APPENDIX A

# 仕様

この付録では、FWSM の仕様について説明します。内容は次のとおりです。



## スイッチ ハードウェアおよびソフトウェアの互換性

FWSM は、Cisco 6500 シリーズ スイッチまたは Cisco 7600 シリーズ ルータに搭載できます。いずれのシリーズも設定が同じであるため、このマニュアルではこれらのシリーズを総称して「スイッチ」と表記しています。このスイッチには、スイッチ（スーパーバイザ エンジン）とルータ（MSFC 2）があります。

スイッチのスーパーバイザ エンジンと統合型の MSFC ルータの両方で Cisco IOS ソフトウェアがサポートされています。

（注） Catalyst オペレーティング システム ソフトウェアはサポートされていません。

WAN ポートではスタティック VLAN が使用されないので、FWSM はスイッチ WAN ポートへの直接接続をサポートしません。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。

FWSM は独自の OS で動作します。

ここでは、次の内容について説明します。

# Catalyst 6500 シリーズの要件

表 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 1　Catalyst 6500 の FWSM のサポート**

| | | FWSM の機能 | | |
|---|---|---|---|---|
| | スーパーバイザ エンジン[1] | PISA 統合 | ルート ヘルス注入 | 仮想スイッチング システム |
| **Cisco IOS Software Release** | | | | |
| 12.2(18)SXF 以上 | 720、32 | No | No | No |
| 12.2(18)SXF2 以上 | 2、720、32 | No | No | No |
| 12.2(33)SXI | 720-10GE | No | **Yes** | **Yes** |
| 12.2(33)SXI | 720、32 | No | **Yes** | No |
| 12.2(33)SXI2 | 720-10GE | No | **Yes** | **Yes** |
| 12.2(33)SXI2 | 720、32 | No | **Yes** | No |
| 12.2(18)ZYA | 32-PISA | **Yes** | No | No |
| **Cisco IOS Software Modularity Release** | | | | |
| 12.2(18)SXF4 | 720、32 | No | No | No |

1. FWSM は、スーパーバイザ 1 および 1A をサポートしていません。

# Cisco 7600 シリーズの要件

表 2 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 2　Cisco 7600 の FWSM のサポート**

| | | FWSM の機能 | | |
|---|---|---|---|---|
| | スーパーバイザ エンジン[1] | PISA 統合 | ルート ヘルス注入 | 仮想スイッチング システム |
| **Cisco IOS Software Release** | | | | |
| 12.2(33)SRA | 720、32 | No | No | No |
| 12.2(33)SRB | 720、32 | No | No | No |
| 12.2(33)SRC | 720、32、720-1GE | No | No | No |
| 12.2(33)SRD | 720、32、720-1GE | No | No | No |
| 12.2(33)SRE | 720、32、720-1GE | No | No | No |
| 12.2(33)SRE2 | 720-3C-1GE | No | No | No |

1. FWSM は、スーパーバイザ 1 および 1A をサポートしていません。

# 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ています。

- マルチセキュリティ コンテキスト。FWSM 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合計 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
- BGP スタブ サポート

# 物理仕様

表 A-3 に、FWSM の物理仕様を示します。

**表 A-3　物理仕様**

| 仕様 | 説明 |
|---|---|
| 帯域幅 | Switch Fabric Module（SFM; スイッチ ファブリック モジュール）（搭載されている場合）への 6 Gbps パス、または 32 Gbps 共有バスを備えた CEF256 ライン カード |
| Memory | • 1 GB メモリ<br>• 128 MB フラッシュ メモリ |
| 各スイッチのモジュール数 | 各スイッチにモジュールを 4 台まで搭載できます。<br>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-4 に、FWSM の機能の制限を示します。

**表 A-4　機能の制限**

| | コンテキスト モード | |
|---|---|---|
| 仕様 | 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 |

表 A-4　機能の制限 （続き）

| 仕様 | コンテキスト モード | |
|---|---|---|
| | シングル | マルチ |
| 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 |
| フラグメント化パケット | • FWSM は、元のサイズが 8782 バイト以下のフラグメント セットを受信すると、そのセットを組み立て直したうえでネットワーク上に送り返しますが、この際にフラグメントのサイズが受信時のサイズと異なる場合があります。<br>• FWSM は、元のサイズが 8783 バイト以上のフラグメント セットを受信すると、次の処理を実行します。<br>– そのフレームが接続で最初のパケットである場合（ICMP の場合と同様）、FWSM は最初の 8782 バイトを組み立て直したうえで転送しますが、残りのフラグメントは廃棄されます。<br>– そのフレームが接続で最初のパケット *でない* 場合、FWSM は最初の 8782 バイトを組み立て直したうえで転送し、残りのフラグメントも転送しますが、再組み立てチェックは実施されません。 | |
| ジャンボ イーサネット パケット | 8,500 バイト | 8,500 バイト |
| セキュリティ コンテキスト | N/A | 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 | 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<br>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。 |
| トランスペアレント 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-5 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.4-22）を参照してください。

**表 A-5　管理対象のシステム リソース**

| | コンテキスト モード | |
|---|---|---|
| **仕様** | **シングル** | **マルチ** |
| MAC アドレス（トランスペアレント ファイアウォール モード限定） | 65,536 | すべてのコンテキスト全体で 65,536 |
| FWSM で接続が許可されるホスト、同時 | 262,144 | すべてのコンテキスト全体で 262,144 |
| インスペクション エンジンの接続、レート | 100,000/秒 | すべてのコンテキスト全体で 100,000/秒 |
| IPSec 管理接続、同時 | 5 | 各コンテキストに 5<br>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<br>すべてのコンテキスト全体で最大 80 |
| NAT の変換（xlate）数、同時 | 262,144 | すべてのコンテキスト全体で 262,144 |
| SSH 管理接続、同時[2] | 5 | 各コンテキストに 5<br>すべてのコンテキスト全体で最大 100 |
| システム ログ メッセージ、レート | FWSM の端末またはバッファに送信されるメッセージは、30,000/秒<br>Syslog サーバに送信されるメッセージは、25,000/秒 | FWSM の端末またはバッファに送信されるメッセージは、すべてのコンテキスト全体で 30,000/秒<br>Syslog サーバに送信されるメッセージは、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[3] [4] 接続、同時接続およびレート | 999,900[5]<br>170,000/秒 | すべてのコンテキスト全体で 999,900[5]<br>すべてのコンテキスト全体で 170,000/秒 |
| Telnet 管理接続、同時[2] | 5 | 各コンテキストに 5<br>すべてのコンテキスト全体で最大 100 の接続 |

1. ASDM セッションでは、2 つの HTTPS 接続を使用します。1 つは常に存在するモニタリング用の接続、もう 1 つは変更時にのみ存在するコンフィギュレーション変更用の接続です。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。
2. 管理コンテキストでは、Telnet 接続と SSH 接続を 15 個まで使用できます。
3. 初期接続は、接続の総数に含まれます。初期接続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。
4. FWSM では、削除のマークが付いた接続を削除するのに、最長で 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と、FWSM でパケットが廃棄されることがあります。

5. 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-6 に、FWSM の固定システム リソースを示します。

**表 A-6　固定システム リソース**

| | コンテキスト モード | |
|---|---|---|
| **仕様** | **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 |
| ネットワーク アクセス許可用にダウンロードされる ACE | 3,500 | すべてのコンテキスト全体で 3,500 |
| ACL ロギングのフロー、同時 | 32,768 | すべてのコンテキスト全体で 32,768 |
| エイリアス ステートメント | 512 | すべてのコンテキスト全体で 512 |
| ARP テーブル エントリ、同時 | 65,536 | すべてのコンテキスト全体で 65,536 |
| 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 | 4204 | すべてのコンテキスト全体で 4204 |
| 検査ステートメント | 32 | 各コンテキストに 32 |
| NAT ステートメント | 2048 | すべてのコンテキスト全体で 2048 |
| 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 | 32,768 | すべてのコンテキスト全体で 32,768 |
| shun ステートメント | 5120 | すべてのコンテキスト全体で 5120 |
| スタティック NAT ステートメント | 2048 | すべてのコンテキスト全体で 2048 |
| 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 |
| URL フィルタリング要求 | 200/秒、CPU 使用率 50% | すべてのコンテキスト全体で 200/秒、CPU 使用率 50% |
| ユーザ認証セッション、同時 | 51,200 | すべてのコンテキスト全体で 51,200 |
| ユーザ許可セッション、同時 | 153,600<br>各ユーザで最大 15 セッション | すべてのコンテキスト全体で 153,600<br>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 は、システム全体で固定数のルールをサポートしています。ここでは、次の内容について説明します。

- 「デフォルトのルール割り当て」（P.A-7）

# デフォルトのルール割り当て

表 A-7 に、機能タイプごとのデフォルトのルール数を示します。

（注）　アクセス リストの中には、他のアクセス リストよりも多量のメモリを消費するものもあります。また、アクセス リストのタイプによっては、システムでサポートできる実際の制限値が最大値よりも小さくなります。ACE とメモリ使用率の詳細については、「ACE の最大数」（P.13-6）を参照してください。

**表 A-7　デフォルトのルール割り当て**

| | コンテキスト モード | |
|---|---|---|
| **仕様** | **シングル** | **12 プール[1] のマルチ（パーティションごとの最大数）** |
| AAA ルール | 8744 | 1345 |
| ACE | 100,567 | 14,801 |
| **established** コマンド[2] | 624 | 96 |
| フィルタ ルール | 3747 | 576 |
| ICMP、Telnet、SSH、および HTTP ルール | 2498 | 384 |
| ポリシー NAT ACE[3] | 2498 | 384 |
| 検査ルール | 5621 | 1537 |
| **合計ルール** | **124,923** | **19,219** |

1. 12 以外のパーティションのデフォルト値を表示するには、**show resource rule** コマンドを使用します。
2. それぞれの **established** コマンドで制御ルールとデータ ルールが作成されるため、この値は「合計ルール」値で 2 倍になります。
3. この制限値はリリース 2.3 の値を下回っています。

# マルチ コンテキスト モードでのルール

デフォルトで 12 個のメモリ パーティションを伴うマルチコンテキスト モードでは、各コンテキストで表 A-7 に示された最大ルール数がサポートされます。所有しているコンテキストの数と設定したパーティションの数によって、コンテキストで実際にサポートされるルール数が異なる場合があります。コンテキスト間のメモリ配分の詳細については、「メモリ パーティションの概要」（P.4-12）を参照してください。

パーティションの数を少なくすると、最大ルール数の再計算が実施されるため、最大ルール数が 12 個のパーティションに利用できる合計システム数と一致しなくなる可能性があります。パーティションの最大ルール数を表示するには、システム実行スペースで次のコマンドを入力します。

```
hostname(config)# show resource rule
```

次に、**show resource rule** コマンドの出力例を示します。この例では、12 個のパーティションでのパーティション当たりの最大ルール数が 19219 と示されています（これは単なる例であり、実際に使用しているシステムでのルール数とは異なります）。

```
hostname(config)# show resource rule
```

```
             Default  Configured  Absolute
 CLS Rule     Limit      Limit      Max
-----------+---------+----------+---------
 Policy NAT     384        384        833
 ACL          14801      14801      14801
 Filter         576        576       1152
 Fixup         1537       1537       3074
 Est Ctl         96         96         96
 Est Data        96         96         96
 AAA           1345       1345       2690
 Console        384        384        768
-----------+---------+----------+---------
 Total        19219      19219

Partition Limit - Configured Limit = Available to allocate
      19219     -      19219       =           0
```

# 機能間のルールの再割り当て

ある機能から別の機能にルールを割り当て直すことができます。

**（注）** マルチコンテキスト モードでは、パーティションごとにルール割り当てを設定することもできます。これにより、グローバル設定が無効になります。「特定のメモリ パーティションに対する機能間でのルールの再割り当て」（P.4-19）を参照してください。

## 注意事項

**注意** 次のガイドラインに従わない場合、アクセス リスト コンフィギュレーションがドロップされたり、ACL ツリー破壊などのその他の異常が発生したりする可能性があります。

- ターゲット パーティションおよびルール割り当て設定は、すべての既存のコンテキストおよびルールを適用できるように、事前に非実稼動環境で注意して計算、計画および可能であればテストしてください。
- フェールオーバーが使用される場合、パーティション変更後に両方の FWSM が同時にリロードされる必要があります。両方の FWSM をリロードすると、ゼロダウンタイムのリロードを回避できず機能停止が発生します。パーティションまたはルール制限の数が異なる 2 つの FWSM はフェールオーバーで同期化されることはありません。

## 手順の詳細

ルールを割り当て直す手順は、次のとおりです。

**ステップ 1**　利用可能な合計ルール数、デフォルト値、現在のルール割り当て、および機能ごとに割り当て可能な絶対最大ルール数を表示するには、次のコマンドを入力します。

```
hostname(config)# show resource rule
```

マルチコンテキスト モードでは、システム実行スペースでこのコマンドを入力します。これにより、パーティション当たりのルール数が表示されます。パーティションの詳細については、「メモリ パーティションの概要」（P.4-12）を参照してください。

次に、**show resource rule** コマンドの出力例を示します。この例では、シングル モードでの最大ルール数が 124923 と示されています（これは単なる例であり、実際に使用しているシステムでのルール数とは異なります）。

```
hostname(config)# show resource rule

             Default  Configured  Absolute
 CLS Rule     Limit      Limit      Max
-----------+---------+----------+---------
 Policy NAT    2498       2498      10000
 ACL         100567     100567     100567
 Filter        3747       3747       7494
 Fixup         5621       5621      10000
 Est Ctl        624        624        624
 Est Data       624        624        624
 AAA           8744       8744      10000
 Console       2498       2498       4996
-----------+---------+----------+---------
 Total       124923     124923

Partition Limit - Configured Limit = Available to allocate
     124923     -     124923       =           0
```

**ステップ 2**　再割り当てを計画できるように、現在使用されているルール数を確認するには、次のいずれかのコマンドを入力します。

- シングルモードまたはコンテキスト内では、次のコマンドを入力します。

  ```
  hostname(config)# show np 3 acl count 0
  ```

- マルチコンテキスト モードでは、システム実行スペースで次のコマンドを入力します。

  ```
  hostname(config)# show np 3 acl count partition_number
  ```

次に、**show np 3 acl count** コマンドの出力例を示します。この例では、最大値 9216 に近い検査数（フィックスアップ ルール）が示されています。検査にいくつかのアクセス リスト ルール（ACL ルール）を割り当て直すことができます。

```
hostname(config)# show np 3 acl count 0

-------------- CLS Rule Current Counts --------------
CLS Filter Rule Count       :             0
CLS Fixup Rule Count        :          9001
CLS Est Ctl Rule Count      :             4
CLS AAA Rule Count          :            15
CLS Est Data Rule Count     :             4
CLS Console Rule Count      :            16
CLS Policy NAT Rule Count   :             0
CLS ACL Rule Count          :         30500
CLS ACL Uncommitted Add     :             0
CLS ACL Uncommitted Del     :             0
...
```

**（注）**　**established** コマンドでは、コントロールとデータという 2 つのタイプのルールが作成されます。これらのタイプは両方とも表示されますが、両方のルールを割り当てるには、**established** コマンドの数を設定します。これらのルールを別々に設定しないでください。

**ステップ 3**　機能間でルールを割り当て直すには、次のコマンドを入力します（マルチコンテキスト モードでは、システム実行スペースでコマンドを入力します）。1 つの機能の値を大きくした場合は、その分だけ 1 つまたは複数の機能の値を小さくする必要があります。これにより、合計ルール数がシステム制限を超えなくなります。ステップ 1 を参照し、**show resource rule** コマンドを使用して許可された合計ルール

数を確認してください。

```
hostname(config)# resource rule nat {max_policy_nat_rules | current | default | max}
acl {max_ace_rules | current | default | max}
filter {max_filter_rules | current | default | max}
fixup {max_inspect_rules | current | default | max}
est {max_established_rules | current | default | max}
aaa {max_aaa_rules | current | default | max}
console {max_console_rules | current | default | max}
```

マルチコンテキスト モードでは、このコマンドに*パーティションごとの*ルール割り当てを設定します。このコマンドですべての引数を入力する必要があります。このコマンドはただちに有効になります。

**nat** *max_nat_rules* 引数には、ポリシー NAT ACE の最大数を 0 ～ 10000 の範囲内で設定します。

**acl** *max_nat_rules* 引数には、ACE の最大数を 0 ～ システム制限の範囲内で設定します。システム制限は、シングルモードかマルチコンテキスト モードのいずれであるか、および設定したメモリ パーティションの数によって異なります。シングルモードの場合、この値は 100567 になります。マルチコンテキスト モードの場合は、ステップ 1 を参照し、**show resource rule** コマンドを使用してください。

**filter** *max_nat_rules* 引数には、フィルタ ルールの最大数を 0 ～ 6000 の範囲内で設定します。

**fixup** *max_nat_rules* 引数には、検査ルールの最大数を 0 ～ 10000 の範囲内で設定します。

**est** *max_nat_rules* 引数には、**established** コマンドの最大数を 0 ～ 716 の範囲内で設定します。established コマンドでは、コントロールとデータという 2 つのタイプのルールが作成されます。これらのタイプは両方とも **show np 3 acl count** と **show resource rules** で表示されますが、**established** コマンドの数と相互に関連している **est** キーワードを使用して両方のルールを設定します。設定済みのルールの合計数と **show** コマンドで示されたルールの合計数を比較する際には、ここで入力する値を必ず 2 倍にしてください。

**aaa** *max_nat_rules* 引数には、AAA ルールの最大数を 0 ～ 10000 の範囲内で設定します。

**console** *max_nat_rules* 引数には、ICMP、Telnet、SSH、および HTTP ルールの最大数を 0 ～ 4000 の範囲内で設定します。

**current** キーワードでは、現在設定されている値が保持されます。

**default** キーワードでは、ルールの最大数をデフォルトに設定します。

**max** キーワードでは、ルールを機能で許可されている最大数に設定します。他の機能はこの値に合わせて低く設定してください。

---

たとえば、シングルモードの ACE（デフォルト値 74,188）から検査（デフォルト値 4147）に 1000 個のルールを割り当て直す場合は、次のコマンドを入力します。

```
hostname(config)# resource rule nat default acl 73188 filter default fixup 5157 est
default aaa default console default
```

12 個のパーティションを伴うマルチコンテキスト モードで、100 個の ACE（デフォルト値 10,633）を検査（デフォルト値 1417）に割り当て直し、さらに 1 個の確立済みルールを除くすべてのルール（デフォルト値 70）をフィルタ（デフォルト値 425）に割り当て直す場合は、次のコマンドを入力します。

```
hostname(config)# resource rule nat default acl 10533 filter 494 fixup 1517 est 1 aaa
default console default
```