Cisco Security Manager 4.25 リリースノート

初版：2022 年 6 月 20 日

はじめに

このマニュアルの構成は、次のとおりです。

（注） このドキュメントは、通信、サービス、およびその他の情報（15 ページ）に示されているドキュメントと併せて使用します。ユーザーマニュアルのオンラインバージョンは、初回リリース後に更新されることもあります。その結果、Cisco.com の『Cisco Security Manager end-user guides』に記載されている情報は、製品に含まれる状況依存ヘルプに記載されている情報よりも優先されます。

このドキュメントには、以下についてのリリースノートの情報が含まれています。

- [Cisco Security Manager 4.25]：Cisco Security Manager でシスコのセキュリティデバイスのセキュリティポリシーを管理できます。Security Manager では、ファイアウォール、VPN、ASA セキュリティアプライアンス、および他のいくつかのサービスモジュールの統合的なプロビジョニングがサポートされています（完全なデバイスのサポート情報は、Cisco.com の『Cisco Security Manager Compatibility Information』で確認できます）。Security Manager では、インターフェイス、ルーティング、ID、QoS、ロギングなど、さまざまなプラットフォーム固有の設定のプロビジョニングもサポートしています。

Security Manager は、数台のデバイスで構成される小規模ネットワークから、数千台のデバイスで構成される大規模ネットワークまで、広範囲のネットワークを効率的に管理します。デバイスのグループ化機能、オブジェクト、共有可能なポリシーの豊富な機能セットにより拡張性が実現されます。

（注） バージョン 4.21 以降、Cisco Security Manager では、すべてのアグリゲーション サービス ルータ、統合サービスルータ、埋め込み型サービスルータ、および次のデバイスを含む Cisco IOS ソフトウェアで動作するすべてのデバイスについて、バグ修正または拡張機能のサポートを含むサポート全体が終了します。

- Cisco Catalyst 6500 および 7600 シリーズ ファイアウォール サービス モジュール（EOL8184）
- Cisco Catalyst 6500 シリーズ Intrusion Detection System サービスモジュール 2（EOL8843）
- Cisco Intrusion Prevention System：IPS 4200、4300、および 4500 シリーズ センサー（EOL9916）
- Cisco SR 500 シリーズ セキュアルータ（EOL7687、EOL7657）
- PIX ファイアウォール（EOL）
- Cisco IOS デバイス

- [Auto Update Server 4.25]：Auto Update Server（AUS）は、ASA ソフトウェアイメージ、Adaptive Security Device Manager（ASDM）イメージ、および ASA 構成ファイルをアップグレードするためのツールです。自動更新機能を使用する、ダイナミック IP アドレスを持つセキュリティアプライアンスは、定期的に AUS に接続して、デバイス コンフィギュレーション ファイルを更新し、デバイスおよびステータス情報を渡します。

（注） Cisco Security Manager 4.25 を使用する前に、このドキュメントをすべて読むことをお勧めします。また、Cisco Security Manager 4.25 をインストールする前に、特記事項 （8 ページ）、設置上の注意事項 （4 ページ）、および『Installation Guide for Cisco Security Manager 4.25』にも目を通してください。

サポートされるコンポーネントバージョンと関連するソフトウェア

アプリケーションの Cisco Security Management Suite には、いくつかのコンポーネント アプリケーションと、それらと組み合わせて使用できる関連アプリケーションのグループが含まれています。次の表に、コンポーネントと関連アプリケーション、およびこのリリースのスイートで一緒に使用できるそれらのアプリケーションのバージョンを示します。これらのアプリケーションの説明については、『Installation Guide for Cisco Security Manager 4.25』を参照してください。

（注） Cisco Security Manager で管理できるサポート対象のソフトウェアおよびハードウェアについては、Cisco.com の『Cisco Security Manager Compatibility Information』にある『Supported Devices and Software Versions for Cisco Security Manager』オンラインドキュメントを参照してください。

表 *1:* コンポーネントと関連アプリケーションでサポートされているバージョン

アプリケーション	サポートされているリリース
コンポーネント アプリケーション	
Cisco Security Manager	4.25
Auto Update Server	4.25
CiscoWorks Common Services	4.2.2
関連アプリケーション	
Cisco Security Monitoring, Analysis and Response System（CS-MARS）	6.0.7、6.1.1
Cisco Configuration Engine	3.5、3.5(1)

（注） バージョン 4.21 以降、Cisco Security Manager は Cisco Identity Services Engine（ISE）を介した TACACS+ 認証のみをサポートします。これは、ACS のサポートが終了しているためです。

最新情報

Cisco Security Manager 4.25 は、次の新機能と拡張機能をサポートしています。

ASA 9.18 (1) バージョンのサポート

- [L2L トンネルグループのデフォルトグループポリシーと名前付きトンネルグループのサポート（L2L Tunnel Group Default Group Policy and Named Tunnel Group support）]：通常の IPsec トポロジと通常の IPsec VTI トポロジは、CSM 4.25 以降の L2L 名前付きトンネルグループとデフォルトグループポリシーのオプションの両方をサポートします。

  L2L トンネルグループのデフォルトグループポリシーのサポート：

  L2L トンネルグループポリシーは、CSM での ASA デバイスの展開と検出の両方をサポートしています。

（注） 展開の失敗を回避するには、ASA にすでに展開されているグループポリシーを L2L トンネルグループに割り当てる必要があります。

L2L 名前付きトンネルグループのサポート：

L2L 名前付きトンネルグループは、デジタル証明書が ASA の認証方式として使用される場合にのみサポートされます。L2L名前付きトンネルグループは、ASAデバイスの展開のみをサポートしています。

（注） L2L トンネルグループ名がデジタル証明書と一致しない場合、トンネルはダウンします。

- [フロー制御サポート（Flow Control support）]：ASA 9.18(1) 以降のデバイスに対する Firepower 3100 デバイスのインターフェイスポリシーでのフロー制御の設定。
- [PBRの評価指標のサポート（Performance Metrics Support in PBR）]：ASA 9.18(1) 以降のデバイスのルート マップ ポリシー オブジェクトでの PBR の設定。
- [FQDNの複数のDNSサーバーのサポート（FQDN Multiple DNS Server support）]：DNS ページの ASA 9.18(1) 以降のデバイスの DNS サーバーグループ名と一致する必要がある DNS グループマップ名の設定。
- [ASDバージョンアップグレードのサポート（ASD version upgrade support）]：CSM 4.25 は ASDv4 をサポートします。
- [Firepowerのパケットサポート（Firepower Packet Support）]：パケットがサードパーティのアプリ、snort、または Lina を通過するときに、パケットキャプチャ設定を切り替えてパケットのパスおよびコンテンツをキャプチャします。
- [大規模なACLのブート時間の最適化（Boot time optimization for large ACLs）]：ASA 9.18(1) 以降のデバイスでデフォルトで有効になっている [オブジェクトグループ検索の有効化（Enable Object Group Search）] オプション。

設置上の注意事項

特定のインストール手順、およびクライアントとサーバーの要件に関する重要な情報については、『Installation Guide for Cisco Security Manager 4.25』を参照してください。Cisco Security Manager 4.25 をインストールする前に、このセクションに記載されている注意事項と 特記事項 （8 ページ） に目を通してください。

- インストールガイドの「Licensing」の章で、必要なライセンスを判断できます（必要なライセンスは、新規にインストールするのか、前のバージョンからアップグレードするのか

によって異なります）。さらに、スタンダード版、プロフェッショナル版、評価版など、入手可能な各種ライセンスについても説明しています。

- STD-TO-PRO アップグレードでは、ST25 ライセンスが PRO50 ライセンスに変換され、50 台のデバイスがサポートされます。追加のデバイスをサポートする必要がある場合は、必要な増分ライセンスを購入する必要があります。
- Security Manager のバージョン 4.7 以降、API の一時ライセンスがシスコから入手できます。
- Security Manager のバージョン 4.7 以降では、Security Manager ライセンスの評価版に増分ライセンスを適用できます。
- 製品のインストール中に設定された casuser（デフォルト サービス アカウント）権限またはディレクトリ権限を変更しないでください。変更した場合は、次の操作ができなくなる可能性があります。
  - Web サーバへのログイン
  - クライアントへのログイン
  - データベースの正常なバックアップ
- サーバーマシンでサポートされているオペレーティングシステムは次のとおりです。
  - Microsoft Windows Server 2019 Standard（64 ビット）
  - Microsoft Windows Server 2019 Datacenter（64 ビット）
  - Microsoft Windows Server 2016 Standard（64 ビット）
  - Microsoft Windows Server 2016 Datacenter（64 ビット）
  - Microsoft Windows Server 2012 R2 Standard（64 ビット）
  - Microsoft Windows Server 2012 Standard（64 ビット）
  - Microsoft Windows Server 2012 R2 Datacenter（64 ビット）
  - Microsoft Windows Server 2012 Datacenter（64 ビット）
- クライアントマシンでサポートされているオペレーティングシステムは次のとおりです。
  - Microsoft Windows 7
  - Microsoft Windows 8.1 Enterprise Edition（64 ビットおよび 32 ビット）
  - Microsoft Windows 10（64 ビットおよび 32 ビット）
  - Microsoft Windows Server 2019 Standard（64 ビット）
  - Microsoft Windows Server 2019 Datacenter（64 ビット）
  - Microsoft Windows Server 2016 Standard（64 ビット）

- Microsoft Windows Server 2016 Datacenter（64 ビット）
- Microsoft Windows Server 2012 R2 Standard（64 ビット）
- Microsoft Windows Server 2012 Standard（64 ビット）
- Microsoft Windows Server 2012 R2 Datacenter（64 ビット）
- Microsoft Windows Server 2012 Datacenter（64 ビット）

- サーバーマシンとクライアントマシンの両方でサポートされるブラウザは次のとおりです。
  - Internet Explorer 8.x、9.x、10.x、または 11.x（ただし互換表示のみ）
  - Firefox 15.0.1 以降（サポートおよび推奨）

- Security Manager サーバーソフトウェアを直接インストールすることも、Security Manager がインストールされているサーバーでソフトウェアをアップグレードすることもできます。『Installation Guide for Cisco Security Manager 4.25』では、アップグレードがサポートされている以前の Security Manager リリースについての説明や、サーバー要件、サーバー設定、およびインストール後のタスクに関する重要な情報を確認できます。
- 以前のバージョンの Security Manager から Security Manager 4.25 へのアップグレードを成功させるためには、Security Manager データベースに保留データが含まれていないようにしてください。保留データとは、データベースに対してコミットされていないデータのことです。Security Manager データベースに保留データが含まれている場合は、コミットされていないすべての変更をコミットまたは破棄してから、アップグレードを実行する前にデータベースをバックアップする必要があります。『Installation Guide for Cisco Security Manager 4.25』には、アップグレードするためのデータベースの準備に必要な手順に関する完全な説明が含まれています。
- 他の Web サーバーまたはデータベースサーバー（IIS や MS-SQL など）を実行しているサーバーへの Security Manager のインストールはサポートしていません。これを行うと、予期しない問題が発生し、Cisco Security Manager へのログインまたは Cisco Security Manager の使用ができなくなる可能性があります。
- アップグレードする前に、次の点に十分に注意してください。
  - アップグレードするすべてのアプリケーションが現在正しく機能していること、および有効なバックアップを作成できること（つまり、バックアッププロセスがエラーなしで完了すること）を確認してください。アップグレード前にアプリケーションが正しく機能していない場合、アップグレードしてもアプリケーションが正しく機能しない可能性があります。

（注） 一部のユーザーがシステムに対し、マニュアルにない、サポートされていない変更を加えているため、バックアッププロセスでインストールされているすべての CiscoWorks アプリケーションがバックアップされない問題をシスコは把握しています。インストールガイドに記載されているアップグレードプロセスは、システムの意図された機能が破壊されていないことを前提としています。すべてのデータよりも少ないデータをバックアップするバックアップを作成する場合は、更新を実行する前に、必要なすべてのバックアップデータがあることを確認する責任があります。これらのサポートされていない変更を元に戻すことを強くお勧めします。それ以外の場合は、古いバージョンと同じサーバーに製品をインストールするインラインアップグレードを実行しないでください。代わりに、更新したアプリケーションを新しいクリーンなサーバーにインストールし、データベースのバックアップを復元します。

- Cisco Security Manager 4.12 SP2 では、インラインアップグレードはサポートされていません。4.12SP2 から 4.13 または 4.14 にアップグレードする場合は、リモートアップグレードの手順に従い、『Installation Guide for Cisco Security Manager 4.25』の「Resolving database errors while upgrading from Cisco Security Manager 4.12 SP2」セクションに記載されている手順を参照して、データベースの移行に関する問題を解決してください。

（注） この例外は、Cisco Security Manager 4.12 からアップグレードする場合には適用されません。

- ご使用のクライアントよりも新しいバージョンを実行している Security Manager サーバにログインすると、通知が表示され、一致するクライアントバージョンをダウンロードするオプションが提供されます。
- Security Manager 4.12 から、インストール時間を短縮するために、AUS および Security Manager クライアントが同時にインストールされます。
- CiscoWorks Common Services 4.2.2 が Security Manager または AUS のインストール時に自動的にインストールされます。
- データベースの移行エラーが発生した場合はエラーメッセージが表示されます。これが表示されるのは、停止しなくてもインストールを先に進めることが可能な時点です。
- 最適なパフォーマンスのために、ディスクサイズの 50 GB 増加ごとにディスクの最適化を行うことを推奨します。

注意 頻繁に最適化を行うことによって、最終的にディスク障害を引き起こす、不良セクタを防ぐこともできます。

- バージョン 4.4 以降、Security Manager にはサーバーインストーラに Windows ファイアウォール設定スクリプトが含まれます。このスクリプトは、Windows ファイアウォールが正しく安全に機能するために必要なポートを開閉するプロセスを自動化します。これは、Security Manager サーバを強化する目的で行われます。

重要 Security Manager プロパティファイルで値を設定するときは、ファイル内の必要な値のみを変更するようにしてください。既存のプロパティファイルからコンテンツ全体をコピーして新しいプロパティファイルに追加すると、同じファイルに重複するエントリが作成され、展開が失敗する可能性があります。

特記事項

次の注意事項は、Security Manager 4.25 リリースに適用されます。

- 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、次の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。

  3. KB2919355、KB2932046、KB2959977、KB2937592、KB2938439、KB2934018
  4. 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。

- ソフトウェアバージョン 9.6(2) 以降を実行しているマルチコンテキスト ASA デバイスのリモートアクセス VPN の場合、デバイスは flash:/ ディレクトリで設定された storage-url を disk0:/ に変更します。デバイスが設定を変更するため、Security Manager はデバイス設

定を無効にして、設定をデバイスに再度プッシュします。これは、Security Manager バージョン 4.12 の制限です。

- [ポリシーオブジェクトマネージャ（Policy Object Manager）]>[アクセス制御リスト（Access Control List）]>[統合ACL（Unified ACL）] で、いずれかのデバイス設定で使用されている ACL を右クリックして [使用状況の検索（Find Usage）] を選択した場合、[使用状況の検索（Find Usage）] オプションには、統合アクセスリストで設定されているデバイスのリストは表示されません。
- Cisco Security Manager は、Transport Layer Security（TLS）およびセキュアソケットレイヤ（SSL）プロトコルに OpenSSL を使用していました。バージョン 4.13 以降、Cisco Security Manager は OpenSSL バージョン 1.0.2 を Cisco SSL バージョン 6.x に置き換えました。Cisco SSL は、完全な FIPS 検証による FIPS 準拠を可能にし、高速で費用対効果の高い接続を実現します。Cisco SSL のコモンクライテリアモードにより、コンプライアンスが容易になります。OpenSSL と比較して、Cisco SSL は機能が進んでいます。Cisco SSL の製品セキュリティベースライン（PSB）要件により、ログイン情報とキーの管理、暗号化標準規格、スプーフィング対策機能、整合性と改ざん防止といったセキュリティの重要な側面が保証され、セッション、データ、ストリームの管理と運用が保護対象となります。バージョン 4.17 では、SSL 1.0.2N が使用されています。
- Security Manager は、差分設定のみを Configuration Engine に送信し、そこで特定のデバイスがその設定を取得します。完全な設定はデバイスにプッシュされません。したがって、デバイスの OSPF、VLAN、およびフェールオーバーでの動作は次のようになります。
  - VLAN：Security Manager は IOS デバイスでの VLAN コマンドの検出をサポートしますが、VLAN コマンドの動的動作はサポートしません。VLAN ポリシーにユーザー主導の変更がある場合、Security Manager は差分設定および完全な設定でコマンドを生成します。つまり、通常のプレビューまたは展開では、Security Manager は完全な設定で VLAN コマンドを生成しません。したがって、Security Manager で生成された設定とデバイスの設定には違いが見られます。

（注） バージョン 4.21 以降、Cisco Security Manager は IOS ルータをサポートしていません。

  - ASA や FWSM などのファイアウォールデバイスおよび IOS デバイスのフェールオーバーポリシー：Security Manager は、フェールオーバーデバイスの動的動作をサポートしていません。つまり、HA のプライマリユニットには「failover lan unit primary」コマンドがあり、セカンダリユニットには「failover lan unit secondary」コマンドがあります。スイッチオーバーが発生すると、Security Manager は「failover lan unit primary」との比較を試み、差分設定を生成します。これは展開の失敗につながります。

（注） Security Manager は、「動的」CLI コマンドをサポートしていません。たとえば、CLI コマンドのシンタックスが変更された場合、「primary」キーワードは「secondary」に変更されます。これは Security Manager ではサポートされません。

- 次の ASA ポリシーは、Security Manager バージョン 4.8 以降でサポートされています。

  — SSL

  — EIGRP

したがって、これらのポリシーは、新しい 4.8 バージョン以降のインストールではデフォルトで管理されます。ただし、Security Manager をバージョン 4.7 から 4.8 に、またはバージョン 4.7 から 4.9 にアップグレードする場合、デフォルトでは、上記のポリシーはインラインおよびリモートでアップグレードされたサーバーの両方で管理されません。

Security Manager 4.7 から 4.9 にアップグレードする場合、SSL および EIGRP ASA ポリシーに加えて、次の ASA ポリシーも管理対象外になります。

— ルートマップ

— CLI プロンプト

— 仮想アクセス

— AAA Exec 認証

以前のバージョンの Security Manager でサポートされていなかったコマンドを使用しているデバイスがある場合、これらのコマンドは、このバージョンの Security Manager へのアップグレードの一部として Security Manager に自動的に読み込まれません。これらのコマンドは Security Manager で設定されたターゲットポリシーの一部ではないため、展開してデバイスに戻すとデバイスから削除されます。次の展開でこれらのコマンドが正しくプロビジョニングされるように、Security Manager で新しく追加された属性に正しい値を設定することをお勧めします。デバイスからプラットフォーム設定を再検出することもできます。ただし、デバイスに割り当てられている共有の Security Manager ポリシーを保存および復元するには、必要な手順を実行する必要があります。

（注） ルートマップが ASA で設定され、同じルートマップが OSPF ポリシーで使用されている場合、Security Manager 4.7 から Security Manager 4.9 にアップグレードした後、OSPF ページに赤いバナーが表示されます。この問題を解決するには、ASA を再検出する必要があります。

- ダイナミック アクセス ポリシーなどの特定のリモートアクセス VPN ポリシーに、オンザフライで統合 ACL オブジェクトを作成することもできます。ただし、オンザフライで統合 ACL オブジェクトを作成すると、Cisco Security Manager にはエラーメッセージが表示されます。[セレクタ（Selector）] ウィンドウで作成した ACL を再度追加し、ポリシーを保存する必要があります。

- S2S マネージャを使用して作成されたサイト間 VPN の IKEv2 認証に PKI 仕様が選択され、PKI 仕様にトラストポイントが選択されている場合は、対応するトラストポイントを [リモートアクセス VPN（Remote Access VPN）] > [公開キーインフラストラクチャ（Public Key Infrastructure）] で選択する必要があります。
- Security Manager によって管理される ASA をリリース 8.2(x) 以前からリリース 8.3(x) 以降にアップグレードする場合は、NAT 再検出オプションを使用して NAT ポリシーを再検出する必要があります（デバイスを右クリックして [デバイスでポリシーを検出（Discover Policies on Device）] を選択し、検出する唯一のポリシータイプとして NAT ポリシーを選択します）。このオプションは、既存の共有ポリシー、継承、flex-config などを保持しながら、デバイス設定と一致するように Security Manager 設定を更新します。

ASA デバイスを 8.4.x から 9.0.1 にアップグレードすると、デバイスポリシーが統合形式に変換されます。NAT 再検出オプションを使用して統合 NAT ルールを再検出するか、Security Manager のルールコンバータを使用して既存の NAT ポリシーを統合 NAT ポリシーに変換できます。詳細については、『User Guide for Cisco Security Manager』またはオンラインヘルプの「Converting IPv4 Rules to Unified Rules」トピックを参照してください。

これらのポリシーを統合ファイアウォールルール形式で管理する場合は、アクセスルール、AAA ルール、インスペクションルールなどの他のファイアウォールルールにルールコンバータを使用することもできます。

- Security Manager ですでに管理しているデバイスを 8.x から 9.0(1) 以降にアップグレードする場合は、Security Manager がデバイスを 9.x デバイスとして解釈し始めるようデバイスインベントリを再検出する必要があります。そして、Security Manager が適切なポリシータイプを検索して検出できるようデバイスのポリシーを再検出する必要があります。または、Security Manager からデバイスを削除してから、デバイスを再度追加することもできます。
- Security Manager ですでに管理しているデバイスに対して次のいずれかのアップグレードを実行する場合。

— 7.x から 8.x へ

— 下位バージョンから 8.3(1) 以降へ

— 8.3(x) から 8.4(2) 以降へ

この場合、Security Manager でデバイスを再検出する必要があります。これは、2 つのリリース間で大幅なポリシー変更が行われたために必要です。

これらのシナリオの詳細については、次の URL にある『User Guide for Cisco Security Manager 4.25』の「Validating a Proposed Image Update on a Device」というタイトルのセクションを参照してください。

https://www.cisco.com/c/ja_jp/support/security/security-manager/products-user-guide-list.html

- ASA 8.3 ACL は、変換された（NAT）アドレスではなく、デバイスの実際の IP アドレスを使用します。アップグレード中に、実際の IP アドレスを使用するようにルールは変換されます。他のすべてのデバイスタイプと古い ASA バージョンは、ACL で NAT アドレスを使用していました。

- ASA 8.3 のデバイスのメモリ要件は、古い ASA リリースよりも高くなります。アップグレードの前に、ASA のマニュアルで説明されているように、デバイスが最小メモリ要件を満たしていることを確認してください。Security Manager は、最小要件を満たしていないデバイスへの展開をブロックします。
- クラスタモードの ASA デバイスの場合、Security Manager はクラスタ全体を単一ノードとして扱い、メインクラスタの IP アドレスを使用してクラスタを管理します。メイン クラスタ IP アドレスは、そのクラスタのための固定アドレスであり、常に現在のマスター ユニットに属します。マスターノードが変更されると、クラスタの SNMP エンジン ID も変更されます。このような場合、Security Manager は、クリアテキストパスワードが設定されているすべての SNMP サーバーのユーザーに対して CLI を再生成します。Security Manager は、暗号化されたパスワードを使用して設定されたユーザーの CLI を再生成しません。

SNMP ページの [SNMPエンジンIDの取得（Get SNMP Engine ID）] ボタンを使用して、現在クラスタのマスターユニットとして機能しているデバイスからエンジン ID を取得できます。

- ロールバック機能は、ASA クラスタではサポートされていません。したがって、ASA クラスタ設定をロールバックしようとしないでください。
- Common Services 内の Device and Credential Repository（DCR）機能は、Security Manager 4.8 以降のバージョンではサポートされていません。
- LACP 設定は、IPS 4500 デバイス シリーズではサポートされていません。
- IPS 5.x+ アプライアンス、Catalyst および ASA サービスモジュール、およびルータ ネットワーク モジュールにシグネチャの更新をインストールするには、Cisco Services for IPS サービスライセンスが必要です。
- パフォーマンスの低下やシステムの予期しない動作が発生する可能性があるため、データベースに直接接続しないでください。
- データベースに対して SQL クエリを実行しないでください。
- ブラウザビューにオンラインヘルプページが空白で表示される場合は、ブラウザを更新します。
- IPS デバイスを管理しない場合は、次のパフォーマンス調整手順の実行を検討してください。$NMSROOT \MDC\ips\etc\sensorupdate.properties の packageMonitorInterval の値を、初期デフォルト値の 30,000 ミリ秒から、より頻度の低い値である 600,000 ミリ秒に変更します。この手順を実行することにより、いくらかパフォーマンスが向上します。$NMSROOT は、Common Services インストールディレクトリ（デフォルトは C:\Program Files (x86)\CSCOpx）のフルパス名です。
- Security Manager に含まれる IPS パッケージには、IPS デバイスの更新に必要なパッケージファイルは含まれていません。更新を適用する前に、Cisco.com またはローカル更新サーバから IPS パッケージをダウンロードする必要があります。ダウンロードされたバージョンにはすべての必要なパッケージ ファイルが含まれ、Security Manager の初期インストールに含まれていた部分的なファイルと置き換えられます。

- Cisco Security Manager 4.4 から、CiscoWorks Common Services のホームページの「License Management」リンクが削除されました。
- CsmReportServer および CsmHPMServer は、64 ビット JRE でサポートされるようになりました。
- 「rsh」サービスが手動開始モードに変更されました。必要に応じて手動で開始できます。
- PCI に準拠するために、Cisco Security Manager 4.15 および 4.16 では、TLS 1.0 と TLS 1.1 がそれぞれ無効になりました。したがって、4.16 以降では、Cisco Security Manager は TLS 1.2 バージョンのみを使用していました。ただし、ISE 1.3 サーバーおよびその下位バージョンは TLS 1.2 をサポートしていません。これは、リリース 4.15 以降の Cisco Security Manager でのレガシー ISE 設定に影響します。この非互換性により、ISE サーバーと Cisco Security Manager の統合が妨げられます。ISE 1.3 以前のバージョンを Cisco Security Manager と正常に統合する必要がある場合は、『User Guide for Cisco Security Manager 4.19』の「Resolving errors while integrating ISE server with Cisco Security Manager」セクションを参照してください。
- バージョン 4.19 以降、Cisco Security Manager は、DES アルゴリズムを使用したデバイス SSL 証明書をサポートしていません。デバイスの SSL が DES アルゴリズムを使用している場合、デバイスを追加しようとすると、Security Manager にエラーが表示されます。このエラーは、セキュリティの脆弱性を理由として、JRE がデフォルトで DES アルゴリズムを無効にするために発生します。
- バージョン 4.21 以降、Cisco Security Manager では、すべてのアグリゲーション サービス ルータ、統合サービスルータ、埋め込み型サービスルータ、および Cisco IOS ソフトウェアで動作するすべてのデバイスについて、バグ修正または拡張機能のサポートを含むサポート全体が終了します。
- バージョン 4.21 以降、Cisco Security Manager は、ASA 9.14(1) 以前のデバイスの ASDM の相互起動をサポートしています。ただし、この機能を利用するには、CLI **http server basic-auth-client Java** が ASA で手動で設定されていることを確認してください。
- 競合検出が無効になっているときに Security Manager を有効にして空き領域を増やすには、クライアントの LAX ファイルに次の変更を加えます。

```
# LAX.NL.JAVA.OPTION.ADDITIONAL
# required for optimized garbage collection
lax.nl.java.option.additional=-client -Djdk.tls.client.protocols="TLSv1.2" -XX:+UseG1GC
 -XX:NewRatio=3 -XX:PermSize=64m -XX:MaxPermSize=128m -XX:+HeapDumpOnOutOfMemoryError
 -XX:HeapDumpPath=./logs -XX:+UseCompressedOops -Xdebug
-Xrunjdwp:transport=dt_socket,address=5005,server=y,suspend=n
```

- ASA デバイス検出時にグループポリシーに vpn-tunnel-protocol を設定しない場合、CSM は DfltGrpPolicy から vpn-tunnel-protocol 値を継承することでグループポリシーの検出を行います。
- Cisco Security Manager は、ASA 9.17(1) 以降のデバイスの FPR-3100 シリーズのデバイスをサポートします。
- バージョン 4.24 以降、次の機能は ASA 9.17(1) 以降のデバイスの CSM から廃止されました。

- [ASAグループポリシー（ASA Group Policies）] ダイアログボックスの [テクノロジー設定（Technology Settings）] 要素の下にある SSL クライアントレス機能
- Smart Tunnel[1]、Auto Start Smart Tunnel[1]、Smart Tunnel Network List[1]、Smart Tunnel Auto Signon Server List[1]、Port Forwarding List[1]、Auto Start Port Forwarding[1]、ASA グループポリシー SSL VPN クライアントレス設定の Port Forwarding Applet Name[1] 機能
- ダイナミック アクセス ポリシーの設定のポートフォワーディング機能
- SSL VPN の高度な設定（ASA）でのオンスクリーンキーボード機能の有効化
- SSL VPN コンテンツリライトルールの設定（ASA）でのコンテンツリライト機能

警告

このリリースで未解決のバグおよび解決済みのバグには、Cisco Bug Search Tool を使用してアクセスできます。この Web ベース ツールから、この製品やその他のシスコハードウェアおよびソフトウェア製品でのバグと脆弱性に関する情報を保守するシスコ バグ トラッキング システムにアクセスできます。

（注） Cisco Bug Search Tool にログインしてこのツールを使用するには、Cisco.com アカウントが必要です。アカウントがない場合は、アカウントを登録できます。

Cisco Bug Search Tool の詳細については、Bug Search Tool（BST）ヘルプおよび FAQ を参照してください。

未解決の警告

バージョン4.25には、重大度3以上の未解決のバグはありません。次のリンクで、このリリースおよびこのリリースより前のリリースで未解決のバグの詳細を確認できます。

- 未解決の警告（4.25 より前のリリース）
- 未解決の警告（リリース 4.25（重大度 3 以上））
- 未解決の警告（リリース 4.25（重大度 4 以上））

解決済みの警告

- 解決済みの警告：リリース 4.25

  これより前のリリースで解決された警告のリストについては、次のドキュメントを参照してください。

http://www.cisco.com/c/en/us/support/security/security-manager/products-release-notes-list.html

次の作業

（注） 次の表のリンクは、Cisco Security Manager バージョン 4.25 以前に関連しています。

目的	操作手順
Security Manager サーバーまたはクライアントソフトウェアをインストールする。	『Installation Guide for Cisco Security Manager』を参照してください。
基本を理解する。	Security Manager を起動すると自動的に表示される対話形式の「JumpStart」ガイドを参照してください。
製品をすぐに起動して実行する。	オンラインヘルプの「Getting Started with Security Manager」か、『User Guide for Cisco Security Manager』の第 1 章を参照してください。
製品の設定を完了する。	オンラインヘルプの「Completing the Initial Security Manager Configuration」か、『User Guide for Cisco Security Manager』の第 1 章を参照してください。
ユーザの認証および認可を管理する。	オンラインヘルプの以下のトピックを参照するか、『Installation Guide for Cisco Security Manager』の第 7 章を参照してください。 • ユーザ権限のセットアップ • Security Manager と Cisco Secure ACS の統合
デバイスをブートストラップする。	オンラインヘルプの「Preparing Devices for Management」か、『User Guide for Cisco Security Manager』の第 2 章を参照してください。

通信、サービス、およびその他の情報

- シスコからタイムリーな関連情報を受け取るには、Cisco Profile Manager でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、シスコサービスにアクセスしてください。
- サービス リクエストを送信するには、シスコサポートにアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、Cisco Marketplace にアクセスしてください。

- 一般的なネットワーク、トレーニング、認定関連の出版物を入手するには、Cisco Press にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、Cisco Warranty Finder にアクセスしてください。

Cisco バグ検索ツール

Cisco Bug Search Tool（BST）は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理する Cisco バグ追跡システムへのゲートウェイとして機能する、Web ベースのツールです。BST は、製品とソフトウェアに関する詳細な障害情報を提供します。

このマニュアルは、「Communications, Services, and Additional Information」のセクションに記載されているマニュアルと併せてご利用ください。

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

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。