ライセンス

この章の情報を使用して、Cisco Security Manager 4.5 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。第 5 章「サーバ 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。

この章の最後には、Cisco Security Manager API を使用するシスコ パートナーの API ライセンスに関する情報を示します。

Security Manager 4.5 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 4.5 の新規インストール

Cisco Security Manager 4.5 を新規でインストールするには、該当する Cisco Security Manager 4.5 ライセンスを購入する必要があります。Cisco Security Manager ライセンスの詳細については、http://www.cisco.com/en/US/products/ps6498/prod_bulletins_list.html にある製品速報を参照してください。

Security Manager 4.0、4.0.1、4.1、4.2、4.3 または 4.4 からのアップグレード

Security Manager 4.0、4.0.1、4.1、4.2、4.3 または 4.4 からアップグレードするためにライセンスを適用する必要はありません。既存のライセンスが有効です。

Security Manager 3.3 または 3.3.1 からのアップグレード

Cisco Security Manager 3.3 または 3.3.1 からアップグレードするお客様は、該当する Cisco Security Manager 4.5 ライセンスまたはバージョン アップグレード ライセンスを購入する必要があります。Cisco Security Manager ライセンスの詳細については、http://www.cisco.com/en/US/products/ps6498/prod_bulletins_list.html にある製品速報を参照してください。

Security Manager 3.2、3.2.1、または 3.2.2 からのアップグレード

Cisco Security Manager 3.2、3.2.1、または 3.2.2 からアップグレードするお客様は、該当する Cisco Security Manager 4.5 ライセンスまたはバージョン アップグレード ライセンスを購入する必要があります。Cisco Security Manager ライセンスの詳細については、http://www.cisco.com/en/US/products/ps6498/prod_bulletins_list.html にある製品速報を参照してください。

Security Manager のライセンスの説明

基本ライセンスとして Standard と Professional の 2 種類が提供されており、無料の 90 日間評価ライセンスもあります。

Standard および Professional

Cisco Security Manager 4.5 に対して使用可能な基本ライセンスのリストについては、表 2-1 を参照してください。

表 2-1　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（「デバイス数」（P.2-5）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

Professional 基本バージョンと Standard 基本バージョンの比較については、表 2-2 を参照してください。

表 2-2　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	Yes	No
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	Yes	No
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	Yes	No
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	Yes	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。

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 [Evaluation Only] を選択することもできます。「Security Manager サーバ、Common Services、および AUS のインストール」（P.5-2）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。

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

Standard から Professional へのアップグレード ライセンスを使用できます。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。

バージョン アップグレード ライセンス

3.3 などの以前のメジャー バージョンから Security Manager 4.5 にアップグレードする必要がある場合は、バージョン アップグレード ライセンスを購入できます。

バージョン アップグレード ライセンスは複数種類あります。各ライセンスは、以前のバージョンの特定の基本ライセンスと対応します。特定のアップグレード ライセンス（たとえば PRO50U）は、それに対応する基本ライセンス（たとえば PRO50）を以前のバージョンの Security Manager に適用していた場合にのみ使用できます。それ以外のアップグレード ライセンスは受け入れられません。

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 4.4 に対する Professional-50 ライセンスを保有している場合、4.3 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。

アクティブ サーバとスタンバイ サーバ

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。

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 にはライセンス ファイルが必要ありません。
- Auto Update Server にライセンス ファイルは必要ありません。

デバイス数

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
- 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 [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。[Map] > [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 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 2-3 を参照してください。

ヒント　必要な Security Manager サーバ ライセンスを決定することを目的として、デバイスは、Security Manager 4.5 に対して Security Manager 4.3 と 4.4 の場合と同様にカウントされます。

表 2-3　デバイス数の決定

デバイス	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）	コメント
除外デバイス			
Advanced Inspection and Prevention Security Services Module（AIP-SSM）		0	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、次の列のコメントを参照）	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。

表 2-3　デバイス数の決定

デバイス	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）	コメント
IPS Advanced Integration Module（IPS AIM）		0	
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	
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	
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。
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	
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：** この表の後のマルチ 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 ブレードの例を参照してください。

表 2-3　デバイス数の決定

デバイス	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）	コメント
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	
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			
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を、*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」も参照してください。

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.
```

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。「Security Manager サーバ、Common Services、および AUS のインストール」（P.5-2）を参照してください。

Common Services および AUS 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 にはライセンス ファイルが必要ありません。Auto Update Server 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」（P.5-15）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 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。

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