

## Cisco Firewall Services Module Software バージョン 3.2 および Cisco Adaptive Security Device Manager バージョン 5.2F の新機能

Cisco® Catalyst® 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータ用のファイアウォール サービス モジュール (FWSM) は、高性能な統合型ステートフル インспекション ファイアウォールで、アプリケーションおよびプロトコル用のインспекション エンジンを搭載し、5.5 Gbps のスループット、毎秒 100,000 の接続処理、および 100 万の同時接続を実現します。また、FWSM を使用したクラスタ処理ソリューションでは、シャーシあたり 20 Gbps を上回るスループットをシームレスに提供できます。Cisco FWSM Software バージョン 3.2 の設定および監視には、統合型で Web GUI ベースの Cisco Adaptive Security Device Manager (ASDM) バージョン 5.2F を使用します。リモート マルチデバイス管理を行う場合は、Cisco Security Manager バージョン 3.1 を使用して Cisco FWSM Software バージョン 3.2 の設定と管理を行います。

Cisco FWSM Software バージョン 3.2 は、次の機能を備えています。

- 中心となるファイアウォール機能の強化
- インテリジェントなネットワーク サービスの追加
- 管理機能の強化
- カットスルー プロキシ機能の強化
- 音声およびモバイル インспекション エンジンの機能強化

### Cisco FWSM Software バージョン 3.2 リリースの重要点

表 1 に、Cisco FWSM Software バージョン 3.2 の新機能を示します。

表 1 Cisco FWSM Software バージョン 3.2 の新機能

機能	利点
<b>中心となるファイアウォール機能の強化</b>	
Network Address Translation (NAT; ネットワーク アドレス変換) バイパス	no nat control コマンドや NAT 除外機能を使用すると NAT 変換エントリが作成されないため拡張性が向上する
TCP 状態のバイパスを選択可能	設定されたトラフィック クラスの TCP 状態確認を選択的にバイパスできる。これは、2 つの FWSM がレイヤ 2 レベルで隣接しない異なる場所に配置されているときに、特定のトラフィックが非対称ルーティング構成を通過できるようにする場合に有効
BGP スタブ	新しいライセンス機能 1 つの BGP ピアとの相互運用を許可し、シングル ファイアウォール モードおよび仮想ファイアウォール モードでのダイナミック ルーティングが可能 トランスペアレント ファイアウォール モードでは使用できない
非 TCP フローに対するフロー単位のタイムアウト	Cisco FWSM Software バージョン 3.1 では、TCP フローに対するフロー単位のタイムアウトが可能。バージョン 3.2 では、TCP 以外のフローでも、フロー単位のタイムアウトが可能になる

機能	利点
<b>インテリジェントなネットワーク サービス</b>	
トランスパレント NAT および Port Address Translation (PAT)	トランスパレント ファイアウォール モードで NAT および PAT をサポート。この機能によりアップストリーム ルータのネットワーク設定が容易になる(特に、マルチ ISP 構成の場合)
インターフェイス単位の Dynamic Host Control Protocol (DHCP)リレー	DHCP リレーをインターフェイス単位で設定できる
<b>管理機能の強化</b>	
シングル コンテキスト モードおよびマルチ コンテキスト モードでの SNMP (簡易ネットワーク管理プロトコル) MIB の追加	追加された MIB には、接続エントリ、変換エントリ、Internet Group Management Protocol (IGMP; インターネット グループ管理プロトコル)エントリ、所定のリソースの現在の使用状況、ピーク時の使用状況、および設定されたしきい値に関する Resource Manager MIB、ファイアウォール同期化の可否、コンテキストのキープアライブ、サービス モジュールのキープアライブ、およびパフォーマンス統計情報などが含まれる
シングル コンテキスト モードおよびマルチ コンテキスト モードでの SNMP トラップの追加	追加されたトラップには、設定されたリソースのしきい値を超えた場合、NAT/PAT エントリが枯渇した場合、Access Control List (ACL; アクセス コントロール リスト)メモリ スペースが枯渇した場合、CPU のしきい値を超えた場合、およびフェールオーバーが発生した場合の Resource Manager トラップなどが含まれる
TACACS+ によるコマンドの許可の改良	TACACS+ の文字列解析ロジックを Cisco IOS® ソフトウェアと類似したものにすることによって管理を容易にしている
システム コンテキストにおける Authentication, Authorization, and Accounting (AAA; 認証、許可、アカウントिंग)	Cisco Catalyst 6500 シリーズ スーパーバイザ エンジンから FWSM システム コンテキストのセッションを開始する管理者が、管理コンテキストからコマンドの認証と許可を継承できるようにする
<b>カットスルー プロキシ機能の強化</b>	
IP アドレスではなく DNS ホスト名による HTTP POST コマンド	カットスルー プロキシ ポリシーの柔軟性を向上させる
絶対的なユーザ認証タイマーが満了した場合のオプションとして、接続の切断を設定可能	より詳細な状態処理が可能になる
TACACS+ および RADIUS サーバでの期限切れパスワードの処理	期限切れパスワードを使用したユーザを識別して、別の Web ページにリダイレクトすることが可能
カスタマイズ可能なリダイレクト Web ページ	リダイレクト Web ページとして、Cisco FWSM に格納されたローカル ファイルを使用できる
再認証動作のオプション	ユーザが既に認証されている場合にユーザの認証状態を維持して、ユーザ名とパスワードの再入力を求めないようにすることができる
仮想 Secure Shell (SSH; セキュア シェル)のサポート	非 GUI 型の認証方式で、暗号化された証明書を使用する
<b>音声およびモバイル インспекション エンジンの機能強化</b>	
Real Time Streaming Protocol (RTSP) PAT	RTSP プロトコルで PAT をサポートする(すべての主要なメディア プレーヤーとの相互運用性に対応)
Session Initiation Protocol (SIP) 機能の強化	RTP ティアダウンおよびタイムアウトを適切に実施して、適正な課金やプロビジョニングを可能にする
H.323 ゲートキーパー クラスターの Gatekeeper Update Protocol (GUP) メッセージのサポート	Cisco Unified CallManager 4.1 および Cisco FWSM 間の相互運用を可能にする
グローバルな GPRS Support Node (GSN; GPRS サポート ノード)ロード バランシングに対応した GPRS Tunneling Protocol (GTP; GPRS トンネリング プロトコル)機能の強化	GTP インспекション エンジンがロード バランシング用に構成された有効な GSN に応答できるようにして、モバイル 3G ネットワークに対応したスケラビリティを実現する

## Cisco ASDM バージョン 5.2F リリースの重要点

Cisco ASDM バージョン 5.2F は、Cisco FWSM Software バージョン 3.2 の新しいすべての設定機能に加えて、Cisco ASDM バージョン 5.2 の新しい GUI、ポリシー テーブル、および Syslog の拡張機能をサポートしています。表 2 に、Cisco ASDM バージョン 5.2F の新機能を示します。

表 2 Cisco ASDM 5.2F の新機能

機能	利点
<b>新しいルール テーブル</b>	
ポリシー作成の簡素化	ACL 管理に必要なすべての項目に容易にアクセスできるようになっている(オブジェクトグループやポリシーの作成と変更、ポリシーの視覚化、オブジェクトグループ内の要素を展開表示するオプション、オブジェクトまたはオブジェクトグループの属性を表示する機能など)
ポリシー クエリー	ACL の高度な検索機能を管理者に提供
<b>Syslog の強化</b>	
ルール テーブルと Syslog の統合	Syslog からシングルクリックでルールを作成し、選択された ACL に基づいて生成される Syslog を即座に表示することができる。Syslog メッセージの説明と推奨される対処法を提供する
新しい Syslog ビューア	Syslog の解析によって日時、Syslog ID、および IP アドレスに基づいてビューをカスタマイズし、重大度に基づいてログを色分けできる
<b>設定サポートの改善</b>	
新しいオブジェクトグループ セレクタ パネルによる設定の簡素化	ネットワーク、サービス、プロトコル、および ICMP タイプのオブジェクトグループをすばやく編集できる

## 関連情報

詳細については、次の URL を参照してください。

- Cisco FWSM: <http://www.cisco.com/jp/product/hs/switches/cat6500/modules/service/fwsm/index.shtml>
- Cisco ASDM: <http://www.cisco.com/jp/go/asdm>
- Cisco Security Manager: <http://www.cisco.com/jp/product/hs/security/csm/index.shtml>

©2007 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、およびCisco Systemsロゴは、Cisco Systems, Inc.またはその関連会社の米国およびその他の一定の国における登録商標または商標です。

本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(0701R)

この資料に記載された仕様は予告なく変更する場合があります。



シスコシステムズ株式会社

〒107-0052 東京都港区赤坂2-14-27 国際新赤坂ビル東館

<http://www.cisco.com/jp>

お問い合わせ先(シスコ コンタクトセンター)

<http://www.cisco.com/jp/go/contactcenter>

0120-092-255 (通話料無料)

電話受付時間：平日 10:00～12:00、13:00～17:00

お問い合わせ先