



ASA FirePOWER モジュールのライセンス

組織に対して ASA FirePOWER 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。

詳細については、以下を参照してください。

- [ライセンスについて \(45-1 ページ\)](#)
- [ライセンスの表示 \(45-4 ページ\)](#)
- [ASA FirePOWER モジュールへのライセンスの追加 \(45-5 ページ\)](#)
- [ライセンスの削除 \(45-6 ページ\)](#)

ライセンスについて

ライセンス:任意 (Any)

組織に対して ASA FirePOWER 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。

ライセンスにより、デバイスは以下を含むさまざまな機能を実行できます。

- 侵入検知と防御
- セキュリティ インテリジェンス フィルタリング
- ファイル制御および高度なマルウェア防御
- アプリケーション、ユーザ、および URL 制御

ASA FirePOWER モジュールの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。ライセンス付きの機能は削除できます。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。

ここでは、ASA FirePOWER モジュール導入環境で使用可能なライセンスのタイプについて説明します。アプライアンス上で有効にできるライセンスは、有効になっている他のライセンスに依存します。

次の表に、ASA FirePOWER モジュール ライセンスの要約を示します。

表 45-1 ASA FirePOWER モジュール ライセンス

ライセンス	付与される機能	要件
Protection	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
Control	ユーザおよびアプリケーション制御	Protection
Malware	高度なマルウェア防御(ネットワークベースのマルウェアの検出とブロック)	Protection
URL Filtering	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

詳細については、以下を参照してください。

- [Protection \(45-2 ページ\)](#)
- [Control \(45-3 ページ\)](#)
- [Malware \(45-4 ページ\)](#)
- [URL Filtering \(45-3 ページ\)](#)

Protection

ライセンス:Protection

Protection 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 インテリジェンスの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。**Malware** ライセンス ([Malware \(45-4 ページ\)](#)) を参照) 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。
- **Security Intelligence** フィルタリングにより、トラフィックをアクセスコントロールルールによる分析対象にする前に、特定の IP アドレス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 フィールドにより、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。

ライセンスがない状態でも Protection 関連の検査を実行するようにアクセスコントロールポリシーを設定できますが、最初に Protection ライセンスを ASA FirePOWER モジュールに追加するまではポリシーを適用できません。

Protection ライセンスを ASA FirePOWER モジュールから削除すると、ASA FirePOWER モジュールは侵入とファイルイベントの検出を停止します。また、ASA FirePOWER モジュールはシスコによって提供される情報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。Protection を再度有効にするまでは、既存のポリシーを再適用できません。

Protection ライセンスは URL Filtering、Malware、および Control ライセンスに必要であるため、Protection ライセンスを削除または無効にすると、URL Filtering、Malware、または Control 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。

Control

ライセンス:Control

Control 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。Control を有効にするには、Protection も有効にする必要があります。

Control ライセンスがない状態でアクセス コントロール ルールにユーザ条件とアプリケーション条件を追加できますが、ポリシーを適用するには、最初に Control ライセンスを ASA FirePOWER モジュールに追加します。

Control ライセンスを削除する場合、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があるルールが含まれていると、それらのポリシーは再適用できません。

URL Filtering

ライセンス:URL Filtering

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、ネットワークを移動可能なトラフィックを判別するアクセス コントロール ルールを作成し、ASA FirePOWER モジュールが シスコ クラウドから取得する URL に関する情報に関連付けることができます。URL Filtering を有効にするには、Protection ライセンスも有効にする必要があります。



ヒント

URL Filtering 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 フィルタリングにはサブスクリプションベースの URL Filtering ライセンスが必要です。URL Filtering ライセンスがない状態でも、アクセス コントロール 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、ASA FirePOWER モジュールは URL 情報を取得するためにクラウドに接続しません。アクセス コントロール ポリシーは、まず URL Filtering ライセンスを ASA FirePOWER モジュールに追加するまで適用できません。

ASA FirePOWER モジュールからライセンスを削除すると、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 Filtering ライセンスが期限切れになることがあります。ライセンスが期限切れになるかまたはライセンスを削除すると、URL 条件が含まれているアクセス コントロール ルールは URL フィルタリングをすぐに停止し、ASA FirePOWER モジュールはクラウドにアクセスできなくなります。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適用することができません。

Malware

ライセンス:Malware

Malware ライセンスでは、拡張マルウェア防御を実行できます。つまり、デバイスを使用して、ネットワーク上で送信されるファイルからマルウェアを検出してブロックできます。デバイス上で Malware を有効にするには、Protection も有効にする必要があります。

ファイル ポリシーの一部としてマルウェア検出を設定し、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。Malware ライセンスにより、マルウェアの制限セットのファイル タイプを検査できます。Malware 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。

Malware ライセンスがなくてもアクセス コントロール ルールにマルウェア検出ファイル ポリシーを追加できますが、アクセス コントロール ルール エディタでこのファイル ポリシーに警告アイコン(▲)が付きます。ファイル ポリシー内でも、マルウェア クラウド ルックアップ ルールに警告アイコンが付きます。マルウェア検出ファイル ポリシーを含むアクセス コントロール ポリシーを適用する前に、Malware ライセンスを必ず追加してください。後でライセンスを削除すると、マルウェア検出を実行するファイル ポリシーが含まれている既存のアクセス コントロール ポリシーを、これらのデバイスに対して再適用することはできません。

Malware ライセンスを削除するかまたはそれが期限切れになると、ASA FirePOWER モジュールはマルウェア クラウド検索の実行と、シスコ クラウドから送信される遡及的イベントの認識を停止します。既存のアクセス コントロール ポリシーにマルウェア検出を実行するファイル ポリシーが含まれている場合、このアクセス コントロール ポリシーを再適用することはできません。Malware ライセンスの期限切れまたは削除後のごく短い時間内は、マルウェア クラウド ルックアップ ファイル ルールで検出されたファイルのキャッシュされた性質を、システムが利用できることに注意してください。この時間枠の経過後は、システムは検索を実行せず Unavailable という性質をこれらのファイルに割り当てます。

ライセンスの表示

ライセンス:任意 (Any)

ASA FirePOWER モジュールのライセンスを表示するには、[ライセンス (Licenses)] ページを使用します。

[ライセンス (Licenses)] ページ以外にも、ライセンスとライセンス制限を確認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 (Device)] ページ ([設定 (Configuration)] > [ASA FirePOWER 設定 (ASA FirePOWER Configuration)] > [デバイス管理 (Device Management)] > [デバイス (Device)]) には、ライセンスがリストされます。

ライセンスを確認するには、次の手順を実行します。

手順 1 [設定 (Configuration)] > [ASA FirePOWER 設定 (ASA FirePOWER Configuration)] > [ライセンス (Licenses)] の順に選択します。

[ライセンス (Licenses)] ページが表示されます。

ASA FirePOWER モジュールへのライセンスの追加

ライセンス:任意(Any)

ASA FirePOWER モジュールにライセンスを追加する前に、ライセンスの購入時にシスコから提供されたアクティベーション キーがあることを確認してください。ライセンス付き機能を使用する前に、必ずライセンスを追加してください。



(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。

ライセンスを追加するには、次の手順を実行します。

- 手順 1 [設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [ライセンス(Licenses)] の順に選択します。
[ライセンス(Licenses)] ページが表示されます。
- 手順 2 [新規ライセンスの追加(Add New License)] をクリックします。
[ライセンスの追加(Add License)] ページが表示されます。
- 手順 3 ライセンスを電子メールで受信しましたか?
 - 電子メールで受信した場合は電子メールからライセンスをコピーし、[ライセンス(License)] フィールドに貼り付け、[ライセンスの送信(Submit License)] をクリックします。
ライセンスが正しい場合、ライセンスが追加されます。残りの手順は省略します。
 - 電子メールで受信していない場合は、[ライセンスの取得(Get License)] をクリックします。
[製品ライセンス登録(Product License Registration)] ポータルが表示されます。インターネットにアクセスできない場合は、インターネットにアクセスできるコンピュータに切り替えてください。ページ下部に表示されるライセンス キーを書きとめ、
<https://www.cisco.com/go/license> [英語]を参照します。
- 手順 4 画面の指示に従ってライセンスを取得します。ライセンスは電子メールで送信されます。



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。

- 手順 5 電子メールからライセンスをコピーし、ASA FirePOWER モジュールの Web ユーザーインターフェイスの [ライセンス(Licenses)] フィールドに貼り付け、[ライセンスの送信(Submit License)] をクリックします。
ライセンスが有効な場合、ライセンスが追加されます。


ライセンスの削除

ライセンス:任意 (Any)

何らかの理由でライセンスを削除する必要がある場合は、次の手順を使用します。シスコは各 ASA FirePOWER モジュールの固有ライセンス キーに基づいてライセンスを生成するため、ある ASA FirePOWER モジュールからライセンスを削除し、この削除したライセンスを別の ASA FirePOWER モジュールで再利用することはできないことに注意してください。

ほとんどの場合、ライセンスを削除すると、そのライセンスによって有効になる機能を使用することができなくなります。詳細については、[ライセンスについて \(45-1 ページ\)](#) を参照してください。

ライセンスを削除するには:

-
- 手順 1 [設定 (Configuration)] > [ASA FirePOWER 設定 (ASA FirePOWER Configuration)] > [ライセンス (Licenses)] の順に選択します。
[ライセンス (Licenses)] ページが表示されます。
 - 手順 2 削除するライセンスの横にある削除アイコン()をクリックします。
 - 手順 3 ライセンスを削除することを確認します。
ライセンスが削除されます。
-