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 （1 ページ）
- Firepower 機能のサービス サブスクリプション （2 ページ）
- Firepower システムのスマート ライセンス （3 ページ）
- Firepower システムのクラシック ライセンス （14 ページ）
- 管理対象デバイスへのライセンスの割り当て （23 ページ）

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。

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。

Firepower 機能のサービス サブスクリプション

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（Threat）
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（Threat に追加するか、Threat なしで使用できます）
AMP	マルウェア（Threat に追加するか、Threat 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）

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
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

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 か月または 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。

必要に応じて、スマート ソフトウェア サテライト サーバをライセンス認証局と通信するように設定できます。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。

Smart Software Satellite Server の設定についての詳細は、*Smart Software Manager Satellite User Guide*を参照してください。

スマート ライセンスのステータス

スマート ライセンスのステータスでは、次のとおり Firepower Management Center でのライセンス使用の概要を説明します。

使用の認証

可能なステータス値は次のとおりです。

- [認証済み（Authorized）]：Firepower Management Center は、アプライアンスのライセンス付与資格を承認するライセンス認証局に正常に連絡して登録されています。
- [コンプライアンス不適合（Out-of-Compliance）]：ライセンス認証局が Firepower Management Center で使用可能なライセンス権限を識別できませんでした。ライセンスされた機能は動作を継続します。ただし、[認証済み（Authorized）] として表示するには、ステータスの追加の権限付与を購入するか、解放するかのいずれかを行う必要があります。
- [認証期限切れ（Authorization Expired）]：Firepower Management Center は、90 日以上ライセンス認証局と通信していません。ライセンスされた機能は動作を継続します。この状態の場合、アプライアンスは認証要求を再試行します。再試行が成功した場合、ステータス

は [コンプライアンス不適合（Out-of-Compliance）] または [認証済み（Authorized）] のどちらかに設定され、新しい認証期間が開始されます。

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。このオプションを有効にすると、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ソフトウェア機能を導入できます。

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。

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。

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
脅威（Threat）	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
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	AMP for Firepower（ネットワークベースの高度なマルウェア防御） AMP Threat Grid
URL フィルタリング（URL Filtering）	• 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
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

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：を参照してください。 スマート ライセンスのステータス （4 ページ）

基本ライセンス

基本ライセンスでは、次のことができます。

- 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
- 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）

Firepower Threat Defense デバイスまたは Firepower Threat Defense Virtual を購入すると、自動的に基本ライセンスが付いてきます。すべての追加ライセンス（Threat、Malware、URL Filtering）はオプションです。

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 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、AMP for Firepower 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 AMP for Firepower 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。AMP for Firepower 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 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。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 AMP for Firepower 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）をブロックできます。マルウェア ライセンスが必要な *AMP for Firepower* 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。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。

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。

Cisco Smart Software Manager での Firepower Management Center 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（Access）
任意（Any）	該当なし	Firepower Threat Defense	グローバルのみ	Admin

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://www.cisco.com/c/en/us/buy/smart-accounts.htmlを参照してください。
- Cisco Smart Software Manager によって提供される製品インスタンス登録トークンを取得します。このトークンは、バーチャル アカウントに固有です。
- 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。

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（Register）] をクリックします。

ステップ 3 製品インスタンス登録トークンがない場合は、[Cisco Smart Software Manager] をクリックして、割り当て済みのバーチャル アカウントからトークンを取得します。

ステップ 4 トークンをコピーして、Firepower Management Center の Web インターフェイス内の [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て、[変更の適用（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。
- ライセンスを Firepower Threat Defense に割り当てます。管理対象デバイスへのライセンスの割り当て （23 ページ）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（Access）
任意（Any）	該当なし	Firepower Threat Defense	グローバルのみ	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 各デバイスのライセンスのステータス、デバイス タイプ、ドメイン、グループを表示するには、目的のライセンス タイプの横にある矢印をクリックします。

スマート ライセンスの編集

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	グローバルのみ	Admin

複数の Firepower Threat Defense デバイスのスマート ライセンスを一度に有効または無効にすることができます。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付けられている機能は使用できなくなります。

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 [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するには、[追加（Add）] 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（Access）
任意（Any）	該当なし	Firepower Threat Defense	グローバルのみ	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	グローバルのみ	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。

Smart Software Satellite Server 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（Access）
任意（Any）	該当なし	Firepower Threat Defense	グローバルのみ	Admin

Cisco Smart Software Manager は、ライセンス認証局と通信してライセンスを管理します。Firepower Management Center はインターネットに接続している場合、Smart Software Manager に直接接続します。また、Smart Software Satellite Server から Smart Software Manager に接続できます。

Smart Software Satellite Server は、ライセンス認証局との定期的な通信を維持し、同期をスケジュールするか、手動でスマート ライセンス認証を Smart Software Manager と同期できます。

Smart Software Satellite Server は、次の場合に使用できます。

- 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。

Smart Software Satellite Server の設定の詳細については、*Smart Software Manager Satellite User Guide*を参照してください。

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 次の選択肢があります。

- Firepower Management Center はインターネットにアクセスできる場合は、[Cisco Smart Software Manager に直接接続（Connect directly to Cisco Smart Software Manager）] を選択します。
- Firepower Management Center がインターネットにアクセスできない場合は、[Cisco Smart Software Satellite Server に接続（Connect to Cisco Smart Software Satellite Server）] を選択して、サーバの URL を入力し、SSL 証明書を選択します。

ステップ 4 [適用（Apply）] 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 ライセンスでは、製品認証キー（PAK）をアクティブ化する必要があり、デバイス間で譲渡することはできません。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（Protection）	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

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
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）	Protection	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	Protection	No
マルウェア（Malware）	TAM、TAMC、または AMP	7000 および 8000 シリーズ ASA FirePOWER NGIPSv	AMP for Firepower（ネットワークベースの高度なマルウェア防御）	Protection	Yes
URL フィルタリング（URL Filtering）	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	Protection	Yes
VPN	なし（詳細は販売担当者にお問い合わせください）	7000 および 8000 シリーズ	バーチャルプライベートネットワークの展開	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）をブロックできます。マルウェア ライセンスが必要な *AMP for Firepower* 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、AMP for Firepower 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 AMP for Firepower 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。AMP for Firepower 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。

AMP for Firepower 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 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。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 AMP for Firepower 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（**Access**）
該当なし	任意（Any）	従来型（Classic）	グローバルのみ	Admin

[Classic ライセンス（Classic Licenses）] ページを使用して、Firepower Management Center に追加した Classic ライセンスを表示します。展開環境内の管理対象デバイスのタイプごとに、所有しているライセンスの総数と、使用中のライセンスの割合がこのページにリストされます。

[ライセンス（Licenses）] ページには、各ライセンスの詳細も表示されます。モデルごとに、各タイプの所有ライセンス数、各タイプのライセンスでライセンス付与できる管理対象デバイスの数が表示されます。有効期限のあるライセンスの場合、このページに有効期限が表示されます。

次のように、ライセンスおよびライセンス制限を表示できます。

- [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、Classic 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

[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。

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（Classic）	グローバルのみ	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）と MAC アドレスで構成されます（たとえば、66:00:00:77:FF:CC:88）。

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 テキストを取得する必要があります。

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。Firepower Management Center への従来型ライセンスの追加 （22 ページ）を参照してください。

Firepower Management Center への従来型ライセンスの追加

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（Access）
該当なし	任意（Any）	従来型（Classic）	グローバルのみ	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

- 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://www.cisco.com/c/en/us/buy/smart-accounts.htmlを参照してください。
- 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 （21 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。

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。管理対象デバイスへのライセンスの割り当て （23 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**。

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	サポートされるドメイン	アクセス（Access）
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。

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

- 設定変更を展開します。設定変更の導入を参照してください。