



## Cisco Secure Firewall ASA の概要

Cisco Secure Firewall ASA は、高度なステートフル ファイアウォールおよび VPN コンセントレータ機能を 1 つのデバイスで提供します。ASA は、複数のセキュリティ コンテキスト（仮想ファイアウォールに類似）、クラスタリング（複数のファイアウォールを 1 つのファイアウォールに統合）、トランスペアレント（レイヤ 2）ファイアウォールまたはルーテッド（レイヤ 3）ファイアウォールオペレーション、高度なインスペクションエンジン、IPsec VPN、SSL VPN、クライアントレス SSL VPN サポートなど、多数の高度な機能を含みます。

- [ハードウェアとソフトウェアの互換性](#) (1 ページ)
- [VPN の互換性](#) (1 ページ)
- [新機能](#) (1 ページ)
- [ファイアウォール機能の概要](#) (5 ページ)
- [VPN 機能の概要](#) (10 ページ)
- [セキュリティ コンテキストの概要](#) (10 ページ)
- [ASA クラスタリングの概要](#) (11 ページ)
- [特殊なサービスおよびレガシー サービス](#) (11 ページ)

## ハードウェアとソフトウェアの互換性

サポートされるすべてのハードウェアおよびソフトウェアの一覧は、[『Cisco ASA Compatibility』](#)を参照してください。

## VPN の互換性

[『Supported VPN Platforms, Cisco ASA Series』](#)を参照してください。

## 新機能

このセクションでは、各リリースの新機能を示します。



(注) syslog メッセージガイドに、新規、変更済み、および廃止された syslog メッセージを記載しています。

## ASA 9.18(2) の新機能

リリース : 2022 年 8 月 10 日

機能	説明
インターフェイス機能	
BGP と管理トラフィックのループバック インターフェイスをサポート	<p>ループバック インターフェイスを追加して、次の機能に使用できるようになりました。</p> <ul style="list-style-type: none"> <li>• BGP</li> <li>• SSH</li> <li>• SNMP</li> <li>• Syslog</li> <li>• AAA</li> <li>• Telnet</li> </ul> <p>新規/変更されたコマンド : <b>interface loopback</b>、<b>logging host</b>、<b>neighbor update-source</b>、<b>snmp-server host</b>、<b>ssh</b>、<b>telnet</b></p>

## ASA 9.18(1) の新機能

リリース日 : 2022 年 6 月 6 日

機能	説明
プラットフォーム機能	
AWS GuardDuty の ASAv-AWS Security center integration	<p>Amazon GuardDuty サービスを ASAv と統合できるようになりました。この統合ソリューションは、Amazon GuardDuty によって報告された脅威分析データや結果（悪意のある IP アドレス）をキャプチャして処理するのに役立ちます。ASAv で悪意のある IP アドレスを設定およびフィードし、基盤となるネットワークとアプリケーションを保護できます。</p>

機能	説明
Alibaba の仮想展開	<p>これで、Alibaba Cloud に Secure Firewall ASA Virtual を展開できます。サポートされる機能は次のとおりです。</p> <ul style="list-style-type: none"> <li>• QCOW2 イメージパッケージ。</li> <li>• 基本的な製品の稼働。</li> <li>• Day-0 構成。</li> <li>• 公開キーまたはパスワードを使用した SSH。 デバッグ目的で ASA v にアクセスするための Alibaba UI コンソール。</li> <li>• Alibaba UI の停止/再起動。</li> <li>• サポートされているインスタンスタイプ : ecs.g5ne.large、ecs.g5ne.xlarge、ecs.g5ne.2xlarge、ecs.g5ne.4xlarge。</li> <li>• BYOL ライセンスのサポート。</li> </ul>
<b>ファイアウォール機能</b>	
ACL とオブジェクトの前方参照は常に有効にです。さらに、アクセス制御のオブジェクトグループ検索がデフォルトで有効になりました。	<p>アクセスグループまたはアクセスルールを設定するときに、まだ存在していない ACL またはネットワークオブジェクトを参照できます。</p> <p>さらに、オブジェクトグループ検索がアクセス制御に対してデフォルトで有効になりました。アップグレード後、オブジェクトグループ検索を無効にした場合、それは有効になりません。無効にする場合（非推奨）、手動で行う必要があります。</p> <p><b>forward-reference enable</b> コマンドを削除し、<b>object-group-search access-control</b> のデフォルトを有効に変更しました。</p>
<b>ルーティング機能</b>	
PBR のパスモニタリングメトリック。	<p>PBR はメトリックを使用して、トラフィックを転送するための最適なパス（出力インターフェイス）を決定します。パスモニタリングは、メトリックが変更されたモニタリング対象インターフェイスを PBR に定期的に通知します。PBR は、モニタリング対象インターフェイスの最新のメトリック値をパスモニタリングデータベースから取得し、データパスを更新します。</p> <p>新規/変更されたコマンド : <b>clear path-monitoring</b>、<b>policy-route</b>、<b>show path-monitoring</b></p>
<b>インターフェイス機能</b>	
Cisco Secure Firewall 3100 のフロー制御に対応するためのフレームの一時停止	<p>トラフィック バーストが発生している場合、バーストが NIC の FIFO バッファまたは受信リングバッファのバッファリング容量を超えると、パケットがドロップされる可能性があります。フロー制御用のポーズフレームをイネーブルにすると、このような問題の発生を抑制できます。</p> <p>新規/変更されたコマンド : <b>flowcontrol send on</b></p>

機能	説明
Secure Firewall 3130 および 3140 のブレイクアウトポート	Cisco Secure Firewall 3130 および 3140 の 40 GB インターフェースごとに 4 つの 10 GB ブレイクアウトポートを構成できるようになりました。 新規/変更されたコマンド : <b>breakout</b>
<b>ライセンス機能</b>	
キャリアライセンスの Secure Firewall 3100 サポート	キャリアライセンスは、Diameter、GTP/GPRS、SCTP 検査を有効にします。 新規/変更されたコマンド : <b>feature carrier</b>
<b>証明書の機能</b>	
相互 LDAPS 認証。	ASA が認証のために証明書を要求したときに LDAP サーバーに提示するように ASA のクライアント証明書を設定できます。この機能は、LDAP over SSL を使用する場合に適用されます。LDAP サーバーがピア証明書を要求するように設定されている場合、セキュア LDAP セッションが完了せず、認証/許可要求が失敗します。 新規/変更されたコマンド : <b>ssl-client-certificate</b>
認証 : 証明書名または SAN の検証	機能固有の参照 ID が設定されている場合、ピア証明書 ID は、指定された一致基準 <b>crypto ca reference-identity &lt;name&gt;</b> コマンドで検証されます。ピア証明書のサブジェクト名または SAN に一致するものが見つからない場合、または <b>reference-identity</b> サブモードコマンドで指定された FQDN が解決されない場合、接続は終了します。 <b>reference-identity</b> CLI は、AAA サーバーホスト設定および <b>ddns</b> 設定のサブモードコマンドとして設定されます。 新規/変更されたコマンド : <b>ldap-over-ssl</b> 、 <b>ddns update method</b> 、および <b>show update method</b> 。
<b>管理、モニタリング、およびトラブルシューティングの機能</b>	
複数の DNS サーバークラスタ	複数の DNS サーバークラスタを使用できるようになりました。1 つのグループがデフォルトで、他のグループを特定のドメインに関連付けることができます。DNS サーバークラスタに関連付けられたドメインに一致する DNS 要求は、そのグループを使用します。たとえば、内部の <b>eng.cisco.com</b> サーバークラスタ宛てのトラフィックで内部の DNS サーバークラスタを使用する場合は、 <b>eng.cisco.com</b> を内部の DNS グループにマッピングできます。ドメインマッピングと一致しないすべての DNS 要求は、関連付けられたドメインを持たないデフォルトの DNS サーバークラスタを使用します。たとえば、 <b>DefaultDNS</b> グループには、外部インターフェイスで使用可能なパブリック DNS サーバークラスタを含めることができます。 新規/変更されたコマンド : <b>dns-group-map</b> 、 <b>dns-to-domain</b>

機能	説明
ダイナミックログインのレート制限	ブロック使用量が指定されたしきい値を超えたときにログインレートを制限する新しいオプションが追加されました。ブロックの使用量が通常の値に戻るとレート制限が無効になるため、ログインレートが動的に制限されます。 新規/変更されたコマンド： <b>logging rate-limit</b>
Secure Firewall 3100 デバイスのパケットキャプチャ	スイッチパケットをキャプチャするプロビジョニングが追加されました。このオプションは、Secure Firewall 3100 デバイスに対してのみ有効にできます。 新規/変更されたコマンド： <b>capture real-time</b>
<b>VPN 機能</b>	
IPsec フローがオフロードされません。	Cisco Secure Firewall 3100 では、IPsec フローはデフォルトでオフロードされます。IPsec サイト間 VPN またはリモートアクセス VPN セキュリティ アソシエーション (SA) の初期設定後、IPsec 接続はデバイスのフィールドプログラマブルゲートアレイ (FPGA) にオフロードされるため、デバイスのパフォーマンスが向上します。 新規/変更されたコマンド： <b>clear flow-offload-ipsec</b> 、 <b>flow-offload-ipsec</b> 、 <b>show flow-offload-ipsec</b>
認証用の証明書と SAML	証明書および SAML 認証用にリモートアクセス VPN 接続プロファイルを設定できます。ユーザーは、SAML 認証/承認が開始される前に、マシン証明書やユーザー証明書を認証するように VPN を設定できます。これは、ユーザー固有の SAML DAP 属性と DAP 証明書属性を使用して実行できます。 新規/変更されたコマンド： <b>authentication saml certificate</b> 、 <b>authentication certificate saml</b> 、 <b>authentication multiple-certificate saml</b>

## ファイアウォール機能の概要

ファイアウォールは、外部ネットワーク上のユーザーによる不正アクセスから内部ネットワークを保護します。また、ファイアウォールは、人事部門ネットワークをユーザーネットワークから分離するなど、内部ネットワーク同士の保護も行います。Web サーバーまたは FTP サーバーなど、外部のユーザーが使用できるようにする必要のあるネットワーク リソースがあれば、ファイアウォールで保護された別のネットワーク（非武装地帯（DMZ）と呼ばれる）上に配置します。ファイアウォールによって DMZ に許可されるアクセスは限定されますが、DMZ にあるのは公開サーバーだけのため、この地帯が攻撃されても影響を受けるのは公開サーバーに限定され、他の内部ネットワークに影響が及ぶことはありません。また、特定アドレスだけに許可する、認証または認可を義務づける、または外部の URL フィルタリング サーバーと協調するといった手段によって、内部ユーザーが外部ネットワーク（インターネットなど）にアクセスする機会を制御することもできます。

ファイアウォールに接続されているネットワークに言及する場合、外部ネットワークはファイアウォールの手前にあるネットワーク、内部ネットワークはファイアウォールの背後にある保

護されているネットワーク、そして **DMZ** はファイアウォールの背後にあるが、外部ユーザーに制限付きのアクセスが許されているネットワークです。ASA を使用すると、数多くのインターフェイスに対してさまざまなセキュリティポリシーが設定できます。このインターフェイスには、多数の内部インターフェイス、多数の DMZ、および必要に応じて多数の外部インターフェイスが含まれるため、ここでは、このインターフェイスの区分は一般的な意味で使用するだけです。

## セキュリティポリシーの概要

他のネットワークにアクセスするために、ファイアウォールを通過することが許可されるトラフィックがセキュリティポリシーによって決められます。デフォルトでは、内部ネットワーク（高セキュリティレベル）から外部ネットワーク（低セキュリティレベル）へのトラフィックは、自由に流れることが ASA によって許可されます。トラフィックにアクションを適用してセキュリティポリシーをカスタマイズすることができます。

### アクセスルールによるトラフィックの許可または拒否

アクセスルールを適用することで、内部から外部に向けたトラフィックを制限したり、外部から内部に向けたトラフィックを許可したりできます。ブリッジグループインターフェイスでは、EtherType アクセスルールを適用して、非 IP トラフィックを許可できます。

### NAT の適用

NAT の利点のいくつかを次に示します。

- 内部ネットワークでプライベートアドレスを使用できます。プライベートアドレスは、インターネットにルーティングできません。
- NAT はローカルアドレスを他のネットワークから隠蔽するため、攻撃者はホストの実際のアドレスを取得できません。
- NAT は、重複 IP アドレスをサポートすることで、IP ルーティングの問題を解決できます。

### IP フラグメントからの保護

ASA は、IP グラグメント保護を提供します。この機能は、すべての ICMP エラーメッセージの完全なリアセンブリと、ASA 経由でルーティングされる残りの IP フラグメントの仮想リアセンブリを実行します。セキュリティチェックに失敗したフラグメントは、ドロップされログに記録されます。仮想リアセンブリはディセーブルにできません。

### HTTP、HTTPS、または FTP フィルタリングの適用

アクセスリストを使用して、特定の Web サイトまたは FTP サーバーへの発信アクセスを禁止できますが、このような方法で Web サイトの使用方法を設定し管理することは、インターネットの規模とダイナミックな特性から、実用的とはいえません。

ASA でクラウド Web セキュリティを設定できます。ASA は、Cisco Web セキュリティ アプライアンス (WSA) などの外部製品とともに使用することも可能です。

## アプリケーションインスペクションの適用

インスペクションエンジンは、ユーザーのデータ パケット内に IP アドレッシング情報を埋め込むサービスや、ダイナミックに割り当てられるポート上でセカンダリチャネルを開くサービスに必要です。これらのプロトコルは、ASA によるディープ パケット インスペクションの実行を必要とします。

## QoS ポリシーの適用

音声やストリーミング ビデオなどのネットワーク トラフィックでは、長時間の遅延は許容されません。QoS は、この種のトラフィックにプライオリティを設定するネットワーク機能です。QoS とは、選択したネットワーク トラフィックによりよいサービスを提供するネットワークの機能です。

## 接続制限と TCP 正規化の適用

TCP 接続、UDP 接続、および初期接続を制限することができます。接続と初期接続の数を制限することで、DoS 攻撃（サービス拒絶攻撃）から保護されます。ASA では、初期接続の制限を利用して TCP 代行受信を発生させます。代行受信によって、TCP SYN パケットを使用してインターフェイスをフラッドする DoS 攻撃から内部システムを保護します。初期接続とは、送信元と宛先の間で必要になるハンドシェイクを完了していない接続要求のことです。

TCP 正規化は、正常に見えないパケットをドロップするように設計された高度な TCP 接続設定で構成される機能です。

## 脅威検出のイネーブル化

スキャン脅威検出と基本脅威検出、さらに統計情報を使用して脅威を分析する方法を設定できます。

基本脅威検出は、DoS 攻撃などの攻撃に関係している可能性のあるアクティビティを検出し、自動的にシステム ログ メッセージを送信します。

典型的なスキャン攻撃では、あるホストがサブネット内の IP アドレスにアクセスできるかどうかを 1 つずつ試みます（サブネット内の複数のホストすべてを順にスキャンするか、1 つのホストまたはサブネットの複数のポートすべてを順にスイープする）。スキャン脅威検出機能は、いつホストがスキャンを実行するかを判別します。トラフィック署名に基づく IPS スキャン検出とは異なり、ASA のスキャン脅威検出機能は、スキャン アクティビティに関して分析できるホスト統計を含む膨大なデータベースを維持します。

ホスト データベースは、不審なアクティビティを追跡します。このようなアクティビティには、戻りアクティビティのない接続、閉じているサービス ポートへのアクセス、脆弱な TCP 動作（非ランダム IPID など）、およびその他の多くの動作が含まれます。

攻撃者に関するシステム ログ メッセージを送信するように ASA を設定できます。または、自動的にホストを排除できます。

## ファイアウォール モードの概要

ASA は、次の 2 つのファイアウォール モードで動作します。

- ルーテッド
- トランスペアレント

ルーテッドモードでは、ASA は、ネットワークのルータ ホップと見なされます。

トランスペアレントモードでは、ASA は「Bump In The Wire」または「ステルス ファイアウォール」のように動作し、ルータホップとは見なされません。ASA は「ブリッジグループ」の内部および外部インターフェイスと同じネットワークに接続します。

トランスペアレントファイアウォールは、ネットワーク コンフィギュレーションを簡単にするために使用できます。トランスペアレントモードは、攻撃者からファイアウォールが見えないようにする場合にも有効です。トランスペアレントファイアウォールは、他の場合にはルーテッドモードでブロックされるトラフィックにも使用できます。たとえば、トランスペアレントファイアウォールでは、EtherType アクセスリストを使用するマルチキャストストリームが許可されます。

ルーテッドモードでブリッジグループの設定、およびブリッジグループと通常インターフェイスの間のルートの設定を行えるように、ルーテッドモードでは Integrated Routing and Bridging をサポートしています。ルーテッドモードでは、トランスペアレントモードの機能を複製できます。マルチコンテキストモードまたはクラスタリングが必要ではない場合、代わりにルーテッドモードを使用することを検討してください。

## ステートフル インспекションの概要

ASA を通過するトラフィックはすべて、アダプティブセキュリティアルゴリズムを使用して検査され、通過が許可されるか、またはドロップされます。単純なパケットフィルタは、送信元アドレス、宛先アドレス、およびポートが正しいかどうかはチェックできますが、パケットシーケンスまたはフラグが正しいかどうかはチェックしません。また、フィルタはすべてのパケットをフィルタと照合してチェックするため、処理が低速になる場合があります。



(注) TCP ステートバイパス機能を使用すると、パケットフローをカスタマイズできます。

ただし、ASA のようなステートフルファイアウォールは、パケットの次のようなステートについて検討します。

- 新規の接続かどうか。

新規の接続の場合、ASA は、パケットをアクセスリストと照合してチェックする必要があり、これ以外の各種のタスクを実行してパケットの許可または拒否を決定する必要があります。



ります。このチェックを行うために、セッションの最初のパケットは「セッション管理パス」を通過しますが、トラフィックのタイプに応じて、「コントロールプレーンパス」も通過する場合があります。

セッション管理パスで行われるタスクは次のとおりです。

- アクセスリストとの照合チェック
- ルートルックアップ
- NAT変換 (xlates) の割り当て
- 「ファストパス」でのセッションの確立

ASAは、TCPトラフィックのファストパスに転送フローとリバースフローを作成します。ASAは、高速パスも使用できるように、UDP、ICMP (ICMPインスペクションがイネーブルの場合) などのコネクションレス型プロトコルの接続状態の情報も作成するので、これらのプロトコルもファストパスを使用できます。



- (注) SCTPなどの他のIPプロトコルの場合、ASAはリバースパスフローを作成しません。そのため、これらの接続を参照するICMPエラーパケットはドロップされます。

レイヤ7インスペクションが必要なパケット (パケットのペイロードの検査または変更が必要) は、コントロールプレーンパスに渡されます。レイヤ7インスペクションエンジンは、2つ以上のチャネルを持つプロトコルが必要です。2つ以上のチャネルの1つは周知のポート番号を使用するデータチャネルで、その他はセッションごとに異なるポート番号を使用するコントロールチャネルです。このようなプロトコルには、FTP、H.323、およびSNMPがあります。

- 確立済みの接続かどうか。

接続がすでに確立されている場合は、ASAでパケットの再チェックを行う必要はありません。一致するパケットの大部分は、両方向で「ファースト」パスを通過できます。高速パスで行われるタスクは次のとおりです。

- IPチェックサム検証
- セッションルックアップ
- TCPシーケンス番号のチェック
- 既存セッションに基づく NAT変換
- レイヤ3ヘッダー調整およびレイヤ4ヘッダー調整

レイヤ7インスペクションを必要とするプロトコルに合致するデータパケットも高速パスを通過できます。

確立済みセッションパケットの中には、セッション管理パスまたはコントロールプレーンパスを引き続き通過しなければならないものがあります。セッション管理パスを通過するパケットには、インスペクションまたはコンテンツフィルタリングを必要とする HTTP パケットが含まれます。コントロールプレーンパスを通過するパケットには、レイヤ 7 インスペクションを必要とするプロトコルのコントロールパケットが含まれます。

## VPN 機能の概要

VPN は、TCP/IP ネットワーク（インターネットなど）上のセキュアな接続で、プライベートな接続として表示されます。このセキュアな接続はトンネルと呼ばれます。ASA は、トンネリングプロトコルを使用して、セキュリティパラメータのネゴシエート、トンネルの作成および管理、パケットのカプセル化、トンネルを通じたパケットの送信または受信、パケットのカプセル化の解除を行います。ASA は、双方向トンネルのエンドポイントとして機能します。たとえば、プレーンパケットを受信してカプセル化し、それをトンネルのもう一方のエンドポイントに送信することができます。そのエンドポイントで、パケットはカプセル化を解除され、最終的な宛先に送信されます。また、セキュリティアプライアンスは、カプセル化されたパケットを受信してカプセル化を解除し、それを最終的な宛先に送信することもできます。ASA は、これらの機能を実行するためにさまざまな標準プロトコルを起動します。

ASA は、次の機能を実行します。

- トンネルの確立
- トンネルパラメータのネゴシエーション
- ユーザーの認証
- ユーザーアドレスの割り当て
- データの暗号化と復号化
- セキュリティキーの管理
- トンネルを通じたデータ転送の管理
- トンネルエンドポイントまたはルータとしての着信と発信のデータ転送の管理

ASA は、これらの機能を実行するためにさまざまな標準プロトコルを起動します。

## セキュリティコンテキストの概要

単一の ASA は、セキュリティコンテキストと呼ばれる複数の仮想デバイスにパーティション化できます。各コンテキストは、独自のセキュリティポリシー、インターフェイス、および管理者を持つ独立したデバイスです。マルチコンテキストは、複数のスタンドアロンデバイスを使用することに似ています。マルチコンテキストモードでは、ルーティングテーブル、ファイアウォール機能、IPS、管理など、さまざまな機能がサポートされています。ただし、サポートされていない機能もあります。詳細については、機能に関する各章を参照してください。

マルチ コンテキスト モードの場合、ASA には、セキュリティ ポリシー、インターフェイス、およびスタンドアロンデバイスで設定できるほとんどのオプションを識別するコンテキストごとのコンフィギュレーションが含まれます。システム管理者がコンテキストを追加および管理するには、コンテキストをシステムコンフィギュレーションに設定します。これが、シングルモード設定と同じく、スタートアップコンフィギュレーションとなります。システムコンフィギュレーションは、ASA の基本設定を識別します。システム コンフィギュレーションには、ネットワーク インターフェイスやネットワーク設定は含まれません。その代わりに、ネットワークリソースにアクセスする必要があるときに（サーバーからコンテキストをダウンロードするなど）、システムは管理コンテキストとして指定されているコンテキストのいずれかを使用します。

管理コンテキストは、他のコンテキストとまったく同じです。ただし、ユーザーが管理コンテキストにログインすると、システム管理者権限を持つので、システムコンテキストおよび他のすべてのコンテキストにアクセス可能になる点が異なります。

## ASA クラスタリングの概要

ASA クラスタリングを利用すると、複数の ASA をグループ化して、1 つの論理デバイスにすることができます。クラスタは、単一デバイスのすべての利便性（管理、ネットワークへの統合）を備える一方で、複数デバイスによって高いスループットおよび冗長性を達成します。

すべてのコンフィギュレーション作業（ブートストラップ コンフィギュレーションを除く）は、制御ユニット上でのみ実行します。コンフィギュレーションは、メンバーユニットに複製されます。

## 特殊なサービスおよびレガシー サービス

一部のサービスのマニュアルは、主要な設定ガイドおよびオンラインヘルプとは別の場所にあります。

### 特殊なサービスに関するガイド

特殊なサービスを利用して、たとえば、電話サービス（Unified Communications）用のセキュリティプロキシを提供したり、ボットネットトラフィックフィルタリングを Cisco アップデート サーバーのダイナミック データベースと組み合わせて提供したり、Cisco Web セキュリティアプライアンス用の WCCP サービスを提供したりすることにより、ASA と他のシスコ製品の相互運用が可能になります。これらの特殊なサービスの一部については、別のガイドで説明されています。

- [『Cisco ASA Botnet Traffic Filter Guide』](#)
- [『Cisco ASA NetFlow Implementation Guide』](#)
- [『Cisco ASA Unified Communications Guide』](#)
- [『Cisco ASA WCCP Traffic Redirection Guide』](#)

- [『SNMP Version 3 Tools Implementation Guide』](#)

#### レガシー サービス ガイド

レガシー サービスは現在も ASA でサポートされていますが、より高度なサービスを代わりに使用できる場合があります。レガシー サービスについては別のガイドで説明されています。

#### [『Cisco ASA Legacy Feature Guide』](#)

このマニュアルの構成は、次のとおりです。

- RIP の設定
- ネットワーク アクセスの AAA 規則
- IP スプーフィングの防止などの保護ツールの使用 (**ip verify reverse-path**)、フラグメントサイズの設定 (**fragment**)、不要な接続のブロック (**shun**)、TCP オプションの設定 (ASDM 用)、および基本 IPS をサポートする IP 監査の設定 (**ip audit**)。
- フィルタリング サービスの設定

## 翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。