Firepower システムのライセンス

ここでは、Firepower システムのライセンスを適用する方法について説明します。

Firepower ライセンスについて

Firepower 製品（Firepower Management Center と管理対象デバイス）には基本的な操作のライセンスが含まれていますが、一部の機能については、この章で説明するように、個別のライセンスまたはサービス サブスクリプションが必要です。

「使用権」ライセンスに有効期限はありませんが、サービス サブスクリプションは定期的に更新する必要があります。

製品に必要なライセンスのタイプ（スマートまたはクラッシック）はそれを実行するハードウェアではなく、使用するソフトウェアによって異なります。

Firepower Management Center のライセンス要件

Firepower Management Center 管理対象デバイスにライセンスを割り当ててシステムのライセンスを管理できます。

単一の Firepower Management Center でクラッシック ライセンスを必要とするデバイスと、スマート ライセンスを必要とするデバイスの両方を管理できます。

ハードウェア FMC

ハードウェアの Firepower Management Center では、デバイスを管理するために追加のライセンスやサービス サブスクリプションを購入する必要はありません。

Virtual FMC

Firepower Management Center Virtual の場合には追加のライセンス要件があります。Firepower Management Center Virtual ライセンス （2 ページ）を参照してください。

Firepower Management Center Virtual ライセンス

通常、Firepower Management Center Virtual の場合は管理するデバイスごとにライセンスの付与資格が必要です。

高可用性ペア内に設定されている Firepower Threat Defense デバイスを FMCv で管理する場合にも、（ペアに 1 つではなく）デバイスごとに 1 つの付与資格が必要です。

複数インスタンスの展開では、セキュリティ モジュールごとに 1 つの付与資格が必要です。

標準的な接続されているスマート ライセンスでは、これらは永続ライセンスです。

特定の永続ライセンスでは、これらは期間ベースのライセンスとなります。

この付与資格は、異なる数の付与資格を持つ **Firepower MCv デバイス ライセンス**として Cisco Smart Software Manager に表示されます。

評価ライセンスに関する注意事項

評価ライセンスではすべての機能を使用できるわけではありません。評価ライセンスで使用できるのは機能の一部であり、評価ライセンスから標準ライセンスへの移行もシームレスに行われない場合があります。

たとえば、クラスタ内に Firepower Threat Defense のデバイスを設定している場合、評価ライセンスからスマート ライセンスに切り替えると変更を展開した時点でサービスが中断されます。

このライセンスに関する章と、各機能の展開に関連する章の情報にある評価ライセンスについての注意事項の情報を確認してください。

スマート ライセンスとクラシック ライセンス

管理対象デバイスの場合、必要なライセンス（スマートまたはクラシック）は、デバイスで実行されるソフトウェアによって異なります。いずれの FMC でも、スマートライセンスのデバイスと従来のライセンスのデバイスを同時に管理できます。各タイプのライセンスを個別に設定する必要があります。

ソフトウェア	ライセンスのタイプ	詳細情報
Firepower Management Center（ハードウェア）	なし	FMC ハードウェア モデル自体にはライセンスは必要ありません。
Firepower Management Center Virtual	デバイスの権限	Firepower Management Center Virtual ライセンス （2 ページ）を参照してください。
Firepower Threat Defense Firepower Threat Defense Virtual	スマート	Firepower Threat Defense デバイスのライセンス （4 ページ）を参照してください。
NGIPS ソフトウェア： • Firepower 7000/8000 シリーズ • ASA FirePOWER • NGIPSv	従来型	Firepower 7000/8000 シリーズのライセンス、ASA FirePOWER、および NGIPSv デバイス（従来のライセンス） （50 ページ）を参照してください。
その他すべてのソフトウェア（Firepower ハードウェア上で実行するものを含む）	ソフトウェア製品のライセンス情報を参照してください。	

Firepower Threat Defense デバイスでの展開のライセンス（スマート ライセンス）

Firepower Threat Defense デバイスにはスマート ライセンスが必要です。

Cisco Smart Licensing によって、ライセンスを購入し、ライセンスのプールを一元管理することができます。製品認証キー（PAK）ライセンスとは異なり、スマート ライセンスは特定のシリアル番号またはライセンス キーに関連付けられません。Smart Licensing を利用すれば、ライセンスの使用状況やニーズをひと目で評価できます。

また、Smart Licensing では、まだ購入していない製品の機能を使用できます。Cisco Smart Software Manager に登録すると、すぐにライセンスの使用を開始することも、後でライセンスを購入することもできます。これによって、機能の展開および使用が可能になり、発注書の承認による遅延がなくなります。

Firepower Threat Defense デバイスのライセンス

Firepower Threat Defense デバイスでは Smart Licensing が使用されます。

ステップ 1 Firepower の展開にスマート ライセンスが必要なことを確認してください。

スマート ライセンスとクラシック ライセンス （3 ページ）を参照してください。

展開に両方のタイプのライセンスが必要な場合は、スマート ライセンスが必要なデバイスについてはこの手順に従い、従来のライセンスを使用するデバイスについてはFirepower 7000/8000 シリーズのライセンス、ASA FirePOWER、および NGIPSv デバイス（従来のライセンス） （50 ページ）に記載の手順に従います。

ステップ 2 スマート アカウントをまだ持っていない場合は、1 つ作成します。

ライセンスを購入する前にスマートアカウントを取得することをお勧めします。新しいスマートアカウントを作成するには、ライセンスを保持するためのスマート アカウントの作成 （18 ページ）を参照してください。

（注） アカウント担当者が、ユーザのためにスマート アカウントを作成していることもあります。その場合は、https://software.cisco.com/#module/SmartLicensingで、Cisco Smart Software Manager（CSSM）のアカウントにアクセスできることを確認します。

ステップ 3 組織に必要なプラットフォーム ライセンスを把握します。

- Firepower Management Center 物理ハードウェア：

  このアプライアンスには必要なライセンスが付属しています。ライセンスを有効化するための操作は不要です。

- Firepower Management Center Virtual：

  追加のライセンスが必要です。詳細については、Firepower Management Center Virtual ライセンス （2 ページ）を参照してください。

  （クラシック ライセンスを使用するデバイスを FNCv でも管理する場合、クラッシク ライセンスを設定する際にそれらのデバイスにもこれらの付与資格が必要になります。）

- Firepower Threat Defense デバイス：

  各デバイスには、基本的な機能のためのライセンスが自動的に含まれています。詳細は、基本ライセンス （12 ページ）を参照してください。

  ベースのライセンスをアクティブ化するのに何も実行する必要はありませんが、次で説明するように、多くの機能で個別のライセンスが必要です。

ステップ 4 組織に必要な機能ライセンス（サービス サブスクリプションと呼ばれることもある）を把握します。

スマート ライセンスのタイプと制約事項 （9 ページ）およびサブトピックを参照してください。

ステップ 5 組織に必要な機能ライセンスまたはサービス サブスクリプションの数を確認してください。

- 一般に、各管理対象デバイスには、使用する各機能のライセンスが必要です。
- 高可用性ペアの Firepower Management Center の場合：

  FMC HA のライセンス要件を参照してください。
- 高可用性ペアの Firepower Threat Defense デバイスの場合：

  各デバイス（アクティブまたはスタンバイ）には、使用する各機能のライセンスが必要です。追加のライセンスは必要ありません。

  高可用性ペアでの FTD デバイスのライセンス要件を参照してください。
- シャーシ間またはシャーシ内クラスタ化 Firepower Threat Defense デバイスの場合：

  クラスタリングのライセンスを参照してください。
- 複数インスタンス展開の場合：

  複数インスタンス展開のライセンス （18 ページ）を参照してください。

ステップ 6 変換または移動の必要がある既存のライセンスがある場合：

- 従来のライセンスを Firepower Threat Defense に使用できるライセンスに変換するには：

  クラシック ライセンスまたは PAK からスマート ライセンスへの変換 （60 ページ）を参照してください。
- 別の Firepower Management Center に現在登録されているスマート ライセンスを転送するには：

  別の にスマート ライセンスを転送します。 Firepower Management Center （47 ページ）およびCisco Smart Software Manager から Firepower Management Center の登録解除 （48 ページ）を参照してください。
- 別の Firepower Threat Defense に現在登録されているスマート ライセンスを移動するには：

  管理対象デバイスからのスマート ライセンスの移動または削除 （46 ページ）を参照してください。

ステップ 7 Firepower アプライアンスのインターネット アクセスが制限されている場合：

状況に最も適したソリューションを決定します。

- エアギャップ展開のライセンスのオプション （25 ページ）を参照してください。
- Firepower Management Center はインターネットに接続されていないが、シスコのライセンス認証局に接続できる内部サーバに接続できるか、または手動でライセンスの更新を受信できる場合：

  Smart Software Satellite Server を展開します。詳細については、Smart Software Satellite Server の概要 （25 ページ）およびSmart Software Satellite Server の展開方法 （26 ページ）を参照してください。

- 展開が完全にエアギャップになっていて、ライセンス認証局や、ライセンス認証局に接続する Satellite Server に接続できない場合、または手動でライセンスの更新を受信できる場合：

  特定のライセンスの予約の概要 （27 ページ）を参照し、この手順の残りはスキップします。

ステップ 8 複数の Firepower Management Center アプライアンスがあり、1 つのプロキシでシスコのライセンス認証局に接続する場合は、次の手順を実行します。

Smart Software Satellite Server を展開します。詳細については、Smart Software Satellite Server の概要 （25 ページ）を参照してください。

ステップ 9 強力な暗号化を使用する機能を有効にしたいが、地理的な領域によって制限されている場合：

輸出規制対象の機能のライセンス （16 ページ）を参照してください。

ステップ 10 必要なライセンスを購入します。

シスコのセールス担当者または認定再販業者に問い合わせてください。

ステップ 11 再販業者やシスコのセールス担当者によってスマート アカウントにライセンスが追加されたことを確認します。

CSSM で https://software.cisco.com/#SmartLicensing-Inventory を参照します。[インベントリ（Inventory）] をクリックした後、[ライセンス（Licenses）] タブをクリックします。必要に応じてリストをフィルタリングします。ライセンスの名前を把握するために購入確認が必要な場合があります。

表示されると予想していたライセンスが表示されない場合は、正しい仮想アカウントを確認していることを確認します。この点についてサポートが必要な場合は、CSSM のリソース リンクを参照してください。

引き続きライセンスが表示されないか、またはライセンスが正しくない場合は、そのライセンスを購入した担当者に問い合わせてください。

ステップ 12 仮想アカウント（スマートアカウント）に予想していたライセンスが表示されたら、Firepower Management Center を CSSM に登録します。

Web インターフェイスを使用して、Firepower Management Center にライセンスを設定する必要があります。

- Firepower Management Center が CSSM に直接接続している場合：

  次のトピックを参照してください。

  - スマート ライセンス用の製品ライセンス登録トークンの取得 （20 ページ）および
  - スマート ライセンスの登録 （21 ページ）

- Firepower Management Center が Smart Software Satellite Server に接続している場合：

  Smart Software Satellite Server への接続の設定 （26 ページ）を参照してください。

- Firepower Management Center がインターネットから完全に分離されている場合：

  特定のライセンスの予約ステータス （38 ページ）およびサブトピックを参照してください。

ステップ 13 登録が正常に実行されたことを確認します。

Firepower Management Center Web インターフェイスで、[システム（System）]>[ライセンス（Licenses）]>[スマートライセンス（Smart Licenses）]に移動します。[製品登録（Product Registration）]に緑のチェックマークが表示されている必要があります。

ステップ 14 まだ実行していない場合は、デバイスを管理対象デバイスとして Firepower Management Center に追加します。

Firepower Management Center へのデバイスの追加を参照してください

ステップ 15 管理対象 Firepower Threat Defense デバイスへのライセンスの割り当て：

複数の管理対象デバイスへのライセンスの割り当て （43 ページ）を参照してください

ステップ 16 デバイスにライセンスが正常に追加されたことを確認します。

スマート ライセンスおよびスマート ライセンス ステータスの表示 （44 ページ）を参照してください。

ステップ 17 必要に応じて、高可用性とクラスタ化された展開のライセンスをセットアップします。

- 高可用性ペアの Firepower Management Center の場合：

  Firepower Management Center ハイ アベイラビリティの確立の前提条件を参照してください。

  FMC 高可用性ペアを設定すると、デバイスのライセンスはアクティブからスタンバイ管理センターに自動的に転送されます。ライセンスに固有の設定は不要です。

- 高可用性ペアの Firepower Threat Defense デバイスの場合：

  高可用性を設定する前に、アクティブとスタンバイの両方のデバイスに使用する機能のライセンスを割り当てます。デバイスにさまざまな機能のライセンスがある場合、スタンバイ デバイスのライセンスがアクティブなデバイスと同じ一連のライセンスで置き換えられます。

- クラスタ化 Firepower Threat Defense デバイスの場合：

  クラスタリングのライセンスを参照してください。ライセンスの手順は、FMC：クラスタの追加に含まれています。

次のタスク

- （オプション）従来のデバイス（7000/8000 シリーズ、ASA FirePOWER、NGIPSv）を管理する必要がある場合は、それらのデバイスにライセンスを設定します。

  Firepower 7000/8000 シリーズのライセンス、ASA FirePOWER、および NGIPSv デバイス（従来のライセンス） （50 ページ）を参照してください。

- 有効期間と期限を把握します。FirePOWER のライセンスとサービス サブスクリプションの期限切れ （64 ページ）を参照してください。

Smart Software Manager

Firepower機能のスマートライセンスを複数購入する場合は、それらのライセンスをCisco Smart Software Manager（http://www.cisco.com/web/ordering/smart-software-manager/index.html）で管理できます。Smart Software Manager では、組織のマスター アカウントを作成できます。

デフォルトでは、ライセンスはマスターアカウントの下のデフォルトの仮想アカウントに割り当てられます。アカウントの管理者として、たとえば、地域、部門、または子会社ごとに、追加の仮想アカウントを作成できます。複数の仮想アカウントを使用することで、多数のライセンスおよびアプライアンスの管理を行うことができます。

ライセンスとアプライアンスは、バーチャル アカウント別に管理します。バーチャル アカウントに割り当てられているライセンスを使用できるのは、そのバーチャルカウントのアプライアンスのみです。追加のライセンスが必要な場合は、別の仮想アカウントから未使用のライセンスを転用できます。また、仮想アカウント間でのアプライアンスの譲渡も可能です。

バーチャル アカウントごとに、製品インスタンス登録トークンを作成できます。各 Firepower Management Center を展開するか、または既存の FMC を登録する場合は、このトークン ID を入力します。既存のトークンの有効期限が切れている場合は、新しいトークンを作成できます。トークンの有効期限が切れても、そのトークンを使用して登録された FMC には影響しませんが、有効期限が切れたトークンを使用して FMC を登録することはできません。また、登録済み FMC は、使用するトークンに基づいてバーチャル アカウントに関連付けられます。

Cisco Smart Software Manager の詳細については、*Cisco Smart Software Manager User Guide*または https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager.html を参照してください。あるいは https://www.cisco.com/web/fw/softwareworkspace/smartlicensing/SSMCompiledHelps/ からもアクセスできる CSSM 内のオンライン ヘルプを参照してください。

License Authority との定期通信

製品ライセンスの権限付与を維持するために、製品は Cisco ライセンス認証局と定期的に通信する必要があります。

Firepower Management Center の登録に製品インスタンス登録トークンを使用すると、このアプライアンスがシスコのライセンス認証局に登録されます。ライセンス認証局は、Firepower Management Center とライセンス認証局の間の通信用に ID 証明書を発行します。この証明書の有効期間は 1 年ですが、6 か月ごとに更新されます。ID 証明書の期限が切れた場合（通常は、9 ヵ月または 1 年間通信がない状態）、Firepower Management Center は登録解除状態に戻り、ライセンス機能の使用は中断されます。

Firepower Management Center は、定期的にライセンス認証局と通信します。Smart Software Manager で変更を加えた場合は、Firepower Management Center 上で認証を更新すると、その変更がすぐに適用されます。また、スケジュールどおりにアプライアンスが通信するのを待つこともできます。

Firepower Management Center は、Cisco Smart Software Manager を介してライセンス認証局に直接インターネットでアクセスするか、スケジュールした期間でスマート ソフトウェア サテライト サーバを介してアクセスする必要があります。通常のライセンスに関する通信は 30 日ごとに行われますが、これには猶予期間があり、アプライアンスはホームをコールすることなく

最大で 90 日間は動作します。90 日が経過する前にライセンス認証局と連絡を取る必要があります。

オプションで、ライセンス認証局との通信用プロキシとして機能するように Smart Software サテライト サーバを設定することができます。詳細については、Smart Software Satellite Server の概要 （25 ページ）を参照してください。

Firepower機能のサービスサブスクリプション（スマートライセンス）

一部の機能にはサービス サブスクリプションが必要です。

サービス サブスクリプションは、所定の時間内限定で、管理対象デバイス上の特定の Firepower 機能を有効にします。サービス サブスクリプションは、1 年、3 年、または 5 年単位で購入できます。サブスクリプションの期限が切れると、サブスクリプションの更新が必要であることが通知されます。Firepower Threat Defense デバイスのサブスクリプションの期限が切れた場合でも、関連する機能は引き続き使用できます。

表 *1*:サブスクリプションおよび対応するスマート ライセンス

購入するサブスクリプション	Firepower システム内で割り当てるスマート ライセンス
T	脅威
TC	脅威 + URL フィルタリング
TM	脅威 + マルウェア
TMC	脅威 + URL フィルタリング + マルウェア
URL	URL フィルタリング（脅威に追加するか、脅威なしで使用できます）
AMP	マルウェア（脅威に追加するか、脅威なしで使用できます）

スマート ライセンスを使用する管理対象デバイスを購入すると、基本ライセンスが自動的に提供されます。このライセンスは無制限であり、システム アップデートを使用可能にします。Firepower Threat Defense デバイスでは、すべてのサービス サブスクリプションがオプションです。

スマート ライセンスのタイプと制約事項

ここでは、Firepower システムの導入環境で使用可能なスマート ライセンスのタイプについて説明します。Firepower Management Center では、Firepower Threat Defense のデバイスを管理するためスマート ライセンスが必要です。

次の表に、Firepower システムのスマート ライセンスの概要を示します。

表 *2 : Firepower* システムのスマート ライセンス

Firepowerシステムで割り当てるライセンス	購入するサブスクリプション	期間	付与される機能
基本 （特定のライセンスの予約を除き、基本ライセンスがすべての Firepower Threat Defenseデバイスに自動的に割り当てられます）	サブスクリプションは不要（デバイスにライセンスが含まれています）	永久	ユーザおよびアプリケーション制御 スイッチングとルーティング NAT 詳細は、基本ライセンス （12 ページ）を参照してください。
脅威	• T • TC（脅威 + URL） • TMC（脅威 + マルウェア + URL）	期間ベース	侵入検知と防御 ファイル制御 セキュリティ インテリジェンス フィルタリング 詳細については、脅威ライセンス （14 ページ）を参照してください。
マルウェア	• TM（脅威 + マルウェア） • TMC（脅威 + マルウェア + URL） • AMP	期間ベース	ネットワーク向け AMP（ネットワーク ベースの高度なマルウェア防御） Cisco Threat Grid ファイル ストレージ 詳細については、Firepower Threat Defense デバイスのマルウェア ライセンス （13 ページ）およびファイルおよびマルウェア ポリシーのライセンス要件 を参照してください。

Firepower システムで割り当てるライセンス	購入するサブスクリプション	期間	付与される機能
URL フィルタリング	• TC（脅威 + URL） • TMC（脅威 + マルウェア + URL） • URL	期間ベース	カテゴリとレピュテーションに基づく URL フィルタリング 詳細は、Firepower Threat Defense デバイスの URL フィルタリング ライセンス（14 ページ）を参照してください。
仮想 Firepower Management Center	ライセンス タイプに基づいています。	ライセンス タイプに基づき期間ベースまたは永久	プラットフォーム ライセンスによって、仮想アプライアンスが管理できるデバイスの数が決まります。 詳細は、Firepower Management Center Virtual ライセンス （2 ページ）を参照してください。
輸出管理機能	ライセンス タイプに基づいています。	ライセンス タイプに基づき期間ベースまたは永久	国家安全保障、外交政策、反テロリズムに関する法律や規制の対象となる機能。輸出規制対象の機能のライセンス （16 ページ） を参照してください。

Firepowerシステムで割り当てるライセンス	購入するサブスクリプション	期間	付与される機能
リモート アクセス VPN： • AnyConnect Apex • AnyConnect Plus • AnyConnect VPN Only	ライセンス タイプに基づいています。	ライセンス タイプに基づきタームベースまたは永久	リモート アクセス VPN の設定。リモート アクセス VPN を設定するには、基本ライセンスがエクスポート制御機能を許可する必要があります。デバイスの登録時に、輸出要件を満たしているかどうかを選択します。Firepower Threat Defense は有効な AnyConnect ライセンスを使用できます。使用できる機能はライセンス タイプによって異なります。 詳細については、AnyConnect ライセンス （15 ページ）およびVPN ライセンスを参照してください。

基本ライセンス

基本ライセンスは、Firepower Threat Defense または Firepower Threat Defense Virtual デバイスを購入するごとに自動的に提供されます。

基本ライセンスでは、次のことができます。

- スイッチングおよびルーティング（DHCP リレーおよび NAT を含む）を実行するように FTD デバイスを設定する
- FTD デバイスをハイ アベイラビリティ ペアとして設定する
- Firepower 9300 シャーシ内のクラスタとしてセキュリティ モジュールを設定する（シャーシ内クラスタリング）
- Firepower Threat Defense を実行している Firepower 9300 または Firepower 4100 シリーズ デバイスをクラスタとして設定する（シャーシ間クラスタリング）
- アクセス コントロール ルールにユーザとアプリケーションの条件を追加することで、ユーザとアプリケーションの制御を実装する

脅威とマルウェアの検出および URL のフィルタリング機能には追加のオプション ライセンスが必要です。

特定のライセンスの予約を使用する展開の場合を除き、基本ライセンスは登録した Firepower Threat Defense デバイスごとに Firepower Management Center に自動的に追加されます。

複数インスタンス展開については、複数インスタンス展開のライセンス （18 ページ）を参照してください。

Firepower Threat Defense デバイスのマルウェア ライセンス

Firepower Threat Defense デバイス用のマルウェア ライセンスを使用すると、ネットワーク向け AMP および Cisco Threat Grid を使用して Cisco Advanced Malware Protection（AMP）を実行することができます。この機能では、Firepower Threat Defense デバイスを使用して、ネットワーク上で伝送されるファイルのマルウェアを検出してブロックできます。この機能ライセンスをサポートするために、スタンドアロン サブスクリプションとしてマルウェア（AMP）サービス サブスクリプションを購入できます。また、脅威（TM）や脅威および URL フィルタリング（TMC）サブスクリプションと組み合わせて購入することもできます。

（注） マルウェア ライセンスが有効になっている Firepower Threat Defense 管理対象デバイスは、動的分析を設定していない場合でも、定期的に AMP クラウドへの接続を試行します。このため、デバイスの [インターフェイス トラフィック（Interface Traffic）] ダッシュボード ウィジェットには、送信済みトラフィックが表示されます。これは正常な動作です。

ファイル ポリシーの一部として ネットワーク向け AMP を設定し、その後 1 つ以上のアクセス コントロール ルールを関連付けます。ファイル ポリシーでは、特定のアプリケーション プロトコルを介した特定のタイプのユーザによるファイルのアップロードとダウンロードを検出できます。ネットワーク向け AMP では、ローカル マルウェア分析とファイルの事前分類を使用して、それらの限られた一連のファイルタイプを検査できます。特定のファイル タイプをダウンロードして Cisco Threat Grid クラウドにアップロードして、動的 Spero 分析でマルウェアが含まれているかどうかを判別することもできます。これらのファイルでは、ファイルがネットワーク内で経由する詳細なパスを示すネットワーク ファイル トラジェクトリを表示できます。マルウェア ライセンスでは、ファイル リストに特定のファイルを追加し、そのファイル リストをファイル ポリシー内で有効にすることもできます。これにより、検出時にこれらのファイルを自動的に許可またはブロックできます。

マルウェア ライセンスをすべて無効にすると、システムは AMP への問い合わせを停止し、AMP クラウドから送信される遡及的イベントの確認応答も停止します。既存のアクセス コントロール ポリシーに ネットワーク向け AMP 構成が含まれている場合は、それらのポリシーを再展開することができません。マルウェア ライセンスが無効にされた後、システムが既存のキャッシュ ファイルの性質を使用できるのは極めて短時間のみであることに注意してください。この時間枠の経過後、システムは `Unavailable` という性質をこれらのファイルに割り当てます。

マルウェア ライセンスが必要なのは、ネットワーク向け AMP および Cisco Threat Grid を展開する場合のみであることに注意してください。マルウェア ライセンスがなければ、Firepower Management Center は AMP クラウドからエンドポイント向け AMP マルウェア イベントおよび侵害の兆候（IOC）を受信できます。

ファイルおよびマルウェア ポリシーのライセンス要件の重要な情報も参照してください。

脅威ライセンス

脅威ライセンスでは、侵入の検出と防御、ファイル制御、およびセキュリティインテリジェンスのフィルタリングを実行することができます。

- 侵入検知および防御により、侵入とエクスプロイトを検出するためネットワークトラフィックを分析できます。またオプションで違反パケットをドロップできます。
- ファイル制御により、特定のアプリケーションプロトコルを介した特定タイプのファイルを検出し、オプションでこれらのファイルのアップロード（送信）またはダウンロード（受信）をユーザからブロックできます。マルウェア ライセンスが必要な ネットワーク向け *AMP* では、マルウェアの性質に基づいて限られたファイル タイプを検査およびブロックすることもできます。
- セキュリティインテリジェンスフィルタリングにより、トラフィックをアクセス制御ルールによる分析対象にする前に、特定の IP アドレス、URL、および DNS ドメイン名をブラックリストに追加（その IP アドレスとの間のトラフィックを拒否）できます。ダイナミック フィードにより、最新の情報に基づいて接続を直ちにブラックリストに追加できます。オプションで、Security Intelligence フィルタリングに「監視のみ」設定を使用できます。

脅威ライセンスは、スタンドアロン サブスクリプション（T）として、または URL フィルタリング（TC）、マルウェア（TM）、またはその両方（TMC）と組み合わせて購入することができます。

管理対象デバイスで脅威ライセンスを無効にすると、Firepower Management Center で、影響を受けたデバイスからの侵入イベントとファイルイベントの確認応答が停止されます。結果として、トリガー条件としてこれらのイベントを使用する相関ルールがトリガーしなくなります。また、Firepower Management Center はシスコ提供またはサードパーティのセキュリティインテリジェンス情報を取得するためにインターネットに接続しなくなります。脅威ライセンスを再度有効にするまでは、既存の侵入ポリシーを適用し直すことができません。

Firepower Threat Defense デバイスの URL フィルタリング ライセンス

URL フィルタリング ライセンスにより、モニタ対象ホストにより要求される URL に基づいて、ネットワーク内を移動できるトラフィックを判別するアクセス制御ルールを作成することができます。この機能ライセンスをサポートするために、スタンドアロンサブスクリプションとして URL フィルタリング（URL）サービス サブスクリプションを購入できます。また、脅威（TM）や脅威およびマルウェア（TMC）サブスクリプションと組み合わせて購入することもできます。

ヒント　URL フィルタリング ライセンスがない状態で、許可またはブロックする個別 URL または URL グループを指定できます。これにより、Web トラフィックをカスタムできめ細かく制御できますが、URL カテゴリおよびレピュテーション データをネットワーク トラフィックのフィルタリングに使用することはできません。

URL フィルタリング ライセンスがない状態でも、アクセス制御ルールにカテゴリ ベースの URL 条件およびレピュテーション ベースの URL 条件を追加できますが、Firepower Management Center は URL 情報をダウンロードしません。最初に URL フィルタリング ライセンスを Firepower Management Center に追加し、ポリシー適用対象デバイスで有効にするまでは、アクセス コントロール ポリシーを適用できません。

管理対象デバイスで URL フィルタリング ライセンスを無効にすると、URL フィルタリングへのアクセスが失われる可能性があります。ライセンスが期限切れになるか、ライセンスを無効にすると、URL 条件が含まれているアクセス制御ルールは URL フィルタリングを直ちに停止し、Firepower Management Center は URL データのアップデートをダウンロードできなくなります。既存のアクセス コントロール ポリシーに、カテゴリ ベースまたはレピュテーション ベースの URL 条件を含むルールが含まれている場合は、それらのポリシーを再展開することができません。

AnyConnect ライセンス

Firepower Threat Defense デバイスを使用して、Cisco AnyConnect セキュア モビリティ クライアント（AnyConnect）と標準規格に準拠した IPSec/IKEv2 を使用するリモート アクセス VPN を設定できます。

Firepower Threat Defense リモート アクセス VPN 機能を有効にするは、次のライセンスのいずれかを購入し、有効にしておく必要があります。[AnyConnect Plus]、[AnyConnect Apex]、または [AnyConnect VPN のみ（AnyConnect VPN Only）]。AnyConnect の任意のライセンス（[Plus]、[Apex]、[VPN のみ（VPN Only）]）を使用できます。両方のライセンスがあり、どちらも使用する場合は、[AnyConnect Plus] と [AnyConnect Apex] を選択できます。[Apex] または [Plus] と一緒に [AnyConnect VPN のみ（AnyConnect VPN Only）] ライセンスを使用することはできません。AnyConnect ライセンスは、スマート アカウントと共有する必要があります。手順については、http://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-og.pdfを参照してください。

指定されたデバイスに指定された AnyConnect ライセンス タイプの権限が 1 つ以上ない場合、リモート アクセス VPN 設定を FTD デバイスに展開することはできません。登録されたライセンスがコンプライアンスに従っていない、または権限の有効期限が切れている場合は、システムにライセンス アラートとヘルス イベントが表示されます。

リモート アクセス VPN を使用する際は、スマート ライセンス アカウントでエクスポート制御機能（高度な暗号化）を有効にしておく必要があります。AnyConnect クライアントとのリモート アクセス VPN 接続を確立するために、FTD はより強力な暗号化を要求します（これは DES よりも高い暗号化です）。デバイスを登録する際に、エクスポート制御機能に対して有効化された Smart Software Manager アカウントによってエクスポートを制御する必要があります。エクスポート制御機能の詳細については、スマート ライセンスのタイプと制約事項 （9 ページ）を参照してください。

次の条件に当てはまる場合、リモート アクセス VPN を展開できません。

- Firepower Management Center でスマート ライセンスが評価モードで実行されている。

- スマートアカウントがエクスポート制御機能（高度な暗号化）を使用するように設定されていない。エクスポート制御機能を持つ基本ライセンスを適用した後に、FTDデバイスを再起動する必要があることに注意してください。

輸出規制対象の機能のライセンス

輸出規制対象の機能が必要な機能

特定のソフトウェア機能は、国家安全保障、外交政策、反テロリズムに関する法律や規制の対象となります。これらの輸出規制対象の機能は次のとおりです。

- セキュリティ認定コンプライアンス
- Firepower Threat Defense リモート アクセス VPN
- 強力な暗号化によるサイト間 VPN
- 強力な暗号化による SSH プラットフォーム ポリシー
- 強力な暗号化による SSL ポリシー
- 強力な暗号化による SNMPv3 などの機能

輸出規制対象の機能がシステムに対して現在有効になっているかどうかを判断する方法

輸出規制対象の機能がシステムに対して現在有効になっているかどうかを判断するには、[システム（System）] > [ライセンス（Licenses）] > [スマート ライセンス（Smart Licenses）] に移動し、[輸出規制対象の機能（Export-Controlled Features）] に [有効（Enabled）] と表示されているかどうかを確認します。

輸出規制対象の機能の有効化について

[輸出規制対象の機能（Export-Controlled Features）] に [無効（Disabled] と表示されており、強力な暗号化が必要な機能を使用する場合：

強力な暗号化機能を有効にする方法は2つあります。組織はどちらか一方を使用する（またはどちらも使用しない）ことができますが、両方を使用することはできません。

- Cisco Smart Software Manager（CSSM）で新しい製品インスタンス登録トークンを生成したときに輸出規制対象の機能を有効にするオプションがない場合は、次のようになります。

  代理店に問い合わせてください。

  Firepower Management Center では、スマート アカウントが輸出規制対象の機能の付与資格がある場合は輸出規制対象の機能を使用することができます。シスコによって承認されると、輸出規制ライセンスが仮想アカウントに追加されるため、輸出規制対象お機能を使用できます。詳細については、輸出規制機能の有効化（グローバル権限のないアカウントの場合） （23 ページ）を参照してください。

- Cisco Smart Software Manager（CSSM）で新しい製品インスタンス登録トークンを生成したときに輸出規制対象の機能を使用するためのオプションが表示された場合：

- これは永続的な付与資格であり、サブスクリプションは必要ありません。
- 輸出規制対象の機能を使用するには、Firepower Management Center にライセンスを取得する前にスマートアカウントがこの機能を使用できるように有効になっている必要があります。
- Cisco Smart Software Manager（CSSM）のスマート アカウントに対して輸出規制対象の機能を有効にした後、新しい製品インスタンス登録トークンを使用して Firepower Management Center を再登録する必要があります。
- 新しい製品インスタンス登録トークンを作成する際に、[このトークンで登録された製品で輸出規制対象の機能を許可する（Allow export-controlled functionality on the products registered with this token）] オプションを選択する必要があります。この機能がスマートアカウントに許可されている場合には、このオプションがデフォルトで有効になっています。
- 輸出規制対象の機能を持つトークンを Firepower Management Center にインストールし、管理対象の Firepower Threat Defense デバイスに関連するライセンスを割り当てた後、次の手順を実行します。
  - 各デバイスを再起動し、新たに有効にした機能を使用できるようにします。
  - 高可用性展開では、アクティブ デバイスとスタンバイ デバイスを一緒に再起動してアクティブ/アクティブの状態を回避する必要があります。

詳細情報

輸出規制に関する一般情報については https://www.cisco.com/c/en/us/about/legal/global-export-trade.html を参照してください。

高可用性構成のライセンス

参照先：

- 高可用性ペア内の Firepower Management Center アプライアンスの場合：

  ライセンス要件

- 高可用性ペア内の Firepower Threat Defense デバイスの場合：

  高可用性ペアでの FTD デバイスのライセンス要件

また、スマート ライセンスのタイプと制約事項 （9 ページ）のトピックの特定のライセンスタイプについてのトピックも参照してください。

FTD クラスタのライセンス

このライセンス章の情報の他に次を参照してください。

- クラスタリングのライセンス

- FMC：クラスタの追加。

複数インスタンス展開のライセンス

すべてのライセンスがコンテナ インスタンスごとではなく、セキュリティ エンジン/シャーシ（Firepower 4100 の場合）またはセキュリティ モジュール（Firepower 9300 の場合）ごとに適用されます。

基本ライセンス

各セキュリティ エンジンまたはモジュールが 1 つの基本ライセンスを使用します。このライセンスは、特定のライセンスの予約を使用している場合を除き、すべての展開に自動的に割り当てられます。

仮想 Firepower Management Center

Firepower Management Center の仮想アプライアンスが管理するセキュリティ エンジン/モジュールごとに 1 つの付与資格が必要です。

機能ライセンス

ライセンス（マルウェア、脅威、URL フィルタリング、AnyConnect Apex、AnyConnect Plus、および AnyConnect VPN 専用）を取得する各機能に、セキュリティ エンジン/モジュール単位で 1 つのライセンスが必要です。エンジン/モジュールのすべてのインスタンスで同じ機能ライセンスを共有できます。

インスタンスごとにライセンスを割り当てる必要があります。

ハイ アベイラビリティ展開

高可用性ペア内のインスタンスは機能ライセンスを相互に共有することはできませんが、各インスタンスがそれぞれのエンジン/モジュール上の他のインスタンスと機能ライセンスを共有することはできます。

ライセンスの例

上記のライセンス要件の連動については、コンテナインスタンスのライセンスを参照してください。

ライセンスを保持するためのスマート アカウントの作成

スマート アカウントはスマート ライセンスのために必要です。また、従来のライセンスを保持することもできます。

スマート ライセンスを購入する前に、スマート アカウントを設定する必要があります。

始める前に

アカウント担当者または再販業者が、ユーザのためにスマートアカウントを設定していることがあります。その場合は、この手順を使用するのではなく、その担当者からアカウントへのアクセスに必要な情報を取得してから、アカウントにアクセスできることを確認してください。

スマート アカウントに関する一般情報については http://www.cisco.com/go/smartaccountsを参照してください。

ステップ 1 スマート アカウントのリクエスト：

この説明については、https://community.cisco.com/t5/licensing-enterprise-agreements/request-a-smart-account-for-customers/ta-p/3636515?attachment-id=150577 を参照してください。

詳細については、https://communities.cisco.com/docs/DOC-57261を参照してください。

ステップ 2 スマート アカウントの設定準備ができたことを知らせる電子メールが届くのを待ちます。電子メールが届いたら、指示に従って、メールに含まれているリンクをクリックします。

ステップ 3 スマート アカウントの設定：

https://software.cisco.com/software/company/smartaccounts/home?route=module/accountcreation を参照してください。

この説明については、https://community.cisco.com/t5/licensing-enterprise-agreements/complete-smart-account-setup-for-customers/ta-p/3636631?attachment-id=132604 を参照してください。

ステップ 4 Cisco Smart Software Manager（CSSM）でアカウントにアクセスできることを確認します。

https://software.cisco.com/#module/SmartLicensing に移動してサインインします。

次のタスク

長いワークフローに従っている場合は、そのワークフローに戻ります。

Firepower Threat Defense デバイスのライセンス （4 ページ）

ダイレクト インターネット アクセスによるスマート ライセンスの設定方法

始める前に

展開が複雑な場合、または必要なライセンスについてご不明な点がある場合は、Firepower Threat Defense デバイスのライセンス （4 ページ）を参照してください。

ステップ 1 Cisco Smart Software Manager ライセンス ポータルでトークンを取得します。

スマート ライセンス用の製品ライセンス登録トークンの取得 （20 ページ）を参照してください。

ステップ 2 スマート ライセンス ポータルに Firepower Management Center を登録します。

スマート ライセンスの登録 （21 ページ）を参照してください。このトピックの前提条件が満たされていることを確認してください。

ステップ 3 FMC がスマート ライセンス ポータルに正常に登録されたことを確認します。

Firepower Management Center Web インターフェイスで、[システム（System）] > [ライセンス（Licenses）] > [スマートライセンス（Smart Licenses）] に移動します。

[製品登録（Product Registration）] に緑のチェックマークが表示されている必要があります。

ステップ 4 FMC にまだデバイスを追加していない場合は、追加します。

Firepower Management Center へのデバイスの追加を参照してください。

ステップ 5 FMC によって管理されているデバイスにライセンスを割り当てます。

複数の管理対象デバイスへのライセンスの割り当て （43 ページ）を参照してください。

ステップ 6 ライセンスが正常にインストールされたことを確認します。

スマート ライセンスおよびスマート ライセンス ステータスの表示 （44 ページ）を参照してください。

次のタスク

必要に応じて、高可用性展開およびクラスタ化展開のライセンスをセットアップします。

Firepower Threat Defense デバイスのライセンス （4 ページ）の最後の手順を参照してください。

スマート ライセンス用の製品ライセンス登録トークンの取得

始める前に

- まだ作成していない場合は、スマート アカウントを作成します。https://software.cisco.com/smartaccounts/setup#accountcreation-accountを参照してください。詳細については、https://www.cisco.com/c/en/us/buy/smart-accounts.htmlを参照してください。
- 必要なライセンスのタイプおよびライセンス数を購入したことを確認します。
- 必要ライセンスがスマート アカウントに表示されていることを確認します。

  ライセンスがスマートアカウントに表示されない場合は、注文した担当者（シスコのセールス担当者または認定再販業者など）にそのライセンスをスマートアカウントに転送するように依頼します。
- 可能ならば、スマート ライセンスの登録 （21 ページ）の前提条件を確認して、登録プロセスがスムーズに進むようにします。
- Cisco Smart Software Manager にサインインするためのクレデンシャルがあることを確認します。

ステップ 1 https://software.cisco.com に進みます。

ステップ 2 （[ライセンシング（Licensing）]セクションで）[スマート ソフトウェア ライセンシング（Smart Software Licensing）] をクリックします。

ステップ 3 Cisco Smart Software Manager にサインインします。

ステップ 4 [インベントリ（Inventory）] をクリックします。

ステップ 5 [General] をクリックします。

ステップ 6 [新規トークン（New Token）] をクリックします。

ステップ 7 [説明（Description）] に、このトークンを使用する Firepower Management Center を一意かつ明確に特定する名前を入力します。

ステップ 8 365 日以内の期限を入力します。

この期限により、トークンを Firepower Management Center に登録しておく必要がある期間が決まります（ライセンスの権限付与期間はこの設定とは関係ありませんが、トークンをまだ登録していない場合でも、カウント ダウンが開始されることがあります）。

ステップ 9 エクスポート制御機能を有効にするオプションが表示されていて、強力な暗号化を必要とする機能を使用する予定の場合は、このオプションを選択します。

重要 このオプションが表示された場合は、この機能を使用する予定かどうかをここで選択する必要があります。輸出規制対象の機能を後で有効にすることはできません。

このオプションが表示されていない場合で、輸出規制対象の機能のライセンスを組織が取得している場合は、輸出規制機能の有効化（グローバル権限のないアカウントの場合） （23 ページ）で説明したように、この機能を後で有効にします。

ステップ 10 [トークンの作成（Create Token）] をクリックします。

ステップ 11 リストで新しいトークンを見つけて、[アクション（Actions）] をクリックして、[コピー（Copy）] または [ダウンロード（Download）] を選択します。

ステップ 12 必要に応じて、Firepower Management Center にトークンを入力する準備ができるまで、トークンを安全な場所に保存します。

次のタスク

スマート ライセンスの登録 （21 ページ）の手順に進みます。

スマート ライセンスの登録

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	該当なし	Firepower Threat Defense	グローバルだけ	Admin

Cisco Smart Software Manager で Firepower Management Center を登録します。

始める前に

- Smart Software Satellite Server または特定のライセンスの予約を使用している場合は、この手順を使用しないでください。代わりに、Smart Software Satellite Server への接続の設定 （26 ページ）または特定のライセンスの予約の実装方法 （28 ページ）をそれぞれ参照してください。
- Firepower Management Center が tools.cisco.com:443 で Cisco Smart Software Manager（CSSM）サーバにアクセスできることを確認します。
- Firepower Management Center で NTP デーモンが実行されていることを確認します。登録時に、NTP サーバと Cisco Smart Software Manager の間でキー交換が実行されるため、適切な登録には時刻の同期が必要です。

  Firepower 4100/9300 シャーシに FTD を展開する場合は、Firepower Management Center と同じ NTP サーバをシャーシに使用して Firepower シャーシに NTP を設定する必要があります。
- 組織に複数の Firepower Management Center アプライアンスがある場合は、各 FMC に明確に識別できる一意の名前が付いていて、同じバーチャルアカウントに登録されている可能性がある他の Firepower Management Center アプライアンスと区別できることを確認します。この名前は、スマート ライセンスの権限付与の管理にとって重要です。あいまいな名前だと後で問題が発生することがあります。
- Cisco Smart Software Manager から必要な製品ライセンス登録トークンを生成します。スマート ライセンス用の製品ライセンス登録トークンの取得 （20 ページ）を参照してください（すべての前提条件を含む）。Firepower Management Center にアクセスするマシンからトークンにアクセスできることを確認します。

ステップ 1 **[System]** > **[Licenses]** > **[Smart Licenses]**を選択します。

ステップ 2 Firepower Management Center の Web インターフェイスで、[登録（Register）] をクリックします。

ステップ 3 生成されたトークンを [製品インスタンス登録トークン（Product Instance Registration Token）] フィールドに貼り付けます。

テキストの前後にスペースや空白の行がないことを確認します。

ステップ 4 使用状況データをシスコに送信するかどうかを決定します。

- [Cisco Success Networkの有効化（Enable Cisco Success Network）] は、デフォルトで有効です。シスコによって収集されるデータの種類を表示するには、[サンプルデータ（sample data）] をクリックします。Cisco Success Network の情報ブロックを読むと、判断に役立ちます。
- （注）
  - 有効にすると、Cisco Support Diagnostics は、次の同期サイクルで Firepower Threat Defense（FTD）デバイスで有効になります。FTD と FMC との同期は、30 分ごとに 1 回実行されます。
  - 有効にすると、今後この FMC に登録される新しい FTD では、Cisco Support Diagnostics が自動的に有効になります。

ステップ 5 [変更を適用（Apply Changes）] をクリックします。

次のタスク

- Firepower Threat Defense デバイスを Firepower Management Center に追加します。Firepower Management Center へのデバイスの追加を参照してください。
- ライセンスを Firepower Threat Defense デバイスに割り当てます。複数の管理対象デバイスへのライセンスの割り当て （43 ページ）を参照してください。

輸出規制機能の有効化（グローバル権限のないアカウントの場合）

重要 この手順は、スマートアカウントに強力な暗号が承認されていない場合にのみ使用します。アカウントが承認されていない場合、またはわからない場合は輸出規制対象の機能のライセンス（16 ページ）を参照してください。

始める前に

- 展開でまだ輸出規制対象の機能がサポート**されていない**ことを確認します。

（注） 展開で輸出規制対象の機能がサポートされている場合、Cisco Smart Software Manager の [登録トークンの作成（Create Registration Token）] ページに輸出規制対象の機能を有効にできるオプションが表示されます。詳細については、https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager.html を参照してください。

- 展開で評価ライセンスが使用されていないことを確認します。
- Cisco Smart Software Manager の **[インベントリ（Inventory）]** > **[ライセンス（Licenses）]** ページで、Firepower Management Center に対応するライセンスがあることを確認します。

輸出規制ライセンス	Firepower Management Center モデル
Cisco Virtual FMC シリーズの強力な暗号化（3DES/AES）	すべての仮想 Firepower Management Center
Cisco FMC 1K シリーズの強力な暗号化（3DES/AES）	750、1000、1500、1600
Cisco FMC 2 K シリーズの強力な暗号化（3DES/AES）	2000、2500、2600

輸出規制ライセンス	Firepower Management Center モデル
Cisco FMC 4K シリーズの強力な暗号化（3DES/AES）	3500、4000、4500、4600

ステップ 1 **[システム（System）] > [ライセンス（Licenses）] > [スマート ライセンス（Smart Licenses）]** を選択します。

（注） [輸出キーの要求（Request Export Key）] が表示されている場合は輸出規制対象の機能がアカウントに承認されています。そのため、必要な機能の使用に進むことができます。

ステップ 2 [エクスポート キーの要求（Request Export Key）] をクリックして、エクスポート キーを生成します。

ヒント エクスポート制御キーの要求に失敗した場合は、バーチャル アカウントに有効なエクスポート制御ライセンスがあることを確認します。

次のタスク

これで、輸出規制対象の機能を使用する設定またはポリシーを展開できるようになります。

メモ これによって有効にされた新しい輸出規制対象のライセンスとすべての機能は、Firepower Threat Defense デバイスが再起動されるまでそのデバイスでは有効になりません。それまでは、前のライセンスでサポートされていた機能のみがアクティブになります。

高可用性展開では、アクティブ/アクティブの状態を避けるために両方の Firepower Threat Defense デバイスを再起動する必要があります。

輸出規制対象の機能の無効化（グローバル権限のないアカウントの場合）

輸出規制機能の有効化（グローバル権限のないアカウントの場合） （23 ページ）で説明した機能を使用して輸出規制対象の機能を有効にした場合は、この手順を使用してこの機能を無効にできます。

ステップ 1 **[システム（System）] > [ライセンス（Licenses）] > [スマート ライセンス（Smart Licenses）]** を選択します。

これによって、このライセンスが開放されて仮想アカウント内の使用可能なライセンスのプールに戻り、再利用できるようになります。

ステップ 2 [輸出キーの返却（Return Export Key）] をクリックして、輸出規制ライセンスを無効にします。

エアギャップ展開のライセンスのオプション

次の表に、インターネットアクセスがない環境でのライセンスの展開に使用できるオプションを比較して示します。特定の状況については、販売担当者が他のアドバイスをできる場合があります。

表 *3:* エアギャップ ネットワークのライセンス オプションの比較

Smart Software Satellite Server	特定のライセンスの予約
大量の製品に対する拡張性	少数のデバイスに最適
ライセンス管理、使用状況、および資産管理の可視性を自動化	使用状況および資産管理の可視性の制限
デバイスを追加するための運用コストの増加なし	デバイスを追加するための経時的な運用コストが線形
柔軟性、使いやすさ、少ないオーバーヘッド	移動、追加、および変更の際の管理および手動によるオーバーヘッドの多さ
初期およびさまざまな期限切れ状態でコンプライアンス不適合ステータスが許可される	コンプライアンス不適合ステータスはシステムの動作に影響を与える
詳細については、Smart Software Satellite Server の概要 （25 ページ）を参照してください。	詳細については、特定のライセンスの予約の概要 （27 ページ）を参照してください。

Smart Software Satellite Server の概要

License Authority との定期通信 （8 ページ） の説明に従って、ライセンス権限を維持するため、システムは Cisco と定期的に通信する必要があります。次の状況のいずれかの場合、ライセンス認証局と接続するためのプロキシとして Smart Software Satellite Server を使用できます。

- Firepower Management Center がオフラインである、接続が制限されている、または接続がない（つまり、エアギャップ ネットワークに展開されている）場合。
- Firepower Management Center に固定接続があるが、ネットワークからの単一の接続によってスマート ライセンスを制御する場合。

スマート ソフトウェア サテライト サーバを使用すると、同期スケジュールを設定、またはスマート ライセンス認証を Smart Software Manager と手動で同期させることができます。

スマート ソフトウェア サテライト サーバの詳細については、https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager-satellite.html を参照してください。

エアギャップ ネットワークの場合の代替ソリューションは特定ライセンスの予約です。詳細については、特定のライセンスの予約の概要 （27 ページ）を参照してください。

Smart Software Satellite Server の展開方法

始める前に

ネットワークがエアギャップの場合、Smart Software Satellite Server または特定ライセンスの予約が展開に最適なソリューションであるかどうかを判断します。詳細については、Smart Software Satellite Server の概要 （25 ページ）および特定のライセンスの予約の概要 （27 ページ）を参照してください。

ステップ 1 Smart Software Satellite Server を展開して設定します。

https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager-satellite.htmlにある『*Smart Software Manager Satellite User Guide*』を参照してください。

ステップ 2 Firepower Management Center を Satellite に接続し、登録トークンを取得して、管理センターを Satellite に登録します。

Smart Software Satellite Server への接続の設定 （26 ページ）を参照してください。

ステップ 3 デバイスを管理対象に追加します。

Firepower Management Center へのデバイスの追加を参照してください。

ステップ 4 管理対象デバイスへのライセンスの割り当て

複数の管理対象デバイスへのライセンスの割り当て （43 ページ）を参照してください

ステップ 5 Satellite を Cisco Smart Software Management Server（CSSM）に同期させます。

上記で使用した『*Smart Software Manager Satellite User Guide*』を参照してください。

ステップ 6 継続的な同期時刻をスケジュールします。

Smart Software Satellite Server への接続の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	該当なし	Firepower Threat Defense	グローバルのみ	管理者

始める前に

- Smart Software Satellite Server を設定します。詳細については、Smart Software Satellite Server の展開方法 （26 ページ）を参照してください。
- サテライト サーバの TLS/SSL 証明書の CN をメモします。

- FMC が Smart Software Satellite Server に到達できることを確認します。たとえば、サテライト サーバの call-home URL として設定された FQDN が内部 DNS サーバによって解決できることを確認します。
- http://www.cisco.com/security/pki/certs/clrca.cer に移動し、TLS/SSL 証明書の本文全体（"-----BEGIN CERTIFICATE-----" から "-----END CERTIFICATE-----" まで）を、設定中にアクセスできる場所にコピーします。

ステップ 1 **[System]** > **[Integration]**を選択します。

ステップ 2 [Smart Software Satellite] タブをクリックします。

ステップ 3 [Cisco Smart Software Satellite Serverに接続（Connect to Cisco Smart Software Satellite Server）] を選択します。

ステップ 4 この手順の前提条件で収集した CN 値を使用して、Smart Software Satellite Server の **URL** を次の形式で入力します。

`https://FQDN_or_hostname_of_Satellite/Transportgateway/services/DeviceRequestHandler`

FQDN またはホスト名は、サテライトによって提示された証明書の CN 値と一致している必要があります。

ステップ 5 新しい [SSL証明書（SSL Certificate）] を追加し、この手順の前提条件でコピーした証明書テキストを貼り付けます。

ステップ 6 [適用（Apply）] をクリックします。

ステップ 7 [システム（System）] > [ライセンス（Licenses）] > [スマートライセンス（Smart Licenses）] を選択し、[登録（Register）] をクリックします。

ステップ 8 Smart Satellite Server で新しいトークンを作成します。

ステップ 9 トークンをコピーします。

ステップ 10 トークンを管理センター ページのフォームに貼り付けます。

ステップ 11 [変更を適用（Apply Changes）] をクリックします。

これで、管理センターが Smart Software Satellite Server に登録されました。

次のタスク

Smart Software Satellite Server の展開方法 （26 ページ）の残りの手順を実行します。

特定のライセンスの予約の概要

特定のライセンスの予約機能を使用して、エアギャップ ネットワークにスマート ライセンスを展開できます。

特定のライセンスの予約が有効になっている場合、Firepower Management Center は、Cisco Smart Software Manager または Smart Software サテライト サーバにアクセスせずに仮想アカウントからライセンスを予約します。

Firepower Management Center では、標準クラシック ライセンスを使用するデバイスを同時に管理することもできます。ただし、これらのデバイスは特定のライセンスの予約を使用しません。

インターネットへのアクセスが必要なパブリック Web サイトに対する URL ルックアップや状況に応じた相互起動などの機能は動作しません。

シスコは、特定のライセンスの予約を使用する展開に関する Web 分析やテレメトリのデータを収集しません。

関連トピック：

- 特定のライセンスの予約のベスト プラクティス （28 ページ）
- 特定のライセンスの予約の要件 （28 ページ）
- 特定のライセンスの予約の実装方法 （28 ページ）
- 特定のライセンスの予約ステータス （38 ページ）
- 特定のライセンスの予約の更新 （35 ページ）
- 特定のライセンスの予約の非アクティブ化と返却 （39 ページ）
- 特定のライセンスの予約のトラブルシューティング （41 ページ）

特定のライセンスの予約のベスト プラクティス

特定のライセンスの予約を正常に実装するには、このドキュメントを必ず読んでください。

試行が失敗した場合は TAC に連絡する必要が生じる可能性があります。

問題を避けるには、前提条件や確認手順を含めて、手順に慎重に従ってください。

特定のライセンスの予約の要件

特定のライセンスの予約の使用状況は、シスコによる承認と認証が必要です。

特定のライセンスの予約の前提条件 （29 ページ）も参照してください。

特定のライセンスの予約の実装方法

	操作手順	詳細情報
ステップ 1	この機能の前提条件を満たします。	特定のライセンスの予約の前提条件 （29 ページ）

	操作手順	詳細情報
ステップ 2	スマートアカウントで特定のライセンスの付与資格を展開する準備が整っていることを確認します。	スマート アカウントが特定のライセンスの予約の展開の準備が整っているかどうかの確認 （30 ページ）
ステップ 3：	Firepower Management Center を使用して特定のライセンスの予約を有効にします。	[特定のライセンス（Specific Licenses）] メニュー オプションの有効化 （31 ページ）
ステップ 4：	Firepower Management Center から予約要求コードを生成します。	Firepower Management Center からの予約要求コードの生成 （32 ページ）
ステップ 5：	予約要求コードを使用して、Cisco Smart Software Manager から予約承認コードを生成します。	Cisco Smart Software Manager からの予約承認コードの生成 （32 ページ）
ステップ 6：	Firepower Management Center に予約承認コードを入力します。	Firepower Management Center に予約承認コードを入力します。 （33 ページ）
ステップ 7	特定のライセンスを管理対象の Firepower Threat Defence デバイスに割り当てます。	管理対象デバイスへの特定のライセンスの割り当て （34 ページ）
ステップ 9	（Firepower Management Center 外）進行中のメンテナンス タスクのリマインダのスケジュールを設定します。	エアギャップ展開の維持

特定のライセンスの予約の前提条件

- スマート アカウントをセットアップします。

  ライセンスを保持するためのスマート アカウントの作成 （18 ページ）を参照してください。

- Firepower Management Center で標準スマート ライセンスを現在使用している場合は、特定のライセンスの予約を実装する前に Firepower Management Center の登録を解除します。詳細については、Cisco Smart Software Manager から Firepower Management Center の登録解除 （48 ページ）を参照してください。

  Firepower Management Center に現在展開されているすべてのスマート ライセンスがアカウントで使用可能なライセンスのプールに戻され、特定のライセンスの予約を実装すると再利用できるようになります。

- 特定のライセンスの予約には、標準スマートライセンスと同じ数およびタイプのライセンスが必要です。展開するデバイスと機能に必要な標準ライセンスとサービスサブスクリプションの数を特定します。必要に応じて、Firepower Management Center Virtual の付与資格を含めてください。

  Firepower のライセンスとサービス サブスクリプションについては、スマート ライセンスのタイプと制約事項 （9 ページ）およびそのサブトピック（特にFirepower Management Center Virtual ライセンス （2 ページ））を参照してください。

- 必要なライセンスを購入します。
- 必要であり、組織にその付与資格がある場合は、輸出規制対象の強力な暗号化機能を手配します。アカウントでその機能が使用できること、または必要な Firepower Management Centerの事前ライセンスが仮想アカウントに表示されていることを確認します。アカウント担当者がサポートします。

  詳細については、輸出規制対象の機能のライセンス （16 ページ）を参照してください。

- Firepower製品の特定ライセンス予約（SLR）の承認を得るため、アカウント担当者が協力いたします。
- 特定のライセンスの予約が使用できる状態になっており、スマートアカウントに反映されていることをアカウント担当者に確認してください。
- 管理対象デバイスを Firepower Management Center に追加します。この説明については、Firepower Management Center へのデバイスの追加 を参照してください。（管理対象デバイスはいつでも追加できますが、今追加すると、このプロセスが簡単になります。）これを実行するには、評価ライセンスを有効にする必要があります（[システム（System）] から [ライセンス（Licenses）] > [スマート ライセンス（Smart Licenses）]）。評価ライセンスは、ライセンス認証局への接続を必要としません。
- （推奨）高可用性構成で Firepower Management Center ペアを展開する場合は、ライセンスを割り当てる前にその設定をします（高可用性構成の FMC で必要なライセンスの数は、単一の FMC の場合と同じです）。すでにセカンダリ アプライアンスにライセンスを展開している場合は、そのアプライアンスからライセンスを登録解除します。

スマート アカウントが特定のライセンスの予約の展開の準備が整っているかどうかの確認

特定のライセンスの予約の展開時の問題を防ぐため、Firepower Management Center に変更を加える前にこの手順を実行します。

始める前に

- 特定のライセンスの予約の前提条件 （29 ページ）で説明した要件を満たしていることを確認します。
- Cisco Smart Software Manager のクレデンシャルがあることを確認します。

ステップ 1 Cisco Smart Software Manager にサインインします。

https://software.cisco.com/#SmartLicensing-Inventory

ステップ 2 必要に応じて、[インベントリ（Inventory）] をクリックします。

ステップ 3 [ライセンス（Licenses）] タブをクリックします。

ステップ 4 次のことを確認してください。

- [ライセンスの予約（License Reservation）] ボタンが表示されている。
- 該当する場合は、デバイスの Firepower Management Center Virtual の付与資格を含めて展開するデバイスおよび機能に十分なプラットフォーム ライセンスと機能ライセンスがある。

ステップ 5 これらのアイテムがないか、または誤っている場合は、アカウント担当者に連絡して問題を解決します。

重要 問題が修正されるまではこのプロセスは続行**しないでください**。

[特定のライセンス（Specific Licenses）] メニュー オプションの有効化

Specific License	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Firepower Management Center	グローバルだけ	管理者

この手順では、Firepower Management Center の [スマート ライセンス（Smart Licenses）] メニュー オプションを [特定のライセンス（Specific Licenses）] に変更します。

ステップ 1 USB キーボードと VGA モニタを使用して Firepower Management Center コンソールにアクセスするか、または SSH を使用して管理インターフェイスにアクセスします。

ステップ 2 Firepower Management Center の **admin** アカウントにログインします。デフォルトでは、これによって Linux シェルへのアクセス権が付与されます。Firepower Management Center の CLI が有効になっている場合は、これによってコマンド ライン インターフェイスへのアクセス権が付与されます。

ステップ 3 CLI が有効になっている Firepower Management Center の場合は、**expert** コマンドを入力して Linux シェルにアクセスします。

ステップ 4 特定のライセンスの予約のオプションにアクセスするには、次のコマンドを実行します。

sudo manage_slr.pl

例：

```
admin@fmc63betaslr: ~$ sudo manage_slr.pl
Password:


*************** Configuration Utility **************

1   Show SLR Status
2   Enable SLR
3   Disable SLR
0   Exit
```

```
************************************************************
Enter choice:
```

ステップ 5 オプション 2 を選択して、Specific License Reservation を有効にします。

ステップ 6 オプション 0 を選択して manage_slr ユーティリティを終了します。

ステップ 7 **exit** と入力し、Linux シェルを終了します。

ステップ 8 CLI が有効になっている Firepower Management Center では、入力 **exit**してコマンドライン インターフェイスを終了します。

ステップ 9 Firepower Management Center の Web インターフェイスの [特定のライセンスの予約（Specific License Reservation）] ページにアクセスできることを確認します。

- [システム（System）] > [ライセンス（Licenses）] > [スマート ライセンス（Smart Licenses）] ページが現在表示されている場合は、ページを更新します。
- それ以外の場合は、[システム（System）] > [ライセンス（Licenses）] > [特定のライセンス（Specific Licenses）] を選択します。

Firepower Management Center からの予約要求コードの生成

Specific License	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Firepower Management Center	グローバルだけ	管理者

ステップ 1 [特定のライセンスの予約（Specific License Reservation）] ページが表示されていない場合は、[システム（System）] > [ライセンス（Licenses）] > [特定のライセンス（Specific Licenses）] を選択します。

ステップ 2 [生成（Generate）] をクリックします。

ステップ 3 **予約要求コード**をメモします。

Cisco Smart Software Manager からの予約承認コードの生成

ステップ 1 Cisco Smart Software Manager に移動します。

https://software.cisco.com/#SmartLicensing-Inventory

ステップ 2 必要に応じて、[インベントリ（Inventory）] をクリックします。

(このページは自動的に表示されることがあります。)

ステップ 3 [ライセンス（Licenses）] タブをクリックします。

ステップ 4 [ライセンスの予約（License Reservation）] をクリックします。

ステップ 5 生成したコードを Firepower Management Center から [予約要求コード（Reservation Request Code）] ボックスに入力します。

ステップ 6 [次へ（Next）] をクリックします。

ステップ 7 [特定のライセンスの予約（Reserve a specific license）] を選択します。

ステップ 8 下にスクロールしてライセンス グリッド全体を表示します。

ステップ 9 [予約する数量（Quantity To Reserve）] に、展開に必要な各プラットフォームと機能の数を入力します。

重要

- 管理対象デバイスごとに **Firepower Threat Defense Base Features** ライセンスを、マルチインスタンス展開の場合は **Firepower Threat Defense ベース機能**ライセンスを明示的に含める必要があります。
- 仮想管理センターを使用している場合は、各モジュール（マルチインスタンス展開）か、または各管理対象デバイス（その他のすべての展開）に **Firepower MCv デバイス ライセンス**の資格を組み込む必要があります。
- 強力な暗号化機能を使用する場合：
  - スマート アカウント全体が輸出規制対象機能に対して有効になっている場合は、ここで何もする必要はありません。
  - 組織の資格が Firepower Management Center 単位の場合は、アプライアンス向けに適切なライセンスを選択する必要があります。

  デバイスに適切なライセンス名を選択するには、輸出規制機能の有効化（グローバル権限のないアカウントの場合） （23 ページ）の前提条件を参照してください。

ステップ 10 [次へ（Next）] をクリックします。

ステップ 11 [承認コードを生成（Generate Authorization Code）] をクリックします。

この時点で、ライセンスは、Smart Software Manager に従って使用中です。

ステップ 12 Firepower Management Center に入力するための準備として承認コードをダウンロードします。

Firepower Management Center に予約承認コードを入力します。

Specific License	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Firepower Management Center	グローバルだけ	管理者

ステップ 1 [特定のライセンスの予約（Specific License Reservation）] ページが表示されていない場合は、Firepower Management Center の Web インターフェイスで [システム（System）] > [ライセンス（Licenses）] > [特定のライセンス（Specific Licenses）] を選択します。

ステップ 2 [参照（Browse）] をクリックして、承認コード ファイル（.txt）をアップロードします。

ステップ 3 [Install（インストール）] をクリックします。

ステップ 4 [特定のライセンスの予約（Specific License Reservation）] ページに [使用の承認（Usage Authorization）] ステータスが [承認済み（authorized）] と表示されていることを確認します。

ステップ 5 [予約済みライセンス（Reserved Licenses）] タブをクリックして、[承認コード（Authorization Code）] の生成時に選択したライセンスを確認します。

必要なライセンスが表示されていない場合は、必要なライセンスを追加します。詳細については、「特定のライセンスの予約の更新」を参照してください。

管理対象デバイスへの特定のライセンスの割り当て

Specific License	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Firepower Management Center	グローバルだけ	管理者

この手順を使用して、複数の管理対象デバイスにライセンスを一度にすばやく割り当てます。

また、この手順を使用してライセンスを無効にするか、または 1 つの Firepower Threat Defense デバイスから別のデバイスに移動できます。デバイスのライセンスを無効にすると、ライセンスに関連付けられた機能をそのデバイスで使用できません。

ステップ 1 [システム（System）] > [ライセンス（Licenses）] > [個別ライセンス（Specific Licenses）] を選択します。

ステップ 2 [ライセンスの編集（Edit Licenses）] をクリックします。

ステップ 3 各タブをクリックし、必要に応じてデバイスにライセンスを割り当てます。

ステップ 4 [適用（Apply）] をクリックします。

ステップ 5 [割り当て済みのライセンス（Assigned Licenses）] タブをクリックし、各デバイスでライセンスが正しくインストールされていることを確認します。

次のタスク

- 輸出規制対象の機能が有効になっている場合は、各デバイスを再起動します。高可用性ペアにデバイスが設定されている場合、両方のデバイスを同時に再起動してアクティブ/アクティブの状態を回避します。
- 設定変更を展開します。設定変更の展開を参照してください。

特定のライセンスの予約の更新

Specific License	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Firepower Management Center	グローバルだけ	管理者

Firepower Management Center で特定のライセンスが正常に展開された後は、この手順を使用して付与資格をいつでも追加または削除できます。

ステップ 1 Firepower Management Center で、このアプライアンスの一意の製品インスタンス識別子を取得します。

a) [システム（System）] > [ライセンス（Licenses）] > [特定のライセンス（Specific Licenses）] を選択します。

b) [製品インスタンス（Product Instance）] の値をメモします。

この値はこのプロセス中に何度か必要になります。

ステップ 2 Cisco Smart Software Manager で、更新する Firepower Management Center のアプライアンスを識別します。

a) Cisco Smart Software Manager に移動します。

https://software.cisco.com/#SmartLicensing-Inventory

b) 必要に応じて、[インベントリ（Inventory）] をクリックします。

(このページは自動的に表示されることがあります。)

c) [製品インスタンス（Product Instances）] タブをクリックします。

d) [タイプ（Type）] 列に **FP**、[名前（Name）] 列に一般的な SKU（ホスト名ではない）が設定されている製品インスタンスを探します。また他のテーブル列の値を使用すると、どの Firepower Management Center が正しい Firepower Management Center かを判断するのに役立ちます。名前をクリックします。

e) **UUID** を調べ、変更しようとしている Firepower Management Center の UUID かどうかを確認します。

違う場合は、正しい Firepower Management Center が見つかるまで、これらの手順を繰り返す必要があります。

ステップ 3 Cisco Smart Software Manager で適切な Firepower Management Center アプライアンスが見つかったら、予約したライセンスを更新し、新しい承認コードを生成します。

a) 正しい UUID が表示されているページで、[アクション（Actions）] > [予約済みのライセンスの更新（Update Reserved Licenses）] を選択します。

b) 必要に応じて、予約済みライセンスを更新します。

重要

- 管理対象デバイスごとに **Firepower Threat Defense Base Features** ライセンスを、マルチインスタンス展開の場合は **Firepower Threat Defense ベース機能**ライセンスを明示的に含める必要があります。
- 仮想管理センターを使用している場合は、各モジュール（マルチインスタンス展開）か、または各管理対象デバイス（その他のすべての展開）に **Firepower MCv デバイス ライセンス**の資格を組み込む必要があります。
- 強力な暗号化機能を使用する場合：
  - スマート アカウント全体が輸出規制対象機能に対して有効になっている場合は、ここで何もする必要はありません。
  - 組織の資格が Firepower Management Center 単位の場合は、アプライアンス向けに適切なライセンスを選択する必要があります。

    デバイスに適切なライセンス名を選択するには、輸出規制機能の有効化（グローバル権限のないアカウントの場合） （23 ページ）の前提条件を参照してください。

c) [次へ（Next）] をクリックして詳細を確認します。
d) [承認コードを生成（Generate Authorization Code）] をクリックします。
e) Firepower Management Center に入力するための準備として承認コードをダウンロードします。
f) [予約の更新（Update Reservation）] ページを開いたままにしておきます。この手順の後半でこのページに戻ります。

ステップ 4 Firepower Management Center での特定のライセンスを更新するには、次の手順を実行します。

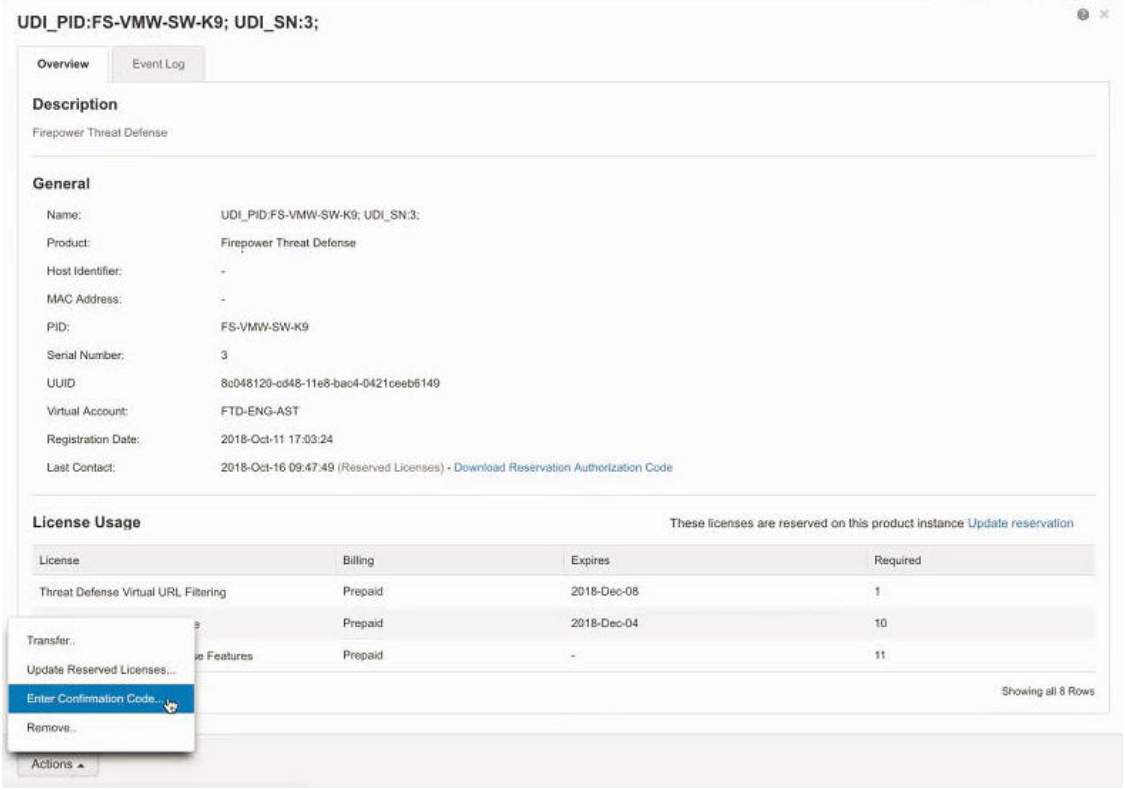
a) [システム（System）] > [ライセンス（Licenses）] > [特定のライセンス（Specific Licenses）] を選択します。
b) [SLR の編集（Edit SLR）] をクリックします。
c) [参照（Browse）] をクリックして、新たに生成された承認コードをアップロードします。
d) [インストール（Install）] をクリックしてライセンスを更新します。

   承認コードが正常にインストールされたら、Firepower Management Center の [予約済み（Reserved）] 列に表示されたライセンスが、Cisco Smart Software Manager で予約したライセンスと一致していることを確認します。

e) **確認コード**をメモします。

ステップ 5 Cisco Smart Software Manager に承認コードを入力するには、次の手順を実行します。

a) この手順の前半で開いたままにしておいた Cisco Smart Software Manager のページに戻ります。
b) [アクション（Actions）] > [確認コードの入力（Enter Confirmation Code）] を選択します。



c) Firepower Management Center から生成したコードを入力します。

ステップ 6 Firepower Management Center で、ライセンスが予期したとおりに予約されていること、および各管理対象デバイスの各機能にチェックマークが付いた緑色の丸（）が表示されていることを確認します。

必要に応じて、詳細については特定のライセンスの予約ステータス （38 ページ）を参照してください。

次のタスク

展開に輸出規制対象の機能が含まれている場合は各デバイスを再起動します。高可用性ペアにデバイスが設定されている場合、両方のデバイスを同時に再起動してアクティブ/アクティブの状態を回避します。

設定変更を展開します。設定変更の展開を参照してください。

重要：SLR 展開の維持

展開を有効に保つ脅威に関するデータとソフトウェアを更新するには、エアギャップ展開の維持を参照してください。

すべての機能が中断せずに動作し続けるようにするには、ライセンスの有効期限を（[予約済みライセンス（Reserved Licenses）] タブ）で監視します。

特定のライセンスの予約ステータス

次に示すように、[システム（System）]>[Licenses（ライセンス）]>[特定のライセンス（Specific Licenses）] ページには Firepower Management Center でのライセンスの使用状況の概要が表示されます。

使用の認証

可能なステータス値は次のとおりです。

- [承認済み（Authorized）]：Firepower Management Center は、アプライアンスのライセンスの付与資格を承認したライセンス認証局に準拠しており、正常に登録されています。
- [コンプライアンス不適合（Out-of-compliance）]：ライセンスの期限が切れているか、または Firepower Management Center が予約していないにもかかわらずライセンスを過剰に使用している場合、[コンプライアンス不適合（Out-of-Compliance）] がステータスに表示されます。[特定のライセンスの予約（Specific License Reservation）] にライセンスの付与資格が適用されるため、アクションを実行する必要があります。

製品登録

特定の登録ステータスと、Firepower Management Center で承認コードが最後にインストールされたか、または更新された日付を指定します。

輸出管理機能

Firepower Management Center の輸出規制対象機能を有効にしたかどうかを指定します。

輸出規制対象機能の詳細については、輸出規制対象の機能のライセンス （16 ページ）を参照してください。

製品インスタンス

この Firepower Management Center のユニバーサル一意識別子 (UUID)。この値は Cisco Smart Software Manager でこのデバイスを識別します。

確認コード

特定のライセンスを更新するか、または非アクティブ化して返却する場合に [確認コード（Confirmation Code）] が必要です。

[割り当て済みライセンス（Assigned Licenses）] タブ

各デバイスとそれぞれのステータスに割り当てられているライセンスを表示します。

[予約済みライセンス（Reserved Licenses）] タブ

割当に使用されているライセンスと使用可能なライセンスの数、およびライセンスの有効期限を表示します。

期限切れと特定のライセンスの予約

必要なライセンスが使用できないか、または期限が切れている場合、次のアクションは制限されています。

- デバイス登録に使用
- ポリシーの展開

特定のライセンスの予約の資格を更新するには、必要なライセンスを購入し、特定のライセンスの予約の更新 （35 ページ）の手順を実行します。

特定のライセンスの予約資格の更新

特定のライセンスの予約資格を更新する時期になったら、必要なライセンスを購入し、特定のライセンスの予約の更新 （35 ページ）の手順を実行します。

特定のライセンスの予約の非アクティブ化と返却

特定のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	Firepower Management Center	グローバルのみ	管理者

特定のライセンスが不要になった場合は、そのライセンスをスマートアカウントに戻す必要があります。

重要 この手順のすべてのステップを実行しないと、ライセンスは使用中の状態のままとなり、再利用できません。

この手順で、Firepower Management Center と関連付けられていたすべてのライセンスの付与資格が仮想アカウントに開放されます。登録を解除すると、ライセンスが付与された機能への更新や変更が許可されなくなります。

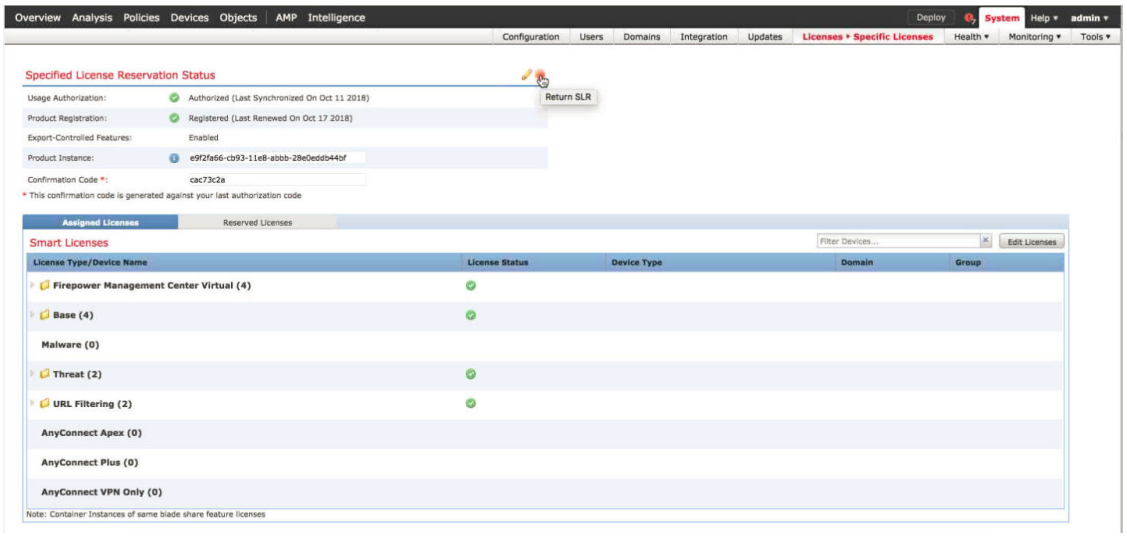
ステップ 1 Firepower Management Center の Web インターフェイスで、[システム（System）]>[ライセンス（Licenses）]>[特定のライセンス（Specific License）] を選択します。

ステップ 2 この Firepower Management Center の [製品インスタンス（Product Instance）] の識別子をメモします。

ステップ 3 Firepower Management Center から返却コードを生成するには、次の手順を実行します。

a) [SLR の返却（Return SLR）]] ボタンをクリックします。

次の図に、[SLR の返却（Return SLR）] ボタンを示します。



Firepower Threat Defense デバイスのライセンスが無効になり、Firepower Management Center が登録解除の状態に移行します。

b) **返却コード**をメモします。

ステップ 4 Cisco Smart Software Manager で、登録を解除する Firepower Management Center のアプライアンスを識別します。

a) Cisco Smart Software Manager に移動します。

https://software.cisco.com/#SmartLicensing-Inventory

b) 必要に応じて、[インベントリ（Inventory）] をクリックします。

(このページは自動的に表示されることがあります。)

c) [製品インスタンス（Product Instances）] タブをクリックします。

d) [タイプ（Type）] 列に **FP**、[名前（Name）] 列に一般的な SKU（ホスト名ではない）が設定されている製品インスタンスを探します。また他のテーブル列の値を使用すると、どの Firepower Management Center が正しい Firepower Management Center かを判断するのに役立ちます。名前をクリックします。

e) **UUID** を調べ、変更しようとしている Firepower Management Center の UUID かどうかを確認します。

違う場合は、正しい Firepower Management Center が見つかるまで、これらの手順を繰り返す必要があります。

ステップ 5 正しい Firepower Management Center が特定されたら、ライセンスをスマート アカウントに戻します。

a) 正しい UUID が表示されたページで、[アクション（Actions）] > [削除（Remove）] を選択します。

b) Firepower Management Center から生成した予約返却コードを [製品インスタンスの削除（Remove Product Instance）] ダイアログボックスに入力します。

c) [製品インスタンスの削除（Remove Product Instance）] をクリックします。

特定の予約済みライセンスがスマート アカウントの使用可能プールに戻り、この Firepower Management Center が Cisco Smart Software Manager の製品インスタンス リストから削除されます。

ステップ 6 Firepower Management Center の Linux シェルで、特定のライセンスを無効にします。

a) USB キーボードと VGA モニタを使用して Firepower Management Center コンソールにアクセスするか、または SSH を使用して管理インターフェイスにアクセスします。

b) Firepower Management Center の **admin** アカウントにログインします。デフォルトでは、これによって Linux シェルへのアクセス権が付与されます。Firepower Management Center の CLI が有効になっている場合は、これによってコマンドライン インターフェイスへのアクセス権が付与されます。

c) CLI が有効になっている Firepower Management Center の場合は、**expert** コマンドを入力して Linux シェルにアクセスします。

d) makecall ディレクトリで、次のコマンドを実行します。

```
sudo manage_slr.pl
```

例：

```
admin@fmc63betaslr: ~$ sudo manage_slr.pl
Password:


*************** Configuration Utility *************

1   Show SLR Status
2   Enable SLR
3   Disable SLR
0   Exit

************************************************************
Enter choice:
```

e) オプション 3 を選択して、特定のライセンスの予約を無効にします。

f) オプション 0 を選択して manage_slr ユーティリティを終了します。

g) **exit** と入力し、Linux シェルを終了します。

h) CLI が有効になっている Firepower Management Center では、入力 **exit** してコマンドライン インターフェイスを終了します。

特定のライセンスの予約のトラブルシューティング

Cisco Smart Software Manager の製品インスタンス リストから特定の Firepower Management Center を識別する方法を教えてください。

Cisco Smart Software Manager の [製品インスタンス（Product Instances）] ページで、テーブル内の列のいずれかの値に基づいて製品インスタンスが識別できない場合は、**FP** タイプの汎用製品インスタンスそれぞれの名前をクリックする必要があります。このページの **UUID** の値は 1 つの Firepower Management Center を一意に識別します。

Firepower Management Center の Web インターフェイスでは、Firepower Management Center の UUID は [システム（System）] > [ライセンス（Licenses）] > [特定のライセンス（Specific License）] ページに表示される [製品インスタンス（Product Instance）] の値です。

Cisco Smart Software Manager の [ライセンスの予約（License Reservation）] ボタンが表示されません。

[ライセンス予約（License Reservation）] ボタンが表示されない場合、お使いのアカウントでは個別ライセンスの予約が承認されていません。Linux シェルで特定のライセンスの予約をすでに有効にし、要求コードを生成している場合は、次の手順を実行します。

1. Firepower Management Center の Web インターフェイスですでに**要求コード**を生成している場合は、その要求コードをキャンセルします。
2. 「特定のライセンスの予約の非アクティブ化と返却 （39 ページ）」のセクションで説明しているように、Firepower Management Center の Linux シェルで特定のライセンスの予約を無効にします。
3. スマート トークンを使用して、通常モードで Firepower Management Center を Cisco Smart Software Manager に登録します。
4. Cisco TAC に連絡して、自分のスマート アカウントの個別ライセンスを有効にします。

ライセンス プロセスの最中に中断が発生しました。中断した場所を取得する方法を教えてください。

承認コードは生成したが、Cisco Smart Software Manager からまだダウンロードしていない場合は、Cisco Smart Software Manager の [製品インスタンス（Product Instance）] ページに移動し、製品インスタンスをクリックした後、[予約承認コードのダウンロード（Download Reservation Authorization Code）] をクリックします。

Firepower Threat Defense デバイスをFirepower Management Center Virtual に登録できません。

登録するデバイスをカバーするのに十分な MCv の資格がスマート アカウントにあることを確認してから展開を更新し、必要な資格を追加します。

特定のライセンスの予約の更新 （35 ページ）を参照してください。

特定のライセンスを有効にしていましたが、[スマート ライセンス（Smart License）] ページが表示されなくなりました。

これは予期されている動作です。[特定のライセンス（Specific Licensing）] を有効にすると、スマート ライセンスは無効になります。[特定のライセンス（Specific License）] ページを使用してライセンスの操作を実行できます。

スマート ライセンスを使用する場合は、特定のライセンスを返却する必要があります。詳細については、特定のライセンスの予約の非アクティブ化と返却 （39 ページ）を参照してください。

Firepower Management Center に [特定のライセンス（Specific License）] ページが表示されません。

[特定のライセンス（Specific License）] ページを表示するには、特定のライセンスを有効にする必要があります。詳細については、[特定のライセンス（Specific Licenses）] メニュー オプションの有効化 （31 ページ）を参照してください。

特定のライセンスを無効にしましたが、返却コードをコピーするのを忘れてしまいました。どうすればよいでしょうか。

[戻りコード（Return Code）] は Firepower Management Center に保存されています。Linux シェルから特定のライセンスをもう一度有効にし（「[特定のライセンス（Specific Licenses）] メニュー オプションの有効化 （31 ページ）」を参照）、Firepower Management Center の Web インターフェイスを更新します。[戻りコード（Return Code）] が表示されます。

複数の管理対象デバイスへのライセンスの割り当て

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	該当なし	Firepower Threat Defense	グローバルのみ	管理者

Firepower Management Center によって管理されるデバイスは、ライセンスを、Cisco Smart Software Manager から直接ではなく Firepower Management Center 経由で取得します。

複数の Firepower Threat Defense デバイスでスマート ライセンスまたは特定のライセンスを一度に有効にするには、次の手順を実行します。

（注） 同じ セキュリティ モジュール/エンジン のコンテナ インスタンスの場合は、ライセンスを各インスタンスに適用します。ただし、セキュリティ モジュール/エンジン のすべてのインスタンスについては、セキュリティ モジュール/エンジン は機能ごとに 1 つのライセンスのみを使用します。

（注） FTD クラスタの場合は、クラスタ全体にライセンスを適用します。ただし、クラスタ内の各ユニットが機能ごとに個別のライセンスを使用します。

始める前に

- まだ割り当てていない場合、Firepower Management Center でデバイスを登録します。Firepower Management Center へのデバイスの追加を参照してください。
- 管理対象デバイスに配布するためのライセンスを準備するには、次を参照してくださいスマート ライセンスの登録 （21 ページ）

ステップ 1 **[System]** > **[Licenses]** > **[Smart Licenses]** または [特定のライセンス（Specific Licenses）] を選択します。

ステップ 2 [ライセンスの編集（Edit Licenses）] をクリックします。

ステップ 3 デバイスに追加するライセンスのタイプごとに、次の手順を実行します。

a) 該当するライセンスのタイプのタブをクリックします。

b) 左側のリスト内のデバイスをクリックします。

c) [追加（Add）] をクリックして、デバイスを右側のリストに移動させます。

d) 各デバイスが該当するタイプのライセンスを受信するまで、この手順をデバイスごとに繰り返します。

ここでは、追加するすべてのデバイスのライセンスをユーザが保持しているかどうかを気にする必要はありません。

e) 追加するライセンスのタイプごとに、この手順を繰り返します。

f) [適用（Apply）] をクリックします。

次のタスク

- ライセンスが正しくインストールされていることを確認します。スマート ライセンスおよびスマート ライセンス ステータスの表示 （44 ページ） の手順に従います。
- 輸出規制対象の機能が新たに有効になった場合は、各デバイスを再起動します。高可用性ペアにデバイスが設定されている場合、両方のデバイスを同時に再起動してアクティブ/アクティブの状態を回避します。
- 設定変更を展開します。設定変更の展開を参照してください。

スマート ライセンスおよびスマート ライセンス ステータスの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	該当なし	Firepower Threat Defense	グローバルのみ	管理者

[スマート ライセンス（Smart Licenses）] ページで、Firepower Management Center とその管理対象 Firepower Threat Defense デバイスのスマート ライセンスを表示します。このページには、展開におけるライセンスのタイプごとに、使用されているライセンスの総数、そのライセンスのコンプライアンスの適合または不適合の状態、デバイス タイプ、およびデバイスが展開されているドメインとグループが表示されます。また、Firepower Management Center のスマート ライセンス ステータスを表示できます。同じ セキュリティ モジュール/エンジン 上の コンテナ インスタンスは セキュリティ モジュール/エンジン ごとに 1 つのライセンスを使用します。したがって、ライセンス タイプごとに各コンテナ ライセンスが個別に FMC に表示されても、機能ライセンス タイプに使用されているライセンスの数は 1 つのみです。

[スマート ライセンス（Smart Licenses）] ページ以外にも、ライセンスを表示できる方法がいくつかあります。

- [製品ライセンス（Product Licensing）] ダッシュボード ウィジェットはライセンスの概要を示します。

  ダッシュボードへのウィジェットの追加、ユーザ ロール別のダッシュボード ウィジェットの可用性、および[製品ライセンス（Product Licensing）] ウィジェットを参照してください。

- [デバイス管理（Device Management）] ページ（**[Devices]** > **[Device Management]**）は、各管理対象デバイスに適用されているライセンスをリストします。
- ヘルス ポリシーで使用される際に、スマート ライセンス モニタのヘルス モジュールはライセンス ステータスを伝達します。

ステップ 1 **[System]** > **[Licenses]** > **[Smart Licenses]**を選択します。

ステップ 2 [スマート ライセンス（Smart Licenses）] テーブルで、各 [ライセンス タイプ（License Type）] フォルダの左側にある矢印をクリックしてそのフォルダを展開します。

ステップ 3 各フォルダで、各デバイスの [ライセンス ステータス（License Status）] 列にチェックマーク付きの緑の円（）が表示されていることを確認します。

（注） Firepower Management Center 仮想ライセンスが重複している場合は、それぞれが 1 つの管理対象デバイスを表します。

すべてのデバイスにチェックマーク付きの緑の円（）が表示されている場合、デバイスには適切なライセンスがあり、使用できる状態にあります。

チェックマーク付きの緑の円（）以外のライセンス ステータスが表示されている場合は、ステータス アイコンにマウスオーバーしてメッセージを確認します。

次のタスク

- チェックマーク付きの緑の円（）が表示されているデバイスがない場合は、追加ライセンスの購入が必要な可能性があります。

スマート ライセンスのステータス

[システム（System）] > [ライセンス（Licenses）] > [スマート ライセンス（Smart Licenses）] ページの [スマート ライセンスのステータス（Smart License Status）] セクションでは、次に示すとおり、Firepower Management Center でのライセンスの使用状況の概要が提供されます。

使用の認証

可能なステータス値は次のとおりです。

- [コンプライアンス適合（In-compliance）]：管理対象デバイスに割り当てられているすべてのライセンスが要求を満たしており、 Firepower Management Center がシスコのライセンス認証局と正常に通信しています。
- ：デバイスのライセンスは要求を満たしていますが、Firepower Management Center がシスコのライセンス認証局と通信できません。
- [コンプライアンス不適合（Out-of-compliance）]またはライセンス認証局と通信できない：1 つ以上の管理対象デバイスがコンプライアンス不適合のライセンスを使用しているか、Firepower Management Center がシスコのライセンス認証局と通信していない期間が 90 日を超えています。

製品登録

Firepower Management Center がライセンス認証局に連絡し登録された最終日を指定します。

割当済みの仮想アカウント

製品インスタンス登録トークンの生成に使用したスマートアカウントの下の仮想アカウントを指定し、Firepower Management Center を登録します。この展開がスマート アカウント内の特定の仮想アカウントに関連付けられていない場合は、この情報は表示されません。

輸出管理機能

このオプションが有効になっている場合、制限機能を展開できます。詳細は、輸出規制対象の機能のライセンス （16 ページ）を参照してください。

Cisco Success Network

Firepower Management Centerの Cisco Success Network を有効にしたかどうかを指定します。このオプションを有効にすると、テクニカルサポートを提供するために不可欠な使用状況に関する情報と統計がシスコに提供されます。また、この情報により、シスコは製品を向上させ、未使用の使用可能な機能を認識させるため、ネットワーク内にある製品の価値を最大限に生かすことができます。詳細については、「Cisco Success Network （70 ページ）」を参照してください。

管理対象デバイスからのスマート ライセンスの移動または削除

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	該当なし	Firepower Threat Defense	グローバルのみ	管理者

1 つの Firepower Threat Defense デバイスから、同じ Firepower Management Center に登録されている別のデバイスにライセンスを移動するか、またはそのデバイスからライセンスを削除するには、次の手順を実行します。デバイスのライセンスを削除（無効化）すると、そのライセンスに関連付けられた機能をそのデバイスで使用できなくなります。

重要 別の Firepower Management Centerで管理されているデバイスにライセンスを移動する必要がある場合は、別の にスマート ライセンスを転送します。 Firepower Management Center （47 ページ）を参照してください。

ステップ 1 **[System]** > **[Licenses]** > **[Smart Licenses]**を選択します。

ステップ 2 [ライセンスの編集（Edit Licenses）] をクリックします。

ステップ 3 [マルウェア（Malware）]、[脅威（Threat）]、[URL フィルタリング（URL Filtering）]、[AnyConnect Plus]、[AnyConnect Apex]、または [AnyConnect VPN のみ（AnyConnect VPN Only）] のいずれかのタブをクリックします。

ステップ 4 ライセンスを付与するデバイスを選択して [追加（Add）] をクリックするか、ライセンスを削除する各デバイス形式をクリックして [Delete] アイコン（） をクリックします。

ステップ 5 [適用（Apply）] をクリックします。

次のタスク

変更内容を管理対象デバイスに展開します。

別の にスマート ライセンスを転送します。 Firepower Management Center

スマート ライセンスを Firepower Management Center に登録すると、バーチャル アカウントでそのライセンスが FMC に割り当てられます。スマート ライセンスを他の Firepower Management Center に移転する必要がある場合は、現在ライセンスが適用されている FMC の登録を解除する必要があります。これにより、バーチャルアカウントからスマート ライセンスが削除され、既存のライセンスが解放されるので、そのライセンスを新しい FMC に登録できるようになります。登録を解除しないと、これらのライセンスを再利用できず、バーチャルアカウントで使用可能なライセンスの数が足りなくなるために、コンプライアンス不適合通知を受け取る場合があります。この説明については、Cisco Smart Software Manager から Firepower Management Center の登録解除 （48 ページ） を参照してください。

その後、目的の Firepower Management Center にライセンスを登録できます。

[スマートライセンスのステータス（Smart License Status）] が [コンプライアンス不適合（Out of Compliance）] の場合

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	該当なし	Firepower Threat Defense	グローバルだけ	管理者

[スマートライセンス（Smart Licenses）] ページ（**[System]** > **[Licenses]** > **[Smart Licenses]**）の [使用の承認（Usage Authorization）] ステータスが [コンプライアンス不適合（Out of Compliance）] の場合はアクションを実行する必要があります。

ステップ 1 このページの下部にある [スマート ライセンス（Smart Licenses）] セクションを確認し、必要なライセンスを判断します。

ステップ 2 必要なライセンスを通常のチャネルを通じて購入します。

ステップ 3 Cisco Smart Software Manager (https://software.cisco.com/#SmartLicensing-Inventory)で、仮想アカウントにライセンスが表示されていることを確認します。

必要なライセンスがない場合はスマート ライセンスのトラブルシューティング （49 ページ）を参照してください。

ステップ 4 Firepower Management Center で、**[System]** > **[Licenses]** > **[Smart Licenses]** を選択します。

ステップ 5 [再承認（Re-Authorize）] ボタンをクリックします。

Cisco Smart Software Manager から Firepower Management Center の登録解除

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	該当なし	Firepower Threat Defense	グローバルのみ	管理者

アプライアンスを再インストール（再イメージ化）する前か、または何らかの理由ですべてのライセンスの付与資格を開放してスマート アカウントに戻す必要がある場合は、Cisco Smart Software Manager から Firepower Management Center の登録を解除（未登録に）します。

登録を解除すると、仮想アカウントから FMC が削除されます。Firepower Management Center リリースに関連付けられているライセンス権限はすべて、ご使用のバーチャルアカウントに戻ります。登録解除後、Firepower Management Center は適用モードになり、ライセンスが適用される機能に対する更新および変更が許可されなくなります。

管理対象の Firepower Threat Defense の一部のデバイスからライセンスを削除する必要がある場合は、複数の管理対象デバイスへのライセンスの割り当て （43 ページ）または[デバイス管理（Device Management）] ページで管理対象デバイスにライセンスを割り当てる （62 ページ）を参照してください。

ステップ 1 **[System]** > **[Licenses]** > **[Smart Licenses]**を選択します。

ステップ 2 登録解除アイコン（）をクリックします。

Cisco Smart Software Manager と Firepower Management Center の同期

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	該当なし	Firepower Threat Defense	グローバルのみ	管理者

Cisco Smart Software Manager に変更を加えた場合は、すぐに変更が有効になるように Firepower Management Center 上で認証を更新できます。

ステップ 1 **[System]** > **[Licenses]** > **[Smart Licenses]**を選択します。

ステップ 2 更新アイコン（）をクリックします。

スマート ライセンスのトラブルシューティング

予期していたライセンスがスマート アカウントに表示されません。

表示されると思っていたライセンスがスマート アカウントにない場合は、次を試してください。

- 他の仮想アカウントにないことを確認します。この問題について、組織のライセンス管理者によるサポートが必要な場合があります。
- ライセンスを販売した担当者と、アカウントへの譲渡が完了していることを確認します。

予期していなかったコンプライアンス不適合の通知またはその他のエラー

- デバイスが別の FMC にすでに登録されている場合は、新しい FMC にデバイスのライセンスを付与する前に元の FMC の登録を解除する必要があります。Cisco Smart Software Manager から Firepower Management Center の登録解除 （48 ページ）を参照してください。

- 同期を試行します。Cisco Smart Software Manager と Firepower Management Center の同期 （49 ページ）を参照してください。

Firepower 7000/8000 シリーズのライセンス、ASA FirePOWER、および NGIPSv デバイス（従来のライセンス）

7000 および 8000 シリーズ デバイス、NGIPSv デバイス、および ASA FirePOWER モジュールには従来のライセンスが必要です。このドキュメントでは、これらのデバイスは多くの場合、クラッシク デバイスと呼ばれています。

重要 Firepower ハードウェアを稼働しているが Firepower ソフトウェアは実行していない場合は、使用しているソフトウェア製品のライセンス情報を参照してください。このドキュメントでは扱っていません。

クラシック ライセンスは、製品認証キー（PAK）をアクティブにする必要があり、デバイスごとに必要です。クラシック ライセンスは、「従来のライセンス」と呼ばれることもあります。

製品ライセンス登録ポータル

Firepower 機能のクラシック ライセンスを 1 つ以上購入する場合は、それらのライセンスを Cisco Product License Registration ポータルで管理します。

http://www.cisco.com/web/go/license

このポータルの使用方法の詳細については、次を参照してください。

https://www.cisco.com/web/fw/tools/swift/xui/html/help.html

Firepower 機能のサービス サブスクリプション（クラシック ライセンス）

一部の機能にはサービス サブスクリプションが必要です。

サービス サブスクリプションは、所定の時間内限定で、管理対象デバイス上の特定の Firepower 機能を有効にします。サービス サブスクリプションは、1 年、3 年、または 5 年単位で購入できます。サブスクリプションの期限が切れると、サブスクリプションの更新が必要であることが通知されます。クラシック デバイスのサブスクリプションの期限が切れた場合、機能のタイプによっては、関連機能を使用できなくなることがあります。

表 *4:* サブスクリプションおよび対応するクラシック ライセンス

購入するサブスクリプション	Firepower システム内で割り当てるクラシック ライセンス
TA	制御 + 保護（別名「脅威 & アプリ」、システム更新に必要）
TAC	制御 + 保護 + URL フィルタリング
TAM	制御 + 保護 +マルウェア
TAMC	制御 + 保護 + URL フィルタリング + マルウェア
URL	URL フィルタリング（TA が既に存在する場合はアドオン）
AMP	マルウェア（TA が既に存在する場合はアドオン）

クラシック ライセンスを使用する管理対象デバイスを購入すると、制御および保護のライセンスが自動的に提供されます。これらのライセンスは無期限ですが、システムの更新を有効にするには、TA サービス サブスクリプションを購入する必要があります。追加機能のサービス サブスクリプションはオプションです。

従来のライセンスのタイプと制約事項

ここでは、Firepower システム展開環境で使用可能な従来のライセンスのタイプについて説明します。デバイスで有効にできるライセンスは、デバイスのモデル、バージョン、および他の有効なライセンスによって異なります。

7000 および 8000 シリーズ デバイス、NGIPSv デバイス、および ASA FirePOWER モジュールの場合、ライセンスはモデル固有です。ライセンスがデバイスのモデルと完全に一致しない限り、管理対象デバイスでライセンスを有効にすることはできません。たとえば、Firepower 8250 マルウェア ライセンス（FP8250-TAM-LIC=）を使用して 8140 デバイスでマルウェア関連の機能を有効にすることはできません。Firepower 8140 マルウェア ライセンス（FP8140-TAM-LIC=）を購入する必要があります。

（注） NGIPSv または ASA FirePOWER では、制御ライセンスを使用してユーザとアプリケーションの制御を実行できますが、それらのデバイスはスイッチング、ルーティング、スタッキング、または 7000 および 8000 シリーズ デバイスの高可用性をサポートしていません。

Firepower システムでライセンス付き機能にアクセスできなくなる状況がいくつかあります。

- Firepower Management Center から従来のライセンスを削除することができますが、そのようにすると、すべての管理対象デバイスに影響します。
- 特定の管理対象デバイスでライセンス付き機能を無効にすることができます。

いくつかの例外がありますが、期限切れライセンスまたは削除済みライセンスに関連付けられている機能は使用できません。

次の表に、Firepower システムにおける従来のライセンスの概要を示します。

表 *5 : Firepower* システムの従来のライセンス

Firepowerシステムで割り当てるライセンス	購入するサービスサブスクリプション	プラットフォーム	付与される機能	併せて必要なライセンス	有効期限設定可/不可
任意	TA、TAC、TAM、またはTAMC	7000 および 8000 シリーズ ASA FirePOWER NGIPSv	ホスト、アプリケーション、ユーザ検出 SSL 暗号化トラフィックと TLS 暗号化トラフィックの復号および検査	なし	ライセンスによって異なる
プロテクション	TA（デバイスに付属）	7000 および 8000 シリーズ ASA FirePOWER NGIPSv	侵入検知と防御 ファイル制御 Security Intelligence フィルタリング	なし	不可
制御	なし（デバイスに付属）	7000 および 8000 シリーズ	ユーザおよびアプリケーション制御 スイッチングとルーティング 7000 および 8000 シリーズ デバイスの高可用性 7000 および 8000 シリーズネットワーク アドレス変換（NAT）	プロテクション	不可
制御	なし（デバイスに付属）	ASA FirePOWER NGIPSv	ユーザおよびアプリケーション制御	プロテクション	不可
マルウェア	TAM、TAMC、または AMP	7000 および 8000 シリーズ ASA FirePOWER NGIPSv	ネットワーク向け AMP（ネットワークベースの高度なマルウェア防御） ファイル ストレージ	プロテクション	可
URL フィルタリング	TAC、TAMC、または URL	7000 および 8000 シリーズ ASA FirePOWER NGIPSv	カテゴリとレピュテーションに基づく URL フィルタリング	プロテクション	可

Firepower システムで割り当てるライセンス	購入するサービス サブスクリプション	プラットフォーム	付与される機能	併せて必要なライセンス	有効期限設定可/不可
VPN	なし（詳細は販売担当者までお問い合わせください）	7000 および 8000 シリーズ	仮想プライベート ネットワークの導入	制御	可

プロテクション ライセンス

プロテクション ライセンスでは、侵入検知および防御、ファイル制御、およびセキュリティ インテリジェンス フィルタリングを実行できます。

- 侵入検知および防御により、侵入とエクスプロイトを検出するためネットワーク トラフィックを分析できます。またオプションで違反パケットをドロップできます。
- ファイル制御により、特定のアプリケーションプロトコルを介した特定タイプのファイルを検出し、オプションでこれらのファイルのアップロード（送信）またはダウンロード（受信）をユーザからブロックできます。マルウェア ライセンスが必要な ネットワーク向け *AMP* では、マルウェアの性質に基づいて限られたファイル タイプを検査およびブロックすることもできます。
- セキュリティインテリジェンス フィルタリングにより、トラフィックをアクセス制御ルールによる分析対象にする前に、特定の IP アドレス、URL、および DNS ドメイン名をブラックリストに追加（その IP アドレスとの間のトラフィックを拒否）できます。ダイナミック フィードにより、最新の情報に基づいて接続を直ちにブラックリストに追加できます。オプションで、Security Intelligence フィルタリングに「監視のみ」設定を使用できます。

プロテクションライセンス（制御ライセンスと共に）は、クラシック管理対象デバイスの購入時に自動的に組み込まれます。このライセンスは無期限ですが、システムの更新を有効にするには、TA サブスクリプションも購入する必要があります。

ライセンスがない状態でプロテクション関連の検査を実行するようにアクセス制御ポリシーを設定できますが、プロテクション ライセンスを Firepower Management Center に追加し、ポリシー展開対象デバイス上でこのライセンスを有効にするまではポリシーを展開できません。

プロテクション ライセンスを Firepower Management Center から削除するか、または管理対象デバイスでプロテクションを無効にすると、Firepower Management Center は対象デバイスからの侵入イベントとファイルイベントを認識しなくなります。結果として、トリガー条件としてこれらのイベントを使用する相関ルールがトリガーしなくなります。また、Firepower Management Center はシスコ提供またはサード パーティのセキュリティ インテリジェンス情報を取得するためにインターネットに接続しなくなります。プロテクションを再度有効にするまでは、既存のポリシーを再度展開することはできません。

プロテクション ライセンスは URL フィルタリング、マルウェア、および制御ライセンスに必要であるため、プロテクションライセンスを削除または無効にすると、URL フィルタリング、マルウェア、または制御ライセンスを削除または無効にすることと同じ効果があります。

制御ライセンス

制御ライセンスでは、アクセス コントロール ルールにユーザとアプリケーションの条件を追加することで、ユーザとアプリケーションの制御を実装できます。7000 および 8000 シリーズ デバイスでは、このライセンスを使用して、スイッチングとルーティング（DHCP リレーおよび NAT を含む）、およびデバイスのハイ アベイラビリティ ペアも構成できます。管理対象デバイスの制御ライセンスを有効にするには、保護ライセンスも有効にする必要があります。制御ライセンスは（保護ライセンスとともに）、従来の管理対象デバイスの購入時に自動的に付属します。このライセンスは無期限ですが、システムの更新を有効にするには、TA サブスクリプションも購入する必要があります。

従来の管理対象デバイスの制御ライセンスを有効にしない場合は、アクセス コントロール ポリシーのルールにユーザおよびアプリケーションの条件を追加できますが、デバイスにポリシーを展開することはできません。7000 または 8000 シリーズ デバイスの制御ライセンスを明確に有効にしないと、次の操作も行えません。

- スイッチド、ルーテッド、またはハイブリッド インターフェイスの作成
- NAT エントリの作成
- 仮想ルータの DHCP リレーの設定
- デバイスへのスイッチまたはルーティングが含まれているデバイス設定の展開
- デバイス間のハイ アベイラビリティの確立

（注） 制御ライセンスがなくても仮想スイッチおよびルータを作成できますが、データを取り込むスイッチドインターフェイスおよびルーテッドインターフェイスがない状態ではこれらのスイッチとルータは有用ではありません。

Firepower Management Center から制御ライセンスを削除するか、個々のデバイスで制御を無効にする場合：

- 対象デバイスでのスイッチングとルーティングの実行が行われなくなったり、デバイスのハイ アベイラビリティ ペアが解除されたりすることはありません。
- 既存の設定の編集や削除を続けることはできますが、影響を受けるデバイスに対する変更を展開することはできません。
- 新しいスイッチド インターフェイス、ルーテッド インターフェイス、またはハイブリッド インターフェイスを追加することも、新しい NAT エントリの追加、DHCP リレーの設定、7000 または 8000 シリーズ デバイスのハイ アベイラビリティの確立もできません。
- 既存のアクセス コントロール ポリシーに、ユーザ条件またはアプリケーション条件を含むルールが含まれている場合は、それらのポリシーを再展開することができません。

従来のデバイスの URL フィルタリング ライセンス

URL フィルタリングにより、モニタ対象ホストにより要求される URL に基づいて、ネットワーク内を移動できるトラフィックを判別するアクセス制御ルールを作成することができます。URL フィルタリング ライセンスを有効にする場合は、保護ライセンスも有効にする必要があります。従来のデバイスの URL フィルタリング ライセンスは、脅威 & アプリ（TAC）または脅威 & アプリおよびマルウェア（TAMC）サブスクリプションと組み合わせてサービス サブスクリプションとして購入できます。また、脅威 & アプリ（TA）が既に有効になっているシステムの場合は、アドオン サブスクリプションとして購入できます。

ヒント URL フィルタリング ライセンスがない状態で、許可またはブロックする個別 URL または URL グループを指定できます。これにより、Web トラフィックをカスタムできめ細かく制御できますが、URL カテゴリおよびレピュテーション データをネットワーク トラフィックのフィルタリングに使用することはできません。

URL フィルタリング ライセンスがない状態でも、アクセス制御ルールにカテゴリ ベースの URL 条件およびレピュテーション ベースの URL 条件を追加できますが、Firepower Management Center は URL 情報をダウンロードしません。最初に URL フィルタリング ライセンスを Firepower Management Center に追加し、ポリシー適用対象デバイスで有効にするまでは、アクセス コントロール ポリシーを適用できません。

Firepower Management Center からライセンスを削除するか、または管理対象デバイスで URL フィルタリングを無効にすると、URL フィルタリングにアクセスできなくなることがあります。また、URL フィルタリング ライセンスの有効期限が切れることもあります。ライセンスが期限切れになるか、ライセンスを削除または無効化すると、URL 条件が含まれているアクセス制御ルールは URL フィルタリングを直ちに停止し、Firepower Management Center は URL データのアップデートをダウンロードできなくなります。既存のアクセス コントロール ポリシーに、カテゴリ ベースまたはレピュテーション ベースの URL 条件を含むルールが含まれている場合は、それらのポリシーを再展開することができません。

従来のデバイスのマルウェア ライセンス

マルウェア ライセンスを使用すると、ネットワーク向け AMP および Cisco Threat Grid を使用して Cisco Advanced Malware Protection（AMP）を実行することができます。管理対象デバイスを使用して、ネットワーク上で伝送されるファイルのマルウェアを検出してブロックできます。マルウェア ライセンスを有効にするには、保護も有効にする必要があります。マルウェア ライセンスは、脅威 & アプリ（TAM）と組み合わせたサブスクリプションまたは脅威 & アプリおよび URL フィルタリング（TAMC）サブスクリプションとして購入できます。また、脅威 & アプリ（TA）が既に有効になっているシステムの場合は、アドオン サブスクリプションとして購入できます。

（注） マルウェア ライセンスが有効になっている 7000 および 8000 シリーズ 管理対象デバイスは、動的分析を設定していない場合でも、定期的に AMP クラウドへの接続を試行します。このため、デバイスの [インターフェイス トラフィック（Interface Traffic）] ダッシュボード ウィジェットには、送信済みトラフィックが表示されます。これは正常な動作です。

ファイル ポリシーの一部として ネットワーク向け AMP を設定し、その後 1 つ以上のアクセス コントロール ルールを関連付けます。ファイル ポリシーでは、特定のアプリケーション プロトコルを介した特定のタイプのユーザによるファイルのアップロードとダウンロードを検出できます。ネットワーク向け AMP では、ローカル マルウェア分析とファイルの事前分類を使用して、それらの限られた一連のファイルタイプを検査できます。特定のファイル タイプをダウンロードして Cisco Threat Grid クラウドにアップロードして、動的 Spero 分析でマルウェアが含まれているかどうかを判別することもできます。これらのファイルでは、ファイルがネットワーク内で経由する詳細なパスを示すネットワーク ファイル トラジェクトリを表示できます。マルウェア ライセンスでは、ファイル リストに特定のファイルを追加し、そのファイル リストをファイル ポリシー内で有効にすることもできます。これにより、検出時にこれらのファイルを自動的に許可またはブロックできます。

ネットワーク向け AMP 構成を含むアクセス コントロール ポリシーを展開する前に、マルウェア ライセンスを追加してから、そのポリシー展開対象デバイスで有効にする**必要があります**。デバイスでライセンスを後で無効にする場合、既存のアクセス コントロール ポリシーをそれらのデバイスに再度展開することはできません。

マルウェア ライセンスをすべて削除するか、それらがすべて期限切れになると、システムは AMP への問い合わせを停止し、AMP クラウドから送信される遡及的イベントの確認応答も停止します。既存のアクセス コントロール ポリシーに ネットワーク向け AMP 構成が含まれている場合は、それらのポリシーを再展開することができません。マルウェア ライセンスが失効したか削除された後、システムが既存のキャッシュ ファイルの性質を使用できるのは極めて短時間のみであることに注意してください。この時間枠の経過後、システムは `Unavailable` という性質をこれらのファイルに割り当てます。

マルウェア ライセンスが必要なのは ネットワーク向け AMP および Cisco Threat Grid を展開する場合のみです。マルウェア ライセンスがなければ、Firepower Management Center は AMP クラウドからエンドポイント向け AMP マルウェア イベントおよび侵害の兆候（IOC）を受信できます。

ファイルおよびマルウェア ポリシーのライセンス要件の重要な情報も参照してください。

7000 および 8000 シリーズ デバイス用の VPN ライセンス

VPN を使用すると、インターネットやその他のネットワークなどの公共ソースを経由してエンドポイント間にセキュア トンネルを確立できます。7000 および 8000 シリーズ デバイスの仮想ルータ間で安全な VPN トンネルを構築するよう、Firepower システムを設定することができます。VPN を有効にするには、保護および制御のライセンスも有効にする必要があります。VPN ライセンスを購入するには、販売担当者までお問い合わせください。

VPN ライセンスがないと、7000 および 8000 シリーズ デバイスで VPN 導入環境を設定できません。導入環境の作成はできますが、データを取り込むための 1 つ以上の VPN 対応スイッチド インターフェイスおよびルーテッド インターフェイスがない状態では、導入環境は有用ではありません。

VPN ライセンスを Firepower Management Center から削除するか、または個別のデバイスで VPN を無効にすると、対象デバイスは現在の VPN 導入環境をブレイクしません。既存の導入環境を編集または削除できますが、対象デバイスに変更を適用することはできません。

デバイス スタックおよびハイ アベイラビリティ ペアのクラシック ライセンス

スタックや 7000 または 8000 シリーズ デバイス ハイ アベイラビリティ ペアを構成するデバイスは、それぞれが同等のライセンスを持っている必要があります。デバイスのスタック構成後に、スタック全体のライセンスを変更できます。ただし、7000 または 8000 シリーズ デバイスのハイ アベイラビリティ ペアでは有効なライセンスを変更することはできません。

「デバイス スタックについて」および「デバイスのハイ アベイラビリティ要件」も参照してください。

従来型ライセンスの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	任意	従来型	グローバルのみ	管理者

必要に応じて、次のいずれかを実行します。

目的	操作手順
Firepower Management Center に追加済みの従来のライセンスおよびそのタイプ、ステータス、使用状況、有効期限、適用されている管理対象デバイスなどの詳細情報	**[System]** > **[Licenses]** > **[Classic Licenses]**を選択します。 概要には、購入したライセンスの数の後に使用中のライセンスの数が括弧内に表示されます。
管理対象デバイスそれぞれに適用されたライセンス	**[Devices]** > **[Device Management]**を選択します。
ヘルスモニタのライセンステータス	正常性ポリシーでクラシックライセンスモニタのヘルスモジュールを使用します。詳細については、ヘルス モニタリング、ヘルス モジュール、および正常性ポリシーの作成を参照してください。

目的	操作手順
ダッシュボードのライセンスの概要	任意のダッシュボードに製品ライセンスウィジェットを追加します。手順については、[製品ライセンス（Product Licensing）] ウィジェット、ダッシュボードへのウィジェットの追加、およびユーザ ロール別のダッシュボード ウィジェットの可用性を参照してください。

ライセンス キーの特定

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	任意	従来型	グローバルのみ	管理者

ライセンス キーによって、Firepower Management Center はシスコ ライセンス登録ポータルで一意に識別されます。これは、Firepower Management Center の製品コード（66 など）と管理ポート（eth0）の MAC アドレスで構成されます（66:00:00:77:FF:CC:88 など）。

シスコ ライセンス登録ポータルでは、ライセンス キーを使用して、Firepower Management Center にライセンスを追加する際に必要になるライセンス テキストを取得します。

ステップ 1 **[System]** > **[Licenses]** > **[Classic Licenses]** を選択します。

ステップ 2 [新規ライセンスの追加（Add New License）] をクリックします。

ステップ 3 [機能ライセンスの追加（Add Feature License）] ダイアログの上部にある [ライセンス キー（License Key）] フィールドの値をメモします。

次のタスク

- ライセンスを Firepower Management Center に追加します。クラシック ライセンスの生成と Firepower Management Center への追加 （59 ページ）を参照してください。

  この手順には、ライセンス キーを使用して実際のライセンス テキストを生成するプロセスが含まれています。

クラシック ライセンスの生成と Firepower Management Center への追加

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
該当なし	任意	従来型	グローバルのみ	管理者

（注） バックアップが完了した後にライセンスを追加した場合は、このバックアップを復元するときに、それらのライセンスが削除されたり上書きされたりすることはありません。復元の際の競合を防止するためにも、バックアップを復元する前に、これらのライセンスを（それらが使用されている場所をメモした上で）削除し、バックアップを復元した後で、追加して再設定してください。競合が発生した場合は、サポートに連絡してください。

ヒント サポート サイトにログインした後で、[ライセンス（Licenses）] タブでライセンスを要求することもできます。

始める前に

- ライセンス購入時にCiscoが提供したソフトウェア権利証明書にある製品アクティベーション キー（PAK）をお手元にご用意ください。レガシーの、以前のシスコのライセンスの場合は、サポートに問い合わせてください。
- Firepower Management Center のライセンス キーの種類を確認します。ライセンス キーの特定 （58 ページ） を参照してください。

ステップ 1 **[System]** > **[Licenses]** > **[Classic Licenses]**を選択します。

ステップ 2 [新規ライセンスの追加（Add New License）] をクリックします。

ステップ 3 必要に応じ、続いて以下を行います。

- ライセンス テキストをすでに取得している場合は、ステップ 8 にスキップしてください。
- ライセンスのテキストを取得する必要がある場合は、次の手順を実行します。

ステップ 4 [ライセンス取得（Get License）] をクリックして、Cisco ライセンス登録ポータルを開きます。

（注） ご使用のコンピュータからインターネットにアクセスできない場合は、アクセスできるコンピュータから http://cisco.com/go/licenseを探します。

ステップ 5 ライセンス登録ポータルで、PAKからライセンスを生成します。詳細については、https://www.cisco.com/web/fw/tools/swift/xui/html/help.htmlを参照してください。

この手順には、購入時に入手した PAK と、Firepower Management Center のライセンスキーが必要です。

ステップ 6 ライセンス登録ポータルの表示から、ないしはライセンス登録ポータルより送られてくるメールからライセンス テキストをコピーします。

重要 ポータルまたは電子メール メッセージ内のライセンス テキスト ブロックには、複数のライセンスを含めることができます。各ライセンスは、BEGIN LICENSE 行と END LICENSE 行で囲まれます。一度に 1 つのライセンスしかコピーして貼り付けることができません。

ステップ 7 Firepower Management Center の web インターフェイスの [機能ライセンスの追加（Add Feature License）] ページに戻ります。

ステップ 8 [ライセンス（License）] フィールドにライセンス テキストを貼り付けます。

ステップ 9 [ライセンスの検証（Verify License）] をクリックします。

ライセンスが無効となる場合は、ライセンス テキストが正しくコピーされているか確認します。

ステップ 10 [ライセンスの提出（Submit License）] をクリックします。

次のタスク

- 管理対象デバイスにライセンスを割り当てます。[デバイス管理（Device Management）] ページで管理対象デバイスにライセンスを割り当てる （62 ページ） を参照してください。管理対象デバイスのライセンス取得済み機能を使用するには、これらのデバイスにライセンスを割り当てる**必要があります**。

クラシック ライセンスまたは PAK からスマート ライセンスへの変換

ライセンス登録ポータル (LRP) または、Cisco Smart Software Manager (CSSM) のいずれかを使用してライセンスを変換し、未使用の製品認証キー（PAK）またはデバイスにすでに割り当てられているクラシック ライセンスに変換することができます。

重要 このプロセスは元に戻すことはできません。そのライセンスが元々はクラッシク ライセンスであっても、スマート ライセンスをクラッシク ライセンスに変換することはできません。

Cosco.com のドキュメントでは、クラッシック ライセンスは「従来型の」ライセンスとも呼ばれています。

始める前に

- 製品インスタンスにまだ割り当てられていない未使用の PAK がある場合、従来のライセンスからスマート ライセンスへの変換は最も簡単です。

- ハードウェアで Firepower Threat Defense を実行できる必要があります。詳細については、https://www.cisco.com/c/en/us/support/security/defense-center/products-device-support-tables-list.html で『*Cisco Firepower Compatibility Guide*』を参照してください。
- スマートアカウントが必要です。ない場合は作成します。ライセンスを保持するためのスマート アカウントの作成 （18 ページ）を参照してください。
- 変換する PAK またはライセンスは、スマート アカウントに表示されている必要があります。
- Cisco Smart Software Manager ではなくライセンス登録ポータルを使用して変換する場合に変換プロセスを開始するには、スマート アカウント クレデンシャルを保有している必要があります。

ステップ 1 実行する変換プロセスは、そのライセンスが使用されたことがあるかどうかによって異なります。

- 変換する PAK が使用されたことがない場合は、PAK の変換の手順を実行します。
- 変換する PAK がデバイスにすでに割り当てられている場合は、クラッシク ライセンスの変換の手順を実行します。

既存の従来のライセンスがまだデバイスに登録されていることを確認します。

ステップ 2 次のドキュメントで変換のタイプ（PAK またはインストール済みのクラシック ライセンス）の手順を参照してください。

- LRP を使用して PAK またはライセンスを変換するには、次の手順を実行します。
  - 変換プロセスのライセンス登録ポータル部分の手順がわかるビデオを表示する場合は、https://salesconnect.cisco.com/#/content-detail/7da52358-0fc1-4d85-8920-14a1b7721780 をクリックします。
  - https://cisco.app.box.com/s/mds3ab3fctk6pzonq5meukvcpjizt7wu のドキュメントで「変換（Convert）」を検索します。

    変換手順は 3 つあります。状況に該当する変換手順を選択します。
  - https://tools.cisco.com/SWIFT/LicensingUI/Home でライセンス登録ポータル（LRP）にサインインし、上記のドキュメントの手順を実行します。
- CSSM を使用して PAK またはライセンスを変換するには、次の手順を実行します。
  - ハイブリッド ライセンスをスマート ソフトウェア ライセンス *QRG* に変換するには、次の手順を実行します。

    https://community.cisco.com/t5/licensing-enterprise-agreements/converting-hybrid-licenses-to-smart-software-licenses-qrg/ta-p/3628609?attachment-id=134907
  - https://software.cisco.com/#SmartLicensing-LicenseConversion で CSSM にサインインし、上記のドキュメントの変換タイプ（PAK またはインストール済みのクラッシック ライセンス）の手順を実行します。

ステップ 3 ハードウェアに Firepower Threat Defense を新たにインストールします。

https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-guides-list.html のハードウェアに関する手順を参照してください。

ステップ 4 Firepower Device Manager を使用してこのデバイスをスタンドアロン デバイスとして管理するには、次の手順を実行します。

https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-and-configuration-guides-list.html の『*Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager*』のデバイスへのライセンス付与に関する情報を参照してください。

この手順の残りは省略してください。

ステップ 5 Firepower Management Center でスマート ライセンスをすでに展開している場合は、次の手順を実行します。

a) 新しい Firepower Threat Defense デバイスでスマート ライセンスを設定します。

複数の管理対象デバイスへのライセンスの割り当て （43 ページ）を参照してください。

b) 新しいスマート ライセンスがデバイスに正常に適用されていることを確認します。

スマート ライセンスおよびスマート ライセンス ステータスの表示 （44 ページ）を参照してください。

ステップ 6 Firepower Management Center でスマート ライセンスをまだ展開していない場合は、次の手順を実行します。

Firepower Threat Defense デバイスのライセンス （4 ページ）を参照してください。（該当しないか、またはすでに完了しているステップはスキップします。）

[デバイス管理（Device Management）] ページで管理対象デバイスにライセンスを割り当てる

スマート ライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
任意	任意	任意	リーフのみ	管理者/ネットワーク管理者

一部の例外はありますが、管理対象デバイスでライセンスを無効にすると、そのライセンスに関連づけられている機能は使用できなくなります。

（注） 同じ セキュリティ モジュール/エンジン のコンテナ インスタンスの場合は、ライセンスを各インスタンスに適用します。ただし、セキュリティ モジュール/エンジン のすべてのインスタンスについては、セキュリティ モジュール/エンジン は機能ごとに 1 つのライセンスのみを使用します。

（注） FTD クラスタの場合は、クラスタ全体にライセンスを適用します。ただし、クラスタ内の各ユニットが機能ごとに個別のライセンスを使用します。

始める前に

- デバイスを Firepower Management Center に追加します。Firepower Management Center へのデバイスの追加を参照してください。
- スマート ライセンスを割り当てる場合、次の手順に従います。
  - スマートライセンスを同時に多くのデバイスに適用する必要がある場合、次の手順ではなく、[スマート ライセンス（Smart Licenses）] ページを使用します。複数の管理対象デバイスへのライセンスの割り当て （43 ページ）を参照してください
  - 管理対象デバイスに配布するためのスマートライセンスを準備するには、次を参照してください。 スマート ライセンスの登録 （21 ページ）

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 ライセンスを割り当てまたは無効にするデバイスの横にある編集アイコン（）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [デバイス（Device）] タブをクリックします。

ステップ 4 [ライセンス（License）] セクションの横にある編集アイコン（）をクリックします。

ステップ 5 適切なチェックボックスをオンまたはオフにして、デバイスのライセンスを割り当て、または無効にします。

ステップ 6 [保存（Save）] をクリックします。

次のタスク

- スマートライセンスを割り当てられている場合、ライセンスのステータスを確認します。

  [System] > **[Licenses]** > **[Smart Licenses]** に移動し、[スマート ライセンス（Smart Licenses）] テーブル上部のフィルタにホスト名またはデバイスの IP アドレスを入力し、各デバイス

および各ライセンス に、チェックマーク（  ）のある緑色の円のみが表示されることを確認します。その他のアイコンが表示される場合は、アイコンにマウスオーバーすると詳細を確認できます。

- 設定変更を展開します。設定変更の展開を参照してください。
- Firepower Threat Defense デバイスのライセンスを供与し、エクスポート制御機能が有効になっている基本ライセンスを適用した場合は、各デバイスを再起動します。高可用性ペアに設定されているデバイスの場合、両方のデバイスを同時に再起動してアクティブ/アクティブの状態を回避します。

FirePOWER のライセンスとサービス サブスクリプションの期限切れ

ライセンスの期限切れとサービス サブスクリプションの期限切れ

Q. FirePOWER の機能ライセンスは期限切れになりますか。

A. 厳密に言えば、FirePOWER の機能ライセンスは期限切れになりません。代わりに、このライセンスをサポートするサービス サブスクリプションが期限切れになります。サービスのサブスクリプションに関する詳細については、https://www.cisco.com/c/en/us/support/security/defense-center/products-installation-and-configuration-guides-list.html から入手できる『*Firepower Management Center Configuration Guide*』の「Service Subscriptions for Firepower Features」を参照してください。

スマート ライセンス

Q. 製品インスタンス登録トークンが期限切れになることはありますか。

A. 特定の有効期間内に製品を登録するために使用されないと、トークンは期限切れになります。Cisco Smart Software Manager でトークンを作成するときに、トークンが有効な日数を設定します。トークンを使用して Firepower Management Center を登録する前にトークンが期限切れになった場合は、新しいトークンを作成する必要があります。

トークンを使用して Firepower Management Center を登録した後は、トークン有効期限は関係がなくなります。トークンの有効期限が経過しても、トークンを使用して登録した Firepower Management Center に影響はありません。

トークンの有効期限の日付は、サブスクリプションの有効期限には影響しません。

詳細については、『*Cisco Smart Software Manager User Guide*』を参照してください。

Q. スマート ライセンス/サービス サブスクリプションが期限切れになっているかどうかや、期限切れが近づいていることを確認するにはどうすればよいですか。

A. サービス サブスクリプションがいつ期限切れになるか（またはいつ期限切れになったか）を判断するには、Cisco Smart Software Manager でエンタイトルメントを確認します。

Firepower Management Center では、**[System]** > **[Licenses]** > **[Smart Licenses]** を選択することで、機能ライセンスのサービス サブスクリプションが現在履行されているかどうかを判断できます。このページでは、製品登録トークンを使用してこの Firepower Management Center に関連付けられているスマート ライセンスのエンタイトルメントが表にまとめられています。[ライセンス ステータス（License Status）] フィールドに基づいて、ライセンスのサービス サブスクリプションが現在履行されているかどうかを判断できます。

Firepower Device Manager で、[スマートライセンス（Smart License）] ページを使用して、システムの現在のライセンス ステータスを表示します。[デバイス（Device）] をクリックしてから、スマート ライセンス サマリーの [設定の表示（View Configuration）] をクリックします。

さらに、Cisco Smart Software Manager はライセンスが期限切れとなる 3 ヵ月前に通知を送信します。

Q. スマート ライセンス/サブスクリプションが期限切れになるとどうなりますか。

A. 購入したサービス サブスクリプションの期限が切れた場合、Firepower Management Center、およびご自分のスマート アカウントに、アカウントが不適合であることが表示されます。Cisco はサブスクリプションの更新が必要なことを通知します。サブスクリプションの更新を参照してください。他の影響はありません。

特定のライセンスの予約

Q. 特定のライセンスの予約の期限が切れた場合はどうなりますか。

A. SLR ライセンスは期間ベースです。

必要なライセンスが使用できないか、または期限が切れている場合、次のアクションは制限されています。

- デバイス登録に使用
- ポリシーの展開

従来のライセンス

Q. クラシック ライセンス/サービス サブスクリプションが期限切れになっているかどうかや、期限切れが近づいていることを確認するにはどうすればよいですか。

A. Firepower Management Center で、**[System]** > **[Licenses]** > **[Classic Licenses]** を選択します。

このページでは、この Firepower Management Center に追加したクラシック ライセンスが表にまとめられています。

[ステータス（Status）] フィールドに基づいて、ライセンスのサービス サブスクリプションが現在履行されているかどうかを判断できます。

[有効期限（Expires）] フィールドの日付により、サービス サブスクリプションがいつ期限切れになるか（またはいつ期限切れになったか）を判断できます。

この情報は、シスコ製品ライセンス登録ポータルでライセンス情報を確認することで得ることもできます。

Q. 「IPSにはIPSの期間サブスクリプションも必要です（IPS Term Subscription is still required for IPS）」とは、どのような意味ですか。

A. このメッセージは、保護および制御の機能には、（期限切れにならない）使用権ライセンスだけでなく、定期的に更新する必要がある 1 つ以上の関連付けられたサービス サブスクリプションも必要であることを伝えているだけです。使用するサービス サブスクリプションが現在のもので、すぐに期限切れにならない場合は、何もする必要はありません。サービス サブスクリプションのステータスを判断するには、クラシック ライセンス/サービス サブスクリプションが期限切れになっているかどうかや、期限切れが近づいていることを確認するにはどうすればよいですか。 （? ページ）を参照してください。

Q. クラシック ライセンス/サブスクリプションが期限切れになるとどうなりますか。

A. クラシック ライセンスをサポートするサービス サブスクリプションの期限が切れると、シスコによってサブスクリプションの更新が必要であることが通知されます。「サブスクリプションの更新」を参照してください。

機能のタイプによっては、関連機能を使用できなくなることがあります。

表 *6:* クラシック ライセンス/サブスクリプションの期限切れによる影響

従来のライセンス	利用可能なサポート サブスクリプション	期限切れによる影響
Control	TA、TAC、TAM、TAMC	既存の FirePOWER の機能を引き続き使用できますが、アプリケーション署名の更新を含む、VDB 更新はダウンロードできません。
Protection	TA、TAC、TAM、TAMC	侵入インスペクションを引き続き実行できますが、侵入ルールの更新をダウンロードすることはできません。

従来のライセンス	利用可能なサポート サブスクリプション	期限切れによる影響
URL フィルタリング	URL、TAC、TAMC	• URL 条件によるアクセス コントロール ルールが、URL のフィルタリングをただちに停止します。 • URL カテゴリとレピュテーションに基づいてトラフィックをフィルタリングするその他のポリシー（SSL ポリシーなど）が、ただちにその処理を停止します。 • Firepower Management Center は、URL データの更新をダウンロードできなくなります。 • URL カテゴリとレピュテーションのフィルタリングを実行する既存のポリシーを再展開することはできません。

従来のライセンス	利用可能なサポート サブスクリプション	期限切れによる影響
Malware	AMP、TAM、TAMC	• 非常に短い時間の間、システムは既存のキャッシュされたファイル性質を使用できます。この時間枠の経過後、システムは `Unavailable` という性質をこれらのファイルに割り当てます。 • システムは AMP クラウドへの問い合わせを停止し、AMP クラウドから送信されたレトロスペクティブイベントの認証を停止します。 • 既存のアクセス コントロール ポリシーに AMP for Firepower 構成が含まれている場合は、それらのポリシーを再展開することができません。

サブスクリプションの更新

Q. 期限切れ間近のクラシック ライセンスを更新する方法を教えてください。

A. 期限切れ間近のクラシック ライセンスを更新するには、新しい PAK キーを購入し、新しいサブスクリプションを実装する場合と同じプロセスを実行するだけです。

Q. Firepower Management Center から FirePOWER サービス サブスクリプションを更新できますか。

A. いいえ。Firepowerサービス サブスクリプション（従来またはスマート）を更新するには、Cisco Commerce Workspace または Cisco Service Contract Center を使用して、新しいサブスクリプションを購入してください。

このガイドのその他のライセンス情報

対象	参照先
スマート ライセンス認証局との FMC 通信用のインターフェイスに関する情報	管理インターフェイスについて およびサブトピック
ライセンスに関するファイアウォールの要件	インターネット アクセス要件
このドキュメントの各手順の最初にある表内のライセンス情報の説明。	ドキュメンテーションのライセンス ステートメント
バックアップからの復元時のライセンスに関する重要な考慮事項	バックアップからの復元：FMC および 7000/8000 シリーズ

対象	参照先
ルールとポリシーの適用時のライセンスの効果とそれらのトリガー方法。	ポリシーとルールに関する情報等： • アクセス コントロール ルールの管理 • アクセス コントロール ルールのコンポーネント、状態に関する情報 • TLS/SSL ルールのガイドラインと制限事項 • TLS/SSL ルールのコンポーネント • QoS ポリシーによるレートの制限
展開とライセンスに関連する展開とポリシーまたはルールの管理エラー	このガイド全体のポリシーとルールに関する情報等： • ルールとその他のポリシーの警告 • QoS ポリシーによるレートの制限
SSL のライセンス要件	Firepower Threat Defense に関する SSL 設定 での前提条件
SSL プリプロセッサ機能のライセンス要件	SSL プリプロセッサ
AMP for Endpoints 統合のライセンス	マルウェア防御の比較：Firepower と AMP for Endpoints
クライアントまたはサーバ サービスでのライセンスとストリーム リアセンブル	TCP ストリームのプリプロセス オプション
ライセンスと Cisco Threat Intelligence Director（TID）	プラットフォーム、要素、およびライセンスに関する要件
接続イベントへのライセンスの影響	接続イベント フィールドの入力の要件
ライセンスとその他のダッシュボード ウィジェットに関する情報	ユーザ ロール別のダッシュボード ウィジェットの可用性 [カスタム分析（Custom Analysis）] ウィジェット
ライセンスのヘルス モニタに関する情報	スマート ライセンス モニタとクラッシク ライセンスモニタに関する情報 ヘルス モジュール

Firepower ライセンスに関するその他の情報

ライセンスに関するよくある質問の解決に役立つその他の情報については、次のドキュメントを参照してください。

- 次の『*Frequently Asked Questions (FAQ) about Firepower Licensing*』のドキュメント
  https://www.cisco.com/c/en/us/td/docs/security/firepower/licensing/faq/firepower-licence-FAQ.html
- 次の『*Cisco Firepower System Feature Licenses* 』のドキュメント
  https://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-licenseroadmap.html

Cisco Success Network

Cisco Success Network はユーザ対応のクラウド サービスです。Cisco Success Network を有効にすると、Firepower Management Center と Cisco Cloud 間にセキュアな接続が確立され、使用状況に関する情報と統計情報がストリーミングされます。テレメトリをストリーミングすることによって、Firepower システムからの対象のデータを選択してそれを構造化形式でリモートの管理ステーションに送信するメカニズムが提供されるため、次のメリットが得られます。

- ネットワーク内の製品の有効性を向上させるために、利用可能な未使用の機能について通知します。
- 製品に利用可能な、追加のテクニカル サポート サービスとモニタリングについて通知します。
- シスコ製品の改善に役立ちます。

Firepower Management Center は常にセキュアな接続を確立および維持し、Cisco Success Network に登録できるようにします。Cisco Success Network を無効にすることで、いつでもこの接続をオフにできます。これにより、デバイスが Cisco Success Network クラウドから接続解除されます。

Cisco Success Network の有効化

Cisco Smart Software Manager に Firepower Management Center を登録するときは、Cisco Success Network を有効にします。スマート ライセンスの登録 （21 ページ）を参照してください。

[ライセンス（Licenses）] > **[スマートライセンス（Smart Licenses）]** ページで、現在の Cisco Success Network の登録ステータスを表示できます。また、登録ステータスを変更することもできます。Cisco Success Network の登録の変更 （84 ページ）を参照してください。

（注） Firepower Management Center に有効な Smart Software Satellite Server 設定がある場合、Cisco Success Network 機能は無効になるか、または特定のライセンスの予約を使用します。

Cisco Success Network テレメトリ データ

Cisco Success Network では、登録済みの Firepower Management Center はリアルタイムの設定と動作状態に関する情報を Cisco Success Network Cloud に継続的にストリーミングすることができます。収集およびモニタ対象のデータには、次の情報が含まれます。

- [登録済みデバイス情報（Enrolled device information）]：これには、Firepower Management Center のデバイス名、モデル、シリアル番号、UUID、システム稼働時間、およびスマート ライセンス情報が含まれます。登録済みデバイス データ （71 ページ）を参照してください。
- [ソフトウェア情報（Software information）]：これには、バージョン番号、ルールの更新バージョン、地理的位置情報データベースのバージョン、脆弱性データベース（VDB）のバージョン情報など、登録済みの Firepower Management Center に関するソフトウェア情報が含まれます。ソフトウェア バージョン データ （72 ページ）を参照してください。
- [管理対象デバイス情報（Managed device information）]：これには、デバイス名、デバイスのモデル、シリアル番号、ソフトウェアのバージョン、およびデバイスごとに使用されているライセンスなど、登録済みの Firepower Management Center に関連付けられているすべての管理対象デバイスに関する情報が含まれます。管理対象デバイス データ （73 ページ）を参照してください。
- [展開情報（Deployment information）]: これには、ポリシーの展開に関する情報が含まれます。展開を設定した後、およびその設定を変更したときは、影響を受けるデバイスにその変更を展開する必要があります。導入情報 （74 ページ）を参照してください。
- [機能の使用状況（Feature usage）]：これには、機能に固有のポリシーおよびライセンスに関する情報が含まれます。
  - [URL フィルタリング（URL filtering）]：これには、デバイスに対して設定され展開されている URL フィルタリング ライセンスの数と、URL フィルタリング機能を使用するポリシーを展開しているデバイスの数が含まれます。
  - [侵入防御（Intrusion prevention）]：これには、侵入防御を設定されている管理対象デバイスの数と、Threat Intelligence Director（TID）に対してデバイスが有効になっているかどうかが含まれます。
  - [マルウェアの検出（Malware detection）]：これには、デバイスに対して設定および展開されているマルウェア ライセンスの数と、マルウェア検出機能を使用するポリシーを展開しているデバイスの数が含まれます

登録済みデバイス データ

Cisco Success Network で Firepower Management Center を登録したら、登録済みの Firepower Management Center のデバイスに関するテレメトリ データがシスコ クラウドにストリーミングされることを選択します。次の表に、登録済みのデバイスに関して収集し、監視しているデータを示します。これには、侵入ポリシー（システムが提供するポリシーとカスタム ポリシーの

両方）および登録済みの Firepower Management Center のマルウェア検出に関する機能に固有の情報が含まれます。

表 *7:* 登録済みデバイスのテレメトリ データ

データ ポイント	値の例
デバイス名	Management Center East
デバイス UUID	24fd0ccf-1464- 491f-a503- d241317bb327
HA ピア UUID	24fe0ccd-1564- 491h-b802- d321317cc827
デバイスモデル	Cisco Firepower Management Center 4000 Cisco Firepower Management Center for VMWare
シリアル番号	9AMDESQP6UN
システム稼動時間	99700000
製品 ID	FMC4000-K9 FS-VMW-SW-K9
スマートライセンス PIID	24fd0ccf-1464- 491f-a503- d241317bb327
仮想アカウント識別子	CiscoSVStemp

ソフトウェア バージョン データ

Cisco Success Network は、ソフトウェアのバージョン、ルールの更新バージョン、地理的位置情報データベースのバージョン、脆弱性データベースのバージョン情報など、登録済みの Firepower Management Center デバイスに関連するソフトウェアの情報を収集します。次の表に、登録済みのデバイスに関して収集し、監視しているソフトウェア情報を示します。

表 *8:* ソフトウェア バージョンのテレメトリ データ

データ ポイント	値の例
Firepower Management Center のソフトウェア バージョン	{ type: "SOFTWARE", version: "6.2.3-10517" }
ルールの更新バージョン	{ type: "SNORT_RULES_DB", version: "2016-11-29-001-vrt", lastUpdated: 1468606837000 }
脆弱性データベース（VDB）のバージョン	{ type: "VULNERABILITY_DB", version: "271", lastUpdated: 1468606837000 }
地理的位置情報データベースのバージョン	{ type: "GEOLOCATION_DB", version: "850" }

管理対象デバイス データ

Cisco Success Network は、登録済みの Firepower Management Center に関連付けられているすべての管理対象デバイスに関する情報を収集します。次の表に、管理対象デバイスに関して収集し、監視している情報を示します。これには、管理対象デバイスの URL フィルタリング、侵略防御、およびマルウェア検出など、機能に固有のポリシーおよびライセンス情報が含まれます。

表 *9*: 管理対象デバイスのテレメトリ データ

データ ポイント	値の例
管理対象デバイス名	firepower
管理対象デバイスのバージョン	6.2.3-10616
管理対象デバイス マネージャ	FMC
管理対象デバイス モデル	Cisco Firepower 2130 NGFW アプライアンス Cisco Firepower Threat Defense VMware
管理対象デバイスのシリアル番号	9AMDESQP6UN
管理対象デバイスの PID	FPR2130-NGFW-K9 NGFWv
デバイスにURLフィルタリング ライセンスを使用しているか	True
URLデバイスごとにURLフィルタリングを使用した AC ルール	10
URL フィルタリングライセンスを使用する URL フィルタリングでの AC ルールの数	3
脅威ライセンスを使用するURLフィルタリングでの AC ルールの数	3
デバイスに脅威ライセンスを使用しているか	True
AC ポリシーに侵略ルールを追加しているか	True
侵略ポリシーを使用する AC ルールの数	10
デバイスにマルウェア ライセンスを使用しているか	True
マルウェア ポリシーを使用する AC ルールの数	10

データ ポイント	値の例
マルウェアライセンスを使用するマルウェアポリシーでの AC ルールの数	5
デバイスに Threat Intelligence Director（TID）を使用しているか	True

導入情報

展開を設定した後、およびその設定を変更したときは、影響を受けるデバイスにその変更を展開する必要があります。次の表に、影響を受けるデバイスの数と成功か失敗かの情報を含む展開のステータスなど、設定の展開に関して収集し、モニタするデータを示します。

表 *10* : 導入情報

データ ポイント	値の例
ジョブ ID	8589936079
展開用に選択したデバイスの数	3
展開に失敗したデバイスの数	1
展開に成功したデバイスの数	2
終了時間	1523993913001
Start Time	1523993840445
Status	SUCCEEDED
ターゲットデバイスの UUID	4f14f644-41e0 -11e8-9354- cf32315d7095
展開したポリシータイプ	NetworkDiscovery NGFWPolicy DeviceConfiguration
現在の実行で収集した最後の展開ジョブの ID	8589936079
コンテナタイプ（スタンドアロンまたは HA ペア）	STANDALONE HAPAIR
コンテナの UUID	5e006633-30fe-11e9-8a70-cd88086eeac0
デバイスモデル	Cisco Firepower Threat Defense for VMWare
デバイスバージョン	6.4.0
ポリシーバンドルのサイズ	3588153

TLS/SSL インスペクション イベント データ

Firepower システムは、デフォルトではセキュア ソケット レイヤ（SSL）プロトコルまたはその後継である Transport Layer Security（TLS）プロトコルで暗号化されたトラフィックを検査できません。TLS/SSL インスペクションを使用すると、暗号化トラフィックをインスペクションを実行せずにブロックしたり、暗号化または復号されたトラフィックをアクセス コントロールを使用して検査したりできます。次の各表では、暗号化されたトラフィックについて Cisco Success Network と共有する統計情報について説明します。

ハンドシェイク プロセス

システムで TCP 接続での TLS/SSL ハンドシェイクが検出された場合、その検出されたトラフィックを復号できるかどうかが判定されます。システムは、暗号化されたセッションを処理する際にトラフィックに関する詳細をログに記録します。

表 *11 : TLS/SSL* インスペクション : ハンドシェイクのテレメトリ データ

データ ポイント	値の例
システムは、トラフィックが**復号できず**次の状態となった場合、適用されたアクションを報告します。 • ブロック • TCP リセットによるブロック • 復号されない	0 以上の整数値
システムは、トラフィックが次の方法で**復号できた**場合、適用されたアクションを報告します。 • 既知の秘密キーを使用 • 置換キーのみを使用 • 自己署名証明書への再署名 • サーバ証明書の再署名	0 以上の整数値

キャッシュ データ

TLS/SSL ハンドシェイクが完了すると、管理対象デバイスは暗号化セッション データをキャッシュに保存し、それによりフル ハンドシェイクを必要とせずにセッションを再開できます。管理対象デバイスもサーバ証明書データをキャッシュに保存し、それにより後続のセッションでのより速いハンドシェイクの処理が可能になります。

表 *12 : TLS/SSL* インスペクション：キャッシュのテレメトリ データ

データ ポイント	値の例
システムは暗号化されたセッション データおよびサーバ証明書データをキャッシュし、**キャッシュ**について SSL 接続ごとにレポートします。具体的な内容は次のとおりです。 • SSL セッション情報がキャッシュされた回数 • SSL 証明書検証キャッシュがヒットした回数 • SSL 証明書検証キャッシュのルックアップが失敗した回数 • SSL 元証明書キャッシュがヒットした回数 • SSL 元証明書キャッシュのルックアップが失敗した回数 • SSL 再署名証明書キャッシュがヒットした回数 • SSL再署名証明書キャッシュのルックアップが失敗した回数	0 以上の整数値

証明書のステータス

システムは暗号化されたトラフィックを評価し、暗号化サーバの証明書のステータスを報告します。

表 *13 : TLS/SSL* インスペクション：証明書ステータスのテレメトリ データ

データ ポイント	値の例
システムは、暗号化サーバの**証明書のステータス**に基づいて暗号化されたトラフィックを評価し、SSL 証明書が次の状態である接続の数を報告します。 • 有効 • 有効期限切れ • 発行元が無効 • 署名が無効 • チェックされていない • まだ有効でない • 取り消されている • 自己署名されている • 不明	0 以上の整数値

失敗の理由

システムは暗号化されたトラフィックを評価し、システムがトラフィックの復号化に失敗している場合は失敗の理由を報告します。

表 *14 : TLS/SSL* インスペクション：失敗のテレメトリデータ

データ ポイント	値の例
システムは暗号化されたトラフィックを評価し、システムが次の理由のためにトラフィックの復号化に失敗している場合は**失敗の理由**を報告します。 • 復号エラー • ハンドシェイク中のポリシー判定の実行 • ハンドシェイク前のポリシー判定の実行 • 圧縮がネゴシエートされている • キャッシュされていないセッション • インターフェイスがパッシブ モードである • 不明な暗号スイート • サポートされていない暗号スイート	0 以上の整数値

バージョン

システムは暗号化されたトラフィックを評価し、ネゴシエートされた TLS/SSL バージョンを接続ごとに報告します。

表 *15 : TLS/SSL* インスペクション：バージョンのテレメトリ データ

データ ポイント	値の例
システムは暗号化されたトラフィックを評価し、次のようなネゴシエートされた**バージョン**を SSL 接続ごとに報告します。 • SSLv2 のネゴシエート • SSLv3 のネゴシエート • 不明なバージョンのネゴシエート • TLSv1.0 のネゴシエート • TLSv1.1 のネゴシエート • TLSv1.2 のネゴシエート • TLSv1.3 のネゴシエート	0 以上の整数値

Snort 再起動データ

管理対象デバイス上の Snort プロセスと呼ばれるトラフィック インスペクション エンジンが再起動すると、プロセスが再開されるまでインスペクションが中断されます。ユーザ定義のアプリケーションの作成/削除を行うか、システムまたはカスタム アプリケーション ディテクタを有効化/無効化すると、展開プロセスを経由することなく、ただちに Snort プロセスが再起動します。Snort プロセスの再起動が続行されていることが警告され、キャンセルが可能になります。再起動は、現在のドメインまたはそのいずれかの子ドメイン内の任意の管理対象デバイスで発生します。

表 *16 : Snort* 再起動のテレメトリ データ

データ ポイント	値の例
カスタムアプリケーションディテクタを有効または無効にした場合の Snort 再起動の数	0 以上の整数値
カスタムアプリケーションディテクタを作成または変更した場合の Snort 再起動の数	0 以上の整数値

Cisco Security Packet Analyzer データ

組織が Cisco Security Packet Analyzer（Firepower システムとは別個の製品）を展開している場合、Cisco Security Packet Analyzer を使用して Firepower システムが検出するインシデントや不審なイベントのコンテキスト情報を、フル パケット キャプチャの形式で収集できます。

Cisco Security Packet Analyzer と Firepower Management Center は互いに独立して展開され、Cisco Security Packet Analyzer の展開は Firepower システムを認識しません。キャプチャされたデータはパケット アナライザと管理センター間を移動しません。

表 *17 : CSPA* のテレメトリ データ

データ ポイント	値の例
FMC に登録されている Cisco Security Packet Analyzer インスタンスの合計数	0 以上の整数値
FMC 上の Cisco Security Packet Analyzer クエリの数	0 以上の整数値
FMC 上の Cisco Security Packet Analyzer クエリグループの数	0 以上の整数値

コンテキスト クロス起動データ

コンテキスト クロス起動機能を使用すると、Firepower Management Center の外部の Web ベースのリソースにおける潜在的な脅威に関するさらなる情報をすばやく検索できます。FMC のイベント ビューアまたはダッシュボードのイベントから、外部リソースの関連情報を直接ク

リックできます。これにより、そのIPアドレス、ポート、プロトコル、ドメイン、またはSHA 256 ハッシュに基づいて、特定のイベントに関連するコンテキストを迅速に収集できます。

表 *18:* コンテキスト クロス起動のテレメトリ データ

データ ポイント	値の例
FMC 上に設定されているコンテキスト クロス起動リソースの数	0 以上の整数値
FMC 上で有効になっているコンテキスト クロス起動リソースの数	0 以上の整数値
ドメイン変数を含むコンテキスト クロス起動インスタンスの数	0 以上の整数値
IP 変数を含むコンテキスト クロス起動インスタンスの数	0 以上の整数値
SHA 256 変数を含むコンテキスト クロス起動インスタンスの数	0 以上の整数値

テレメトリ ファイルの例

次に、Firepower Management Center とその管理対象デバイスに関してポリシーと展開情報をストリーミングするための Cisco Success Network テレメトリ ファイルの例を示します。

```
{
    "recordType" : "CST_FMC",
    "recordVersion" : "6.4.0",
    "recordedAt" : 1550467152050,
    "fmc" : {
      "deviceInfo" : {
        "deviceModel" : "Cisco Firepower Management Center for VMWare",
        "deviceName" : "firepower",
        "deviceUuid" : "18842483-30cf-11e9-a090-503c97636361",
        "serialNumber" : "None",
       "smartLicenseProductInstanceIdentifier" : "cbs246a5-6d51-4eb7-9gc2-118b177dc4de",

        "smartLicenseVirtualAccountName" : "FTD-ENG-BLR",
        "systemUptime" : 262007000,
        "udiProductIdentifier" : "FS-VMW-SW-K9"
      },
      "versions" : {
        "items" : [ {
          "lastUpdated" : 0,
          "type" : "SOFTWARE",
          "version" : "6.4.0-1335"
        }, {
          "lastUpdated" : 0,
          "type" : "SNORT_RULES_DB",
          "version" : "2018-10-10-001-vrt"
        }, {
          "lastUpdated" : 1550200610000,
          "type" : "VULNERABILITY_DB",
```

```
      "version" : "309"
    }, {
      "lastUpdated" : 0,
      "type" : "GEOLOCATION_DB",
      "version" : "None"
    } ]
  }
},
"managedDevices" : {
  "items" : [ {
    "deviceInfo" : {
      "deviceManager" : "FMC",
      "deviceModel" : "Cisco Firepower Threat Defense for VMWare",
      "deviceName" : "10.10.17.220",
      "deviceVersion" : "6.4.0-1335",
      "serialNumber" : "9AUVT5GTRPA"
    },
    "malware" : {
      "malwareLicenseUsed" : false,
      "numberOfACRulesNeedMalwareLicense" : 10,
      "numberOfACRulesWithMalware" : 20
    },
    "sslUsage" : {
      "isSSLEnabled" : false
    },
    "threat" : {
      "acPolicyHasIntrusion" : true,
      "acRulesWithIntrusion" : 20,
      "isTIDEnabled" : true,
      "threatLicenseUsed" : true
    },
    "urlFiltering" : {
      "acRulesWithURLFiltering" : 10,
      "numberOfACRulesNeedThreatLicense" : 3,
      "numberOfACRulesNeedURLLicense" : 3,
      "urlFilteringLicenseUsed" : true
    }
  }, {
    "deviceInfo" : {
      "deviceManager" : "FMC",
      "deviceModel" : "Cisco Firepower Threat Defense for VMWare",
      "deviceName" : "10.10.17.221",
      "deviceVersion" : "6.4.0-1335",
      "serialNumber" : "9A0NMB3VAL7"
    },
    "malware" : {
      "malwareLicenseUsed" : false,
      "numberOfACRulesNeedMalwareLicense" : 0,
      "numberOfACRulesWithMalware" : 0
    },
    "sslUsage" : {
      "isSSLEnabled" : false
    },
    "threat" : {
      "acPolicyHasIntrusion" : false,
      "acRulesWithIntrusion" : 0,
      "isTIDEnabled" : false,
      "threatLicenseUsed" : false
    },
    "urlFiltering" : {
      "acRulesWithURLFiltering" : 0,
      "urlFilteringLicenseUsed" : false
    }
  }, {
```

```
    "deviceInfo" : {
      "deviceManager" : "FMC",
      "deviceModel" : "Cisco Firepower Threat Defense for VMWare",
      "deviceName" : "10.10.17.222",
      "deviceVersion" : "6.4.0-1335",
      "serialNumber" : "9ATSKTCFNXA"
    },
    "malware" : {
      "malwareLicenseUsed" : true,
      "numberOfACRulesNeedMalwareLicense" : 0,
      "numberOfACRulesWithMalware" : 0
    },
    "sslUsage" : {
      "isSSLEnabled" : false
    },
    "threat" : {
      "acPolicyHasIntrusion" : false,
      "acRulesWithIntrusion" : 0,
      "isTIDEnabled" : false,
      "threatLicenseUsed" : true
    },
    "urlFiltering" : {
      "acRulesWithURLFiltering" : 0,
      "urlFilteringLicenseUsed" : true
    }
  }, {
    "deviceInfo" : {
      "deviceManager" : "FMC",
      "deviceModel" : "Cisco Firepower Threat Defense for VMWare",
      "deviceName" : "10.10.17.223",
      "deviceVersion" : "6.4.0-1335",
      "serialNumber" : "9AP4B2J9BC1"
    },
    "malware" : {
      "malwareLicenseUsed" : true,
      "numberOfACRulesNeedMalwareLicense" : 0,
      "numberOfACRulesWithMalware" : 0
    },
    "sslUsage" : {
      "isSSLEnabled" : false
    },
    "threat" : {
      "acPolicyHasIntrusion" : false,
      "acRulesWithIntrusion" : 0,
      "isTIDEnabled" : false,
      "threatLicenseUsed" : true
    },
    "urlFiltering" : {
      "acRulesWithURLFiltering" : 0,
      "urlFilteringLicenseUsed" : true
    }
  } ]
},
"deploymentData" : {
  "deployJobInfoList" : [ {
    "jobDeviceList" : [ {
      "containerType" : "STANDALONE",
      "deployEndTime" : "1550466953538",
      "deployStartTime" : "1550466890057",
      "deployStatus" : "SUCCEEDED",
      "deviceModel" : "Cisco Firepower Threat Defense for VMWare",
      "deviceOSVersion" : "6.4.0",
      "deviceUuid" : "8918db92-30de-11e9-a576-92cc6a3b249d",
      "pgTypes" : "[PG.FIREWALL.NGFWAccessControlPolicy]",
```

```
      "policyBundleSize" : 3588153
    }, {
      "containerType" : "STANDALONE",
      "deployEndTime" : "1550466953634",
      "deployStartTime" : "1550466890057",
      "deployStatus" : "SUCCEEDED",
      "deviceModel" : "Cisco Firepower Threat Defense for VMWare",
      "deviceOSVersion" : "6.4.0",
      "deviceUuid" : "87cf54e6-30de-11e9-8fdb-ce9d0fc91a42",
      "pgTypes" : "[PG.FIREWALL.NGFWAccessControlPolicy]",
      "policyBundleSize" : 3588172
    }, {
      "containerID" : "5f009744-30fe-11e9-8a70-cd88086eeac0",
      "containerType" : "HAPAIR",
      "deployEndTime" : "1550467052791",
      "deployStartTime" : "1550466890057",
      "deployStatus" : "SUCCEEDED",
      "deviceModel" : "Cisco Firepower Threat Defense for VMWare",
      "deviceOSVersion" : "6.4.0",
      "deviceUuid" : "c8df3b96-30ce-11e9-b5e5-d6beeb6498f5",
      "pgTypes" : "[PG.FIREWALL.NGFWAccessControlPolicy]",
      "policyBundleSize" : 3588212
    } ],
    "jobId" : "12884903350",
    "numberOfDevices" : 3,
    "numberOfFailedDevices" : 0,
    "numberOfSuccessDevices" : 3
  } ],
  "lastJobId" : "12884903350"
},
"cspa" : {
  "cspaCount" : 0,
  "queryCount" : 0,
  "queryGroupCount" : 0
},
"analysis" : {
  "crossLaunchInfo" : {
    "count" : 28,
    "enabledCount" : 28,
    "iocInfo" : [ {
      "domain" : 10,
      "ip" : 9,
      "sha256" : 9
    } ]
  }
},
"SSLStats" : {
  "action" : {
    "block" : 10,
    "block_with_reset" : 4,
    "decrypt_resign_self_signed" : 0,
    "decrypt_resign_self_signed_replace_key_only" : 0,
    "decrypt_resign_signed_cert" : 227,
    "decrypt_with_known_key" : 0,
    "do_not_decrypt" : 9094
  },
  "cache_status" : {
    "cached_session" : 18693,
    "cert_validation_cache_hit" : 0,
    "cert_validation_cache_miss" : 10883,
    "orig_cert_cache_hit" : 15720,
    "orig_cert_cache_miss" : 0,
    "resigned_cert_cache_hit" : 14,
    "resigned_cert_cache_miss" : 4,
```

```
        "session_cache_hit" : 4398,
        "session_cache_miss" : 1922
      },
      "cert_status" : {
        "cert_expired" : 155,
        "cert_invalid_issuer" : 866,
        "cert_invalid_signature" : 0,
        "cert_not_checked" : 1594,
        "cert_not_yet_valid" : 0,
        "cert_revoked" : 0,
        "cert_self_signed" : 362,
        "cert_unknown" : 0,
        "cert_valid" : 9659
      },
      "failure_reason" : {
        "decryption_error" : 0,
        "handshake_error_before_verdict" : 254,
        "handshake_error_during_verdict" : 17,
        "ssl_compression" : 0,
        "uncached_session" : 984,
        "undecryptable_in_passive_mode" : 0,
        "unknown_cipher_suite" : 56,
        "unsupported_cipher_suite" : 125
      },
      "version" : {
        "ssl_v20" : 0,
        "ssl_v30" : 0,
        "ssl_version_unknown" : 10,
        "tls_v10" : 32,
        "tls_v11" : 8,
        "tls_v12" : 11355,
        "tls_v13" : 922
      }
    },
    "snortRestart" : {
      "appDetectorSnortRestartCnt" : 3,
      "appSnortRestartCnt" : 1
    }
}
```


Cisco Success Network の登録の変更

Cisco Smart Software Manager に Firepower Management Center を登録するときは、Cisco Success Network を有効にします。その後、次の手順を使用して、登録ステータスを表示または変更します。

（注） Cisco Success Network は評価モードでは機能しません。

ステップ 1 [システム（System）] をクリックしてから、**[ライセンス（Licenses）]** > **[スマートライセンス（Smart Licenses）]** をクリックします。

ステップ 2 スマート ライセンスのステータスの下で、Cisco Success Network の横にある、Cisco Success Network 機能の [有効/無効（Enabled/Disabled）] コントロールをクリックして、必要に応じて設定を変更します。

ステップ 3 シスコから提供された情報を読み、[Cisco Success Networkの有効化（Enable Cisco Success Network）] を行うかどうかを選択して、[変更内容を適用（Apply Changes）] をクリックします。

次のタスク

（オプション）（オプション）Web 分析トラッキングのオプトアウトを参照してください。

エンドユーザ ライセンス契約書

本製品の使用について規定するシスコ エンドユーザ ライセンス契約書（EULA）および適用される補足契約書（SEULA）は、http://www.cisco.com/go/softwareterms から入手できます。

ライセンスの履歴

機能	バージョン	詳細
Firepower 4100/9300 の FTD に対する複数インスタンス機能のライセンス	6.3	Firepower 4100/9300 に複数の FTD コンテナインスタンスを展開できるようになりました。セキュリティ モジュール/エンジンの機能ごとに必要なライセンスは 1 つのみです。基本ライセンスは、各インスタンスに自動的に割り当てられます。 新規/変更された画面：**[システム（System）] > [ライセンス（Licenses）] > [スマートライセンス（Smart Licenses）]** サポート対象プラットフォーム：Firepower 4100/9300 の FTD

機能	バージョン	詳細
エアギャップ展開に対する特定のライセンスの予約	6.3	展開でインターネットに接続してシスコのライセンス認証局と通信できない顧客は特定のライセンスの予約を使用できます。詳細については、特定のライセンスの予約の概要 （27 ページ）を参照してください。 新規/変更された画面：**[システム（System）] > [ライセンス（Licenses）] > [特定のライセンス（Specific Licenses）]**（このオプションはデフォルトでは使用できません。） サポートされるプラットフォーム：FMC、FTD
制限付きの顧客の輸出規制対象機能	6.3	スマートアカウントで制限付き機能を使用する資格を持たない特定の顧客は、期間ベースのライセンスを承認を受けて購入することができます。詳細については、輸出規制機能の有効化（グローバル権限のないアカウントの場合） （23 ページ） を参照してください。 サポートされるプラットフォーム：FMC、FTD
Firepower Threat Defense デバイスのスマートライセンスを展開するための拡張手順	6.3	新しいトピックFirepower Threat Defense デバイスのライセンス （4 ページ）で、エンドツーエンドのガイダンスを提供しています。また、このトピックからリンクされているトピックでも、新しいよりよい情報を提供しています。