サーバのインストール準備

ターゲットサーバーが「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ー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ると、Security Manager サーバー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. シスコでは、Security Manager サーバーに他の製品をインストールしないことを推奨しています。** **他の目的に使用しているサーバー上に Security Manager をインストールする場合は、すべての重要なサーバーデータをバックアップしてから、ブート CD または DVD を使用してサーバーからすべてのデータをワイプします。** Security Manager 4.24 と 4.2.2 以前のリリースの Common Services を 1 台のサーバー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. Security Manager は複数のネットワーク インターフェイスカードを持つことができますが、ロードバランシングのために複数の NIC をチーミングすることは推奨されません。**
❑	**5. 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。**
❑	**6. 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 バージョン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、[スタート（Start）] > [実行（Run）] を選択してから、**wupdmgr** と入力します。 （注） パッチまたは Windows アップデートを適用する前に、Security Manager サーバーをバックアップし、Security Manager サービスを停止します。シスコでは、Security Manager が実行されていないメンテナンス期間中にパッチと Windows アップデートを適用することを推奨しています。
❑	**7. 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。**
❑	**8. 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。
❑	**9. 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、アンチウイルス スキャナ、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。
❑	**10. 内部ユーザーアカウントの「強化」**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。

❑	**11. 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。[スタート（Start）] > [管理ツール（Administrative Tools）] > [ローカルセキュリティポリシー（Local Security Policy）] を選択します。
❑	**12. 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。**次に例を示します。 **1.** 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。 **2.** このマニュアルまたは http://www.cisco.com/go/csmanager [英語] 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。 **3.** 1 台のサーバー上で、このバージョンの Security Manager と 4.2.2 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。 **4.** 1 台のサーバー上で、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。 **5.** 同じサーバ上での Security Manager と Cisco Secure ACS for Windows の共存はサポートされていません。
❑	**13. 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。
❑	**14. 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。
❑	**15. 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。
❑	**1. 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

Cisco 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
❑	Microsoft Windows Server 2012 R2 で重要な Cisco Security Manager サービスを実行するには、次のパッチが必要です。パッチのインストールに失敗すると、サービスが停止します。サーバーにこれらのパッチがインストールされていることを確認してください。そうでない場合は、次と同じ順序でパッチをインストールします。 **1.** KB2919442 **2.** clearcompressionflag.exe を実行します。 （注） clearcompressionflag.exe ファイルは、セキュリティ更新の累積セットの一部です。このツールは、バックグラウンドで Windows Update 用にコンピュータを準備します。実行ファイルは、Microsoft のサイト（https://support.microsoft.com/en-in/kb/2919355）からダウンロードできます。 **1.** KB2919355、KB2932046、KB2959977、KB2937592、KB2938439、KB2934018 **2.** KB2999226 Cisco Security Manager のインストール後にこれらのパッチをインストールして、重要なサービスを起動することもできます。Windows サービスにサービスを登録するには、「<CSMInstalledDirectory>\CSCOpx\bin」にある「RegisterApache.bat」スクリプトを実行してからサーバーを再起動する必要があります。 （注） これらの Windows パッチがインストールされるまでに少なくとも 30 分かかる場合があり、インストール時間は Windows Server によって異なる場合があります。これらのパッチのインストール中にエラーが発生した場合、Cisco Security Manager ではなく Microsoft に関連します。
❑	**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、ターゲットサーバー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。 （注） インストール後にウイルス対策ソフトウェアを再度イネーブルにします。ただし、Security Manager がサーバーにインストールされている場合は、NMSROOT ディレクトリとイベントフォルダをスキャンから除外する必要があります。

❑	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　サーバー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 (x86)\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。Security Manager は、内部動作に事前定義されたダイナミックポートを使用します。これらのポートはポートスキャナによってブロックされる可能性があり、Security Manager はこれらのプロセスを実行できません。したがって、Qualys などのポートスキャナは有効にしないでください。**有効にすると、Security Manager プロセスのクラッシュの問題が発生し、Security Manager の完全な再インストールが必要になる可能性があります。必要なサービスとポート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ーに 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ー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。 （注）　ライセンス ファイルのパスには、アンパサンド（&）などの特殊文字が含まれていてはなりません。

❑	**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、サーバー上のすべてのアクティブな Maria 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 Maria を再イネーブルするか、再起動するかを選択できますが、同じサーバー上での 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。
❑	**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。**Windows Server 2008 のグループ セキュリティ ポリシーで、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イネーブルになっていることがあります。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 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.** [スタート（Start）] > [管理ツール（Administrative Tools）] > [ローカルセキュリティポリシー（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.** [ローカルポリシー（Local Policies）] > [セキュリティオプション（Security Options）] をクリックします。 **3.** [システム暗号化：暗号化、ハッシュ、署名のためのFIPS準拠アルゴリズムを使う（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、[プロパティ（Properties）] をクリックします。 **5.** [有効（Enabled）] または [無効（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。

❑	**12. Internet Explorer Enhanced Security Configuration（IE ESC）をディセーブルにします。**クライアントのダウンロードが IE ESC によって禁止されるため、この作業を行う必要があります。 **手順** Security Manager のインストール準備をしているサーバ上で IE ESC をディセーブルにするには、次の手順を実行します。 **1.** Windows で、Server Manager を開きます。これを行うには、[コンピュータ（Computer）] を右クリックしてから、[管理（Manage）] をクリックします。 **2.** [セキュリティ情報（Security Information）] の下で、[IE ESCの設定（Configure IE ESC）] をクリックし、IE ESC を無効にします。
❑	**13. ポートスキャナソフトウェアを無効にします。**Security Manager は、内部動作に事前定義されたダイナミックポートを使用します。ポートスキャナはこれらのポートをブロックする可能性があり、Security Manager はこれらのプロセスを実行できません。このため、Qualys などのポートスキャナを有効にしないでください。有効にすると、Security Manager プロセスのクラッシュが発生し、Security Manager の完全な再インストールが必要になる可能性があります。
❑	**14. CSM のインストールフォルダをインストール、アンインストール、または CSM の操作中に開くことはできません。**

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。