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 の機能ライセンスについて

組織に対して Firepower システムの最適な展開を実現するために、さまざまな機能についてライセンスを取得することができます。Firepower Management Center では、これらの機能ライセンスを管理してデバイスに割り当てることができます。

（注） Firepower Management Center はデバイスの機能ライセンスを管理しますが、Firepower Management Center を使用するための機能ライセンスは必要ありません。

「使用権」機能ライセンスに加えて、多くの機能にはサービス 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。

ライセンスに関してよく寄せられる質問の回答については、https://www.cisco.com/c/en/us/td/docs/security/firepower/licensing/faq/firepower-licence-FAQ.html で『*Frequently Asked Questions (FAQ) about Firepower Licensing*』ドキュメントを参照してください。

スマート ライセンスとクラシック ライセンス

Firepower 機能ライセンスは、デバイスの種類に応じて次のように異なります。

- スマート ライセンスは Firepower Threat Defense および Firepower Threat Defense Virtual デバイスに使用可能です。
- 従来型ライセンスは 7000 および 8000 シリーズ、ASA FirePOWER、および NGIPSv デバイスに使用可能です。従来のライセンスを使用するデバイスは、クラシック デバイスと呼ばれることもあります。

1 つの Firepower Management Center で従来のライセンスとスマート ライセンスの両方を管理できます。

各プラットフォームでのスマート ライセンスとクラシック ライセンスの比較の詳細については、https://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-licenseroadmap.html で『*Cisco Firepower System Feature Licenses*』を参照してください。

スマート ライセンス、クラシック ライセンス、使用権ライセンス、およびサービス サブスクリプションに関するよくある質問への回答については、https://www.cisco.com/c/en/us/td/docs/security/firepower/licensing/faq/firepower-licence-FAQ.html で『*Frequently Asked Questions (FAQ) about Firepower Licensing*』ドキュメント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

一部の機能ライセンスには、関連するサービス 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場合、期限が切れても、関連する機能を引き続き使用できます。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。

サービス サブスクリプションは、Firepower システムで管理対象デバイスに割り当てるライセンスと、次のように対応しています。

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

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
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。

表 *2:* 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。

Firepower システムのスマート ライセンス

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

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できます。また、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。

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 Management Center 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 Management Center 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 Management Center を登録することはできません。また、登録済み Management Center 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* を参照してください。

ライセンス認証局との定期通信

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 ヵ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、ライセンス認証局のプロキシとしての Smart Software Satellite Server の使用について （5 ページ）を参照してください。

ライセンス認証局のプロキシとしての Smart Software Satellite Server の使用について

ライセンス認証局との定期通信 （4 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。ただし、次の状況のいずれかが発生している場合、ライセンス認証局への接続用プロキシとして、スマート ソフトウェア サテライト サーバを使用することができます。

- Firepower Management Center がオフラインであるか、接続が制限されているか、接続がない場合。
- 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。

Smart Software Satellite Server の展開方法

始める前に

Smart Software Satellite Server の必要性を確認します。ライセンス認証局のプロキシとしての Smart Software Satellite Server の使用について （5 ページ）を参照してください。

手順

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 （6 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

参照先 #unique_187

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	サポートされるドメイン	アクセス
任意（Any）	該当なし	Firepower Threat Defense	グローバルだけ	Admin

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 （5 ページ）を参照してください。
- Smart Software Satellite Server にログインして、Smart Call Home の宛先 URL を取得します。
- http://www.cisco.com/security/pki/certs/clrca.cer に移動し、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。

手順

ステップ 1 **[システム（System）] > [統合（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 [URL] を入力します。

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 （5 ページ）の残りの手順を実行します。

スマート ライセンスの移転

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 Management Center 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 Management Center 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 Management Center に登録できるようになります。登録を解除しないと、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ので、非準拠通知を受け取ります。

Cisco Smart Software Manager から Firepower Management Center の登録解除 （20 ページ） を参照し、次に Cisco Smart Software Management Center オンライン ヘルプで「ライセンスを転送する」を検索します。

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 *3 : 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	時間（Duration）	付与される機能
基本（自動的にすべての Firepower Threat Defense デバイスに付属）	なし（デバイスに付属）	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 （9 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	時間（Duration）	付与される機能
脅威	T	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 詳細の参照先：脅威ライセンス （10 ページ）
マルウェア	• TM（脅威（Threat）＋マルウェア（Malware）） • TMC（脅威（Threat）＋マルウェア（Malware）＋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） AMP Threat Grid 詳細は、Firepower Threat Defenseデバイスのマルウェア ライセンス （9 ページ）を参照してください。
URL フィルタリング	• TC（脅威（Threat）＋URL） • TMC（脅威（Threat）＋マルウェア（Malware）＋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 （11 ページ）を参照してください。
仮想 Firepower Management Center	なし（ソフトウェアに付属）	永久	Firepower Management Center 仮想アプライアンスでの Firepower Threat Defense デバイスの登録 詳細は、Firepower Management Center Virtual ライセンス （9 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	時間（Duration）	付与される機能
輸出管理機能	なし（製品インスタンス登録オプション）	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。輸出管理機能 （12ページ）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 Firepower Threat Defense デバイスを設定する
- Firepower Threat Defense 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

その他のすべての機能には、付加的なオプション ライセンス（脅威、マルウェア、または URL フィルタリング）が必要です。

基本ライセンスは、登録するすべての Firepower Management Center デバイスの Firepower Threat Defense に追加されます。

Firepower Management Center Virtual ライセンス

Firepower Management Center Virtual ライセンスは、機能ライセンスではなく、プラットフォーム ライセンスです。ご購入いただく仮想ライセンスのバージョンによって、Firepower Management Center を介して管理可能なデバイスの数が決まります。たとえば、2 台、10 台、または 25 台のデバイスを管理可能なライセンスをご購入いただけます。各デバイスには権限付与が必要です。

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 AMP 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 ポリシーは、特定のアプリケーション プロトコルを使用して特定のファイルをアップロードまたはダウンロードするユーザを検出できます。ネットワーク向け AMP によって、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、これらの制限されたファイル タイプのセットにマルウェアがないかを検査できます。特定のファイル タイプをダウンロードして AMP 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 AMP 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。

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。ネットワーク向け *AMP*マルウェア ライセンス

が必要な を使用すると、制限されたファイル タイプ セットを、その処置に基づいて検査およびブロックすることができます。

- 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ただちにブラックリストに追加できます。オプションで、セキュリティ インテリジェンス フィルタリングに「モニタのみ」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（TCM）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。

輸出管理機能

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。

Firepower Management Center でエクスポート制御オプションを変更することはできません。このオプションは、Smart Software Manager で Firepower Management Center の製品インスタンス登録トークンを作成するときに設定されます。

この機能を使用するための要件の概要については、強力な暗号化のライセンスについて （12 ページ） を参照してください。

導入にこれらの機能を使用するライセンスがあるかどうかを確認するには、スマート ライセンスのステータス （18 ページ） を参照してください。

強力な暗号化のライセンスについて

強力な暗号化を必要とする機能を有効にする場合、次の手順に従います。

-
- 強力な暗号化を有効にするには、スマートアカウントをエクスポート制御機能に関して承認済みにする必要があります。アカウント担当者に問い合わせて、この認証の手続きをしてください。
- Firepower システムのライセンスを設定する場合、Cisco Smart Software Manager（CSSM）で製品インスタンス登録トークンを生成する時に、エクスポート制御機能を選択する必要があります。この機能を既存の導入に遡及的に追加することはできず、新しいトークンを生成してインストールする必要があります。
- エクスポート制御を含むトークンを Firepower Management Center にインストールして、関連するライセンスを管理対象デバイスに割り当てた後、新しく有効化された機能を使用できるようにするには、各管理対象デバイスをリブートする必要があります。

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

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、次の手順を使用する代わりに、その相手からアカウントにアクセスするために必要な情報を取得します。アカウントにアクセスできることを確認します。

手順

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：

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/#SmartLicensing-Alerts 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 Management Center によって管理されている Firepower Threat Defense デバイスのライセンス方法

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 （15 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。

手順

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 後でこのトークンのエクスポート制御機能を有効にすることはできません。

表示されると想定していたのに、このオプションが表示されていない場合は、この手順をキャンセルし、シスコのアカウント担当者に問い合わせてください。

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 （15 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	サポートされるドメイン	アクセス
任意（Any）	該当なし	Firepower Threat Defense	グローバルだけ	Admin

Cisco Smart Software Manager での Firepower Management Center の登録.

始める前に

- Smart Software Satellite Server 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 （6 ページ）を参照してください。
- 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。詳細については、*Firepower Management Center* コンフィギュレーション ガイド [英語] の付録を参照してください。管理対象デバイスは CSSM に接続する必要はありません。
- 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。
- 各 Firepower Management Center に明確に特定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 インスタ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 （13 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。

手順

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。

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 [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。#unique_187を参照してください。

[スマートライセンス（Smart Licenses）]ページでライセンスを管理対象デバイスに割り当てる

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	サポートされるドメイン	アクセス
任意（Any）	該当なし	Firepower Threat Defense	グローバルだけ	Admin

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 ライセンスを一度に有効にするには、次の手順を使用します。

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 （15 ページ）

手順

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。

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 （17 ページ） の手順に従います。
- 、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。
- 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	サポートされるドメイン	アクセス
任意（Any）	該当なし	Firepower Threat Defense	グローバルだけ	Admin

[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。このページでは、展開におけるライセンスのタイプごとに、そのライセンスを使用している管理対象デバイスの合計数、そのライセンスが準拠されているかどうか、デバイス タイプ、デバイスが配置されているドメインとグループが示されます。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。

[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。
- [デバイス管理（Device Management）] ページ（**[デバイス（Devices）]** > **[デバイス管理（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。

手順

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。

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。

- ：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。
- ：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。

輸出管理機能

Smart Software Manager で Firepower Management Center のエクスポート制御機能を有効にしたかどうかを指定します。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、輸出管理機能 （12 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	サポートされるドメイン	アクセス
任意（Any）	該当なし	Firepower Threat Defense	グローバルだけ	Admin

1 つの Firepower Threat Defense デバイスから別のデバイスにライセンスを移動するか、またはデバイスからライセンスを削除するには、次の手順を使用します。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、スマート ライセンスの移転 （7 ページ）を参照してください。

手順

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。

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）]、または [URL フィルタリング（URL Filtering）] 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 削除アイコン（  ） をクリックします。

ステップ 5 [適用（Apply）] をクリックします。

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	サポートされるドメイン	アクセス
任意（Any）	該当なし	Firepower Threat Defense	グローバルだけ	Admin

Cisco Smart Software Manager から Firepower Management Center の登録を解除すると、バーチャル アカウントから Management Center 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。

手順

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。

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	サポートされるドメイン	アクセス（**Access**）
任意（Any）	該当なし	Firepower Threat Defense	グローバルだけ	Admin

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。

手順

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。

ステップ 2 更新アイコン（）をクリックします。

Firepower システムのクラシック ライセンス

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。

7000 および 8000 シリーズ デバイス、NGIPSv デバイス、および ASA FirePOWER モジュールはクラシック ライセンスを使用します。

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

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、ライセンスはモジュール固有です。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 *4 : 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（Any）	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	none	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 セキュリティ インテリジェンス フィルタリング	none	No
Control	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	No
Control	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	No
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）	プロテクション	Yes
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	Yes

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	Control	Yes

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。ネットワーク向け *AMP*マルウェア ライセンスが必要な を使用すると、制限されたファイル タイプ セットを、その処置に基づいて検査およびブロックすることができます。
- 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ただちにブラックリストに追加できます。オプションで、セキュリティ インテリジェンス フィルタリングに「モニタのみ」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。

制御ライセンスを Firepower Management Center から削除するか、または個別のデバイスで制御を無効にしても、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 AMP 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 ポリシーは、特定のアプリケーション プロトコルを使用して特定のファイルをアップロードまたはダウンロードするユーザを検出できます。ネットワーク向け AMP によって、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、これらの制限されたファイル タイプのセットにマルウェアがないかを検査できます。特定のファイル タイプをダウンロードして AMP 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 AMP 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。

関連トピック

ファイル制御および Cisco AMP の基本

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。

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	サポートされるドメイン	アクセス
該当なし	任意（Any）	従来型	グローバルだけ	Admin

手順

必要に応じて、次のいずれかを実行します。

内容	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。	**[システム（System）] > [ライセンス（Licenses）] > [クラシック ライセンス（Classic Licenses）]**を選択します。
管理対象デバイスそれぞれに適用されたライセンス	**[デバイス（Devices）] > [デバイス管理（Device Management）]**を選択します。
ヘルス モニタのライセンス ステータス	正常性ポリシーで従来のライセンス 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。
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。この説明については、ダッシュボードへのウィジェットの追加 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	サポートされるドメイン	アクセス（Access）
該当なし	任意（Any）	従来型	グローバルだけ	Admin

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。

手順

ステップ 1 **[システム（System）] > [ライセンス（Licenses）] > [クラシック ライセンス（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 （28 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	サポートされるドメイン	アクセス
該当なし	任意（Any）	従来型	グローバルだけ	Admin

（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 （28 ページ） を参照してください。

手順

ステップ 1 **[システム（System）]>[ライセンス（Licenses）]>[クラシック ライセンス（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 （30 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**。

[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	サポートされるドメイン	アクセス
任意（Any）	任意（Any）	任意（Any）	リーフのみ	Admin/Network Admin

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。

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。参照先 #unique_187

- 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 （15 ページ）

手順

ステップ 1 **[デバイス（Devices）] > [デバイス管理（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。

  [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、[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。

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* コンフィギュレーション ガイド』の「Firepower 機能のサービス サブスクリプション」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、**[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。

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、**[システム（System）] > [ライセンス（Licenses）] > [クラシック ライセンス（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 *5:* 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。
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（クラシックまたはスマート）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。