Security Manager のライセンス

この章の情報を使用して、Cisco Security Manager 4.26 をインストールおよび使用するために必要なライセンスを決定できます。さらにこの章では、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。

この章の情報を使用して、Cisco Security Manager 4.27 をインストールおよび使用するために必要なライセンスを決定できます。さらにこの章では、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。

いくつかの注釈を除き、この章ではライセンス インストールについて説明しません。「サーバーアプリケーションのインストールとアップグレード」を参照してください。

この章では、どの Security Manager サーバ ライセンスが必要かを判断する手引きとして、デバイス数について説明します。

ライセンスタイプ

Cisco Security Manager には、Standard と Professional の 2 つの基本ライセンスタイプがあります。基本ライセンスとは別に、Cisco Security Manager には次の機能があります。

基本ライセンス（Standard および Professional）

表 1 : 使用可能な基本ライセンスのリスト に、Cisco Security Manager 4.26 で使用可能な Standard および Professional の基本ライセンスのリストを示します。

表 *1* : 使用可能な基本ライセンスのリスト

ライセンス名	ライセンスの略称	管理可能なデバイスの台数（購入するライセンスのデバイス数について （5 ページ） を参照）
Standard-5	ST5	5
Standard-10	ST10	10
Standard-25	ST25	25
Professional-50	PRO50	50
Professional-100	PRO100	100
Professional-250	PRO250	250

表 2 : Professional 基本バージョンと Standard 基本バージョンの比較 に、Professional 基本バージョンと Standard 基本バージョンの比較を示します。

表 *2* : *Professional* 基本バージョンと *Standard* 基本バージョンの比較

機能	Professional でサポートされるか	Standard でサポートされるか
50、100、および 250 台単位でデバイス数を追加する差分（「追加」）デバイスライセンス パッケージのサポート	対応	×
Cisco Catalyst 6500 および 7600 シリーズ スイッチと関連サービス モジュールの管理に対するサポート	対応	×
ファイアウォール サービス モジュールの管理に対するサポート	対応	×
一時ライセンス（有効期限付きのライセンス）に対するサポート	あり	No（永久ライセンスのみサポート）

基本ライセンスを取得するには、Cisco.com のユーザ ID を保有（または取得）している必要があり、Cisco.com 上でソフトウェアのコピーを登録する必要があります。登録時に、購入したソフトウェア パッケージ内部の Software License Claim Certificate に貼られている Product Authorization Key（PAK; 製品認証キー）を入力する必要があります。

- Cisco.com の登録ユーザーの場合は、http://www.cisco.com/go/license から始めてください。
- Cisco.com の登録ユーザーでない場合は、http://tools.cisco.com/RPF/register/register.do から始めてください。

使用開始から 90 日以内のできるだけ早い時期に、製品の連続使用を保証するために必要なデバイスの台数分の Security Manager を登録する必要があります。アプリケーションを起動するたびに、評価ライセンスの残りの日数が表示され、評価期間中のアップグレードが促されます。評価期間が終了すると、ライセンスをアップグレードするまでログインできなくなります。

登録後に、基本ソフトウェア ライセンスが、指定した電子メールアドレスに送られてきます。ライセンスは安全な場所に保管してください。

Standard から Professional へのアップグレード ライセンス

Catalyst セキュリティブレードの管理など、ニーズが Standard ライセンスの機能を超えた場合や、導入デバイスが 25 台を超えた場合は、Cisco Security Manager Professional にアップグレードする必要があります。Standard から Professional へのアップグレードライセンスを購入できます。ただし、このアップブレードライセンスは基本ライセンスが Standard-25（「ST25」）ライセンスの場合にのみ適用できます。Standard から Professional へのアップグレードライセンスの発注可能な部品 ID（PID）は L-CSMSTPR-U-K9 です。

差分（「追加」）ライセンス

ご使用の基本ライセンスが（Standard 版や評価版ではなく）Professional 版の場合、差分（「追加」）ライセンスを購入して、管理可能なデバイスの台数を増やすことができます。差分ライセンスは、必要な数だけ購入できます。

以前のバージョンに対する差分（「追加」）ライセンスは、現在のバージョンに対しても有効です。たとえば、Security Manager 4.27 に対する Professional-50 ライセンスを保有している場合、4.22 の差分デバイスライセンスを使用できます。

差分ライセンスは、50、100、および 250 台単位でデバイス数を追加できます。

API ライセンス

API を使用するシスコ パートナーは、API ライセンスを保有している必要があります。API ライセンスを購入するには、基本 PRO ライセンスが必要です。API ライセンスには、次の 2 種類があります。

- 開発者ライセンス。これは、開発者がそれぞれの製品を Security Manager と統合するために使用できる 90 日間のライセンスです。
- 製品ライセンス。これは、特定のサードパーティ製品を使用するエンドカスタマーに必要なライセンスです。

（注） API の評価ライセンスはありません。開発者ライセンスと製品ライセンスはいずれも、API を使用するシスコ パートナーが明示的に注文する必要があります。

Northbound API ライセンスの注文可能部品 ID（PID）は L-CSMPR-API です。

ライセンスおよび導入シナリオ

アクティブ/アクティブ

[アクティブ/アクティブセットアップ（Active/Active setup）] で Cisco Security Manager の 2 つのライセンスを購入する必要があります。

アクティブおよびスタンバイ

Cisco Security Manager ライセンスでは、Cisco Security Manager の使用は 1 台のサーバ上でのみ許可されます。常に 1 台のサーバのみがアクティブになる場合は、スタンバイの Cisco Security Manager サーバ（ハイ アベイラビリティ設定やディザスタ リカバリ設定などで使用される）に別個のライセンスを用意する必要はありません。これは、ハイ アベイラビリティ（HA）が使用されている場合にも当てはまります。

（注） スタンバイ サーバを使用するユーザは、定期的にアクティブ サーバからデータベースを手動で復元する必要があります。

ライセンスタイプと適用性

Cisco Security Manager 4.27 のライセンスとその適用性を表 3 : ライセンスとその適用性 に示します。

表 *3:* ライセンスとその適用性

ライセンス	適用性	説明
L-CSMST-5-K9 L-CSMST-10-K9 L-CSMST-25-K9 L-CSMPR-50-K9 L-CSMPR-100-K9 L-CSMPR-250-K9	基本ライセンス（Standard および Professional ライセンス）	
L-CSMPR-LIC- 50/100/250	差分ライセンス	すべての Professional ライセンスに適用可能
L-CSMSTPR-U-K9	Standard ライセンスから Professional ライセンスへのアップグレード	Cisco Security Manager Standard 25-Device Limit から Cisco Security Manager Professional へのアップグレード
L-CSMPR-API	API の場合	

コンポーネント アプリケーションに対するライセンス

一部のコンポーネント アプリケーションには、ライセンス ファイルは必要ありません。

- Common Services

購入するライセンスのデバイス数について

Security Manager では、次のいずれかをデバイス インベントリに追加すると、（ライセンスで許可される台数から）デバイス数が 1 つ消費されます。

- 物理デバイス
- セキュリティ コンテキスト
- 追加された各 Cisco Catalyst 6500 シリーズのサービス モジュール
- 仮想センサー

Advanced Inspection and Prevention Security Services Module（AIP-SSM）、IDS Network Module、IPS Advanced Integration Module（IPS AIM）、およびホスト デバイスにインストールされた AIP-SSC 5 および Catalyst 6500 または 7600 以外のデバイスに対してサポートされるその他のモジュールは、デバイス数を消費しません。ただし、追加の仮想センサー（最初のセンサーの後に追加されたセンサー）はデバイス数を消費します。

Firewall Services Module（FWSM）または ASA デバイスの場合は、モジュール自体がデバイス数を消費し、セキュリティコンテキストが追加されるたびに追加のデバイス数を消費します。たとえば、2 つのセキュリティ コンテキストを含む FWSM は、モジュール用、管理コンテキスト用、2 つめのセキュリティ コンテキスト用の 3 つのデバイス数を消費します。

特殊なケースとして、管理対象外デバイスがあります。Security Manager では、管理対象外デバイスをデバイスインベントリに追加することができます。管理対象外デバイスとは、デバイスプロパティ内で [Cisco Security Managerでの管理（Manage in Cisco Security Manager）] を選択解除したデバイスのことです。管理対象外デバイスはデバイス数を消費しません。

別のクラスの管理対象外デバイスは、トポロジ マップに追加されたオブジェクトです。[マップ（Map）] > [マップオブジェクトの追加（Add Map Object）] コマンドを使用して、ネットワーククラウド、ファイアウォール、ホスト、ネットワーク、ルータなどのさまざまなタイプのオブジェクトをマップに追加できます。このようなオブジェクトは、デバイスインベントリに含まれないため、デバイス数を消費しません。

どの Security Manager サーバーライセンスを必要とするかを決定するため判断すべき、デバイス数を決定するには、表 4 : デバイス数の決定 を参照してください。

ヒント　どの Security Manager サーバーライセンスを必要とするかを決定することを目的として、デバイスは、Security Manager 4.22 に対して Security Manager 4.27 の場合と同様にカウントされます。

表 *4:* デバイス数の決定

デバイス（**Device**）	モード（コンテキストとも呼ばれる）	デバイス数（またはライセンス数、単にライセンスとも呼ばれる）	説明
スタンドアロン ファイアウォール デバイス			
任意のスタンドアロン ファイアウォール デバイス	シングル コンテキスト モード	1	
任意のスタンドアロン ファイアウォール デバイス	マルチ コンテキスト モード	*c*、ここで *c* はシステム コンテキスト以外のコンテキスト数です。	
ファイアウォール ブレード			
任意のスタンドアロン ファイアウォール ブレード	シングル コンテキスト モード	1	

デバイス（Device）	モード（コンテキストとも呼ばれる）	デバイス数（またはライセンス数、単にライセンスとも呼ばれる）	説明
任意のスタンドアロン ファイアウォール ブレード	マルチ コンテキスト モード	*c*、ここで *c* はシステム コンテキスト以外のコンテキスト数です。	**例**： この表の下の「マルチ コンテキスト モードのスタンドアロン ファイアウォール ブレードの例（9 ページ）」を参照してください。
フェールオーバー構成のファイアウォール			
フェール オーバー構成の任意のファイアウォール	シングル コンテキスト モード	1	
フェール オーバー構成の任意のファイアウォール	マルチ コンテキスト モード	*c*、ここで *c* はシステム コンテキスト以外のコンテキスト数です。	
スタンドアロン IPS デバイス			
任意のスタンドアロン IPS デバイス		*n*、ここで *n* は仮想センサーの数で、仮想センサー vs0 が含まれます。	追加の仮想センサー（最初のセンサーの後に追加された）が 1 ライセンスを個別に消費します。
非スタンドアロン IPS デバイス			
IPS モジュール、IPS ブレードおよび IPS 仮想マシン		*n*、ここで *n* は仮想センサーの数で、仮想センサー vs0 が含まれます。	IPS モジュール、IPS ブレードおよび IPS 仮想マシンは Security Manager で個別に検出されます。 IPS 仮想マシンは 5512-X、5515-X、5525-X、5545-X および 5555-X である Cisco ASA 5500 シリーズの適応型セキュリティ アプライアンスで使用されます。
ASA フェールオーバー構成に含まれる IPS モジュールまたは仮想マシン			

デバイス（**Device**）	モード（コンテキストとも呼ばれる）	デバイス数（またはライセンス数、単にライセンスとも呼ばれる）	説明
各 IPS デバイス		*n*、ここで *n* は仮想センサーの数で、仮想センサー vs0 が含まれます。	追加の仮想センサー（最初のセンサーの後に追加された）が 1 ライセンスを個別に消費します。
ASA ロード バランシング クラスタに関連するライセンス			
各 ASA ロードバランス クラスタ	シングル コンテキスト モード	*N*、ここで *N* はシングル コンテキスト ASA クラスタ内のノード数です。	システムと管理コンテキストで、1 個のコンテキストを表します
各 ASA ロードバランス クラスタ	マルチ コンテキスト モード	*N*c*、ここで *N* はマルチ コンテキスト ASA クラスタ内のノード数、*c* はコンテキストの数です。	システムと管理コンテキストで、1 個のコンテキストを表します。 ASA ロード バランシング クラスタに関連するライセンスの例 （9 ページ）も参照してください。
[除外デバイス（Excluded Devices）]			
Advanced Inspection and Prevention Security Services Module（AIP-SSM）		0 ただし、追加の仮想センサー（最初のセンサーの後に追加された）が 1 ライセンスを個別に消費します。	追加の仮想センサー（最初のセンサーの後に追加された）が 1 ライセンスを個別に消費します。
IDS ネットワーク モジュール		0 ただし、追加の仮想センサー（最初のセンサーの後に追加された）が 1 ライセンスを個別に消費します。	追加の仮想センサー（最初のセンサーの後に追加された）が 1 ライセンスを個別に消費します。
IPS Advanced Integration Module（IPS AIM）		0	

デバイス（Device）	モード（コンテキストとも呼ばれる）	デバイス数（またはライセンス数、単にライセンスとも呼ばれる）	説明
ホスト デバイスにインストールされた AIP-SSC 5 および Catalyst 6500 または 7600 以外のデバイスに対してサポートされるその他のモジュール		0	

マルチコンテキストモードのスタンドアロンファイアウォールブレードの例

ここでは、デバイス数を理解するうえで役立つコンテキストの例を示します。

次のコマンドが 2 つのセキュリティ コンテキスト（admin および ctx1）とともに、ファイアウォール システム上のシステム コンテキストで実行されました。

```
r41-appinfra-arsenal# sh context
Context Name Class Interfaces Mode URL
*admin default GigabitEthernet3/2, Routed disk0:/admin.cfg
Management0/0
ctx1 default Routed disk0:/ctx1.cfg
Total active Security Contexts: 2
r41-appinfra-arsenal# sh context count
Total active Security Contexts: 2
```

ASA ロード バランシング クラスタに関連するライセンスの例

ここでは、マルチ コンテキスト モードの ASA ロード バランシング クラスタのデバイス数の例を示しています。

```
3 Nodes with 4 security contexts each: License Count = 3 * 5 = 15.
```

必要なライセンスの決定

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。

- Security Manager 4.27 の新規インストール
- Security Manager 4.x からのアップグレード （10 ページ）

Security Manager 4.27 の新規インストール

Cisco Security Manager 4.27 を新規でインストールするには、該当する Cisco Security Manager ライセンスを購入する必要があります。

Security Manager 4.x からのアップグレード

- 有効な SAS 契約がある場合は、追加料金なしで Cisco Security Manager の最新バージョンにアップグレードできます。現在のライセンスは Security Manager インストールプログラムによって認識されて保持されるため、アップグレード中にライセンスを申請する必要はありません。
- SAS 契約のないユーザーは、SAS 契約を購入するか、有効な Security Manager 4.27 ライセンスを購入する必要があります。

（注） SAS 契約では、ユーザーは最新バージョンに無料でアップグレードできます。

90 日間の評価ライセンス

インストール時にライセンスを入力しないと、そのインストールは評価版になります。また、インストール時に [評価のみ（Evaluation Only）] を選択することもできます。「、Common Services、および のインストール」を参照してください。

評価ライセンスでは、使用可能なデバイスが 50 台までに制限されます。

評価ライセンスでは、Professional 版ライセンスと同じ権限が与えられます。ただし、差分ライセンスを評価版に適用することはできません。

4.x を新規に購入する場合の適切なライセンスの選択

新しい 4.x Cisco Security Manager のお客様の一般的なシナリオとライセンスオプションについては、次のように説明されています。

1. [基本（BASE）] : CSM 基本製品バージョンの選択
    1. Cisco Security Manager を使用して管理する必要があるデバイスの数に基づいて（将来の成長の見通しを考慮した後）、次を取得します。
2. L-CSMST5-K9/L-CSMST10-K9/L-CSMST25-K9（それぞれ 5、10、25 台以下のデバイスのネットワーク向け）
3. L-CSMPR-50-K9/L-CSMPR-100-K9/L-CSMPR-250-K9（大規模ネットワーク向け）。さらに、[差分（INCREMENTAL）] ライセンスを検討します。

1. Catalyst 6500 または FWSM/IDSM スイッチブレードを管理する必要がある場合は、L-CSMPR-50-K9 を選択します。
2. 標準ライセンスを取得したが、後で Catalyst スイッチまたはスイッチブレードを管理する必要が生じた場合、または 25 台を超えるデバイスを管理する必要が生じた場合は、L-CSMSTPR-U-K9 を取得して製品の PRO バージョンにアップグレードします。
3. すでに PRO ライセンスを購入しているが、後で 50 台を超えるデバイスを管理する必要が生じた場合は、4.x の差分ライセンスを取得します。

4. [差分（INCREMENTAL）] : 差分ライセンスではより多くのデバイスを管理できます。管理する必要があるネットワークのサイズに基づいて、次の情報を取得します。
   1. L-CSMPR-LIC-50/L-CSMPR-LIC-100/L-CSMPR-LIC-250（それぞれ 50、100、または 250 台の追加デバイスの管理を追加する場合）
   2. 大規模ネットワーク向け
5. 同じ Cisco Security Manager サーバーにインストールする場合は、[差分（INCREMENTAL）] ライセンスを複数購入してください。
6. 複数の Cisco Security Manager サーバーをインストールしてパフォーマンスを向上させる場合は、[基本（BASE）] ライセンスまたは [差分（INCREMENTAL）] ライセンスを購入してください。
7. サポート : [基本（BASE）] および [差分（INCREMENTAL）] ライセンスに加えて、同等の SAS 契約を購入する必要があります。SAS 契約があると、追加料金なしで Cisco Security Manager の最新バージョンにアップグレードできます。

既存の 4.x を使用している場合の適切なライセンスの選択

既存の 4.x Cisco Security Manager のお客様の一般的なシナリオとライセンスオプションについては、次のように説明されています。

1. [基本（BASE）] : CSM 4.x Standard から CSM 4.x PRO にアップグレードするには、L-CSMSTPR-U-K9 を購入し、成長に合わせて差分を追加します。
2. [差分（INCREMENTAL）] : すでに所有している既存の差分ライセンスは、最新の Cisco Security Manager バージョンにも適用されます。同じ数のデバイスを管理するために、新しい差分ライセンスを取得する必要はありません。大規模なネットワークのイベント管理をイネーブルにする場合は、複数の Cisco Security Manager サーバーの導入を検討する必要があります。これには、追加の [基本（BASE）] 製品ライセンスの取得が含まれます。
3.
4. サポート : CSM 4.x サポート契約は、CSM 4.27 を引き続きサポートします。

Security Manager またはコンポーネント アプリケーションに対するライセンスのインストール

Security Manager のインストール中に、ライセンス情報の入力を求められます。「、Common Services、および のインストール」を参照してください。

Common Services のインストール中に、ライセンス情報の入力を求められることはありません。Common Services にライセンス ファイルは必要ありません。

Security Manager またはコンポーネント アプリケーションに対するライセンスの更新

Security Manager またはコンポーネント アプリケーションに対するライセンス ファイルの更新方法については、Security Manager の更新を参照してください。

ライセンスに関するその他のマニュアル

使用可能なライセンスの種類やサポートされているアップグレードパスに関する詳細の他、購入可能な Cisco Software Application Support サービス契約については、http://www.cisco.com/en/US/products/ps6498/prod_bulletins_list.html [英語] で Security Manager の最新メジャーリリースの製品速報を参照してください。

ライセンスに関する支援

Security Manager のライセンスに関する問題については、Cisco Technical Assistance Center（TAC）の Licensing Department にお問い合わせください。

- 電話：+1（800）553-2447
- 電子メール：licensing@cisco.com
- http://www.cisco.com/tac

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。