CHAPTER 3

サーバのインストール準備

ターゲット サーバが第 2 章「要件と依存関係」に記載されている要件を満たしていることを確認したら、このチェックリストを使用してサーバをインストール用に準備し、最適化できます。

サーバのパフォーマンスとセキュリティを向上させるためのベスト プラクティス

ベスト プラクティスのフレームワーク、推奨事項、およびその他の準備タスクを使用すれば、そうしなかった場合よりも Security Manager サーバの速度と信頼性を高めることができます。

注意 このチェックリスト内のタスクを完了することによって、すべてのサーバのパフォーマンスが向上するわけではありません。それでも、これらのタスクを完了しなかった場合は、Security Manager が設計どおりに動作しないことがあります。

このチェックリストは、推奨タスクの進捗を追跡するために使用できます。

✓	タスク
❑	**1. サーバへのインストールが推奨されているすべてのアップデート、パッチ、サービス パック、ホット フィックス、およびセキュリティ ソフトウェアを探して、インストーラ アプリケーションを編成します。**
❑	**2. アップグレードが入手可能な場合は、サーバ BIOS をアップグレードします。**
❑	**3. 他の目的に使用しているサーバ上に Security Manager をインストールする場合は、すべての重要なサーバ データをバックアップしてから、ブート CD または DVD を使用してサーバからすべてのデータをワイプします。** Security Manager 4.0 と 3.3 以前のリリースの Common Services を 1 台のサーバ上にインストールまたは共存させることは*できません*。また、このマニュアルまたは http://www.cisco.com/go/csmanager に明記されていない場合は、サードパーティ ソフトウェアまたはその他のシスコ ソフトウェアと共存させることもできません。
❑	**4. サーバ管理用のメーカー カスタマイズが施されていないベースライン サーバ OS のみのクリーン インストールを実行します。**

✓	タスク
❑	**5. ターゲット サーバ上に必要なすべての OS サービス パックと OS パッチをインストールします。**使用している Windows に関してどのサービス パックまたはアップデートが必要なのかをチェックするには、[Start] > [Run] を選択してから、**wupdmgr** と入力します。
❑	**6. ドライバとファームウェアに関して推奨されているすべてのアップデートをターゲット サーバにインストールします。**
❑	**7. システム上でマルウェアをスキャンします。**ターゲット サーバとその OS をセキュリティで保護するには、システム上でウイルス、トロイの木馬、スパイウェア、キーロガー、およびその他のマルウェアをスキャンしてから、見つかったすべての関連問題に対処します。
❑	**8. セキュリティ製品の競合を解消します。**ポップアップ ブロック、ウイルス対策スキャナ、Cisco Security Agent、他社の同等製品などのセキュリティ ツールに関する既知の非互換性または制約事項を理解して解決します。このような製品の競合や相互作用を理解するに当たって、インストール、アンインストール、または一時的にディセーブルにするものを決定し、従うべき順序を考慮します。次の例を参考にしてください。 • 組織でシスコ製以外のホストベースの侵入防御ユーティリティが使用されている場合は、Security Manager のインストールが完了するまでそのユーティリティをターゲット サーバにインストール*しないでください*。そうしなければ、ほとんどの場合、Security Manager インストールの一部として自動的にインストールされる Cisco Security Agent のインストールと競合する可能性があります。別の IPS ユーティリティがインストールされたサーバを使用する場合は、そのユーティリティをアンインストールしてから Security Manager をインストールして、Cisco Security Agent をアンインストールしてからそのユーティリティを再インストールします。 • 任意のバージョンの Cisco Security Agent が Security Manager サーバ上にインストールされている場合は、サーバが Security Manager サーバ固有のエージェント ポリシー セットに依存します。ただし、このようなポリシーを含むカスタマイズされたスタンドアロン エージェントは、ターゲット サーバにフル バージョンの Cisco Security Agent が事前にインストールされていない場合にのみインストールされます。フル エージェント バージョンには、Security Manager サーバに必要な特定のポリシーが含まれていません。スタンドアロン エージェントよりフル エージェントを優先する場合は、Security Manager インストール DVD 上（¥csm<*version*>_win_server¥CSA サブフォルダ内）で見つかったすべてのエクスポートされたエージェント ポリシーをフル エージェントにインポートする必要があります。スタンドアロン エージェントは、信頼できる別の手段を通して同等のサーバ セキュリティを入手するまで、アンインストールしないことを推奨します。DVD 上のファイルからポリシーをインポートする場合は、それらのインポート対象ポリシーを、組織で管理対象エージェント用に設定しているすべての競合ポリシーと調整する必要があります。
❑	**9. ユーザ アカウントを「強化」します。**ターゲット サーバを総当たり攻撃から保護するには、ゲスト ユーザ アカウントをディセーブルにして、管理者ユーザ アカウントの名前を変更し、管理環境内の悪用される可能性のあるその他のユーザ アカウントを削除します。
❑	**10. 管理者ユーザ アカウントと残りのユーザ アカウントに対して強力なパスワードを使用します。**強力なパスワードは、8 文字以上で構成され、数字、文字（大文字と小文字の両方）、および記号が含まれています。 **ヒント** Local Security Settings ツールを使用して、強力なパスワードを要求します。[Start] > [Settings] > [Control Panel] > [Administrative Tools] > [Local Security Policy] を選択します。

✓	タスク
❑	**11. 未使用のアプリケーション、不必要なアプリケーション、および互換性のないアプリケーションを削除します。**次の例を参考にしてください。 • Microsoft Internet Information Server（IIS）は Security Manager と互換性がありません。IIS がインストールされている場合は、それをアンインストールしてから Security Manager をインストールする必要があります。 • このマニュアルまたは http://www.cisco.com/go/csmanager に明記されていなければ、Security Manager とサードパーティ ソフトウェアまたはその他のシスコ ソフトウェア（LAN Management Solution（LMS）などの CiscoWorks ブランドの「ソリューション」または「バンドル」を含む）の共存がサポートされません。Security Manager、AUS、Performance Monitor、および RME の同じサーバ上へのインストールはサポートされますが、非常に低速なネットワークにのみ推奨されている設定です。また、これらの製品をインストールする前に、CiscoWorks Common Services をインストールする必要があります。 • 1 台のサーバ上で、このバージョンの Security Manager と 3.3 以前のリリースの Common Services をインストールまたは共存させることはできません。 • 1 台のサーバ上で、Security Manager と Security Manager の購入時に受領したものではない CD-ONE コンポーネント（CiscoView Device Manager を含む）を共存させることはできません。 • 1 台のサーバ上で、Security Manager と Cisco Secure ACS for Windows を共存させることはできません。 • 1 台のサーバ上で、Security Manager とフル バージョンの Cisco IPS Event Viewer を共存させることはできません。
❑	**12. 未使用のサービスと不必要なサービスをディセーブルにします。**Windows では、少なくとも、DNS クライアント、イベント ログ、プラグ アンド プレイ、保護された記憶域、およびセキュリティ アカウント マネージャを実行する必要があります。 ソフトウェアとハードウェアのマニュアルをチェックして、特定のサーバでその他のサービスが必要ないかどうかを確認します。
❑	**13. TCP と UDP を除くすべてのネットワーク プロトコルをディセーブルにします。**どのプロトコルもサーバへのアクセス権の取得に使用される可能性があります。ネットワーク プロトコルを制限することによって、サーバへのアクセス ポイントが制限されます。
❑	**14. ネットワーク共有は作成しないでください。**ネットワーク共有を作成しなければならない場合は、共有リソースを強力なパスワードで保護してください。 **（注）**　ネットワーク共有はあまり推奨できません。NETBIOS を完全にディセーブルにすることを推奨します。
❑	**15. サーバ ブート設定を構成します。**起動時間を 0 秒に設定して、Windows をデフォルトでロードするように設定し、システム障害発生時の自動リブートをイネーブルにします。

インストール準備状況チェックリスト

Security Manager をインストールする前に、次のタスクを完了する必要があります。

✓	準備状況要因
❑	⚠ **注意**　セキュリティ アプリケーションをアンインストールまたはディセーブルにした場合は、サーバが攻撃に対して脆弱になる可能性があります。 1. **一時的にセキュリティ アプリケーションをディセーブルにします。**たとえば、Security Manager をインストールする前に、ターゲット サーバ上のウイルス対策ソフトウェアを一時的にディセーブルにする必要があります。これらのプログラムがアクティブの間はインストールを実行できません。
❑	**ヒント**　サーバに SSL 証明書の有効期間以外の日付と時刻を設定した場合は、サーバ上の SSL 証明書が無効になります。サーバの SSL 証明書が無効になっている場合は、DCRServer プロセスが起動できません。 2. **サーバに適用する日付と時刻の設定は慎重に検討してください。**NTP サーバを使用して、サーバの日付と時刻の設定と管理対象デバイスの日付と時刻の設定を同期させる方法が理想的です。また、Security Manager を Cisco Security Monitoring, Analysis, and Response System（Cisco Security MARS）アプライアンスと組み合わせて使用する場合は、使用する NTP サーバを Cisco Security MARS アプライアンスが使用するサーバと同じにする必要があります。ネットワーク上で発生したものを正確に再構成するためにはタイムスタンプ情報が不可欠なため、特に、Cisco Security MARS で同期化された時間が重要です。 **ヒント**　サーバ上の日付と時刻の設定を変更して SSL 証明書が無効になった場合は、java.security.cert.CertificateNotYetValidException エラーが *NMSROOT*¥log¥DCRServer.log ファイルに記録されます。ここで、*NMSROOT* は Security Manager インストール ディレクトリへのパスです。デフォルトは **C:¥Program Files¥CSCOpx** です。
❑	3. **必要なサービスとポートがイネーブルになっており、Security Manager から使用可能なことを確認します。**「必要なサービスとポート」（P.2-1）を参照してください。
❑	4. **Terminal Services がアプリケーション モードでイネーブルになっている場合は、Terminal Services をディセーブルにして、サーバをリブートします。**Terminal Services がアプリケーション モードでイネーブルになっているサーバ上に Security Manager をインストールできません。リモート管理モードでイネーブルにされた Terminal Services はサポートされます。 Terminal Services がアプリケーション モードでイネーブルになっているターゲット サーバに Security Manager をインストールしようとすると、エラーでインストールが終了します。
❑	5. **実行中のドメイン コントローラ サービス（プライマリまたはバックアップ）をディセーブルにします。**
❑	6. **インストールのターゲット ディレクトリが暗号化されていないことを確認します。**暗号化されたディレクトリに Security Manager をインストールしようとすると失敗します。
❑	7. **フレッシュ インストールを実行している場合は、インストールの前にライセンス ファイルをターゲット サーバに配置する必要があります。**インストール中にこのファイルの選択が要求されます。
❑	8. **インストールされている IIS をアンインストールします。**IIS は Security Manager と互換性がありません。
❑	9. **存在する場合の Cisco Secure ACS for Windows を含めて、サーバ上のすべてのアクティブな Sybase インスタンスをディセーブルにします。**Security Manager のインストール後に Sybase を再イネーブルにするか、再起動するかを選択できますが、同じサーバ上での Security Manager と Cisco Secure ACS for Windows の共存がサポートされていないことに注意してください。

✓	準備状況要因
❑	**10. Cisco Security Manager クライアントがすでにサーバ上にインストールされている場合は、そのクライアントを停止する必要があります。**この状態はインストール中にチェックされます。
❑	**11. FIPS 準拠の暗号化をディセーブルにします。**Federal Information Processing Standard（FIPS; 連邦情報処理標準）準拠の暗号化アルゴリズムが、Windows Server 2003 と Windows Server 2008 上のグループ セキュリティ ポリシーに対してイネーブルになっている場合があります。FIPS 準拠がオンになっている場合は、CiscoWorks サーバ上の SSL 認証が失敗する可能性があります。CiscoWorks を正しく機能させるためには、FIPS 準拠をディセーブルにする必要があります。 **手順** Windows Server 2003 または Windows Server 2008 上で FIPS をイネーブルまたはディセーブルにするには、次の手順を実行します。 **1.** [Start] > [Settings] > [Control Panel] > [Administrative Tools] > [Local Security Policy] に移動します。[Local Security Policy] ウィンドウが表示されます。 **2.** [Local Polices] > [Security Options] をクリックします。 **3.** [System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing] を選択します。 **4.** 選択したポリシーを右クリックして、[Properties] をクリックします。 **5.** [Enabled] または [Disabled] を選択して、FIPS 順序アルゴリズムをイネーブルまたはディセーブルにします。 **6.** [Apply] をクリックします。 サーバをリブートして変更を有効にする必要があります。