



仕様

この付録では、FWSM の仕様について説明します。次の内容について説明します。

- [スイッチ ハードウェアおよびソフトウェアの互換性 \(p.A-2\)](#)
- [ライセンス対象機能 \(p.A-2\)](#)
- [物理仕様 \(p.A-3\)](#)
- [機能の制限 \(p.A-3\)](#)
- [管理対象のシステム リソース \(p.A-4\)](#)
- [固定システム リソース \(p.A-5\)](#)
- [ルールの制限 \(p.A-6\)](#)

スイッチ ハードウェアおよびソフトウェアの互換性

FWSM をサポートするスイッチ モデルには、次のプラットフォームがあります。

- 次の必須コンポーネントを装備した Catalyst 6500 シリーズ スイッチ
 - Cisco IOS ソフトウェア（スーパーバイザ IOS） または Catalyst Operating System（OS; オペレーティング システム）を搭載したスーパーバイザ エンジン。サポート対象のスーパーバイザ エンジンおよびソフトウェア リリースについては、[表 A-1](#) を参照してください。
 - Cisco IOS ソフトウェアを搭載した MSFC 2。サポート対象の Cisco IOS リリースについては、[表 A-1](#) を参照してください。
- 次の必須コンポーネントを装備した Cisco 7600 シリーズ ルータ
 - Cisco IOS ソフトウェアを搭載したスーパーバイザ エンジン。サポート対象のスーパーバイザ エンジンおよびソフトウェア リリースについては、[表 A-1](#) を参照してください。
 - Cisco IOS ソフトウェアを搭載した MSFC 2。サポート対象の Cisco IOS リリースについては、[表 A-1](#) を参照してください。



(注)

WAN ポートはスタティック VLAN（仮想 LAN）を使用しないので、スイッチの WAN ポートに FWSM を直接接続することはできません。ただし、WAN ポートから MSFC に接続し、MSFC から FWSM に接続することは可能です。

[表 A-1](#) に、スーパーバイザ エンジンのバージョンとソフトウェアを示します。

表 A-1 FWSM 3.1 のサポート

| | スーパーバイザ エンジン ¹ |
|--------------------------------|---------------------------|
| Cisco IOS | |
| 12.2(18)SXF 以上 | 720、32 |
| 12.2(18)SXF2 以上 | 2、720、32 |
| Catalyst OS² | |
| 8.5(3) 以上 | 2、720、32 |

1. FWSM は、スーパーバイザ 1 および 1A をサポートしません。
2. スーパーバイザ上で Catalyst OS を使用する場合、MSFC 上でサポート対象の任意の Cisco IOS リリースを使用できます（スーパーバイザ上で Cisco IOS ソフトウェアを使用する場合は、MSFC 上でも同じリリースを使用します）。

ライセンス対象機能

FWSM は次のライセンス対象機能をサポートします。

- マルチセキュリティ コンテキスト。FWSM では、ライセンスなしでも、2つの仮想コンテキストと1つの管理コンテキストの計3つのセキュリティ コンテキストをサポートしています。4つ以上のコンテキストが必要な場合、次のいずれかのライセンスを取得してください。
 - 20
 - 50
 - 100
 - 250
- GTP/GPRS サポート

物理仕様

表 A-2 に、FWSM の物理仕様を示します。

表 A-2 物理仕様

| 仕様 | 説明 |
|--------------|--|
| 帯域幅 | SFM (搭載されている場合) への 6 Gbps パスを備えた CEF256 ラインカード、または 32 Gbps 共有バス |
| メモリ | <ul style="list-style-type: none"> 1 GB RAM 128 MB フラッシュメモリ |
| 各スイッチのモジュール数 | 各スイッチに 4 台までのモジュールを搭載可能。 フェールオーバーを使用して 2 台をスタンバイモードにした場合でも、各スイッチに搭載できるモジュールは 4 台までです。 |

機能の制限

表 A-3 に、FWSM の機能の制限を示します。

表 A-3 機能の制限

| 仕様 | コンテキストモード | |
|---|-----------|---|
| | シングル | マルチ |
| AAA サーバ (RADIUS および TACACS+) | 16 | 各コンテキストに 4 |
| モニタできるフェールオーバーインターフェイス | 250 | すべてのコンテキスト全体で 250 |
| フィルタリングサーバ (Websense Enterprise および N2H2 の Sentian) | 16 | 各コンテキストに 4 |
| ジャンボイーサネットパケット | 8500 バイト | 8500 バイト |
| セキュリティコンテキスト | 適用外 | 250 セキュリティコンテキスト (ソフトウェアライセンスによる) |
| Syslog サーバ | 16 | 各コンテキストに 4 |
| VLAN インターフェイス ルーテッドモード | 256 | 各コンテキストに 100 FWSM の VLAN インターフェイス数は、すべてのコンテキスト全体で 1000 までに限定されています。外部インターフェイスは複数のコンテキストで共有でき、状況によっては内部インターフェイスも共有できます。 |
| 透過モード | 8 ペア | 各コンテキストに 8 ペア |

管理対象のシステム リソース

表 A-4 に、FWSM の管理対象のシステム リソースを示します。リソース マネージャを使用して、これらのリソースをコンテキスト単位で管理できます。「リソース管理の設定」(p.4-13) を参照してください。

表 A-4 管理対象のシステム リソース

| 仕様 | コンテキスト モード | |
|--|---|---|
| | シングル | マルチ |
| MAC アドレス (透過ファイアウォールモードのみ) | 64 K | すべてのコンテキスト全体で 64 K |
| FWSM で接続が許可されるホスト、同時 | 256 K | すべてのコンテキスト全体で 256 K |
| インスペクション エンジンの接続、レート | 10,000/ 秒 | すべてのコンテキスト全体で 10,000/ 秒 |
| IPSec 管理接続、同時 | 5 | 各コンテキストに 5 すべてのコンテキスト全体で最大 10 |
| ASDM 管理セッション、同時 ¹ | 5 | 各コンテキストで最大 5 すべてのコンテキスト全体で最大 80 |
| NAT 変換、同時 | 256 K | すべてのコンテキスト全体で 256 K |
| SSH 管理接続、同時 | 5 | 各コンテキストに 5 すべてのコンテキスト全体で最大 100 |
| システム メッセージ、レート | FWSM の端末またはバッファへの送信メッセージは、30,000/ 秒 Syslog サーバへの送信メッセージは、25,000/ 秒 | FWSM の端末またはバッファへの送信メッセージは、すべてのコンテキスト全体で 30,000/ 秒 Syslog サーバへの送信メッセージは、すべてのコンテキスト全体で 25,000/ 秒 |
| 1 台のホストと複数の他のホスト間の接続を含む、任意の 2 つのホスト間の TCP/UDP ^{2 3} 接続、同時接続およびレート | 999,900 ⁴ 100,000/ 秒 | すべてのコンテキスト全体で 999,900 ⁴ すべてのコンテキスト全体で 100,000/ 秒 |
| Telnet 管理接続、同時 | 5 | 各コンテキストに 5 すべてのコンテキスト全体で最大 100 の接続 |

- ASDM セッションでは、2 つの HTTPS 接続を使用します。1 つは常に使用されるモニタ用、もう 1 つは変更時のみに使用される設定変更用です。たとえば、システム制限の ASDM セッション数が 80 の場合、HTTPS 接続数は 160 に制限されます。
- 初期接続は、接続の総数に含まれます。初期接続の制限を設定した場合、制限を超える初期接続はカウントされません。
- FWSM では、削除のマークが付いた接続を削除するために、最大 500 ミリ秒かかることがあります。この間、接続上のトラフィックは廃棄されるため、接続が削除されるまで、同じ送信元ポートおよび宛先ポートを使用して同じ宛先への新しい接続を開始することはできません。大部分の TCP アプリケーションでは、バックツーバック接続で同じポートを再利用しませんが、RSH は同じポートを再利用することがあります。RSH など、バックツーバック接続で同じポートを再利用するアプリケーションを使用する場合、FWSM によりパケットが廃棄されることがあります。
- PAT (ポートアドレス変換) では各接続に個別の変換が必要なので、PAT を使用する接続の有効な制限値は、接続制限ではなく変換の制限 (256 K) になります。接続制限を適用するには、同じ変換セッションで複数の接続が可能な NAT を使用する必要があります。

固定システム リソース

表 A-5 に、FWSM の固定システム リソースを示します。

表 A-5 固定システム リソース

| 仕様 | コンテキスト モード | |
|----------------------------|------------------|-----------------------------|
| | シングル | マルチ |
| AAA 接続、レート | 80/ 秒 | すべてのコンテキスト全体で 80/ 秒 |
| ACL ロギングのフロー、同時 | 32 K | すべてのコンテキスト全体で 32 K |
| エイリアス ステートメント | 1 K | すべてのコンテキスト全体で 1 K |
| ARP テーブル エントリ、同時 | 64 K | すべてのコンテキスト全体で 64 K |
| DNS 検査、レート | 5000/ 秒 | すべてのコンテキスト全体で 5000/ 秒 |
| グローバル ステートメント | 4 K | すべてのコンテキスト全体で 4 K |
| インスペクション ステートメント | 32 | 各コンテキストに 32 |
| NAT ステートメント | 2 K | すべてのコンテキスト全体で 2 K |
| パケット再組み立て、同時 | 30,000 | すべてのコンテキスト全体で 30,000 フラグメント |
| ルート テーブル エントリ、同時 | 32 K | すべてのコンテキスト全体で 32 K |
| shun ステートメント | 5 K | すべてのコンテキスト全体で 5 K |
| SIP 接続、同時 | 5 K | すべてのコンテキスト全体で 5 K |
| スタティック NAT ステートメント | 2 K | すべてのコンテキスト全体で 2 K |
| TFTP セッション、同時 ¹ | 999,100 | すべてのコンテキスト全体で 999,100 |
| ユーザ認証セッション、同時 | 50 K | すべてのコンテキスト全体で 50 K |
| ユーザ許可セッション、同時 | 150 K | すべてのコンテキスト全体で 150 K |
| | 各ユーザで最大 15 セッション | 各ユーザで最大 15 セッション |

1. FWSM Version 1.1 では、TFTP セッションの数は 1024 セッションに制限されていました。

ルールの制限

FWSM がシステム全体でサポートできるルール数は、シングルモードで約 80 K、マルチモードで約 142 K です。

デフォルトが 12 メモリパーティションのマルチコンテキストモードでは、各コンテキストで最大 12,130 のルールをサポートできますが、実際に 1 つのコンテキストでサポートできるルール数は、設定するコンテキスト数とパーティション数に応じて、これより増減ことがあります。コンテキスト間のメモリ配分の詳細については、「[メモリパーティションの設定](#)」(p.4-18)を参照してください。

表 A-6 に、タイプ別のルールの最大数を示します。

表 A-6 **ルールの制限**

| 仕様 | コンテキストモード | |
|------------------------------|-----------|----------------------------|
| | シングル | 12 プールのマルチ (パーティションごとの最大数) |
| AAA ルール | 6451 | 992 ¹ |
| ACE | 72,806 | 11,200 |
| ネットワーク アクセス許可用にダウンロードされる ACE | 5000 | 5000 |
| established ルール | 460 | 70 |
| フィルタ ルール | 2764 | 425 |
| ICMP、Telnet、SSH、および HTTP ルール | 1843 | 283 |
| ポリシー NAT ACE | 1843 | 283 |
| inspect ルール | 5529 | 850 |

- たとえば、96 のコンテキストを 12 プールに均等に割り当てた場合、各プールに 8 つのコンテキストがあるので、各コンテキストが均等に使用できるフィルタ ルール数は 75 になります。