イベント数	1 日当たりの最大ハートビート数	エージェントごとの 1 日当たりの最大推奨ハートビート数	最小ハートビート間隔 (秒 (時) 単位)	レスポンスのないエージェント・グループのしきい値 (分 (時) 単位)	Event Collector と Agent Manager のペアの推奨追加数
100,000	5,000,000	600,000	6	14,400 (4)	240 (4)	3[a]

24 ページの『パフォーマンスに関する考慮事項』[a] トピックを参照してください。

ハードウェアおよびソフトウェア

以下の表に、大規模デプロイメント向けのハードウェアおよびソフトウェアの推奨事項を示します。

コンピューター	項目	推奨
1 (Database)	プロセッサー	(2) 3.00 GHz Intel Xeon E5450 (12 MB キャッシュ搭載)
	オペレーティング・システム	Windows Server 2012[1]
	SQL Server	SQL Server 2012
	RAM	8 GB
	データベース・ハード・ディスク構成	
	30 日間のデータベース使用量 (GB 単位)	176 GB
	90 日間のデータベース使用量 (GB 単位)	528 GB
	データベース・ハード・ディスク・ドライブ速度	15K RPM SCSI ディスク
	データベース・ハード・ディスク・ドライブ構成	RAID 5 / RAID 1+0
	データベース・ハード・ディスク・ドライブ・アクセス	2G+ ファイバー・チャネル SAN

コンピューター	項目	推奨
2 (アプリケーション・サーバー)	プロセッサー	(2) 3.00 GHz Intel Xeon E5450 (12 MB キャッシュ搭載)
	オペレーティング・システム	Windows Server 2012[1]
	RAM	8 GB
	空きハード・ディスク・スペース	36 GB
	OS ハード・ディスク・ドライブ速度	10K RPM ディスク
	OS ハード・ディスク・ドライブ構成	RAID 1+0
3、4、および 5 (Event Collector/Agent Manager)	プロセッサー	(1) 3.00 GHz Intel Xeon E5450 (12 MB キャッシュ搭載)
	オペレーティング・システム	Windows Server 2012[1]
	RAM	2 GB
	空きハード・ディスク・スペース	36 GB

[1]Windows Server 2012 は、通常モードでインストールする必要があります。SiteProtector は、「コアのみ」のモードでインストールされた Windows Server 2012 をサポートしていません。

注: 最小要件およびサポートされているすべてのオペレーティング・システムとデータベース・サーバーのリストについては、5 ページの『第 2 章 ハードウェア要件とソフトウェア要件』を参照してください。

複数サイトのデプロイメント

デプロイメントが大きくなりすぎる場合は、複数のサイトに分割することができます。

現在の構成が大きすぎる場合は、構成をより小さい複数のサイトに分割することを検討してください。小規模、中規模、および大規模のデプロイメント向けのガイドラインと要件は、サイトごとに最適なデプロイメントを選択する上で役立ちます。

複数サイトのデプロイメントは、サイト要約インスタンスにレポートする複数の大規模デプロイメントで構成されます。以下の条件が該当する場合は、複数サイトのデプロイメントを使用してください。

- 構成のサイジング基準が大規模デプロイメントに指定された数を超えている。
- 構成が広範な地理的領域に分散されている。

インストールに関する考慮事項

SiteProtector System をインストールする前に、さまざまな要因を考慮する必要があります。

インストール・オプション

SiteProtector インストール・オプションは多くの環境に適しています。『計画』セクションで詳しく説明します。

以下の表で、SiteProtector インストール・オプションについて説明します。

インストール・オプション	説明
Express	簡素化バージョンの SiteProtector を 1 台のコンピューターにインストールします。Express オプションは、テストまたは評価での使用と、小規模環境での使用を目的としています。

インストール・オプション	説明
手動インストール	3 台以上のコンピューターに SiteProtector をインストールできます。これにより、大規模な環境でのパフォーマンスが向上します。必要に応じてコンポーネントを追加できます。
クラスター化された SQL	2 台以上のコンピューターに SiteProtector をインストールし、クラスター化 SQL 環境で使用できるように SiteProtector を構成することができます。

ヒント: 上記のすべての SiteProtector インストールでは、Windows 認証または SQL 認証を使用できます。

Event Collector、Agent Manager、および SiteProtector Console はインストールに組み込まれています。Event Collector および Agent Manager は Site Database および Application Server と通信し、SiteProtector Console は Application Server と通信します。

インストール・プログラムの場所

SiteProtector には、基本的なインストール・パッケージ、アドオン・コンポーネント、およびモジュールのスタンドアロン・プログラムが用意されています。

スタンドアロン・プログラム

スタンドアロン・プログラム (パッケージとも呼ばれます) を使用して、SiteProtector コンポーネントを個別にインストールできます。これらのファイルはセントラル・ロケーションからインストールされないため、使用する場合は追加情報の入力が必要になります。

インストール・プログラムの場所

次のいずれかの場所から、Express インストール・プログラムにアクセスできます。

- IBM Security ダウンロード・センター (https://ibmss.flexnetoperations.com)。
- IBM パスポート・アドバンテージ - IBM パスポート・アドバンテージで販売されている一部の IBM Security 製品には、SiteProtector のソフトウェア・ダウンロードが含まれます。

IBM Security ダウンロード・センターは、Express インストール・プログラムおよびすべてのスタンドアロン・インストール・パッケージ (プログラム) の最新バージョンを提供しています。

インストールに関するその他の注意点

SiteProtector のインストール前に考慮する必要があるその他の要因について説明します。SiteProtector バージョン 3.0 の時点では、Deployment Manager はサポートされておらず、使用されない点に注意してください。

追加要件

システム要件以外に、以下の要件も満たす必要があります。

- SiteProtector を専用のコンピューターにインストールする。
- SiteProtector コンピューターを DNS サーバーやプロキシー・サーバーとして使用しない。
- 1 次またはバックアップ・ドメイン・コントローラーとしてセットアップされているシステム上に SiteProtector をインストールしない。

Express インストールのドメイン名

Express インストール時に最大 64 文字までの完全修飾ドメイン名を使用する必要があります。

ヒント: SiteProtector ドメイン名を設定するときには下線文字 (_) は使用しないでください。

暗号鍵のアーカイブ

以下のコンポーネントの暗号鍵をアーカイブすることができます。

- Agent Manager
- X-Press Update Server (スタンドアロン・バージョン)

これらのコンポーネントのインストールまたはアンインストール時に、アーカイブ・ディレクトリーを指定するようプロンプトが出されます。ローカル以外のロケーション (取り外し可能メディアを推奨) を指定してください。暗号鍵のアーカイブは、サーバーで障害が発生した場合の障害回復を単純化します。暗号鍵をアーカイブしない場合に、これらの鍵を使用するコンポーネントをアンインストールすると、これらの証明書が削除されます。そのため、このサーバーと通信するクライアントに証明書を再配布する必要があります。サーバー証明書の再配布にはかなりの時間と労力が必要になる場合があります。例えば、サーバーが、多数の Desktop Endpoint Security エージェントと通信する必要がある Agent Manager である場合です。これに該当するのは、クライアントでこのサーバーからの証明書を検証する必要がある場合のみです (「明示的な信頼」または「初回のみ信頼」オプション)。

暗号プロバイダーの選択のガイドライン

RSA は、すべての SiteProtector 通信のデフォルト暗号プロバイダーです。RSA は Microsoft オペレーティング・システムのデフォルトのプロバイダーであり、すべての IBM Security 製品でサポートされています。

重要: デフォルト以外の暗号プロバイダーがサポートされていないが、ご使用のコンピューターにインストールされている場合、これらのデフォルト以外の暗号プロバイダーを使用できます。したがって、お客様の責任において、これらのプロバイダーを構成して、SiteProtector と通信するエージェントおよびコンポーネントと互換性があることを確認する必要があります。

複数の IP アドレスとハード・ディスク

IP アドレスまたはハード・ディスクが複数ある場合:

- IP アドレスが複数ある場合: クライアント (他のコンピューター上のコンポーネント) がコンピューターとの通信に使用する IP アドレスを選択する必要があります。
- ハード・ディスクが複数ある場合: ハード・ディスクを指定する必要があります。

データベースへのユーザーの手動による追加

ユーザーを SQL Server または Site Database に手動で追加するには、Domain¥Username 形式を使用します。この作業に失敗すると、コンポーネントのインストール時にユーザー競合が発生する可能性があります。Windows 認証を使用するには、SiteProtector コンポーネントをインストールする前に、ユーザーを手動で追加する必要があります。

Microsoft Windows Server 2008

Microsoft Windows Server 2008 を実行している場合:

- 強化されたダウンロード・オプションを無効にします。デフォルトでは、Microsoft Windows Server ではブラウザーからプログラム・ファイルを開けないようになっています。インストール・プログラムは、ファイルを保存して、ローカル・ドライブで実行するようプロンプトを出します。リモート・ロケーションからインストール・プログラムを実行するには、このセキュリティー設定を無効にする必要があります。
- IBM Security ダウンロード・センターからファイルをダウンロードする前に、信頼済みサイト・リストに以下のサイトを追加します。
  - https://www.iss.net
  - http://www.iss.net

Windows リモート・デスクトップ

Windows リモート・デスクトップ (RDP) を使用するときには、RDP クライアント設定でフォント・スムージングが無効になっていることを確認してください。

SQL Server クラスター

SiteProtector Database は、SQL Server クラスターにインストールできる唯一の SiteProtector コンポーネントです。

インストール・プログラムによって生成される情報

インストール・プログラムによって、インストール・プロセスに関する情報を含むログ・ファイルが生成されます。この情報は、インストールの問題のトラブルシューティング時、または IBM サポートとの通信時に使用します。

ログ・ファイル

インストール・プログラムによって、インストール対象の SiteProtector コンポーネントごとにログ・ファイルが生成されます。また、インストール・プログラムによって、Site Database の特定の表にロードされるデータのバルク・コピーごとに詳細なログ・ファイルが作成されます。インストール・プログラムは、エラーまたは警告が発生している状態でインストール・プログラムが完了した場合に、これらのログを表示するようプロンプトを出します。

SiteProtector のインストールの準備

SiteProtector をインストールする前に、セキュリティーを強化し、SiteProtector のインストール先となるシステムを確実に保護するための対策を実施する必要があります。

セキュリティーに関する考慮事項

SiteProtector コンポーネントをシステムにインストールする前に、スクリーン・セーバーの有効化やインストールするアプリケーションの数の制限など、システム・セキュリティーを強化できる方法を考慮してください。

以下の対策を実施することでシステム・セキュリティーを強化できます。

- パスワード承認を使用するスクリーン・セーバーを有効にする。これは、SiteProtector が無許可で使用されないようにするのに役立ちます。
- SiteProtector System にインストールされるアプリケーションの数を制限する。

スクリーン・セーバー

スクリーン・セーバーを有効にする場合は、以下のガイドラインに従ってください。

- 空白画面のスクリーン・セーバーを使用します。空白のスクリーン・セーバーでは、他のスクリーン・セーバーほど多くの CPU またはメモリーを使用しません。
- タイムアウトの期間を短く設定します。
- スクリーン・セーバーをパスワードで保護します。

ヒント: 無許可アクセスを防ぐため、無人の場合はシステムをロックします。

アプリケーション数の制限

可能であれば、SiteProtector コンポーネントのインストール先となるシステムには追加アプリケーションをインストールしないでください。アプリケーションを追加すると、セキュリティー・リスクが生じる可能性があります。

厳重な (SP800-131A) 暗号セキュリティーに関する考慮事項

米国連邦情報・技術局 (NIST) Special Publication 800-131A (SP800-131A) 標準は、セキュリティーを改善するためにアルゴリズムを強化し、鍵の長さを増しています。SiteProtector コンポーネントをシステムにインストールする前に、厳重暗号化のために SP800-131A 標準に準拠する必要があるかどうかを決定してください。

SP800-131A 標準では、新しい標準に移行するための移行期間も設定されています。この移行期間により、ユーザーは、この標準の下でサポートされない設定とサポートされる設定が混在した環境で実行できるようになります。SP800-131A 標準では、この標準の厳重な適用に向けてユーザーが構成されている必要があります。詳しくは、米国連邦情報・技術局の Web サイト (http://www.nist.gov/index.html) を参照してください。

SP800-131A 標準に準拠するには、コンポーネントが以下の基準を満たしている必要があります。

- SiteProtector コンポーネント間のセキュア通信のために Transport Layer Security (TLS) v1.2 を使用している。Secure Sockets Layer (SSL) が TLS v1.2 プロトコルを使用する必要があります。
- SHA-256 またはこれより強力なハッシュ関数を使用している。
- 2048 ビットまたはこれより強度が高い RSA 鍵を使用している。

注: 強力な暗号に対応している IBM Security エージェント・タイプについては、技術情報記事 1636383 (http://www.ibm.com/support/docview.wss?uid=swg21636383) を参照してください。

注: SP800-131A 標準に準拠する厳重モードは、SiteProtector アプライアンスではサポートされていません。

厳重暗号化と互換暗号化の選択

SiteProtector v3.0 Express インストールまたは SiteProtector v3.0 コンポーネント・インストールを実行するときには、厳重暗号化と互換暗号化のいずれかを選択する必要があります。

- *厳重* とは、プロトコル TLS v1.2、SHA-256 以上の強力なハッシュ関数、および 2048 ビット以上の強度の RSA 鍵のみを使用することを意味します。
- *互換* とは、プロトコル TLS v1.0、TLS v1.1、または TLS v1.2 のいずれか、SHA-1 ハッシュ関数、および 2048 ビット強度の RSA 鍵を使用することを意味します。

状況に応じて、次の 2 種類の暗号化シナリオが考えられます。

- 厳重: すべてのデバイスが SP800-131A 標準を使用するように構成されている。
- 互換: すべてのデバイスが SP800-131A 標準を使用するように構成されていない。

注: 厳重モードと互換モードの混合はサポートされていません。

さまざまなインストール

SP800-131A に関連して 3 種類のインストール・シナリオが考えられます。

インストール・シナリオ	プロセス
古いバージョンの SiteProtector (v2.9 など) を SiteProtector v3.0 にアップグレードする	この状況では SP800-131A 標準はサポートされません。SP800-131A 機能を導入するため、v3.0 の SiteProtector の再インストールを実行する必要があります。
SiteProtector v3.0 Express インストールを実行する	インストール・プロセスで厳重暗号化と互換暗号化のいずれかを選択する必要があります。
SiteProtector v3.0 コンポーネント・インストールを実行する	インストール・プロセスで、コンポーネントごとに厳重暗号化または互換暗号化のいずれを使用するかを選択する必要があります。 **重要:** 1 番目のコンポーネントについて選択した内容が、同じコンピューターにインストールされるそれ以降のすべてのコンポーネントに自動的に適用されます。

Internet Explorer での TLS v1.2 の設定

SiteProtector で厳重 (SP800-131A) 暗号化を使用する場合は、Transport Layer Security (TLS) v1.2 を使用するように Internet Explorer を設定する必要があります。TLS v1.2 は Internet Explorer v 8 以上でのみサポートされています。

このタスクについて

Internet Explorer は SiteProtector System でサポートされているブラウザーです。TLS v1.2 をサポートしている Internet Explorer のバージョンを次に示します。

- Microsoft Windows 7: IE v8 以上
- Microsoft Windows 8: IE v10
- Windows Server 2008 R2 Standard (64 ビットのみ): IE v8 以上
- Windows Server 2008 R2 Enterprise (64 ビットのみ): IE v8 以上
- Windows Server 2012 Standard: IE v10

手順

1. Internet Explorer を開きます。
2. 「**ツール**」 > 「**インターネット オプション**」を選択します。
3. 「**詳細設定**」タブを選択します。
4. 「**セキュリティ**」セクションにスクロールします。
5. 厳重暗号化を使用するため、「**TLS 1.2 を使用する**」チェック・ボックスにチェック・マークを付けます。

注: 厳重暗号化を使用して SiteProtector に接続する目的で**のみ** Internet Explorer を使用し、その他のサイトへの接続には Internet Explorer を使用**しない**場合は、以下のチェック・ボックスのチェック・マークを外します。

- **SSL 2.0 を使用する**
- **SSL 3.0 を使用する**
- **TLS 1.0 を使用する**
- **TLS 1.1 を使用する**

この操作を行うと、TLS v1.2 をサポートしていない他のサイトはこれ以降接続しなくなります。

6. 「**OK**」をクリックします。

セキュア通信を行うための SiteProtector データベースの IPsec の構成

SiteProtector で厳重 (SP800-131A) 暗号化を使用する場合は、セキュア通信のために SiteProtector データベースとその他の SiteProtector コンポーネントの間で IPsec を構成する必要があります。この機能を使用するには、Windows ファイアウォールを使用する必要があります。

このタスクについて

注: セキュア通信を行うための SiteProtector データベースの IPsec の構成は、SiteProtector アプライアンスではサポートされていません。

重要: SiteProtector データベースの IPsec を構成するには、Windows ファイアウォールが有効になっている必要があります。IBM Security Server Protection for Windows を使用している場合は、デフォルトで Windows ファイアウォールが開始しないように設定されているため、IBM Security Server Protection for Windows をアンインストールするか、またはエージェント・サービスを手動で無効にしてから、Windows ファイアウォールを有効にする必要があります。

SiteProtector データベースとその他の SiteProtector コンポーネント間でのセキュア通信のための IPsec の構成手順については、技術情報記事 1638945 (http://www.ibm.com/support/docview.wss?uid=swg21638945) を参照してください。

Site Database システムの準備

Microsoft SQL Server ソフトウェアは、最新の SiteProtector イベント情報を整理して保守する際に役立つ強力なデータベース照会アプリケーションです。ただし、 SQL Server を使用すると、特定のタイプの攻撃に対してシステムがぜい弱になる可能性があります。 Site Database システム (または SQL Server がインストールされている別のシステム) に SiteProtector をインストールする前に、システムが正しく準備されていることを確認してください。

手順

1. Microsoft Windows の最新の更新を適用します。 更新は Microsoft Web サイト (http://www.microsoft.com) からダウンロードできます。
2. SQL Server のセキュリティーを強化します。

SiteProtector コンポーネントのインストール先となるシステムの準備

SiteProtector コンポーネントをインストールする前に、システムが正しく準備されていることを確認します。

手順

1. Microsoft Service Pack とホット・フィックスをインストールします。
2. 最新バージョンの Microsoft Internet Explorer と関連するすべてのパッチがインストールされていることを確認します。
3. パスワード承認を使用するスクリーン・セーバーが有効になっていることを確認します。

Microsoft 更新のインストール

潜在的なセキュリティー上の欠陥を修正するには、最新の Service Pack、ホット・フィックス、およびセキュリティー・パッチを適用して、Microsoft Windows オペレーティング・システムを更新します。更新を適用する場合は、変更制御をテストして実行する品質保証などのベスト・プラクティスに従ってください。

Microsoft 更新

Microsoft では、Service Pack、ホット・フィックス、およびセキュリティー・パッチなど、さまざまなタイプの更新を提供しています。

Service Pack
: 既知の問題を修正し、製品機能を拡張するツール、ドライバー、および更新を提供する累積的な更新。

ホット・フィックス
: 問題発生時に個々のお客様に提供される製品のコード・パッチ。より厳しいテストを受けるホット・フィックスのグループは、定期的に Service Pack に取り込まれます。

セキュリティー・パッチ
: ホット・フィックスに似ているが、実際にセキュリティーのぜい弱性を除去するコード・パッチ。セキュリティー・パッチはウィルスや攻撃者から構成を保護するため、できる限り早急にインストールしてください。

Microsoft 更新のダウンロード

このタスクについて

最新の Microsoft パッチを Microsoft の Web サイト (http://www.microsoft.com) からダウンロードします。この Web サイトからは重要な更新パッケージの通知サービスもダウンロードできます。このサービスをインストールすると、重要な更新が自動的に通知されます。

Microsoft 更新の管理

このタスクについて

インターネットにアクセスできない場合に更新を管理するためのユーティリティーが、Microsoft からいくつか提供されています。以下の表に示すユーティリティーを使用して、ダウンロードする更新、およびコンピューターにインストールした後の更新の管理方法を判別してください。

ユーティリティー	説明
HFNetChk	特定のコンピューターに適用されていないホット・フィックスを識別します。 **ヒント:** このユーティリティーは冗長モード (-v サフィックス) で実行します。

ユーティリティー	説明
QChain	ホット・フィックスが正しい順序でインストールされたかどうかを検証します。 **ヒント:** QChain は -z サフィックスを指定して実行します。
Qfecheck	ホット・フィックスが正しくインストールされたかどうかを検証します。 **ヒント:** このユーティリティーは冗長モード (-v サフィックス) で実行します。

インストールのチェックリスト

この章では、サイトで必要なタスクを理解し、そのタスクを効率的に実行できることを確認する上で役立つプロセスの概要とチェックリストを示します。

推奨

IBM Security では、このセクションのチェックリストをコピーし、それを使用して進行状況を追跡することを推奨しています。チェック・ボックスを使用して、完了したタスクにチェック・マークを付けるか、状況に当てはまらないタスクは線を引いて消してください。

インストール前のチェックリスト

SiteProtector をインストールする前に、一定の要件を満たし、いくつかのセットアップ・タスクを完了する必要があります。このトピックでは、これらのタスクを完了する上で役立つチェックリストを示します。

チェックリスト

以下の表に、SiteProtector をインストールする前に必要なタスクをすべて実行したかどうかを確認するためのチェックリストを示します。

✓	タスク
☐	SiteProtector に追加する計画のエージェントのライセンスを購入し、ライセンス・ファイルをインストールで使用できるようにする。 **注:** これらのファイルを受け取っていない場合は、mailto://licenses@iss.net にメールを送信してください。
☐	使用するコンピューターがシステム要件を満たしていることを確認する。
☐	SQL Server の管理者特権を含む、SiteProtector コンポーネントのインストール先となる各コンピューターの管理者特権を取得する。
☐	使用するインストール・オプションを決定する。
☐	インストールする SiteProtector リリースに適用される README 文書を読む。
☐	必要なサード・パーティー・ソフトウェアと最新のパッチをインストールする。 必要なサード・パーティー・ソフトウェアのリストについては、『*SiteProtector System の要件*』を参照してください。
☐	Windows および SQL Server ソフトウェアを強化する。
☐	信頼済みサイト・リストに以下のサイトを追加します。 • https://www.iss.net • http://www.iss.net
☐	Internet Explorer を使用して、Application Server にインターネット接続をセットアップする。

✓	タスク
□	リモート・ロケーションまたは取り外し可能メディアでの暗号鍵の保管など、暗号鍵のアーカイブ方針を策定する。

必要な情報のチェックリスト

このトピックでは、本書のインストール手順を完了するために必要になる可能性のある情報のチェックリストを示します。このチェックリストを見直して、情報を用意してあることを確認してからインストール・プロセスを開始してください。

重要: インストールする特定のプログラムの追加情報が必要になる場合があります。この情報は各トピックにリストされています。

チェックリスト

以下の表に、SiteProtector をインストールする前に取得する必要がある情報のチェックリストを示します。

✓	インストール・プログラムの情報
□	複数サイトまたは複数コンポーネント環境でサイトまたはコンポーネントを区別するためのそれらの固有名。
□	SiteProtector のインストール先の各コンピューターの IP アドレスまたは完全修飾ドメイン名。
□	次のいずれかの形式の Site Database コンピューターの完全修飾 SQL Server 名: • *ComputerName* • *ComputerName¥NamedInstance* • *ComputerName.DomainName.com* • *ComputerName.DomainName.com¥NamedInstance*
□	複数のドライブが使用可能な場合に、SiteProtector コンポーネントのインストール先となるコンピューター・ドライブ。
□	コンピューター上に複数のネットワーク・インターフェース・カードがある場合は、他の SiteProtector コンポーネントがインストール対象のコンポーネントとの通信で使用する IP アドレスを把握しておく必要があります。

Express オプションのインストール・タスク・リスト

Express オプションでは、1 台のコンピューターに SiteProtector System をインストールします。

タスクの概要

以下の表に、Express オプションをインストールするために完了する必要があるタスクの概要を示します。

タスク	説明
1	IBM Security ダウンロード・センター (https://ibmss.flexnetoperations.com)。から SiteProtector Express セットアップ・プログラム・ファイル (`SiteProtectorExpress-Setup.exe`) をダウンロードします。
2	Express オプションをインストールします。
3	SiteProtector のインストール先となるコンピューターで TCP/IP プロトコルが有効であることを確認します。
4	IBM Security ダウンロード・センターからオプションのモジュールをダウンロードしてインストールします。Event Archiver の構成については、「*IBM Security SiteProtector System 構成ガイド*」を参照してください。

SiteProtector パッケージのインストール・タスク・リスト

このトピックでは、個々の SiteProtector パッケージをインストールするために実行する必要がある手順のタスク概要を示します。

以下のタスクを実行する計画の場合は、この方法を使用します。

- SQL Server データベースでの Windows NT の認証
- SQL Server クラスター環境でのインストール
- Express オプション以外の構成での SiteProtector コンポーネントのインストール

タスクの概要

以下の表に、Windows NT 認証インストール・タスクのチェックリストを示します。

タスク	説明
1	IBM Security ダウンロード・センターからパッケージのインストール・ファイルにアクセスします。
2	Site Database をインストールします。
3	次の順序でパッケージをインストールします。 1. Java ランタイム環境 2. Application Server (X-Press Update Server と Web Console を含む) 3. Console (Event Viewer を含む) 4. Event Collector 5. Agent Manager
4	オプションのモジュール (追加の X-Press Update Server や Event Archiver など) をインストールします。Event Archiver の構成については、「*IBM Security SiteProtector System 構成ガイド*」を参照してください。

インストール後のタスク

以下のタスクは、SiteProtector コンポーネントがセキュアに通信できることを確認する際に役立ちます。以下のタスクは、SiteProtector とオプションのモジュールをインストールしてから、SiteProtector を構成する前に実行します。

タスクの概要

以下の表に、オプションであるインストール後のタスクのリストを示します。

タスク	説明
1	データベース通信を保護します。
2	ファイアウォールを介した通信を有効にします。 「*IBM Security SiteProtector System SiteProtector Traffic のファイアウォールの構成*」資料 (http://publib.boulder.ibm.com/infocenter/sprotect/v2r8m0/topic/com.ibm.siteprotector.doc/pdfs/sp_printable_pdfs.htm で入手可) を参照してください。

次のステップ

SiteProtector をインストールしたら、SiteProtector セットアップ・プロセスを完了する必要があります。このプロセス中に、初めて SiteProtector を使用する際に必要な以下のすべてのタスクを実行します。

- ライセンス/トークンの追加
- SiteProtector エージェントの構成
- SiteProtector エージェントの更新
- SiteProtector ユーザーと権限のセットアップ
- ネットワーク・アセットのグループのセットアップ
- SiteProtector と共に使用する他の IBM Security 製品のセットアップ
- セキュリティー・ポリシーとレスポンスの構成
- SiteProtector へのネットワーク・アセットの追加

このプロセスのガイド情報と手順については、「*IBM Security SiteProtector System 構成ガイド*」および「*IBM Security SiteProtector System ポリシーおよびレスポンス構成ガイド*」を参照してください。

第 4 章 SiteProtector のインストール

この章では、SiteProtector のインストールで使用するオプションと手順について説明します。

Express インストールを使用した最小デプロイメントまたは小規模デプロイメントのインストール

Express インストールを使用して最小デプロイメントまたは小規模デプロイメントをインストールできます。インストールされる SiteProtector のバージョンは、評価目的、テスト目的、または最小環境での使用に最も適しています。デフォルトの SiteProtector コンポーネントがすべて含まれています。IBM Security ダウンロード・センターから Express インストールをダウンロードできます。

Express インストール実行の準備

Express インストールでは、コンピューター上の既存の SQL Server データベースを使用します。

このタスクについて

コンピューター上の既存の SQL Server データベースが最新のものでない場合は、以下のアクションのいずれかを実行してから、Express インストールを再実行する必要があります。

- データベースを最小要件にアップグレードします。
- 最小要件を満たしていないデータベース・インスタンスをアンインストールします。

Express オプションをインストールする前に、以下のようにします。

- IBM Security ダウンロード・センター (https://ibmss.flexnetoperations.com)。から SiteProtector Express セットアップ・プログラム・ファイル (`SiteProtectorExpress-Setup.exe`) をダウンロードします。
- 対象のコンピューターに 2 つ以上の SQL Server インスタンスがある場合は、Site Database のインストール先となるインスタンスを選択する必要があります。
- 英語以外の言語バージョンの SQL Server をインストールする場合は、最初にそれをインストールしてから Express インストールを実行する必要があります。

TCP/IP 経由の SQL Server Express 通信の有効化

デフォルトでは、SQL Server 2012 Express® データベースは TCP/IP プロトコル経由で通信するように構成されていません。SQL Server Express を使用する Site Database をインストールする場合、Site Database が正しく機能できるように、事前に TCP/IP プロトコルを有効にする必要があります。

手順

1. 「スタート」メニューで「**すべてのプログラム**」 > 「**Microsoft SQL Server 2012**」 > 「**構成ツール**」 > 「**SQL Server 構成マネージャー**」をクリックします。
2. 「**SQL Server 2012 Services**」をクリックします。
3. 「**SQL Server 2012 Network Configuration**」ノードを展開してから、「**Protocols for MSSQLServer *(SQL Instance Name)***」を選択します。
4. 「**TCP/IP**」を右クリックしてから、「**使用可能**」をクリックします。
5. ツリーで「**SQL Server 2012 Services**」を選択します。

© Copyright IBM Corp. 1994, 2013

6. 「**SQL Server** ***(SQL Instance Name)***」を右クリックしてから、「**再起動**」をクリックします。

Express インストールの実行

IBM Security ダウンロード・センター (https://ibmss.flexnetoperations.com)。から Express インストールをダウンロードできます。

始める前に

SQL Server インスタンスをインストールしていない場合は、作業を続行する前に、サポートされているバージョンの SQL Server をインストールする必要があります。サポートされている SQL サーバーのバージョンのリストについては、6 ページの『SiteProtector Express インストールのシステム要件』を参照してください。

手順

1. `SiteProtectorExpress-Setup.exe` ファイルを実行します。 「ようこそ」ウィンドウが表示されます。
2. 「**次へ**」をクリックします。 「言語の選択」ウィンドウが表示されます。
3. SiteProtector で使用する言語を選択します。
4. 「**次へ**」をクリックします。 「ご使用条件」ウィンドウが表示されます。
5. ご使用条件を確認し、「**同意する**」をクリックしてから「**次へ**」をクリックします。 「宛先の場所の選択」ウィンドウが表示されます。
6. デフォルトのフォルダーを選択するか、「開く」ウィンドウでフォルダーを選択してから、「**次へ**」をクリックします。 「暗号セキュリティー標準」ウィンドウが表示されます。
7. SiteProtector を互換暗号化モードまたは厳重暗号モードのいずれで実行するかを選択します。 「サイト名」ウィンドウが表示されます。
8. 作成するサイトの名前を入力してから、「**次へ**」をクリックします。

   ヒント: マルチサイト環境でこのサイトと他のサイトを区別するために分かりやすい名前を選択してください。
9. SQL Server のウィンドウが表示された場合は、Site Database のインストール先となる SQL Server インスタンスを選択してから、「**次へ**」をクリックします。
10. 「暗号鍵のアーカイブ」ウィンドウで、「**フォルダー**」ロケーションを入力してから「**次へ**」をクリックします。 ネットワークや zip ドライブなどの、非ローカル・メディア上のフォルダーを指定します。
11. 「InstallShield ウィザードの完了」ウィンドウで、「**完了**」をクリックします。

    注: デフォルトでは、インストール・プログラムによって、SiteProtector Console アイコンが自動的に作成され、デスクトップ・フォルダーに配置されます。SiteProtector Console アイコンを作成しない場合は、チェック・ボックスをクリアしてください。

次のタスク

注: Windows ドメイン・アカウントを使用して Site Database にアクセスする計画の場合は、SQL Server を実行するために適切な権限を持つドメイン・アカウントとして実行するように SQL Server と SQL エージェントのサービスを構成する必要があります。正確な要件については、SQL Server の資料を参照してください。

中規模 SiteProtector デプロイメントのインストール

3 台から 4 台のコンピューターに中規模 SiteProtector デプロイメントをインストールするには、以下の手順に従います。中規模 SiteProtector デプロイメントには、Site Database、Application Server、X-Press Update Server、Web Console、Event Viewer、Event Collector、および Agent Manager が含まれています。

始める前に

28 ページの『中規模デプロイメント』トピックと、『計画』セクションにあるハードウェアおよびソフトウェアの要件に関するトピックで詳しく説明する要件に、ご使用のコンピューターが対応していることを確認してください。

SiteProtector コンポーネントのインストール先となる各コンピューターの管理者特権 (Microsoft SQL Server の管理者特権を含む) を取得します。

インストール・プロセスを開始する前に、以下の情報を確認して書きとめておいてください。

- SiteProtector サイトに使用する名前。
- SiteProtector コンポーネントのインストール先となる各コンピューターの IP アドレスまたは完全修飾ドメイン名。
- 次のいずれかの形式の Site Database コンピューターの完全修飾 SQL Server 名:
  - *ComputerName*
  - *ComputerName¥NamedInstance*
  - *ComputerName.DomainName.com*
  - *ComputerName.DomainName.com¥NamedInstance*
- Application Server、Event Collector、および Agent Manager をインストールする場合は、Windows ドメイン・ユーザーの認証資格情報を入力する必要があります。ドメイン名とユーザー名を指定してください。例えば、*SP_domain¥SP_User_Name* のように指定します。
- サービスを実行する権限が付与されている Windows ドメイン・ユーザーの認証資格情報。
- サーバーの公開鍵管理者の追加ユーザー名。
- 複数のドライブが使用可能な場合は、SiteProtector コンポーネントをインストールするコンピューター・ドライブを把握しておく必要があります。
- コンピューターに複数のネットワーク・インターフェース・カード (NIC) がある場合は、他の SiteProtector コンポーネントがインストール対象コンポーネントとの通信で使用する IP アドレスを把握しておく必要があります。
- プロキシーを使用する場合は、インターネットのプロキシー情報とエージェント・マネージャーのプロキシー情報が必要です。

手順

1. IBM Security ダウンロード・センター (https://ibmss.flexnetoperations.com)。にアクセスします。
2. IBM Security ダウンロード・センターにログインし、「My Software」ヘッダーの「**Download**」をクリックします。
3. 「My Products」の下にある「**IBM Security SiteProtector System**」をクリックします。
4. 「Product Lines」の下にある「**SiteProtector 3.0**」をクリックします。
5. 「**Installation Packages**」リンクをクリックします。
6. IBM Security ダウンロード・センターから次に示すファイルを既知の場所にダウンロードします。

オプション	説明
SiteProtectorJRE-Setup.exe	Java ランタイム環境 (JRE)
SiteDatabase-Setup.exe	SiteProtector Database
ApplicationServer-Setup.exe	Application Server (X-Press Update Server と Web Console を含む)
Console-Setup.exe	Console (Event Viewer を含む)
EventCollector-Setup.exe	Event Collector
AgentManager-Setup.exe	Agent Manager

7. 1 番目のコンピューターで `SiteDatabase-Setup.exe` を実行し、必要なすべての情報を入力します。

   注: Windows ドメイン・アカウントを使用して Site Database にアクセスする計画の場合は、SQL Server を実行するために適切な権限を持つドメイン・アカウントとして実行するように SQL Server と SQL エージェントのサービスを構成する必要があります。正確な要件については、SQL Server の資料を参照してください。
   SiteProtector Database がインストールされます。
8. 2 番目のコンピューターで `SiteProtectorJRE-Setup.exe` を実行し、Java ランタイム環境をインストールします。
9. 2 番目のコンピューターで `ApplicationServer-Setup.exe` を実行し、必要なすべての情報を入力します。 Application Server、X-Press Update Server、および Web Console が 2 番目のコンピューターにインストールされます。
10. 2 番目のコンピューターで `Console-Setup.exe` を実行し、必要なすべての情報を入力します。
    Console と Event Viewer が 2 番目のコンピューターにインストールされます。
11. 3 番目のコンピューターで `SiteProtectorJRE-Setup.exe` を実行し、Java ランタイム環境をインストールします。
12. 3 番目のコンピューターで `EventCollector-Setup.exe` を実行し、必要なすべての情報を入力します。
    Event Collector が 3 番目のコンピューターにインストールされます。
13. 3 番目のコンピューターで `AgentManager-Setup.exe` を実行し、必要なすべての情報を入力します。
    Agent Manager が 3 番目のコンピューターにインストールされます。
14. Event Collector と Agent Manager を 4 番目のコンピューターにインストールする場合は、`SiteProtectorJRE-Setup.exe` を実行して Java ランタイム環境をインストールします。
15. オプション: 4 番目のコンピューターで `EventCollector-Setup.exe` を実行し、必要なすべての情報を入力します。
16. オプション: 4 番目のコンピューターで `AgentManager-Setup.exe` を実行し、必要なすべての情報を入力します。

次のタスク

これで、IBM Security ダウンロード・センターからオプション・コンポーネント (追加の X-Press Update Server (`UpdateServer-Setup.exe`) や Event Archiver (`EventArchiver-Setup.exe`) など) をダウンロードしてインストールできます。 Event Archiver の構成については、「*IBM Security SiteProtector System 構成ガイド*」を参照してください。

大規模 SiteProtector デプロイメントのインストール

4 台から 5 台のコンピューターに大規模 SiteProtector デプロイメントをインストールするには、以下の手順に従います。大規模 SiteProtector デプロイメントには、Site Database、Application Server、X-Press Update Server、Web Console、Event Viewer、Event Collector、および Agent Manager が含まれています。

始める前に

29 ページの『大規模デプロイメント』トピックと、『計画』セクションにあるハードウェアおよびソフトウェアの要件に関するトピックで詳しく説明する要件に、ご使用のコンピューターが対応していることを確認してください。

SiteProtector コンポーネントのインストール先となる各コンピューターの管理者特権 (Microsoft SQL Server の管理者特権を含む) を取得します。

インストール・プロセスを開始する前に、以下の情報を確認して書きとめておいてください。

- SiteProtector サイトに使用する名前。
- SiteProtector コンポーネントのインストール先となる各コンピューターの IP アドレスまたは完全修飾ドメイン名。
- 次のいずれかの形式の Site Database コンピューターの完全修飾 SQL Server 名:
  - *ComputerName*
  - *ComputerName¥NamedInstance*
  - *ComputerName.DomainName.com*
  - *ComputerName.DomainName.com¥NamedInstance*
- Application Server、Event Collector、および Agent Manager をインストールする場合は、Windows ドメイン・ユーザーの認証資格情報を入力する必要があります。ドメイン名とユーザー名を指定してください。例えば、*SP_domain¥SP_User_Name* のように指定します。
- サービスを実行する権限が付与されている Windows ドメイン・ユーザーの認証資格情報。
- サーバーの公開鍵管理者の追加ユーザー名。
- 複数のドライブが使用可能な場合は、SiteProtector コンポーネントをインストールするコンピューター・ドライブを把握しておく必要があります。
- コンピューターに複数のネットワーク・インターフェース・カード (NIC) がある場合は、他の SiteProtector コンポーネントがインストール対象コンポーネントとの通信で使用する IP アドレスを把握しておく必要があります。
- プロキシーを使用する場合は、インターネットのプロキシー情報とエージェント・マネージャーのプロキシー情報が必要です。

手順

1. IBM Security ダウンロード・センター (https://ibmss.flexnetoperations.com)。にアクセスします。
2. IBM Security ダウンロード・センターにログインし、「My Software」ヘッダーの「**Download**」をクリックします。
3. 「My Products」の下にある「**IBM Security SiteProtector System**」をクリックします。
4. 「Product Lines」の下にある「**SiteProtector 3.0**」をクリックします。
5. 「**Installation Packages**」リンクをクリックします。
6. IBM Security ダウンロード・センターから次に示すファイルを既知の場所にダウンロードします。

オプション	説明
SiteProtectorJRE-Setup.exe	Java ランタイム環境 (JRE)
SiteDatabase-Setup.exe	SiteProtector Database
ApplicationServer-Setup.exe	Application Server (X-Press Update Server と Web Console を含む)
Console-Setup.exe	Console (Event Viewer を含む)
EventCollector-Setup.exe	Event Collector
AgentManager-Setup.exe	Agent Manager

7. 1 番目のコンピューターで `SiteDatabase-Setup.exe` を実行し、必要なすべての情報を入力します。

   注: Windows ドメイン・アカウントを使用して Site Database にアクセスする計画の場合は、SQL Server を実行するために適切な権限を持つドメイン・アカウントとして実行するように SQL Server と SQL エージェントのサービスを構成する必要があります。正確な要件については、SQL Server の資料を参照してください。
   SiteProtector Database がインストールされます。
8. 2 番目のコンピューターで `SiteProtectorJRE-Setup.exe` を実行し、Java ランタイム環境をインストールします。
9. 2 番目のコンピューターで `ApplicationServer-Setup.exe` を実行し、必要なすべての情報を入力します。 Application Server、X-Press Update Server、および Web Console が 2 番目のコンピューターにインストールされます。
10. 2 番目のコンピューターで `Console-Setup.exe` を実行し、必要なすべての情報を入力します。
    Console と Event Viewer が 2 番目のコンピューターにインストールされます。
11. 3 番目のコンピューターで `SiteProtectorJRE-Setup.exe` を実行し、Java ランタイム環境をインストールします。
12. 3 番目のコンピューターで `EventCollector-Setup.exe` を実行し、必要なすべての情報を入力します。
    Event Collector が 3 番目のコンピューターにインストールされます。
13. 3 番目のコンピューターで `AgentManager-Setup.exe` を実行し、必要なすべての情報を入力します。
    Agent Manager が 3 番目のコンピューターにインストールされます。
14. 4 番目のコンピューターで `SiteProtectorJRE-Setup.exe` を実行し、Java ランタイム環境をインストールします。
15. 4 番目のコンピューターで `EventCollector-Setup.exe` を実行し、必要なすべての情報を入力します。
    Event Collector が 4 番目のコンピューターにインストールされます。
16. 4 番目のコンピューターで `AgentManager-Setup.exe` を実行し、必要なすべての情報を入力します。
    Agent Manager が 4 番目のコンピューターにインストールされます。
17. Event Collector と Agent Manager を 5 番目のコンピューターにインストールする場合は、`SiteProtectorJRE-Setup.exe` を実行して Java ランタイム環境をインストールします。
18. オプション: 5 番目のコンピューターで `EventCollector-Setup.exe` を実行し、必要なすべての情報を入力します。
19. オプション: 5 番目のコンピューターで `AgentManager-Setup.exe` を実行し、必要なすべての情報を入力します。

次のタスク

これで、IBM Security ダウンロード・センターからオプション・コンポーネント (追加の X-Press Update Server (`UpdateServer-Setup.exe`) や Event Archiver (`EventArchiver-Setup.exe`) など) をダウンロードし

てインストールできます。 Event Archiver の構成については、「*IBM Security SiteProtector System 構成ガイド*」を参照してください。

SQL Server クラスターでの SiteProtector のインストール

SQL Server クラスターでは、SQL 認証または Windows 認証のいずれかを使用できます。暗黙的なトラストは使用できません。以下で説明する手順は、SQL 認証と Windows 認証の両方に適用されます。

始める前に

『計画』セクションのデプロイメント・タイプを説明するトピックとハードウェア要件およびソフトウェア要件に関するトピックで詳しく説明する要件に、ご使用のコンピューターが対応していることを確認してください。

SiteProtector コンポーネントのインストール先となる各コンピューターの管理者特権 (Microsoft SQL Server の管理者特権を含む) を取得します。

インストール・プロセスを開始する前に、以下の情報を確認して書きとめておいてください。

- SiteProtector サイトに使用する名前。
- SiteProtector コンポーネントのインストール先となる各コンピューターの IP アドレスまたは完全修飾ドメイン名。
- 次のいずれかの形式の Site Database コンピューターの完全修飾 SQL Server 名:
  - *ComputerName*
  - *ComputerName¥NamedInstance*
  - *ComputerName.DomainName.com*
  - *ComputerName.DomainName.com¥NamedInstance*
- Application Server、Event Collector、および Agent Manager をインストールする場合は、Windows ドメイン・ユーザーの認証資格情報を入力する必要があります。ドメイン名とユーザー名を指定してください。例えば、*SP_domain¥SP_User_Name* のように指定します。
- サービスを実行する権限が付与されている Windows ドメイン・ユーザーの認証資格情報。
- サーバーの公開鍵管理者の追加ユーザー名。
- 複数のドライブが使用可能な場合は、SiteProtector コンポーネントをインストールするコンピューター・ドライブを把握しておく必要があります。
- コンピューターに複数のネットワーク・インターフェース・カード (NIC) がある場合は、他の SiteProtector コンポーネントがインストール対象コンポーネントとの通信で使用する IP アドレスを把握しておく必要があります。
- プロキシーを使用する場合は、インターネットのプロキシー情報とエージェント・マネージャーのプロキシー情報が必要です。

手順

1. IBM Security ダウンロード・センター (https://ibmss.flexnetoperations.com)。にアクセスします。
2. IBM Security ダウンロード・センターにログインし、「My Software」ヘッダーの「**Download**」をクリックします。
3. 「My Products」の下にある「**IBM Security SiteProtector System**」をクリックします。
4. 「Product Lines」の下にある「**SiteProtector 3.0**」をクリックします。
5. 「**Installation Packages**」リンクをクリックします。

6. IBM Security ダウンロード・センターから次に示すファイルを既知の場所にダウンロードします。

オプション	説明
SiteProtectorJRE-Setup.exe	Java ランタイム環境 (JRE)
SiteDatabase-Setup.exe	SiteProtector Database
ApplicationServer-Setup.exe	Application Server (X-Press Update Server と Web Console を含む)
Console-Setup.exe	Console (Event Viewer を含む)
EventCollector-Setup.exe	Event Collector
AgentManager-Setup.exe	Agent Manager

7. すべてのクラスター・ノードに SSL 証明書をインストールします。

   注: SSL 証明書のインストールについて詳しくは、以下の Microsoft Web ページのいずれかを参照してください。

   - 『[プロトコルの暗号化を設定する] オプションが有効になっている場合の SQL Server における証明書の使用』(http://support.microsoft.com/kb/318605/ja-jp)
   - 『Microsoft 管理コンソールで SQL Server 用に SSL 暗号化を有効にする方法』(http://support.microsoft.com/kb/316898/ja-jp)
   - SQL Server 2008 および 2008 R2 の SSL 暗号化を有効にする方法 (http://technet.microsoft.com/en-us/library/ms189067%28v=sql.105%29.aspx)
   - SQL Server 2012 用に SSl 暗号化を有効にする方法 (http://technet.microsoft.com/en-us/library/ms191192%28v=sql.110%29.aspx)

8. プロンプトに従い、必要なすべての情報を入力して、`SiteDatabase-Setup.exe` パッケージから SiteProtector Database をインストールします。

   重要: クラスター化された SQL がインストールされているコンピューターには、SiteProtector Database 以外のものをインストールしないでください。

   注: Windows ドメイン・アカウントを使用して Site Database にアクセスする計画の場合は、SQL Server を実行するために適切な権限を持つドメイン・アカウントとして実行するように SQL Server と SQL エージェントのサービスを構成する必要があります。正確な要件については、SQL Server の資料を参照してください。

9. 2 番目のコンピューターで `SiteProtectorJRE-Setup.exe` を実行し、Java ランタイム環境をインストールします。
10. 2 番目のコンピューターで `ApplicationServer-Setup.exe` を実行し、必要なすべての情報を入力します。

    注: Application Server では、Site Database と通信するために SSL 証明書が必要になります。Application Server のインストール・プログラムは、クラスター・プラットフォームでのインストールを検証し、必要な SSL 証明書を検査します。証明書が無効な場合、SSL はオフになります。Application Server、X-Press Update Server、および Web Console が 2 番目のコンピューターにインストールされます。

11. 2 番目のコンピューターで `Console-Setup.exe` を実行し、必要なすべての情報を入力します。Console と Event Viewer が 2 番目のコンピューターにインストールされます。
12. 3 番目のコンピューターで `SiteProtectorJRE-Setup.exe` を実行し、Java ランタイム環境をインストールします。

13. 3 番目のコンピューターで `EventCollector-Setup.exe` を実行し、必要なすべての情報を入力します。Event Collector が 3 番目のコンピューターにインストールされます。
14. 3 番目のコンピューターで `AgentManager-Setup.exe` を実行し、必要なすべての情報を入力します。Agent Manager が 3 番目のコンピューターにインストールされます。
15. Event Collector と Agent Manager を 4 番目のコンピューターにインストールする場合は、`SiteProtectorJRE-Setup.exe` を実行して Java ランタイム環境をインストールします。
16. オプション: 4 番目のコンピューターで `EventCollector-Setup.exe` を実行し、必要なすべての情報を入力します。
17. オプション: 4 番目のコンピューターで `AgentManager-Setup.exe` を実行し、必要なすべての情報を入力します。

次のタスク

これで、IBM Security ダウンロード・センターからオプション・コンポーネント (追加の X-Press Update Server (`UpdateServer-Setup.exe`) や Event Archiver (`EventArchiver-Setup.exe`) など) をダウンロードしてインストールできます。 Event Archiver の構成については、「*IBM Security SiteProtector System 構成ガイド*」を参照してください。

64 ビット・プラットフォームでの SiteProtector のインストール

SiteProtector は Windows 64 ビット・プラットフォームまたは SQL Server Enterprise 64 ビット・プラットフォームにインストールできます。以下で説明する手順は、SQL 認証と Windows 認証の両方に適用されます。

このタスクについて

注: システムはすべて同じドメインに存在する必要があり、Windows ドメイン・アカウントを使用する必要があります。

64 ビット・プラットフォームに SiteProtector をインストールするには、次のいずれかの手順を実行します。

- 43 ページの『Express インストールを使用した最小デプロイメントまたは小規模デプロイメントのインストール』
- 45 ページの『中規模 SiteProtector デプロイメントのインストール』
- 47 ページの『大規模 SiteProtector デプロイメントのインストール』
- 49 ページの『SQL Server クラスターでの SiteProtector のインストール』

Windows NT 認証を使用する場合の SiteProtector のインストール

Windows NT 認証を使用するネットワークに SiteProtector をインストールする場合は、コンポーネントをそれぞれ個別にインストールする必要があります。IBM Security ダウンロード・センター (https://ibmss.flexnetoperations.com)。 からコンポーネントのインストール・パッケージを取得することができます。

始める前に

以下の情報が必要になります。

- SQL Server 名

- サービスを実行する権限を持つ Windows NT ユーザーの認証資格情報
- アプリケーション・サーバー名
- サーバーの Public Key Administrator の追加ユーザー名
- サイト名
- Agent Manager のロケーション
- Agent Manager の認証アカウント名とパスワード

  注: これにより、Agent Manager と対話するためのアカウントが X-Press Update Server で作成されます。
- (オプション) SiteProtector グループ名
- インターネットのプロキシー情報
- Agent Manager のプロキシー情報

Event Collector をインストールする前に、SiteProtector JRE をインストールする必要もあります。

注: Windows ドメイン・アカウントを使用して Site Database にアクセスする計画の場合は、SQL Server を実行するために適切な権限を持つドメイン・アカウントとして実行するように SQL Server と SQL エージェントのサービスを構成する必要があります。正確な要件については、SQL Server の資料を参照してください。

このタスクについて

個々のパッケージは次の順序でインストールする必要があります。

1. Site Database
2. Java ランタイム環境
3. Application Server (X-Press Update Server と Web Console を含む)
4. Console (Event Viewer を含む)
5. Event Collector
6. Agent Manager
7. その他のパッケージ (追加の X-Press Update Server や Event Archiver など)

手順

1. IBM Security ダウンロード・センター (https://ibmss.flexnetoperations.com) からコンポーネント・パッケージをダウンロードします。
2. 小規模、中規模、または大規模のデプロイメントのインストール手順に従ってください。ネットワークのサイズに最適なデプロイメントを選択してください。

第 5 章 追加コンポーネントのインストール

別の Console、Event Collector、Agent Manager、X-Press Update Server、Event Viewer など、追加コンポーネントをインストールできます。Event Archiver をインストールすることもできます。

追加コンポーネントの概要

SiteProtector コンポーネントがどのように連動するかを理解することは重要です。

以下の図はコンポーネント間の依存関係を示しています。初期インストール後にインストールされた追加コンポーネントは、以下の図では破線で表されています。

© Copyright IBM Corp. 1994, 2013

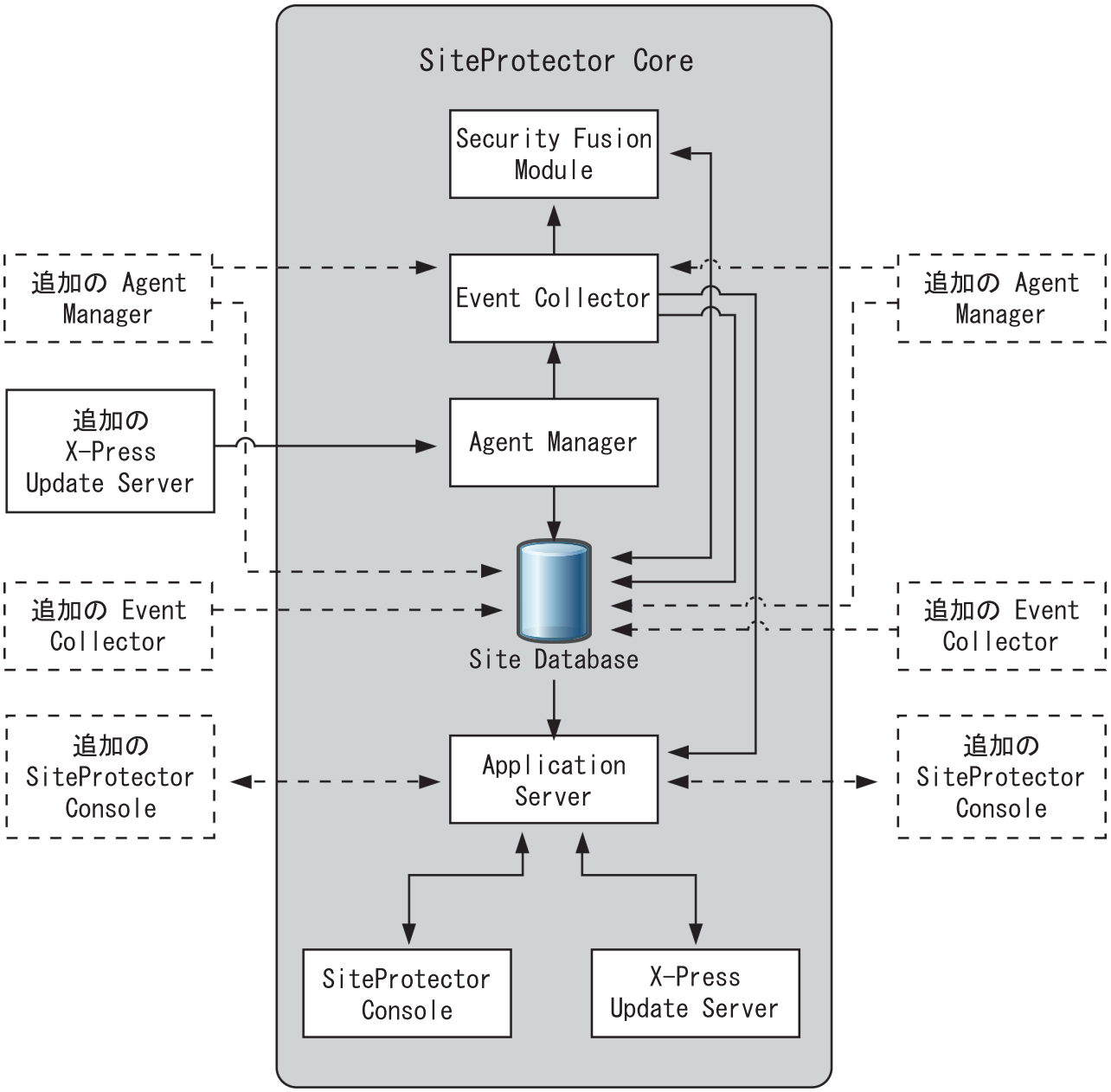

図 2. SiteProtector コンポーネントとイベント・フロー

以下の表に、インストール可能な追加コンポーネントのリストを示し、インストールする理由を簡単に説明します。

コンポーネント	追加インストールの理由
Agent Manager	• 多数のエージェントのスケーリングを行う。 • ネットワークがさまざまな地理的位置に分割されている。
Console	複数のユーザーに SiteProtector をモニターするための独自の Console を提供する。
Event Collector	現行の Event Collector でさらにエージェントを使用できるようにサポートする。Express インストールでは 1 つの Event Collector がインストールされます。

コンポーネント	追加インストールの理由
Event Viewer	他の SiteProtector コンポーネントがインストールされていないコンピューター上のイベントをモニターする。
Event Archiver	イベント・データを保管し、Site Database で保管する必要があるイベントの数を減らしてパフォーマンスを向上させる。
X-Press Update Server	X-Press Update Server をクラスター化し、パフォーマンスを向上させ、フェイルオーバーを提供する。

追加の Console のインストール

SiteProtector をインストールしたら、追加の SiteProtector Console をインストールできます。これにより、複数のユーザーが SiteProtector をリモートでモニターできるようになります。追加の SiteProtector Console をインストールすると、追加の Event Viewer も自動的にインストールされます。

手順

1. IBM Security ダウンロード・センター (https://ibmss.flexnetoperations.com)。にアクセスします。
2. IBM Security ダウンロード・センターにログインし、「My Software」ヘッダーの「**Download**」をクリックします。
3. 「My Products」の下にある「**IBM Security SiteProtector System**」をクリックします。
4. 「Product Lines」の下にある「**SiteProtector 3.0**」をクリックします。
5. 「**Installation Packages**」リンクをクリックします。
6. `Console-Setup.exe` パッケージを既知の場所にダウンロードします。
7. `Console-Setup.exe` を実行します。
8. インストール・プロンプトに従い、必要なすべての情報を入力します。 Console と Event Viewer がコンピューターにインストールされます。

追加の Event Collector のインストール

ご使用の環境で追加エージェントをサポートする場合は、追加の Event Collector のインストールを検討してください。追加の Event Collector をインストールしたら、エージェントをリダイレクトする必要があります。

始める前に

Event Collector をインストールする前に、Java ランタイム環境 (JRE) をインストールする必要があります。

手順

1. IBM Security ダウンロード・センター (https://ibmss.flexnetoperations.com)。にアクセスします。
2. IBM Security ダウンロード・センターにログインし、「My Software」ヘッダーの「**Download**」をクリックします。
3. 「My Products」の下にある「**IBM Security SiteProtector System**」をクリックします。
4. 「Product Lines」の下にある「**SiteProtector 3.0**」をクリックします。
5. 「**Installation Packages**」リンクをクリックします。

6. `SiteProtectorJRE-Setup.exe` パッケージと `EventCollector-Setup.exe` パッケージを既知の場所にダウンロードします。
7. `SiteProtectorJRE-Setup.exe` を実行して Java ランタイム環境をインストールします。
8. `EventCollector-Setup.exe` を実行します。
9. インストール・プロンプトに従い、必要なすべての情報を入力します。 Event Collector がコンピューターにインストールされます。
10. エージェントを Event Collector にリダイレクトします。
    a. エージェントを選択します。
    b. 「**アクション**」 > 「**エージェントの構成**」 > 「**Event Collector の割り当て**」を選択します。「Event Collector の割り当て」ウィンドウが表示されます。
    c. 新たにインストールした Event Collector を選択してから、「**OK**」をクリックします。

追加の Agent Manager のインストール

ご使用の環境に多数のエージェントが含まれている場合、またはご使用の環境がさまざまな地理的位置に分割されている場合は、追加の Agent Manager のインストールを検討してください。Agent Manager の各インスタンスはそれぞれ別々のシステムにインストールする必要があります。

始める前に

Agent Manager をインストールする前に、Java ランタイム環境 (JRE) をインストールする必要があります。

このタスクについて

環境でネットワーク・アドレス変換 (NAT) を使用する場合は、インストール・プログラムが IP アドレスを入力するようプロンプトを出したときに、Agent Manager にカスタムの IP アドレスを割り当てることを検討してください。ネットワーク・インターフェース・カード (NIC) に現在割り当てられている IP アドレスのリストを無効にするオプションを選択し、「**カスタム IP アドレス**」フィールドに IP アドレスを入力する必要があります。

手順

1. IBM Security ダウンロード・センター (https://ibmss.flexnetoperations.com)。にアクセスします。
2. IBM Security ダウンロード・センターにログインし、「My Software」ヘッダーの「**Download**」をクリックします。
3. 「My Products」の下にある「**IBM Security SiteProtector System**」をクリックします。
4. 「Product Lines」の下にある「**SiteProtector 3.0**」をクリックします。
5. 「**Installation Packages**」リンクをクリックします。
6. `SiteProtectorJRE-Setup.exe` パッケージと `AgentManager-Setup.exe` パッケージを既知の場所にダウンロードします。
7. `SiteProtectorJRE-Setup.exe` を実行して Java ランタイム環境をインストールします。
8. `AgentManager-Setup.exe` を実行します。
9. インストール・プロンプトに従い、必要なすべての情報を入力します。 Agent Manager がコンピューターにインストールされます。

追加の Event Viewer のインストール

別の Event Collector と Application Server に正常に接続できる場合は、他の SiteProtector コンポーネントがインストールされていないシステムに Event Viewer をインストールすることができます。これにより、セキュリティー・イベント情報にほぼリアルタイムにアクセスできるようになります。(Express インストールでは、Console と同じシステムに Event Viewer が自動的にインストールされます。)

手順

1. IBM Security ダウンロード・センター (https://ibmss.flexnetoperations.com)。にアクセスします。
2. IBM Security ダウンロード・センターにログインし、「My Software」ヘッダーの「**Download**」をクリックします。
3. 「My Products」の下にある「**IBM Security SiteProtector System**」をクリックします。
4. 「Product Lines」の下にある「**SiteProtector 3.0**」をクリックします。
5. 「**Installation Packages**」リンクをクリックします。
6. `SiteProtectorJRE-Setup.exe` パッケージと `EventViewer-Setup.exe` パッケージを既知の場所にダウンロードします。
7. `SiteProtectorJRE-Setup.exe` を実行して Java ランタイム環境をインストールします。
8. `EventViewer-Setup.exe` を実行します。
9. インストール・プロンプトに従い、必要なすべての情報を入力します。 Event Viewer がコンピューターにインストールされます。

追加 XPU Server のインストール

追加の X-Press Update (XPU) Server をインストールするには、次の手順に従います。

始める前に

重要: Agent Manager がインストールされている同じコンピューターに XPU Server をインストールしないでください。インストールすると、Agent Manager のパフォーマンスに関して問題が発生する場合があります。

手順

1. IBM Security ダウンロード・センター (https://ibmss.flexnetoperations.com) にアクセスします。
2. IBM Security ダウンロード・センターにログインし、「My Software」ヘッダーの「**Download**」をクリックします。
3. 「My Products」の下にある「**IBM Security SiteProtector System**」をクリックします。
4. 「Product Lines」の下にある「**SiteProtector 3.0**」をクリックします。
5. 「**Installation Packages**」リンクをクリックします。
6. `UpdateServer-Setup.exe` パッケージを既知の場所にダウンロードします。
7. `UpdateServer-Setup.exe` を実行します。 「InstallShield ウィザードへようこそ」ウィンドウが表示されます。
8. 「**次へ**」をクリックします。 「ご使用条件」ウィンドウが表示されます。
9. ご使用条件を確認し、「**同意する**」をクリックしてから「**次へ**」をクリックします。 「宛先の場所の選択」ウィンドウが表示されます。

10. インストール先フォルダーを選択し、「**次へ**」をクリックします。 「X-Press Update Server の構成 (Agent Manager の場所の指定)」ウィンドウが表示されます。
11. 以下のフィールドに入力し、「**次へ**」をクリックします。

フィールド	説明
名前	XPU Server が接続する Agent Manager の名前。 **例:** AgentManager_100
アドレス (IP または DNS)	Agent Manager が配置されている場所の IP アドレスまたは DNS。
ポート	XPU Server が Agent Manager と通信するために使用するポート (3995 がデフォルト・ポートです)。
アカウント名	XPU Server が Agent Manager と通信を開始するときに使用するユーザー名。
パスワード	XPU Server が Agent Manager と通信を開始するときに使用するパスワード。

「X-Press Update Server の構成 (SiteProtector グループ名の指定)」ウィンドウが表示されます。

12. 以下のフィールドに入力し、「**次へ**」をクリックします。

フィールド	説明
SiteProtector グループ名	XPU Server を追加するグループの名前。 このフィールドをブランクのままにすると、SiteProtector System により XPU Server は「未グループ化アセット」に追加されます。
X-Press Update Server セキュリティー・モード	以下のいずれかを選択します。 • すべて信頼する: 他のサーバーは、接続を試行するたびに XPU Server に接続できます。認証のために証明書は使用されません。 • 初回のみ信頼: 他のサーバーは、この XPU Server に 1 回のみ接続できます。初回の接続後、XPU Server は、接続サーバーの証明書を使用して以後のすべての接続を認証します。 • 明示的な信頼: この XPU Server は、ローカル証明書を使用して XPU Server に接続するサーバーを認証する必要があります。
1 次 IP	ローカル・コンピューターに複数のネットワーク・インターフェースがある場合、XPU Server 通信に使用する IP アドレスを選択します。
アドレス (IP または DNS)	XPU Server がファイアウォールまたはプロキシー・サーバーを通じてアクセスする必要がある場合は、そのファイアウォールまたはプロキシー・サーバーの IP アドレスまたは DNS を入力します。
ポート	XPU Server がファイアウォールまたはプロキシー・サーバーにアクセスするときに使用するポート。

「アーカイブ: 秘密鍵のアーカイブ」ウィンドウが表示されます。

13. 「**フォルダー**」ボックスに、秘密鍵をアーカイブする場所を入力し、「**次へ**」をクリックします。

    ヒント: IBM Security では、鍵はリムーバブル・メディアにアーカイブすることが推奨されています。

    プログラムの「インストールの準備完了」ウィンドウが表示されます。
14. 「**インストール**」をクリックします。 「InstallShield ウィザードの完了」ウィンドウが表示されます。
15. 「**完了**」をクリックします。

タスクの結果

追加の X-Press Update Server がコンピューターにインストールされました。

Event Archiver のインストール

イベント・データをアーカイブしてデータベース・パフォーマンスを強化するために、Event Archiver をインストールできます。Event Archiver により、Site Database で保管する必要があるイベントの数が減ります。(Event Archiver はすべての SiteProtector 価格プランに含まれているわけではありません。)

始める前に

以下の情報が必要になります。

- Agent Manager のインストール先のシステムのホスト名または IP アドレス
- アプリケーション・サーバー名
- (オプション) Agent Manager のアカウント名とパスワード
- (オプション) SiteProtector グループ名

手順

1. IBM Security ダウンロード・センター (https://ibmss.flexnetoperations.com)。にアクセスします。
2. IBM Security ダウンロード・センターにログインし、「My Software」ヘッダーの「**Download**」をクリックします。
3. 「My Products」の下にある「**IBM Security SiteProtector System**」をクリックします。
4. 「Product Lines」の下にある「**SiteProtector 3.0**」をクリックします。
5. 「**Installation Packages**」リンクをクリックします。
6. `EventArchiver-Setup.exe` パッケージを既知の場所にダウンロードします。
7. 「**Installation Packages**」リンクをクリックします。
8. `EventArchiver-Setup.exe` を実行します。
9. インストール・プロンプトに従い、必要なすべての情報を入力します。 Event Archiver がコンピューターにインストールされます。

第 6 章 インストールの問題のトラブルシューティング

失敗したインストールのトラブルシューティング

このタスクについて

SiteProtector の標準インストールがどのように機能するかが分かっていれば、失敗したインストールを修正するプロセスを理解しやすくなります。

- Site Database のインストールに失敗した場合、インストール・プログラムは他のいずれのコンポーネントもインストールしません。
- Site Database 以外のコンポーネントのインストールに失敗した場合、インストール・プログラムは選択されている他のコンポーネントを引き続きインストールします。

失敗したインストールを修正するには、以下のようにコンポーネントを再インストールする必要があります。

- Site Database の場合、SiteProtector の各コンポーネントをアンインストールしてから再インストールします。

  注意:
  Site Database のみを再インストールすると、SiteProtector はインストール前の状態に戻りません。
- Site Database 以外の各コンポーネントの場合、そのコンポーネントのインストール・プログラムを再実行します。
- 複数のコンポーネントのインストールに失敗した場合は、必ず正しい順序でコンポーネントを再インストールしてください。

インストールの問題

このセクションには、一般的なインストールの問題とその解決方法についての情報が含まれています。

issApp ログインが既に存在する

Application Server のインストール時に、Application Server ログイン issApp が既に存在していることを示すエラーが表示されてから、インストール・プロセスが強制終了されます。

問題

通常、これは Application Server のインストールを、アンインストールが正常に行われなかった状態で試行した場合に発生します。アンインストール・プロセス時に Application Server サービスまたは Sensor Controller サービスを停止できない場合、issApp ログインはまだ使用中であるため、Site Database から削除できません。

解決策

1. 両方のサービス (またはアプリケーション (稼働している場合)) が停止していることを確認します。
2. SQL Server 2005/2008/2012 Management Studio を使用して、既存の issApp ログイン (Site Database の `/Security/Logins` フォルダーにあります) を手動で削除します。

© Copyright IBM Corp. 1994, 2013

Event Collector ログインを削除できない

Event Collector のアンインストール時に、サービスが稼働中であるために `EventCollector_<machine>` ログインを削除できないことを示すエラーが表示されてから、アンインストール・プロセスが強制終了されます。

以下のタスクのいずれかを実行します。

- Site Database をアンインストールする場合は、そのデータベースをアンインストールしてから、Event Collector のアンインストール・プロセスを繰り返します。
- Site Database をアンインストールしない場合は、issDaemon サービスを停止してから、Event Collector のアンインストール・プロセスを繰り返します。アンインストール・プロセスは続行されるが、ログインがまだ存在することを示す警告が表示される場合は、SQL Server 2005/2008/2012 Management Studio を使用して、既存の **EventCollector_<computer>** ログイン (Site Database の `/Security/Logins` フォルダーにあります) を手動で削除します。

関連タスク:

63 ページの『SiteProtector コンポーネントのアンインストール』
SiteProtector コンポーネントをアンインストールする場合は、以下の手順に従ってください。

Event Collector を停止できない

Application Server と Console を削除しましたが、Event Collector を停止できません。

以下のタスクのいずれかを実行します。

- Site Database を削除します。
- Site Database を削除しない場合は、IBM サポートに連絡し、Event Collector の手動による停止について支援を求めてください。

関連タスク:

63 ページの『SiteProtector コンポーネントのアンインストール』
SiteProtector コンポーネントをアンインストールする場合は、以下の手順に従ってください。

データベースが使用中である

Site Database のアンインストール時に、データベースが使用中であることを示すエラーが表示されます。

SQL Server 2005/2008/2012 Management Studio を使用して、Site Database に関連付けられているすべてのプロセスを手動で停止してから、データベースをアンインストールします。

関連タスク:

63 ページの『SiteProtector コンポーネントのアンインストール』
SiteProtector コンポーネントをアンインストールする場合は、以下の手順に従ってください。

第 7 章 アンインストール

SiteProtector コンポーネントのアンインストール

SiteProtector コンポーネントをアンインストールする場合は、以下の手順に従ってください。

手順

1. タスクバーの「**開始**」をクリックしてから、「**プログラム**」 > 「**ISS**」 > 「**SiteProtector**」 > 「**Uninstall SiteProtector**」を選択します。 「コンポーネントの選択」ダイアログが表示されます。
2. 削除するコンポーネントを選択してから、「**アンインストール**」をクリックします。 メッセージに選択したコンポーネントがリストされます。
3. 「**はい**」をクリックします。
4. 「SQL ログイン・パスワード」ウィンドウが表示された場合は、以下のいずれかのアクションを実行します。
   - データベースを削除しなかった場合は、SQL ログオン用のユーザー ID とパスワードを入力します。
   - データベースを削除しなかった場合、または正しくないパスワード以外の理由でデータベースにコンポーネントを接続できない場合は、「**データベースに接続しない**」チェック・ボックスを選択します。
5. プログラムでコンポーネントが正常に削除されない場合は、以下のいずれかのアクションを実行します。
   - コンポーネントの削除を初めて試行した場合は、ステップ 1 に移動し、コンポーネントのアンインストールを再試行します。
   - コンポーネントの削除を複数回試行した場合は、「はい」をクリックしてログ・ファイルを表示し、さらに支援が必要であれば、IBM サポートに連絡してください。
6. 「**OK**」をクリックしてから、コンピューターを再起動します。

関連資料:

62 ページの『Event Collector ログインを削除できない』
Event Collector のアンインストール時に、サービスが稼働中であるために `EventCollector_<machine>` ログインを削除できないことを示すエラーが表示されてから、アンインストール・プロセスが強制終了されます。

62 ページの『Event Collector を停止できない』
Application Server と Console を削除しましたが、Event Collector を停止できません。

62 ページの『データベースが使用中である』
Site Database のアンインストール時に、データベースが使用中であることを示すエラーが表示されます。

SiteProtector のアンインストール

このトピックでは、SiteProtector を完全に削除する方法について説明します。ほとんどの場合、SiteProtector コンポーネントはすべて同時に削除する必要があります。

© Copyright IBM Corp. 1994, 2013

このタスクについて

コンポーネントを削除する順序が重要です。

重要: 以下の手順に従って「スタート」メニューから「**SiteProtector のアンインストール**」を選択してコンポーネントを削除する場合、アンインストール・プログラムによりコンポーネントが正しい順番で自動的に削除されます。

コンポーネントを Windows のコントロール・パネルから削除する場合は、以下の順序で削除する必要があります。

1. SiteProtector Console
2. X-Press Update Server
3. Agent Manager
4. Application Server
5. Event Collector
6. SecurityFusion Module
7. Site Database

複数のコンピューターに SiteProtector をインストールした場合は、コンピューターごとに順次コンポーネントを削除してください。

手順

1. タスクバーの「**開始**」をクリックしてから、「**プログラム**」 > 「**ISS**」 > 「**SiteProtector**」 > 「**Uninstall SiteProtector**」を選択します。
2. インストール済みのコンポーネントをすべて選択してから、「**アンインストール**」をクリックします。SiteProtector のインストール・メッセージに、削除対象として選択したコンポーネントがリストされます。
3. 「**はい**」をクリックします。 コンポーネントが正常に削除されたことを示すメッセージが表示されます。
4. プログラムでコンポーネントが正常に削除されない場合は、以下のいずれかのアクションを実行します。
   - コンポーネントの削除を初めて試行した場合は、ステップ 1 からステップ 3 を繰り返し、コンポーネントの削除を再試行します。
   - コンポーネントの削除を複数回試行した場合は、「はい」をクリックしてログ・ファイルを表示します。さらに支援が必要な場合は、IBM サポートに連絡してください。
5. 「**OK**」をクリックしてから、コンピューターを再起動します。

第 8 章 データベース通信の保護

Site Database と SiteProtector コンポーネントと間の通信は自動的に有効になりません。Site Database にはネットワークのセキュリティーに関する機密情報が含まれているため、 Secure Sockets Layer (SSL) を使用してデータベース通信を暗号化および認証することを検討してください。

暗号化プロトコル

Secure Sockets Layer (SSL) を使用して、Site Database と SiteProtector コンポーネントの間の通信を保護することができます。

Secure Sockets Layer (SSL) 暗号化プロトコルを使用して、データベース通信を保護します。SSL 暗号化を行うには、証明書を購入する必要があります。詳しくは、Microsoft の記事『*SQL Server への接続の暗号化*』(http://msdn.microsoft.com/ja-jp/library/ms189067.aspx) を参照してください。

SSL 暗号化の有効化

Event Collector、Application Server、Agent Manager、および SecurityFusion Module が Site Database と同じシステムにインストールされていない場合、これらのコンポーネントで SSL を手動で有効にする必要があります。

SSL 暗号化に関する考慮事項

注: SSL を使用することを選択した場合は、Site Database にアクセスするために SSL を使用するすべてのコンピューターに SQL サーバーの証明書をインストールする必要があります。

Event Collector での SSL の有効化

Secure Sockets Layer (SSL) を Event Collector で有効にして、データベース通信を保護することができます。

始める前に

以下の特権が必要になります。

- SiteProtector 管理者特権
- Site Database に対する SA 特権

手順

1. Event Collector がインストールされているコンピューターで、「スタート」メニューの「検索」または「ファイル名を指定して実行」ダイアログから次のいずれかのプログラムを実行して、モジュールの ODBC データ・ソースを見つけます。
   - 32 ビット・システムの場合、`%systemroot%¥System32¥odbcad32.exe` を実行します。
   - 64 ビット・システムの場合、`%systemroot%¥SysWoW64¥odbcad32.exe` を実行します。
2. 「ODBC データ ソース アドミニストレーター」ウィンドウで、「**システム DSN**」タブを選択します。
3. 「**RSNTEventCollector**」を選択します。

© Copyright IBM Corp. 1994, 2013

4. 「**構成**」をクリックして、「**次へ**」をクリックします。
5. 接続するためのログイン情報を入力し、「**次へ**」をクリックしてから、再度「**次へ**」をクリックします。
6. 「**データに強力な暗号を使用する**」を選択して、「**完了**」をクリックします。
7. 要約ウィンドウで、「**データ ソースのテスト**」をクリックして、すべて正しく動作していることを確認します。
8. テストが正しく動作しない場合は、65 ページの『暗号化プロトコル』トピックに示されている Microsoft の記事を参照して、問題点を特定します。
9. SiteProtector Console で、Event Collector を停止してから再始動します。

Application Server での SSL の有効化

Secure Sockets Layer (SSL) を Application Server で有効にして、データベース通信を保護することができます。

始める前に

以下の特権が必要になります。

- SiteProtector 管理者特権
- Site Database に対する SA 特権

手順

1. Application Server がインストールされているコンピューターで、`geronimo-ra.xml` ファイルを見つけます。このファイルで jdbc 設定を変更する必要があります。

   ヒント: 標準インストールでは、このファイルは次のフォルダー内にあります。

   ```
   C:¥Program Files¥ISS¥SiteProtector¥JavaEE¥Geronimo2.1.8¥repository¥iss¥
   SPDataSource¥1.0¥SPDataSource-1.0.rar¥rar¥META-INF¥geronimo-ra.xml
   ```

2. 次の行を変更します。

   ```
   jdbc:jtds:sqlserver://computer name:1433/RealSecureDB;ssl=off
   ```

   この行を次のように変更します。

   ```
   jdbc:jtds:sqlserver://computer name:1433/RealSecureDB;ssl=require
   ```

3. Application Server がインストールされている同じコンピューターで、モジュールの ODBC データ・ソースを見つけます。

   ヒント: これは、IssADReconciler という名前のシステム DSN です。
4. データ・ソースを選択し、「**構成**」をクリックしてから「**次へ**」をクリックします。
5. 接続するためのログイン情報を入力し、「**次へ**」をクリックしてから、再度「**次へ**」をクリックします。
6. 「**データに強力な暗号を使用する**」を選択して、「**完了**」をクリックします。
7. 要約ウィンドウで、「**データ ソースのテスト**」をクリックして、すべて正しく動作していることを確認します。
8. テストが正しく動作しない場合は、65 ページの『暗号化プロトコル』トピックに示されている Microsoft の記事を参照して、問題点を特定します。
9. SiteProtector Console で、ISS Application Server サービスを停止してから再始動します。

Agent Manager での SSL の有効化

Secure Sockets Layer (SSL) を Agent Manager で有効にして、データベース通信を保護することができます。

始める前に

以下の特権が必要になります。

- SiteProtector 管理者特権
- Site Database に対する SA 特権

手順

1. Agent Manager のインストール・ディレクトリーを見つけて、RSSPDC.INI ファイルをテキスト・エディターで開きます。
2. **dbEncrypt** という名前のプロパティーを検索して、その値を「1」に設定します。
3. ファイルを保存して閉じます。
4. SiteProtector Console で、Agent Manager を停止してから再始動します。

   注: Agent Manager が Site Database と通信できないことが原因で始動に失敗した場合、システムはログ・エラーを生成します。問題点を特定するには、65 ページの『暗号化プロトコル』トピックに示されている Microsoft の記事を参照してください。

SecurityFusion Module での SSL の有効化

Secure Sockets Layer (SSL) を SecurityFusion Module で有効にして、データベース通信を保護することができます。

始める前に

以下の特権が必要になります。

- SiteProtector 管理者特権
- Site Database に対する SA 特権

手順

1. SiteProtector Console で、更新する SecurityFusion モジュールを見つけます。
2. SecurityFusion モジュールを右クリックして、「**ポリシーの管理**」を選択します。 FusionPolicy が表示されます。
3. FusionPolicy を右クリックして、「**開く**」を選択します。 FusionPolicy が Policy Editor に表示されます。
4. 左側のツリーで、「**拡張設定**」を選択します。
5. ツリーで「**SSL を使用して Site Database との通信を暗号化**」を選択します。

   注意:
   オンにする前にヘルプを参照してください。
6. 設定を保存してから、Policy Editor を閉じます。
7. SiteProtector Console で、更新する SecurityFusion モジュールを選択してから、変更済みポリシーをセンサーに適用します。

注: SecurityFusion モジュールが Site Database と通信できないことが原因で起動に失敗した場合、システムによりログ・エラーが生成されます。問題点を特定するには、 65 ページの『暗号化プロトコル』トピックに示されている Microsoft の記事を参照してください。

付録 A. サポートされるエージェントとアプライアンス

SiteProtector は、IBM Security によって生成されるエージェントとアプライアンスをサポートします。このトピックでは、サポートされる製品とそのモデルおよびバージョンの情報をリストします。

製品 (アルファベット順)	モデル	Version
IBM Proventia Network Multi-Function Security (MFS)	MX0804	4.6 (サポート) 4.1 から 4.5 (ベスト・エフォート)
	MX1004	4.6 (サポート) 4.1 から 4.5 (ベスト・エフォート)
	MX3006	4.6 (サポート) 4.1 から 4.5 (ベスト・エフォート)
	MX4006	4.6 (サポート) 4.1 から 4.5 (ベスト・エフォート)
	MX5008	4.6 (サポート) 4.1 から 4.5 (ベスト・エフォート)
	MX5010	4.6 (サポート) 4.1 から 4.5 (ベスト・エフォート)
	MX5010A	4.6 (サポート) 4.1 から 4.5 (ベスト・エフォート)
	MX5110	4.6 (サポート) 4.1 から 4.5 (ベスト・エフォート)
	MX5110A	4.6 (サポート) 4.1 から 4.5 (ベスト・エフォート)
IBM RealSecure Server Sensor	AIX® 用	7.0 SR 4.3
	Solaris 用	7.0 SR 4.4
	HP-UX 用	7.0 SR 4.1
	Windows 用	7.0 SR 4.4
IBM Security Network Intrusion Prevention System (IPS)	G400	すべてのモデル
	G2000	すべてのモデル

© Copyright IBM Corp. 1994, 2013

製品 (アルファベット順)	モデル	Version
IBM Security Network Intrusion Prevention System (IPS) GX モデル	GC1200	
	GX3002	
	GX4002	GX4002-C
	GX4004	GX4004-C
	GX5008	GX5008-C GX5008-CF
	GX5108	GX5108-C GX5108-CF
	GX5208	
	GX6116	
	GX7800	GX7800SFP
	GX7412	
	GX7412-10	
	GX7412-05	
IBM Security Network Protection	XGS 5100	5.1
IBM Security QRadar Vulnerability Manager		7.2
IBM Security Server Protection	Windows 用	2.2
IBM Security Virtual Server Protection	VMware 用	1.1
Proventia Desktop Endpoint Security		8.0, 9.0, 10.0, 10.1
Proventia Network Anomaly Detection System	AD5003	4.0
	AD5100	4.0
	AD5200	4.0
	AD5300	4.0
Proventia Network Enterprise Scanner	ES750	
	ES1500	
Proventia Network Internet Scanner		7.0 Service Pack 2
Proventia Server	Linux 用	1.0, 1.5, 1.5.2
	Windows 用	1.0, 2.0, 2.1

付録 B. IBM サポートへの連絡

以下は英語のみの対応となります。IBM サポートは、製品の問題に関する支援を提供し、FAQ (よくある質問) に回答し、ユーザーが製品の問題を解決できるように支援します。

始める前に

IBM サポートに連絡する前に、まず、以下の他のオプションを使用して、回答または解決策を検索します。

- 使用可能なサポートのタイプについては、「*Software Support Handbook*」の Support portfolio トピックを参照してください。
- IBM 技術情報 (IBM サポート・ポータルからアクセス可能) を確認してください。

サポート・ポートフォリオまたは IBM 技術情報で回答や解決策が見つからない場合は、IBM サポートにご連絡いただく前に、お客様の会社または組織が有効な IBM 保守契約をお持ちであり、お客様が IBM への問題報告の権限をお持ちであることを確認してください。

手順

IBM サポートへの連絡方法:

1. 問題を明確にし、背景情報を収集し、問題の重要度を判断します。 詳しくは、「*Software Support Handbook*」の『Getting IBM support』トピックを参照してください。
2. 診断情報を収集します。
3. 次のいずれかの方法で、問題を IBM サポートに送信します。
   - IBM Support Assistant (ISA) を使用 (ご使用の製品でサービス要求ツールが有効な場合)。
     - 収集されたすべてのデータをこのサービス要求に添付することができます。この方法で ISA を使用すると、迅速な分析が可能になり、解決までの時間を短縮できます。
   - IBM サポート・ポータルからオンラインで送信: 「サービス・リクエスト」ページのサービス要求ポートレットから、すべてのサービス・リクエストを開いたり、更新したり、表示することができます。
   - 電話 (重大な問題、システム・ダウン、あるいは重要度 1 の問題が発生した場合)。国別の電話番号については、『Directory of worldwide contacts』Web ページを参照してください。

タスクの結果

お客様が送信した問題が、ソフトウェア障害または資料の欠落や不正確さが原因である場合、IBM サポートはプログラム診断依頼書 (APAR) を作成します。APAR には問題が詳細に記述されます。IBM サポートは、可能な限り、APAR が解決されて解決策が提供されるまで、お客様が実施できる回避策を提供します。IBM では、同じ問題に直面している他のお客様が解決策を利用できるように、解決された APAR を IBM サポートの Web サイトに毎日公開しています。

© Copyright IBM Corp. 1994, 2013

特記事項

本書は米国 IBM が提供する製品およびサービスについて作成したものです。

本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。日本で利用可能な製品、サービス、および機能については、日本 IBM の営業担当員にお尋ねください。本書で IBM 製品、プログラム、またはサービスに言及していても、その IBM 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。これらに代えて、IBM の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、IBM 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

IBM は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、お客様にこれらの特許権について実施権を許諾することを意味するものではありません。実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

〒103-8510
東京都中央区日本橋箱崎町19番21号
日本アイ・ビー・エム株式会社
法務・知的財産
知的財産権ライセンス渉外

以下の保証は、国または地域の法律に沿わない場合は、適用されません。 IBM およびその直接または間接の子会社は、本書を特定物として現存するままの状態で提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。 IBM は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書において IBM 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この IBM 製品の資料の一部ではありません。それらの Web サイトは、お客様の責任でご使用ください。

IBM は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

本プログラムのライセンス保持者で、(i) 独自に作成したプログラムとその他のプログラム (本プログラムを含む) との間での情報交換、および (ii) 交換された情報の相互利用を可能にすることを目的として、本プログラムに関する情報を必要とする方は、下記に連絡してください。

IBM Corporation
Project Management
C55A/74KB
6303 Barfield Rd.,
Atlanta, GA 30328
U.S.A

© Copyright IBM Corp. 1994, 2013

本プログラムに関する上記の情報は、適切な使用条件の下で使用することができますが、有償の場合もあります。

本書で説明されているライセンス・プログラムまたはその他のライセンス資料は、IBM 所定のプログラム契約の契約条項、IBM プログラムのご使用条件、 またはそれと同等の条項に基づいて、IBM より提供されます。

IBM の将来の方向または意向に関する記述については、予告なしに変更または撤回される場合があり、単に目標を示しているものです。

商標

IBM、IBM ロゴおよび ibm.com は、世界の多くの国で登録された International Business Machines Corporation の商標です。他の製品名およびサービス名等は、それぞれ IBM または各社の商標である場合があります。現時点での IBM の商標リストについては、http://www.ibm.com/legal/copytrade.shtml をご覧ください。

Linux は、Linus Torvalds の米国およびその他の国における登録商標です。

UNIX は The Open Group の米国およびその他の国における登録商標です。

Microsoft および Windows は、Microsoft Corporation の米国およびその他の国における商標です。

通信規制の注記

This product is not intended to be connected directly or indirectly by any means whatever to interfaces of public telecommunications networks.

本製品は、電気通信事業者の通信回線への直接、またはそれに準ずる方法での接続を目的とするものではありません。

プライバシー・ポリシーに関する考慮事項

サービス・ソリューションとしてのソフトウェアも含めた IBM ソフトウェア製品 (「ソフトウェア・オファリング」) では、製品の使用に関する情報の収集、エンド・ユーザーの使用感の向上、エンド・ユーザーとの対話またはその他の目的のために、Cookie はじめさまざまなテクノロジーを使用することがあります。多くの場合、ソフトウェア・オファリングにより個人情報が収集されることはありません。 IBM の「ソフトウェア・オファリング」の一部には、個人情報を収集できる機能を持つものがあります。ご使用の「ソフトウェア・オファリング」が、これらの Cookie およびそれに類するテクノロジーを通じてお客様による個人情報の収集を可能にする場合、以下の具体的事項を確認ください。

この「ソフトウェア・オファリング」は、Cookie もしくはその他のテクノロジーを使用して個人情報を収集することはありません。

この「ソフトウェア・オファリング」が Cookie およびさまざまなテクノロジーを使用してエンド・ユーザーから個人を特定できる情報を収集する機能を提供する場合、お客様は、このような情報を収集するにあたって適用される法律、ガイドライン等を遵守する必要があります。これには、エンドユーザーへの通知や同意の要求も含まれますがそれらには限られません。

このような目的での Cookie を含む様々なテクノロジーの使用の詳細については、IBM の『IBM オンラインでのプライバシー・ステートメント』(http://www.ibm.com/privacy/details/jp/ja/) の『クッキー、ウェブ・ビーコン、その他のテクノロジー』を参照してください。

適切なセキュリティーの実践に関する注意事項

IT システムのセキュリティーでは、企業内および企業外からの不適切なアクセスの防止、検出、およびそれらのアクセスへの対応により、システムおよび情報を保護する必要があります。不適切なアクセスにより、情報が改ざん、破壊、盗用、または悪用されたり、あるいはご使用のシステムの損傷または他のシステムへの攻撃のための利用を含む悪用につながる可能性があります。完全に安全と見なすことができる IT システムまたは IT 製品は存在せず、また単一の製品、サービス、またはセキュリティー対策が、不適切な使用またはアクセスを防止する上で、完全に有効となることもありません。 IBM のシステム、製品およびサービスは、包括的なセキュリティーの取り組みの一部となるように設計されており、これらには必ず追加の運用手順が伴います。また、最高の効果を得るために、他のシステム、製品、またはサービスを必要とする場合があります。IBM は、システム、製品、またはサービスが、悪意のある行為または不正な行為から影響を受けないこと、またはこれらの行為がお客様の企業に影響を与えないことを保証しません。

索引

日本語, 数字, 英字, 特殊文字の順に配列されています。なお, 濁音と半濁音は清音と同等に扱われています。

[ア行]

アプライアンス、説明　1
暗号化
　厳重　35
暗号プロバイダー、選択のガイドライン　33
インストール
　追加コンポーネント、図　53
　追加の Event Collector　55
　追加の Event Viewer　57
　追加の X-Press Update Server　57
　64 ビット・プラットフォーム　51
　Event Viewer、追加のインストール　57
インストール (installation)
　オプション　55
　サード・パーティー・ソフトウェアのセキュリティー問題　37
　フェーズ　43
エージェント、説明　1

[カ行]

技術サポート、IBM Security　71
厳重暗号化　35, 37
厳重暗号化の要件　36
コンポーネント図　1
コンポーネントの削除、順序　64

[サ行]

サード・パーティー・ソフトウェア
　事前のセキュリティー対策　37
　セキュリティー問題　37
サポート　71
資料
　SiteProtector ヘルプ　v
信頼済みサイト　34
スキャナー、説明　1
セキュア通信　37
センサー、説明　1

[タ行]

データベース
　英語以外のデータベースのインストール　43
　完全修飾名のリスト　40
データベース使用中エラー　62
停止できないエラー、Event Collector　62
トラブルシューティング
　インストール・プロセスにおける　34
　SiteProtector のアンインストール　64

[ハ行]

ハード・ディスク、複数あるコンピューター　33
パッチ、Microsoft の適用　37
秘密鍵
　アーカイブするインストール・プログラム　33
　事前の考慮事項　33
ヘルプ、SiteProtector、内容　v
ホット・フィックス、最新のインストール　38

[ラ行]

ログインを削除できないエラー　62
ログ・ファイル　34

[数字]

64 ビット・プラットフォーム　51

A

Agent Manager
　インストール　56

E

Event Archiver　59
Event Archiver のインストール　59
Event Collector
　追加のインストール　55
　停止できないエラー　62
Event Viewer、追加のインストール　57

H

HFNetChk　38

I

IBM Security
　技術サポート　71
　サポート・ポータル　71
　トラブルシューティング　71
IP アドレス、複数あるコンピューター　33
issApp が既に存在するエラー　61

M

Microsoft SQL Server
　暗号化　65
　英語以外のバージョン　43
　既存の issApp ログインの削除　61
　セキュリティー問題　37
Microsoft Windows Server 2008
　ダウンロードの設定　33

N

NIST 800-131A 標準　35

S

SecureSync Failover　4
SecurityFusion SSL　67
Service Pack、最新のインストール　38
SiteProtector
　アーキテクチャー　1
　使用される通信チャネル　2
　説明　1
SiteProtector Express オプションの評価　43
SiteProtector Traffic のファイアウォールの構成　v
SiteProtector 構成ガイド　v
SiteProtector コンポーネント
　アンインストール　63
SiteProtector コンポーネントのアンインストール　63
SiteProtector セキュリティー・アナリスト向けユーザー・ガイド　v
SiteProtector データベースの IPsec　37
SiteProtector のアンインストール　64

© Copyright IBM Corp. 1994, 2013

SiteProtector ポリシーおよびレスポンス構
成ガイド v
SiteProtectorExpress-Setup.exe 44
SP800-131A NIST 標準 35
SSL 65
SSL、SecurityFusion 67

T

TLS v1.2 36
Transfer Layer Security 36

W

Windows ファイアウォール 37

X

X-Press Update Server
インストール 57

Printed in Japan

日本アイ･ビー･エム株式会社
〒103-8510 東京都中央区日本橋箱崎町19-21