
# シスコ ASA FirePOWER モジュールの概要

シスコ ASA FirePOWER モジュール® は、Cisco ASA5506-X、ASA5506H-X、ASA5506W-X、ASA5508-X、ASA5512-X、ASA5515-X、ASA5516-X、ASA5525-X、ASA5545-X、ASA5555-X、ASA5585-X-SSP-10、ASA5585-X-SSP-20、ASA5585-X-SSP-40、ASA5585-X-SSP-60 の各デバイスに展開できるモジュールです。モジュールは、組織のセキュリティ ポリシー（ネットワークを保護するためのガイドライン）に準拠した方法でネットワーク トラフィックを処理するように設計されています。セキュリティ ポリシーにはアクセプタブル ユース ポリシー（AUP）も含まれていることがあります。AUP は、組織のシステムの使用方法に関するガイドラインを従業員に提供します。

このガイドでは、ASDM 経由でアクセス可能な、ASA FirePOWER モジュールの機能の onbox 設定に関する情報を提供します。各章の説明、図、および手順では、ユーザ インターフェイスのナビゲート、システム パフォーマンスの最大化、問題のトラブルシューティングに役に立つ詳細な情報を記載しています。

(注) ASA FirePOWER モジュールをホストしている ASA でコマンドの権限を有効にする場合は、特権レベル 15 を持つユーザ名でログインして、ASA FirePOWER のホーム、設定、およびモニタリングのページを参照できるようにする必要があります。ステータス ページ以外の ASA FirePOWER のページに対する読み取り専用またはモニタ専用のアクセス権限は、サポートされていません。

続く各トピックでは、ASA FirePOWER モジュールの概要、主要なコンポーネント、およびこのマニュアルの使用方法について説明しています。



# ASA FirePOWER モジュールの概要

ASA FirePOWER モジュールは、ネットワーク セグメントにインストールされている ASA デバイスで動作し、分析用のトラフィックをモニタします。

インラインで展開されたシステムは、*アクセス コントロール*を使用してトラフィックのフローに影響を与えることができ、これによって、ネットワークを出入りしたり通過したりするトラフィックを処理する方法を詳細に指定できます。ネットワーク トラフィックについて収集したデータおよびそのデータから収集したすべての情報は、次に基づいてそのトラフィックのフィルタ処理や制御ができます。

- シンプルで容易に決定されるトランスポート層およびネットワーク層の特性（送信元と宛先、ポート、プロトコルなど）
- レピュテーション、リスク、ビジネスとの関連性、使用されたアプリケーション、または訪問した URL などの特性を含む、トラフィックに関する最新のコンテキスト情報
- 組織内の Microsoft Active Directory LDAP ユーザ

各タイプのトラフィックのインスペクションと制御は、最大限の柔軟性とパフォーマンスを引き出すために最も意味がある局面で実行されます。たとえば、レピュテーション ベースのブラックリスト登録は、単純な送信元と宛先のデータを使用するため、禁止されたトラフィックをプロセスの初期段階でブロックできます。その一方、侵入およびエクスプロイトの検出とブロックは、プロセスの最後の防衛ラインとして実行されます。

# ASA FirePOWER モジュール コンポーネント

以下のトピックでは、組織のセキュリティ、適用可能な使用ポリシー、およびトラフィック管理の戦略に対して有用な ASA FirePOWER モジュール の主な機能について説明します。



## アクセス コントロール

*アクセス コントロール*はポリシーベースの機能で、ユーザはこれを使用してネットワークを横断できるトラフィックを指定、検査、および記録できます。*アクセス コントロール ポリシー*は、システムがネットワーク上のトラフィックを処理する方法を決定します。

最も単純なアクセス コントロール ポリシーは、その*デフォルト アクション*を使用してすべてのトラフィックを処理します。このデフォルト アクションは、すべてのトラフィックをさらなるインスペクションを行わずにブロックまたは信頼するように設定するか、あるいは、侵入がないかトラフィックをインスペクションするように設定することができます。

より複雑なアクセス コントロール ポリシーは、セキュリティ インテリジェンス データに基づいてトラフィックをブラックリスト登録することができます。さらに、*アクセス コントロール ルール*を使用して、ネットワーク トラフィックのロギングおよび処理を細かく制御することができます。これらのルールは単純にすることも複雑にすることもでき、複数の基準を使用してトラフィックを照合およびインスペクションします。セキュリティ ゾーン、ネットワークもしくは地理的位置、ポート、アプリケーション、要求された URL、ISE 属性、およびユーザ別にトラフィックを制御できます。アクセス コントロールの詳細オプションには、復号化、前処理、およびパフォーマンスが含まれます。

各アクセス コントロール ルールには*アクション*も含まれており、一致するトラフィックをモニタ、信頼、ブロック、または許可するかどうかを決定します。トラフィックを許可するときは、システムが侵入ポリシーまたはファイル ポリシーを使用してトラフィックを最初に検査し、アセットに到達したりネットワークを出る前に、エクスプロイト、マルウェア、または禁止されたファイルをブロックするように指定できます。

# 侵入検知および侵入防御

侵入検知および侵入防御は、トラフィックが宛先に許可される前のシステムの最後の防御ラインです。*侵入ポリシー*は、アクセス コントロール ポリシーによって呼び出される侵入検知および侵入防御の設定の定義済みセットです。*侵入ルール*およびその他の設定を使用して、これらのポリシーはセキュリティ違反がないかトラフィックを検査し、インライン展開では、悪意のあるトラフィックをブロックまたは変更できます。

システムが提供するポリシーが組織のセキュリティのニーズに十分に対応していない場合は、カスタム ポリシーを作成することで、環境内のシステムのパフォーマンスを向上させ、ネットワーク上で発生する悪意のあるトラフィックやポリシー違反に焦点を当てたビューを提供できます。設定できるカスタム ポリシーを作成および調整することにより、システムがネットワーク上のトラフィックを処理して侵入の有無について検査する方法を非常にきめ細かく設定できます。

# 高度なマルウェア防御とファイル制御

マルウェアを特定してその影響を軽減するため、ASA FirePOWER モジュールのファイル制御コンポーネントおよび高度なマルウェア防御コンポーネントでは、ネットワーク トラフィック内のファイル（マルウェア ファイル、アーカイブ ファイル内にネストされたファイルを含む）の伝送を検出、追跡、キャプチャ、分析し、必要に応じてブロックすることができます。

### ファイル制御

*ファイル制御*により、デバイスは、ユーザが特定のアプリケーション プロトコルを介して特定のタイプのファイルをアップロード（送信）またはダウンロード（受信）するのを検出およびブロックすることができます。ファイル制御は、全体的なアクセス コントロール設定の一部として設定します。アクセス コントロール ルールに関連付けられたファイル ポリシーによって、ルールの条件を満たすネットワーク トラフィックが検査されます。

### ネットワークベースの高度なマルウェア防御（AMP）

ネットワークベースの*高度なマルウェア防御*（AMP）によって、複数のファイル タイプのマルウェアに関してネットワーク トラフィックを検査できます。

検出されたファイルは、保存済みかどうかに関係なく、ファイルの SHA-256 ハッシュ値を使用して単純な既知の性質の検索を行うために Collective Security Intelligence クラウド に送信できます。このコンテキスト情報を使用して、特定のファイルをブロックまたは許可するようにシステムを設定できます。

マルウェア防御は、総合的なアクセス コントロール設定の一部として設定することができます。アクセス コントロール ルールに関連付けられているファイル ポリシーは、ルール条件に一致するネットワーク トラフィックを検査します。

# アプリケーション プログラミング インターフェイス

アプリケーション プログラミング インターフェイス（API）を使用してシステムと対話する方法がいくつか用意されています。詳細については、次のいずれかのサポート サイトから追加資料をダウンロードできます。

- **シスコ：**（http://www.cisco.com/cisco/web/support/index.html）

# ライセンスの規則

項の先頭に記載されているライセンス文は、その項に記載されている機能を使用するのに必要なライセンスを示しています。具体的なライセンスは次のとおりです。

**Protection**

Protection ライセンスでは、デバイスで侵入の検出および防御、ファイル制御、セキュリティ インテリジェンス フィルタリングを実行することができます。

**Control**

Control ライセンスでは、デバイスでユーザおよびアプリケーションの制御を実行することができます。Control ライセンスには Protection ライセンスが必要です。

**URL Filtering**

URL Filtering ライセンスでは、デバイスは、定期的に更新されるクラウドベースのカテゴリおよびレピュテーション データを使用して、モニタ対象ホストが要求した URL に基づいて、ネットワークを通過できるトラフィックを判別できます。URL Filtering ライセンスには Protection ライセンスが必要です。

**Malware**

Malware ライセンスでは、デバイスはネットワークベースの高度なマルウェア防御（AMP）を実行できます。これはネットワーク上で転送されるファイルに含まれるマルウェアを検出し、ブロックする機能です。Malware ライセンスには Protection ライセンスが必要です。

ライセンス付きの機能の多くは追加的であるため、このドキュメントでは、各機能で最も必要なライセンスについてのみ記載しています。たとえば、ある機能には Protection ライセンスおよび Control ライセンスが必要である場合は、Control のみを記載しています。ただし、追加的でないライセンスを機能が必要とする場合、マニュアルではそのライセンスをプラス（+）文字で示しています。

ライセンス文の「または」という語は、その項に記載されている機能を使用するには特定のライセンスが必要であるが、追加のライセンスで機能を追加できることを示しています。たとえば、あるファイル ポリシー内で、一部のファイル ルール アクションには Protection ライセンスが必要であり、他のファイル ルール アクションには Malware ライセンスが必要であるとします。この場合、そのファイル ルールの説明のライセンス文には、「Protection または Malware」と示されます。

# IP アドレスの規則

IPv4 Classless Inter-Domain Routing（CIDR）の表記、および IPv6 の類似のプレフィックス長の表記を使用して、ASA FirePOWER モジュールの多数の場所でアドレス ブロックを定義することができます。

CIDR 表記は、ネットワーク IP アドレスとビット マスクを組み合わせて使用し、指定されたアドレス ブロック内の IP アドレスを定義します。たとえば次の表に、プライベート IPv4 アドレス空間を CIDR 表記で示します。

*表 1-1　CIDR 表記の構文例*

| CIDR ブロック | CIDR ブロックの IP アドレス | サブネット マスク | IP アドレスの数 |
|---|---|---|---|
| 10.0.0.0/8 | 10.0.0.0 ～ 10.255.255.255 | 255.0.0.0 | 16,777,216 |
| 172.16.0.0/12 | 172.16.0.0 ～ 172.31.255.255 | 255.240.0.0 | 1,048,576 |
| 192.168.0.0/16 | 192.168.0.0 ～ 192.168.255.255 | 255.255.0.0 | 65,536 |

同様に、IPv6 はネットワーク IP アドレスとプレフィックス長を組み合わせて使用し、指定されたブロック内の IP アドレスを定義します。たとえば 2001:db8::/32 は、プレフィックス長が 32 ビットの 2001:db8:: ネットワーク内の IPv6 アドレスを表します。つまり、2001:db8:: ～ 2001:db8:ffff:ffff:ffff:ffff:ffff:ffff を表します。

CIDR またはプレフィックス長の表記を使用して IP アドレスのブロックを指定する場合、ASA FirePOWER モジュール は、マスクまたはプレフィックス長で指定されたネットワーク IP アドレスの部分**のみ**を使用します。たとえば、10.1.2.3/8 と入力した場合、ASA FirePOWER モジュール では 10.0.0.0/8 が使用されます。

つまり シスコ は、CIDR またはプレフィックス長の表記を使用する場合に、ビット境界上でネットワーク IP アドレスを使用する標準の方法を推奨していますが、ASA FirePOWER モジュールではこれは必要ありません。