Cisco ASA の概要

Cisco ASA は、追加モジュールとの統合サービスに加え、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（Cisco ASA の互換性）』[英語] を参照してください。

VPN の互換性

『Supported VPN Platforms, Cisco ASA Series』[英語] 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 9.6(4) の新機能

リリース：2017年12月13日

このリリースに新機能はありません。

ASA 9.6(3.1) の新機能

リリース：2017年4月3日

（注） バージョン 9.6(3) は、バグ CSCvd78303 に基づき Cisco.com から削除されました。

機能	説明
AAA 機能	
SSH公開キー認証を使用するユーザの認証とパスワードを使用するユーザの認証を区別します。	9.6(2) より前のリリースでは、ローカル ユーザ データベース（**ssh authentication**）を使用して AAA SSH 認証を明示的に有効にしなくても、SSH 公開キー認証（**aaa authentication ssh console LOCAL**）を有効にすることができました。9.6(2) では、ASA で AAA SSH 認証を明示的に有効にする必要がありました。このリリースでは、AAA SSH 認証を明示的に有効にする必要はありません。ユーザに対して **ssh authentication** コマンドを設定すると、このタイプの認証を使用するユーザのローカル認証がデフォルトで有効になります。さらに、明示的に AAA SSH 認証を設定すると、この設定はパスワード付きのユーザ名にのみ適用されます。また、任意の AAA サーバ タイプ（**aaa authentication ssh console radius_1** など）を使用できます。たとえば、一部のユーザはローカル データベースを使用して公開キー認証を使用し、他のユーザは RADIUS でパスワードを使用できます。 変更されたコマンドはありません。

ASA 9.6(2) の新機能

リリース：**2016年8月24日**

機能	説明
プラットフォーム機能	
Firepower 4150 用の ASA を導入しました。	Firepower 4150 用の ASA を導入しました。 FXOS 2.0.1 が必要です。 追加または変更されたコマンドはありません。
ASAv のホット プラグ インターフェイス	システムがアクティブの状態で、ASAv の Virtio 仮想インターフェイスを追加または削除できます。ASAv に新しいインターフェイスを追加すると、仮想マシンがインターフェイスを検出し、プロビジョニングが行われます。既存のインターフェイスを削除すると、仮想マシンはインターフェイスに関連付けられているリソースを解放します。ホットプラグインターフェイスはカーネルベース仮想マシン（KVM）のハイパーバイザ上にある Virtio 仮想インターフェイスに制限されます。
ASAv10 での Microsoft Azure サポート	Microsoft Azure は、プライベート Microsoft Hyper V ハイパーバイザを使用するパブリック クラウド環境です。ASAv は、Hyper V ハイパーバイザの Microsoft Azure 環境でゲストとして実行されます。Microsoft Azure 上の ASAv は、4 つの vCPU、14 GB、4 つのインターフェイスをサポートする Standard D3 の 1 つのインスタンス タイプをサポートします。 バージョン *9.5(2.200)* でも同様です。
ASAv の管理 0/0 インターフェイスでの通過トラフィック サポート	ASAv の管理 0/0 インターフェイスでトラフィックを通過させることができるようになりました。以前は、Microsoft Azure 上の ASAv のみで通過トラフィックをサポートしていました。今後は、すべての ASAv で通過トラフィックがサポートされます。任意で、このインターフェイスを管理専用に設定できますが、デフォルトでは管理専用に設定されていません。 次のコマンドが変更されました。 **management-only**

機能	説明
コモン クライテリア証明書	ASA は、コモン クライテリアの要件に適合するように更新されました。この証明書に追加された次の機能については、この表の行を参照してください。 • ASDM での ASA SSL サーバ モード マッチング • SSL クライアントの RFC 6125 サポート： • セキュアな syslog サーバの接続とスマート ライセンシング接続のための参照 ID • ASA クライアントによるサーバ証明書の拡張キーの使用状況確認 • ASA が TLS1.1 と 1.2 の TLS クライアントとして動作する際の相互認証 • PKI デバッグ メッセージ • 暗号キー抹消検査 • IKEv2 の IPsec/ESP トランスポート モードのサポート • 追加された syslog メッセージ
ファイアウォール機能	
TCP 経由での DNS インスペクション	DNS over TCP トラフィック（TCP/53）を検査できるようになりました。 次のコマンドが追加されました。 **tcp-inspection**
MTP3 User Adaptation（M3UA）インスペクション	M3UA トラフィックを検査できるようになりました。また、ポイントコード、サービスインジケータ、およびメッセージのクラスとタイプに基づいてアクションを適用できるようになりました。 次のコマンドが追加または変更されました。**clear service-policy inspect m3ua** {**drops** | **endpoint** [*IP_address*]}、**inspect m3ua**、**match dpc**、**match opc**、**match service-indicator**、**policy-map type inspect m3ua**、**show asp table classify domain inspect-m3ua**、**show conn detail**、**show service-policy inspect m3ua** {**drops** | **endpoint** *IP_address*}、**ss7 variant**、**timeout endpoint**
Session Traversal Utilities for NAT（STUN）インスペクション	Cisco Spark を含む WebRTC アプリケーションの STUN トラフィックを検査できるようになりました。インスペクションでは、リターン トラフィックに必要なピンホールが開きます。 次のコマンドが追加または変更されました。**inspect stun**、**show conn detail**、**show service-policy inspect stun**

機能	説明
Cisco クラウド Web セキュリティのアプリケーション層健全性チェック	サーバが正常かどうかを判断する際に、クラウド Web セキュリティアプリケーションの健全性をチェックするように Cisco クラウド Web セキュリティを設定できるようになりました。アプリケーションの健全性を確認することで、プライマリ サーバが TCP スリーウェイ ハンドシェイクに応答する場合に、システムはバックアップ サーバにフェールオーバーできますが、要求を処理することはできません。これにより、より信頼性の高いシステムを実現します。 次のコマンドが追加されました。**health-check application url**、**health-check application timeout**
ルートの収束に対する接続ホールドダウン タイムアウト	接続で使用されているルートがもう存在していない、または非アクティブになったときに、システムが接続を保持する時間を設定できるようになりました。このホールドダウン期間内にルートがアクティブにならない場合、接続は解放されます。ルートの収束がさらに迅速に行われるようにホールドダウン タイマーを短縮することができます。ただし、ほとんどのネットワークでは、ルートのフラッピングを防止するためにデフォルトの 15 秒が適切です。 次のコマンドが追加されました。 **timeout conn-holddown** バージョン *9.4(3)* でも同様です。
TCP オプション処理の変更	TCP マップを設定する際にパケットの TCP ヘッダー内の TCP MSS および MD5 オプションに対するアクションを指定できるようになりました。さらに、MSS、タイムスタンプ、ウィンドウ サイズ、および選択的確認応答オプションのデフォルトの処理が変更されました。以前は、これらのオプションは、ヘッダーに特定のタイプのオプションが 2 つ以上ある場合でも許可されていました。現在は、パケットに特定のタイプのオプションが 2 つ以上含まれている場合、そのパケットはデフォルトでドロップされます。たとえば、以前は 2 つのタイムスタンプ オプションがあるパケットは許可されていましたが、現在はドロップされます。 MD5、MSS、選択的確認応答、タイムスタンプ、およびウィンドウ サイズに対し、同じタイプの複数のオプションを有効にするための TCP マップを設定できます。MD5 オプションの場合、以前のデフォルトではオプションがクリアされたのに対し、現在のデフォルトでは許可されます。また、MD5 オプションを含むパケットをドロップすることもできます。MSS オプションの場合は、TCP マップで最大セグメント サイズを設定できます（トラフィック クラスごとに）。他のすべての TCP オプションのデフォルトに変更はありません。これらはクリアされます。 次のコマンドが変更されました。 **tcp-options**
トランスペアレント モードで、ブリッジ グループごとのインターフェイス数が最大で 64 に増加	ブリッジ グループあたりのインターフェイスの最大数が 4 から 64 に拡張されました。 変更されたコマンドはありません。

機能	説明
トランスペアレント モードでのマルチキャスト接続のフロー オフロードのサポート	トランスペアレント モードの Firepower 4100 および 9300 シリーズ デバイスで、NIC に直接切り替えられるマルチキャスト接続をオフロードできるようになりました。マルチキャスト オフロードは、インターフェイスを 2 つだけ含むブリッジ グループに使用できます。 この機能には、新規のコマンドまたは ASDM 画面はありません。
カスタマイズ可能な ARP レート制限	1 秒あたり許可される ARP パケットの最大数を設定できます。デフォルト値は ASA モデルによって異なります。この値は ARP ストーム攻撃を防ぐためにカスタマイズできます。 次のコマンドを追加しました。**arp rate-limit**、**show arp rate-limit**
IEEE 802.2 論理リンク制御（LLC）パケットの Destination Service Access Point（DSAP）アドレスに対する Ethertype ルールのサポート	IEEE 802.2 論理リンク制御パケットの宛先サービス アクセス ポイントのアドレスに対する Ethertype のアクセス制御ルールを作成できるようになりました。この追加により、**bpdu** キーワードが対象トラフィックに一致しなくなります。**dsap 0x42** に対して **bpdu** ルールを書き換えます。 次のコマンドが変更されました。 **access-list ethertype**
リモート アクセス機能	
マルチ コンテキスト モードの場合の証明書の事前入力/ユーザ名	AnyConnect SSL サポートが拡張され、これまでシングル モードでのみ使用可能だった証明書の事前入力とユーザ名取得機能の CLI がマルチコンテキストモードでも有効にできるようになりました。 変更されたコマンドはありません。
リモート アクセス VPN のフラッシュ仮想化	マルチ コンテキスト モードのリモート アクセス VPN はフラッシュ仮想化をサポートします。使用可能な合計フラッシュに基づき、コンテキストごとにプライベート記憶域と共有ストレージの場所が設定できます。 • プライベート記憶域：該当ユーザのみに関連付けられ、該当ユーザ対象コンテンツ固有のファイルを保存します。 • 共有ストレージ：有効になると、この領域にファイルがアップロードされ、あらゆるユーザ コンテキストが読み取り/書き込みできるようこの領域へのアクセスが許可されます。 次のコマンドが導入されました。**limit-resource storage**、**storage-url**
マルチ コンテキスト モードでの AnyConnect クライアント プロファイルのサポート	マルチ コンテキスト モードで AnyConnect クライアント プロファイルがサポートされました。ASDM を使用して新しいプロファイルを追加するには、AnyConnect セキュア モビリティ クライアント リリース 4.2.00748 または 4.3.03013 以降が必要です。

機能	説明
マルチ コンテキスト モードの AnyConnect 接続のステートフル フェールオーバー	マルチ コンテキスト モードで AnyConnect 接続のステートフル フェールオーバーがサポートされました。 変更されたコマンドはありません。
マルチ コンテキスト モードでリモート アクセス VPN ダイナミック アクセス ポリシー（DAP）がサポートされました。	マルチ コンテキスト モードで、コンテキストごとに DAP を設定できるようになりました。 変更されたコマンドはありません。
マルチ コンテキスト モードでリモート アクセス VPN CoA（認可変更）がサポートされました。	マルチ コンテキスト モードで、コンテキストごとに CoA を設定できるようになりました。 変更されたコマンドはありません。
マルチ コンテキスト モードで、リモート アクセス VPN のローカライズがサポートされました。	ローカリゼーションがグローバルでサポートされました。複数のコンテキストで共有されるローカリゼーション ファイル セットは 1 つだけです。 変更されたコマンドはありません。
Umbrella ローミング セキュリティ モジュールのサポート	アクティブな VPN がない場合には、DNS 層のセキュリティを強化するため、AnyConnect セキュア モビリティ クライアントの Umbrella ローミング セキュリティ モジュールを設定できます。 変更されたコマンドはありません。
IKEv2 の IPsec/ESP トランスポート モードのサポート	ASA IKEv2 ネゴシエーションでトランスポート モードがサポートされるようになりました。これは、トンネル（デフォルト）モードの代わりに使用できます。トンネル モードでは IP パケット全体がカプセル化されます。トランスポート モードでは IP パケットの上位層プロトコルだけがカプセル化されます。トランスポート モードでは、送信元ホストと宛先ホストの両方が IPSec をサポートしている必要があります。また、トランスポート モードは、トンネルの宛先ピアが IP パケットの最終宛先である場合にだけ使用されます。 次のコマンドが変更されました。**crypto map set ikev2 mode**
IPsec 内部パケットに対するパケット単位のルーティング ルックアップ	デフォルトでは、外部 ESP パケットに対してはパケット単位の隣接関係（アジャセンシー）ルックアップが行われ、IPsec トンネル経由で送信されるパケットに対してはルックアップが行われません。一部のネットワーク トポロジでは、ルーティング アップデートによって内部パケットのパスが変更され、ローカル IPsec トンネルが引き続きアップ状態である場合、トンネル経由のパケットは正しくルーティングされず、宛先に到達しません。これを防止するには、新しいオプションを使用し、IPsec 内部パケットに対してパケット単位のルーティング ルックアップを有効にします。 次のコマンドが追加されました。**crypto ipsec inner-routing-lookup**
証明書とセキュアな接続の機能	

機能	説明
ASA クライアントによるサーバ証明書の拡張キーの使用状況確認	syslog、スマート ライセンス サーバ証明書は、[Extended Key Usage] フィールドに [ServerAuth] を含める必要があります。そうしない場合、接続は失敗します。
ASA が TLS1.1 と 1.2 の TLS クライアントとして動作する際の相互認証	サーバが認証のために ASA からクライアント証明書を要求した場合、ASA はそのインターフェイス用に設定されたクライアント アイデンティティ証明書を送信します。証明書は **ssl trust-point** コマンドで設定されます。
PKI デバッグ メッセージ	ASA PKI モジュールは、SCEP 登録、HTTP を使用した失効チェックなどのために CA サーバへ接続します。これらすべての ASA PKI 通信はデバッグ追跡のため、debug crypto ca メッセージ 5 を付してログに記録されます。
ASDM での ASA SSL サーバ モード マッチング	証明書マップと照合するために、証明書で認証を行う ASDM ユーザに対して証明書を要求できるようになりました。 次のコマンドを変更しました。**http authentication-certificate match**
セキュアな syslog サーバの接続とスマート ライセンシング接続のための参照 ID	TLS クライアント処理は、RFC 6125 のセクション 6 に定義されるサーバ ID の検証ルールをサポートするようになりました。ID 確認は syslog サーバとスマート ライセンス サーバへの TLS 接続の PKI 確認中に行われます。提示された ID が設定されたリファレンス ID と一致しない場合、接続を確立できません。 次のコマンドが追加または変更されました。**crypto ca reference-identity**、**logging host**、**call home profile destination address**
暗号キー抹消検査	ASA の暗号化システムは、新しい暗号キー抹消要件に適合するように更新されました。キーはすべてゼロで上書きされ、データを読み出して上書きが正しく行われたか確認する必要があります。
SSH 公開キー認証の改善	以前のリリースでは、ローカル ユーザ データベース（**(aaa authentication ssh console LOCAL)**）を使用して AAA SSH 認証を有効にしなくても、SSH 公開キー認証（**(ssh authentication)**）を有効にすることができました。この設定は修正されたため、AAA SSH 認証を明示的に有効にする必要があります。ユーザが秘密キーの代わりにパスワードを使用できないよう、パスワード未定義のユーザ名を作成できるようになりました。 次のコマンドが変更されました。**ssh authentication**、**username**
インターフェイス機能	
Firepower 4100/9300 シャーシの ASA のMTU サイズ増加	Firepower 4100 および 9300 で、最大 MTU を 9188 バイトに設定できます。これまでは 9000 バイトが最大でした。この MTU は FXOS 2.0.1.68 以降でサポートされます。 次のコマンドが変更されました。**mtu**
ルーティング機能	

機能	説明
Bidirectional Forwarding Detection（BFD）のサポート	ASAは、BFD ルーティング プロトコルをサポートするようになりました。BFD テンプレート、インターフェイスおよびマッピングの設定が新たにサポートされました。BFD を使用するための BGP ルーティング プロトコルのサポートも追加されました。 次のコマンドが追加または変更されました。**authentication**、**bfd echo**、**bfd interval**、**bfd map**、**bfd slow-timers**、**bfd template**、**bfd-template**、**clear bfd counters**、**echo**、**debug bfd**、**neighbor fall-over bfd**、**show bfd drops**、**show bfd map**、**show bfd neighbors**、**show bfd summary**
IPv6 DHCP	ASA で IPv6 アドレッシングの次の機能がサポートされました。 • DHCPv6 アドレス クライアント：ASA は DHCPv6 サーバから IPv6 グローバル アドレスとオプションのデフォルト ルートを取得します。 • DHCPv6 プレフィックス委任クライアント：ASA は DHCPv6 サーバから委任プレフィックスを取得します。ASA は、これらのプレフィックスを使用して他の ASA インターフェイスのアドレスを設定し、ステートレス アドレス自動設定（SLAAC）クライアントが同じネットワーク上で IPv6 アドレスを自動設定できるようにします。 • 委任プレフィックスの BGP ルータ アドバタイズメント • DHCPv6 ステートレス サーバ：SLAAC クライアントが ASA に情報要求（IR）パケットを送信すると、ASA はドメインインネームなどの他の情報を SLAAC クライアントに提供します。ASA は、IR パケットを受け取るだけで、クライアントにアドレスを割り当てません。 次のコマンドが追加または変更されました。**clear ipv6 dhcp statistics**、**domain-name**、**dns-server**、**import**、**ipv6 address autoconfig**、**ipv6 address dhcp**、**ipv6 dhcp client pd**、**ipv6 dhcp client pd hint**、**ipv6 dhcp pool**、**ipv6 dhcp server**、**network**、**nis address**、**nis domain-name**、**nisp address**、**nisp domain-name**、**show bgp ipv6 unicast**、**show ipv6 dhcp**、**show ipv6 general-prefix**、**sip address**、**sip domain-name**、**sntp address**
ハイ アベイラビリティとスケーラビリティの各機能	
アクティブ/スタンバイ フェールオーバーを使用するとき、AnyConnect からのダイナミック ACL の同期時間が改善されました。	フェールオーバー ペアで AnyConnect を使用するとき、関連付けられているダイナミック ACL（dACL）のスタンバイ ユニットへの同期時間が改善されました。以前は、大規模な dACL の場合、スタンバイユニットが可用性の高いバックアップを提供するのではなく同期作業で忙しい間は、同期時間が長時間に及ぶことがありました。 変更されたコマンドはありません。
ライセンシング機能	

機能	説明
ASAv の永続ライセンス予約	Cisco Smart Software Manager との通信が許可されていない非常にセキュアな環境では、ASAv 用に永続ライセンスを要求できます。9.6(2) では、Amazon Web サービスの ASAv 向けに、この機能のサポートが追加されました。この機能は Microsoft Azure ではサポートされません。 （注） すべてのアカウントがパーマネント ライセンスの予約について承認されているわけではありません。設定を開始する前にこの機能についてシスコの承認があることを確認します。 次のコマンドが導入されました。**license smart reservation**、**license smart reservation cancel**、**license smart reservation install**、**license smart reservation request universal**、**license smart reservation return** バージョン *9.5(2.200)* でも同様です。
ASAv のサテライト サーバのサポート	デバイスがセキュリティ上の理由でインターネットにアクセスができない場合、オプションで、仮想マシン（VM）としてローカル Smart Software Manager サテライト サーバをインストールできます。 変更されたコマンドはありません。
ASAv の短かい文字列の拡張機能向けの永続ライセンス予約	スマート エージェント（1.6.4 への）の更新により、要求と認証コードには短い文字列が使用されます。 変更されたコマンドはありません。
Firepower 4100/9300 シャーシ 上の ASA の永続ライセンス予約	Cisco Smart Software Manager との通信が許可されていない非常にセキュアな環境では、FirePOWER 9300 および FirePOWER 4100 の ASA 用に永続ライセンスを要求できます。永続ライセンスには、標準層、高度暗号化（該当する場合）、セキュリティ コンテキスト、キャリア ライセンスをはじめ、使用可能なすべてのライセンス権限が含まれます。FXOS 2.0.1 が必要です。 すべての設定はFirepower 4100/9300 シャーシで実行され、ASA の設定は不要です。

機能	説明
ASAv 用スマート エージェントの v1.6 へのアップグレード	スマート エージェントはバージョン 1.1 からバージョン 1.6 へアップグレードされました。このアップグレードは永続ライセンス予約をサポートするほか、ライセンス アカウントに設定された権限に従って、高度暗号化（3DES/AES）ライセンス権限の設定もサポートします。 （注） バージョン 9.5 （2.200）からダウングレードした場合、ASAv はライセンス登録状態を保持しません。**license smart register idtoken** *id_token* **force** コマンドを使用し、再登録する必要があります。Smart Software Manager から ID トークンを取得します。 次のコマンドが導入されました。**show license status**、**show license summary**、**show license udi**、**show license usage** 次のコマンドが変更されました。**show license all**、**show tech-support license** 次のコマンドが非推奨になりました。 **show license cert**、**show license entitlement**、**show license pool**、**show license registration** バージョン *9.5(2.200)* でも同様です。
モニタリング機能	
type asp-drop のパケット キャプチャは、ACL と一致フィルタリングをサポートします。	asp-drop タイプのパケット キャプチャを作成するとき、ACL または一致するオプションを指定してキャプチャの範囲を制限できるようになりました。 次のコマンドが変更されました。**capture type asp-drop**
フォレンジック分析の強化	ASA で実行されているすべてのプロセスのコア ダンプを作成できます。主な ASA プロセスのテキスト セクションを抽出し、検証用にコピーできます。 次のコマンドが変更されました。**copy system:text**、**verify system:text**、**crashinfo force dump process**
NetFlow経由の接続ごとのトラッキング パケット数の追跡	NetFlow ユーザがある接続上で双方向に送受信されるレイヤ 4 パケットの数を確認することを可能にする 2 つのカウンタが追加されました。これらのカウンタを使用して、平均パケット レートおよびサイズを判断し、トラフィック タイプ、異常、イベントをより適切に予測できます。 変更されたコマンドはありません。

機能	説明
フェールオーバーの SNMP engineID の同期	フェールオーバー ペアでは、一対の ASA の SNMP engineID は両方のユニットで同期されます。ASA ごとに、同期された engineID、ネイティブ engineID、およびリモート engineID による engineID が 3 セット維持されます。 SNMPv3 ユーザは、ローカライズされた **snmp-server user** 認証とプライバシー オプションを保存するためのプロファイルを作成するときに ASA の engineID も指定できます。ユーザがネイティブ engineID を指定しない場合、**show running config** 出力に engineID がユーザごとに 2 つずつ表示されます。 次のコマンドが変更されました。**snmp-server user** バージョン *9.4(3)* でも同様です。

ASA 9.6(1) の新機能

リリース：2016年3月21日

（注） Microsoft Azure サポートを含む ASAv 9.5.2(200) の各機能は 9.6(1) では使用できません。 これらは、9.6(2) では使用可能です。

機能	説明
プラットフォーム機能	
Firepower 4100 シリーズ の ASA	Firepower 4110、4120、4140 用の ASA を導入しました。 FXOS 1.1.4 が必要です。 追加または変更されたコマンドはありません。
ISA 3000 の SD カードのサポート	ISA 3000 の外部ストレージとして SD カードが使用できるようになりました。カードは、ASA ファイル システムのディスク 3 として表示されます。プラグ アンド プレイをサポートするにはハードウェア バージョン 2.1 以降が必要です。ハードウェア バージョンをチェックするには、**show module** コマンドを使用します。 追加または変更されたコマンドはありません。
ISA 3000 のデュアル電源サポート	ISA 3000 のデュアル電源では、ASA OS に望ましい構成としてデュアル電源を設定できます。1 つの電源に障害が発生すると、ASA はアラームを発します。デフォルトでは、ASA は単一電源を想定していますが、装備される電源のいずれかが機能しているかぎりアラームを発しません。 次のコマンドが導入されました。**power-supply dual**。
ファイアウォール機能	

機能	説明
Diameter インスペクションの改善	TCP/TLS トラフィック上の Diameter を検査し、厳密なプロトコル準拠チェックを適用し、クラスタ モードで SCTP 上の Diameter を検査できるようになりました。 次のコマンドが導入または変更されました。**client clear-text**、**inspect diameter**、**strict-diameter**。
クラスタ モードでの SCTP ステートフル インスペクション	SCTP ステートフル インスペクションがクラスタ モードで動作するようになりました。また、クラスタ モードで SCTP ステートフル インスペクション バイパスを設定することもできます。 追加または変更されたコマンドはありません。
H.460.18 互換性に関連する H.225 SETUP メッセージの前に着信する H.255 FACILITY メッセージに対する H.323 インスペクションのサポート。	H.225 FACILITY メッセージが H.225 SETUP メッセージの前に着信する（これは、エンドポイントが H.460.18 に準拠する場合に発生する場合があります）ことを許可するように H.323 インスペクション ポリシー マップを設定できるようになりました。 次のコマンドが導入されました。**early-message**。
Security Exchange Protocol（SXP）バージョン 3 の Cisco TrustSec サポート。	ASA の Cisco Trustsec は、ホスト バインディングよりも効率的な SGT とサブネット間のバインディングを可能にする SXPv3 を実装するようになりました。 次のコマンドが導入または変更されました。**cts sxp mapping network-map** *maximum_hosts*、**cts role-based sgt-map**、**show cts sgt-map**、**show cts sxp sgt-map**、**show asp table cts sgt-map**。
Firepower 4100 シリーズのフローオフロードのサポート。	ASA からオフロードされ、Firepower 4100 シリーズの NIC で直接切り替える必要があるフローを特定できるようになりました。 FXOS 1.1.4 が必要です。 追加または変更されたコマンドはありません。
リモート アクセス機能	
IKEv2 フラグメンテーション、RFC-7383 サポート	ASA では、IKEv2 パケットのこの標準的なフラグメンテーションがサポートされるようになりました。これにより、Apple、Strongswan など、他の IKEv2 の実装との相互運用性を実現します。ASA は、AnyConnect クライアントなどの RFC-7383 をサポートしないシスコ製品との後方互換性を保つため、独自の IKEv2 フラグメンテーションを引き続きサポートします。 次のコマンドが導入されました。 **crypto ikev2 fragmentation**、**show running-config crypto ikev2**、**show crypto ikev2 sa detail**
Firepower 9300 と Firepower 4100 シリーズでの VPN スループット パフォーマンス強化	**crypto engine accelerator-bias** コマンドが Firepower 9300 と Firepower 4100 シリーズ上の ASA セキュリティ モジュールでサポートされるようになりました。このコマンドにより、IPSec または SSL に対して暗号コアを「優先的に使用」できます。 次のコマンドが変更されました。 **crypto engine accelerator-bias**

機能	説明
設定可能な SSH 暗号機能と HMAC アルゴリズム	ユーザはSSH暗号化を管理するときに暗号化モードを選択し、さまざまなキー交換アルゴリズムに対して HMAC と暗号化を設定できます。アプリケーションに応じて、暗号の強度を強くしたり弱くする必要がある場合があります。セキュアなコピーのパフォーマンスは暗号化アルゴリズムに一部依存します。デフォルトで、ASA は 3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr の順にアルゴリズムをネゴシエートします。提示された最初のアルゴリズム（3des-cbc）が選択された場合、aes128-cbc などの一層効率的なアルゴリズムが選択された場合よりも大幅にパフォーマンスが低下します。たとえば、提示された暗号方式に変更するには、**ssh cipher encryption custom aes128-cbc** を使用します。 次のコマンドが導入されました。**ssh cipher encryption**、**ssh cipher integrity**。 *9.1(7)* 、*9.4(3)* および *9.5(3)* でも使用可能です。
IPv6 の HTTP リダイレクト サポート	ASDM アクセスまたはクライアントレス SSL VPN 用の HTTPS に HTTP リダイレクトを有効にすると、IPv6アドレスへ送信されるトラフィックもリダイレクトできるようになりました。 次のコマンドに機能が追加されました。**http redirect** *9.1(7)* および *9.4(3)* でも使用可能です。
ルーティング機能	
IS-IS ルーティング	ASA で Intermediate System to Intermediate System（IS-IS）のルーティング プロトコルがサポートされました。IS-IS ルーティング プロトコルを使用した、データのルーティング、認証の実行、およびルーティング情報の再配布とモニタについて、サポートが追加されました。 次のコマンドを導入しました。 **advertise passive-only, area-password, authentication key, authentication mode, authentication send-only, clear isis, debug isis, distance, domain-password, fast-flood, hello padding, hostname dynamic, ignore-lsp-errors, isis adjacency-filter, isis advertise prefix, isis authentication key, isis authentication mode, isis authentication send-only, isis circuit-type, isis csnp-interval, isis hello-interval, isis hello-multiplier, isis hello padding, isis lsp-interval, isis metric, isis password, isis priority, isis protocol shutdown, isis retransmit-interval, isis retransmit-throttle-interval, isis tag, is-type, log-adjacency-changes, lsp-full suppress, lsp-gen-interval, lsp-refresh-interval, max-area-addresses, max-lsp-lifetime, maximum-paths, metric, metric-style, net, passive-interface, prc-interval, protocol shutdown, redistribute isis, route priority high, route isis, set-attached-bit, set-overload-bit, show clns, show isis, show router isis, spf-interval, summary-address.**
ハイ アベイラビリティとスケーラビリティの各機能	

機能	説明
ルーテッドおよびスパンド EtherChannel モードのサイト固有の IP アドレスのポート	スパンド EtherChannel のルーテッド モードでのサイト間クラスタリングの場合、サイト個別の MAC アドレスに加えて、サイト個別の IP アドレスを設定できるようになりました。サイト IP アドレスを追加することにより、グローバル MAC アドレスからの ARP 応答を防止するために、ルーティング問題の原因になりかねない Data Center Interconnect（DCI）経由の移動によるオーバーレイ トランスポート仮想化（OTV）デバイスの ARP 検査を使用することができます。MAC アドレスをフィルタ処理するために VACL を使用できないスイッチには、ARP 検査が必要です。 次のコマンドが変更されました。**mac-address**、**show interface**
管理機能	
ローカルの **username** および **enable** パスワードでより長いパスワード（127 文字まで）がサポートされます。	127 文字までのローカル **username** および **enable** パスワードを作成できます（以前の制限は 32 文字でした）。32 文字以上のパスワードを作成すると、PBKDF2（パスワードベース キー派生関数 2）のハッシュを使用して設定に保存されます。これよりも短いパスワードは引き続き MD5 ベースのハッシュを使用します。 次のコマンドを変更しました。**enable**、**username**
CISCO-ENHANCED-MEMPOOL-MIB の cempMemPoolTable のサポート	CISCO-ENHANCED-MEMPOOL-MIB の cempMemPoolTable がサポートされました。これは、管理型システムのすべての物理エンティティのメモリプール モニタリング エントリのテーブルです。 （注） CISCO-ENHANCED-MEMPOOL-MIB は 64 ビットのカウンタを使用して、プラットフォーム上の 4 GB 以上のメモリのレポーティングをサポートします。 追加または変更されたコマンドはありません。 *9.1(7)* および *9.4(3)* でも使用可能です。
REST API バージョン 1.3.1	REST API バージョン 1.3.1 のサポートが追加されました。

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 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 サーバまたは FTP サーバなど、外部のユーザ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 サーバと協調するといった手段

によって、内部ユーザ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したり、URL およびその他のフィルタリング サービス（ASA CX や ASA FirePOWER など）を提供する ASA モジュールをインストールすることができます。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。

サポート対象のハードウェアモジュールまたはソフトウェアモジュールへのトラフィックの送信

一部の ASA モデルでは、ソフトウェア モジュールの設定、またはハードウェア モジュールのシャーシへの挿入を行うことで、高度なサービスを提供することができます。これらのモジュールを通じてトラフィック インスペクションを追加することにより、設定済みのポリシーに基づいてトラフィックをブロックできます。また、これらのモジュールにトラフィックを送信することで、高度なサービスを利用することができます。

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
- Transparent

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。

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
- ユーザの認証
- ユーザ 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、マスター 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 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