# 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

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 9.20(4) の新機能

リリース：**2025 年 7 月 2 日**

| 機能 | 説明 |
|---|---|
| **ライセンス機能** | |
| Smart Transport はスマートライセンスのデフォルトの転送です | スマートライセンスでは現在、デフォルトの転送として Smart Transport を使用しています。必要に応じて、旧タイプの Smart Call Home を任意で有効にできます。<br>新規/変更されたコマンド：**transport proxy**、**transport type**、**transport url**<br>*9.22(1)* でも同様です。 |
| **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** | |
| SSH X.509 証明書認証 | X.509v3 証明書を使用して SSH のユーザーを認証できるようになりました（RFC 6187）。<br>Firepower 4100/9300 の場合、FXOS バージョン 2.16（2.109 以降）または 2.18 以降が必要です。<br>（注）<br>ASDM 7.20(4) のバンドルバージョンには、この機能のサポートは含まれていません。機能をサポートするには、Cisco.com から ASDM 7.20(4) をダウンロードしてインストールしてください。バンドルバージョンを上書きする場合は、必ずイメージ名を asdm.bin に変更してください。<br>新規/変更されたコマンド：**aaa authorization exec ssh-x509**、**ssh authentication method**、**ssh trustpoint sign**、**ssh username-from-certificate**、**validation-usage ssh-client**<br>*9.22(3)*、*9.24(1)* でも同様です。 |
| AES-256-GCM SSH 暗号 | ASA は、SSH の AES-256-GCM 暗号をサポートしています。デフォルトでは、暗号化レベル [すべて（all）] と [高（high）] で有効になっています。<br>新規/変更されたコマンド： **ssh cipher encryption**<br>*9.22(3)*、*9.24(1)* でも同様です。 |

| 機能 | 説明 |
|---|---|
| 接続ステータス出力での UDP のイニシエータおよびレスポンダ値の表示 | UDP トラフィックフローの場合、Cisco ASA は接続の詳細ステータスにイニシエータおよび応答側フィールド値を表示します。これらのフィールド値は通信の方向を示すため、ネットワーク接続の問題のトラブルシュートに役立ちます。<br>新規/変更されたコマンド： **show conn detail** |

# ASA 9.20(3) の新機能

リリース日：**2024 年 7 月 31 日**

| 機能 | 説明 |
|---|---|
| **プラットフォーム機能** | |
| ASA 仮想 AWS IMDSv2 のサポート | AWS Instance Metadata Service バージョン 2（IMDSv2）の API が ASA 仮想でサポートされるようになりました。これにより、インスタンスメタデータを取得して検証できます。IMDSv2 は、インスタンス メタデータ サービスをターゲットにした脆弱性に対して追加のセキュリティを提供します。ASA 仮想 を AWS に展開するときに、ASA 仮想のメタデータバージョンを次のように設定できるようになりました。<br>• ASA 仮想 9.20(3) 以降では IMDSv2 のみをサポート（トークンが必要）：IMDSv2 を有効にするには、[V2のみ（トークンが必要）（V2 only (token required)）] を設定します。<br>• ASA 仮想 の以前のバージョンでは、IMDS オプション [IMDSv1またはIMDSv2（トークンはオプション）（IMDSv1 or IMDSv2 (token optional)）] を介して IMDSv1 API のみをサポート：[V1およびV2（トークンはオプション）（V1 and V2 (token optional)）] を設定します。<br>既存の ASA 仮想 展開がある場合は、9.20(3) 以降にアップグレードした後で「IMDSv2 必須」モードに移行できます。AWS のドキュメント（https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/configuring-instance-metadata-options.html）を参照してください<br>詳細については、『Cisco Secure Firewall ASA Virtual Getting Started Guide, 9.20』を参照してください。 |
| **ファイアウォール機能** | |

| 機能 | 説明 |
|---|---|
| VPN サービスの脅威検出 | VPN サービスの脅威検出を設定して、IPv4 アドレスからの次のタイプの VPN 攻撃に対して保護できます。<br>• リモートアクセス VPN への過剰な認証失敗の試行（ユーザー名/パスワードをスキャンするブルートフォース攻撃など）。<br>• クライアント初期化攻撃。攻撃者は単一のホストからリモートアクセス VPN ヘッドエンドへの接続試行を繰り返し開始しますが、完了しません。<br>• 無効な VPN サービス、つまり内部専用サービスへのアクセス試行。<br>アクセスに失敗したとしても、これらの攻撃によってコンピューティングリソースを消費し、場合によってはサービス拒否（DoS）を引き起こす可能性があります。<br>**clear threat-detection service**、**show threat-detection service**、**shun**、**threat-detection service** の各コマンドが導入または変更されました。 |
| **VPN 機能** | |
| webvpn コンフィギュレーションおよび tunnel-group 内の複数の IdP 証明書 | webvpn コンフィギュレーションで、トンネルグループ固有の IdP 証明書および複数の IdP 証明書を設定できるようになりました。この機能を使用すると、新しい証明書だけでなく古い証明書も信頼できるようになるため、新しい証明書への移行が容易になります。<br>新規/変更されたコマンド：**saml idp-trustpoint**、**trustpoint idp** |
| 事前認証済み SSL 接続のレート制限 | ASA 仮想 は、事前認証された SSL 接続のレートを制限できます。この制限は、デバイスの VPN 接続制限の 3 倍として計算されます。この制限を超えると、新しい SSL 接続は許可されません。デバイスは、事前認証された SSL 接続数がゼロになった後にのみ、新しい SSL 接続を許可します。ただし、この制限は管理接続には適用されません。<br>新規/変更されたコマンド： **show counters** |

# ASA 9.20(2) の新機能

リリース日：**2023 年 12 月 13 日**

| 機能 | 説明 |
|---|---|
| **プラットフォーム機能** | |
| Cisco Secure Firewall 3100 における 100GB ネットワークモジュールのサポート | Cisco Secure Firewall 3100 で 100GB のネットワークモジュールを使用できるようになりました。このモジュールは、Cisco Secure Firewall 4200 でもサポートされています。 |

| 機能 | 説明 |
|---|---|
| Cisco Secure Firewall 4200 の接続制限の引き上げ | 最大接続数が引き上げられました。<br>• 4215：15M → **40M**<br>• 4225：30M → **80M**<br>• 4245：60M → **80M** |
| OCI 上の ASAv：追加のインスタンス | OCI 上の ASA 仮想インスタンスは、最高のパフォーマンスとスループットレベルを達成するために追加のシェイプをサポートするようになりました。 |
| **ハイ アベイラビリティとスケーラビリティの各機能** | |
| Azure 上の ASAv：ゲートウェイロード バランシングによるクラスタリング | Azure Resource Manager（ARM）テンプレートを使用した Azure での ASA 仮想クラスタリングの展開がサポートされるようになり、ネットワークトラフィックのロードバランシングにゲートウェイロードバランサ（GWLB）を使用するように ASAv クラスタが設定されています。<br>新しい/変更されたコマンド： |
| AWS 上の ASAv：ゲートウェイロード バランシングによるクラスタリングの復元力 | AWS のターゲットグループサービスでターゲット フェールオーバー オプションを設定できます。これにより、仮想インスタンスのフェールオーバーが発生した場合に GWLB が既存のフローを正常なターゲットに転送できます。ASAv クラスタリングでは、各インスタンスがターゲットグループに関連付けられ、ターゲット フェールオーバー オプションが有効になっています。これは、GWLB が異常なターゲットを識別して、ターゲットグループ内のターゲットノードとして識別または登録されている正常なインスタンスにネットワークトラフィックをリダイレクトまたは転送するのに役立ちます。 |
| シャーシハートビート障害後にクラスタに再参加するための設定可能な遅延（Firepower 4100/9300） | デフォルトでは、シャーシハートビート障害から回復すると、ノードはすぐにクラスタに再参加します。ただし、**health-check chassis-heartbeat-delay-rejoin** コマンドを設定すると、**health-check system auto-rejoin** コマンドの設定に従って再参加します。<br>新規/変更されたコマンド： **health-check chassis-heartbeat-delay-rejoin** |
| **show failover statistics** にクライアント統計情報を追加 | フェールオーバー クライアントのパケット統計情報が拡張され、デバッグ機能が向上しました。**show failover statistics** コマンドは、**np-clients**（データパスクライアント）および **cp-clients**（コントロールプレーン クライアント）の情報を表示するように拡張されています。<br>変更されたコマンド：**show failover statistics cp-clients**、**show failover statistics np-clients**<br>*9.18(4)* でも同様です。 |

| 機能 | 説明 |
|---|---|
| **show failover statistics events** に新しいイベントを追加 | **show failover statistics events** コマンドが拡張され、アプリケーション エージェントによって通知されるローカル障害（フェールオーバーリンクの稼働時間、スーパーバイザハートビート障害、およびディスクフルの問題）を表示するようになりました。<br>変更されたコマンド： **show failover statistics events**<br>*9.18(4)* でも同様です。 |

# ASA 9.20(1) の新機能

リリース：**2023** 年 **9** 月 **7** 日

（注） このリリースは、Cisco Secure Firewall 4200 でのみサポートされます。

| 機能 | 説明 |
|---|---|
| **プラットフォーム機能** | |
| Cisco Secure Firewall 4200 | Cisco Secure Firewall 4215、4225、および 4245 向けの ASA を導入しました。Cisco Secure Firewall 4200 は、スパンド EtherChannel クラスタリングで最大 8 ユニットをサポートします。ファイアウォールの電源が入っているときに、再起動することなく、同じタイプのネットワークモジュールをホットスワップできます。他のモジュールの変更を行う場合には、再起動が必要です。Cisco Secure Firewall 4200 の 25 Gbps 以上のインターフェイスは、Forward Error Correction と、インストールされている SFP に基づく速度検出をサポートします。SSD は自己暗号化ドライブ（SED）です。SSD が 2 つある場合、ソフトウェア RAID を形成します。管理インターフェイスが 2 つあります。 |
| **ファイアウォール機能** | |
| データプレーンにオフロードされた ASP ルールエンジンのコンパイル。 | デフォルトでは、ルールベースのポリシー（ACL、NAT、VPN など）に 100 を超えるルール更新がある場合、ASP ルールエンジンのコンパイルはコントロールプレーンではなくデータプレーンにオフロードされます。このオフロードにより、コントロールプレーンで他のタスクを実行する時間が長くなります。<br>次のコマンドが追加または変更されました。**asp rule-engine compile-offload**、**show asp rule-engine**。 |

| 機能 | 説明 |
|---|---|
| データプレーンのクイックリロード | データプレーンを再起動する必要がある場合、デバイスを再起動する代わりに、データプレーンプロセスをリロードできるようになりました。データプレーンのクイックリロードを有効にすると、データプレーンとその他のプロセスが再起動されます。<br>新規/変更されたコマンド：**data-plane quick-reload**、**show data-plane quick-reload status**。 |
| **ハイ アベイラビリティとスケーラビリティの各機能** | |
| ASA の高可用性のための偽フェールオーバーの削減 | ASA 高可用性のデータプレーンに追加のハートビートモジュールが導入されました。このハートビートモジュールは、コントロールプレーンのトラフィックの輻輳や CPU の過負荷が原因で発生する可能性のある、偽フェールオーバーやスプリットブレインシナリオを回避するのに役立ちます。<br>*9.18(4)* でも同様です。 |
| フローステータスの設定可能なクラスタキープアライブ間隔 | フローオーナーは、キープアライブ（clu_keepalive メッセージ）と更新（clu_update メッセージ）をディレクタおよびバックアップオーナーに送信して、フローの状態を更新します。キープアライブ間隔を設定できるようになりました。デフォルトは 15 秒で、15 ～ 55 秒の範囲で間隔を設定できます。クラスタ制御リンクのトラフィック量を減らすために長い間隔を設定できます。<br>新規/変更されたコマンド： **clu-keepalive-interval** |
| **ルーティング機能** | |
| EIGRPv6 | EIGRP for IPv6 を設定し、それらを個別に管理できるようになりました。各インターフェイスで EIGRP を設定するときは、IPv6 を明示的に有効にする必要があります。<br>新規/変更されたコマンド：新しく導入されたコマンドは、次のとおりです。**ipv6 eigrp**、**ipv6 hello-interval eigrp**、**ipv6 hold-time eigrp**、**ipv6 split-horizon eigrp**、**show ipv6 eigrp interface** 、**show ipv6 eigrp traffic**、**show ipv6 eigrp neighbors** 、**show ipv6 eigrp interface**、**ipv6 summary-address eigrp**、**show ipv6 eigrp topology**、**show ipv6 eigrp events** 、**show ipv6 eigrp timers**、**clear ipv6 eigrp**、および **clear ipv6 router eigrp**<br>IPv6 をサポートするため、次のコマンドが変更されました。**default-metric**、**distribute-list prefix-list**、**passive-interface**、**eigrp log-neighbor-warnings**、**eigrp log-neighbor-changes**、**eigrp router-id**、および **eigrp stub** |
| **インターフェイス機能** | |
| VXLAN VTEP IPv6 のサポート | VXLAN VTEP インターフェイスに IPv6 アドレスを指定できるようになりました。IPv6 では、ASA 仮想 クラスタ制御リンクまたは Geneve カプセル化がサポートされていません。<br>新規/変更されたコマンド：**default-mcast-group**、**mcast-group**、**peer ip** |

| 機能 | 説明 |
|---|---|
| DNS、HTTP、ICMP、IPsec フローオフロードのループバックインターフェイスのサポート | ループバックインターフェイスを追加して、以下に使用できるようになりました。<br>• DNS<br>• HTTP<br>• ICMP<br>• IPsec フローのオフロード |
| **ライセンス機能** | |
| スマートライセンスや Smart Call Home といったクラウドサービスの IPv6 | ASA は、スマートライセンスや Smart Call Home などのクラウドサービスの IPv6 をサポートするようになりました。 |
| **証明書の機能** | |
| OCSP および CRL の IPv6 PKI | ASA で、IPv4 と IPv6 両方の OCSP および CRL URL をサポートするようになりました。URL で IPv6 を使用する場合は、角カッコで囲む必要があります。<br>新規/変更されたコマンド：**crypto ca trustpointcrl**、**cdp url**、**ocsp url** |
| **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** | |
| SNMP syslog のレート制限 | システム全体のレート制限を設定しない場合、SNMP サーバーに送信される syslog に対して個別にレート制限を設定できるようになりました。<br>新規/変更されたコマンド： **logging history rate-limit** |
| スイッチのパケットキャプチャ | スイッチの出力および入力トラフィックパケットをキャプチャするように設定できるようになりました。このオプションは、Secure Firewall 4200 モデルデバイスに対してのみ使用できます。<br>新しい/変更されたコマンド：<br>**capture** *capture_name* **switch interface** *interface_name* [ **direction** { **both** \| **egress** \| **ingress** } ] |
| **VPN 機能** | |

| 機能 | 説明 |
|---|---|
| 暗号デバッグの機能拡張 | 暗号デバッグの機能拡張は次のとおりです。<br>• 暗号アーカイブは、テキスト形式とバイナリ形式の 2 つの形式で使用できるようになりました。<br>• 追加の SSL カウンタ。<br>• スタックした暗号化ルールは、デバイスを再起動せずにASPテーブルから削除できます。<br>新しい/変更されたコマンド：<br>• **show counters** |
| IKEv2 の複数のキー交換 | ASA は、量子コンピュータ攻撃から IPsec 通信を保護するために、IKEv2 で複数のキー交換をサポートします。<br>新規/変更されたコマンド： **additional-key-exchange** |

# 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ディングする 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 つずつ試します（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 のスキャニング脅威検出機能は、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 インスペクションの概要

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。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で必要です。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、トンネルを通し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
- トンネルを通し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生じたときに（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。

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。